



Konsep dan Prosedur Lanjutan AMS

Panduan Pengguna Tingkat Lanjut AMS



Versi October 3, 2025

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

Panduan Pengguna Tingkat Lanjut AMS: Konsep dan Prosedur Lanjutan AMS

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

Merek dagang dan tampilan dagang Amazon tidak dapat digunakan sehubungan dengan produk atau layanan yang bukan milik Amazon, dalam bentuk apa pun yang mungkin menimbulkan kebingungan di kalangan pelanggan, atau dalam bentuk apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan properti dari masing-masing pemilik, yang mungkin berafiliasi, terkait dengan, atau disponsori oleh Amazon, atau tidak.

Table of Contents

Apa itu AWS Managed Services?	1
Tentang panduan ini	2
Rencana operasi	2
Mempercepat rencana operasi	3
Rencana operasi lanjutan	3
Memulai	3
Istilah kunci	4
Deskripsi layanan	10
AWS Managed Services (AMS) AMS Fitur rencana operasi lanjutan	11
Apa yang kita lakukan, apa yang tidak kita lakukan	16
Matriks tanggung jawab AMS (RACI)	17
Komponen dasar lingkungan AMS	40
Batas akun AMS	43
Tujuan tingkat layanan AMS (SLOs)	45
AWS Layanan yang didukung	47
Konfigurasi yang didukung	50
Sistem operasi yang tidak didukung	52
Antarmuka AMS Lanjutan	53
Titik akhir VPC	54
Ruang nama yang dilindungi AMS	55
Awalan cadangan AMS	57
Jendela pemeliharaan AMS	58
Sumber informasi AMS	58
Kepatuhan AMS	59
Standar Kepatuhan yang Didukung AMS	59
Tanggung Jawab Bersama	63
Gambar Mesin AMS Amazon (AMIs)	63
Keamanan ditingkatkan AMIs	67
Cara kerja integrasi antara AD FS dan AMS	67
Direktori Aktif Terkelola AMS	68
Penerapan aplikasi	71
Manajemen layanan	73
Tata kelola akun	73
Dimulainya layanan	74

Manajemen hubungan pelanggan (CRM)	74
Proses CRM	75
Rapat CRM	76
Pengaturan Rapat CRM	77
Laporan bulanan CRM	78
Optimalisasi biaya	79
Kerangka kerja pengoptimalan biaya	79
Matriks tanggung jawab optimasi biaya	81
Jam layanan	83
Mendapatkan bantuan	84
Manajemen acara yang direncanakan	85
Kriteria AMS PEM	85
Jenis PEM	85
Proses AMS PEM	86
PEM FAQs	86
Arsitektur jaringan	88
Arsitektur jaringan MALZ	88
Tentang arsitektur jaringan landing zone multi-akun	88
Memilih MALZ tunggal atau ganda MALZs	90
Akun Zona Pendaratan Multi-Akun	96
Arsitektur jaringan SALZ	129
Layanan bersama landing zone akun tunggal AMS	130
Menyiapkan AMS	132
Pengaturan default AMS	133
Default resolusi DNS (MALZ)	133
EC2 Profil instans IAM	134
Peringatan dari pemantauan dasar di AMS	141
Retensi log dan default rotasi	159
Menggunakan konsol AMS	160
Menggunakan AMS API dan CLI	162
Titik akhir HTTP AMS API untuk panggilan REST	162
Menginstal atau memutakhirkan AMS CLI	162
Menggunakan AMS API di CLI, Ruby, Python, dan Java	164
AMS membawa EPS Anda sendiri	173
Aktifkan BYOEPS untuk akun Anda	175
Menerima pemberitahuan AMS	178

Pemberitahuan AMS AMI dengan SNS	179
Pemberitahuan layanan	183
Pemberitahuan perubahan status RFC	184
Menyiapkan DNS pribadi dan publik	187
Manajemen lalu lintas jalan keluar AMS	189
Menyebarkan sumber daya IAM	190
Penyediaan IAM Otomatis	191
Mengatur izin dengan peran dan profil IAM	214
Meminta peran pengguna IAM baru atau profil instans	214
Batasi izin dengan pernyataan kebijakan peran IAM	214
Batasi izin dengan profil instans Amazon EC2 IAM	216
Aturan klaim AD FS dan setelan SAMP	217
Konfigurasi aturan klaim ADFS	217
Konsol web	218
Akses API dan CLI dengan SAMP	218
Batasi dengan ACL jaringan	222
AMS di Outposts	222
AWS Outposts instalasi dan manajemen operasional	223
Menyediakan sumber daya terkelola AMS di AWS Outposts	225
Keterbatasan AMS pada AWS Outposts	226
AMS tentang AWS Outposts kepatuhan	227
AMS pada AWS Outposts FAQs	228
Menggunakan tanda	230
Penandaan otomatis infrastruktur AMS	231
Tag yang direkomendasikan AMS	233
Menandai catatan pembaruan massal	237
Penjadwal Sumber Daya	239
Menyebarkan Penjadwal Sumber Daya	240
Menyesuaikan Penjadwal Sumber Daya	240
Menggunakan Resource Scheduler	241
Penaksir biaya Penjadwal Sumber Daya AMS	241
Praktik terbaik Penjadwal Sumber Daya AMS	243
AWS Systems Manager di AMS Lanjutan	245
Dokumen SSM AMS Advanced yang tersedia	245
Versi dokumen SSM AMS Advanced	246
Harga Systems Manager	246

Akun AMS offboard	246
Offboard dari akun landing zone akun tunggal	247
Offboard dari akun landing zone multi-akun	251
Ubah mode manajemen	271
Ikhtisar mode	272
Jenis mode dan akun di AMS	273
Mode dan aplikasi AMS atau beban kerja	276
Kasus penggunaan dunia nyata untuk mode AMS	284
Modus RFC	287
Pelajari tentang RFCs	288
Apa itu jenis perubahan?	328
Memecahkan masalah kesalahan RFC	341
Mode Ubah Langsung	351
Memulai dengan mode Perubahan Langsung	352
Keamanan dan kepatuhan	355
Ubah manajemen dalam mode Perubahan Langsung	360
Membuat tumpukan menggunakan mode Perubahan Langsung	363
Kasus penggunaan Mode Perubahan Langsung	366
Mode pengembang	367
Memulai dengan mode Pengembang	368
Keamanan dan kepatuhan	370
Manajemen perubahan	372
Penyediaan infrastruktur	377
Kontrol detektif	378
Pencatatan, pemantauan, dan manajemen acara	378
Manajemen insiden	378
Manajemen tambalan	379
Manajemen kontinuitas	379
Keamanan dan manajemen akses	379
Mode Penyediaan Layanan Mandiri di AMS	380
Memulai dengan mode SSP di AMS	381
Amazon API Gateway	381
Alexa for Business	382
Amazon AppStream 2.0	384
Amazon Athena	386
Amazon Bedrock	387

Amazon CloudSearch	389
Amazon CloudWatch Synthetics	390
Amazon Cognito	391
Amazon Comprehend	393
Amazon Connect	394
Amazon Data Firehose	396
DevOpsGuru Amazon	397
Amazon DocumentDB (dengan kompatibilitas MongoDB)	398
Amazon DynamoDB	399
Amazon Elastic Container Registry	400
EC2 Image Builder	401
Amazon ECS aktif AWS Fargate	403
Amazon EKS di AWS Fargate	406
Amazon EMR	409
Amazon EventBridge	412
Amazon Forecast	414
Amazon FSx	417
Amazon FSx untuk OpenZFS	418
Amazon FSx untuk NetApp ONTAP	420
Amazon Inspector Klasik	421
Amazon Kendra	423
Amazon Kinesis Data Streams	423
Amazon Kinesis Video Streams	424
Amazon Lex	425
Amazon MQ	426
Layanan Terkelola Amazon untuk Apache Flink	427
Amazon Managed Streaming untuk Apache Kafka	428
Layanan Terkelola Amazon untuk Prometheus	430
Amazon Personalize	431
Amazon QuickSight	434
Amazon Rekognition	435
Amazon SageMaker AI	436
Layanan Email Sederhana Amazon	440
Layanan Alur Kerja Sederhana Amazon	441
Amazon Textract	442
Amazon Transcribe	443

Amazon WorkSpaces	444
Layanan Kode AMS	446
AWS Amplify	449
AWS AppSync	450
AWS App Mesh	451
AWS Audit Manager	452
AWS Batch	453
AWS Certificate Manager	455
AWS Private Certificate Authority	456
AWS CloudEndure	459
AWS CloudHSM	460
AWS CodeBuild	462
AWS CodeCommit	463
AWS CodeDeploy	465
AWS CodePipeline	466
AWS Compute Optimizer	468
AWS DataSync	469
AWS Device Farm	470
AWS Elastic Disaster Recovery	471
AWS Elemental MediaConvert	472
AWS Elemental MediaLive	473
AWS Elemental MediaPackage	474
AWS Elemental MediaStore	475
AWS Elemental MediaTailor	476
AWS Global Accelerator	477
AWS Glue	478
AWS Lake Formation	479
AWS Lambda	481
AWS License Manager	482
AWS Migration Hub	483
AWS Outposts	484
AWS Resilience Hub	485
AWS Secrets Manager	486
AWS Security Hub	489
AWS Service Catalog AppRegistry	490
AWS Shield	491

AWS Snowball Edge	492
AWS Step Functions	494
AWS Systems Manager Toko Parameter	495
AWS Systems Manager Otomasi	496
AWS Transfer Family	499
AWS Transit Gateway	501
AWS WAF	502
AWS Well-Architected Tool	503
AWS X-Ray	504
VM Import/Export	505
Modus Dikelola Pelanggan	506
Memulai mode Customer Managed	507
AMS dan AWS Service Catalog	507
Memulai Service Catalog	508
Service Catalog di AMS sebelum Anda mulai	508
Menemukan data yang Anda butuhkan (SKMS)	512
Apa itu manajemen pengetahuan layanan?	512
Temukan VPC IDs	513
Temukan subnet IDs	515
Temukan AMI IDs	518
Temukan grup keamanan (SG) IDs	519
Temukan entitas IAM	519
Temukan tumpukan IDs	520
Temukan contoh IDs atau alamat IP	522
Menemukan ARNs	525
Temukan sumber daya oleh ARN	526
Temukan pengaturan akun	528
Menemukan FQDNs	529
Temukan zona ketersediaan (AZs)	530
Temukan topik SNS	531
Temukan pengaturan cadangan	531
Manajemen akses	532
Apa itu Manajemen Akses?	532
Mengapa dan kapan kami mengakses akun Anda	533
Bagaimana dan kapan menggunakan root	538
Konsol AMS Advanced dan EC2 akses Amazon	539

Mengakses konsol AWS Manajemen dan konsol AMS	540
Akses konsol AMS sementara	540
Mengakses instance menggunakan benteng	541
Nama benteng ramah DNS	543
Menghemat biaya pada benteng single-account landing zone (SALZ)	544
Menggunakan alamat IP bastion	545
Contoh akses instans	546
Kontrol akses berbasis tim, atau peran, di akun AMS	556
Konfigurasi EC2 instans otomatis	557
Prasyarat untuk konfigurasi instans otomatis	557
Instalasi otomatis Agen SSM	558
Prasyarat	558
Minta instalasi otomatis Agen SSM	559
Cara kerja instalasi otomatis Agen SSM	559
Perubahan otomatis	560
Secara otomatis memperbarui kode pada instance Linux	560
Secara otomatis memperbarui PBIS pada instance Linux	561
Secara otomatis memperbarui versi minimum SSM dan agen CloudWatch	562
CloudWatch file konfigurasi, perbarui detail	563
Log yang dikonfigurasi secara otomatis	563
Pemantauan dan manajemen acara	565
Apa itu pemantauan?	566
Apa yang dipantau oleh sistem pemantauan AMS?	567
Pemantauan proaktif Zona Pendaratan Akun Tunggal dari Active Directory Trust	568
Cara kerja pemantauan	568
EC2 pemberitahuan yang dikelompokkan misalnya	570
Pemberitahuan peringatan berbasis tag	571
Melihat konfigurasi pemantauan untuk akun	572
Mengubah konfigurasi pemantauan untuk akun	572
Pemberitahuan insiden sadar aplikasi di AMS	573
Penyediaan AppRegistry di akun AMS Anda dan buat aplikasi	573
Buat tag untuk mengaktifkan pengayaan kasus	573
Sesuaikan tingkat keparahan kasus dukungan AMS untuk aplikasi Anda	574
Tinjau izin yang diperlukan	575
Menggunakan OpsCenter	575
Pemberitahuan peringatan	576

Menerima peringatan	576
Pemberitahuan peringatan berbasis tag	577
Remediasi peringatan otomatis AMS	578
Membuat CloudWatch alarm tambahan	587
Membuat CloudWatch metrik dan alarm khusus	588
Menggunakan Wawasan CloudWatch Aplikasi untuk server .Net dan SQL	590
Router Acara AMS	590
Aturan EventBridge Terkelola Amazon yang diterapkan oleh AMS	591
Membuat Aturan Terkelola untuk AMS	591
Mengedit Aturan Terkelola untuk AMS	591
Menghapus Aturan Terkelola untuk AMS	592
Remediator Tepercaya	592
Manfaat utama	592
Cara kerja Remediator Tepercaya	593
Istilah kunci	593
Memulai dengan Remediator Tepercaya	595
Rekomendasi Compute Optimizer yang Didukung	598
Trusted Advisor Cek yang didukung	601
Konfigurasikan remediasi cek	659
Alur kerja keputusan mode eksekusi	663
Konfigurasikan tutorial remediasi	663
Bekerja dengan remediasi	666
Log remediasi	670
Praktik terbaik	673
FAQs	673
Manajemen log	676
Apa itu manajemen log?	676
Cara kerja pencatatan AMS	676
Mengakses log Anda	677
Log layanan agregat AMS	677
Log layanan bersama AMS	690
Amazon Elastic Compute Cloud (Amazon EC2) - log tingkat sistem	693
Integrasi dengan Splunk	694
Menyesuaikan konfigurasi log Anda	695
Mengubah retensi CloudWatch log	695
Mengaktifkan pencatatan untuk layanan yang didukung	695

Manajemen keamanan	696
Perlindungan data di AMS	696
Amazon Macie	697
GuardDuty	699
Amazon Route 53 Resolver DNS Firewall	701
AWS Certificate Manager Sertifikat (ACM)	703
Enkripsi data di AMS	703
Manajemen identitas dan akses	705
Pengamanan IAM Zona Pendaratan Multi-Akun (MALZ)	705
Mengautentikasi dengan identitas	706
Pencatatan dan pemantauan peristiwa keamanan	728
Keamanan Titik Akhir (EPS)	728
Proses mitigasi malware	733
Keamanan Amazon Inspector	734
Tanggapan insiden AMS	736
Validasi kepatuhan	737
Zona Pendaratan Multi-Akun yang melihat status kepatuhan Anda Aturan AWS Config	738
Pembatasan kebijakan kontrol layanan landing zone multi-akun AMS	739
Ketahanan	739
Keamanan infrastruktur	739
Praktik terbaik keamanan	772
Pengaturan non-default EPS landing zone multi-akun AMS	772
Pagar Pembatas AMS	772
Kebijakan kontrol layanan MALZ	772
Respons Insiden Keamanan	772
Cara kerjanya	773
Persiapkan	774
Mendeteksi	775
Analisis	775
Mengandung	776
Membasmi	779
Memulihkan	779
Laporan Pasca Insiden	780
Runbook Respons Insiden Keamanan	781
Ubah ulasan keamanan permintaan di AMS Advanced	786
Proses Manajemen Risiko Keamanan Pelanggan	787

AMS Standar teknis lanjutan	788
Kontrol standar di AMS Advanced	788
Perubahan yang menimbulkan risiko keamanan tinggi atau sangat tinggi di lingkungan Anda	813
Manajemen kontinuitas	817
Apa itu manajemen kontinuitas?	817
Bagaimana manajemen kontinuitas bekerja	817
Rencana pencadangan	818
Vault pencadangan	821
Jenis perubahan Backup	822
Pemantauan dan pelaporan untuk cadangan	823
Respon pemulihan bencana	824
Perencanaan pemulihan bencana	824
Multi-situs atau sangat tersedia (HA)	825
Warm standby	826
Pilot light	827
Pencadangan dan pemulihan	828
Manajemen tambalan	833
AMS Patch Orchestrator: model patching berbasis tag	834
Menggunakan Patch Orchestrator	836
Prasyarat Patch Orchestrator	839
Jendela tambalan	841
Pemberitahuan tambalan	841
Garis dasar patch	844
Tag yang dicadangkan Patch Orchestrator	844
Penambalan sesuai permintaan	845
Penambalan standar AMS	845
Sistem operasi yang didukung	847
Patch yang didukung	847
Patching dan desain infrastruktur	850
Cara kerja patching standar AMS	850
Kegagalan penambalan standar AMS	856
Tindakan yang dapat Anda lakukan dalam penambalan standar AMS	856
Penambalan standar AMS FAQs	860
Menambal komitmen layanan	862
Penambalan standar	862

Penambalan kritis	865
Laporan dan opsi	869
Laporan berdasarkan permintaan	869
Laporan AMS Patch	870
Laporan Cadangan AMS	879
Insiden Mencegah dan Memantau Laporan Pembicara Teratas	881
Laporan Detail Biaya Penagihan	883
Laporan Remediator Tepercaya	885
Laporan layanan mandiri	888
Operasi API internal	889
Laporan patch (harian)	892
Laporan Backup (harian)	902
Laporan insiden (mingguan)	905
Laporan penagihan (bulanan)	909
Laporan agregat	912
Dasbor laporan layanan mandiri AMS	914
Kebijakan retensi data	921
Offboard dari SSR	922
Dapatkan dukungan	923
Manajemen insiden	923
Apa itu manajemen insiden?	925
Komitmen layanan manajemen insiden	926
Contoh manajemen insiden	929
Manajemen permintaan layanan	935
Kapan menggunakan permintaan layanan	936
Cara kerja manajemen permintaan layanan	937
Menguji permintaan layanan	937
Membuat permintaan layanan	938
Memantau dan memperbaiki permintaan layanan	940
Menanggapi permintaan layanan yang dihasilkan AMS	942
Pertanyaan penagihan	942
Operasi Sesuai Permintaan	944
Meminta Operasi AMS Sesuai Permintaan	953
Membuat perubahan pada penawaran Operations on Demand	954
Riwayat dokumen	955
Pembaruan lebih awal	972

..... mii

Apa itu AWS Managed Services?

Selamat datang di AWS Managed Services (AMS), manajemen operasi infrastruktur untuk Amazon Web Services (AWS). AMS adalah layanan perusahaan yang menyediakan manajemen AWS infrastruktur Anda secara berkelanjutan.

Panduan pengguna ini ditujukan untuk profesional pengembang TI dan aplikasi. Pemahaman dasar tentang fungsionalitas TI, jaringan, dan istilah dan praktik penyebaran aplikasi diasumsikan.

AMS menerapkan praktik terbaik dan memelihara infrastruktur Anda untuk mengurangi overhead dan risiko operasional Anda. AMS menyediakan layanan siklus hidup penuh untuk menyediakan, menjalankan, dan mendukung infrastruktur Anda, serta mengotomatiskan aktivitas umum seperti permintaan perubahan, pemantauan, manajemen tambalan, keamanan, dan layanan pencadangan. AMS memberlakukan kebijakan infrastruktur perusahaan dan keamanan Anda, dan memungkinkan Anda mengembangkan solusi dan aplikasi menggunakan pendekatan pengembangan pilihan Anda.

Untuk lebih memahami arsitektur AMS, lihat [diagram ini](#).

Topik

- [Tentang panduan pengguna AMS ini](#)
- [Rencana operasi AMS](#)
- [Memulai AWS Managed Services](#)
- [Istilah kunci AMS](#)
- [Deskripsi layanan](#)
- [Sumber informasi AMS](#)
- [Kepatuhan AMS](#)
- [Gambar Mesin AMS Amazon \(AMIs\)](#)
- [Cara kerja integrasi antara AD FS dan AMS](#)
- [Direktori Aktif Terkelola AMS](#)
- [Penerapan aplikasi AMS](#)

Note

Baru Wilayah AWS sering ditambahkan. Untuk sistem operasi terbaru yang didukung AMS Wilayah AWS, dan sistem operasi terbaru yang didukung AMS, lihat [Konfigurasi yang didukung](#)

Untuk mempelajari selengkapnya Wilayah AWS, lihat [Mengelola Wilayah AWS](#).

AMS berusaha untuk terus meningkatkan layanan kami berdasarkan umpan balik Anda. Kami menggunakan beberapa mekanisme untuk mengaktifkan layanan mandiri Anda, untuk mengotomatiskan tugas berulang, dan untuk mengimplementasikan fitur baru Layanan AWS dan saat dirilis. Anda dapat mengirimkan permintaan layanan AMS kapan saja untuk menyarankan fitur baru atau peningkatan fitur.

Jam kerja AMS adalah 24 jam sehari, 7 hari seminggu, 365 hari setahun.

AMS mengikuti serangkaian praktik untuk manajemen layanan TI (ITSM) yang berfokus pada penyelarasan layanan TI dengan kebutuhan bisnis Anda.

Tentang panduan pengguna AMS ini

Panduan pengguna ini ditujukan untuk pelanggan AMS Advanced dengan landing zone multi-akun atau single-account. Untuk detail selengkapnya tentang penawaran landing zone AMS, lihat [Ketentuan Utama AMS](#); lihat juga arsitektur Zona Pendaratan [Multi-Akun dan arsitektur Zona Pendaratan Akun Tunggal](#).

Rencana operasi AMS

AWS Managed Services (AMS) tersedia dengan dua paket operasi: AMS Accelerate dan AMS Advanced. Rencana operasi menawarkan serangkaian fitur tertentu dan memiliki tingkat layanan, kemampuan teknis, persyaratan, harga, dan batasan yang berbeda. Rencana operasi kami memberi Anda fleksibilitas untuk memilih kemampuan operasional berukuran tepat untuk setiap beban AWS kerja Anda. Bagian ini menguraikan kemampuan dan perbedaan, serta tanggung jawab, fitur, dan manfaat yang terkait dengan setiap rencana, sehingga Anda dapat memahami rencana operasi mana yang terbaik untuk akun Anda.

Untuk perbandingan fitur mendetail dari dua paket operasi, lihat [Fitur AWS Managed Services](#).

AMS Mempercepat rencana operasi

AMS Accelerate adalah rencana operasi AMS yang membantu Anda mengoperasikan manajemen day-to-day infrastruktur AWS lingkungan baru atau yang sudah ada. AMS Accelerate menyediakan layanan operasional, seperti pemantauan, manajemen insiden, dan keamanan. AMS Accelerate juga menawarkan add-on patch opsional untuk beban kerja EC2 berbasis Amazon yang memerlukan penambalan reguler.

Dengan AMS Accelerate, Anda memutuskan mana yang Akun AWS Anda inginkan agar AMS Accelerate beroperasi, Wilayah AWS tempat Anda ingin AMS Accelerate beroperasi, add-on yang Anda butuhkan, dan perjanjian tingkat layanan (SLAs) yang Anda butuhkan. Untuk detail selengkapnya, lihat [Menggunakan paket operasi Akselerasi AMS](#) dan [Deskripsi Layanan](#).

Rencana operasi AMS Advanced

AMS Advanced menyediakan layanan siklus hidup penuh untuk menyediakan, menjalankan, dan mendukung infrastruktur Anda. Selain layanan operasional yang disediakan oleh AMS Accelerate, AMS Advanced juga mencakup layanan tambahan, seperti manajemen landing zone, perubahan infrastruktur dan penyediaan, manajemen akses, dan keamanan endpoint.

AMS Advanced menerapkan landing zone tempat Anda memigrasikan AWS beban kerja dan menerima layanan operasional AMS. Zona pendaratan multi-akun terkelola kami telah dikonfigurasi sebelumnya dengan infrastruktur untuk memfasilitasi otentikasi, keamanan, jaringan, dan pencatatan.

AMS Advanced juga mencakup sistem manajemen perubahan dan akses yang melindungi beban kerja Anda dengan mencegah akses yang tidak sah atau penerapan perubahan berisiko pada infrastruktur Anda AWS. Pelanggan perlu membuat permintaan perubahan (RFC) menggunakan sistem manajemen perubahan kami untuk menerapkan sebagian besar perubahan di akun AMS Advanced Anda. Anda membuat RFCs dari pustaka perubahan otomatis yang telah diperiksa sebelumnya oleh tim keamanan dan operasi kami atau meminta perubahan manual yang ditinjau dan diimplementasikan oleh tim operasi kami jika dianggap aman dan didukung oleh AMS Advanced.

AMS Advanced juga menawarkan yang berbeda SLAs. Untuk informasi selengkapnya, lihat [deskripsi layanan AWS Managed Services AMS Advanced](#).

Memulai AWS Managed Services

Untuk detail tentang memulai layanan AMS landing zone multi-akun, lihat [AWS Managed Services Onboarding](#) Introduction. Dua panduan orientasi memberikan deskripsi layanan dan pertanyaan

yang perlu dipertimbangkan untuk membantu Anda memulai. Tinjau fitur yang ditetapkan Fitur [AWS Managed Services](#), dan sumber daya terkini di [AWS Managed Services Resources](#).

Istilah kunci AMS

- **AMS Advanced:** Layanan yang dijelaskan di bagian “Deskripsi Layanan” pada Dokumentasi Lanjutan AMS. Lihat [Deskripsi Layanan](#).
- **Akun Lanjutan AMS:** AWS akun yang setiap saat memenuhi semua persyaratan dalam Persyaratan Orientasi Lanjutan AMS. Untuk informasi tentang manfaat AMS Advanced, studi kasus, dan untuk menghubungi staf penjualan, lihat [AWS Managed Services](#).
- **Akun Akselerasi AMS:** AWS akun yang setiap saat memenuhi semua persyaratan dalam Persyaratan Akselerasi Akselerasi AMS. Lihat [Memulai dengan AMS Accelerate](#).
- **AWS Managed Services:** AMS dan atau AMS Accelerate.
- **Akun AWS Managed Services:** Akun AMS dan atau akun AMS Accelerate.
- **Rekomendasi Kritis:** Rekomendasi yang dikeluarkan oleh AWS melalui permintaan layanan yang memberi tahu Anda bahwa tindakan Anda diperlukan untuk melindungi terhadap potensi risiko atau gangguan pada sumber daya Anda atau. Layanan AWS Jika Anda memutuskan untuk tidak mengikuti Rekomendasi Kritis pada tanggal yang ditentukan, Anda bertanggung jawab penuh atas segala kerugian yang diakibatkan oleh keputusan Anda.
- **Konfigurasi yang Diminta Pelanggan:** Perangkat lunak, layanan, atau konfigurasi lain apa pun yang tidak diidentifikasi dalam:
 - **Mempercepat:** [Konfigurasi yang Didukung](#) atau [Akselerasi AMS; Deskripsi Layanan](#).
 - **AMS Lanjutan:** [Konfigurasi yang Didukung](#) atau [AMS Lanjutan; Deskripsi Layanan](#).
- **Komunikasi insiden:** AMS mengkomunikasikan Insiden kepada Anda atau Anda meminta Insiden dengan AMS melalui Insiden yang dibuat di Support Center for AMS Accelerate dan di AMS Console for AMS. AMS Accelerate Console menyediakan ringkasan Insiden dan Permintaan Layanan di Dasbor dan tautan ke Pusat Dukungan untuk detailnya.
- **Lingkungan Terkelola:** Akun AMS Advanced dan atau akun AMS Accelerate yang dioperasikan oleh AMS.

Untuk AMS Advanced, ini termasuk akun landing zone multi-akun (MALZ) dan single-account landing zone (SALZ).

- **Tanggal mulai penagihan:** Hari kerja berikutnya setelah AWS menerima informasi yang Anda minta di Email Onboarding AWS Managed Services. Email Onboarding AWS Managed Services

mengacu pada email yang dikirim oleh Anda AWS untuk mengumpulkan informasi yang diperlukan guna mengaktifkan AWS Managed Services di akun Anda.

Untuk akun yang Anda daftarkan selanjutnya, tanggal mulai penagihan adalah hari berikutnya setelah AWS Managed Services mengirimkan Pemberitahuan Aktivasi AWS Managed Services untuk akun yang terdaftar. Pemberitahuan Aktivasi AWS Managed Services terjadi saat:

1. Anda memberikan akses ke AWS akun yang kompatibel dan menyerahkannya ke AWS Managed Services.
 2. AWS Managed Services mendesain dan membangun Akun AWS Managed Services.
- Penghentian Layanan: Anda dapat menghentikan AWS Managed Services untuk semua akun AWS Managed Services, atau untuk akun AWS Managed Services tertentu dengan alasan apa pun dengan memberikan pemberitahuan AWS setidaknya 30 hari melalui permintaan layanan. Pada Tanggal Penghentian Layanan, baik:
 1. AWS menyerahkan kontrol semua akun AWS Managed Services atau akun AWS Managed Services yang ditentukan sebagaimana berlaku, untuk Anda, atau
 2. Para pihak menghapus AWS Identity and Access Management peran yang memberikan AWS akses dari semua akun AWS Managed Services atau akun AWS Managed Services yang ditentukan, sebagaimana berlaku.
 - Tanggal penghentian layanan: Tanggal penghentian layanan adalah hari terakhir bulan kalender setelah berakhirnya periode pemberitahuan penghentian 30 hari yang diperlukan. Jika akhir periode pemberitahuan penghentian yang diperlukan jatuh setelah hari ke-20 bulan kalender, maka tanggal penghentian layanan adalah hari terakhir dari bulan kalender berikutnya. Berikut ini adalah contoh skenario untuk tanggal penghentian.
 - Jika pemberitahuan penghentian diberikan pada 12 April, maka pemberitahuan 30 hari berakhir pada 12 Mei. Tanggal penghentian layanan adalah 31 Mei.
 - Jika pemberitahuan penghentian diberikan pada 29 April, maka pemberitahuan 30 hari berakhir pada 29 Mei. Tanggal penghentian layanan adalah 30 Juni.
 - Penyediaan AWS Managed Services AWS : menyediakan bagi Anda dan Anda dapat mengakses serta menggunakan AWS Managed Services untuk setiap akun AWS Managed Services sejak tanggal dimulainya layanan.
 - Penghentian untuk akun AWS Managed Services tertentu: Anda dapat menghentikan AWS Managed Services untuk akun AWS Managed Services tertentu dengan alasan apa pun dengan memberikan AWS pemberitahuan melalui permintaan layanan (“Permintaan Penghentian Akun AMS”).

Ketentuan manajemen insiden:

- Acara: Perubahan di lingkungan AMS Anda.
- Peringatan: Setiap kali peristiwa dari yang didukung Layanan AWS melebihi ambang batas dan memicu alarm, peringatan dibuat dan pemberitahuan dikirim ke daftar kontak Anda. Selain itu, insiden dibuat dalam daftar Insiden Anda.
- Insiden: Gangguan yang tidak direncanakan atau penurunan kinerja lingkungan AMS atau AWS Managed Services yang menghasilkan dampak seperti yang dilaporkan oleh AWS Managed Services atau Anda.
- Masalah: Akar penyebab bersama dari satu atau lebih insiden.
- Resolusi Insiden atau Menyelesaikan Insiden:
 - AMS telah memulihkan semua layanan AMS yang tidak tersedia atau sumber daya yang berkaitan dengan insiden tersebut ke keadaan yang tersedia, atau
 - AMS telah menetapkan bahwa tumpukan atau sumber daya yang tidak tersedia tidak dapat dikembalikan ke status yang tersedia, atau
 - AMS telah memulai pemulihan infrastruktur yang diotorisasi oleh Anda.
- Waktu Respons Insiden: Perbedaan waktu antara saat Anda membuat insiden, dan saat AMS memberikan respons awal melalui konsol, email, pusat layanan, atau telepon.
- Waktu Resolusi Insiden: Perbedaan waktu antara saat AMS atau Anda membuat insiden, dan kapan insiden diselesaikan.
- Prioritas Insiden: Bagaimana insiden diprioritaskan oleh AMS, atau oleh Anda, sebagai Rendah, Sedang, atau Tinggi.
 - Rendah: Masalah non-kritis dengan layanan AMS Anda.
 - Medium: Layanan AWS dalam lingkungan terkelola Anda tersedia tetapi tidak berfungsi sebagaimana dimaksud (sesuai deskripsi layanan yang berlaku).
 - Tinggi: Baik (1) Konsol AMS, atau satu atau beberapa AMS APIs dalam lingkungan terkelola Anda tidak tersedia; atau (2) satu atau beberapa tumpukan AMS atau sumber daya dalam lingkungan terkelola Anda tidak tersedia dan ketidaktersediaannya mencegah aplikasi Anda menjalankan fungsinya.

AMS dapat mengkategorikan ulang insiden sesuai dengan pedoman di atas.

- Pemulihan Infrastruktur: Menyebarkan kembali tumpukan yang ada, berdasarkan templat tumpukan yang terkena dampak, dan memulai pemulihan data berdasarkan titik pemulihan terakhir yang diketahui, kecuali ditentukan lain oleh Anda, ketika resolusi insiden tidak memungkinkan.

Istilah infrastruktur:

- Lingkungan produksi terkelola: Akun pelanggan tempat aplikasi produksi pelanggan berada.
- Lingkungan non-produksi yang dikelola: Akun pelanggan yang hanya berisi aplikasi non-produksi, seperti aplikasi untuk pengembangan dan pengujian.
- AMS stack: Sekelompok satu atau lebih AWS sumber daya yang dikelola oleh AMS sebagai satu unit.
- Infrastruktur yang tidak dapat diubah: Model pemeliharaan infrastruktur yang khas untuk grup Auto EC2 Scaling Amazon ASGs () di mana komponen infrastruktur yang diperbarui AWS, (dalam, AMI) diganti untuk setiap penerapan, daripada diperbarui di tempat. Keuntungan dari infrastruktur yang tidak dapat diubah adalah bahwa semua komponen tetap dalam keadaan sinkron karena selalu dihasilkan dari basis yang sama. Kekekalan tidak tergantung pada alat atau alur kerja apa pun untuk membangun AMI.
- Infrastruktur yang dapat berubah: Model pemeliharaan infrastruktur yang khas untuk tumpukan yang bukan grup Auto EC2 Scaling Amazon dan berisi satu instance atau hanya beberapa instance. Model ini paling dekat mewakili penyebaran sistem tradisional, berbasis perangkat keras, di mana sistem digunakan pada awal siklus hidupnya dan kemudian pembaruan berlapis ke sistem itu dari waktu ke waktu. Setiap pembaruan pada sistem diterapkan ke instance satu per satu, dan dapat menyebabkan downtime sistem (tergantung pada konfigurasi tumpukan) karena aplikasi atau sistem restart.
- Grup keamanan: Firewall virtual untuk instans Anda untuk mengontrol lalu lintas masuk dan keluar. Grup keamanan bertindak pada tingkat instans, bukan tingkat subnet. Oleh karena itu, setiap instance dalam subnet di VPC Anda dapat memiliki kumpulan grup keamanan yang berbeda yang ditugaskan padanya.
- Perjanjian Tingkat Layanan (SLAs): Bagian dari kontrak AMS dengan Anda yang menentukan tingkat layanan yang diharapkan.
- SLA Tidak Tersedia dan Tidak Tersedia:
 - Permintaan API yang dikirimkan oleh Anda yang menghasilkan kesalahan.
 - Permintaan Konsol yang dikirimkan oleh Anda yang menghasilkan respons HTTP 5xx (server tidak mampu melakukan permintaan).
 - Setiap Layanan AWS penawaran yang merupakan tumpukan atau sumber daya dalam infrastruktur yang dikelola AMS Anda berada dalam keadaan “Gangguan Layanan” seperti yang ditunjukkan di Dashboard Service Health.

- Ketidaktersediaan yang dihasilkan secara langsung atau tidak langsung dari pengecualian AMS tidak dipertimbangkan dalam menentukan kelayakan untuk kredit layanan. Layanan dianggap tersedia kecuali memenuhi kriteria karena tidak tersedia.
- Tujuan Tingkat Layanan (SLOs): Bagian dari kontrak AMS dengan Anda yang menentukan sasaran layanan khusus untuk layanan AMS.

Ketentuan penambalan:

- Patch wajib: Pembaruan keamanan penting untuk mengatasi masalah yang dapat membahayakan keadaan keamanan lingkungan atau akun Anda. “Pembaruan Keamanan Kritis” adalah pembaruan keamanan yang dinilai sebagai “Kritis” oleh vendor sistem operasi yang didukung AMS.
- Patch diumumkan versus dirilis: Patch umumnya diumumkan dan dirilis sesuai jadwal. Patch yang muncul diumumkan ketika kebutuhan akan tambalan telah ditemukan dan, biasanya segera setelah itu, tambalan dilepaskan.
- Patch add-on: Patching berbasis tag untuk instans AMS yang memanfaatkan fungsionalitas AWS Systems Manager (SSM) sehingga Anda dapat menandai instance dan menambal instance tersebut menggunakan baseline dan jendela yang Anda konfigurasi.
- Metode tambalan:
 - Penambalan di tempat: Penambalan yang dilakukan dengan mengubah instance yang ada.
 - Patching pengganti AMI: Penambalan yang dilakukan dengan mengubah parameter referensi AMI dari konfigurasi peluncuran grup Auto EC2 Scaling yang ada.
- Penyedia patch (vendor OS, pihak ketiga): Patch disediakan oleh vendor atau badan pengatur aplikasi.
- Jenis Patch:
 - Pembaruan Keamanan Kritis (CSU): Pembaruan keamanan yang dinilai sebagai “Kritis” oleh vendor sistem operasi yang didukung.
 - Pembaruan Penting (IU): Pembaruan keamanan yang dinilai sebagai “Penting” atau pembaruan non-keamanan yang dinilai sebagai “Kritis” oleh vendor sistem operasi yang didukung.
 - Other Update (OU): Pembaruan oleh vendor dari sistem operasi yang didukung yang bukan CSU atau IU.
- Patch yang didukung: AMS mendukung patch tingkat sistem operasi. Upgrade dirilis oleh vendor untuk memperbaiki kerentanan keamanan atau bug lain atau untuk meningkatkan kinerja. Untuk daftar dukungan saat ini OSs, lihat [Support Configurations](#).

Ketentuan keamanan:

- Kontrol Detektif: Pustaka monitor yang dibuat atau diaktifkan oleh AMS yang menyediakan pengawasan berkelanjutan terhadap lingkungan dan beban kerja yang dikelola pelanggan untuk konfigurasi yang tidak selaras dengan kontrol keamanan, operasional, atau pelanggan, dan mengambil tindakan dengan memberi tahu pemilik, memodifikasi, atau menghentikan sumber daya secara proaktif.

Ketentuan Permintaan Layanan:

- Permintaan layanan: Permintaan oleh Anda untuk tindakan yang Anda ingin AMS ambil atas nama Anda.
- Pemberitahuan peringatan: Pemberitahuan yang diposting oleh AMS ke halaman daftar permintaan Layanan Anda saat peringatan AMS dipicu. Kontak yang dikonfigurasi untuk akun Anda juga diberitahu oleh metode yang dikonfigurasi (misalnya, email). Jika Anda memiliki tag kontak pada instans/sumber daya Anda, dan telah memberikan persetujuan kepada manajer pengiriman layanan cloud (CSDM) Anda untuk pemberitahuan berbasis tag, informasi kontak (nilai kunci) dalam tag juga diberitahu untuk peringatan AMS otomatis.
- Pemberitahuan layanan: Pemberitahuan dari AMS yang diposting ke halaman daftar permintaan Layanan Anda.

Istilah lain-lain:

- AWS Managed Services Interface: Untuk AMS: AWS Managed Services Advanced Console, AMS CM API, dan Dukungan API. Untuk AMS Accelerate: Dukungan Konsol dan Dukungan API.
- Kepuasan Pelanggan (CSAT): AMS CSAT diinformasikan dengan analitik mendalam termasuk Peringkat Korespondensi Kasus pada setiap kasus atau korespondensi saat diberikan, survei triwulanan, dan sebagainya.
- DevOps: DevOps adalah metodologi pengembangan yang sangat menganjurkan otomatisasi dan pemantauan di semua langkah. DevOps bertujuan untuk siklus pengembangan yang lebih pendek, peningkatan frekuensi penyebaran, dan rilis yang lebih dapat diandalkan dengan menyatukan fungsi pengembangan dan operasi yang terpisah secara tradisional di atas fondasi otomatisasi. Ketika pengembang dapat mengelola operasi, dan operasi menginformasikan pengembangan, masalah dan masalah lebih cepat ditemukan dan diselesaikan, dan tujuan bisnis lebih mudah dicapai.

- ITIL: Perpustakaan Infrastruktur Teknologi Informasi (disebut ITIL) adalah kerangka kerja ITSM yang dirancang untuk membakukan siklus hidup layanan TI. ITIL diatur dalam lima tahap yang mencakup siklus hidup layanan TI: strategi layanan, desain layanan, transisi layanan, operasi layanan, dan peningkatan layanan.
- Manajemen layanan TI (ITSM): Serangkaian praktik yang menyelaraskan layanan TI dengan kebutuhan bisnis Anda.
- Managed Monitoring Services (MMS): AMS mengoperasikan sistem pemantauan sendiri, Managed Monitoring Service (MMS), yang mengkonsumsi peristiwa AWS Kesehatan dan mengumpulkan data CloudWatch Amazon, dan data dari Layanan AWS lainnya, memberi tahu operator AMS (online 24x7) dari alarm apa pun yang dibuat melalui topik Amazon Simple Notification Service (Amazon SNS).
- Namespace: Saat Anda membuat kebijakan IAM atau bekerja dengan Amazon Resource Names (ARNs), Anda mengidentifikasi Layanan AWS dengan menggunakan namespace. Anda menggunakan ruang nama saat mengidentifikasi tindakan dan sumber daya.

Deskripsi layanan

AMS Advanced (AMS) adalah rencana operasi layanan AWS Managed Services untuk mengelola operasi AWS infrastruktur Anda. AMS Advanced menyediakan operasi infrastruktur rutin seperti patch, manajemen kontinuitas, manajemen keamanan, dan proses manajemen TI seperti insiden, perubahan, dan manajemen permintaan layanan. Untuk daftar layanan yang didukung, lihat [AWS Layanan yang didukung](#).

YouTube Video: [Bagaimana AMS dapat membantu saya mencapai keunggulan operasional di cloud?](#)

Topik

- [AWS Managed Services \(AMS\) AMS Fitur rencana operasi lanjutan](#)
- [Apa yang kita lakukan, apa yang tidak kita lakukan](#)
- [Matriks tanggung jawab AMS \(RACI\)](#)
- [Komponen dasar lingkungan AMS](#)
- [Batas akun AMS](#)
- [Tujuan tingkat layanan AMS \(SLOs\)](#)
- [AWS Layanan yang didukung](#)
- [Konfigurasi yang didukung](#)
- [Kemampuan untuk sistem operasi yang tidak didukung di AMS](#)

- [Antarmuka AMS Lanjutan](#)
- [Titik akhir AMS VPC](#)
- [Ruang nama yang dilindungi AMS](#)
- [Awalan cadangan AMS](#)
- [Jendela pemeliharaan AMS](#)

AWS Managed Services (AMS) AMS Fitur rencana operasi lanjutan

AMS Advanced menawarkan fitur-fitur berikut untuk AWS layanan yang didukung:

- Logging, Monitoring, Guardrails, dan Manajemen Acara:

AMS mengonfigurasi dan memantau lingkungan terkelola Anda untuk aktivitas logging dan menentukan peringatan berdasarkan berbagai pemeriksaan kesehatan. Peringatan diselidiki oleh AMS untuk layanan AWS yang berlaku, dan peringatan yang berdampak negatif terhadap penggunaan layanan tersebut mengakibatkan terjadinya insiden. AMS mengumpulkan dan menyimpan semua log yang dihasilkan sebagai hasil dari semua operasi di CloudWatch, CloudTrail, dan log sistem di Amazon S3. Anda dapat meminta peringatan tambahan untuk diberlakukan. Selain kontrol pencegahan AMS, AMS menerapkan pagar pembatas konfigurasi dan kontrol detektif untuk memberikan perlindungan berkelanjutan bagi Anda dari kesalahan konfigurasi yang dapat mengurangi integritas operasional dan keamanan akun yang dikelola, untuk menegakkan kontrol Anda seperti penandaan dan kepatuhan. Ketika kontrol yang dipantau terdeteksi, alarm dihasilkan yang menghasilkan pemberitahuan, modifikasi, atau penghentian sumber daya berdasarkan default AMS yang telah ditentukan sebelumnya yang dapat dimodifikasi oleh Anda.

- Manajemen kontinuitas (Backup dan Restore):

AMS menyediakan cadangan sumber daya menggunakan fungsionalitas AWS Backup standar yang ada pada interval terjadwal yang ditentukan oleh Anda. Mengembalikan tindakan dari snapshot tertentu dapat dilakukan oleh AMS dengan RFC Anda. Perubahan data yang terjadi di antara interval snapshot adalah tanggung jawab Anda untuk membuat cadangan. Anda dapat mengirimkan RFC untuk permintaan cadangan atau snapshot di luar interval terjadwal. Jika Availability Zone (AZ) tidak tersedianya di AWS Wilayah, dengan izin Anda, AMS memulihkan lingkungan terkelola dengan membuat ulang tumpukan baru berdasarkan templat dan snapshot EBS yang tersedia dari Stacks yang terkena dampak.

- Keamanan dan manajemen akses:

AMS menyediakan keamanan endpoint (EPS) seperti mengkonfigurasi perlindungan anti-virus dan anti-malware. Anda juga dapat menggunakan alat dan proses EPS Anda sendiri dan tidak menggunakan AMS untuk EPS menggunakan fitur yang disebut bring your own EPS (BYOEPS). AMS juga mengonfigurasi kemampuan AWS keamanan default yang disetujui oleh Anda selama orientasi, seperti peran AWS Identity and Access Management (IAM) dan grup EC2 keamanan Amazon, serta menggunakan AWS alat standar (misalnya, Amazon AWS Security Hub Macie, Amazon GuardDuty) untuk memantau dan menanggapi masalah keamanan. Anda mengelola pengguna Anda melalui layanan direktori yang disetujui yang disediakan oleh Anda. Untuk daftar layanan direktori yang disetujui, lihat [Konfigurasi yang didukung](#).

AMS mencakup keamanan endpoint (EPS), yang mencakup antivirus (AV), dan perlindungan anti-malware, malware dan deteksi intrusi (Trend Micro). Grup keamanan didefinisikan per template tumpukan dan dimodifikasi saat peluncuran tergantung pada visibilitas grup keamanan aplikasi (publik/swasta).

Akses ke sistem diminta melalui permintaan manajemen perubahan untuk perubahan (RFCs). Manajemen akses menyediakan akses ke sumber daya yang berbeda, seperti EC2 instans Amazon, instans AWS Management Console, dan APIs. Setelah membangun kepercayaan satu arah dengan penerapan AMS Microsoft Active Directory selama orientasi dan federasi ke AWS, Anda dapat menggunakan kredensi perusahaan yang ada untuk semua interaksi.

- Manajemen tambalan:

AMS menerapkan dan menginstal pembaruan untuk EC2 instans untuk sistem operasi yang didukung (OSs) dan perangkat lunak yang telah diinstal sebelumnya dengan sistem operasi yang didukung. Untuk daftar sistem operasi yang didukung, lihat [Konfigurasi yang didukung](#).

AMS menawarkan dua model untuk ditambah:

- Patch standar AMS untuk penambalan berbasis akun tradisional, dan
- AMS Patch Orchestrator, untuk penambalan berbasis tag.

Di tambalan standar AMS, jendela pemeliharaan bulanan dipilih oleh Anda untuk AMS untuk melakukan sebagian besar aktivitas penambalan. AMS menerapkan pembaruan keamanan penting di luar jendela pemeliharaan yang dipilih (dengan pemberitahuan yang sesuai) dan pembaruan penting selama jendela pemeliharaan yang dipilih. AMS juga menerapkan pembaruan untuk alat manajemen infrastruktur selama jendela pemeliharaan yang dipilih. Anda dapat mengecualikan tumpukan dari manajemen tambalan atau menolak pembaruan, jika Anda mau.

Dengan AMS Patch Orchestrator, jendela pemeliharaan default per akun, ditentukan oleh Anda agar AMS dapat melakukan aktivitas penambalan. Anda dapat menjadwalkan jendela pemeliharaan khusus tambahan untuk AMS untuk menambal serangkaian instance tertentu yang ditentukan oleh Anda dengan tag. AMS menerapkan semua pembaruan yang tersedia, tetapi Anda dapat memfilter atau menolak pembaruan dengan membuat baseline patch khusus. Untuk kedua model, jika Anda menyetujui atau menolak pembaruan yang disediakan di bawah manajemen tambalan tetapi kemudian berubah pikiran, Anda bertanggung jawab untuk memulai pembaruan melalui RFC. AMS melacak status tambalan sumber daya dan menyoroti sistem yang tidak terkini dalam tinjauan bisnis bulanan. Manajemen patch terbatas pada tumpukan di lingkungan terkelola, termasuk semua aplikasi yang dikelola AMS dan layanan AWS yang didukung dengan kemampuan patching (misalnya, RDS). Untuk mendukung semua jenis konfigurasi infrastruktur saat pembaruan dirilis, AMS a) memperbarui EC2 instance dan b) menyediakan AMS AMI yang diperbarui untuk Anda gunakan. Anda bertanggung jawab untuk menginstal, mengkonfigurasi, menambal, dan memantau aplikasi tambahan apa pun yang tidak tercakup secara khusus di atas.

- Manajemen perubahan:

Manajemen perubahan AMS adalah mekanisme bagi Anda untuk mengontrol perubahan di lingkungan terkelola Anda. AMS menggunakan kombinasi kontrol preventif dan detektif untuk memfasilitasi proses ini dan memberikan tingkat kontrol yang berbeda dan risiko terkait tergantung pada mode AMS yang dipilih.

Semua tindakan di lingkungan AMS Anda masuk AWS CloudTrail.

Untuk informasi selengkapnya tentang Manajemen Perubahan AMS dan berbagai mode, lihat [panduan Manajemen Perubahan AMS dan Mode AMS](#).

- Manajemen penyediaan otomatis dan layanan mandiri:

Anda dapat menyediakan sumber daya AWS di AMS Advanced dengan beberapa cara:

- Kirim Permintaan penyediaan dan konfigurasi untuk Perubahan () RFCs
- Menyebarkan melalui AWS Service Catalog
- Menyebarkan melalui mode [Perubahan Langsung](#)
- Menyebarkan melalui [mode Pengembang](#). Ingat bahwa sumber daya yang dibuat melalui mode Pengembang tidak dikelola oleh AMS.
- Konfigurasi layanan AWS secara langsung menggunakan penyediaan layanan mandiri untuk memilih Layanan AWS (lihat). [AWS Layanan yang didukung](#)

- Manajemen insiden:

AMS secara proaktif memberi tahu Anda tentang insiden yang terdeteksi oleh AMS. AMS menanggapi insiden yang diajukan pelanggan dan AMS serta menyelesaikan insiden berdasarkan prioritas insiden. Kecuali jika diinstruksikan lain oleh Anda, insiden yang ditentukan oleh AMS berisiko terhadap keamanan lingkungan terkelola Anda, dan insiden yang berkaitan dengan ketersediaan AMS dan layanan AWS lainnya, ditindaklanjuti secara proaktif. AMS mengambil tindakan atas semua insiden lain setelah otorisasi Anda diterima. Insiden berulang ditangani oleh proses manajemen masalah.

- Manajemen masalah:

AMS melakukan analisis tren untuk mengidentifikasi dan menyelidiki masalah dan untuk mengidentifikasi akar penyebabnya. Masalah diperbaiki baik dengan solusi atau solusi permanen yang mencegah terulangnya dampak layanan future serupa. Laporan pasca insiden (PIR) dapat diminta untuk insiden “Tinggi” apa pun, setelah resolusi. PIR menangkap akar penyebab dan tindakan pencegahan yang diambil, termasuk implementasi tindakan pencegahan.

- Pelaporan:

AMS memberi Anda laporan layanan bulanan yang merangkum metrik kinerja utama AMS, termasuk ringkasan dan wawasan eksekutif, metrik operasional, sumber daya terkelola, kepatuhan perjanjian tingkat layanan AMS (SLA), dan metrik keuangan seputar pengeluaran, penghematan, dan pengoptimalan biaya. Laporan disampaikan oleh manajer pengiriman layanan cloud AMS (CSDM) yang ditetapkan untuk Anda.

- Manajemen permintaan layanan:

Untuk meminta informasi tentang lingkungan terkelola, AMS, atau penawaran AWS layanan Anda, kirimkan permintaan layanan menggunakan konsol AMS. Anda dapat mengirimkan permintaan layanan untuk pertanyaan “Bagaimana” tentang AWS layanan dan fitur atau untuk meminta layanan AMS tambahan.

- Meja Layanan:

Staf AMS merekayasa operasi dengan karyawan Amazon penuh waktu untuk memenuhi permintaan non-otomatis termasuk manajemen insiden, manajemen permintaan layanan, dan manajemen perubahan. Service Desk beroperasi 24 x 7 365 hari setahun.

- Sumber daya yang ditunjuk:

Setiap pelanggan diberi Cloud Service Delivery Manager (CSDM) dan Cloud Architect (CA).

- CSDMs dapat dihubungi langsung. Mereka melakukan tinjauan layanan, dan pelaporan pengiriman dan wawasan melalui semua fase implementasi, migrasi, dan siklus hidup operasional. CSDMs melakukan tinjauan bisnis bulanan dan item detail seperti pengeluaran keuangan, rekomendasi penghematan biaya, pemanfaatan layanan, dan pelaporan risiko. Mereka menyelam jauh ke dalam statistik kinerja operasional dan memberikan rekomendasi bidang perbaikan.
- CAs dapat dihubungi secara langsung dan memberikan keahlian teknis untuk membantu Anda mengoptimalkan penggunaan AWS cloud Anda. Contoh kegiatan CA termasuk, memilih beban kerja untuk migrasi, membantu dengan orientasi akun tambahan dan beban kerja, bertindak sebagai pemimpin teknis dalam kegiatan operasional seperti hari permainan, pengujian pemulihan bencana, manajemen masalah, dan saran teknis untuk mendapatkan hasil maksimal dari AMS dan. AWS CAs mendorong diskusi teknis di semua tingkatan organisasi Anda dan membantu manajemen insiden, membuat trade-off, menetapkan praktik terbaik, dan mitigasi risiko teknis.

- Mode pengembang:

Fitur ini memungkinkan Anda untuk mengulangi desain dan penerapan infrastruktur dengan cepat dalam akun yang dikonfigurasi AMS [1] dengan mengizinkan akses langsung ke layanan AWS dan APIs konsol AWS selain akses ke proses manajemen perubahan AMS. Sumber daya yang disediakan atau dikonfigurasi dengan izin mode pengembang di luar proses manajemen perubahan adalah tanggung jawab Anda untuk mengelola (Lihat “Manajemen Penyediaan Otomatis dan Layanan Mandiri”). Sumber daya yang disediakan melalui proses manajemen perubahan AMS didukung seperti beban kerja lain yang disediakan manajemen perubahan di AMS.

- Dukungan AWS:

Pelanggan AMS dapat memilih tingkat AWS Support yang mereka butuhkan untuk melengkapi paket Operasi AMS mereka. Akun yang terdaftar di AMS dapat berlangganan Business Support atau Enterprise Support. Untuk mempelajari perbedaan dalam Support Plans, lihat [AWS Support Plans](#).

- Akun yang dikelola pelanggan:

Fitur ini memungkinkan Anda untuk meminta akun AWS dalam lingkungan terkelola yang sama, tetapi pengoperasian beban kerja dan sumber daya AWS yang sedang berlangsung dalam akun tersebut adalah tanggung jawab Anda. AMS menyediakan akun yang dikelola pelanggan, tetapi setelah akun dibuat, tidak ada fitur atau layanan AMS lain yang disediakan untuk akun tersebut.

AWS tidak akan mendaftarkan akun yang dikelola pelanggan dalam dukungan premium tingkat perusahaan. Anda bertanggung jawab untuk mendaftarkan akun yang dikelola pelanggan di dukungan AWS sesuai tingkat dukungan yang Anda pilih.

- Manajemen firewall:

AMS menyediakan solusi firewall terkelola opsional untuk Layanan Firewall yang Didukung, yang memungkinkan pemfilteran lalu lintas jalan keluar ke internet untuk jaringan di lingkungan terkelola Anda. Ini tidak termasuk layanan publik yang tidak menggunakan infrastruktur jaringan AWS dan lalu lintasnya langsung ke internet. Solusi ini menggabungkan teknologi firewall terdepan di industri dengan kemampuan manajemen infrastruktur AMS untuk menyebarkan, memantau, mengelola, menskalakan, dan memulihkan infrastruktur firewall.

Saat Anda menggunakan AMS, Anda menerima daftar lengkap infrastruktur jaringan AMS Anda. Untuk mendapatkan daftar layanan terbaru yang berjalan untuk mendukung infrastruktur AMS Anda kapan saja, ajukan permintaan layanan dengan spesifik tentang informasi yang Anda inginkan. Untuk meminta perubahan pada desain jaringan Anda, buat permintaan layanan yang menjelaskan perubahan yang ingin Anda buat—misalnya, menambahkan VPC atau meminta perubahan aturan grup keamanan.

Apa yang kita lakukan, apa yang tidak kita lakukan

AMS memberi Anda pendekatan standar untuk menerapkan infrastruktur AWS dan menyediakan manajemen operasional berkelanjutan yang diperlukan. Untuk deskripsi lengkap tentang peran, tanggung jawab, dan layanan yang didukung, lihat [Deskripsi Layanan](#).

Note

Untuk meminta agar AMS menyediakan layanan AWS tambahan, ajukan permintaan layanan. Untuk informasi selengkapnya, lihat [Membuat Permintaan Layanan](#).

- Apa yang kita lakukan:

Setelah Anda menyelesaikan orientasi, lingkungan AMS tersedia untuk menerima permintaan perubahan (RFCs), insiden, dan permintaan layanan. Interaksi Anda dengan layanan AMS berkisar pada siklus hidup tumpukan aplikasi. Tumpukan baru diurutkan dari daftar templat yang telah dikonfigurasi sebelumnya, diluncurkan ke subnet virtual private cloud (VPC) tertentu, dimodifikasi

selama masa operasionalnya melalui permintaan perubahan (RFCs), dan dipantau untuk kejadian dan insiden 24/7.

Tumpukan aplikasi aktif dipantau dan dipelihara oleh AMS, termasuk penambalan, dan tidak memerlukan tindakan lebih lanjut selama masa pakai tumpukan kecuali perubahan diperlukan atau tumpukan dinonaktifkan. Insiden yang terdeteksi oleh AMS yang memengaruhi kesehatan dan fungsi tumpukan menghasilkan pemberitahuan dan mungkin atau mungkin tidak memerlukan tindakan Anda untuk menyelesaikan atau memverifikasi. Pertanyaan cara dan pertanyaan lainnya dapat dilakukan dengan mengirimkan permintaan layanan.

Selain itu, AMS memungkinkan Anda mengaktifkan layanan AWS yang kompatibel yang tidak dikelola oleh AMS. Untuk informasi tentang layanan yang kompatibel dengan AWS-AMS, lihat Mode penyediaan [layanan mandiri](#).

- Apa yang tidak kita lakukan:

Meskipun AMS menyederhanakan penerapan aplikasi dengan menyediakan sejumlah opsi manual dan otomatis, Anda bertanggung jawab atas pengembangan, pengujian, pembaruan, dan pengelolaan aplikasi Anda. AMS menyediakan bantuan pemecahan masalah untuk masalah infrastruktur yang berdampak pada aplikasi, tetapi AMS tidak dapat mengakses atau memvalidasi konfigurasi aplikasi Anda.

Matriks tanggung jawab AMS (RACI)

Note

Untuk memenuhi kewajibannya tepat waktu, AWS Managed Services (AMS) mungkin memerlukan masukan dari Anda untuk memutuskan tindakan yang tepat. AMS akan menghubungi kontak pelanggan yang ditunjuk untuk semua klarifikasi dan masukan tersebut. AMS akan mengharapkan respons terhadap pertanyaan tersebut dalam waktu 24 jam kerja. Jika tidak ada balasan dalam 24 jam kerja, AMS dapat memilih tindakan atas nama Anda.

Matriks AMS yang bertanggung jawab, bertanggung jawab, dikonsultasikan, dan diinformasikan, atau RACI, memberikan tanggung jawab utama baik kepada pelanggan atau AMS untuk berbagai kegiatan.

AMS mengelola infrastruktur AWS Anda. Tabel berikut memberikan gambaran umum tentang tanggung jawab pelanggan dan AMS untuk aktivitas dalam siklus hidup aplikasi yang berjalan dalam lingkungan yang dikelola AMS.

AMS tidak bertanggung jawab atas aktivitas berikut untuk akun yang Dikelola Pelanggan atau infrastruktur yang berjalan di dalamnya; oleh karena itu RACI ini tidak berlaku.

- R adalah singkatan dari pihak yang bertanggung jawab yang melakukan pekerjaan untuk mencapai tugas.
- C adalah singkatan dari konsultasikan; pihak yang pendapatnya dicari, biasanya sebagai ahli materi pelajaran; dan dengan siapa ada komunikasi bilateral.
- Saya singkatan dari Informed; sebuah pihak yang diinformasikan tentang kemajuan, seringkali hanya pada penyelesaian tugas atau deliverable.
- Penyediaan Layanan Mandiri mengacu pada sumber daya yang disediakan oleh pelanggan dengan layanan mandiri melalui AWS API atau Konsol, termasuk Mode Pengembang dan Layanan Penyediaan Layanan Mandiri.

Note

Beberapa bagian berisi 'R' untuk AMS dan Pelanggan. Ini karena, dalam model AWS Shared Responsibility, AMS dan pelanggan mengambil kepemilikan bersama untuk menanggapi masalah infrastruktur dan aplikasi.

Untuk menyediakan kemampuan penyediaan layanan mandiri, AMS telah menciptakan peran IAM yang ditingkatkan dengan batasan izin untuk membatasi perubahan yang tidak diinginkan dari akses layanan langsung. AWS Peran tidak mencegah semua perubahan dan Anda bertanggung jawab untuk mematuhi kontrol internal, kepatuhan, dan untuk memvalidasi bahwa semua AWS layanan yang digunakan memenuhi sertifikasi yang diperlukan. Kami menyebutnya mode Penyediaan Layanan Mandiri. Untuk detail tentang persyaratan AWS kepatuhan, lihat [AWS Kepatuhan](#).

Untuk sumber daya yang Anda sediakan melalui layanan mandiri, AMS menyediakan manajemen insiden, kontrol detektif dan pagar pembatas, pelaporan, sumber daya yang ditunjuk (Cloud Service Delivery Manager dan Cloud Architect), Keamanan & akses, dan dukungan teknis melalui permintaan layanan. Selain itu, jika berlaku, Anda bertanggung jawab atas manajemen kontinuitas,

manajemen patch, pemantauan infrastruktur, dan manajemen perubahan untuk sumber daya yang disediakan atau dikonfigurasi di luar sistem manajemen perubahan AMS.

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Siklus hidup aplikasi		
Pengembangan aplikasi	R	I
Analisis dan desain persyaratan infrastruktur aplikasi	R	C
Desain dan pengoptimalan untuk tumpukan AMS non-standar	R	C
Desain dan optimalisasi tumpukan standar AMS	I	R
Deployment aplikasi	R	C
Penerapan Infrastruktur AWS	C	R
Pemantauan aplikasi	R	I
Pengujian/pengoptimalan aplikasi	R	I
Panduan pengoptimalan infrastruktur AWS	I	R
Pemantauan infrastruktur AWS	I	R
Memecahkan masalah dan menyelesaikan masalah aplikasi	R	C
Memecahkan masalah dan mengatasi masalah jaringan AWS	C	R
Memecahkan masalah dan menyelesaikan masalah sistem operasi dan infrastruktur	C	R
	R	C

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Penyediaan Layanan Mandiri		
Aplikasi dan Integrasi ITSM		
Integrasi aplikasi dengan AWS Service Offerings	R	C
Integrasi ITSM dengan AWS Managed Services Interface	R	C
Jaringan		
Pengaturan dan konfigurasi VPC dan VPC Lingkungan Terkelola	C	R
Alokasikan ruang alamat pribadi untuk VPCs (mis. /16)	R	C
Mengonfigurasi & Mengoperasikan Layanan Terkelola Non-AWS, yang dikelola Pelanggan Firewalls/Proxy/Bastions/HOSTs	R	C
Konfigurasi & Operasikan AWS Security Groups/NAT/Customer Bastions/NACL di dalam Lingkungan Terkelola	I	R
Jaringan (misalnya DirectConnect) konfigurasi dan implementasi dalam jaringan pelanggan	R	C
Konfigurasi dan implementasi jaringan dalam Lingkungan Terkelola	C	R
Konfigurasi lingkungan terkelola		
Tentukan pengaturan Auto Scaling default untuk template Stack baseline	I	R

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Rekomendasikan optimasi RI	C	R
Beli kapasitas RI dan PIOP	R	C
Hapus kapasitas saat kapasitas lebih dari yang disediakan (bila didukung oleh aplikasi pelanggan)	C	R
Buat/perbarui informasi spesifik pelanggan AWS untuk AWS Managed Services	C	R
Konfigurasi S3	C	R
Penyediaan layanan mandiri	R	C
Konfigurasi gletser	C	R
Tentukan kebijakan arsip	R	C
Konfigurasi kebijakan arsip	C	R
Memilih jendela pemeliharaan pelanggan	R	I
Manajemen AWS RDS		
Pantau source/replica/RO kesehatan replikasi	I	R
Identifikasi RCA dari failover sumber	I	R
Konfigurasi snapshot (cadangan) otomatis	C	R
Penyediaan layanan mandiri	R	C
Mengkoordinasikan dan menjadwalkan manajemen patch mesin DB	C	R
Penyediaan layanan mandiri	R	C

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Merekomendasikan penyimpanan DB dan kapasitas PIOP	C	R
Penyediaan layanan mandiri	R	C
Merekomendasikan ukuran instance untuk menjalankan database	C	R
Penyediaan layanan mandiri	R	C
Merekomendasikan optimasi RI untuk Lingkungan Terkelola	C	R
Penyediaan layanan mandiri	R	C
Pemantauan kinerja RDS () CloudWatch	C	R
Penyediaan layanan mandiri	R	C
Konfigurasi langganan acara RDS (SNS)	C	R
Penyediaan layanan mandiri	R	C
Konfigurasi grup keamanan RDS	C	R
Penyediaan layanan mandiri	R	C
Konfigurasi mesin parameter/option RDS	R	C
Desain meja DB	R	I
Pengindeksan DB	R	I
Analisis log DB	R	I
Manajemen Perubahan AMS		

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Membuat pelanggan RFCs (misalnya akses ke creating/updating/deleting managed stacks, deploying/updating aplikasi sumber daya, perubahan konfigurasi Penawaran AWS Layanan)	R	I
Menyetujui Pelanggan RFCs	I	R
Membuat AWS Managed Services RFCs (misalnya akses ke sumber daya, membuat sumber daya atas nama pelanggan, menerapkan pembaruan ke OS sebagai bagian dari Manajemen Patch)	I	R
Menyetujui non-otomatis RFCs	R	I
Mengirimkan permintaan untuk Jenis Perubahan baru	R	C
Membuat Jenis Perubahan baru	I	R
Pemeliharaan kalender perubahan aplikasi	R	C
Pemberitahuan Jendela Pemeliharaan yang akan datang	I	R
AWS Service Catalog		
Buat portofolio dan produk	R	I
Mendistribusikan produk ke pengguna akhir	R	I
Buat pustaka opsi tag dan tag	R	C
Berbagi portofolio dan produk dengan pengguna akhir	R	I

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Merevis/memperbarui portofolio dan produk	R	I
Membuat dan menetapkan kendala untuk portofolio dan produk	R	C
Mengaitkan Tindakan Layanan dengan produk	R	C
Perbarui sumber daya yang disediakan dengan versi produk baru	R	I
Penyediaan		
Penambahan khusus pelanggan ke AMI baseline AWS Managed Services	R	C
Konfigurasi Jenis Perubahan tambahan yang disetujui yang digunakan untuk menyediakan templat Stack	C	R
Luncurkan Stack terkelola dan sumber daya AWS terkait yang dikirimkan melalui proses manajemen perubahan AMS atau AWS Service Catalog. Penyediaan layanan mandiri	I	R
	R	I
Install/Update aplikasi kustom dan pihak ketiga pada Instans yang disediakan melalui proses manajemen perubahan AMS atau AWS Service Catalog.	R	I
Penyediaan - Arsitektur Stack		

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Menyediakan lisensi OS (termasuk biaya penggunaan untuk layanan AWS yang berlaku — misalnya EC2 dan RDS)	I	R
	R	Aku
Penyediaan Layanan Mandiri		
Tentukan templat infrastruktur dasar (Stacks) untuk penerapan aplikasi melalui sistem manajemen perubahan AMS.	I	R
	R	Aku
Penyediaan Layanan Mandiri		
Membuat baseline disetujui 8 AMIs	I	R
Evaluasi inventaris aplikasi pelanggan dan tentukan kecocokan dengan templat infrastruktur yang tersedia (Tumpukan)	R	C
Tentukan Tumpukan unik yang merupakan tambahan dari penawaran template dasar	R	C
Logging, Monitoring dan Manajemen Acara		
Merekam log perubahan infrastruktur AWS	I	R
Merekam semua log perubahan aplikasi	R	C
Instalasi dan konfigurasi agen dan skrip untuk penambalan, keamanan, pemantauan, dll. Infrastruktur AWS yang disediakan melalui proses manajemen perubahan AMS.	I	R
	R	C
Penyediaan Layanan Mandiri		
Tentukan pemantauan khusus pelanggan dan persyaratan insiden	R	C

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Mengkonfigurasi peringatan untuk Lingkungan Terkelola	I	R
Memantau semua peringatan yang dikonfigurasi AMS Penyediaan Layanan Mandiri	I	R
	R	C
Menyelidiki Peringatan infrastruktur untuk pemberitahuan Insiden Penyediaan Layanan Mandiri	I	R
	R	C
Menyelidiki alarm aplikasi	R	C
Manajemen Insiden		
Memberi tahu Insiden secara proaktif pada infrastruktur AWS berdasarkan pemantauan Penyediaan Layanan Mandiri	I	R
	R	C
Menangani masalah kinerja aplikasi dan pemadaman	R	I
Kategorikan Prioritas Insiden	I	R
Berikan respon Insiden	I	R

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Memberikan resolusi Insidensi/pemulihan infrastruktur	C	R
 Note SLAs tidak berlaku untuk sumber daya berbasis instans yang disediakan di luar manajemen perubahan AMS, termasuk yang disediakan menggunakan penyediaan layanan mandiri dan mode pengembang.		
Manajemen Masalah		
Identifikasi Masalah dalam Lingkungan yang Dikelola	C	R
Lakukan RCA untuk Masalah di Lingkungan Terkelola	C	R
Remediasi Masalah di Lingkungan yang Dikelola	C	R
Identifikasi dan atasi masalah aplikasi	R	I
Manajemen Keamanan		
Keamanan infrastruktur pelanggan and/or menetapkan dasar untuk proses kepatuhan keamanan sebagaimana ditentukan dan disepakati selama orientasi pelanggan.	C	R
	R	C
Penyediaan Layanan Mandiri		
Mempertahankan lisensi yang valid untuk EPS Terkelola	R	C

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Konfigurasi EPS Terkelola	I	R
Penyediaan Layanan Mandiri	R	C
Perbarui EPS Terkelola	I	R
Penyediaan Layanan Mandiri	R	C
Memantau malware pada instans yang disediakan melalui proses AMS CM.	I	R
Penyediaan Layanan Mandiri	R	C
Mempertahankan dan memperbarui tanda tangan virus.	I	R
Penyediaan Layanan Mandiri	R	C
Remediasi kasus yang terinfeksi malware.	C	R
Penyediaan Layanan Mandiri	R	C
Manajemen acara keamanan	C	R
Keamanan - Manajemen Akses		
Mengelola siklus hidup pengguna, dan izin mereka untuk layanan direktori lokal, yang digunakan untuk mengakses AWS Managed Services	R	I
Mengoperasikan sistem otentikasi federasi untuk akses pelanggan ke konsol/ AWS APIs	R	C
Menerima dan mempertahankan kepercayaan an Active Directory (AD) dari AWS Managed Services AD ke AD yang dikelola pelanggan	R	C

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Selama orientasi, buat peran Admin IAM lintas akun dalam setiap akun terkelola	R	C
Amankan kredensi AWS root untuk setiap akun	I	R
Mendefinisikan sumber daya IAM untuk Lingkungan Terkelola	C	R
Kelola kredensyal istimewa untuk akses OS untuk teknisi AMS	I	R
Kelola kredensyal istimewa untuk akses OS yang diberikan kepada pelanggan oleh AMS	R	I
Respon Insiden Keamanan - Siapkan		
Komunikasi		
Memberikan detail kontak keamanan pelanggan agar AMS dapat digunakan selama pemberitahuan peristiwa keamanan dan eskalasi keamanan	R	I
Menyimpan dan mengelola rincian kontak keamanan pelanggan yang disediakan untuk digunakan selama acara keamanan dan eskalasi keamanan	CI	R
Pelatihan		
Memberikan dokumentasi kepada pelanggan untuk mendukung AMS selama proses respons insiden	I	R

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Berlatih tanggung jawab bersama selama proses respons insiden melalui permainan keamanan	RI	RC
Manajemen sumber daya		
Konfigurasi manajemen keamanan yang didukung Layanan AWS untuk peringatan, korelasi peringatan, pengurangan kebisingan, dan aturan tambahan	I	R
Pertahankan persediaan aset (AWS sumber daya), dan ketahui nilai aset dan kekritisannya. Informasi ini berguna selama strategi penanganan insiden	R	CI
Gunakan AWS tag untuk mengidentifikasi sumber daya dan beban kerja	R	CI
Menentukan dan mengkonfigurasi penyimpanan log dan arsip	CI	R
Dasar, konfigurasi Akun AWS, kebijakan, dan manajemen akses yang aman	CI	RC
Respon Insiden Keamanan - Deteksi		
Pencatatan, indikator, dan pemantauan		
Konfigurasi pencatatan dan pemantauan untuk mengaktifkan manajemen acara misalnya dan akun	CI	R
Monitor didukung Layanan AWS untuk peringatan keamanan	I	R

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Menyebarkan dan mengelola alat keamanan titik akhir	CI	R
Pantau malware pada instans menggunakan alat keamanan endpoint yang didukung AMS	I	R
Beri tahu pelanggan tentang kejadian yang terdeteksi melalui pesan keluar	I	R
Pemberitahuan rute dan pembaruan berikutnya kepada pembuat keputusan untuk akun dan beban kerja tertentu untuk meningkatkan waktu respons insiden	R	CI
Menentukan, menerapkan, dan memelihara layanan deteksi standar AMS (misalnya, Amazon GuardDuty dan AWS Config)	CI	R
Rekam log perubahan AWS infrastruktur	I	RC
Aktifkan dan konfigurasi logging, pemantauan untuk mengaktifkan manajemen acara untuk aplikasi	R	C
Menerapkan dan memelihara daftar izin, daftar penolakan, dan deteksi kustom pada layanan AWS keamanan yang didukung (misalnya, Amazon GuardDuty)	RCI	R
Pelaporan acara keamanan		
Beri tahu AMS tentang aktivitas mencurigakan atau investigasi keamanan aktif	R	CI
Beri tahu kejadian dan insiden keamanan yang terdeteksi kepada pelanggan	I	R

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Beri tahu peristiwa yang direncanakan yang dapat memicu proses Respons Insiden Keamanan	R	CI
Respon Insiden Keamanan - Analisis		
Investigasi dan analisis		
Lakukan respons awal untuk peringatan keamanan yang didukung yang dihasilkan oleh sumber deteksi yang didukung	I	RC
Menilai false/true positif menggunakan data yang tersedia	RI	RC
Buat snapshot dari instans yang terpengaruh untuk dibagikan dengan pelanggan jika diperlukan	I	R
Melakukan tugas forensik seperti rantai penahanan, analisis sistem file, forensik memori, dan analisis biner	R	CI
Kumpulkan log aplikasi untuk membantu penyelidikan	R	I
Kumpulkan data dan log untuk membantu investigasi peringatan keamanan	RCI	RC
Terlibat SMEs dalam Layanan AWS investigasi keamanan	CI	R
Libatkan vendor pihak ketiga selama investigasi (misalnya, untuk investigasi anti-malware EPS dan terlibat dengan tim dukungan) TrendMicro	RCI	I

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Bagikan log investigasi dari yang didukung Layanan AWS ke pelanggan selama investigasi	I	R
Komunikasi		
Kirim peringatan dan pemberitahuan dari sumber deteksi AMS untuk sumber daya terkelola	I	R
Mengelola peringatan dan pemberitahuan untuk acara keamanan aplikasi	R	I
Libatkan titik kontak keamanan pelanggan selama investigasi insiden keamanan	R	I
Respon Insiden Keamanan - Mengandung		
Strategi dan eksekusi penahanan		
Tentukan pelaksanaan strategi penahanan yang disepakati dan setuju dengan konsekuensi yang mungkin memengaruhi ketersediaan layanan selama jendela penahanan	R	CI
Buat cadangan sistem yang terpengaruh untuk analisis lebih lanjut	CI	R
Berisi aplikasi dan beban kerja (melalui konfigurasi spesifik aplikasi atau aktivitas respons)	R	CI
Tentukan strategi penahanan berdasarkan insiden keamanan dan sumber daya yang terpengaruh	CI	R

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Aktifkan enkripsi dan penyimpanan cadangan point in time yang aman dari sistem yang terpengaruh	CI	R
Jalankan tindakan penahanan yang didukung untuk AWS sumber daya termasuk EC2 instance, jaringan, dan IAM	CI	R
Respon Insiden Keamanan - Membasmi		
Strategi dan eksekusi pemberantasan		
Tentukan opsi pemberantasan berdasarkan insiden keamanan dan sumber daya yang terpengaruh pada beban kerja aplikasi pelanggan	R	CI
Tentukan strategi pemberantasan yang disepakati, waktu eksekusi pemberantasan, dan konsekuensinya	R	CI
Menentukan langkah-langkah pemberantasan berdasarkan insiden keamanan dan sumber daya yang terpengaruh pada beban kerja yang dikelola AMS	CI	R
Membasmi dan mengeraskan AWS sumber daya termasuk EC2 instans, jaringan, dan pemberantasan IAM	CI	R
Membasmi dan mengeraskan aplikasi dan beban kerja (melalui konfigurasi spesifik aplikasi atau aktivitas respons)	R	I
Respon Insiden Keamanan - Pulihkan		

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Persiapan dan eksekusi pemulihan		
Konfigurasi rencana dan target cadangan seperti yang diminta oleh pelanggan	R	I
Tinjau rencana pencadangan untuk memulihkan beban kerja yang dikelola AMS	CI	R
Melakukan kegiatan restorasi cadangan untuk sumber daya yang didukung Layanan AWS	I	R
Backup aplikasi pelanggan, konfigurasi APP, dan pengaturan penerapan, dan tinjau rencana pencadangan untuk memulihkan aplikasi dan beban kerja pelanggan pasca-insiden	R	I
Kembalikan aplikasi dan beban kerja pelanggan (melalui langkah-langkah restorasi khusus aplikasi)	R	I
Respon Insiden Keamanan — Laporan Pasca Insiden		
Pelaporan pasca insiden		
Bagikan pelajaran yang sesuai dan item tindakan dengan insiden pasca pelanggan sesuai kebutuhan	I	R
Manajemen Patch ⁹		
Pantau pembaruan yang berlaku untuk OS dan perangkat lunak yang didukung yang telah diinstal sebelumnya dengan OS yang didukung untuk EC2 instans.	I	R
	R	C
Penyediaan Layanan Mandiri		

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Beri tahu pelanggan tentang pembaruan yang akan datang (hanya berlaku untuk AMS Standard Patch)	I	R
Kecualikan pembaruan tertentu Tumpukan and/or tertentu dari aktivitas penambalan	R	I
Tentukan jadwal jendela pemeliharaan default dan kustom serta parameter lainnya (misalnya durasi jendela pemeliharaan) untuk menerapkan tambalan (berlaku untuk AMS Patch Hanya orkestrator)	R	I
Tentukan Garis Dasar Patch kustom untuk memfilter dan mengecualikan tambalan tertentu (hanya berlaku untuk AMS Patch Orchestrator)	R	I
Tandai instance untuk mengaitkannya dengan jendela pemeliharaan khusus dan Garis Dasar Patch (hanya berlaku untuk AMS Patch Orchestrator)	R	I
Lacak status tambalan sumber daya dan sorot sistem yang tidak terkini dalam tinjauan bisnis bulanan.	C	R
Patch sistem operasi Windows, dan paket Microsoft diinstal pada sistem operasi yang diatur oleh Windows Update	I R	R -
Penyediaan Layanan Mandiri		

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Patch aplikasi, perangkat lunak, atau dependensi aplikasi yang diinstal tidak dikelola oleh Pembaruan Windows	R	I
Penyediaan layanan mandiri	R	-
Patch sistem operasi Linux dan paket apa pun yang diaktifkan untuk manajemen oleh manajer paket asli sistem operasi (misalnya Yum, Apt, Zypper)	I	R
Penyediaan layanan mandiri	R	-
Patch aplikasi, perangkat lunak, atau dependensi aplikasi yang diinstal tidak dikelola oleh manajer paket asli sistem operasi Linux	R	I
Penyediaan layanan mandiri	R	-
Manajemen Kontinuitas		
Tentukan jadwal cadangan	R	I
Jalankan backup per jadwal.	I	R
Penyediaan Layanan Mandiri	R	C
Validasi cadangan	R	I
Minta kegiatan restorasi cadangan	R	I
Jalankan kegiatan restorasi cadangan.	I	R
Penyediaan Layanan Mandiri	R	C

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Kembalikan Tumpukan yang terpengaruh dan VPCs.	I	R
Penyediaan Layanan Mandiri	R	C
Kembalikan aplikasi kustom/pihak ketiga yang terpengaruh	R	C
Pelaporan		
Mempersiapkan dan menyampaikan laporan layanan bulanan	I	R
AMS pada AWS Outposts	R	I
Konfigurasi dan ambil riwayat audit API sesuai permintaan (CloudTrail).	I	R
Penyediaan layanan mandiri	R	I
Menyediakan akses ke riwayat insiden melalui AWS Managed Services Interface	I	R
Menyediakan akses untuk mengubah riwayat melalui AWS Managed Services Interface.	I	R
Penyediaan layanan mandiri	N/A	N/A
Manajemen Permintaan Layanan		
Meminta informasi menggunakan permintaan layanan	R	I
Balas permintaan layanan	I	R
Firewall Terkelola		
Minta penerapan Firewall yang dikelola AMS	R	I

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Desain dan optimalisasi arsitektur Firewall yang dikelola AMS	I	R
Penerapan Infrastruktur AWS dan alat Firewall yang dikelola AMS	I	R
Memberikan lisensi Firewall (termasuk biaya penggunaan untuk layanan AWS yang berlaku — misalnya) EC2	R	I
Tentukan daftar izin domain default	I	R
Permintaan untuk menambah, memodifikasi, dan menghapus daftar izin khusus dan kebijakan keamanan	R	I
Mengkonfigurasi peringatan untuk Firewall yang dikelola AMS	I	R
Memantau semua peringatan yang dikonfigurasi dengan Firewall yang dikelola AMS	I	R
Jalankan Backup konfigurasi firewall	I	R
Minta kegiatan restorasi cadangan	R	I
Perbarui sumber daya yang disediakan dengan versi produk baru	I	R
Merekam log Firewall yang dikelola AMS	I	R
Teruskan log dari Firewall yang dikelola AMS ke CloudWatch	I	R
Minta perubahan konfigurasi di Firewall yang dikelola AMS	R	I

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Menyetujui perubahan konfigurasi di Firewall yang dikelola AMS	I	R
Jalankan perubahan konfigurasi di Firewall yang dikelola AMS	I	R

⁸ AMS EC2 hanya menyediakan AMIs untuk Amazon

⁹ AMS bertanggung jawab atas End of Life OSes hanya ketika pelanggan menandatangani perjanjian dukungan yang diperpanjang dengan vendor OS

Komponen dasar lingkungan AMS

Multi-Account Landing Zone

Ini adalah perkiraan komponen, dan biaya potensial, dari infrastruktur di akun inti. Ini tidak termasuk biaya lain seperti bandwidth, pemantauan CloudWatch terperinci, pencatatan, alarm, Route53, Amazon S3, Simple Notification Service (Amazon SNS), snapshot, atau instans Amazon yang dipesan. EC2

Anda membayar komponen yang diperlukan oleh infrastruktur landing zone AWS yang dikelola AMS. Perkiraan menempatkan biaya lingkungan landing zone multi-akun AMS biasa pada \$2.450 per bulan dan \$50 untuk akun aplikasi biasa.

Untuk informasi tentang harga, lihat [harga AWS](#).

Komponen Lingkungan Dasar

Komponen	Est. Biaya	Deskripsi
Akun manajemen	\$60	Akun AWS Organizations Management; membuat dan mengelola akun anggota secara finansial. Ini berisi kerangka AWS Landing Zone (ALZ), set tumpukan konfigurasi akun, dan kebijakan kontrol layanan AWS Organization (SCPs). Directory Service: \$35

Komponen	Est. Biaya	Deskripsi
		• CloudTrail: \$7 • CloudWatch: \$6 • Lainnya: \$12
Akun Layanan Bersama	\$2000	Berisi infrastruktur dan sumber daya yang diperlukan untuk manajemen akses (yaitu, Active Directory), manajemen keamanan titik akhir (Trend Micro), dan benteng Anda (SSH/RDP); perkiraannya adalah \$2400 sebulan. Perkiraan ini tidak termasuk biaya lisensi Trend Micro. • EC2: \$800 (dengan jumlah minimum Bastions) • RDS: \$300 (EPS) • VPC (titik akhir): \$400 • Directory Service: \$300 • CloudWatch: \$100 • GuardDuty : \$15 • Secrets Manager: \$10 • Transfer Data: \$10 • Config: \$10 • Lainnya: \$45
Akun Jaringan	\$350	Hub pusat untuk perutean jaringan antara akun AMS, jaringan on-premise Anda, dan lalu lintas keluar ke Internet. Selain itu, berisi benteng DMZ publik (titik masuk bagi insinyur AMS untuk mengakses host di lingkungan AMS Anda). Harga dapat meningkat tergantung pada lalu lintas yang melintasi Transit Gateway dan Direct Connect. • EC2: \$250 (Benteng) • VPC: \$80 • Lainnya: \$20

Komponen	Est. Biaya	Deskripsi
Akun Arsip Log	\$20	Bucket S3 dengan salinan file log AWS CloudTrail dan AWS Config dari setiap akun lingkungan AMS Anda. Biaya meningkat karena lebih banyak log dikumpulkan. • S3: \$10 • CloudWatch: \$5 • Lainnya: \$5
Akun Keamanan	\$20	Hub pusat untuk operasi terkait keamanan, dan titik utama untuk menyalurkan pemberitahuan dan peringatan ke layanan pesawat kontrol AMS. Selain itu, menampung akun manajemen Amazon Guard Duty. Biaya meningkat karena lebih banyak acara dianalisis menggunakan Amazon GuardDuty. • CloudWatch: \$15 • Lainnya: \$5

Single-Account Landing Zone

Tabel berikut mencantumkan komponen contoh infrastruktur yang dikelola AMS.

Komponen Lingkungan Dasar, Terakhir Diperbarui 2020/07/09

Nama	Tipe Instans	OS	# Komponen
mc-eps-dsm	m5.large	Linux	2
manajemen mc-	m5.large	Windows	2
mc-bastion-dmz-ssh	m5.large	Linux	2
mc-bastion-customer-rdp	m5.large	Windows	2
mc-eps-relay	m5.large	Linux	2
layanan direktori	N/A	N/A	

Nama	Tipe Instans	OS	# Komponen
komponen tambahan	N/A	N/A	

Untuk informasi tentang harga, lihat [Harga AWS](#).

Batas akun AMS

Ada tiga jenis batasan berbeda yang perlu dipertimbangkan dalam landing zone multi-akun AMS: batas AMS API, batas sumber daya AMS, dan batas AWS.

Ada dua jenis batasan berbeda yang perlu dipertimbangkan dalam landing zone akun tunggal AMS: batas AMS API, dan batas AWS.

Batas API akun AMS

Bagian ini menjelaskan batas level akun setelah AWS Managed Services (AMS) membatasi layanan AMS SKMS API. Ini berarti, jika Anda memanggil salah satu yang terdaftar APIs lebih dari 10 kali dalam satu detik, salah satu panggilan “dibatasi” (Anda menerima `aThrottleException`). Dalam situasi yang jarang terjadi, dependensi eksternal atau hilir mungkin menghambat API AMS dan kemudian AMS dapat membatasi panggilan API Anda pada tingkat yang mungkin lebih rendah.

Note

Untuk informasi tentang AMS SKMS API, unduh referensi melalui tab Laporan pada konsol Artifact AWS.

Untuk setiap API AMS SKMS yang terdaftar, operasi dibatasi setelah 10 TPS (transaksi per detik):

- `GetStack`
- `GetSubnet`
- `GetVpc`
- `ListAmis`
- `ListStackSummaries`
- `ListSubnetSummaries`

- `ListVpcSummaries`

Batas sumber daya akun landing zone multi-akun AMS

Batas sumber daya akun terkait dengan akun dan subnet aplikasi landing zone multi-akun VPCs AMS.

Batas sumber daya akun aplikasi

Ada batas lunak 50 akun aplikasi per organisasi. Jika Anda memiliki kasus penggunaan untuk lebih dari 50 akun aplikasi, hubungi manajer pengiriman layanan cloud (CSDM) Anda untuk menyampaikan persyaratan Anda.

VPCs dan batas sumber daya subnet

Ada batas lunak 10 VPCs per akun aplikasi dalam Wilayah AWS yang telah ditentukan sebelumnya untuk organisasi.

Setiap VPC mungkin memiliki 1 hingga 10 tingkatan subnet pribadi yang membentang di 2 hingga 3 zona ketersediaan. Selain itu, setiap VPC mungkin memiliki 0 hingga 5 tingkatan subnet publik yang membentang di 2 hingga 3 zona ketersediaan. Jika Anda memiliki persyaratan di luar batas ini, beri tahu CSDM atau Cloud Architect Anda untuk meninjau kasus penggunaan Anda.

Aplikasi multi-akun landing zone AMS terhadap rasio akun

Satu akun per aplikasi didukung di landing zone multi-akun AMS; namun, setiap akun Aplikasi memiliki biaya yang kecil, dan Anda dikenakan biaya untuk jumlah koneksi ke Transit Gateway per jam, dan jumlah lalu lintas yang mengalir melalui AWS Transit Gateway. Jadi, semakin banyak aplikasi terpisah ke dalam akun atau VPCs, semakin tinggi biayanya.

Untuk mengurangi biaya dan tetap memastikan pemisahan tugas yang tepat, AMS merekomendasikan agar Anda 1) mengelompokkan aplikasi berdasarkan tim dengan proses bisnis yang digabungkan secara erat, dan 2) tidak mencampur aplikasi yang berada dalam tahap yang berbeda (prod vs non-prod) atau dikelola oleh tim yang berbeda. Dengan cara ini, Anda akan memiliki lebih sedikit akun, manajemen akses dan pemisahan tugas akan lebih mudah, dan biaya lalu lintas dapat dikurangi.

Misalnya: Perusahaan telah memproduksi aplikasi Perdagangan dan aplikasi Manajemen Portofolio, kedua aplikasi dikelola oleh tim TI Investasi dan bertukar banyak lalu lintas satu sama lain. Dalam skenario ini perusahaan dapat memperoleh manfaat dari pengelompokan kedua aplikasi dalam akun

yang sama dan sama dengan VPC, karena tim TI Investasi tidak perlu meminta akses ke beberapa akun Aplikasi dan perusahaan akan menghemat biaya lalu lintas. Dalam hal ini, perusahaan harus membuat akun lain untuk aplikasi yang sama dalam tahap pengembangan dan menyediakan akses ke tim pengembangan.

Dalam skenario lain, perusahaan telah memproduksi aplikasi Penggajian dan aplikasi Akuntansi, yang dikelola oleh tim TI Sumber Daya Manusia dan Akuntansi TI masing-masing. Meskipun aplikasi Payroll harus bertukar informasi dengan aplikasi Akuntansi, kami sarankan memisahkan kedua aplikasi dalam akun yang berbeda, satu per tim, dan membuat koneksi antara kedua aplikasi VPCs menggunakan akun Jaringan. Dengan cara ini, perusahaan akan mencegah perubahan permintaan tim TI SDM yang memengaruhi infrastruktur aplikasi akuntansi, yang tidak akan mereka ketahui.

Kiat tentang cara mengelompokkan akun ke dalam unit organisasi (OUs). OU adalah mekanisme pengelompokan logis yang memungkinkan Anda untuk mengkategorikan akun (grup) dan menerapkan kebijakan dan konfigurasi berdasarkan grup tersebut. Pendekatan yang disarankan untuk membuat OUs adalah mendasarkan mereka pada kebijakan yang perlu diterapkan pada grup akun tertentu, bukan pada hierarki internal tim dalam struktur pelaporan Anda. OU tidak setara dengan OU Direktori Aktif, dan mencoba mereplikasi struktur AD OU tidak AWS Organizations disarankan dan menghasilkan struktur operasi yang sulit dipertahankan. and/or

AWS batas akun

AWS batas akun berlaku untuk akun AWS Managed Services (AMS) Anda. Metode termudah untuk menentukan batas default dan saat ini untuk AWS layanan adalah dengan memanfaatkan [AWS Service](#) Quotas. AMS merekomendasikan batas layanan individual dengan ukuran yang tepat ke ukuran yang sesuai untuk menjalankan layanan di akun. Batas bertindak seperti pagar pelindung untuk melindungi akun Anda demi keamanan dan pelarian biaya. Jika Anda ingin menaikkan batas tertentu, kirimkan permintaan layanan dengan AMS, dan Operasi AMS akan menaikkan batas atas nama Anda. Misalnya, batas default (atau kuota) untuk instans RDS adalah 40; jika beban kerja Anda memerlukan 50 instans RDS, tingkatkan permintaan layanan untuk Operasi AMS untuk menaikkan batas ke nilai yang Anda butuhkan.

Tujuan tingkat layanan AMS (SLOs)

Tabel berikut menjelaskan tujuan layanan AWS Managed Services (AMS). Perjanjian Tingkat Layanan (SLAs) untuk aspek lain dari layanan AMS, termasuk manajemen insiden, tercakup dalam dokumen SLA yang dibagikan kepada Anda saat Anda berlangganan AMS. Untuk informasi lebih lanjut, bicaralah dengan CSDM Anda.

Tujuan Tingkat Layanan AMS

Fitur	Indikator Kinerja (PI)	Ditambah (Business Days, M-F 8AM to 6PM local time)	Premium (Calendar Days, 24 x 7)
Manajemen perubahan	Waktu yang dibutuhkan untuk menjadwalkan atau menolak otomatis RFCs	<= 30 menit	<= 30 menit
	Waktu inisiasi yang dijadwalkan RFCs dibandingkan dengan waktu eksekusi yang dijadwalkan	<= 1 menit	<= 1 menit
	Waktu yang dibutuhkan untuk approve/reject non-otomatis RFCs, tersedia dalam katalog CT	<=48 jam	<=24 jam
	Waktu yang dibutuhkan untuk approve/reject non-otomatis RFCs tidak tersedia dalam katalog CT	<=5 hari	<=5 hari
Manajemen masalah	Waktu yang dibutuhkan untuk menyelesaikan analisis akar penyebab (RCA)	<=10 hari	<=10 hari
Manajemen permintaan layanan	Waktu respons untuk balasan pertama dan setiap balasan berikutnya	<=8 jam	<=4 jam

AWS Layanan yang didukung

AWS Managed Services (AMS) menyediakan layanan dukungan manajemen operasional untuk AWS layanan berikut. Setiap AWS layanan berbeda, dan sebagai hasilnya tingkat manajemen operasional AMS, dukungan bervariasi tergantung pada sifat dan karakteristik AWS layanan yang mendasarinya. AWS Layanan khusus dikelompokkan berdasarkan kompleksitas dan ruang lingkup layanan dukungan manajemen operasional yang disediakan oleh AMS.

Note

Ketiga grup, A, B, dan C, menunjukkan harga sebagai persentase dari total pengeluaran bulanan per akun untuk layanan AMS, berdasarkan paket dukungan (Plus atau Premium), untuk pelanggan AMS sebelum 16 Maret 2021. Pelanggan AMS yang bergabung setelah 16 Maret 2021 harus mengajukan permintaan layanan untuk informasi harga tambahan. Grup A menunjukkan tidak ada biaya tambahan. Grup B menunjukkan biaya tambahan sebesar 12% (Plus) atau 18% (Premium). Grup C menunjukkan biaya tambahan sebesar 25% (Plus) atau 42% (Premium).

One star (*) menunjukkan layanan yang digunakan dalam lingkungan yang dikelola AMS oleh pelanggan yang menggunakan AWS Konsol dan APIs. Lihat 'Manajemen penyediaan layanan otomatis dan layanan' [AWS Managed Services \(AMS\) AMS Fitur rencana operasi lanjutan](#) untuk detail tambahan tentang tanggung jawab pelanggan saat menyediakan dan mengonfigurasi layanan dengan cara ini.

Dua bintang (**) menunjukkan bahwa Amazon EC2 on AWS Outposts akan ditagih sebagai layanan Grup B; semua sumber daya lain yang dihosting AWS Outposts akan ditagih dengan tarif standar mereka.

AWS Layanan yang didukung

Grup A	Grup B	Grup C
Amazon Alexa for Business* Amazon Managed Streaming for Apache Kafka* Amazon CloudFront Amazon Elastic File System Amazon Glacier	Amazon API Gateway* Amazon AppStream* Amazon Athena* Amazon Bedrock* Amazon CloudSearch* Amazon Cognito* Amazon Comprehend* Amazon Connect*	Amazon Aurora Amazon CloudWatch Amazon Elastic Block Store (EBS) Amazon Elastic Compute Cloud** Amazon Elastic Load Balancing (classic,

Grup A	Grup B	Grup C
Amazon Simple Storage Service AWS Amplify* AWS AppMesh* AWS Auto Scaling AWS Backup AWS CloudFormation AWS Compute Optimizer AWS Global Accelerator* AWS Identity and Access Management AWS License Manager* AWS Management Console AWS Marketplace AWS Lake Formation* AWS Well Architected Tool* VM Import/ Export*	Amazon Document DB (with MongoDB compatibility)* Amazon DynamoDB* Amazon EC2 Container Registry (ECR)* Amazon Elastic Container Service (ECS) on AWS Fargate* Amazon Elastic Kubernetes Service (EKS) on Fargate* Amazon Elemental MediaConvert* Amazon Elemental MediaPackage* Amazon Elemental MediaStore* Amazon Elemental MediaTailor* Amazon Elastic MapReduce* AmazonEventBridge* Amazon Forecast* Amazon FSx* Amazon Inspector* Amazon Kendra* Amazon Kinesis Analytics* Amazon Kinesis Data Stream* Amazon Kinesis Firehose* Amazon Kinesis Video Streams* Amazon Lex* Amazon Managed Service for Prometheus* Amazon MQ* Amazon Personalize** Amazon Quantum Ledger Database (QLDB)* Amazon QuickSight*	application, and network; not gateway) Amazon ElastiCache Amazon OpenSearch Service Amazon GuardDuty Amazon Macie Amazon Redshift Amazon Relational Database Service Amazon Route 53 Amazon Route 53 Resolver DNS Firewall Amazon Simple Email Service Amazon Simple Notification Service Amazon Simple Queue Service Amazon Virtual Private Cloud (VPC) AWS CloudTrail AWS Config AWS Database Migration Service AWS Data Transfer AWS Direct Connect AWS Directory Service AWS Key Management Service AWS Systems Manager (SSM)

Grup A	Grup B	Grup C
	Amazon Rekognition* Amazon SageMaker* Amazon SimpleDB* Amazon Simple Workflow* Amazon Textract* Amazon Transcribe* Amazon Translate* Amazon WorkSpaces* AWS AppSync* AWS Audit Manager* AWS Batch* AWS Certificate Manager* AWS CloudEndure* AWS CloudHSM* AWS CodeBuild* AWS CodeCommit* AWS CodeDeploy* AWS CodePipeline* AWS DataSync* AWS Elemental MediaLive* AWS Glue* AWS Lambda* AWS MigrationHub* AWS Outposts** AWS Resilience Hub* AWS Secrets Manager* AWS Security Hub* AWS Service Catalog AWS Service Catalog AppRegistry* AWS Transfer for SFTP* AWS Shield* AWS Snowball* AWS Step Functions* AWS Transit Gateway* AWS WAF* AWS X-Ray*	

Jika Anda meminta AWS Managed Services untuk menyediakan layanan untuk perangkat lunak atau layanan apa pun yang tidak secara tegas diidentifikasi sebagaimana didukung di bawah ini, AWS Managed Services yang disediakan untuk konfigurasi yang diminta pelanggan tersebut akan diperlakukan sebagai “Layanan Beta” berdasarkan Ketentuan Layanan.

Konfigurasi yang didukung

Berikut adalah konfigurasi yang didukung AWS Managed Services (AMS):

- Bahasa: AMS tersedia dalam bahasa Inggris.
- Layanan Firewall:
 - Amazon Route 53 Resolver DNS Firewall
 - Palo Alto VM-Series Firewall Generasi Berikutnya
- Perangkat lunak keamanan: Deep Security dari Trend Micro (Diperlukan). AWS Marketplace: [Trend Micro Deep Security](#)
- Layanan direktori yang disetujui: Microsoft Active Directory (AD)
- [AWS Layanan yang didukung](#).
- AWS Wilayah yang Didukung:

AMS beroperasi dalam subset dari semua AWS Wilayah; namun, AMS hanya API/CLI kehabisan Wilayah “USA East (N. Virginia)”. Jika Anda menjalankan AMS change management API (`amscm`) atau API manajemen pengetahuan layanan AMS (`amsskms`), di Wilayah Timur non-AS, Anda `--region us-east-1` harus menambahkan perintah.

- AS Timur (Virginia)
- AS Barat (California Utara)
- AS Barat (Oregon)
- AS Timur (Ohio)
- Kanada (Pusat)
- Amerika Selatan (Sao Paulo)
- EU (Ireland)
- EU (Frankfurt)
- EU (London)
- Uni Eropa Barat (Paris)
- Asia Pasifik (Mumbai)

- Asia Pasifik (Seoul)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Tokyo)
- Gambar mesin Amazon (AMIs): AMS menyediakan gambar yang disempurnakan keamanan (AMIs) berdasarkan benchmark CIS Level 1 untuk subset sistem operasi yang didukung oleh AMS. Untuk menemukan sistem operasi yang memiliki gambar yang disempurnakan keamanan yang tersedia, lihat Panduan Pengguna Keamanan AMS. Untuk mengakses panduan ini AWS Artifact, filter tab Laporan untuk AWS Managed Services. Untuk mengakses AWS Artifact, hubungi CSDM Anda atau lihat, [Memulai dengan AWS Artifact](#).
- Sistem operasi yang didukung:

Sistem operasi yang didukung (x86-64)

- Amazon Linux 2023
- Amazon Linux 2 (diharapkan tanggal akhir dukungan AMS 30 Juni 2026)
- Oracle Linux 9.x, 8.x
- Red Hat Enterprise Linux (RHEL) 9.x, 8.x
- SUSE Linux Server Perusahaan 15 SP6
- SUSE Linux Enterprise Server untuk SAP 15 SP3 dan yang lebih baru
- Microsoft Windows Server 2022, 2019, 2016
- Ubuntu 20.04, 22.04, 24.04

Sistem operasi yang didukung (ARM64)

- Amazon Linux 2023
- Amazon Linux 2 (diharapkan tanggal akhir dukungan AMS 30 Juni 2026)
- Sistem operasi End of Support (EOS) yang didukung:

Note

Sistem operasi End of Support (EOS) berada di luar periode dukungan umum produsen sistem operasi dan memiliki risiko keamanan yang meningkat. Sistem operasi EOS dianggap konfigurasi yang didukung hanya jika agen yang diperlukan AMS mendukung sistem operasi dan...

1. Anda telah memperluas dukungan dengan vendor sistem operasi yang memungkinkan Anda menerima pembaruan, atau
 2. instans apa pun yang menggunakan sistem operasi EOS mengikuti [kontrol keamanan](#) seperti yang ditentukan oleh AMS dalam Panduan Pengguna Lanjutan, atau
 3. Anda mematuhi kontrol keamanan kompensasi lainnya yang diwajibkan oleh AMS. Jika AMS tidak lagi dapat mendukung sistem operasi EOS, AMS mengeluarkan [Rekomendasi Kritis](#) untuk meningkatkan sistem operasi.
- Agan yang diperlukan AMS dapat mencakup tetapi tidak terbatas pada: CloudWatch, AWS Systems Manager Amazon, agen Endpoint Security (EPS), dan Active Directory (AD) Bridge (hanya Linux).

- Ubuntu Linux 18.04
- SUSE Linux Enterprise Server 15 SP3, SP4, dan SP5
- SUSE Linux Enterprise Server untuk SAP 15 SP2
- SUSE Linux Server Perusahaan 12 SP5
- Layanan SUSE Linux Enterprise untuk SAP 12 SP5
- Microsoft Windows Server 2012/2012 R2
- Red Hat Enterprise Linux (RHEL) :7.x
- Oracle Linux 7.5-7.9

Kemampuan untuk sistem operasi yang tidak didukung di AMS

Sistem operasi yang tidak didukung adalah sistem operasi apa pun yang tidak tercantum dalam [Konfigurasi yang didukung](#) AMS menganggap instance dengan sistem operasi yang tidak didukung sebagai “Konfigurasi yang Diminta Pelanggan” yang tunduk pada persyaratan layanan [AWS Beta](#) dan Pratinjau.

Kumpulan terbatas kemampuan AMS berikut tersedia untuk instans dengan sistem operasi yang tidak didukung:

Kemampuan	Catatan
Manajemen insiden	AMS memberikan respons insiden.

Kemampuan	Catatan
Manajemen permintaan layanan	AMS menanggapi permintaan layanan.
Permintaan untuk perubahan (RFCs)	AMS mengevaluasi RFCs untuk eksekusi. Sistem operasi yang tidak didukung dapat memengaruhi kemampuan untuk mengeksekusi RFCs.
Pemantauan	AMS memantau dan merespons pemeriksaan status EC2 sistem Amazon dan pemeriksaan status instans. Pemeriksaan status sistem meliputi: hilangnya konektivitas jaringan, hilangnya daya sistem, masalah perangkat lunak pada host fisik, dan masalah perangkat keras pada host fisik yang memengaruhi jangkauan jaringan. Pemeriksaan status instance meliputi: konfigurasi jaringan atau startup yang salah, memori habis, sistem file rusak, dan kernel yang tidak kompatibel.
Manajemen keamanan	AMS memantau dan menanggapi EC2 GuardDuty temuan Amazon.
Manajemen Backup	AMS menyediakan manajemen Kontinuitas di AMS Advanced untuk EC2 menggunakan AWS Backup paket dan brankas yang disesuaikan AMS.

Antarmuka AMS Lanjutan

- **Konsol AMS Advanced:** Anda menggunakan konsol AMS Advanced untuk membuat RFCs, melaporkan, dan menanggapi insiden, membuat permintaan layanan, dan menemukan informasi tentang yang ada VPCs dan tumpukan. Jika ragu tentang apa yang harus dilakukan, atau ketika Anda memerlukan bantuan dengan AMS atau sumber daya terkelola Anda, buat permintaan layanan dengan menggunakan antarmuka ini.
- **AWS Management Console:** Banyak AWS konsol dapat berguna untuk melihat informasi AMS, misalnya:
 - **EC2 Konsol Amazon:** Gunakan untuk melihat informasi instans termasuk alamat IP bastion, grup Amazon EC2 Auto Scaling, dan penyeimbang beban.

- Kepatuhan AWS Config Aturan Zona Pendaratan Multi-Akun: Anda dapat melihat status kepatuhan di seluruh akun dan mengidentifikasi sumber daya yang tidak sesuai.
- AWS CloudFormation konsol: Gunakan untuk melihat informasi tumpukan termasuk tumpukan IDs (Anda dapat menemukan tumpukan Amazon RDS dan instans Amazon RDS IDs di sini, dan informasi acara).
- Konsol Amazon RDS: Gunakan untuk melihat informasi peristiwa seperti posting yang dibuat ke WordPress aplikasi di situs di akun Anda. Catatan Anda harus memiliki ID instans Amazon RDS.

Bergantung pada mode peran login Anda, Anda memiliki tingkat akses yang berbeda ke Konsol AWS Manajemen. Untuk informasi selengkapnya tentang mode, lihat [mode AMS](#).

- AMS Advanced change management API — Baca/Tulis: Gunakan API manajemen perubahan (CM API) untuk meminta penambahan dan perubahan spesifik pada infrastruktur terkelola Anda termasuk pemantauan sumber daya, log, pencadangan, dan konfigurasi tambalan. Selain itu, gunakan API ini untuk meminta akses ke sumber daya, menghapus sumber daya, membuat AMIs, dan membuat profil instans IAM. Anda dapat mengakses CM API melalui AMS CLI dan SDKs
- AMS SKMS API — Read-Only: Gunakan API ini untuk membuat daftar sumber daya terkelola dan mendapatkan informasi yang diperlukan untuk melaporkan atau menyiapkan permintaan perubahan.
- Dukungan API: Gunakan Dukungan API standar untuk membuat dan menanggapi insiden dan permintaan layanan secara terprogram. Untuk mempelajari lebih lanjut, lihat [Memulai dengan Dukungan](#).
- AWS APIs— Hanya Baca: Administrator TI utama Anda dapat menggunakan AWS APIs untuk melihat semua sumber daya yang dikelola, melihat CloudTrail log, informasi penagihan, dan banyak fungsi baca lainnya.

Titik akhir AMS VPC

Endpoint VPC memungkinkan Anda menghubungkan VPC Anda secara pribadi tanpa memerlukan gateway Internet. Layanan AWS Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan sumber daya di layanan.

Endpoint adalah perangkat virtual. Mereka adalah komponen VPC yang diskalakan secara horizontal, redundan, dan sangat tersedia yang memungkinkan komunikasi antara instance di VPC dan layanan Anda tanpa memaksakan risiko ketersediaan atau kendala bandwidth pada lalu lintas jaringan Anda. Untuk mempelajari lebih lanjut, lihat Titik [Akhir VPC](#).

Ada dua jenis titik akhir VPC: titik akhir antarmuka dan titik akhir gateway.

- Titik akhir Gateway: VPC di akun memiliki titik akhir Amazon S3 Gateway yang diaktifkan secara default.
- Titik akhir antarmuka: Instans di lingkungan AMS Anda dapat berbicara dengan layanan yang didukung tanpa meninggalkan jaringan Amazon. Ini opsional untuk landing zone akun tunggal dan tidak diaktifkan di akun secara default; kirimkan permintaan layanan ke operasi AMS untuk mengaktifkan ini. Namun, untuk landing zone multi-akun, titik akhir antarmuka diaktifkan secara default di akun Layanan Bersama.

Daftar titik akhir antarmuka yang didukung oleh AMS:

- AWS CloudFormation
- AWS CloudTrail
- AWS Config
- EC2 API Amazon
- AWS Key Management Service
- Amazon CloudWatch
- CloudWatch Acara Amazon
- CloudWatch Log Amazon
- AWS Secrets Manager
- Amazon SNS
- AWS Systems Manager
- AWS Security Token Service

Ruang nama yang dilindungi AMS

Daftar ruang nama yang dilindungi untuk AWS Managed Services (AMS). Saat Anda bekerja dengan AWS resource, cegah konflik dengan AMS dengan tidak menggunakan ruang nama ini. Untuk detail tentang ruang nama AWS layanan lainnya, lihat [Amazon Resource Names \(ARNs\) dan Ruang Nama AWS Layanan](#).

- `ams-*` (ini adalah standar penamaan yang disukai untuk sumber daya baru)
- `/ams/` (ini adalah standar penamaan yang disukai untuk sumber daya berbasis jalur)

- `AWSManagedServices*` (ini adalah standar penamaan yang disukai untuk sumber daya CamelCase jika sesuai)
- `ams*` `AMS*` dan `Ams*`
- `AWS_*` dan `aws*`
- `*/aws_reserved/*`
- `CloudTrail*` dan `Cloudtrail*`
- `codedeploy_service_role`
- `customer-mc-*`
- `eps` dan `EPS`
- `EPSThresholdSubscriptionRole`
- `EPSDB*`
- `IAMPolicy*`
- `INGEST*`
- `LandingZone*`
- `Managed_Services*`
- `managementhost`
- `mc*` `MC*` dan `Mc*`
- `MMS*`
- `ms-`
- `NewAMS*`
- `Root*`
- `sentinel*` dan `Sentinel*`
- `sentinel.int.`
- `StateMachine*`
- `StackSet-ams*`
- `StackSet-AWS-Landing-Zone`
- `TemplateId*`
- `UnhealthyInServiceBastion`
- `VPC_*`

Awalan cadangan AMS

Atribut sumber daya AMS harus sesuai dengan pola tertentu; misalnya, nama profil instans IAM, BackupVault nama, nama tag, dan sebagainya, tidak boleh dimulai dengan awalan cadangan AMS. Awalan yang dicadangkan tersebut adalah:

```
*/aws_reserved/*
ams- *
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc- *
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc *
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
```


Jendela pemeliharaan AMS

AWS Managed Services Maintenance Window (atau Maintenance Window) melakukan aktivitas pemeliharaan untuk AWS Managed Services (AMS) dan berulang pada hari Kamis kedua setiap bulan mulai pukul 15:00 hingga 16:00 Waktu Pasifik. AMS dapat mengubah jendela pemeliharaan dengan pemberitahuan 48 jam. Ini untuk AWS Managed Services (AMS); untuk melakukan aktivitas pemeliharaan untuk infrastruktur terkelola, seperti menerapkan AMS baru. AMIs

Jendela pemeliharaan Anda adalah saat AMS akan menerapkan patching dan Anda menentukan jendela pemeliharaan Anda saat orientasi. Anda juga dapat menyetujui jendela patching yang diusulkan yang disediakan dalam pemberitahuan layanan patching Anda, atau menyarankan jendela yang berbeda.

Untuk panduan cara membuat jendela pemeliharaan, lihat [Jendela Pemeliharaan](#).

Sumber informasi AMS

AMS menyediakan beberapa sumber informasi untuk membantu Anda sukses.

- Panduan Pengguna Akselerasi AMS: Membantu Anda memahami komponen dan fitur yang disediakan AMS Accelerate dan cara menggunakannya. Lihat di sini untuk informasi latar belakang AMS Accelerate dan detail tentang pengaturan default, menemukan sumber daya, dan contoh caranya. [Indeks HTML](#), [PDF](#)
- Panduan Pengguna AMS Advanced: Membantu Anda memahami komponen dan fitur yang disediakan AMS Advanced dan cara menggunakannya. Lihat di sini untuk informasi latar belakang AMS Advanced dan detail tentang pengaturan default, menemukan sumber daya, dan contoh caranya. [Indeks HTML](#), [PDF](#)
- Panduan Aplikasi Lanjutan AMS: Menjelaskan langkah-langkah untuk menerapkan aplikasi ke infrastruktur AWS Managed Services. Lihat di sini untuk informasi tentang penerapan aplikasi dan metodologi pemeliharaan dan pertimbangan. [Indeks HTML](#), [PDF](#).
- Panduan Orientasi Lanjutan AMS: Menjelaskan langkah-langkah awal untuk membuat infrastruktur landing zone multi-akun AWS Managed Services dasar, atau akun tunggal, di akun AMS. Lihat di sini untuk informasi tentang dasar-dasar akun AMS, validasi, dan pertanyaan untuk mempersiapkan Anda untuk orientasi ke AMS. [Indeks HTML](#), [PDF](#).

- Referensi Jenis Perubahan Lanjutan AMS: Menyediakan materi referensi tentang jenis perubahan saat ini yang disediakan AWS Managed Services, termasuk skema jenis perubahan dan contoh penelusuran untuk setiap jenis dan tip perubahan. Menyertakan informasi umum tentang jenis perubahan Membantu Anda memahami semua aspek permintaan untuk change (RFCs) dan tipe perubahan AMS (CTs). Lihat di sini untuk spesifik tentang jenis perubahan, termasuk tautan ke informasi yang relevan. [Indeks HTML](#), [PDF](#).
- Referensi API AMS CM (manajemen perubahan): Menjelaskan AWS Managed Services CM API, yang menyediakan operasi untuk membuat dan memantau permintaan perubahan serta memberikan informasi tentang sumber daya Anda yang dikelola oleh Managed Services. [Indeks HTML](#).
- Panduan Keamanan AMS: Jelaskan informasi keamanan AMS milik.

Pribadi; tersedia di tab Laporan AMS di AWS Artifact Console.
- Sumber Daya Pengembang AMS: Akses ke AMS CLI dan SDK, untuk amscm dan amsskm. Lihat <https://console.aws.amazon.com/managedservices/>.
- YouTube Video AMS: Operasi pelanggan utama dijelaskan dalam video. Lihat [Video YouTube Instruksional AWS Managed Services](#).
- Postingan Blog AMS: Informasi khusus tentang AWS Managed Services. Lihat [Blog AWS](#).

Kepatuhan AMS

AMS telah menjalani audit untuk standar berikut dan memenuhi syarat untuk digunakan sebagai bagian dari solusi di mana Anda harus mendapatkan sertifikasi kepatuhan.

Standar Kepatuhan yang Didukung AMS

AMS mendukung standar AWS kepatuhan. Untuk mempelajari lebih lanjut tentang program AWS kepatuhan, lihat [AWS Kepatuhan](#).

Ini adalah standar kepatuhan saat ini yang didukung oleh AMS.

FedRAMP: Pemerintah Federal AS berdedikasi untuk memberikan layanannya kepada rakyat Amerika dengan cara yang paling inovatif, aman, dan hemat biaya. Komputasi awan memainkan peran penting dalam bagaimana pemerintah federal dapat mencapai efisiensi operasional dan berinovasi sesuai

permintaan untuk memajukan misi mereka di seluruh negeri. Itulah sebabnya banyak lembaga federal saat ini menggunakan layanan AWS cloud untuk memproses, menyimpan, dan mengirimkan data pemerintah federal.

Untuk informasi lebih lanjut, lihat [FedRAMP](#).

HIPAA: [AWS telah memperluas program kepatuhan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan \(HIPAA\) untuk memasukkan AMS sebagai Layanan yang Memenuhi Syarat HIPAA](#). Jika Anda memiliki Business Associate Agreement (BAA) dengan AWS, Anda dapat menggunakan AMS untuk membantu membangun aplikasi yang sesuai dengan HIPAA.

Lihat [whitepaper yang berfokus pada HIPAA](#) untuk mempelajari cara memanfaatkan AMS untuk pemrosesan dan penyimpanan informasi kesehatan. Untuk informasi lebih lanjut, lihat [Kepatuhan HIPAA](#).

HITRUST: Health Information Trust Alliance Common Security Framework (HITRUST CSF) memanfaatkan standar dan peraturan yang diterima secara nasional dan internasional seperti GDPR, ISO, NIST, PCI, dan HIPAA untuk menciptakan serangkaian kontrol keamanan dan privasi dasar yang komprehensif.

Untuk informasi lebih lanjut, lihat [HITRUST CSF](#).

ISO 27001: ISO/IEC 27001:2013 adalah standar manajemen keamanan yang menetapkan praktik terbaik manajemen keamanan dan kontrol keamanan komprehensif mengikuti panduan praktik terbaik 27002. ISO/IEC Dasar dari sertifikasi ini adalah pengembangan dan implementasi program keamanan yang ketat, yang mencakup pengembangan dan implementasi Sistem Manajemen Keamanan Informasi (ISMS) yang mendefinisikan bagaimana AWS terus-menerus mengelola keamanan secara holistik dan komprehensif.

Untuk informasi lebih lanjut, lihat [ISO/IEC 27001:2013](#).

ISO 27017: ISO/IEC 27017:2015 memberikan panduan tentang aspek keamanan informasi komputasi awan, merekomendasikan penerapan kontrol keamanan informasi khusus cloud yang melengkapi panduan standar 27002 dan 27001. ISO/IEC Kode praktik ini memberikan panduan implementasi kontrol keamanan informasi tambahan khusus untuk penyedia layanan cloud.

Untuk informasi lebih lanjut, lihat Kepatuhan [ISO/IEC 27017:2015](#).

ISO 27018: ISO/IEC 27018:2019 adalah kode praktik yang berfokus pada perlindungan data pribadi di cloud. Hal ini didasarkan pada standar keamanan ISO/IEC informasi 27002 dan memberikan panduan implementasi pada ISO/IEC 27002 kontrol yang berlaku untuk public cloud Personally Identifiable Information (PII). Ini juga menyediakan serangkaian kontrol tambahan dan panduan terkait yang dimaksudkan untuk mengatasi persyaratan perlindungan PII cloud publik yang tidak ditangani oleh set kontrol ISO/IEC 27002 yang ada.

Untuk informasi lebih lanjut, lihat Kepatuhan [ISO/IEC 27018:2019](#).

ISO 9001: ISO 9001:2015 menguraikan pendekatan berorientasi proses untuk mendokumentasikan dan meninjau struktur, tanggung jawab, dan prosedur yang diperlukan untuk mencapai manajemen mutu yang efektif dalam suatu organisasi. Bagian tertentu dari standar berisi informasi tentang topik-topik seperti:

- Persyaratan untuk sistem manajemen mutu, termasuk dokumentasi manual kualitas, kontrol dokumen, dan menentukan interaksi proses
- Tanggung jawab manajemen
- Manajemen sumber daya, termasuk sumber daya manusia dan lingkungan kerja organisasi
- Pengembangan layanan, termasuk langkah-langkah dari desain hingga pengiriman
- Kepuasan pelanggan
- Pengukuran, analisis, dan peningkatan SMM melalui kegiatan seperti audit internal dan tindakan korektif dan preventif

Untuk informasi selengkapnya, lihat [Kepatuhan ISO 9001:2015](#).

PCI: AMS memiliki Pengesahan Kepatuhan untuk Standar Keamanan Data (DSS) Industri Kartu Pembayaran (PCI) versi 3.2 di Penyedia Layanan Level 1. Pelanggan yang menggunakan produk dan layanan AWS untuk menyimpan, memproses, atau mengirimkan data pemegang kartu dapat menggunakan AMS saat mereka mengelola sertifikasi kepatuhan PCI DSS mereka sendiri.

Untuk informasi lebih lanjut tentang PCI DSS, termasuk cara meminta salinan AWS PCI Compliance Package, lihat [PCI DSS Level 1](#). Yang penting, Anda harus mengonfigurasi kebijakan kata sandi berbutir halus di AMS agar konsisten dengan standar PCI DSS versi 3.2. Untuk detail tentang kebijakan mana yang harus diberlakukan, lihat [Mengaktifkan Kepatuhan PCI untuk Direktori AWS Microsoft AD](#) Anda.

SOC: Laporan AMS System & Organization Control (SOC) adalah laporan pemeriksaan pihak ketiga independen yang menunjukkan bagaimana AMS mencapai kontrol dan tujuan kepatuhan utama. Tujuan dari laporan ini adalah untuk membantu Anda dan auditor Anda memahami kontrol AMS yang dibuat untuk mendukung operasi dan kepatuhan. Ada tiga jenis laporan AMS SOC:

- Laporan AWS SOC 1 - [Unduh dengan AWS Artifact](#)
- AWS SOC 2: Laporan Keamanan, Ketersediaan, & Kerahasiaan - Unduh [dengan](#) Artifact AWS
- [AWS SOC 3: Laporan Keamanan, Ketersediaan, & Kerahasiaan](#)

Untuk informasi selengkapnya, lihat [Kepatuhan SOC](#).

Tanggung Jawab Bersama

Keamanan, termasuk kepatuhan PCI, adalah [tanggung jawab bersama](#). Penting untuk dipahami bahwa status kepatuhan AMS tidak berlaku secara otomatis untuk aplikasi yang Anda jalankan di AWS Cloud. Anda perlu memastikan bahwa penggunaan AWS layanan Anda sesuai dengan standar. Untuk detail selengkapnya tentang cara AMS bekerja sama dengan pelanggan di seluruh aktivitas tertentu, lihat AMS [Matriks tanggung jawab AMS \(RACI\)](#).

Gambar Mesin AMS Amazon (AMIs)

AMS memproduksi Amazon Machine Images (AMIs) yang diperbarui setiap bulan untuk sistem operasi yang didukung AMS. Selain itu, AMS juga menghasilkan gambar yang ditingkatkan keamanan (AMIs) berdasarkan benchmark CIS Level 1 untuk subset sistem operasi yang [didukung AMS](#). Untuk mengetahui sistem operasi mana yang memiliki gambar yang disempurnakan keamanan, lihat Panduan Pengguna Keamanan AMS, yang tersedia melalui halaman AWS Artifact - > Reports (temukan opsi Laporan di panel navigasi kiri) yang difilter untuk AWS Managed Services. Untuk mengakses AWS Artifact, dapat menghubungi CSDM Anda untuk mendapatkan petunjuk atau buka [Memulai dengan AWS](#) Artifact.

Untuk menerima peringatan saat AMS AMIs baru dirilis, Anda dapat berlangganan topik notifikasi Amazon Simple Notification Service (Amazon SNS) yang disebut “AMS AMI”. Untuk detailnya, lihat [notifikasi AMS AMI dengan SNS](#).

Konvensi penamaan AMS AMI adalah: `customer-ams-<operating system>-<release date>-<version>`. (misalnya, `customer-ams-rhel6-2018.11-3`)

Hanya gunakan AMS AMIs yang dimulai dengan `customer`.

AMS merekomendasikan untuk selalu menggunakan AMI terbaru. Anda dapat menemukan yang terbaru AMIs dengan:

- Mencari di konsol AMS, di AMI halaman.
- Melihat file CSV AMS AMI terbaru, tersedia dari CSDM Anda atau melalui file ZIP ini: AMS [11.2024 konten AMI dan file CSV](#) dalam ZIP.

Untuk file ZIP AMI sebelumnya, lihat [Riwayat Dokumen](#).

- Menjalankan SKMS perintah AMS ini (diperlukan AMS SKMS SDK):

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name, 'customer')].[Name,AmiId,CreationTime]" --output table
```

Konten AMS AMI ditambahkan ke basis AWS AMIs, oleh sistem operasi (OS)

- Linux AMIs:
 - [AWS Alat CLI](#)
 - [NTP](#)
 - [Agen Layanan Perlindungan Trend Micro Endpoint](#)
 - [Penyebaran Kode](#)
 - [PBIS/Beyond Trust AD Bridge](#)
 - [Agen SSM](#)
 - Yum Upgrade untuk tambalan kritis
 - Skrip/perangkat lunak manajemen khusus AMS (mengontrol boot, AD join, pemantauan, keamanan, dan logging)
- Server Windows AMIs:
 - [Microsoft .NET Framework 4.5](#)

- [PowerShell 5.1](#)
- [AWS Alat untuk Windows PowerShell](#)
- PowerShell Modul AMS mengontrol boot, AD join, monitoring, keamanan, dan logging
- [Agen Layanan Perlindungan Trend Micro Endpoint](#)
- [Agen SSM](#)
- [CloudWatch Agen](#)
- EC2Layanan Config (melalui Windows Server 2012 R2)
- EC2Peluncuran (Windows Server 2016 dan Windows Server 2019)
- EC2Launchv2 (Windows Server 2022 dan yang lebih baru)

Berbasis Linux AMIs:

- Amazon Linux 2023 (Rilis Kecil Terbaru) (AMI Minimal tidak didukung)
- Amazon Linux 2 (Rilis Kecil Terbaru)
- Amazon Linux 2 (ARM64)
- Red Hat Enterprise 7 (Rilis Kecil Terbaru)
- Red Hat Enterprise 8 (Rilis Kecil Terbaru)
- Red Hat Enterprise 9 (Rilis Kecil Terbaru)
- SUSE Linux Server Perusahaan 15 SP6
- Ubuntu Linux 18.04
- Ubuntu Linux 20.04
- Ubuntu Linux 22.04
- Ubuntu Linux 24.04
- Amazon Linux: Untuk ikhtisar produk, informasi harga, informasi penggunaan, dan informasi dukungan, lihat [Amazon Linux AMI \(HVM/64-bit\)](#) dan [Amazon Linux 2](#).

Untuk informasi selengkapnya, lihat [Amazon Linux 2 FAQs](#).

- RedHat Enterprise Linux (RHEL): Untuk ikhtisar produk, informasi harga, informasi penggunaan, dan informasi dukungan, lihat [Red Hat Enterprise Linux \(RHEL\) 7 \(HVM\)](#).
- Ubuntu Linux 18.04: Untuk ikhtisar produk, informasi harga, informasi penggunaan, dan informasi dukungan, lihat [Ubuntu 18.04 LTS](#) - Bionic.
- SUSE Linux Enterprise Server untuk aplikasi SAP 15: SP6

- Jalankan langkah-langkah berikut sekali per akun:
 1. Arahkan ke AWS Marketplace.
 2. Cari produk SUSE 15 SAP.
 3. Pilih Lanjutkan untuk berlangganan.
 4. Pilih Terima persyaratan.
- Selesaikan langkah-langkah berikut setiap kali Anda perlu meluncurkan SUSE Linux Enterprise Server baru untuk aplikasi SAP 15 SP6 instance:
 1. Perhatikan ID AMI untuk SUSE Linux Enterprise Server berlangganan untuk Aplikasi SAP 15 AMI.
 2. Buat Deployment | Komponen tumpukan lanjutan | EC2 tumpukan | Buat jenis perubahan ct-14027q0sjyt1h RFC. Ganti *InstanceAmiId* dengan ID AWS Marketplace AMI yang Anda berlangganan.

Berbasis Windows AMIs:

Microsoft Windows Server (2016, 2019 dan 2022), berdasarkan Windows terbaru AMIs.

Untuk contoh pembuatan AMIs, lihat [Membuat AMI](#).

AMIsAMS Offboarding:

AMS tidak membatalkan pembagian apa pun AMIs dari Anda selama offboarding untuk menghindari dampak bagi setiap depedensi Anda. Jika Anda ingin menghapus AMS AMIs dari akun Anda, Anda dapat menggunakan `cancel-image-launch-permission` API untuk menyembunyikan spesifik AMIs. Misalnya, Anda dapat menggunakan skrip di bawah ini untuk menyembunyikan semua AMS AMIs yang dibagikan dengan akun Anda sebelumnya:

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
do
  aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

Anda harus menginstal AWS CLI v2 agar skrip dapat dijalankan tanpa kesalahan apa pun. Untuk langkah-langkah penginstalan AWS CLI, lihat [Menginstal atau memperbarui AWS CLI versi terbaru](#). Untuk detail tentang `cancel-image-launch-permission` perintah, lihat [cancel-image-launch-permission](#).

Keamanan ditingkatkan AMIs

AMS menyediakan gambar yang disempurnakan keamanan (AMIs) berdasarkan benchmark CIS Level 1 untuk subset sistem operasi yang didukung AMS. Untuk mengetahui sistem operasi mana yang memiliki image yang disempurnakan keamanan yang tersedia, lihat Panduan Keamanan Pelanggan AWS Managed Services (AMS). Untuk mengakses panduan ini, buka AWS Artifact, pilih Laporan di panel navigasi kiri, lalu filter untuk AWS Managed Services. Untuk petunjuk tentang cara mengakses AWS Artifact, hubungi CSDM Anda atau lihat [Memulai dengan AWS Artifact](#) untuk informasi selengkapnya.

Cara kerja integrasi antara AD FS dan AMS

Kepercayaan satu arah antara jaringan lokal Anda dan domain AMS adalah sarana default untuk akses ke tumpukan dan VPCs. Ketika VPC dan tumpukan dibuat, akses diberikan melalui grup keamanan Direktori Aktif yang telah dikonfigurasi sebelumnya. Selain itu, akses ke AWS Management Console dapat dikonfigurasi menggunakan Active Directory Federation Service (AD FS), atau perangkat lunak federasi apa pun yang mendukung SAMP, untuk sistem masuk tunggal (SSO) ke Konsol Manajemen AWS.

Note

AMS dapat berfederasi ke banyak layanan federasi, Ping, Okta, dan sebagainya. Anda tidak terbatas pada AD FS; di sini kami menyediakan contoh satu teknologi federasi yang tersedia untuk Anda.

Informasi di sini digandakan dari posting blog ini: [Mengaktifkan Federasi untuk AWS Menggunakan Windows Active Directory, AD FS, dan SAMP 2.0](#).

1. Alur dimulai ketika pengguna (sebut saja dia Bob) menelusuri situs sampel AD FS (<https://Fully.Qualified.Domain.Name.Here/adfs/ls/IdpInitiatedSignOn.aspx>) di dalam domainnya. Ketika Anda menginstal AD FS, Anda mendapatkan direktori virtual baru bernama adfs untuk situs web default Anda, yang mencakup halaman ini.
2. Halaman masuk mengautentikasi Bob terhadap AD. Tergantung pada browser yang digunakan Bob, dia mungkin diminta untuk nama pengguna dan kata sandi IKLAN-nya.
3. Browser Bob menerima pernyataan SAMP dalam bentuk respons otentikasi dari AD FS.

4. Browser Bob memposting pernyataan SAMP ke titik akhir AWS masuk untuk SAMP (/saml).
<https://signin.aws.amazon.com> Di belakang layar, login menggunakan [AssumeRoleWithSAMP API untuk meminta kredensial](#) keamanan sementara dan kemudian membuat URL login untuk file. AWS Management Console
5. Browser Bob menerima URL masuk dan diarahkan ke konsol.

Dari sudut pandang Bob, prosesnya terjadi secara transparan. Dia mulai di situs web internal dan berakhir di AWS Management Console, tanpa harus memberikan AWS kredensi apa pun.

Note

Informasi lebih lanjut tentang mengonfigurasi federasi ke konsol AMS disediakan di:

- Zona Pendaratan Multi-Akun: [Mengonfigurasi Federasi ke Konsol AMS](#)
- Zona Pendaratan Akun Tunggal: [Mengonfigurasi Federasi ke Konsol AMS](#)

Selain itu, lihat [Lampiran: Aturan klaim AD FS dan setelan SAMP](#). Untuk informasi tentang penggunaan AWS Microsoft AD untuk mendukung aplikasi sadar Direktori Aktif Anda, di AWS Cloud, yang tunduk pada persyaratan kepatuhan, lihat Mengelola Kepatuhan [Microsoft](#) AD.

Direktori Aktif Terkelola AMS

AMS sekarang menawarkan layanan baru yang disebut Managed Active Directory (alias Managed AD) yang memungkinkan AMS untuk mengurus operasi infrastruktur Active Directory (AD) Anda, sambil menjaga Anda tetap mengendalikan administrasi Direktori Aktif Anda.

Dukungan AMS untuk Managed AD mirip dengan dukungan AMS untuk Amazon Relational Database Service (Amazon RDS). Dalam kedua kasus, AWS (termasuk AMS) mendukung pembuatan dan pengelolaan infrastruktur yang menjalankan layanan, sementara Anda melakukan kontrol akses dan semua fungsi administrasi. Model ini memiliki keunggulan sebagai berikut:

- Membatasi risiko keamanan: AWS dan AMS tidak memerlukan hak administratif untuk domain Anda.
- Integrasi langsung: Anda dapat menggunakan model otorisasi saat ini dan mengintegrasikannya dengan AD tanpa perlu berinteraksi dengan AMS.

Catatan:

- Baik AMS maupun Anda tidak akan memiliki akses ke pengontrol domain AD Terkelola Anda, sehingga tidak ada perangkat lunak yang dapat diinstal pada pengontrol domain. Ini penting karena solusi pihak ketiga yang memerlukan perangkat lunak untuk diinstal pada pengontrol domain tidak diperbolehkan.

Access berfungsi seperti ini:

- AWS Tim Directory Service: Memiliki akses ke pengontrol domain.
- AMS: Memiliki akses ke Directory Service APIs untuk melakukan tindakan tertentu pada domain. Tindakan ini termasuk mengambil snapshot AD, mengubah skema AD, dan tindakan lainnya.
- Anda: Memiliki akses ke domain (AD) untuk membuat pengguna, grup, dan sebagainya.
- Kami menyarankan Anda melakukan bukti konsep pada AD Terkelola sebelum memigrasikan iklan perusahaan Anda, karena tidak semua fungsionalitas dari lingkungan AD tradisional tersedia di lingkungan AD Terkelola.
- AMS tidak akan mengelola atau memberikan panduan tentang manajemen AD Anda. Misalnya, AMS tidak akan memberikan panduan tentang struktur Unit Organisasi, struktur kebijakan grup, konvensi penamaan pengguna AD, dan sebagainya.

Ini bekerja seperti ini:

1. AMS melakukan onboard baru Akun AWS untuk Anda, terpisah dari dan selain akun AMS Anda, dan menyediakan lingkungan Active Directory (AD) melalui AWS Directory Service (lihat juga [Apa itu AWS Directory Service?](#)).

Berikut ini adalah informasi yang perlu dikumpulkan oleh integrator sistem dari Anda agar AMS dapat bergabung dengan AD Terkelola:

- Informasi akun
 - ID akun Akun AWS yang dibuat untuk AD yang dikelola AMS: nomor Akun AWS
 - Wilayah untuk memasukkan iklan Terkelola Anda ke: Wilayah AWS
- Informasi Direktori Aktif Terkelola:
 - Microsoft AD Edition: Standar/Perusahaan. AWS Microsoft AD (Edisi Standar) mencakup 1 GB penyimpanan objek direktori. Kapasitas ini dapat mendukung hingga 5.000 pengguna atau 30.000 objek direktori, termasuk pengguna, grup, dan komputer. AWS Microsoft AD

(Enterprise Edition) mencakup penyimpanan objek direktori 17 GB, yang dapat mendukung hingga 100.000 pengguna atau 500.000 objek.

Untuk informasi selengkapnya, lihat [AWS Directory Service FAQs](#).

- Domain FQDN: FQDN untuk domain AMS Managed AD Anda.
- Nama Domain NetBIOS: Nama NetBIOS untuk domain AMS Managed AD Anda.
- Nomor akun standar AMS yang Anda inginkan untuk integrasi AD Terkelola (AMS mengonfigurasi kepercayaan satu arah dari AD akun AMS-Standard ke AD Terkelola)
- Apakah modifikasi Active Directory Schema diperlukan dan jika demikian, modifikasi apa?
- Secara default, dua pengontrol domain disediakan. Apakah Anda membutuhkan lebih banyak? Jika demikian, berapa banyak yang Anda butuhkan dan untuk alasan apa?
- Jaringan untuk informasi Direktori Aktif Terkelola:
 - CIDR VPC AD terkelola untuk pengontrol domain (CIDR dalam rentang subnet pribadi Anda untuk pengontrol domain AD Terkelola):
 - Subnet CIDR 1 untuk pengontrol domain: [CIDR Anda, harus menjadi bagian dari AMS Managed AD VPC CIDR]
 - Subnet CIDR 2 untuk pengontrol domain: [CIDR Anda, harus menjadi bagian dari AMS Managed AD VPC CIDR]

Misalnya:

- CIDR VPC AD Terkelola: 192.168.0.0/16
- CIDR 1 untuk pengontrol domain: 192.168.1.0/24
- CIDR 2 untuk pengontrol domain: 192.168.2.0/24

Untuk menghindari konflik alamat IP, pastikan CIDR VPC AD Terkelola yang Anda tentukan tidak bertentangan dengan CIDR subnet pribadi lainnya yang Anda gunakan di jaringan perusahaan Anda.

- Teknologi VPN (opsional): [Direct Connect/Direct Connect dan VPN]
 - Nomor Sistem Otonomi BGP (ASN) gateway Anda: [ASN yang disediakan pelanggan]
 - Alamat IP yang dapat dirutekan Internet untuk antarmuka luar gateway Anda, alamatnya harus statis: [Alamat IP yang Diberikan Pelanggan]
 - Apakah koneksi VPN Anda memerlukan rute statis atau tidak: [ya/tidak]

2. AMS memberi Anda kata sandi akun Admin untuk lingkungan AD dan meminta Anda untuk

mengatur ulang kata sandi sehingga teknisi AMS tidak dapat lagi mengakses lingkungan AD Anda.

3. Untuk mengatur ulang kata sandi akun Admin, sambungkan ke lingkungan Active Directory menggunakan Active Directory Users and Computers (ADUC). ADUC dan Remote Server Administration Tools (RSAT) lainnya harus diinstal dan dijalankan pada host Administratif yang disediakan oleh Anda pada infrastruktur non-AMS. Microsoft memiliki praktik terbaik untuk mengamankan host administratif tersebut. Untuk selengkapnya, lihat [Menerapkan Host Administratif Aman](#). Anda mengelola lingkungan Direktori Aktif Anda menggunakan host Administratif ini.
4. Dalam operasi harian, AMS mengelola Akun AWS hingga ke sisi AWS Directory Service; misalnya, konfigurasi VPC, pencadangan AD, pembuatan dan penghapusan kepercayaan AD, dan sebagainya. Anda menggunakan, dan mengelola, lingkungan iklan Anda; misalnya, pembuatan pengguna, pembuatan grup, pembuatan kebijakan grup, dan sebagainya.

Untuk tabel RACI terbaru, lihat bagian “Peran dan Tanggung Jawab” di Lihat [deskripsi Layanan](#).

Penerapan aplikasi AMS

Panduan Pengembang Aplikasi AMS memberikan deskripsi dan panduan terperinci untuk penerapan berikut:

- CT yang menyerap beban kerja AMS memungkinkan Anda dan mitra migrasi cloud AMS untuk dengan mudah memindahkan beban kerja yang ada ke VPC yang dikelola AMS. Menggunakan konsumsi beban kerja AMS, Anda dapat membuat AMS AMI dengan mengirimkan RFC dengan Deployment | Ingestion | Stack from migration partner migrated instance | Create CT (ct-257p9zjk14ija). Anda harus memiliki instance yang dimigrasikan dari lokal ke AWS mitra migrasi, serta VPC dan subnet AMS target, tempat instans akan tertelan.

Untuk detailnya, lihat panduan Pengembang Aplikasi AMS di [Workload Ingest](#).

- Fitur tipe perubahan AWS CloudFormation ingest (ct-36cn2avfrj9v) memungkinkan Anda menggunakan templat yang ada dengan mudah untuk menerapkan tumpukan khusus di VPC yang dikelola AMS. CloudFormation

Untuk detailnya, lihat panduan Pengembang Aplikasi AMS di [CloudFormation Template Ingest](#).

- Anda dapat mengimpor database lokal ke database baru ke bucket Amazon S3 yang dikelola AMS atau instans Amazon RDS. Anda melakukan ini menggunakan Deployment | Komponen tumpukan lanjutan | Jenis perubahan Database Migration Service (DMS), termasuk Buat instance

replikasi (ct-27apldkhqr0ol), Buat grup subnet replikasi (ct-2q5azjd8p1ag5), Buat tugas replikasi (ct-1d2fml15b9eth), Buat titik akhir sumber (ct-0attesnjqy2cx) atau Buat titik akhir sumber (S3) (ct-2oxl37nphsrjz), dan Buat titik akhir target (ct-3gf8dolbo8x9p) atau Buat titik akhir target (S3) (ct-05muqzievnk5).

Untuk detailnya, lihat panduan Pengembang Aplikasi AMS di [Database Migration Service](#).

- Anda dapat mengimpor database MS SQL lokal ke database baru pada instans SQL RDS yang dikelola AMS. Anda melakukan ini menggunakan berbagai jenis perubahan AMS, dan Amazon RDS API, ditambah AWS konsol.

Untuk detailnya, lihat Panduan Aplikasi AMS di [Database \(DB\) Impor ke MS SQL RDS](#).

Manajemen layanan di AWS Managed Services

Topik

- [Tata kelola akun di AWS Managed Services](#)
- [Dimulainya layanan di AWS Managed Services](#)
- [Manajemen hubungan pelanggan \(CRM\)](#)
- [Optimalisasi biaya di AWS Managed Services](#)
- [Jam layanan di AWS Managed Services](#)
- [Mendapatkan bantuan di AWS Managed Services](#)

Bagaimana layanan AMS bekerja untuk Anda.

Tata kelola akun di AWS Managed Services

Bagian ini mencakup tata kelola akun AMS.

Anda ditunjuk sebagai manajer pengiriman layanan cloud (CSDM) yang memberikan bantuan konsultasi di seluruh AMS, dan memiliki pemahaman terperinci tentang kasus penggunaan dan arsitektur teknologi Anda untuk lingkungan terkelola. CSDMs bekerja dengan manajer akun, manajer akun teknis, arsitek cloud AWS Managed Services (CAs), dan arsitek solusi AWS (SAs), sebagaimana berlaku, untuk membantu meluncurkan proyek baru dan memberikan rekomendasi praktik terbaik di seluruh proses pengembangan dan operasi perangkat lunak. CSDM adalah titik kontak utama untuk AMS. Tanggung jawab utama CSDM Anda adalah:

- Atur dan pimpin pertemuan tinjauan layanan bulanan dengan pelanggan.
- Berikan detail tentang keamanan, pembaruan perangkat lunak untuk lingkungan dan peluang untuk pengoptimalan.
- Juara persyaratan Anda termasuk permintaan fitur untuk AMS.
- Menanggapi dan menyelesaikan permintaan pelaporan penagihan dan layanan.
- Memberikan wawasan untuk rekomendasi optimalisasi keuangan dan kapasitas.

Dimulainya layanan di AWS Managed Services

Dimulainya Layanan: Tanggal Dimulainya Layanan untuk akun AWS Managed Services adalah hari pertama bulan kalender pertama setelah AWS memberi tahu Anda bahwa aktivitas yang ditetapkan dalam Persyaratan Orientasi untuk akun AWS Managed Services telah selesai; dengan ketentuan bahwa jika AWS membuat pemberitahuan tersebut setelah hari ke-20 dalam satu bulan kalender, Tanggal Dimulainya Layanan adalah hari pertama bulan kalender kedua setelah tanggal dari pemberitahuan tersebut.

Dimulainya Layanan

- R adalah singkatan dari pihak yang bertanggung jawab yang melakukan pekerjaan untuk mencapai tugas.
- Saya singkatan dari Informed; sebuah pihak yang diinformasikan tentang kemajuan, seringkali hanya pada penyelesaian tugas atau deliverable.

Dimulainya layanan

Langkah #	Judul langkah	Deskripsi	Pelanggan	AMS
1.	Serah terima akun AWS pelanggan	Pelanggan membuat akun AWS baru dan menyerahkannya ke AWS Managed Services	R	I
2.	Akun AWS Managed Services - desain	Menyelesaikan desain Akun AWS Managed Services	I	R
3.	Akun AWS Managed Services - build	Akun AWS Managed Services dibuat sesuai desain di Langkah 2	I	R

Manajemen hubungan pelanggan (CRM)

AWS Managed Services (AMS) menyediakan proses manajemen hubungan pelanggan (CRM) untuk memastikan bahwa hubungan yang terdefinisi dengan baik dibuat dan dipertahankan dengan Anda.

Dasar dari hubungan ini didasarkan pada wawasan AMS tentang kebutuhan bisnis Anda. Proses CRM memfasilitasi pemahaman yang akurat dan komprehensif tentang:

- Kebutuhan bisnis Anda dan cara mengisi kebutuhan tersebut
- Kemampuan dan kendala Anda
- AMS dan tanggung jawab dan kewajiban Anda yang berbeda

Proses CRM memungkinkan AMS untuk menggunakan metode yang konsisten untuk memberikan layanan kepada Anda dan menyediakan tata kelola untuk hubungan Anda dengan AMS. Proses CRM meliputi:

- Mengidentifikasi pemangku kepentingan utama Anda
- Membangun tim tata kelola
- Melakukan dan mendokumentasikan pertemuan tinjauan layanan dengan Anda
- Menyediakan prosedur pengaduan layanan formal dengan prosedur eskalasi
- Menerapkan dan memantau kepuasan dan proses umpan balik Anda
- Mengelola kontrak Anda

Proses CRM

Proses CRM mencakup kegiatan-kegiatan ini:

- Mengidentifikasi dan memahami proses dan kebutuhan bisnis Anda. Perjanjian Anda dengan AMS mengidentifikasi pemangku kepentingan Anda.
- Mendefinisikan layanan yang akan diberikan untuk memenuhi kebutuhan dan persyaratan Anda.
- Bertemu dengan Anda dalam rapat tinjauan layanan untuk membahas setiap perubahan dalam lingkup layanan AMS, SLA, kontrak, dan kebutuhan bisnis Anda. Pertemuan sementara dapat diadakan dengan Anda untuk membahas kinerja, prestasi, masalah, dan rencana tindakan.
- Memantau kepuasan Anda dengan menggunakan survei kepuasan pelanggan kami dan umpan balik yang diberikan pada rapat.
- Melaporkan kinerja pada laporan kinerja bulanan yang diukur secara internal.
- Meninjau layanan dengan Anda untuk menentukan peluang perbaikan. Ini termasuk komunikasi yang sering dengan Anda mengenai tingkat dan kualitas layanan AMS yang disediakan.

Rapat CRM

Manajer pengiriman layanan cloud AMS (CSDMs) melakukan pertemuan dengan Anda secara teratur untuk mendiskusikan jalur layanan (operasi, keamanan, dan inovasi produk) dan trek eksekutif (laporan SLA, ukuran kepuasan, dan perubahan kebutuhan bisnis Anda).

Rapat	Tujuan	Mode	Peserta
Ulasan status mingguan (opsional)	Masalah atau insiden yang luar biasa, penambalan, peristiwa keamanan, catatan masalah Tren operasional 12 minggu (+/- 6) Kekhawatiran operator aplikasi Jadwal akhir pekan	Pelanggan di tempat location/ Telecom/Chime	AMS: CSDM dan arsitek cloud (CA) Anggota tim yang ditugaskan pelanggan (mis.: Cloud/ Infrastructure, Application Support, Architecture teams, dll.)
Ulasan bisnis bulanan	Meninjau kinerja tingkat layanan (laporan, analisis, dan tren) Analisis keuangan Peta jalan produk CSAT	Pelanggan di tempat location/ Telecom/Chime	AMS: CSDM, arsitek cloud (CA), tim akun AMS, manajer produk teknis AMS (TPM) (opsional), manajer AMS OPS (opsional) Anda: Perwakilan Operator Aplikasi

Rapat	Tujuan	Mode	Peserta
Ulasan bisnis triwulanan	Kinerja dan tren Scorecard dan Service Level Agreement (SLA) (6 bulan) Rencana/migrasi 3/6/9/12 bulan mendatang Mitigasi risiko dan risiko Inisiatif perbaikan utama Item peta jalan produk Peluang selaras arah masa depan Keuangan Inisiatif penghematan biaya Optimalisasi bisnis	Lokasi pelanggan di tempat	AMS: CSDM, arsitek cloud, tim akun AMS, direktur layanan AMS, manajer operasi AMS Anda: Perwakilan operator aplikasi, perwakilan layanan, direktur layanan

Pengaturan Rapat CRM

AMS CSDM bertanggung jawab untuk mendokumentasikan pertemuan, termasuk:

- Membuat agenda, termasuk item tindakan, masalah, dan daftar peserta.
- Membuat daftar item tindakan yang ditinjau pada setiap pertemuan untuk memastikan item selesai dan diselesaikan sesuai jadwal.
- Mendistribusikan notulen rapat dan daftar item tindakan kepada peserta rapat melalui email dalam satu hari kerja setelah rapat.
- Menyimpan notulen rapat di repositori dokumen yang sesuai.

Dengan tidak adanya CSDM, perwakilan AMS yang memimpin rapat membuat dan mendistribusikan risalah.

Note

CSDM Anda bekerja sama dengan Anda untuk menetapkan tata kelola akun Anda.

Laporan bulanan CRM

AMS CSDM Anda mempersiapkan dan mengirimkan presentasi kinerja layanan bulanan. Presentasi mencakup informasi tentang hal-hal berikut:

- Tanggal laporan
- Ringkasan dan Wawasan:
 - Key Call Out: jumlah tumpukan total dan aktif, status tambalan tumpukan, status orientasi akun (hanya selama orientasi), ringkasan masalah khusus pelanggan
 - Performa: Statistik tentang resolusi insiden, peringatan, penambalan, permintaan perubahan (RFCs), permintaan layanan, dan ketersediaan konsol dan API
 - Masalah, tantangan, kekhawatiran, dan risiko: Status masalah khusus pelanggan
 - Item mendatang: Rencana orientasi atau resolusi insiden khusus pelanggan
- Sumber Daya Terkelola: Grafik dan diagram lingkaran tumpukan
- Metrik AMS: Metrik pemantauan dan peristiwa, metrik insiden, metrik kepatuhan AMS SLA, metrik permintaan layanan, metrik manajemen perubahan, metrik penyimpanan, metrik kontinuitas, metrik Trusted Advisor, dan ringkasan biaya (disajikan beberapa cara). Permintaan fitur. Informasi kontak.

Note

Selain informasi yang dijelaskan, CSDM Anda juga memberi tahu Anda tentang perubahan material dalam ruang lingkup atau ketentuan, termasuk penggunaan subkontraktor oleh AMS untuk kegiatan operasional.

AMS menghasilkan laporan tentang penambalan dan pencadangan yang disertakan CSDM Anda dalam laporan bulanan Anda. Sebagai bagian dari sistem pembuatan laporan, AMS menambahkan beberapa infrastruktur ke akun Anda yang tidak dapat diakses oleh Anda:

- Bucket S3, dengan data mentah dilaporkan
- Contoh Athena, dengan definisi kueri untuk menanyakan data
- Glue Crawler untuk membaca data mentah dari bucket S3

Optimalisasi biaya di AWS Managed Services

AWS Managed Services menyediakan laporan pemanfaatan biaya dan penghematan terperinci setiap bulan kepada Anda selama tinjauan bisnis bulanan Anda (MBRs).

AMS mengikuti serangkaian proses dan mekanisme standar untuk mengidentifikasi jalan penghematan biaya di akun terkelola Anda dan membantu Anda merencanakan dan meluncurkan perubahan untuk mengoptimalkan pengeluaran AWS Anda.

Note

AMS sedang mengembangkan video untuk membantu optimasi biaya. Langkah pertama adalah memberi Anda PDF dan spreadsheet Excel tentang praktik terbaik pengoptimalan biaya. Untuk mengakses sumber daya ini, buka [Panduan cepat untuk pengoptimalan biaya](#) file ZIP.

Kerangka kerja pengoptimalan biaya

AMS mengikuti pendekatan tiga tahap dengan Anda untuk mengoptimalkan biaya AWS Anda:

1. Identifikasi jalan pengoptimalan biaya di lingkungan terkelola Anda
2. Sajikan rencana pengoptimalan biaya untuk Anda
3. Membantu dalam mencapai optimalisasi biaya dengan cara yang terukur

Identifikasi jalan optimasi biaya di lingkungan yang dikelola

AMS menggunakan alat AWS asli seperti Cost explorer, dan Trusted Advisor sambil memanfaatkan lebih dari 20 pola penghematan biaya di seluruh pengoptimalan arsitektur EC2, instans, AWS dan pengoptimalan yang berfokus pada akun untuk membangun rekomendasi penghematan biaya yang disesuaikan untuk Anda.

Beberapa rekomendasi pengoptimalan meliputi yang berikut ini.

Rekomendasi optimasi arsitektur:

- Penggunaan kelas penyimpanan S3 yang optimal: Amazon S3 menawarkan berbagai kelas penyimpanan untuk memenuhi berbagai persyaratan beban kerja berdasarkan akses data,

ketahanan, dan biaya. Analisis kelas penyimpanan S3 Intelligent-Tiering dan S3 berdasarkan kebutuhan beban kerja memungkinkan Anda mengelola biaya S3 secara efisien.

- Menggunakan arsitektur caching: Memanfaatkan instance cache, jika berlaku, dapat membantu Anda mengganti beberapa instance database, sekaligus memenuhi persyaratan IOPS Anda.
- Penghematan peningkatan EBS: Migrasi volume EBS Anda dari gp2 ke gp3 memberikan penghematan biaya hingga 20% dan Anda dapat memanfaatkan kinerja dasar 3.000 IOPS yang dapat diprediksi dan 125 MiB/s, terlepas dari ukuran volume.
- Menggunakan elastisitas: Kemampuan auto-scaling yang menyediakan memungkinkan pemanfaatan sumber daya AWS yang efektif dan jalan untuk optimalisasi biaya. Meninjau dan memperbarui kebijakan penskalaan instans secara teratur berdasarkan kebutuhan, selanjutnya memberikan penghematan biaya.

EC2 rekomendasi yang berfokus pada contoh

- Pengukuran instans: Rekomendasi berfokus pada ukuran instance dan konfigurasi optimal berdasarkan penggunaan. Rekomendasi juga mencakup penggunaan fitur Amazon EC2 Auto Scaling dan EC2 mengganti instans jika berlaku AWS Lambda dengan atau konten web statis di Amazon S3, dll.
- Penjadwalan instans: Menggunakan Penjadwal Sumber Daya AMS untuk memulai dan menghentikan instans secara otomatis berdasarkan jadwal waktu membantu menahan biaya, terutama untuk instans non-produksi yang tidak digunakan selama jam non-bisnis.
- Berlangganan paket Tabungan: Paket tabungan adalah cara termudah untuk menghemat AWS penggunaan. EC2 Instance Savings Plans menawarkan penghematan hingga 72% dibandingkan dengan harga Sesuai Permintaan untuk penggunaan EC2 instans Amazon Anda. Amazon SageMaker AI Savings Plans menawarkan penghematan hingga 64% untuk penggunaan layanan Amazon SageMaker AI Anda. AMS memberikan rekomendasi yang sesuai tentang paket Tabungan berdasarkan penggunaan AWS sumber daya Anda.
- Panduan penggunaan dan konsumsi instans cadangan (RI): Instans EC2 Cadangan Amazon (RI) memberikan diskon signifikan (hingga 75%) dibandingkan dengan harga Sesuai Permintaan dan menyediakan reservasi kapasitas saat digunakan di zona ketersediaan tertentu.
- Penggunaan instans spot: Beban kerja toleran kesalahan dapat memanfaatkan instans Spot dan mengurangi harga hingga 90%.
- Pengakhiran instans idle: Mengidentifikasi dan melaporkan instance yang menganggur atau memiliki pemanfaatan rendah yang dapat dihentikan.

Rekomendasi yang berfokus pada akun

- Pembersihan akun: Pada tingkat akun, AMS juga mengidentifikasi volume EBS yang tidak digunakan, CloudTrail jejak duplikat, akun kosong dengan sumber daya yang tidak digunakan, dan sebagainya, dan memberikan rekomendasi untuk pembersihan.
- Rekomendasi SLA: Selanjutnya, AMS secara teratur meninjau akun Plus dan Premium Anda dan merekomendasikan memilih tingkat SLA yang tepat untuk akun tersebut.
- Optimalisasi otomatisasi AMS: AMS terus memilih otomatisasi AMS dan infrastruktur yang digunakan untuk menyediakan layanan AMS.

Hadir untuk pelanggan dan membantu dalam perencanaan

AMS melakukan tinjauan bisnis bulanan (MBRs) dengan pemangku kepentingan pelanggan utama dan menyajikan jalan penghematan biaya, mekanisme, dan rekomendasi yang diidentifikasi bersama dengan potensi penghematan biaya. Kami selanjutnya bekerja dengan Anda untuk merencanakan perubahan yang diperlukan.

Membantu dalam implementasi rekomendasi dan mengukur dampak biaya

AMS membantu dalam mencapai dan mengukur dampak biaya dan perubahan optimasi.

Anda menilai dampak aplikasi, risiko, dan kriteria keberhasilan dari perubahan yang disarankan, dan mengajukan permintaan perubahan (RFCs) yang sesuai melalui konsol AMS. AMS berkolaborasi dengan Anda dan mengimplementasikan perubahan yang terkait dengan pengoptimalan biaya di akun terkelola Anda. AMS mengukur dampak biaya dan memasukkan penghematan yang direalisasikan dalam tinjauan bisnis bulanan (MBRs).

Matriks tanggung jawab optimasi biaya

Tanggung jawab dalam optimasi biaya AMS.

Optimalisasi biaya RACI

Aktifitas	Pelanggan	AMS
Menyusun rekomendasi penghemat	I	R

Aktifitas	Pelanggan	AMS
an biaya dan menyiapka n laporan		
Menyajika n laporan penghemat an biaya	C	R
Perubahan perencana an yang terkait dengan penghemat an biaya	R	C
Menilai dampak dan risiko perubahan	R	C
Meningkat kan RFCs untuk menerapka n perubahan	R	C

Aktifitas	Pelanggan	AMS
Meninjau RFCs dan menerapkan perubahan	C	R
Menguji aplikasi dan memvalidasi implementasi perubahan	R	C
Mengukur dampak biaya pasca perubahan dan presentasi kepada pelanggan	I	R

Jam layanan di AWS Managed Services

Fitur	AMS Lanjutan
	Tingkat Premium
Permintaan layanan	24/7

Fitur	AMS Lanjutan
	Tingkat Premium
Manajemen insiden (P2-P3)	24/7
Pencadangan dan pemulihan	24/7
Manajemen tambalan	24/7
Pemantauan dan peringatan	24/7
Permintaan otomatis untuk perubahan (RFC)	24/7
Permintaan perubahan non-otomatis (RFC)	24/7
Manajer pengiriman layanan cloud (CSDM)	Senin sampai Jumat: 08:00 — 17:00, jam kerja lokal

Mendapatkan bantuan di AWS Managed Services

AMS mendukung Anda dengan Manajemen Insiden, Manajemen Permintaan Layanan, dan Manajemen Perubahan 24 jam sehari, 7 hari seminggu, 365 hari setahun (sesuai dengan Perjanjian Tingkat Layanan AMS yang diterapkan pada akun).

Untuk melaporkan masalah kinerja layanan AWS atau AMS yang memengaruhi lingkungan terkelola Anda, gunakan konsol AMS dan kirimkan laporan insiden. Untuk detailnya, lihat [Melaporkan insiden](#). Untuk informasi umum tentang manajemen insiden AMS, lihat [Respons insiden](#).

Untuk meminta informasi atau saran, atau meminta layanan tambahan dari AMS, gunakan konsol AMS dan kirimkan permintaan layanan. Untuk detailnya, [Membuat Permintaan Layanan](#). Untuk informasi umum tentang permintaan layanan AMS, lihat [Manajemen Permintaan Layanan](#).

Manajemen acara yang direncanakan di AWS Managed Services

AWS Managed Services (AMS) planned event management (PEM) adalah penawaran layanan AMS. PEM terlibat, mengkoordinasikan, dan membantu selama acara dan proyek pelanggan menggunakan layanan AMS. PEM membantu dalam mengoordinasikan serangkaian terkait RFCs yang selaras dengan ruang lingkup dan garis waktu yang disepakati dari acara atau proyek PEM.

Kriteria AMS PEM

Acara yang direncanakan adalah proyek yang terikat ruang lingkup dan terikat waktu. AMS menggunakan detail yang Anda berikan (termasuk rencana dan ruang lingkup, hasil yang diharapkan, dan perubahan yang diharapkan dilakukan oleh operasi AMS) untuk mendukung Anda secara efektif selama aktivitas PEM. Cloud Architects (CAs) Anda kemudian meninjau dan menilai aktivitas PEM untuk kelengkapan, implementasi teknis, dan keterlibatan operasi AMS. Setelah peninjauan CA, operasi AMS meninjau rencana dan berkoordinasi dengan manajer pengiriman layanan cloud (CSDM) Anda untuk keterlibatan tim operasi.

Jenis PEM

Berikut ini adalah jenis PEM yang tersedia:

- Gamedays
 - Operational Gameday: Pendekatan game berbasis skenario untuk respons operasional, yang bertujuan untuk memvalidasi integrasi proses, orang, dan sistem.
 - Security Gameday: Strategi respons insiden keamanan yang menggunakan pendekatan game berbasis skenario untuk menilai integrasi sistem, proses, dan personel.
- CATATAN: Gunakan fitur AMS “bawa keamanan titik akhir Anda sendiri” (BYOEPS) untuk mengganti agen Trend Micro Deep Security default dengan solusi keamanan titik akhir pilihan Anda atau lisensi Trend Micro khusus. Untuk informasi selengkapnya, lihat [AMS membawa EPS Anda sendiri](#).
- Pemulihan Bencana: Acara Pemulihan Bencana melibatkan AMS yang membantu Anda selama kegiatan DR yang direncanakan. Untuk informasi selengkapnya, lihat [Perencanaan pemulihan bencana](#).

- Acara Keamanan Pelanggan: Acara keamanan yang direncanakan. Misalnya, aktivitas pengguna root dan pengujian penetrasi.
- Dukungan Migrasi: Dukungan untuk aktivitas orientasi dan migrasi yang direncanakan.

Alur kerja ini memfasilitasi kolaborasi dengan AMS untuk mengoordinasikan acara yang direncanakan dan aktivitas migrasi terkait dukungan AMS. Untuk pelaksanaan prioritas RFCs, ini adalah praktik terbaik untuk menggunakan keterlibatan Operations on Demand (OOD). Untuk informasi selengkapnya, lihat [Operasi Sesuai Permintaan](#).

Proses AMS PEM

Proses PEM terdiri dari fase-fase berikut:

- Inisiasi PEM: Anda bekerja dengan CSDM Anda untuk menentukan tujuan Anda untuk acara yang direncanakan dan menentukan apa yang dibutuhkan dari Operasi AMS. AMS CAs meninjau aspek teknis dari rencana PEM. CAs Bekerja dengan AMS Security and Operations pada kepatuhan, optimasi eksekusi dan otomatisasi, dan untuk menentukan tugas dan kiriman eksekusi pra-PEM. Kemudian, CSDM Anda membuat tiket PEM dan memberikan AMS informasi proyek dan detail teknis. AMS memerlukan waktu tunggu 14 hari kalender untuk memungkinkan waktu tim Operasi AMS merencanakan, memberikan tinjauan teknis, dan menetapkan sumber daya.
- Tinjauan PEM: Tim Operasi AMS meninjau permintaan PEM dan bekerja dengan CSDM Anda untuk memverifikasi bahwa informasi dalam paket PEM sudah benar dan lengkap.
- Penerimaan PEM: AMS meninjau informasi yang diberikan dan mengkomunikasikan kepada CSDM berapa tingkat dukungan selama aktivitas PEM. Jika PEM berisi informasi lengkap dan CSDM Anda setuju dengan ruang lingkup pekerjaan, maka PEM disetujui.
- Kesiapan dan eksekusi: AMS memastikan bahwa tugas yang diperlukan sebelum PEM dimulai selesai dan memfasilitasi komunikasi internal dan pelanggan. AMS memastikan bahwa paket PEM berjalan dengan benar dan menyediakan pelaporan status dan kemajuan.

PEM FAQs

Bagaimana cara melibatkan AMS dengan RFC/Service Permintaan (SR) selama acara PEM?

- Gunakan ID PEM yang dibagikan oleh CSDM Anda di baris RFC/SR subjek dalam format. **PEM-ID**

- Anda juga dapat membuat Permintaan Layanan (SR) untuk mendiskusikan kasus penggunaan Anda atau untuk pertanyaan tentang acara yang Anda rencanakan. Jika Anda menggunakan SR, maka PEM tidak harus valid.

Validasi apa yang dilakukan ketika RFC terkait PEM dikirimkan?

- Verifikasi bahwa ID Akun terdaftar di PEM.
- Verifikasi bahwa status PEM disetujui dan aktif antara tanggal mulai dan berakhir yang disediakan.

Apakah ada SLAs atau SLOs untuk permintaan PEM?

- PEMs tidak terkait dengan SLAs atau SLOs.
- SLAs dan SLOs untuk item pekerjaan terkait PEM (RFC/Permintaan Layanan) ditentukan oleh AMS. SLOs

Untuk informasi selengkapnya, lihat [sasaran tingkat layanan AMS \(SLOs\)](#).

Bisakah kita membuat PEM melalui Permintaan Layanan (SR)?

- Tidak, pembuatan PEM harus dikelola oleh Cloud Service Delivery Manager (CSDM).

Arsitektur jaringan

AWS Managed Services (AMS) menawarkan dua arsitektur jaringan:

- Multi-account landing zone (MALZ): menyediakan layanan umum - seperti akses, keamanan titik akhir, jaringan - dari akun bersama untuk beban kerja yang digunakan di akun anggota terpisah.
- Single-account landing zone (SALZ): menyediakan akun mandiri di mana layanan umum seperti akses, keamanan titik akhir, jaringan digunakan di akun yang sama dengan beban kerja. Disarankan untuk beban kerja yang memerlukan tingkat isolasi yang tinggi karena menimbulkan biaya AWS yang lebih tinggi.

Arsitektur jaringan MALZ

Tentang arsitektur jaringan landing zone multi-akun

Sebelum memulai proses orientasi ke AWS Managed Services (AMS) Multi-account landing zone (MALZ) AWS Managed Services (AMS), penting untuk memahami arsitektur dasar, atau landing zone, yang dibuat AMS atas nama Anda, komponen, dan fungsinya.

AMS multi-account landing zone adalah arsitektur multi-akun, pra-konfigurasi dengan infrastruktur untuk memfasilitasi otentikasi, keamanan, jaringan, dan logging.

Note

Untuk perkiraan biaya, lihat [komponen dasar lingkungan landing zone multi-akun AMS](#).

Topik

- [Wilayah layanan](#)
- [Unit organisasi](#)
- [Kebijakan kontrol layanan dan AWS Organization](#)

Diagram berikut menguraikan pada tingkat tinggi struktur akun dan bagaimana infrastruktur dipisahkan ke dalam masing-masing akun:

Wilayah layanan

Semua sumber daya dalam landing zone multi-akun AMS digunakan dalam satu Wilayah AWS pilihan Anda, karena batasan lintas wilayah saat ini dengan Active Directory dan Transit Gateway.

Unit organisasi

Landing zone multi-akun AMS yang khas terdiri dari empat unit organisasi tingkat atas (OUs):

- Unit Organisasi inti (OU) (digunakan untuk mengelompokkan akun bersama untuk mengelola sebagai satu unit)
- Aplikasi OU
- OU yang dikelola pelanggan
- Percepatan OU

Landing zone multi-akun yang dikelola AMS juga memungkinkan Anda membuat kustom OUs untuk mengelompokkan dan mengatur Akun AWS dan mengaitkan kustom SCPs dengannya; untuk contoh dalam melakukan ini, lihat Akun manajemen | Membuat [akun Kustom OUs dan Manajemen | Buat SCP Kustom \(perlu ditinjau\)](#), masing-masing. AMS menyediakan empat yang sudah ada OUs di mana akun baru OUs dan dapat diminta: akselerasi, aplikasi> dikelola, aplikasi> pengembangan, dan dikelola pelanggan.

- mempercepat OU:

Ini adalah OU tingkat atas di AMS multi-account landing zone (MALZ). Akun di bawah OU ini disediakan oleh AMS dengan RFC (Deployment | Managed landing zone | Managed landing zone | Management account | Create Accelerate account, change type ID: ct-2p93tyd5angmi). Dalam akun aplikasi akselerasi ini, Anda bisa mendapatkan keuntungan dari mempercepat layanan operasional seperti pemantauan dan peringatan, manajemen insiden, manajemen keamanan, dan manajemen cadangan. Untuk detail selengkapnya, lihat [akun AMS Accelerate](#).

- aplikasi> OU terkelola:

Dalam unit sub organisasi Aplikasi OU ini, akun dikelola sepenuhnya oleh AMS termasuk semua tugas operasional. Tugas operasional meliputi manajemen permintaan layanan, manajemen insiden, manajemen keamanan, manajemen kontinuitas, manajemen patch, optimalisasi biaya, pemantauan dan manajemen acara. Tugas-tugas ini dilakukan untuk manajemen infrastruktur

Anda. Beberapa anak OUs dapat dibuat sesuai kebutuhan, hingga batas maksimum nested OUs tercapai untuk organisasi AWS. Untuk detailnya, lihat [Kuota untuk AWS Organizations](#).

- aplikasi> pengembangan OU:

Di bawah Sub-OU aplikasi OU ini di landing zone yang dikelola AMS, akun adalah akun [mode Pengembang](#) yang memberi Anda izin tinggi untuk menyediakan dan memperbarui sumber daya AWS di luar proses manajemen perubahan AMS. OU ini juga mendukung penciptaan anak-anak baru OU sesuai kebutuhan.

- OU yang dikelola pelanggan:

Ini adalah OU tingkat atas di landing zone multi-akun AMS. Akun di bawah OU ini disediakan oleh AMS dengan RFC. Di akun ini, pengoperasian beban kerja dan sumber daya AWS adalah tanggung jawab Anda. OU ini juga mendukung penciptaan anak-anak baru OU sesuai kebutuhan.

Sebagai praktik terbaik, kami merekomendasikan agar akun di bawah ini OUs dan sub- permintaan khusus OUs dikelompokkan berdasarkan fungsi dan kebijakan mereka.

Kebijakan kontrol layanan dan AWS Organization

AWS menyediakan kebijakan kontrol layanan (SCPs) untuk manajemen izin di Organisasi AWS. SCPs digunakan untuk menentukan pagar pembatas tambahan untuk tindakan apa yang dapat dilakukan pengguna di mana. OUs Secara default, AMS menyediakan satu set yang SCPs digunakan dalam akun manajemen yang memberikan perlindungan pada tingkat OU default yang berbeda. Untuk pembatasan SCP, silakan hubungi CSDM Anda.

Anda juga dapat membuat kustom SCPs dan melampirkannya ke spesifik OUs. Mereka dapat diminta dari akun Manajemen Anda menggunakan jenis perubahan ct-33ste5yc7hprs. AMS kemudian meninjau kustom SCPs yang diminta sebelum menerapkannya ke target OUs. Untuk contoh, lihat [Akun manajemen | Membuat akun Kustom OUs](#) dan [Manajemen | Buat SCP Kustom \(Review Required\)](#).

Memilih MALZ tunggal atau ganda MALZs

Tabel berikut memberikan beberapa pertimbangan tingkat tinggi untuk memutuskan antara landing zone multi-akun tunggal (MALZ) vs beberapa zona pendaratan multi-akun (misalnya, dua zona pendaratan multi-akun - Prod dan non-PROD). Secara umum, pilihan tergantung pada kebutuhan individu, persyaratan hukum, dan praktik operasi.

Landing zone multi-akun tunggal vs. beberapa zona pendaratan multi-akun

Entitas	Zona pendaratan AMS tunggal	Beberapa (dua atau lebih) zona pendaratan
Biaya dasar	Lebih rendah, dioptimalkan sekitar \$3.000 per bulan.	Lebih tinggi, biaya tambahan sekitar \$3.000 per lingkungan.
Penagihan	Tagihan tunggal, karena akun Penagihan/Manajemen tunggal.	Pisahkan tagihan untuk setiap landing zone multi-akun. Saat ini AWS Org tidak mendukung akun Multi-manajemen dengan satu tagihan.
Portabilitas instance cadangan yang ada () RIs	Rendah. AWS RIs saat ini tidak dapat dikonversi di beberapa akun penagihan . Anda akan menggunakan kembali yang ada RIs untuk landing zone multi-akun.	Lebih rendah. Anda akan menggunakan kembali dan mendistribusikan RIs di semua landing zone multi-akun.
Diskon tingkat produk	Tinggi. Lihat diskon Volume .	Rendah. Lihat diskon Volume .
Overhead pengaturan awal (pada project/migration garis waktu)	Rendah. Integrasi Active Directory , jaringan dan single sign-on (SSO) hanya sekali.	Tinggi. Anda akan melakukan Active Directory, integrasi jaringan, dan integrasi SSO untuk setiap landing zone. Ini dapat menyebabkan penundaan potensial pada proyek migrasi apa pun.
Konfigurasi layanan umum	Upaya rendah. Anda mengonfigurasi common/shared layanan seperti DNS, cadangan, pemantauan, pencatatan, dll.	Upaya tinggi. Perencanaan tambahan diperlukan untuk mengatasi di mana infrastruktur atau layanan umum akan duduk. Lalu lintas melintasi beberapa gateway transit (TGWs) di setiap landing zone, dapat menyebabkan biaya tambahan.

Entitas	Zona pendaratan AMS tunggal	Beberapa (dua atau lebih) zona pendaratan
Skalabilitas	Sedang. AMS memiliki batas praktis saat ini sebesar 150 akun per landing zone multi-akun. Beberapa tim atau vendor yang menjalankan aplikasi di akun yang sama dapat memiliki akses ke tumpukan yang dimiliki oleh tim yang berbeda. Keterbatasan ini dapat dikurangi dengan mengontrol akses ke tumpukan khusus aplikasi di ServiceNow lapisan (dengan mengintegrasikan aplikasi ServiceNow Konektor AMS dan memanfaatkan tag). Tanyakan kepada manajer pengiriman teknis AMS (TDMs) atau arsitek cloud (CAs) bagaimana menerapkan ini.	Tinggi. Kemampuan untuk memanfaatkan beberapa landing zone multi-akun untuk mendistribusikan akun sambil mencapai tingkat segregasi akun atau aplikasi. Mengelola sejumlah besar akun dapat menyebabkan overhead operasional atau biaya.
Risiko Operasional	(Tergantung) Rendah. Integrasi operasional dan kesiapan hanya sekali. Lebih sedikit peluang proses melayang.	(Tergantung) Rendah. Integrasi ganda dan kegiatan operasional. Melayang di beberapa zona pendaratan selama periode tersebut dapat menyebabkan risiko operasional.
Wilayah Multi AWS	Wilayah AWS Tunggal. AMS multi-account landing zone dibatasi untuk satu Wilayah AWS. Untuk menjangkau beberapa Wilayah AWS, gunakan beberapa landing zone multi-akun.	Wilayah Multi AWS. Dengan beberapa zona pendaratan multi-akun, Anda dapat menempatkan setiap MALZ di satu wilayah dan menghubungkannya menggunakan pengintip transit gateway (TGW).

Entitas	Zona pendaratan AMS tunggal	Beberapa (dua atau lebih) zona pendaratan
Migrasi akun atau portabilitas	Ya. Memindahkan akun dari satu OU ke OU lainnya dalam AWS Organization yang sama dimungkinkan.	Tidak. AMS tidak mendukung migrasi akun di seluruh zona pendaratan; yaitu, di seluruh AWS Organizations. Beban kerja dapat menjangkau melintasi zona pendaratan dengan transit gateway (TGW) atau VPC peering.
Manajemen perubahan	Sedang. Membuat perubahan destruktif pada komponen umum seperti TGW, Active Directory (AD), atau outbound (egress) dapat memengaruhi semua beban kerja di landing zone multi-akun. Namun, perubahan pada komponen yang dikelola AMS diuji secara internal dan didorong dalam pembaruan bergulir.	Rendah. Membuat perubahan destruktif pada komponen umum seperti TGW, AD, atau outbound (egress) hanya dapat memengaruhi beban kerja di landing zone multi-akun tertentu.
Kontrol data dan akses	(Tergantung) Kontrol rendah jika Anda ingin terhubung ke lokasi ADs dan jaringan yang berbeda untuk beban kerja Prod vs Non-Prod. Federasi SAM, domain TGW, dan kelompok keamanan (SGs) dapat membantu mengimplementasikan kontrol yang diperlukan juga.	(Tergantung) Kontrol tinggi jika Anda ingin terhubung ke lokasi ADs dan jaringan yang berbeda untuk beban kerja Prod vs Non-Prod. Gunakan zona pendaratan terpisah untuk persyaratan kepatuhan yang ketat.

Entitas	Zona pendaratan AMS tunggal	Beberapa (dua atau lebih) zona pendaratan
Kepatuhan dan Keamanan	(Tergantung) Rendah jika ada kebutuhan kepatuhan yang ketat untuk sepenuhnya memisahkan beban kerja material vs non-material. Kontrol pencegahan dan detektif standar AMS diberlakukan.	(Tergantung) Tinggi karena beberapa landing zone multi-akun dapat membantu mencapai persyaratan kepatuhan yang ketat dengan sepenuhnya memisahkan beban kerja material vs non-material. Kontrol pencegahan dan detektif standar AMS diberlakukan.

Rekomendasi: Tanpa Kepatuhan yang ketat atau kebutuhan Multi-wilayah, dimulai dengan landing zone multi-akun AMS tunggal akan mencapai keseimbangan yang baik antara biaya, keamanan, keunggulan operasional, dan kompleksitas migrasi. Anda selalu dapat mengatur landing zone tambahan, jika ada kendala akun atau bisnis yang ditemui.

Landing zone multi-akun tunggal vs. Beberapa landing zone multi-akun FAQs

Beberapa pertanyaan umum ketika memilih untuk mengatur satu landing zone multi-akun atau beberapa zona pendaratan multi-akun:

T1: Dapatkah saya memulai dengan landing zone multi-akun tunggal dan pindah ke beberapa landing zone multi-akun, jika ada batasan akun atau kendala bisnis yang ditemui?

A: Ya. Anda dapat memilih untuk mengatur landing zone multi-akun lain pada waktu tertentu:

- Akun pembayar tagihan baru akan diminta untuk disiapkan (saat ini AWS tidak mendukung akun multi-pembayar dalam satu organisasi AWS).
- Pembuatan basis Zona Pendaratan Multi-Akun membutuhkan waktu tunggu hingga 2 minggu setelah kuesioner landing zone multi-akun diisi.
- Setiap landing zone multi-akun berarti penambahan biaya operasional ~ 3K USD/bulan.
- Integrasi N/W, AD, DNS, dan SSO akan diperlukan untuk membangun MALZ baru.
- Setiap Instans Cadangan (RIs), paket Penghematan Biaya akan diperlukan untuk disiapkan untuk landing zone multi-akun baru (RIs tidak dapat ditransfer).

- AMS multi-account landing zone tidak mendukung migrasi akun di seluruh akun landing zone multi-akun; misalnya, di AWS Orgs. Namun, untuk memindahkan aplikasi dari satu akun ke akun lain dimungkinkan menggunakan metode migrasi standar.

T2: Apa pendekatan AMS terhadap MALZ updates/changes terhadap underlying/shared infrastruktur dan mengukur risiko bagi pelanggan? Berikan rincian tentang jaminan apa yang dibungkus ke dalam proses. Bagaimana Pelanggan merasa nyaman bahwa MALZ tidak updates/changes akan berdampak pada pelanggan? Apakah ada tindakan yang perlu dilakukan Pelanggan untuk mencegah gangguan?

J: AMS mengikuti metodologi perubahan ketat menggunakan alat internal yang memungkinkan kami untuk menentukan, meninjau, menjadwalkan, dan mengeksekusi perubahan pada lingkungan pelanggan.

Proses untuk merilis pembaruan memberlakukan tinjauan kode, pengujian integrasi, penerapan di lingkungan gamma dan beta, serta waktu pemanggangan dan pengujian tambahan di lingkungan beta dan gamma sebelum dirilis ke lingkungan pelanggan. Semua rilis mencakup prosedur rollback dan dipantau secara ketat oleh tim rilis dan tim yang membuat dan meminta perubahan. Ruang lingkup rilis terbatas pada tumpukan yang dimiliki dan disediakan oleh AMS. Rata-rata, kami mengeksekusi setidaknya satu rilis per minggu.

Selain itu:

- AMS SLA berlaku. Sesuai deskripsi layanan AMS, setiap insiden yang muncul setelah aktivitas pemeliharaan infra bersama akan mematuhi SLA yang berhak untuk resolusi atau kredit.
- Tidak ada tindakan pencegahan khusus yang diperlukan oleh Pelanggan untuk mencegah gangguan pada infrastruktur umum. Pelanggan memiliki izin Hanya Baca di akun AWS Org atau Core OU, sehingga pelanggan tidak dapat membuat perubahan destruktif apa pun pada env inti MALZ. Semua permintaan pelanggan terhadap infrastruktur Inti memerlukan peninjauan dan persetujuan AMS.
- Pelanggan dapat menguji perubahan level Org tertentu seperti SCPs/Roles pada level akun non-prod individu sebelum menyebarkan perubahan di level App OU. Ini ada di peta jalan AMS untuk memungkinkan beberapa APP OUs (Q2 2020), yang selanjutnya akan mengurangi risiko dalam membuat beberapa perubahan tingkat ORG. Tim MALZ telah merilis OU terpisah untuk akun "Build Mode", untuk memastikan pemisahan kepemilikan pelanggan dan kontrol terpisah yang jelas.
- Sebagian besar adalah perubahan yang memungkinkan AMS untuk mengoperasikan beban kerja secara efektif dan efisien dan tidak selalu memengaruhi beban kerja pelanggan. Di mana

AMS percaya perubahan infra bersama dapat berdampak pada beban kerja pelanggan, mereka kemudian diselaraskan dengan jendela perubahan pelanggan.

Rekomendasi tingkat tinggi, mulailah dengan beberapa zona pendaratan multi-akun jika:

- Jika itu membantu Anda mencapai kepatuhan tertentu.
- Jika Anda perlu menggunakan Multi-Region.
- Jika Anda memiliki on-prem ADs dan Networks yang berbeda untuk Prod/Material vs Non-beban kerjaProd/Non-Material workloads, to clearly segregate b/w.

Akun Zona Pendaratan Multi-Akun

Topik

- [Akun manajemen](#)
- [Akun jaringan](#)
- [Akun Layanan Bersama](#)
- [Akun Arsip Log](#)
- [Akun keamanan](#)
- [Jenis akun aplikasi](#)
- [Akun AMS Tools \(memigrasikan beban kerja\)](#)

Akun manajemen

Akun manajemen adalah akun AWS awal Anda saat Anda mulai melakukan orientasi dengan AMS. Ini menggunakan AWS Organizations sebagai akun manajemen (juga dikenal sebagai akun pembayar yang membayar biaya semua akun anggota), yang memberikan akun kemampuan untuk membuat dan mengelola akun anggota secara finansial. Ini berisi kerangka kerja AWS landing zone (ALZ), set tumpukan konfigurasi akun, kebijakan kontrol layanan AWS Organization (SCPs), dll.

Untuk informasi selengkapnya tentang penggunaan akun manajemen, lihat [Praktik terbaik untuk akun manajemen](#).

Diagram berikut memberikan gambaran tingkat tinggi dari sumber daya yang terkandung dalam akun manajemen.

Sumber daya di akun manajemen

Selain layanan standar di atas, tidak ada sumber daya AWS tambahan yang dibuat di akun manajemen selama orientasi. Input berikut diperlukan selama orientasi ke AMS:

- ID akun manajemen: ID Akun AWS yang awalnya dibuat oleh Anda.
- Email Akun Inti: Berikan email yang akan dikaitkan dengan masing-masing akun inti: Jaringan, Layanan Bersama, Logging, dan akun Keamanan.
- Wilayah Layanan: Menyediakan wilayah AWS tempat semua sumber daya dari landing zone AMS Anda akan digunakan.

Akun jaringan

Akun Networking berfungsi sebagai hub pusat untuk perutean jaringan antara akun landing zone multi-akun AMS, jaringan lokal Anda, dan lalu lintas keluar ke Internet. Selain itu, akun ini berisi benteng DMZ publik yang merupakan titik masuk bagi insinyur AMS untuk mengakses host di lingkungan AMS. Untuk detailnya, lihat diagram tingkat tinggi berikut dari akun jaringan di bawah ini.

Arsitektur akun jaringan

Diagram berikut menggambarkan lingkungan landing zone multi-akun AMS, menampilkan arus lalu lintas jaringan di seluruh akun, dan merupakan contoh pengaturan yang sangat tersedia.

AMS mengonfigurasi semua aspek jaringan untuk Anda berdasarkan templat standar kami dan opsi pilihan Anda yang disediakan selama orientasi. Desain jaringan AWS standar diterapkan ke akun AWS Anda, dan VPC dibuat untuk Anda dan terhubung ke AMS oleh VPN atau Direct Connect. Untuk informasi selengkapnya tentang Direct Connect, lihat [AWS Direct Connect](#). Standar VPCs termasuk DMZ, layanan bersama, dan subnet aplikasi. Selama proses orientasi, tambahan VPCs mungkin diminta dan dibuat agar sesuai dengan kebutuhan Anda (misalnya, divisi pelanggan, mitra). Setelah onboarding, Anda diberikan diagram jaringan: dokumen lingkungan yang menjelaskan bagaimana jaringan Anda telah diatur.

Note

Untuk informasi tentang batasan dan batasan layanan default untuk semua layanan aktif, lihat dokumentasi [AWS Service Limits](#).

Desain jaringan kami dibangun di sekitar [“Prinsip Hak Istimewa Terkecil”](#) Amazon. Untuk mencapai hal ini, kami merutekan semua lalu lintas, masuk dan keluar, melalui DMZ, kecuali lalu lintas yang berasal dari jaringan tepercaya. Satu-satunya jaringan tepercaya adalah jaringan yang dikonfigurasi antara lingkungan lokal Anda dan VPC melalui penggunaan and/or VPN dan AWS Direct Connect (DX). Akses diberikan melalui penggunaan instans benteng, sehingga mencegah akses langsung ke sumber daya produksi apa pun. Semua aplikasi dan sumber daya Anda berada di dalam subnet pribadi yang dapat dijangkau melalui penyeimbang beban publik. Lalu lintas jalan keluar publik mengalir melalui NAT Gateways di jalan keluar VPC (di akun Jaringan) ke Internet Gateway dan kemudian ke Internet. Atau, lalu lintas dapat mengalir melalui VPN atau Direct Connect ke lingkungan lokal Anda.

Konektivitas jaringan pribadi ke lingkungan landing zone multi-akun AMS

AWS menawarkan konektivitas pribadi melalui konektivitas jaringan pribadi virtual (VPN), atau jalur khusus dengan AWS Direct Connect. Konektivitas pribadi di lingkungan multi-akun Anda, diatur menggunakan salah satu metode yang dijelaskan berikut:

- Konektivitas Edge terpusat menggunakan Transit Gateway
- Menghubungkan Direct Connect (DX) and/or VPN ke akun virtual private cloud () VPCs

Konektivitas tepi terpusat menggunakan gateway transit

AWS Transit Gateway adalah layanan yang memungkinkan Anda menghubungkan jaringan lokal VPCs dan lokal ke satu gateway. Transit gateway (TGW) dapat digunakan untuk mengkonsolidasikan konektivitas edge yang ada dan mengarahkannya melalui satu titik. ingress/egress Transit gateway dibuat di akun jaringan lingkungan multi-akun AMS Anda. Untuk detail selengkapnya tentang gateway transit, lihat [AWS Transit Gateway](#).

Gateway AWS Direct Connect (DX) digunakan untuk menghubungkan koneksi DX Anda melalui antarmuka virtual transit ke VPCs atau VPNs yang dilampirkan ke gateway transit Anda. Anda mengaitkan gateway Direct Connect dengan transit gateway. Kemudian, buat antarmuka virtual

transit untuk koneksi AWS Direct Connect Anda ke gateway Direct Connect. Untuk informasi tentang antarmuka virtual DX, lihat [AWS Direct Connect Virtual Interfaces](#).

Konfigurasi ini menawarkan manfaat sebagai berikut. Anda dapat:

- Kelola satu koneksi untuk beberapa VPCs atau VPNs yang berada di Wilayah AWS yang sama.
- Iklankan awalan dari lokal ke AWS, dan dari AWS ke lokal.

Note

[Untuk informasi tentang penggunaan DX dengan layanan AWS, lihat bagian Ketahanan Toolkit Klasik.](#) Untuk informasi selengkapnya, lihat [asosiasi Transit Gateway](#).

Untuk meningkatkan ketahanan konektivitas Anda, kami sarankan Anda melampirkan setidaknya dua antarmuka virtual transit dari lokasi AWS Direct Connect yang berbeda ke gateway Direct Connect. Untuk informasi selengkapnya, lihat rekomendasi [ketahanan AWS Direct Connect](#).

Menghubungkan DX atau VPN ke akun VPCs

Dengan opsi ini, lingkungan landing zone multi-akun AMS Anda terhubung langsung ke Direct Connect atau VPN. VPCs Lalu lintas langsung mengalir dari VPCs ke Direct Connect atau VPN tanpa melintasi gateway transit.

Sumber daya di akun jaringan

Seperti yang ditunjukkan pada diagram akun jaringan, komponen berikut dibuat di akun dan memerlukan masukan Anda.

Akun Networking berisi dua VPCs: Egress VPC dan DMZ VPC juga dikenal sebagai Perimeter VPC.

Manajer Jaringan AWS

AWS Network Manager adalah layanan yang memungkinkan Anda memvisualisasikan jaringan transit gateway (TGW) Anda tanpa biaya tambahan ke AMS. Ini menyediakan pemantauan jaringan terpusat pada sumber daya AWS dan pada jaringan lokal, satu tampilan global jaringan pribadi mereka dalam diagram topologi dan dalam peta geografis, dan metrik pemanfaatan, seperti status

koneksi byte. in/out, packets in/out, packets dropped, and alerts for changes in the topology, routing, and up/down Untuk informasi, lihat [AWS Network Manager](#).

Gunakan salah satu peran berikut untuk mengakses sumber daya ini:

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

Keluar VPC

VPC Egress terutama digunakan untuk lalu lintas keluar ke Internet dan terdiri dari public/private subnet di hingga tiga zona ketersediaan (). AZs Gateway terjemahan alamat jaringan (NAT) disediakan di subnet publik, dan lampiran VPC transit gateway (TGW) dibuat di subnet pribadi. Jalan keluar, atau keluar, lalu lintas internet dari semua jaringan masuk melalui subnet pribadi melalui TGW, di mana kemudian dialihkan ke NAT melalui tabel rute VPC.

Untuk Anda VPCs yang berisi aplikasi yang menghadap publik di subnet publik, lalu lintas yang berasal dari internet terkandung dalam VPC itu. Lalu lintas kembali tidak diarahkan ke TGW atau Egress VPC, tetapi dirutekan kembali melalui internet gateway (IGW) di VPC.

Note

Rentang CIDR VPC Jaringan: Saat Anda membuat VPC, Anda harus menentukan rentang alamat IPv4 untuk VPC dalam bentuk blok Classless Inter-Domain Routing (CIDR); misalnya, 10.0.16.0/24. Ini akan menjadi blok CIDR utama VPC Anda.

Tim landing zone multi-akun AMS merekomendasikan rentang 24 (dengan lebih banyak alamat IP) untuk menyediakan beberapa buffer jika sumber daya/peralatan lain, digunakan di masa mendatang.

Firewall jalan keluar Palo Alto yang dikelola

AMS menyediakan solusi firewall jalan keluar Palo Alto Terkelola, yang memungkinkan pemfilteran lalu lintas keluar internet untuk semua jaringan di lingkungan Zona Pendaratan Multi-Akun (tidak termasuk layanan yang dihadapi publik). Solusi ini menggabungkan teknologi firewall terkemuka di industri (Palo Alto VM-300) dengan kemampuan manajemen infrastruktur AMS untuk menyebarkan, memantau, mengelola, menskalakan, dan memulihkan infrastruktur dalam lingkungan operasi yang

sesuai. Pihak ketiga, termasuk Palo Alto Networks, tidak memiliki akses ke firewall; mereka dikelola hanya oleh insinyur AMS.

Kontrol lalu lintas

Solusi firewall keluar terkelola mengelola daftar izin domain yang terdiri dari domain yang diperlukan AMS untuk layanan seperti cadangan dan tambalan, serta domain yang Anda tentukan. Ketika lalu lintas internet keluar diarahkan ke firewall, sesi dibuka, lalu lintas dievaluasi, dan jika cocok dengan domain yang diizinkan, lalu lintas diteruskan ke tujuan.

Arsitektur

Solusi firewall jalan keluar terkelola mengikuti model ketersediaan tinggi, di mana dua hingga tiga firewall digunakan tergantung pada jumlah zona ketersediaan (). AZs Solusinya menggunakan bagian dari ruang IP dari VPC keluar default, tetapi juga menyediakan ekstensi VPC (/24) untuk sumber daya tambahan yang diperlukan untuk mengelola firewall.

Aliran jaringan

Pada tingkat tinggi, perutean lalu lintas jalan keluar publik tetap sama, kecuali bagaimana lalu lintas diarahkan ke internet dari VPC jalan keluar:

1. Lalu lintas jalan keluar yang ditujukan untuk internet dikirim ke Transit Gateway (TGW) melalui tabel rute VPC
2. TGW merutekan lalu lintas ke VPC jalan keluar melalui tabel rute TGW
3. VPC merutekan lalu lintas ke internet melalui tabel rute subnet pribadi
 - a. Di lingkungan Zona Pendaratan Multi-Akun default, lalu lintas internet dikirim langsung ke gateway terjemahan alamat jaringan (NAT). Solusi firewall terkelola mengkonfigurasi ulang tabel rute subnet pribadi untuk mengarahkan rute default (0.0.0.0/0) ke antarmuka firewall sebagai gantinya.

Firewall itu sendiri berisi tiga antarmuka:

1. Antarmuka tepercaya: Antarmuka pribadi untuk menerima lalu lintas yang akan diproses.
2. Antarmuka tidak tepercaya: Antarmuka publik untuk mengirim lalu lintas ke internet. Karena firewall menjalankan NAT, server eksternal menerima permintaan dari alamat IP publik ini.

3. Antarmuka manajemen: Antarmuka pribadi untuk API firewall, pembaruan, konsol, dan sebagainya.

Sepanjang semua perutean, lalu lintas dipertahankan dalam zona ketersediaan yang sama (AZ) untuk mengurangi lalu lintas lintas AZ. Lalu lintas hanya melintas AZs ketika failover terjadi.

Modifikasi daftar izinkan

Setelah onboarding, daftar izin default dibuat, berisi titik akhir publik yang diperlukan AMS serta titik akhir publik untuk `ams-allowlist` menambal host Windows dan Linux. Setelah beroperasi, Anda dapat membuat RFC di konsol AMS di bawah kategori Manajemen | Managed Firewall | Outbound (Palo Alto) untuk membuat atau menghapus daftar yang diizinkan, atau memodifikasi domain. Ketahuilah bahwa `ams-allowlist` tidak dapat dimodifikasi. RFC ditangani dengan otomatisasi penuh (tidak manual).

Kebijakan keamanan khusus

Kebijakan keamanan menentukan apakah akan memblokir atau mengizinkan sesi berdasarkan atribut lalu lintas, seperti zona keamanan sumber dan tujuan, alamat IP sumber dan tujuan, dan layanan. Kebijakan keamanan khusus didukung dengan sepenuhnya otomatis RFCs. CTs untuk membuat atau menghapus kebijakan keamanan dapat ditemukan di bawah kategori Manajemen | Firewall Terkelola | Keluar (Palo Alto), dan CT untuk mengedit kebijakan keamanan yang ada dapat ditemukan di bawah kategori Deployment | Managed Firewall | Outbound (Palo Alto). Anda akan dapat membuat kebijakan keamanan baru, mengubah kebijakan keamanan, atau menghapus kebijakan keamanan.

Note

Kebijakan keamanan default `ams-allowlist` tidak dapat diubah

CloudWatch Dasbor jalan keluar PA

Dua dasbor dapat ditemukan CloudWatch untuk memberikan tampilan agregat Palo Alto (PA). dasbor AMS-MF-PA-Egress-config-menyajikan ikhtisar konfigurasi PA, tautan ke daftar izin, dan daftar semua kebijakan keamanan termasuk atributnya. Dasbor AMS-MF-PA-Egress dapat disesuaikan untuk memfilter log lalu lintas. Misalnya, untuk membuat dasbor untuk kebijakan keamanan, Anda dapat membuat RFC dengan filter seperti:

[illegible]

Model failover

Solusi firewall mencakup dua-tiga host Palo Alto (PA) (satu per AZ). Kenari cek sehat berjalan dengan jadwal konstan untuk mengevaluasi kesehatan tuan rumah. Jika host diidentifikasi sebagai tidak sehat, AMS diberi tahu dan lalu lintas untuk AZ tersebut secara otomatis dialihkan ke host yang sehat di AZ yang berbeda melalui perubahan tabel rute. Karena alur kerja pemeriksaan kesehatan berjalan terus-menerus, jika host menjadi sehat kembali karena masalah sementara atau remediasi manual, lalu lintas digeser kembali ke AZ yang benar dengan host yang sehat.

Penskalaan

AMS memonitor firewall untuk batas throughput dan penskalaan. Ketika batas throughput melebihi ambang batas watermark yang lebih rendah (CPU/jaringan), AMS menerima peringatan. Ambang batas pembuat air yang rendah menunjukkan bahwa sumber daya mendekati saturasi, mencapai titik di mana AMS akan mengevaluasi metrik dari waktu ke waktu dan menjangkau untuk menyarankan solusi penskalaan.

Pencadangan dan Pemulihan

Cadangan dibuat selama peluncuran awal, setelah perubahan konfigurasi apa pun, dan pada interval reguler. Pencadangan peluncuran awal dibuat berdasarkan per host, tetapi perubahan konfigurasi dan pencadangan interval reguler dilakukan di semua host firewall saat alur kerja cadangan dipanggil. Insinyur AMS dapat membuat cadangan tambahan di luar jendela tersebut atau memberikan detail cadangan jika diminta.

Insinyur AMS dapat melakukan pemulihan cadangan konfigurasi jika diperlukan. Jika restorasi diperlukan, itu akan terjadi di semua host untuk menjaga konfigurasi antar host tetap sinkron.

Restorasi juga dapat terjadi ketika host membutuhkan daur ulang lengkap dari sebuah instance. Pemulihan otomatis cadangan terbaru terjadi ketika EC2 instance baru disediakan. Secara umum, host tidak didaur ulang secara teratur, dan dicadangkan untuk kegagalan berat atau swap AMI yang diperlukan. Daur ulang host dimulai secara manual, dan Anda diberi tahu sebelum daur ulang terjadi.

Selain cadangan konfigurasi firewall, aturan daftar izin khusus Anda dicadangkan secara terpisah. Cadangan dibuat secara otomatis ketika aturan daftar izin yang Anda tetapkan diubah. Pemulihan cadangan daftar izin dapat dilakukan oleh insinyur AMS, jika diperlukan.

Pembaruan

Solusi Firewall Terkelola AMS memerlukan berbagai pembaruan dari waktu ke waktu untuk menambahkan peningkatan pada sistem, fitur tambahan, atau pembaruan ke sistem operasi firewall (OS) atau perangkat lunak.

Sebagian besar perubahan tidak akan mempengaruhi lingkungan berjalan seperti memperbarui infrastruktur otomatisasi, tetapi perubahan lain seperti rotasi instance firewall atau pembaruan OS dapat menyebabkan gangguan. Ketika potensi gangguan layanan karena pembaruan dievaluasi, AMS akan berkoordinasi dengan Anda untuk mengakomodasi jendela pemeliharaan.

Akses operator

Operator AMS menggunakan ActiveDirectory kredensialnya untuk masuk ke perangkat Palo Alto untuk melakukan operasi (misalnya, menambal, menanggapi suatu peristiwa, dll.). Solusi ini mempertahankan otentikasi Operator AMS standar dan log perubahan konfigurasi untuk melacak tindakan yang dilakukan pada Host Palo Alto.

Log default

Secara default, log yang dihasilkan oleh firewall berada di penyimpanan lokal untuk setiap firewall. Seiring waktu, log lokal akan dihapus berdasarkan pemanfaatan penyimpanan. Solusi AMS menyediakan pengiriman log off mesin secara real-time ke CloudWatch log; untuk informasi lebih lanjut, lihat [CloudWatch Integrasi log](#).

Insinyur AMS masih memiliki kemampuan untuk menanyakan dan mengekspor log langsung dari mesin jika diperlukan. Selain itu, log dapat dikirim ke Panorama milik pelanggan; untuk informasi lebih lanjut, lihat [Integrasi Panorama](#)

Log yang dikumpulkan oleh solusi adalah sebagai berikut:

Kode Status RFC

Jenis Log	Deskripsi
Lalu lintas	Menampilkan entri untuk awal dan akhir setiap sesi. Setiap entri mencakup tanggal dan waktu, zona sumber dan tujuan, alamat dan port, nama aplikasi, nama aturan keamanan yang diterapkan pada alur, tindakan aturan (izinkan, tolak, atau jatuhkan), antarmuka masuk dan keluar, jumlah byte, dan alasan akhir sesi. Kolom Type menunjukkan apakah entri untuk awal atau akhir sesi, atau apakah sesi ditolak atau dibatalkan. “Penurunan” menunjukkan bahwa aturan keamanan yang memblokir lalu lintas yang ditentukan aplikasi “apa saja”, sedangkan “penolakan” menunjukkan aturan mengidentifikasi aplikasi tertentu. Jika lalu lintas dijatuhkan sebelum aplikasi diidentifikasi, seperti ketika aturan menjatuhkan semua lalu lintas untuk layanan tertentu, aplikasi ditampilkan sebagai “tidak berlaku”.
Ancaman	Menampilkan entri untuk setiap alarm keamanan yang dihasilkan oleh firewall. Setiap entri mencakup tanggal dan waktu, nama ancaman atau URL, zona sumber dan tujuan, alamat, dan port, nama aplikasi, dan tindakan alarm (izinkan atau blokir) dan tingkat keparahan. Kolom Type menunjukkan jenis ancaman, seperti “virus” atau “spyware;” kolom Nama adalah deskripsi ancaman atau URL; dan kolom Kategori adalah kategori ancaman (seperti “keylogger”) atau kategori URL.
Penyaringan URL	Menampilkan log untuk filter URL, yang mengontrol akses ke situs web dan apakah pengguna dapat mengirimkan kredensial ke situs web.
Konfigurasi	Menampilkan entri untuk setiap perubahan konfigurasi. Setiap entri mencakup tanggal dan waktu, nama pengguna administrator, alamat IP dari mana perubahan dilakukan, jenis klien (antarmuka web atau CLI), jenis perintah yang dijalankan, apakah perintah berhasil atau gagal, jalur konfigurasi, dan nilai sebelum dan sesudah perubahan.

Jenis Log	Deskripsi
Sistem	Menampilkan entri untuk setiap acara sistem. Setiap entri mencakup tanggal dan waktu, tingkat keparahan acara, dan deskripsi acara.
Alarm	Log alarm mencatat informasi terperinci tentang alarm yang dihasilkan oleh sistem. Informasi dalam log ini juga dilaporkan di Alarm. Lihat “Tentukan Pengaturan Alarm”.
Autentikasi	Menampilkan informasi tentang peristiwa otentikasi yang terjadi ketika pengguna akhir mencoba mengakses sumber daya jaringan yang aksesnya dikendalikan oleh aturan kebijakan Otentikasi. Pengguna dapat menggunakan informasi ini untuk membantu memecahkan masalah akses dan menyesuaikan kebijakan Autentikasi pengguna sesuai kebutuhan. Dalam hubungannya dengan objek korelasi, pengguna juga dapat menggunakan log Otentikasi untuk mengidentifikasi aktivitas mencurigakan di jaringan pengguna, seperti serangan brute force. Secara opsional, pengguna dapat mengonfigurasi aturan Otentikasi ke Timeout Otentikasi Log. Batas waktu ini berhubungan dengan periode waktu ketika pengguna membutuhkan otentikasi untuk sumber daya hanya sekali tetapi dapat mengaksesnya berulang kali. Melihat informasi tentang batas waktu membantu pengguna memutuskan apakah dan bagaimana menyesuaikannya.
Terpadu	Menampilkan entri log Traffic, Threat, URL Filtering, WildFire Submissions, dan Data Filtering terbaru dalam satu tampilan. Tampilan log kolektif memungkinkan pengguna untuk menyelidiki dan memfilter berbagai jenis log ini bersama-sama (alih-alih mencari setiap set log secara terpisah). Atau, pengguna dapat memilih jenis log mana yang akan ditampilkan: klik panah di sebelah kiri bidang filter dan pilih lalu lintas, ancaman, url, data, and/or api untuk hanya menampilkan jenis log yang dipilih.

Manajemen acara

AMS terus memantau kapasitas, status kesehatan, dan ketersediaan firewall. Metrik yang dihasilkan dari firewall, serta metrik AWS/AMS yang dihasilkan, digunakan untuk membuat alarm yang diterima

oleh insinyur operasi AMS, yang akan menyelidiki dan menyelesaikan masalah. Alarm saat ini mencakup kasus-kasus berikut:

Alarm Acara:

- Pemanfaatan CPU Dataplane Firewall
 - Pemanfaatan CPU - CPU Dataplane (Memproses lalu lintas)
- Pemanfaatan Paket Dataplane Firewall di atas 80%
 - Pemanfaatan paket - Dataplane (Memproses lalu lintas)
- Pemanfaatan Sesi Dataplane Firewall
- Sesi Dataplane Firewall Aktif
- Pemanfaatan CPU Firewall Agregat
 - Pemanfaatan CPU di semua CPUs
- Failover Oleh AZ
 - Alarm saat kegagalan terjadi di AZ
- Host Syslog Tidak Sehat
 - Host Syslog gagal dalam pemeriksaan kesehatan

Alarm Manajemen:

- Alarm Kegagalan Monitor Pemeriksaan Kesehatan
 - Ketika alur kerja pemeriksaan kesehatan gagal secara tak terduga
 - Ini untuk alur kerja itu sendiri, bukan jika pemeriksaan kesehatan firewall gagal
- Alarm Kegagalan Rotasi Sandi
 - Saat rotasi kata sandi gagal
 - Kata sandi pengguna API/layanan diputar setiap 90 hari

Metrik

Semua metrik ditangkap dan disimpan CloudWatch di akun Jaringan. Ini dapat dilihat dengan mendapatkan akses konsol ke akun Jaringan dan menavigasi ke konsol. CloudWatch Metrik individual dapat dilihat di bawah tab metrik atau tampilan dasbor panel tunggal dari metrik tertentu dan metrik agregat dapat dilihat dengan menavigasi ke tab Dasbor, dan memilih dasbor AMS-MF-PA-Egress.

Metrik Kustom:

- Pemeriksaan Kondisi
 - Namespace: AMS/MF/PA/Egress
 - PARouteTableConnectionsByAZ
 - PAUnhealthyByInstance
 - PAUnhealthyAggregatedByAZ
 - PAHealthCheckLockState
- Firewall Dihasilkan
 - Ruang nama:/AMS/MF/PA/Egress<instance-id>
 - DataPlaneCPUUtilizationPct
 - DataPlanePacketBufferUtilization
 - panci GPGateway UtilizationPct
 - panSessionActive
 - panSessionUtilization

CloudWatch Integrasi log

CloudWatch Integrasi log meneruskan log dari firewall ke CloudWatch Log, yang mengurangi risiko kehilangan log karena pemanfaatan penyimpanan lokal. Log diisi secara real-time saat firewall menghasilkannya, dan dapat dilihat sesuai permintaan melalui konsol atau API.

Kueri kompleks dapat dibuat untuk analisis log atau diekspor ke CSV menggunakan Wawasan. CloudWatch Selain itu, CloudWatch dasbor AMS Managed Firewall kustom juga akan menampilkan tampilan cepat dari kueri log lalu lintas tertentu dan visualisasi grafik lalu lintas dan klik kebijakan dari waktu ke waktu. Memanfaatkan CloudWatch log juga memungkinkan integrasi asli ke layanan AWS lainnya seperti AWS Kinesis.

Note

Log PA tidak dapat langsung diteruskan ke kolektor Syslog on-prem atau pihak ketiga yang ada. Solusi AMS Managed Firewall menyediakan pengiriman real-time log off dari mesin PA ke AWS CloudWatch Logs. Anda dapat menggunakan fitur CloudWatch Log Insight untuk menjalankan kueri ad-hoc. Selain itu, log dapat dikirim ke solusi manajemen Panorama Palo Alto Anda. CloudWatch log juga dapat diteruskan ke tujuan lain menggunakan Filter

CloudWatch Langganan. Pelajari lebih lanjut tentang Panorama di bagian berikut. Untuk mempelajari lebih lanjut tentang Splunk, lihat [Mengintegrasikan dengan Splunk](#).

Integrasi Panorama

AMS Managed Firewall dapat, opsional, diintegrasikan dengan Panorama Anda yang ada. Ini memungkinkan Anda untuk melihat konfigurasi firewall dari Panorama atau meneruskan log dari firewall ke Panorama. Integrasi Panorama dengan AMS Managed Firewall hanya dibaca, dan perubahan konfigurasi pada firewall dari Panorama tidak diperbolehkan. Panorama sepenuhnya dikelola dan dikonfigurasi oleh Anda, AMS hanya akan bertanggung jawab untuk mengonfigurasi firewall untuk berkomunikasi dengannya.

Lisensi

Harga Firewall Terkelola AMS tergantung pada jenis lisensi yang digunakan, setiap jam atau membawa lisensi Anda sendiri (BYOL), dan ukuran instans di mana alat berjalan. Anda diharuskan memesan ukuran instans dan lisensi firewall Palo Alto yang Anda inginkan melalui AWS Marketplace.

- Lisensi Marketplace: Terima syarat dan ketentuan Bundel Firewall Generasi Berikutnya Seri VM 1 dari akun jaringan di MALZ.
- Lisensi BYOL: Terima syarat dan ketentuan Firewall Generasi Berikutnya (BYOL) Seri VM dari akun jaringan di MALZ dan bagikan “kode autentikasi BYOL” yang diperoleh setelah membeli lisensi ke AMS.

Batasan

Saat ini, AMS mendukung firewall seri VM-300 atau seri VM-500. Konfigurasi dapat ditemukan di sini: Model [Seri VM pada Instans AWS](#), EC2

Note

Solusi AMS berjalan dalam mode Aktif-Aktif karena setiap instans PA di AZ-nya menangani lalu lintas keluar untuk AZ mereka yang dihormati. Jadi, dengan dua AZs, setiap instans PA menangani lalu lintas keluar hingga 5 Gbps dan secara efektif memberikan throughput 10 Gbps keseluruhan di dua. AZs Hal yang sama berlaku untuk semua batasan di setiap AZ. Jika pemeriksaan kesehatan AMS gagal, kami mengalihkan lalu lintas dari AZ dengan PA buruk ke AZ lain, dan selama penggantian instans, kapasitas dikurangi ke AZs batas yang tersisa.

AMS saat ini tidak mendukung bundel Palo Alto lain yang tersedia di AWS Marketplace; misalnya, Anda tidak dapat meminta “Bundel Firewall Generasi Berikutnya Seri VM 2”. Perhatikan bahwa solusi AMS Managed Firewall yang menggunakan Palo Alto saat ini hanya menyediakan penawaran pemfilteran lalu lintas keluar, jadi menggunakan bundel seri VM lanjutan tidak akan memberikan fitur atau manfaat tambahan apa pun.

Persyaratan orientasi

- Anda harus meninjau dan menyetujui Syarat dan Ketentuan Firewall Generasi Berikutnya Seri VM dari Palo Alto di AWS Marketplace.
- Anda harus mengonfirmasi ukuran instans yang ingin Anda gunakan berdasarkan beban kerja yang diharapkan.
- Anda harus menyediakan Blok CIDR /24 yang tidak bertentangan dengan jaringan di lingkungan Zona Pendaratan Multi-Akun atau On-Prem Anda. Itu harus dari kelas yang sama dengan Egress VPC (Solusi menyediakan ekstensi/24 VPC ke VPC Egress).

Harga

Biaya infrastruktur dasar AMS Managed Firewall dibagi dalam tiga driver utama: EC2 instance yang menghosting firewall Palo Alto, lisensi perangkat lunak Palo Alto VM-series lisensi, dan Integrasi CloudWatch

Harga berikut didasarkan pada firewall seri VM-300.

- EC2 Contoh: Firewall Palo Alto berjalan dalam model ketersediaan tinggi 2-3 EC2 instance, di mana instance didasarkan pada beban kerja yang diharapkan. Biaya untuk contoh tergantung pada wilayah dan jumlah AZs
 - Mantan us-east-1, m5.xlarge, 3 AZs
 - $\$0,192 * 24 * 30 * 3 = \$414,72$
 - [https://aws.amazon.com/ec2/harga/sesuai permintaan/](https://aws.amazon.com/ec2/harga/sesuai%20permintaan/)
- Lisensi Palo Alto: Biaya lisensi perangkat lunak dari firewall generasi berikutnya Palo Alto VM-300 tergantung pada jumlah AZ serta jenis instans.
 - Mantan us-east-1, m5.xlarge, 3 AZs
 - $\$0,87 * 24 * 30 * 3 = \$1879,20$
 - https://aws.amazon.com/marketplace/pp/B083m7jpkB?ref_=srh_res_product_title#pdp-harga

- CloudWatch Integrasi CloudWatch Log: integrasi log menggunakan SysLog server (EC2 - t3.medium), NLB, dan Log. CloudWatch Biaya server didasarkan pada wilayah dan jumlah AZs, dan biaya NLB/CloudWatch log bervariasi berdasarkan pemanfaatan lalu lintas.
- Contoh us-east-1, t3.medium, 3AZ
 - $\$0,0416 * 24 * 30 * 3 = \$89,86$
- [https://aws.amazon.com/ec2/harga/sesuai permintaan/](https://aws.amazon.com/ec2/harga/sesuai%20permintaan/)
- <https://aws.amazon.com/cloudwatch/harga/>

Perimeter (DMZ) VPC

Perimeter, atau DMZ, VPC berisi sumber daya yang diperlukan untuk insinyur Operasi AMS untuk mengakses jaringan AMS. Ini berisi subnet publik di 2-3 AZs, dengan host SSH Bastions dalam grup Auto Scaling (ASG) untuk insinyur Operasi AMS untuk masuk atau melalui terowongan. Kelompok keamanan yang melekat pada benteng DMZ berisi aturan masuk port 22 dari Amazon Corp Networks.

Rentang CIDR VPC DMZ: Saat Anda membuat VPC, Anda harus menentukan rentang alamat IPv4 untuk VPC dalam bentuk blok Classless Inter-Domain Routing (CIDR); misalnya, 10.0.16.0/24. Ini akan menjadi blok CIDR utama VPC Anda.

Note

Tim AMS merekomendasikan rentang 24 (dengan lebih banyak alamat IP) untuk menyediakan beberapa buffer jika sumber daya lain, seperti firewall, digunakan di masa depan.

AWS Transit Gateway

AWS Transit Gateway (TGW) adalah layanan yang memungkinkan Anda menghubungkan Amazon Virtual Private Clouds (VPCs) dan jaringan lokal Anda ke satu gateway. Transit gateway adalah backbone jaringan yang menangani routing antara jaringan akun AMS dan jaringan eksternal. Untuk informasi tentang Transit Gateway, lihat [AWS Transit Gateway](#).

Berikan masukan berikut untuk membuat sumber daya ini:

- Nomor ASN Transit Gateway *: Berikan Nomor Sistem Otonomi pribadi (ASN) untuk gateway transit Anda. Ini harus menjadi ASN untuk sisi AWS dari sesi Border Gateway Protocol (BGP). Kisarannya adalah 64512 hingga 65534 untuk 16-bit. ASNs

Akun Layanan Bersama

Akun Layanan Bersama berfungsi sebagai hub pusat untuk sebagian besar layanan pesawat data AMS. Akun berisi infrastruktur dan sumber daya yang diperlukan untuk manajemen akses (AD), manajemen keamanan titik akhir (Trend Micro), dan berisi benteng pelanggan (SSH/RDP). Gambaran umum tingkat tinggi dari sumber daya yang terkandung dalam Akun Layanan Bersama ditampilkan dalam grafik berikut.

VPC Layanan Bersama terdiri dari subnet AD, subnet EPS, dan subnet benteng pelanggan di tiga zona ketersediaan (). AZs Sumber daya yang dibuat dalam VPC Layanan Bersama tercantum di bawah ini dan memerlukan masukan Anda.

- Rentang CIDR VPC Layanan Bersama: Saat Anda membuat VPC, Anda harus menentukan rentang alamat IPv4 untuk VPC dalam bentuk blok Classless Inter-Domain Routing (CIDR); misalnya, 10.0.1.0/24. Ini akan menjadi blok CIDR utama VPC Anda.

Note

Tim AMS merekomendasikan kisaran /23.

- Detail Direktori Aktif: Microsoft Active Directory (AD) digunakan untuk user/resource manajemen, autentikasi/otorisasi, dan DNS, di semua akun landing zone multi-akun AMS Anda. AMS AD juga dikonfigurasi dengan kepercayaan satu arah ke Direktori Aktif Anda untuk otentikasi berbasis kepercayaan. Input berikut diperlukan untuk membuat AD:
 - Domain Fully Qualified Domain Name (FQDN): Nama domain yang sepenuhnya memenuhi syarat untuk direktori AWS Managed Microsoft AD. Domain tidak boleh menjadi domain yang ada atau domain anak dari domain yang ada di jaringan Anda.
 - Nama Domain NetBIOS: Jika Anda tidak menentukan nama NetBIOS, AMS default nama ke bagian pertama dari DNS direktori Anda. Misalnya, corp untuk direktori DNS corp.example.com.
- Trend Micro — endpoint protection security (EPS): Trend Micro endpoint protection (EPS) adalah komponen utama dalam AMS untuk keamanan sistem operasi. Sistem ini terdiri dari Deep Security

Manager (DSM), EC2 instance, EC2 instance relay, dan agen yang hadir dalam semua data plane dan instance pelanggan. EC2

Anda harus mengasumsikan akun Layanan Bersama, dan berlangganan AMI Trend Micro Deep Security (BYOL), atau Trend Micro Deep Security (Marketplace).
EPSTMarketplaceSubscriptionRole

Input default berikut diperlukan untuk membuat EPS (jika Anda ingin mengubah dari default):

- Jenis Instance Relay: Nilai Default - m5.large
- Jenis Instans DSM: Nilai Default - m5.xlarge
- Ukuran Instans DB: Nilai Default - 200 GB
- Jenis Instans RDS: Nilai Default - db.m5.large
- Benteng pelanggan: Anda diberikan benteng SSH atau RDP (atau keduanya) di Akun Layanan Bersama, untuk mengakses host lain di lingkungan AMS Anda. Untuk mengakses jaringan AMS sebagai pengguna (SSH/RDP), you must use "customer" Bastions as the entry point. The network path originates from the on-premise network, goes through DX/VPN gateway transit (TGW), dan kemudian dialihkan ke VPC Layanan Bersama. Setelah Anda dapat mengakses benteng, Anda dapat melompat ke host lain di lingkungan AMS, asalkan permintaan akses telah diberikan.
- Input berikut diperlukan untuk bastion SSH.
 - Kapasitas Instans yang Diinginkan Bastion SSH: Nilai Default - 2.
 - Instans Maksimum SSH Bastion: Nilai Default - 4.
 - Instans Minimum Bastion SSH: Nilai Default -2.
 - SSH Bastion Instance Type: Default Value - m5.large (dapat diubah untuk menghemat biaya; misalnya t3.medium).
 - SSH Bastion Ingress CIDRs: alamat IP berkisar dari mana pengguna di jaringan Anda mengakses SSH Bastions.
- Input berikut diperlukan untuk benteng Windows RDP.
 - Jenis Instans Bastion RDP: Nilai Default - t3.medium.
 - Sesi Minimum yang Diinginkan Benteng RDP: Nilai Default - 2.
 - Sesi Maksimum RDP: Nilai Default -10.
 - Jenis Konfigurasi Bastion RDP: Anda dapat memilih salah satu konfigurasi di bawah ini
 - SecureStandard = Seorang pengguna menerima satu benteng dan hanya satu pengguna yang dapat terhubung ke benteng.

- SecureHa = Seorang pengguna menerima dua benteng dalam dua AZ yang berbeda untuk terhubung dan hanya satu pengguna yang dapat terhubung ke benteng.
- SharedStandard = Seorang pengguna menerima satu benteng untuk terhubung dan dua pengguna dapat terhubung ke benteng yang sama sekaligus.
- SharedHa = Seorang pengguna menerima dua benteng dalam dua AZ yang berbeda untuk terhubung dan dua pengguna dapat terhubung ke benteng yang sama sekaligus.
- Customer RDP Ingress CIDRs: Rentang alamat IP dari mana pengguna di jaringan Anda akan mengakses RDP Bastions.

Pembaruan untuk layanan bersama: Zona Pendaratan Multi-Akun

AMS menerapkan rilis pesawat data ke akun terkelola setiap bulan, tanpa pemberitahuan sebelumnya.

AMS menggunakan OU inti untuk menyediakan layanan bersama seperti akses, jaringan, EPS, penyimpanan log, agregasi peringatan di Zona Pendaratan Multi-Akun Anda. AMS bertanggung jawab untuk mengatasi kerentanan, penambalan, dan penerapan layanan bersama ini. AMS secara teratur memperbarui sumber daya yang digunakan untuk menyediakan layanan bersama ini sehingga pengguna memiliki akses ke fitur terbaru, dan pembaruan keamanan. Pembaruan biasanya terjadi setiap bulan. Sumber daya yang merupakan bagian dari pembaruan ini adalah:

- Akun yang merupakan bagian dari inti OU.

Akun manajemen, akun layanan bersama, akun jaringan, akun keamanan, dan akun arsip log memiliki sumber daya untuk benteng RDP dan SSH, proxy, host manajemen, dan keamanan titik akhir (EPS), yang biasanya diperbarui setiap bulan. AMS menggunakan EC2 penerapan yang tidak dapat diubah sebagai bagian dari infrastruktur layanan bersama.

- AMS baru AMIs menggabungkan pembaruan terbaru.

Note

Operator AMS menggunakan tipe perubahan penekanan alarm internal (CT) saat menjalankan perubahan bidang data dan RFC untuk CT tersebut muncul di daftar RFC Anda. Ini karena, saat rilis pesawat data dikerahkan, berbagai infrastruktur dapat dimatikan, di-boot ulang, diambil offline, atau mungkin ada lonjakan CPU atau efek lain dari penyebaran yang memicu alarm yang, selama penyebaran pesawat data, bersifat asing. Setelah penyebaran

selesai, semua infrastruktur diverifikasi untuk berjalan dengan baik dan alarm diaktifkan kembali.

Akun Arsip Log

Akun Arsip Log berfungsi sebagai hub pusat untuk pengarsipan log di lingkungan landing zone multi-akun AMS Anda. Ada bucket S3 di akun yang berisi salinan file log AWS CloudTrail dan AWS Config dari masing-masing akun lingkungan landing zone multi-akun AMS. Anda dapat menggunakan akun ini untuk solusi Pencatatan Terpusat dengan AWS Firehose, atau Splunk, dan sebagainya. Akses AMS ke akun ini terbatas pada beberapa pengguna; terbatas pada auditor dan tim keamanan untuk kepatuhan dan investigasi forensik yang terkait dengan aktivitas akun.

Akun keamanan

Akun Keamanan adalah hub pusat untuk operasi terkait keamanan perumahan dan titik utama untuk menyalurkan pemberitahuan dan peringatan ke layanan pesawat kontrol AMS. Selain itu, akun Keamanan menampung akun manajemen Amazon Guard Duty dan agregator AWS Config.

Jenis akun aplikasi

Akun aplikasi adalah akun AWS dalam arsitektur landing zone terkelola AMS yang Anda gunakan untuk meng-host beban kerja Anda. AMS menawarkan tiga jenis akun Aplikasi:

- [Akun aplikasi yang dikelola AMS](#)
- [AMS Mempercepat akun](#)
- [Akun aplikasi yang Dikelola Pelanggan](#)

Akun aplikasi dikelompokkan OUs dalam AWS Organizations yang berbeda tergantung pada jenis akun Application:

- Akar OU:
 1. Aplikasi OU
 - OU Terkelola: Akun yang dikelola AMS
 - Pengembangan OU: Akun yang dikelola AMS dengan mode Pengembang diaktifkan

2. Mempercepat OU: AMS Mempercepat akun Aplikasi
3. OU yang dikelola pelanggan: Akun Aplikasi yang dikelola pelanggan

Akun aplikasi disediakan melalui RFC yang dikirimkan dari akun Manajemen:

- [Buat Akun Aplikasi Dengan VPC ct-1zdasmc2ewzrs](#)
- Buat Accelerate Account [ct-2p93tyd5angmi](#)
- [Buat Akun Aplikasi yang Dikelola Pelanggan ct-3pwbixz27n3tn](#)

Akun aplikasi yang dikelola AMS

Akun aplikasi yang dikelola sepenuhnya oleh AMS disebut sebagai akun aplikasi yang dikelola AMS, di mana beberapa atau semua tugas operasional, seperti manajemen permintaan layanan, manajemen insiden, manajemen keamanan, manajemen kontinuitas (cadangan), manajemen patch, pengoptimalan biaya, atau pemantauan dan manajemen peristiwa infrastruktur, dilakukan oleh AMS.

Jumlah tugas yang dilakukan oleh AMS bergantung pada mode Manajemen Perubahan yang Anda pilih. Akun yang dikelola AMS mendukung berbagai mode untuk manajemen perubahan:

- [Modus RFC](#)
- [Mode Perubahan Langsung di AMS](#)
- [AMS dan AWS Service Catalog](#)
- [Mode Pengembang AMS Lanjutan](#)
- [Mode Penyediaan Layanan Mandiri di AMS](#)

Untuk informasi selengkapnya tentang manajemen perubahan dan mode yang berbeda, lihat [Ubah mode manajemen](#).

Ada beberapa layanan AWS yang dapat Anda gunakan di akun yang dikelola AMS tanpa manajemen AMS. Daftar layanan AWS ini dan cara menambahkannya ke akun AMS Anda dijelaskan di bagian [Penyediaan layanan mandiri](#).

AMS Mempercepat akun

AMS Accelerate adalah rencana operasi AMS yang dapat mengoperasikan infrastruktur AWS yang mendukung beban kerja. Anda dapat memperoleh manfaat dari layanan operasional AMS

Accelerate seperti pemantauan dan peringatan, manajemen insiden, manajemen keamanan, dan manajemen cadangan, tanpa melalui migrasi baru, mengalami downtime, atau mengubah cara Anda menggunakan AWS. AMS Accelerate juga menawarkan add-on patch opsional untuk beban kerja EC2 berbasis yang memerlukan penambalan reguler.

Dengan AMS Accelerate, Anda memiliki kebebasan untuk menggunakan, mengonfigurasi, dan menerapkan semua layanan AWS secara native, atau dengan alat pilihan Anda. Anda akan menggunakan mekanisme akses dan perubahan pilihan Anda sementara AMS secara konsisten menerapkan praktik terbukti yang membantu meningkatkan skala tim Anda, mengoptimalkan biaya, meningkatkan keamanan dan efisiensi, dan meningkatkan ketahanan.

 Note

Akun AMS Accelerate di AMS Advanced tidak memiliki AMS change management (RFCs) atau konsol AMS Advanced. Sebaliknya, mereka memiliki konsol dan fungsionalitas AMS Accelerate.

Accelerate account hanya dapat disediakan dari akun Manajemen landing zone multi-akun AMS Anda. Accelerate menawarkan kemampuan operasional yang berbeda. Untuk mempelajari lebih lanjut, lihat [deskripsi layanan Accelerate](#).

- Anda akan terus menikmati beberapa fitur dari akun inti multi-account landing zone (MALZ) seperti logging terpusat, penagihan tunggal, Config Aggregator di akun keamanan dan SCPs
- AMS Accelerate tidak menyediakan beberapa layanan AMS Advanced seperti EPS, Manajemen akses, manajemen perubahan, dan penyediaan. Kami menyarankan Anda mengikuti langkah-langkah selanjutnya untuk mendapatkan akses dan mengkonfigurasi gateway transit (TGW).

Untuk detail selengkapnya tentang Accelerate, lihat [Apa itu Mempercepat](#).

Membuat akun Accelerate Anda

Untuk membuat akun Accelerate, ikuti langkah-langkah yang diuraikan di sini [Buat akun Accelerate](#).

Mengakses akun Accelerate Anda

Setelah Anda menyediakan akun Accelerate di akun multi-account landing zone (MALZ) Anda, peran dengan izin [akses Administratif](#) AccelerateDefaultAdminRole, ada di akun yang dapat Anda asumsikan.

Untuk mengakses akun Accelerate baru:

1. Masuk ke konsol IAM untuk akun manajemen dengan `CustomerDefaultAssumeRole` peran tersebut.
2. Di konsol IAM, pada bilah navigasi, pilih nama pengguna Anda.
3. Pilih Ganti Peran. Jika ini pertama kalinya Anda memilih opsi ini, akan muncul halaman dengan informasi lebih lanjut. Setelah itu, pilih Ganti Peran. Jika Anda menghapus cookie peramban Anda, halaman ini dapat muncul lagi.
4. Pada halaman Beralih Peran, ketik Accelerate account ID dan nama peran yang akan diambil: `AccelerateDefaultAdminRole`.

Sekarang setelah Anda memiliki akses, Anda dapat membuat Peran IAM baru untuk terus mengakses lingkungan Anda. Jika Anda ingin memanfaatkan SAFL Federation untuk akun Accelerate, lihat [Mengaktifkan pengguna federasi SALL 2.0 untuk mengakses AWS Management Console](#).

Menghubungkan akun Accelerate Anda dengan Transit Gateway

AMS tidak mengelola pengaturan jaringan akun Accelerate. Anda memiliki opsi untuk mengelola jaringan Anda sendiri menggunakan AWS APIs (lihat [Solusi Jaringan](#)) atau menghubungkan ke jaringan MALZ yang dikelola oleh AMS, menggunakan Transit Gateway (TGW) yang ada yang digunakan di AMS MALZ.

 Note

Anda hanya dapat memiliki VPC yang dilampirkan ke TGW jika akun Accelerate berada di Wilayah AWS yang sama. Untuk informasi lebih lanjut, lihat [Transit gateway](#).

Untuk menambahkan akun Accelerate ke Transit Gateway, minta rute baru menggunakan jenis perubahan [Deployment](#) | [Managed landing zone](#) | [Networking account](#) | [Add static route](#) (ct-3r2ckznmt0a59), sertakan informasi ini:

- **Blackhole:** Benar untuk menunjukkan bahwa target rute tidak tersedia. Lakukan ini ketika lalu lintas untuk rute statis akan dijatuhkan oleh Transit Gateway. Salah untuk merutekan lalu lintas ke ID lampiran TGW yang ditentukan. Nilai default adalah false.
- **DestinationCidrBlock:** Rentang IPV4 CIDR yang digunakan untuk pertandingan tujuan. Keputusan routing didasarkan pada kecocokan yang paling spesifik. Contoh: 10.0.2.0/24.

- `TransitGatewayAttachmentId`: ID Lampiran TGW yang akan berfungsi sebagai target tabel rute. Jika Blackhole salah, parameter ini diperlukan, jika tidak biarkan parameter ini kosong. Contoh: `tgw-attach-04eb40d1e14ec7272`.
- `TransitGatewayRouteTableId`: ID dari tabel rute TGW. Contoh: `tgw-rtb-06ddc751c0c0c881c`.

Buat rute di tabel rute TGW untuk terhubung ke VPC ini:

1. Secara default VPC ini tidak akan dapat berkomunikasi dengan yang lain VPCs di jaringan MALZ Anda.
2. Putuskan dengan arsitek solusi Anda apa yang VPCs Anda inginkan untuk berkomunikasi dengan VPC Accelerate ini.
3. Kirim [Deployment | Managed landing zone | Akun jaringan | Tambahkan rute statis](#) (ct-3r2ckznmt0a59) jenis perubahan, sertakan informasi ini:
 - `Blackhole`: Benar untuk menunjukkan bahwa target rute tidak tersedia. Lakukan ini ketika lalu lintas untuk rute statis akan dijatuhkan oleh Transit Gateway. Salah untuk merutekan lalu lintas ke ID lampiran TGW yang ditentukan. Nilai default adalah false.
 - `DestinationCidrBlock`: Rentang IPV4 CIDR yang digunakan untuk pertandingan tujuan. Keputusan routing didasarkan pada kecocokan yang paling spesifik. Contoh: `10.0.2.0/24`.
 - `TransitGatewayAttachmentId`: ID Lampiran TGW yang akan berfungsi sebagai target tabel rute. Jika Blackhole salah, parameter ini diperlukan, jika tidak biarkan parameter ini kosong. Contoh: `tgw-attach-04eb40d1e14ec7272`.
 - `TransitGatewayRouteTableId`: ID dari tabel rute TGW. Contoh: `tgw-rtb-06ddc751c0c0c881c`.

Menghubungkan VPC Accelerate account baru ke jaringan AMS Multi-Account Landing Zone (membuat lampiran VPC TGW):

1. Di akun jaringan landing zone multi-akun Anda, buka konsol [Amazon VPC](#).
2. Pada panel navigasi, pilih Transit Gateways. Catat ID TGW dari gateway transit yang Anda lihat.
3. Di akun Accelerate Anda, buka [konsol VPC Amazon](#).
4. Di panel navigasi, pilih Lampiran Transit Gateway > Buat Lampiran Gateway Transit. Buat pilihan ini:
 - Untuk ID Transit Gateway, pilih ID gateway transit yang Anda rekam di Langkah 2.
 - Untuk jenis Lampiran, pilih VPC.
 - Di bawah Lampiran VPC, secara opsional ketik nama untuk tag nama Lampiran.

- Pilih apakah akan mengaktifkan Dukungan dan IPv6 Dukungan DNS.
- Untuk ID VPC, pilih VPC yang dilampirkan pada transit gateway. VPC ini harus memiliki setidaknya satu subnet yang terkait dengannya.
- Untuk Subnet IDs, pilih satu subnet untuk setiap Availability Zone yang akan digunakan oleh gateway transit untuk merutekan lalu lintas. Anda harus memilih setidaknya satu subnet. Anda hanya dapat memilih satu subnet per Availability Zone.

5. Pilih Buat lampiran. Catat ID Lampiran TGW yang baru dibuat.

Mengaitkan lampiran TGW ke tabel rute:

1. Tentukan tabel rute TGW mana yang ingin Anda kaitkan dengan VPC. Sebaiknya buat tabel rute aplikasi baru untuk Accelerate account VPCs menggunakan Deployment | Managed landing zone | Akun jaringan | Buat tabel rute gateway transit (ct-3dscwaeyi6cup) mengubah jenis.
2. Kirim [Manajemen | Managed landing zone | Akun jaringan | Associate TGW attachment](#) (ct-3nmhh0qr338q6) RFC pada akun Networking untuk mengaitkan lampiran VPC atau TGW ke tabel rute yang Anda pilih.

Buat rute di tabel rute TGW untuk terhubung ke VPC ini:

1. Secara default, VPC ini tidak akan dapat berkomunikasi dengan yang lain VPCs di jaringan landing zone multi-akun Anda.
2. Putuskan dengan arsitek solusi Anda apa yang VPCs Anda inginkan untuk berkomunikasi dengan VPC akun Accelerate ini.
3. Kirim [Deployment | Managed landing zone | Akun jaringan | Tambahkan rute statis](#) (ct-3r2ckznmt0a59) RFC terhadap akun jaringan untuk membuat rute TGW yang Anda butuhkan.

Mengonfigurasi tabel Rute VPC Anda untuk menunjuk ke gateway transit landing zone multi-akun AMS:

1. Tentukan dengan arsitek solusi Anda lalu lintas apa yang ingin Anda kirim ke gateway transit Zona Pendaratan Multi-Akun AMS.
2. Kirim [Deployment | Managed landing zone | Akun jaringan | Tambahkan rute statis](#) (ct-3r2ckznmt0a59) RFC terhadap akun jaringan untuk membuat rute TGW yang Anda butuhkan.

Akun aplikasi yang Dikelola Pelanggan

Anda dapat membuat akun yang tidak dikelola AMS dengan cara standar. Akun tersebut disebut akun yang dikelola pelanggan dan mereka memberi Anda kontrol penuh untuk mengoperasikan sendiri infrastruktur di dalam akun sambil menikmati manfaat arsitektur terpusat yang dikelola oleh AMS.

Akun yang Dikelola Pelanggan tidak memiliki akses ke konsol AMS atau layanan apa pun yang kami sediakan (tambalan, cadangan, dan sebagainya).

Akun yang Dikelola Pelanggan hanya dapat disediakan dari akun manajemen landing zone multi-akun AMS Anda.

Mode AMS yang berbeda bekerja dengan akun Aplikasi secara berbeda; untuk mempelajari lebih lanjut tentang mode, lihat [mode AWS Managed Services](#).

Untuk membuat akun aplikasi yang Dikelola Pelanggan, lihat Akun [manajemen | Membuat Akun Aplikasi yang Dikelola Pelanggan](#).

Untuk menghapus akun aplikasi yang Dikelola Pelanggan, gunakan [akun Manajemen | Akun Aplikasi Offboard](#). (CT [Confirm Offboarding](#) tidak berlaku untuk akun aplikasi yang Dikelola Pelanggan.)

Mengakses akun yang Dikelola Pelanggan

Setelah Anda menyediakan akun Terkelola Pelanggan (CMA) di landing zone multi-akun, (MALZ) peran Admin, `CustomerDefaultAdminRole`, ada di akun yang dapat Anda asumsikan, melalui federasi SAFL, untuk mengonfigurasi akun.

Untuk mengakses CMA:

1. Masuk ke konsol IAM untuk akun manajemen dengan `CustomerDefaultAssumeRole` peran tersebut.
2. Di konsol IAM, pada bilah navigasi, pilih nama pengguna Anda.
3. Pilih Ganti Peran. Jika ini pertama kalinya Anda memilih opsi ini, akan muncul halaman dengan informasi lebih lanjut. Setelah itu, pilih Ganti Peran. Jika Anda menghapus cookie peramban Anda, halaman ini dapat muncul lagi.
4. Pada halaman Beralih Peran, ketik ID akun yang Dikelola Pelanggan dan nama peran yang akan diambil: `CustomerDefaultAdminRole`.

Sekarang setelah Anda memiliki akses, Anda dapat membuat Peran IAM baru untuk terus mengakses lingkungan Anda. Jika Anda ingin memanfaatkan Federasi SAM untuk Akun CMA Anda, lihat [Mengaktifkan pengguna federasi SALL 2.0 untuk mengakses](#) AWS Management Console.

Menghubungkan CMA Anda dengan Transit Gateway

AMS tidak mengelola pengaturan jaringan akun yang Dikelola Pelanggan (CMAs). Anda memiliki opsi untuk mengelola jaringan Anda sendiri menggunakan AWS APIs (lihat [Solusi Jaringan](#)) atau menghubungkan ke jaringan landing zone multi-akun yang dikelola oleh AMS, menggunakan Transit Gateway (TGW) yang ada yang digunakan di AMS MALZ.

Note

Anda hanya dapat memiliki VPC yang dilampirkan ke TGW jika CMA berada di Wilayah AWS yang sama. Untuk informasi lebih lanjut, lihat [Transit gateway](#).

Untuk menambahkan CMA Anda ke Transit Gateway, minta rute baru dengan [akun Jaringan | Tambahkan rute statis \(ct-3r2ckznmt0a59\)](#) jenis perubahan dan sertakan informasi ini:

- **Blackhole:** Benar untuk menunjukkan bahwa target rute tidak tersedia. Lakukan ini ketika lalu lintas untuk rute statis akan dijatuhkan oleh Transit Gateway. Salah untuk merutekan lalu lintas ke ID lampiran TGW yang ditentukan. Nilai default adalah false.
- **DestinationCidrBlock:** Rentang IPV4 CIDR yang digunakan untuk pertandingan tujuan. Keputusan routing didasarkan pada kecocokan yang paling spesifik. Contoh: 10.0.2.0/24.
- **TransitGatewayAttachmentId:** ID Lampiran TGW yang akan berfungsi sebagai target tabel rute. Jika Blackhole salah, parameter ini diperlukan, jika tidak biarkan parameter ini kosong. Contoh: tgw-attach-04eb40d1e14ec7272.
- **TransitGatewayRouteTableId:** ID dari tabel rute TGW. Contoh: tgw-rtb-06ddc751c0c0c881c.

Menghubungkan VPC baru yang dikelola pelanggan ke jaringan Zona Pendaratan Multi-Akun AMS (membuat lampiran VPC TGW):

1. Di akun jaringan landing zone multi-akun Anda, buka konsol [Amazon VPC](#).
2. Di panel navigasi, pilih Transit Gateways. Catat ID TGW dari gateway transit yang Anda lihat.
3. Di akun yang Dikelola Pelanggan, buka [konsol VPC Amazon](#).

4. Di panel navigasi, pilih Lampiran Transit Gateway > Buat Lampiran Gateway Transit. Buat pilihan ini:
 - a. Untuk ID Transit Gateway, pilih ID gateway transit yang Anda rekam di Langkah 2.
 - b. Untuk jenis Lampiran, pilih VPC.
 - c. Di bawah Lampiran VPC, secara opsional ketik nama untuk tag nama Lampiran.
 - d. Pilih apakah akan mengaktifkan DNS Support and IPv6 Support.
 - e. Untuk ID VPC, pilih VPC yang dilampirkan pada transit gateway. VPC ini harus memiliki setidaknya satu subnet yang terkait dengannya.
 - f. Untuk Subnet IDs, pilih satu subnet untuk setiap Availability Zone yang akan digunakan oleh gateway transit untuk merutekan lalu lintas. Anda harus memilih setidaknya satu subnet. Anda hanya dapat memilih satu subnet per Availability Zone.
5. Pilih Buat lampiran. Catat ID Lampiran TGW yang baru dibuat.

Mengaitkan lampiran TGW ke tabel rute:

Tentukan tabel rute TGW mana yang ingin Anda kaitkan dengan VPC. Sebaiknya buat tabel rute aplikasi baru untuk Pelanggan Dikelola VPCs dengan mengirimkan Deployment | Managed landing zone | Akun jaringan | Buat tabel rute gateway transit (ct-3dscwaeyi6cup) RFC. Untuk mengaitkan lampiran VPC atau TGW ke tabel rute yang Anda pilih, kirimkan Deployment | Managed landing zone | Akun jaringan | Associate TGW attachment (ct-3nmhh0qr338q6) RFC di akun Networking.

Buat rute di tabel rute TGW untuk terhubung ke VPC ini:

1. Secara default, VPC ini tidak akan dapat berkomunikasi dengan yang lain VPCs di jaringan Zona Pendaratan Multi-Akun Anda.
2. Putuskan dengan arsitek solusi Anda apa yang VPCs Anda inginkan untuk berkomunikasi dengan VPC yang dikelola pelanggan ini. Kirim Deployment | Managed landing zone | Akun jaringan | Tambahkan rute statis (ct-3r2ckznmt0a59) RFC terhadap akun jaringan untuk membuat rute TGW yang Anda butuhkan.

Note

CT (ct-3r2ckznmt0a59) ini tidak mengizinkan penambahan rute statis ke tabel rute inti EgressRouteDomain; jika CMA Anda perlu mengizinkan lalu lintas jalan keluar, kirimkan Manajemen | Lainnya | Lainnya (MOO) RFC dengan ct-0xdawir96cy7k.

Mengonfigurasi tabel Rute VPC Anda untuk menunjuk ke gateway transit Zona Pendaratan Multi-Akun AMS:

Tentukan dengan arsitek solusi Anda lalu lintas apa yang ingin Anda kirim ke gateway transit Zona Pendaratan Multi-Akun AMS. Perbarui tabel rute VPC Anda untuk mengirim lalu lintas ke lampiran TGW yang dibuat sebelumnya

Mendapatkan bantuan operasional dengan akun yang Dikelola Pelanggan

AMS dapat membantu Anda mengoperasikan beban kerja yang Anda gunakan di akun yang Dikelola Pelanggan dengan memasukkan akun ke AMS Accelerate. Dengan AMS Accelerate, Anda dapat memperoleh manfaat dari layanan operasional seperti pemantauan dan peringatan, manajemen insiden, manajemen keamanan, dan manajemen cadangan, tanpa melalui migrasi baru, mengalami downtime, atau mengubah cara Anda menggunakan. AWS AMS Accelerate juga menawarkan add-on patch opsional untuk beban kerja EC2 berbasis yang memerlukan penambalan reguler. Dengan AMS Accelerate, Anda terus menggunakan, mengonfigurasi, dan menerapkan semua AWS layanan secara native, atau dengan alat pilihan Anda; seperti yang Anda lakukan dengan akun AMS Advanced Customer Managed. Anda menggunakan mekanisme akses dan perubahan pilihan Anda sementara AMS menerapkan praktik terbukti yang membantu meningkatkan skala tim Anda, mengoptimalkan biaya, meningkatkan keamanan dan efisiensi, dan meningkatkan ketahanan. Untuk mempelajari lebih lanjut, lihat [deskripsi layanan Accelerate](#).

Untuk memasukkan akun Terkelola Pelanggan Anda ke Accelerate, hubungi CSDM Anda dan ikuti langkah-langkah dari [Memulai dengan](#) AMS Accelerate.

Note

Akun AMS Accelerate di AMS Advanced tidak memiliki manajemen perubahan AMS (permintaan untuk perubahan atau RFCs) atau konsol AMS Advanced. Sebaliknya, mereka memiliki konsol dan fungsionalitas AMS Accelerate.

Akun AMS Tools (memigrasikan beban kerja)

Akun alat Zona Pendaratan Multi-Akun Anda (dengan VPC) membantu mempercepat upaya migrasi, meningkatkan posisi keamanan Anda, mengurangi biaya dan kompleksitas, dan menstandarisasi pola penggunaan Anda.

Akun alat menyediakan yang berikut:

- Batas yang terdefinisi dengan baik untuk akses ke instance replikasi untuk integrator sistem di luar beban kerja produksi Anda.
- Memungkinkan Anda membuat ruang terisolasi untuk memeriksa beban kerja untuk malware, atau rute jaringan yang tidak dikenal, sebelum menempatkannya ke akun dengan beban kerja lainnya.
- Sebagai pengaturan akun yang ditentukan, ini menyediakan waktu yang lebih cepat untuk onboard dan menyiapkan untuk memigrasi beban kerja.
- Rute jaringan terisolasi untuk mengamankan lalu lintas dari on-premise -> -> Tools account CloudEndure -> AMS menelan gambar. Setelah gambar tertelan, Anda dapat membagikan gambar ke akun tujuan melalui Manajemen AMS | Komponen tumpukan lanjutan | AMI | Bagikan (ct-1eiczxw8ihc18) RFC.

Diagram arsitektur tingkat tinggi:

Gunakan Deployment | Managed landing zone | Akun manajemen | Buat akun alat (dengan VPC) jenis perubahan (ct-2j7q1hgf26x5c), untuk dengan cepat menyebarkan akun alat dan membuat instance proses Penyerapan Beban Kerja dalam lingkungan Zona Pendaratan Multi-Akun. Lihat [Akun manajemen, Akun alat: Membuat \(dengan VPC\)](#).

Note

Kami merekomendasikan memiliki dua zona ketersediaan (AZs), karena ini adalah hub migrasi.

Secara default, AMS membuat dua grup keamanan berikut (SGs) di setiap akun.

Konfirmasikan bahwa SGs keduanya hadir. Jika mereka tidak hadir, silakan buka permintaan layanan baru dengan tim AMS untuk memintanya.

- SentinelDefaultSecurityGroupPrivateOnlyEgressAll
- InitialGarden-SentinelDefaultSecurityGroupPrivateOnly

Pastikan bahwa instance CloudEndure replikasi dibuat di subnet pribadi di mana ada rute kembali ke on-premise. Anda dapat mengonfirmasi bahwa dengan memastikan bahwa tabel rute untuk subnet pribadi memiliki rute default kembali ke TGW. Namun, melakukan pemotongan CloudEndure mesin harus masuk ke subnet pribadi “terisolasi” di mana tidak ada rute kembali ke on-premise, hanya lalu lintas keluar Internet yang diizinkan. Sangat penting untuk memastikan cutover terjadi di subnet yang terisolasi untuk menghindari potensi masalah pada sumber daya di lokasi.

Prasyarat:

1. Baik tingkat dukungan Plus atau Premium.
2. Akun aplikasi IDs untuk kunci KMS tempat AMIs dikerahkan.
3. Akun alat, dibuat seperti yang dijelaskan sebelumnya.

AWS Layanan Migrasi Aplikasi (AWS MGN)

[AWS Layanan Migrasi Aplikasi](#) (AWS MGN) dapat digunakan di akun MALZ Tools Anda melalui peran `AWSManagedServicesMigrationRole` IAM yang dibuat secara otomatis selama penyediaan akun Tools. [Anda dapat menggunakan AWS MGN untuk memigrasikan aplikasi dan database yang berjalan pada versi sistem operasi Windows dan Linux yang didukung.](#)

Untuk up-to-date informasi paling banyak tentang Wilayah AWS dukungan, lihat [Daftar Layanan AWS Regional](#).

Jika pilihan Anda saat Wilayah AWS ini tidak didukung oleh AWS MGN, atau sistem operasi tempat aplikasi Anda berjalan saat ini tidak didukung oleh AWS MGN, pertimbangkan untuk menggunakan akun [CloudEndure Migrasi](#) di Alat Anda.

Meminta Inisialisasi AWS MGN

AWS MGN harus [diinisialisasi](#) oleh AMS sebelum digunakan pertama kali. Untuk meminta ini untuk akun Tools baru, kirimkan Manajemen | Lainnya | RFC lain dari akun Tools dengan rincian berikut:

```
RFC Subject=Please initialize AWS MGN in this account
RFC Comment=Please click 'Get started' on the MGN welcome page here:
```

https://console.aws.amazon.com/mgn/home?region=MALZ_PRIMARY_REGION#/welcome using all default values to 'Create template' and complete the initialization process.

Setelah AMS berhasil menyelesaikan RFC dan menginisialisasi AWS MGN di akun Tools Anda, Anda dapat menggunakannya `AWSTemplateIngestionRole` untuk mengedit template default untuk kebutuhan Anda.

Aktifkan akses ke akun AMS Tools baru

Setelah akun alat dibuat, AMS memberi Anda ID akun. Langkah Anda selanjutnya adalah mengonfigurasi akses ke akun baru. Ikuti langkah-langkah ini.

1. Perbarui grup Direktori Aktif yang sesuai ke akun yang sesuai IDs.

Akun baru yang dibuat AMS disediakan dengan kebijakan `ReadOnly` peran serta peran untuk memungkinkan pengguna mengajukan RFCs

Akun Tools juga memiliki peran IAM tambahan dan pengguna yang tersedia:

- IAM role: `AWSTemplateIngestionRole`
- Pengguna IAM: `customer_cloud_endure_user`

2. Minta kebijakan dan peran untuk memungkinkan anggota tim integrasi layanan menyiapkan alat tingkat berikutnya.

Arahkan ke konsol AMS dan ajukan yang berikut ini RFCs:

a. Buat kunci KMS. Gunakan [Create KMS Key \(auto\)](#) atau [Create KMS Key \(review required\)](#).

Saat Anda menggunakan KMS untuk mengenkripsi sumber daya yang tertelan, menggunakan satu kunci KMS yang dibagikan dengan akun aplikasi Zona Pendaratan Multi-Akun lainnya, memberikan keamanan untuk gambar yang dicerna di mana mereka dapat didekripsi di akun tujuan.

b. Bagikan kunci KMS.

Gunakan Manajemen | Komponen tumpukan lanjutan | Kunci KMS | Bagikan (perlu ditinjau) jenis perubahan (`ct-05yb337abq3x5`) untuk meminta agar kunci KMS baru dibagikan dengan akun aplikasi Anda di mana tertelan akan berada. AMIs

Contoh grafik pengaturan akun akhir:

Contoh kebijakan IAM yang telah disetujui AMS CloudEndure

Untuk melihat CloudEndure kebijakan IAM AMS yang telah disetujui sebelumnya:

Buka paket file [Contoh Zona Pendaratan Cloud Endure WIGS](#) dan buka file.

customer_cloud_endure_policy.json

Menguji konektivitas dan end-to-end penyiapan akun AMS Tools

1. Mulailah dengan mengkonfigurasi CloudEndure dan menginstal CloudEndure agen di server yang akan mereplikasi ke AMS.
2. Buat proyek di CloudEndure.
3. Masukkan AWS kredensi yang dibagikan saat Anda melakukan prasyarat, meskipun manajer rahasia.
4. Dalam pengaturan Replikasi:
 - a. Pilih kedua grup keamanan AMS “Sentinel” (Hanya Pribadi dan EgressAll) untuk Pilih Grup Keamanan untuk diterapkan ke opsi Server Replikasi.
 - b. Tentukan opsi cutover untuk mesin (instance). Untuk informasi lebih lanjut, lihat [Langkah 5. Potong](#)
 - c. Subnet: Subnet pribadi.
5. Grup Keamanan:
 - a. Pilih kedua grup keamanan AMS “Sentinel” (Hanya Pribadi dan EgressAll).
 - b. Instans cutover harus berkomunikasi ke Active Directory (MAD) yang dikelola AMS dan ke titik akhir publik: AWS
 - i. IP elastis: Tidak ada
 - ii. IP Publik: tidak
 - iii. Peran IAM: customer-mc-ec 2-instance-profile
 - c. Tetapkan tag sesuai konvensi penandaan internal Anda.
6. Instal CloudEndure agen di mesin dan cari contoh replikasi yang muncul di akun AMS Anda di EC2 konsol.

Proses konsumsi AMS:

Kebersihan akun AMS Tools

Anda akan ingin membersihkan setelah Anda selesai di akun telah membagikan AMI dan tidak lagi membutuhkan instance yang direplikasi:

- Posting WIGs konsumsi contoh:
 - Instans cutover: Minimal, hentikan atau hentikan instance ini, setelah pekerjaan selesai, melalui konsol AWS
 - Pencadangan AMI Pra-Penyerapan: Hapus setelah instance tertelan dan instance di lokasi dihentikan
 - Instans yang dicerna AMS: Matikan tumpukan atau hentikan setelah AMI dibagikan
 - AMS-ingested AMIs: Hapus setelah berbagi dengan akun tujuan selesai
- Pembersihan akhir migrasi: Dokumentasikan sumber daya yang digunakan melalui mode Pengembang untuk memastikan pembersihan terjadi secara teratur, misalnya:
 - Grup keamanan
 - Sumber daya yang dibuat melalui Formasi Cloud
 - Jaringan ACK
 - Subnet
 - VPC
 - Tabel Rute
 - Peran
 - Pengguna dan akun

Migrasi dalam skala - Pabrik Migrasi

Lihat [Memperkenalkan Solusi Pabrik CloudEndure Migrasi AWS](#).

Arsitektur jaringan SALZ

Diagram berikut menggambarkan tata letak jaringan VPC AWS Managed Services (AMS) single-account landing zone (SALZ) AWS Managed Services (AMS) dan merupakan contoh penyiapan yang sangat tersedia.

AMS mengonfigurasi semua aspek jaringan untuk Anda berdasarkan templat standar kami dan opsi pilihan Anda yang disediakan selama orientasi. Desain jaringan AWS standar diterapkan ke akun AWS Anda, dan virtual private cloud (VPC) dibuat untuk Anda dan terhubung ke AMS oleh VPN atau Direct Connect. Pelajari selengkapnya tentang Direct Connect di [AWS Direct Connect](#). Standar VPCs termasuk DMZ, layanan bersama, dan subnet aplikasi. Selama proses orientasi, tambahan VPCs mungkin diminta dan dibuat agar sesuai dengan kebutuhan Anda (misalnya, divisi pelanggan, mitra). Setelah onboarding, Anda diberikan diagram jaringan. dokumen lingkungan yang menjelaskan bagaimana jaringan Anda telah diatur.

Note

Untuk mempelajari batasan dan batasan layanan default untuk semua layanan aktif, lihat dokumentasi [AWS Service Limits](#).

Desain jaringan kami dibangun di sekitar [“Prinsip Hak Istimewa Paling Sedikit”](#) Amazon. Untuk mencapai hal ini, kami merutekan semua lalu lintas, masuk dan keluar, melalui gateway, kecuali lalu lintas yang berasal dari jaringan tepercaya. Satu-satunya jaringan tepercaya adalah jaringan yang dikonfigurasi antara lingkungan lokal Anda dan VPC melalui penggunaan and/or VPN dan AWS Direct Connect (DX). Akses diberikan melalui penggunaan instans benteng, sehingga mencegah akses langsung ke sumber daya produksi apa pun. Semua aplikasi dan sumber daya Anda berada di dalam subnet pribadi yang dapat dijangkau melalui penyeimbang beban publik. Lalu lintas jalan keluar publik mengalir melalui proxy penerusan kami ke Internet Gateway dan kemudian ke Internet. Atau, lalu lintas dapat mengalir melalui VPN atau Direct Connect ke lingkungan lokal Anda.

Layanan bersama landing zone akun tunggal AMS

Subnet layanan bersama berisi Layanan Direktori AMS, Host Manajemen yang mengotomatiskan penyediaan dan tugas umum, server manajemen antivirus (TrendMicro), dan host benteng internal:

- Layanan Direktori AMS = Pengontrol Domain AD

Membuat Direktori Aktif di akun AMS, membuat domain AMS, menggabungkan tumpukan terkelola ke domain saat diluncurkan.

- Host manajemen = Host Manajemen AMS (mengotomatiskan penyediaan dan tugas umum)

Bertindak sebagai endpoint API untuk memodifikasi AWS Directory Service, berinteraksi dengan pengontrol AWS Directory Service domain.

- Layanan keamanan: Server manajemen Antivirus (TrendMicro) = EPS DSM+EPS Relay

Memanfaatkan perangkat lunak Trend Micro™ Deep Security (DSM), beroperasi dalam model client-server dan memiliki database back-end, termasuk manajer Deep Security, agen, dan relay.

- Host benteng internal = Benteng pelanggan

Server tujuan khusus yang dirancang untuk menjadi titik akses utama dari Internet dan bertindak sebagai proxy ke EC2 instans Amazon Anda yang lain.

Menyiapkan AMS

Topik

- [Memahami setelan default AMS](#)
- [Menggunakan konsol AMS](#)
- [Menggunakan AMS API dan CLI](#)
- [AMS membawa EPS Anda sendiri](#)
- [Menerima pemberitahuan AMS](#)
- [Menyiapkan DNS pribadi dan publik](#)
- [Manajemen lalu lintas jalan keluar AMS](#)
- [Menerapkan sumber daya IAM di AMS Advanced](#)
- [Menyetel izin di AMS dengan peran dan profil IAM](#)
- [Aturan klaim AD FS dan setelan SAMP](#)
- [Batasi dengan ACL jaringan](#)
- [AMS di Outposts](#)
- [Menggunakan tag di AMS](#)
- [AWS Managed Services Resource Scheduler](#)
- [AWS Systems Manager di AMS Lanjutan](#)
- [Akun AMS offboard](#)

Beberapa tugas penyiapan AMS mungkin diselesaikan saat orientasi.

Untuk deskripsi lengkap tentang peran dan tanggung jawab, termasuk AMS [AWS Layanan yang didukung](#), lihat [Matriks tanggung jawab AMS \(RACI\)](#).

Note

Untuk meminta agar AMS menyediakan AWS layanan tambahan, ajukan permintaan layanan. Untuk informasi tentang cara membuat permintaan ini, lihat [Manajemen permintaan layanan](#).

Memahami setelan default AMS

Jaringan AWS Managed Services (AMS) Anda memiliki konfigurasi standar dengan default untuk sebagian besar layanan.

Bagian ini menjelaskan pengaturan default yang digunakan AMS untuk akses, pemantauan, dan pencatatan, manajemen.

Untuk contoh biaya infrastruktur landing zone multi-akun atau single-account landing zone, lihat.

[Komponen dasar lingkungan AMS](#)

Topik

- [Default resolusi DNS \(MALZ\)](#)
- [EC2 Profil instans IAM](#)
- [Peringatan dari pemantauan dasar di AMS](#)
- [Retensi log dan default rotasi](#)

Default resolusi DNS (MALZ)

AWS Managed Services (AMS) multi-account landing zone: Di lingkungan AWS, resolusi sistem nama domain (DNS) antara Route 53 Resolver dan DNS resolver dalam VPC dapat diintegrasikan dengan mengonfigurasi aturan penerusan Resolver. Sebelum aturan ini dapat digunakan untuk meneruskan kueri DNS, titik akhir resolver masuk dan keluar perlu diatur ke mana kueri ini dapat diteruskan.

Secara default, kueri DNS dalam akun VPCs aplikasi dalam pengaturan multi-akun di AMS diteruskan ke penerusan bersyarat domain AWS Directory Service untuk Microsoft Active Directory (juga dikenal sebagai Managed AD) yang ada di akun layanan bersama. AMS secara opsional memungkinkan Anda menggunakan AmazonProvided DNS; misalnya, DNS untuk meneruskan AmazonProvided kueri DNS ke. Ini membantu Anda memanfaatkan titik akhir VPC yang saat ini hanya mendukung DNS yang disediakan Amazon melalui Amazon Route 53. Sejalan dengan itu, Aturan Resolver juga secara otomatis diatur untuk titik akhir VPC umum yang digunakan secara default di akun layanan bersama. Untuk informasi lebih lanjut tentang titik akhir VPC umum ini, lihat.

[Titik akhir AMS VPC](#)

Untuk mengonfigurasi Set Opsi Dynamic Host Configuration Protocol (DHCP) di semua akun aplikasi Anda VPCs untuk menggunakan DNS yang disediakan Amazon untuk titik akhir VPC, dan memiliki aturan Resolver Route53 yang menunjuk ke titik akhir VPC umum di akun layanan bersama Anda

(dengan Aturan Resolver opsional untuk domain lokal), buat Manajemen | Lainnya | Lainnya | Buat permintaan perubahan (RFC) yang menentukan akun layanan bersama, dan meminta pemberdayaan akun aplikasi VPC lokal DNS dan aturan Route 53 Resolver untuk titik akhir VPC.

EC2 Profil instans IAM

Profil instance adalah wadah untuk peran IAM yang dapat Anda gunakan untuk meneruskan informasi peran ke EC2 instance saat instance dimulai.

MALZ

Ada dua profil instance default AMS, `customer-mc-ec2-instance-profile` dan `customer-mc-ec2-instance-profile-s3`. Profil instance ini memberikan izin yang dijelaskan dalam tabel berikut.

Deskripsi kebijakan

Profil	Kebijakan
customer-mc-ec2-instance-profile	AmazonSSMManagedInstanceCore : Memungkinkan instans Ec2 untuk menggunakan agen SSM.
	AMSInstanceProfileLoggingPolicy : Memungkinkan instance Ec2 untuk mendorong log ke S3 dan. CloudWatch
	AMSInstanceProfileManagementPolicy : Mengizinkan instance Ec2 melakukan tindakan booting, seperti bergabung dengan Active Directory.
	AMSInstanceProfileMonitoringPolicy : Memungkinkan instans Ec2 melaporkan temuan ke layanan pemantauan AMS.
customer-mc-ec2-instance-profile-s3	AMSInstanceProfilePatchPolicy : Memungkinkan instans Ec2 menerima tambalan.
	AMSInstanceProfileBYOEPSPolicy : Memungkinkan instans Ec2 untuk menggunakan AMS membawa EPS Anda sendiri .

Profil	Kebijakan
	AMSInstanceProfileLoggingPolicy : Memungkinkan instance Ec2 untuk mendorong log ke S3 dan. CloudWatch
	AMSInstanceProfileManagementPolicy : Mengizinkan instance Ec2 melakukan tindakan booting, seperti bergabung dengan Active Directory.
	AMSInstanceProfileMonitoringPolicy : Memungkinkan instans Ec2 melaporkan temuan ke layanan pemantauan AMS.
	AMSInstanceProfilePatchPolicy : Memungkinkan instans Ec2 menerima tambalan.
	AMSInstanceProfileS3WritePolicy : Mengizinkan instans Ec2 read/write ke bucket S3 pelanggan.

SALZ

Ada satu profil instans default AMS, `customer-mc-ec2-instance-profile`, yang memberikan izin dari kebijakan instans IAM. `customer_ec2_instance_profile_policy` Profil instance ini memberikan izin yang dijelaskan dalam tabel berikut. Profil memberikan izin ke aplikasi yang berjalan pada instance, bukan kepada pengguna yang masuk ke instance.

Kebijakan sering menyertakan beberapa pernyataan, di mana setiap pernyataan memberikan izin ke kumpulan sumber daya yang berbeda atau memberikan izin dalam kondisi tertentu.

CW = CloudWatch. ARN = Nama Sumber Daya Amazon. * = wildcard (apa saja).

EC2 izin profil instans IAM default

CW = CloudWatch. ARN = Nama Sumber Daya Amazon. * = wildcard (apa saja).

Pernyataan kebijakan	Efek	Tindakan	Deskripsi dan sumber daya (ARN)
Amazon Elastic Compute Cloud (Amazon EC2)			
EC2 Tindakan Pesan	Izinkan	AcknowledgeMessage, DeleteMessage, FailMessage, GetEndpoint, GetMessages, SendReply	Mengizinkan tindakan perpesanan EC2 Systems Manager di akun Anda.
Ec2 Jelaskan	Izinkan	* (Semua)	Memungkinkan konsol menampilkan detail konfigurasi EC2 di akun Anda.
Saya Dapatkan ID Peran	Izinkan	GetRole	Memungkinkan EC2 untuk mendapatkan ID IAM Anda dari <code>aws:iam::*:role/customer-*</code> dan <code>aws:iam::*:role/customer_*</code> .
Instance Untuk Mengunggah Peristiwa Log	Izinkan	Buat Grup Log	Mengizinkan log dibuat di: <code>aws:logs::*:log-group:i-*</code>
		Buat Aliran Log	Memungkinkan log dialirkan ke: <code>aws:logs::*:log-group:i-*</code>
CW Untuk MMS	Izinkan	DescribeAlarms,	Memungkinkan CloudWatch untuk mengambil alarm di akun Anda.

CW = CloudWatch. ARN = Nama Sumber Daya Amazon. * = wildcard (apa saja).

Pernyataan kebijakan	Efek	Tindakan	Deskripsi dan sumber daya (ARN)
		PutMetricAlarm, PutMetricData	Memungkinkan CW membuat atau memperbarui alarm dan mengaitkannya dengan metrik yang ditentukan. Memungkinkan CW mempublikasikan titik data metrik ke akun Anda.
Tag Ec2	Izinkan	CreateTags, DescribeTags,	Memungkinkan tag ditambahkan, ditimpa, dan dijelaskan pada instance yang ditentukan di akun Anda.
Secara Eksplisit Menolak Log CW	Menyangkal	DescribeLogStreams, FilterLogEvents, GetLogEvents	Tidak mengizinkan daftar, memfilter, atau mendapatkan aliran log untuk: <code>aws:logs:*:*:log-group:/mc/*</code>
Amazon EC2 Simple Systems Manager (SSM)			
Tindakan SSM	Izinkan	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	Memungkinkan berbagai fungsi SSM di akun Anda.

CW = CloudWatch. ARN = Nama Sumber Daya Amazon. * = wildcard (apa saja).

Pernyataan kebijakan	Efek	Tindakan	Deskripsi dan sumber daya (ARN)
Akses SSM Di S3	Izinkan	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadParts, ListBucketMultipartUploads	Memungkinkan SSM EC2 untuk mendapatkan dan memperbarui objek, dan membatalkan unggahan objek multi-bagian ke, dan daftar port dan ember yang tersedia untuk, unggahan multi-bagian di. <code>aws:s3:::mc-internal-*/aws/ssm*</code>

Amazon EC2 Simple Storage Service (S3)

Dapatkan Objek Di S3	Izinkan	Dapatkan Daftar	Memungkinkan EC2 aplikasi untuk mengambil dan mencantumkan objek dalam bucket S3 di akun Anda.
Akses Log S3 Terenkripsi Pelanggan	Izinkan	PutObject	Memungkinkan EC2 aplikasi untuk memperbarui objek di <code>aws:s3:::mc-logs-*/encrypted/app/*</code>
Patch Data Letakkan Objek S3	Izinkan	PutObject	Memungkinkan EC2 aplikasi untuk mengunggah data patching ke bucket S3 Anda di <code>aws:s3:::awsms-a*-patch-data-*</code>
Mengunggah Log Sendiri Ke S3	Izinkan	PutObject	Memungkinkan EC2 aplikasi untuk mengunggah log kustom ke: <code>aws:s3:::mc-a*-logs-*/aws/instances/*/\${aws:userid}/*</code>

CW = CloudWatch. ARN = Nama Sumber Daya Amazon. * = wildcard (apa saja).

Pernyataan kebijakan	Efek	Tindakan	Deskripsi dan sumber daya (ARN)
Secara Eksplisit Menolak Log MC Namespace S3	Menyangkal	GetObject* Meletakkan*	Melarangkan EC2 aplikasi mendapatkan atau meletakkan objek apa pun dari atau ke: aws:s3:::mc-*logs-*/encrypted/mc* , aws:s3:::mc-*logs-*/mc/*, aws:s3:::mc-a*-logs-*audit/*
Secara Eksplisit Tolak Hapus S3	Menyangkal	* (semua)	Melarangkan EC2 aplikasi mengambil tindakan apa pun pada objek di: aws:s3:::mc-a*-logs-*/* , aws:s3:::mc-a*-internal-*/* ,
Secara Eksplisit Menolak Bucket CFN S3	Menyangkal	Hapus*	Melarangkan EC2 aplikasi menghapus objek apa pun dari: aws:s3:::cf-templates-*
Secara Eksplisit Menolak Daftar Bucket S3	Menyangkal	ListBucket	Melarang Anda mencantumkan objek terenkripsi, log audit, atau cadangan (mc) dari: aws:s3:::mc-*logs-*

AWS Secrets Manager di Amazon EC2

CW = CloudWatch. ARN = Nama Sumber Daya Amazon. * = wildcard (apa saja).

Pernyataan kebijakan	Efek	Tindakan	Deskripsi dan sumber daya (ARN)
Akses Rahasia Trend Cloud One	Izinkan	GetSecretValue	Memungkinkan Amazon EC2 mengakses rahasia untuk migrasi Trend Cloud One: <pre>aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- id* , arn:aws:secretsman ager:~::~secret:/ams/ eps/cloud-one-agent- activation-token* , aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- id* , aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- guid*</pre>

AWS Key Management Service di Amazon EC2

Kunci Dekripsi Trend Cloud One	Izinkan	Dekripsi	Izinkan Amazon EC2 mendekripsi AWS KMS kunci dengan nama alias/-migrasi ams/eps/cloudone <pre>arn:aws:kms:~::~alias/ ams/eps/cloudone-migrat ion</pre>

Jika Anda tidak terbiasa dengan kebijakan Amazon IAM, lihat [Ikhtisar Kebijakan IAM untuk informasi penting](#).

 Note

Kebijakan sering menyertakan beberapa pernyataan, di mana setiap pernyataan memberikan izin ke kumpulan sumber daya yang berbeda atau memberikan izin dalam kondisi tertentu.

Peringatan dari pemantauan dasar di AMS

Pelajari tentang default pemantauan AMS. Untuk informasi selengkapnya, lihat [Pemantauan dan manajemen acara di AMS](#).

Tabel berikut menunjukkan apa yang dipantau, dan ambang batas peringatan default. Anda dapat mengubah ambang peringatan dengan Manajemen | Lainnya | Lainnya | Perbarui (ct-0xdawir96cy7k) RFC setelah menentukan perubahan apa yang Anda inginkan dan berlangganan topik Amazon SNS yang relevan. CloudWatch Untuk informasi tentang membuat dan berlangganan topik, lihat [Berlangganan Topik](#). Untuk informasi umum, lihat [Amazon SNS FAQs](#). Untuk diberi tahu secara langsung saat alarm melewati ambang batas, selain proses peringatan standar AMS, ikuti petunjuk berikut tentang cara menimpa konfigurasi alarm, [Menerima peringatan yang dihasilkan oleh AMS](#)

Amazon CloudWatch menyediakan retensi metrik yang diperpanjang. Untuk informasi selengkapnya, lihat [CloudWatch Batasan-batasan](#).

 Note

AMS mengkalibrasi pemantauan baseline secara periodik. Akun baru selalu disertakan dengan pemantauan dasar terbaru dan tabel menjelaskan pemantauan dasar untuk akun yang baru di-onboard. AMS memperbarui pemantauan dasar di akun yang ada secara berkala dan Anda mungkin mengalami jeda waktu sebelum pembaruan dilakukan. Untuk informasi selengkapnya, lihat [Melihat konfigurasi pemantauan untuk akun AMS](#).

Note

Peringatan EC2 Non-root volume usage instance DINONAKTIFKAN secara default. Jika Anda memerlukan pembuatan peringatan berdasarkan alarm ini, maka Anda harus mengaktifkannya menggunakan RFC Change Type ct-0erkoad6uyvg

Peringatan dari pemantauan dasar

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan

Untuk peringatan berbintang (*), AMS secara proaktif menilai dampak dan memulihkan bila memungkinkan; jika remediasi tidak memungkinkan, AMS menciptakan insiden. Jika otomatisasi gagal memperbaiki masalah, AMS memberi tahu Anda tentang kasus insiden dan seorang insinyur AMS terlibat. Selain itu, peringatan ini dapat dikirim langsung ke email Anda (jika Anda telah memilih topik Direct-Customer-Alerts SNS).

Contoh Application Load Balancer (ALB)	Tidak	RejectedConnectionCount jumlah > 0 selama 1 menit, 5 kali berturut-turut.	CloudWatch alarm jika jumlah koneksi yang ditolak karena load balancer mencapai maksimum.
Target Application Load Balancer (ALB)	Tidak	TargetConnectionErrorCount jumlah > 0 selama 1 menit, 5 kali berturut-turut.	CloudWatch alarm jika jumlah koneksi tidak berhasil dibuat antara penyeimbang beban dan instans terdaftar.
EC2 Contoh Amazon - Windows	Tidak	SecureChannelFailure > 0,0 untuk 10 dari 15 titik data terakhir.	CloudWatch alarm pada instance Windows untuk mengingatkan ketika koneksi Secure a Channel gagal.
Contoh Aurora	Tidak	CPUUtilization	CloudWatch alarm.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
		> 85% selama 5 menit, 2 kali berturut-turut.	
AWS Backup	Ya	DeleteRecoveryPoint Prinsipal peran IAM yang tidak terduga atau prinsipal pengguna IAM telah menghapus titik AWS Backup pemulihan.	CloudWatch acara. Dipancarkan saat titik pemulihan cadangan dihapus.
AWS Outposts	Ya	AMSOupostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 80% selama 5 menit, 12 kali berturut-turut.	CloudWatch alarm pada ketersediaan kapasitas keluarga misalnya AWS Outposts sumber daya.
		AMSOupostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80% selama 5 menit, 12 kali berturut-turut.	CloudWatch alarm pada ketersediaan kapasitas tipe instans AWS Outposts sumber daya.
		AMSOupostsConnectedStatus ConnectedStatus < 1 selama 5 menit, 1 kali berturut-turut.	CloudWatch alarm pada koneksi tautan AWS Outposts layanan, kurang dari 1 hitungan terganggu.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
EC2 contoh - semua OSs	Tidak	AMSOutpostsCapacityExceptionCapacityExceptions 0 selama 5 menit, 1 kali berturut-turut.	CloudWatch alarm pada kesalahan kapasitas yang tidak mencukupi misalnya peluncuran untuk sumber daya AWS Outposts s .
		CPUUtilization* >= 95% selama 5 menit, 6 kali berturut-turut.	CloudWatch alarm. Pemanfaatan CPU yang tinggi adalah indikator perubahan status aplikasi seperti kunci mati, loop tak terbatas, serangan berbahaya, dan anomali lainnya.
		StatusCheckFailed > 0 selama 5 menit, 3 kali berturut-turut. Penggunaan Volume Root >= 95% selama 5 menit, 6 kali berturut-turut.	CloudWatch alarm.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
EC2 Contoh Amazon - Linux		Penggunaan Volume Non-root > 85% selama 5 menit, 2 kali berturut-turut. Dinonaktifkan secara default; untuk informasi tambahan, lihat https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info.	
		Bebas Memori* MemoryFree < 5% selama 5 menit, 6 kali berturut-turut.	
	Ya	Malware EPS Malware ditemukan pada contoh.	CloudWatch acara.
	Tidak	Penggunaan Inode Volume Root Rata-rata >= 95% selama 5 menit, 6 kali berturut-turut. Bebas Swap * Memory Swap < 5% selama 5 menit, 6 kali berturut-turut.	CloudWatch alarm. Diterapkan untuk instance Linux saja.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
ElastiCache Cluster	Tidak	CurrConnections = 65000	Alarm ini memberi tahu AMS tentang batas koneksi maksimum ElastiCache Host. CloudWatch Alarm. Jika Anda ingin memperbarui ambang batas ini, hubungi dukungan AMS.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
ElastiCache Node	Tidak	CPUUtilization Rata-rata > nilai yang telah ditentukan selama 15 menit, 2 kali berturut-turut.	CloudWatch alarm. Defaultnya adalah 90. Jika Redis, gunakan salah satu nilai berikut berdasarkan jenis instance: • cache.t1.micro: 90% • cache.m1.small: 90% • cache.m1.medium: 90% • cache.m1.large: 45% • cache.m1.xlarge: 22,5% • cache.m2.xlarge: 45% • cache.m2.4xlarge: 11,25% • cache.c1.xlarge: 11,25% • cache.t2.micro: 90% • cache.t2.small: 90% • cache.t2.medium: 45% • cache.m3.medium: 90% • cache.m3.large: 45% • cache.m3.xlarge: 22,5% • cache.m3.2xlarge: 11,25% • cache.r3.large: 45% • cache.r3.xlarge: 22,5% • cache.r3.2xlarge: 11,25% • cache.r3.4xlarge: 5.625% • cache.r3.8xlarge: 2.8125%

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
Elasticache Node - memcache	Tidak	SwapUsage maksimum > 50.000.000 byte selama 5 menit, 5 kali berturut-turut.	CloudWatch alarm. Diterapkan hanya untuk memcached.
OpenSearch kluster	Tidak	ClusterStatus.merah maksimum adalah >= 1 selama 1 menit, 1 kali berturut-turut. AMS mengambil tindakan proaktif untuk mengurangi dampak operasional, saat peringatan ini dipicu.	CloudWatch alarm. Setidaknya satu serpihan utama dan replika yang tidak dialokasikan untuk simpul. Untuk mempelajari lebih lanjut, lihat Status Cluster Merah .
OpenSearch domain	Tidak	KMSKeyKesalahan >= 1 selama 1 menit, 1 kali berturut-turut.	CloudWatch alarm. Kunci enkripsi KMS yang digunakan untuk mengenkripsi data yang ada di domain Anda dinonaktifkan. Aktifkan kembali untuk mengembalikan operasi normal. Untuk mempelajari lebih lanjut, lihat Enkripsi Data saat Istirahat untuk OpenSearch Layanan Layanan .
		ClusterStatus.kuning maksimum adalah >= 1 selama 1 menit, 1 kali berturut-turut AMS mengambil tindakan proaktif untuk mengurangi dampak operasional, saat peringatan ini dipicu.	Setidaknya satu serpihan replika tidak dialokasikan ke simpul. Untuk mempelajari lebih lanjut, lihat Status Cluster Kuning .

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
		FreeStorageSpace minimum adalah ≤ 20480 selama 1 menit, 1 kali berturut-turut AMS mengambil tindakan proaktif untuk mengurangi dampak operasional, saat peringatan ini dipicu.	Sebuah simpul di klaster Anda turun ke 20 GiB ruang penyimpanan gratis. Untuk mempelajari lebih lanjut, lihat Kurangnya Ruang Penyimpanan yang Tersedia.
		ClusterIndexWritesBlocked ≥ 1 selama 5 menit, 1 kali berturut-turut AMS mengambil tindakan proaktif untuk mengurangi dampak operasional, saat peringatan ini dipicu.	Cluster memblokir permintaan tulis. Untuk mempelajari lebih lanjut, lihat ClusterBlockException.
		Simpul minimum $< x$ selama 1 hari, 1 kali berturut-turut AMS mengambil tindakan proaktif untuk mengurangi dampak operasional, saat peringatan ini dipicu.	x adalah jumlah simpul dalam klaster Anda. Alarm ini menunjukkan bahwa setidaknya satu simpul di klaster Anda telah tidak terjangkau untuk satu hari. Untuk mempelajari selengkapnya, lihat Node Cluster Gagal.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
		CPUUtilization Rata-rata adalah $\geq 80\%$ selama 15 menit, 3 kali berturut-turut AMS mengambil tindakan proaktif untuk mengurangi dampak operasional, saat peringatan ini dipicu.	Pemanfaatan CPU 100% adalah umum, tetapi rata-rata tinggi yang berkelanjutan bermasalah. Pertimbangkan untuk menggunakan jenis instans yang lebih besar atau menambahkan instans.
		JVMMemoryTekanan maksimum adalah $\geq 80\%$ selama 5 menit, 3 kali berturut-turut AMS mengambil tindakan proaktif untuk mengurangi dampak operasional, saat peringatan ini dipicu.	Klaster bisa mengalami kesalahan kehabisan memori jika penggunaan meningkat. Pertimbangkan penskalaan vertikal. Amazon ES menggunakan separuh dari RAM instans untuk Java heap, hingga ukuran tumpukan 32 GiB. Anda dapat menskalakan instans secara vertikal hingga 64 GiB RAM, di mana Anda dapat menskalakan secara horizontal dengan menambahkan instans.
		Guru CPUUtilization Rata-rata adalah $\geq 50\%$ selama 15 menit, 3 kali berturut-turut AMS mengambil tindakan proaktif untuk mengurangi dampak operasional, saat peringatan ini dipicu.	Pertimbangkan untuk menggunakan tipe instans yang lebih besar untuk node master khusus Anda. Karena perannya dalam stabilitas dan blue/green penerapan cluster, node master khusus harus memiliki penggunaan CPU rata-rata yang lebih rendah daripada node data.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
		JVMMemoryTekanan Master maksimum adalah $\geq 80\%$ selama 15 menit, 1 kali berturut-turut AMS mengambil tindakan proaktif untuk mengurangi dampak operasional, saat peringatan ini dipicu.	Pertimbangkan untuk menggunakan tipe instans yang lebih besar untuk node master khusus Anda. Karena perannya dalam stabilitas dan blue/green penerapan cluster, node master khusus harus memiliki penggunaan CPU rata-rata yang lebih rendah daripada node data.
OpenSearch contoh	Tidak	AutomatedSnapshotFailure maksimum adalah ≥ 1 selama 1 menit, 1 kali berturut-turut.	CloudWatch alarm. Sebuah snapshot otomatis gagal. Kegagalan ini sering merupakan hasil dari status kesehatan klaster merah. Lihat Status Cluster Merah.
Contoh Elastic Load Balancing	Tidak	SurgeQueueLength > 100 selama 1 menit, 15 kali berturut-turut.	CloudWatch alarm jika kelebihan jumlah permintaan sedang menunggu perutean.
		HTTPCode_ELB_5xx_Hitung jumlah > 0 selama 5 menit, 3 kali berturut-turut.	CloudWatch alarm pada kelebihan jumlah kode respons HTTP 5XX yang berasal dari penyeimbang beban.
		SpilloverCount > 1 selama 1 menit, 15 kali berturut-turut.	CloudWatch alarm jika kelebihan jumlah permintaan yang ditolak karena antrian lonjakan penuh.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
GuardDuty layanan	Ya	Tidak berlaku; semua temuan (tujuan ancaman) dipantau. Setiap temuan sesuai dengan peringatan. Perubahan dalam GuardDuty temuan. Perubahan ini termasuk temuan yang baru dihasilkan atau kejadian selanjutnya dari temuan yang ada.	Daftar jenis GuardDuty temuan yang didukung ada di Jenis Penemuan GuardDuty Aktif .
Kondisi	Bervariasi	AWS Health Dashboard	Pemberitahuan dikirim ketika ada perubahan status AWS Health Dashboard (AWS Health) peristiwa sehubungan dengan layanan dasar yang didukung oleh AMS. Untuk informasi selengkapnya, lihat Layanan yang didukung .
AWS Managed Microsoft AD	Tidak	Status Direktori Aktif AWS Managed Microsoft AD instance mengirimkan acara status aktif.	Acara layanan. Dipancarkan ketika direktori beroperasi secara normal setelah suatu peristiwa.
		Status Direktori Terganggu AWS Managed Microsoft AD instance mengirimkan peristiwa status direktori terganggu.	Acara layanan. Dipancarkan saat direktori berjalan dalam keadaan terdegradasi. Satu atau lebih masalah telah terdeteksi, dan tidak semua operasi direktori dapat bekerja pada kapasitas operasional penuh.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
		Status Direktori Tidak Dapat Dioperasikan AWS Managed Microsoft AD instance mengirimkan peristiwa status yang tidak dapat dioperasikan.	Acara layanan. Dipancarkan ketika direktori tidak berfungsi. Semua titik akhir direktori telah melaporkan masalah.
		Menghapus Status Direktori AWS Managed Microsoft AD misalnya mengirimkan acara status direktori penghapusan.	Acara layanan. Dipancarkan saat direktori sedang dihapus.
		Status Direktori Gagal AWS Managed Microsoft AD instance mengirimkan peristiwa status gagal.	Acara layanan. Dipancarkan ketika direktori tidak dapat dibuat.
		RestoreFailed Status Direktori AWS Managed Microsoft AD instance mengirimkan peristiwa status direktori yang gagal dipulihkan.	Acara layanan. Dipancarkan saat memulihkan direktori dari snapshot gagal.
Contoh Amazon RDS	Tidak	Peringatan Penyimpanan Rendah dipicu ketika penyimpanan yang dialokasikan untuk instans DB telah habis.	RDS-EVENT-0007, lihat detail di Menggunakan pemberitahuan acara Amazon RDS.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
		Instans DB gagal Instans DB gagal karena konfigurasi tidak kompatibel atau masalah penyimpanan yang mendasarinya. Mulailah a point-in-time-restore untuk instance DB.	Acara layanan. RDS-EVENT-0031, Kategori Acara Amazon RDS dan Pesan Acara.
		Failover tidak dicoba Amazon RDS tidak mencoba failover yang diminta karena failover baru-baru ini terjadi pada instans DB.	Acara layanan. RDS-EVENT-0034, Kategori Acara Amazon RDS dan Pesan Acara.
		Parameter instans DB tidak valid Misalnya, MySQL tidak dapat memulai karena parameter terkait memori disetel terlalu tinggi untuk kelas instance ini, sehingga tindakan pelanggan adalah memodifikasi parameter memori dan me-reboot instance DB.	Acara layanan. RDS-EVENT-0035, Kategori Acara Amazon RDS dan Pesan Acara.
		Instans IDs subnet DB tidak valid Instans DB ada di jaringan yang tidak kompatibel. Beberapa subnet yang ditentukan IDs tidak valid atau tidak ada.	Acara layanan. RDS-EVENT-0036, Kategori Acara Amazon RDS dan Pesan Acara.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
		Contoh DB membaca kesalahan replika Terjadi kesalahan dalam proses replikasi baca. Untuk mengetahui informasi selengkapnya, lihat pesan peristiwa. Untuk informasi tentang pemecahan masalah kesalahan Baca Replika, lihat Memecahkan Masalah Replica MySQL Read Replica.	Acara layanan. RDS-EVENT-0045, Kategori Acara Amazon RDS dan Pesan Acara.
		Replikasi baca instans DB berakhir Replikasi pada Read Replica telah berakhir.	Acara layanan. RDS-EVENT-0057, Kategori Acara Amazon RDS dan Pesan Acara.
		Kesalahan membuat akun pengguna statspack Terjadi kesalahan saat membuat akun pengguna Statspack PERFSTAT. Jatuhkan akun sebelum menambahkan opsi Statspack.	Acara layanan. RDS-EVENT-0058, Kategori Acara Amazon RDS dan Pesan Acara.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
		Pemulihan instans DB dimulai	Acara layanan. RDS-EVENT-0066, Kategori Acara Amazon RDS dan Pesan Acara.
		Instans DB SQL Server membangun ulang cerminnya. Performa akan diturunkan hingga cermin dibangun kembali. Basis data ditemukan dengan model pemulihan non-FULL. Model pemulihan diubah kembali ke FULL dan pemulihan mirroring dimulai. (<dbname>: <recovery model found>[,...]).	
		Failover untuk klaster DB telah gagal.	
		Bucket S3 pemulihan izin tidak valid	
		Peran IAM yang Anda gunakan untuk mengakses bucket Amazon S3 untuk pencadangan dan pemulihan native SQL Server tidak dikonfigurasi dengan benar. Untuk informasi selengkapnya, lihat Menyiapkan Pencadangan dan Pemulihan Asli .	Acara layanan. RDS-EVENT-0081, Kategori Acara Amazon RDS dan Pesan Acara.
		Aurora tidak dapat menyalin data cadangan dari bucket Amazon S3.	RDS-EVENT-0082, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
		Peringatan penyimpanan rendah ketika instans DB telah mengkonsumsi lebih dari 90% penyimpanan yang dialokasikan	RDS-EVENT-0089, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
		Layanan notifikasi saat penskalaan gagal untuk klaster DB Tanpa Server Aurora.	RDS-EVENT-0143, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
		Instans DB dalam keadaan tidak valid. Tidak ada tindakan yang diperlukan. Penskalaan otomatis akan dicoba lagi nanti.	RDS-EVENT-0219, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
		Instans DB telah mencapai ambang penyimpanan penuh, dan database telah dimatikan.	RDS-EVENT-0221, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
		Peristiwa ini menunjukkan penskalaan otomatis penyimpanan instans RDS tidak dapat diskalakan, mungkin ada beberapa alasan mengapa penskalaan otomatis gagal.	RDS-EVENT-0223, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
		Penskalaan otomatis penyimpanan telah memicu tugas penyimpanan skala tertunda yang akan mencapai ambang penyimpanan maksimum.	RDS-EVENT-0224, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
		Instans DB memiliki tipe penyimpanan yang saat ini tidak tersedia di Availability Zone. Penskalaan otomatis akan dicoba lagi nanti.	RDS-EVENT-0237, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
		RDS gagal menyediakan kapasitas untuk proksi karena tidak ada alamat IP yang cukup yang tersedia di subnet Anda.	RDS-EVENT-0243, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
		Penyimpanan untuk akun AWS Anda telah melebihi kuota penyimpanan yang diizinkan.	RDS-EVENT-0254, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
		CPUUtilization Pemanfaatan CPU rata-rata > 90% selama 15 menit, 2 kali berturut-turut.	CloudWatch alarm.
		DiskQueueDepth Jumlahnya > 75 selama 1 menit, 15 kali berturut-turut.	
		FreeStorageSpace Rata-rata < 1.073.741.824 byte selama 5 menit, 2 kali berturut-turut.	
		SwapUsage Rata-rata >= 104.857.600 byte selama 5 menit, 2 kali berturut-turut.	
Klaster Amazon Redshift	Tidak	RedshiftClusterStatus Kesehatan cluster saat tidak dalam mode pemeliharaan < 1 selama 5 menit.	1 mewakili cluster yang sehat.

Layanan	Peringatan keamanan	Nama peringatan dan kondisi pemicu	Catatan
Amazon Macie	Ya	Peringatan yang baru dibuat dan pembaruan untuk peringatan yang ada. Macie menemukan perubahan dalam temuan. Perubahan ini termasuk temuan yang baru dihasilkan atau kejadian selanjutnya dari temuan yang ada.	Peringatan Amazon Macie. Untuk daftar jenis peringatan Macie yang didukung, lihat Menganalisis Temuan Amazon Macie. Perhatikan bahwa Macie tidak diaktifkan untuk semua akun.

AMS mengambil tindakan pro-aktif (menskalakan klaster) saat peringatan ini dipicu.

Untuk informasi tentang upaya remediasi, lihat [Remediasi peringatan otomatis AMS](#).

[Tonton video Andrew untuk mempelajari lebih lanjut \(7:03\)](#)

Retensi log dan default rotasi

[Bagian ini menjelaskan default manajemen log AMS; untuk informasi selengkapnya, lihat Manajemen Log.](#)

- Rotasi = Perputaran log di dalam instance
- Retensi = Periode waktu kami menyimpan log di Amazon Logs dan Amazon CloudWatch Simple Storage Service (S3)

Log disimpan di CloudWatch Log sesuai kebutuhan (Anda dapat mengonfigurasi ini), dan di S3. Mereka tidak kedaluwarsa atau dihapus dan tunduk pada daya tahan layanan. Untuk informasi ketahanan S3 yang mendetail, lihat [Perlindungan data di Amazon S3](#).

Anda dapat meminta perubahan penyimpanan log untuk semua log, kecuali AWS CloudTrail log, yang disimpan tanpa batas waktu untuk alasan audit dan keamanan.

Rotasi log dikonfigurasi di dalam instance. Secara default, sistem operasi dan log keamanan berputar setiap jam jika mencapai lebih dari 100MB, ini dilakukan untuk memastikan bahwa Anda tidak kekurangan disk dalam instance.

Agen log di dalam instance mengunggah log online ke Log, dari sana CloudWatch log diarsipkan ke S3.

Log disimpan dalam CloudWatch Log dan S3 dalam format mentah yang dihasilkan, tidak ada pra-pemrosesan.

Menggunakan konsol AMS

Konsol AMS di AWS Management Console tersedia bagi Anda untuk berinteraksi dengan AMS dan mengoperasikan sumber daya AMS Advanced-managed dan AMS Accelerate Anda. Konsol AMS umumnya berperilaku seperti AWS konsol apa pun; Namun, karena AMS adalah organisasi pribadi, hanya akun yang diaktifkan untuk AMS yang dapat mengakses konsol. Setelah AMS diaktifkan di akun Anda, Anda dapat mengakses konsol dengan mencari “Managed Services” di bilah pencarian terpadu.

Note

Bergantung pada peran akun Anda, Anda mengakses konsol AMS Advanced atau konsol AMS Accelerate.

Saat menggunakan konsol AMS, perhatikan peringatan berikut:

- Konsol AMS khusus untuk akun. Jadi, jika Anda berada di akun “Uji” untuk organisasi Anda, Anda tidak akan dapat melihat sumber daya di akun “Prod” untuk organisasi itu. Demikian juga, Anda harus memiliki peran AMS Advanced untuk mengakses konsol AMS Advanced.
- Konsol AMS menerapkan kebijakan IAM saat Anda mengautentikasi yang menentukan konsol mana yang dapat Anda akses dan apa yang dapat Anda lakukan di sana. Administrator Anda dapat menerapkan kebijakan tambahan pada kebijakan AMS default untuk membatasi apa yang dapat Anda lihat dan lakukan di konsol.

Konsol AMS Advanced memiliki fitur-fitur ini:

- Halaman pembuka: Halaman pembuka memiliki kotak informasi dan tautan untuk memfasilitasi akses Anda ke yang ada RFCs, insiden, permintaan layanan, dan laporan Anda.
- Halaman fitur, tautan di panel navigasi sebelah kiri:
 - Dasbor: Memberikan ikhtisar status akun Anda saat ini termasuk:
 - Permintaan perubahan: Lihat berapa banyak RFCs yang Menunggu respons Anda, dan lompat ke halaman daftar RFC dengan filter tersebut aktif. Lihat berapa banyak RFCs yang Menunggu persetujuan Anda, dan lompat ke halaman daftar RFC dengan filter itu aktif. Lihat berapa banyak RFCs yang Terbuka, dan lompat ke halaman daftar RFC dengan filter itu aktif. Buka halaman daftar RFCs dengan mengklik tautan Lihat semua.
 - Insiden: Lihat berapa banyak kasus insiden yang Menunggu tanggapan Anda, dan lompat ke halaman daftar insiden dengan filter tersebut aktif. Lihat dan berapa banyak yang Terbuka, dan lompat ke halaman daftar insiden dengan filter itu aktif. Buka halaman daftar insiden dengan mengklik tautan Lihat semua.
 - Permintaan layanan: Lihat berapa banyak permintaan layanan yang Menunggu respons Anda, dan langsung ke halaman daftar permintaan layanan dengan filter tersebut aktif. Lihat dan berapa banyak yang Terbuka, dan lompat ke halaman daftar permintaan layanan dengan filter itu aktif. Buka halaman daftar permintaan layanan dengan mengklik tautan Lihat semua.
 - Baru-baru ini diperbarui RFCs: Tanggal, tautan ke detail RFC, dan status
 - Insiden dan permintaan layanan yang baru dibuat: Tanggal, tautan ke detail kasus, dan jenis (insiden atau permintaan layanan)
 - RFCs: Membuka daftar yang ada RFCs untuk akun
 - Insiden: Membuka daftar insiden terbuka untuk akun
 - Permintaan layanan: Membuka daftar permintaan layanan terbuka untuk akun
 - Laporan: Membuka halaman Laporan dan laporan default, Backup Harian dan Patch Harian dan Penagihan Bulanan
 - Sumber Daya:
 - VPCs: Membuka daftar yang ada VPCs untuk akun
 - Tumpukan: Membuka daftar tumpukan yang ada untuk akun
 - AMIs: Membuka daftar AMS yang tersedia AMIs
 - Sorotan fitur: Informasi tentang pembaruan terbaru ke konsol
 - Sumber Daya Pengembang: Halaman file yang dapat diunduh, termasuk SDK manajemen perubahan AMS Advanced dan lainnya
 - Dokumentasi: Halaman landing dokumentasi AWS Managed Services

Menggunakan AMS API dan CLI

AWS Managed Services (AMS) API mirip dengan APIs untuk AWS layanan lainnya. Anda dapat membaca tentang AMS API di [Referensi API AMS](#).

Titik akhir HTTP AMS API untuk panggilan REST

Selain beragam SDKs, AMS menyediakan CLI; Anda juga dapat memanggil panggilan REST API terhadap titik akhir AMS.

Ada dua AMS APIs (titik akhir untuk keduanya berada di us-east-1):

- **Manajemen Perubahan:** Gunakan API ini untuk meminta akses atau perubahan pada infrastruktur Anda, termasuk membuat dan memperbarui RFCs, menerapkan instance baru, memperbarui dan menghapus instance, mendapatkan informasi, dan membuat. CTs AMIs Titik akhir HTTP adalah:

`https://amscm.us-east-1.amazonaws.com`

- **SKMS:** Gunakan API ini untuk mendapatkan informasi tentang infrastruktur Anda, termasuk, tumpukan VPCs, subnet, dan. AMIs Titik akhir HTTP adalah:

`https://amsskms.us-east-1.amazonaws.com`

Menginstal atau memutakhirkan AMS CLI

AMS CLI adalah cara mudah untuk berinteraksi dengan AMS API dan digunakan dalam contoh di bagian ini. Untuk konvensi penggunaan untuk AWS CLI dan AMS CLI, [lihat Menggunakan AWS Antarmuka Baris perintah](#).

Untuk informasi tentang menginstal SAFL, lihat [Aturan klaim AD FS dan setelan SAMP](#).

Untuk menginstal atau memutakhirkan AMS CLI, ikuti petunjuk berikut:

Note

Anda harus memiliki kredensi administrator untuk prosedur ini.

AWS CLI adalah prasyarat untuk menggunakan AWS Managed Services (AMS) CLIs (Change Management and SKMS).

1. Untuk menginstal AWS CLI, lihat [Menginstal AWS Command Line Interface](#), dan ikuti petunjuk yang sesuai. Perhatikan bahwa di bagian bawah halaman itu ada instruksi untuk menggunakan installer yang berbeda, [Linux](#), [MS Windows](#), [macOS](#), [Virtual Environment](#), [Bundled Installer \(Linux, macOS, atau Unix\)](#).

Setelah instalasi, jalankan `aws help` untuk memverifikasi instalasi.

2. Setelah AWS CLI diinstal, untuk menginstal atau memutakhirkan AMS CLI, unduh file zip yang dapat didistribusikan AMS CLI atau AMS SDK dan unzip. Anda dapat mengakses distribusi AMS CLI melalui tautan [Sumber Daya Pengembang](#) di navigasi kiri konsol AMS.
3. File README memberikan instruksi untuk instalasi apa pun.

Buka:

- CLI zip: Hanya menyediakan AMS CLI.
- SDK zip: Menyediakan semua AMS APIs dan AMS CLI.

Untuk Windows, jalankan installer yang sesuai (hanya 32 atau 64 bit sistem):

- 32 Bit: `ManagedCloudAPI_x86.msi`
- 64 Bit: `ManagedCloudAPI_x64.msi`

Untuk Mac/Linux, jalankan file bernama: `AWSManagedServices_InstallCLI.sh` dengan menjalankan perintah ini: `sh AWSManagedServices_InstallCLI.sh` Perhatikan bahwa direktori `amscm` dan `amsskms` dan isinya harus berada di direktori yang sama dengan file `sh`. `AWSManagedServices_InstallCLI`

4. Jika kredensial perusahaan Anda digunakan melalui federasi dengan AWS (konfigurasi default AMS), Anda harus menginstal alat manajemen kredensi yang dapat mengakses layanan federasi Anda. Misalnya, Anda dapat menggunakan AWS Security Blog [Cara Menerapkan API Federasi dan Akses CLI Menggunakan SAFL 2.0 dan AD FS](#) untuk bantuan mengonfigurasi alat manajemen kredensi Anda.
5. Setelah instalasi, jalankan `aws amscm help` dan `aws amsskms help` untuk melihat perintah dan opsi.

 Note

AMS CLI harus diinstal agar perintah ini berfungsi. Untuk menginstal AMS API atau CLI, buka halaman Sumber Daya Pengembang konsol AMS. Untuk materi referensi tentang AMS CM API atau AMS SKMS API, lihat bagian Sumber Informasi AMS di Panduan Pengguna. Anda mungkin perlu menambahkan `--profile` opsi untuk otentikasi; misalnya, `aws amsskms ams-cli-command --profile SAML`. Anda mungkin juga perlu menambahkan `--region` opsi karena semua perintah AMS kehabisan `us-east-1`; misalnya, `aws amscm ams-cli-command --region=us-east-1`

Menggunakan AMS API di CLI, Ruby, Python, dan Java

Berikut ini adalah daftar cuplikan kode untuk `ListChangeTypeClassificationSummaries` operasi AMS API, dalam semua bahasa yang tersedia.

Untuk Python, Ruby, dan Java SDKs, lihat [Alat untuk Amazon Web Services](#) dan gulir ke bawah ke bagian tersebut. SDKs Setiap penginstal SDK berisi README dengan cuplikan kode tambahan.

Contoh AMS API ke CLI

Setelah Anda menginstal AMS CLI (memerlukan AWS CLI; lihat [Menginstal atau memutakhirkan AMS CLI](#)), Anda dapat menjalankan operasi AMS API apa pun dengan mereformasi panggilan terlebih dahulu menentukan AMS API mana, `aws amscm` atau `aws amsskms`, dan kemudian memberikan tindakan dengan tanda hubung menggantikan kasus unta. Terakhir, berikan kredensial, seperti SALL.

Untuk mempelajari lebih lanjut, lihat [Menggunakan Antarmuka Baris AWS Perintah](#).

Contoh:

- API: `'ChangeTypeClassificationSummaries[].[Category,Subcategory,Item,Operation,ChangeTypeId]'`
- CLI: `amscm list-change-type-classification-summaries --query "ChangeTypeClassificationSummaries[*].[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table`

Note

Jika Anda mengautentikasi dengan SAFL, tambahkan `aws --profile saml` ke awal perintah. Misalnya,

```
aws --profile saml amscm list-change-type-classification-  
summaries --query "ChangeTypeClassificationSummaries[*].  
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

Contoh AMS API ke Python

Untuk menggunakan AMS API dengan Python, instal AMS CLI dan instal boto3. Ikuti langkah-langkah ini:

1. Instal AMS CLI. Lihat [Menginstal atau memutakhirkan AMS CLI](#).
2. Instal boto3, AWS SDK untuk Python. Untuk informasi lebih lanjut, lihat posting blog ini [Sekarang Tersedia — AWS SDK Untuk Python \(Boto3\)](#).

```
import boto3
```

3. Dapatkan klien AMS Change Management:

```
cm = boto3.client('amscm')
```

4. Dapatkan AMS CTs:

```
cts = cm.list_change_type_classification_summaries()  
  
print(cts)
```

Contoh Python

Berikut ini adalah beberapa contoh untuk menggunakan Python di AMS, untuk membuat EC2 instance, gunakan and/or Lambda.

Contoh Python untuk membuat sebuah EC2

Contoh ini menunjukkan bagaimana Anda dapat menggunakan RESTFul API amscm dari dalam kode Python untuk mengajukan dan melakukan proses RFC.

1. Instal AMS CLI di suatu tempat yang dapat Anda akses; Anda memerlukan file yang disediakan.
2. Panggil pustaka Python dan buat instance: EC2

```
import boto3
import json
import time

# Create the amscm client
cm = boto3.client('amscm')

# Define the execution parameters for EC2 Create
AMSExecParams = {
    "Description": "EC2-Create",
    "VpcId": "VPC_ID",
    "Name": "My-EC2",
    "TimeoutInMinutes": 60,
    "Parameters": {
        "InstanceAmiId": "INSTANCE_ID",
        "InstanceSubnetId": "SUBNET_ID"
    }
}

# Create the AMS RFC
cts = cm.create_rfc(
    ChangeTypeId="ct-14027q0sjyt1h",
    ChangeTypeVersion="3.0",
    Title="Python Code RFC Create",
    ExecutionParameters=json.dumps(AMSExecParams)
)

# Extract the RFC ID from the response
NewRfcID = cts['RfcId']

# Submit the RFC
RFC_Submit_Return=cm.submit_rfc(RfcId=NewRfcID)

# Check the RFC status every 30 seconds
RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']

while RFC_Status_Code != "Success":
```

```
if RFC_Status_Code == "PendingApproval":
    print(RFC_Status_Code)
    time.sleep(30)
elif RFC_Status_Code == "InProgress":
    print(RFC_Status_Code)
    time.sleep(30)
elif RFC_Status_Code == "Failure":
    print(RFC_Status_Code)
    break
else:
    print(RFC_Status_Code)

RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']
```

Contoh Python dengan Lambda

Contoh ini menunjukkan cara menggabungkan model AMS dengan kode Anda sehingga Anda dapat menggunakannya dengan Lambda, atau EC2; tempat yang tidak akan, atau tidak bisa, instal. `amsccli`

Note

AMS tidak menyediakan SDK Python khusus AMS yang dapat diimpor. Skrip penginstalan menginstal model data layanan AMS di jalur normal CLI. `amsccli` Untuk penggunaan CLI dan penggunaan Python sistem, tidak apa-apa, karena keduanya `awscli` dan `boto3` membaca model layanan mereka dari lokasi default yang sama (`~/.aws/models`). Namun, ketika Anda ingin menggunakan layanan AMS melalui `boto3` di Lambda (atau runtime non-lokal lainnya), itu rusak, karena Anda tidak lagi memiliki model data. Berikut ini adalah metode untuk memperbaikinya dengan mengemas model data dengan fungsi.

Ada langkah-langkah sederhana yang dapat Anda ambil untuk menjalankan kode Python terintegrasi AMS di Lambda atau runtime lain seperti, Fargate, dll. EC2 Alur kerja berikut menunjukkan langkah-langkah yang diperlukan untuk fungsi Lambda terintegrasi AMS.

Dengan menambahkan model data ke paket penerapan kode dan memperbarui jalur pencarian SDK, Anda dapat mensimulasikan pengalaman SDK.

 Important

Contoh ini dan semua perintah non-python yang ditampilkan diuji pada komputer Mac.

Contoh Alur Kerja:

1. Instal `amsccli`. Ini membuat folder `~/.aws/models` di komputer Anda (Mac).
2. Salin model ke direktori lokal: `cp ~/.aws/models ./models`.
3. Sertakan model ke dalam paket penyebaran kode Anda.
4. Perbarui kode fungsi Anda untuk menambahkan model baru ke jalur SDK. Perhatikan bahwa kode ini harus dijalankan sebelum `boto3` atau `botocore` diimpor!

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

 Note

Karena model contoh berada dalam direktori bernama `models`, kita tambahkan `./models` ke `AWS_DATA_PATH`. Jika direktori diberi nama `ams/boto3models`, kami akan menambahkan kode berikut:

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

Kode Anda harus berhasil menemukan model AMS. Sebagai contoh yang lebih spesifik re: packaging, inilah alur kerja spesifik Lambda.

Contoh Alur Kerja AMS Lambda:

Langkah-langkah ini menerapkan contoh generik sebelumnya untuk membuat fungsi AWS Lambda.

1. Instal amscli. Ini membuat folder ~/.aws/models di komputer Anda (Mac).
2. Salin model ke direktori lokal:

```
cp ~/.aws/models ./models
```

3. Tambahkan model ke file zip penerapan fungsi Anda:

```
zip -r9 function.zip ./models
```

Important

Perbarui kode fungsi Anda untuk menambahkan model baru ke jalur SDK. Perhatikan bahwa kode ini harus dijalankan sebelum boto3 atau botocore diimpor!

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

Note

Karena contoh model dalam direktori bernama models, Kami menambahkan ./models ke AWS_DATA_PATH. Jika direktori diberi nama/ams/boto3models, kami akan menambahkan kode berikut:

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

Sekarang, terapkan fungsi Anda:

1. Tambahkan kode fungsi Anda ke file zip penerapan (jika Anda belum melakukannya):


```
zip -g function.zip lambda-amscm-test.py
```

2. Buat atau perbarui fungsi Anda dengan file zip yang Anda buat (konsol atau CLI):

```
aws lambda update-function-code --function-name lambda-amscm-test --zip-file fileb://  
function.zip --region us-east-1
```

Lambda Python terintegrasi AMS Anda sekarang seharusnya berfungsi.

Note

Fungsi Anda harus memiliki izin IAM amscm atau Anda mendapatkan kesalahan izin.

Contoh kode fungsi Lambda untuk menguji amscm (isi dari.py): lambda-amscm-test

```
import json  
  
# Force lambda to search local directory for boto3 data models  
import os  
os.environ['AWS_DATA_PATH'] = './models'  
  
import boto3  
import botocore  
  
def lambda_handler(event, context):  
    use_session = boto3.session.Session(region_name="us-east-1")  
    try:  
        cm = use_session.client("amscm")  
        cts = cm.list_change_type_categories()  
        print(cts)  
    except botocore.exceptions.UnknownServiceError:  
        print("amscm not found")  
  
    return {  
        'statusCode': 200,  
        'body': json.dumps('Hello from Lambda!')  
    }
```

Uji output (sukses):

Respon Fungsi:

```
{
  "statusCode": 200,
  "body": "\"Hello from Lambda!\""
}
```

Request ID:

"1cea13c0-ed46-43b1-b102-a8ea28529c27"

Log Fungsi:

```
START RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27 Version: $LATEST
{'ChangeTypeCategories': ['Deployment', 'Internal Infrastructure Management',
  'Management'], 'ResponseMetadata': {'RequestId': 'e27276a0-e081-408d-
bcc2-10cf0aa19ece', 'HTTPStatusCode': 200, 'HTTPHeaders': {'x-amzn-requestid':
  'e27276a0-e081-408d-bcc2-10cf0aa19ece', 'content-type': 'application/x-amz-json-1.1',
  'content-length': '89', 'date': 'Sun, 10 May 2020 23:21:19 GMT'}, 'RetryAttempts': 0}}
END RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27
```

Contoh AMS API ke Ruby

Untuk menggunakan AMS API dengan Ruby, instal AWS Ruby SDK dan AMS CLI. Ikuti langkah-langkah ini:

1. Instal AMS CLI. Lihat [Menginstal atau memutakhirkan AMS CLI](#).
2. Instal AWS Ruby SDK. Lihat [Alat untuk Amazon Web Services](#).
3. Konfigurasi Ruby dengan perintah ini:

```
require 'aws-sdk'

config = {
  region: 'us-east-1',
  credentials: Aws::Credentials.new('ACCESS_KEY', 'SECRET_KEY')}
```

4. Dapatkan AMS CTs:

```
ams_cm = Aws::amscm::Client.new(config)
```

```
cts = ams_cm.list_change_type_classification_summaries

print(cts)
```

Contoh AMS API ke Java

Untuk menggunakan AMS API dengan Java, instal AWS Java SDK dan AMS CLI. Ikuti langkah-langkah ini:

1. Instal AMS CLI. Lihat [Menginstal atau memutakhirkan AMS CLI](#).
2. Instal AWS Java SDK. Lihat [Alat untuk Amazon Web Services](#).
3. Konfigurasi Java dengan perintah ini:

```
import com.amazonaws.auth.BasicAWSCredentials;

import com.amazonaws.services.amscm.model.AWSManagedServicesCMClient;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesRequest;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesResult;

public static void getChangeTypeClassificationSummaries() {
```

4. Atur kredensialnya. Kami menyarankan Anda untuk tidak melakukan hardcode ini.

```
final BasicAWSCredentials awsCredsCm =

    new BasicAWSCredentials("ACCESS_KEY", "SECRET_KEY");
```

5. Buat klien AMS Change Management:

```
final AWSManagedServicesCMClient cmClient =

    new AWSManagedServicesCMClient(awsCredsCm);
```

6. Dapatkan AMS CTs:

```
final ListChangeTypeClassificationSummariesRequest listCtsRequest = new
ListChangeTypeClassification SummariesRequest();
```

```
final ListChangeTypeClassificationSummariesResult listCtsResult =  
cmClient.listChangeTypeClassificationSummaries(listCtsRequest);  
  
System.out.println("List of CTs");  
  
listCtsResult.getChangeTypeClassificationSummaries().stream()  
    .map(x -> x.getCategory() + "/" + x.getSubcategory() + "/" +  
x.getItem() + "/" + x.getOperation())  
    .forEach(System.out::println);  
}
```

AMS membawa EPS Anda sendiri

Gunakan fitur AMS “bring your own end point security” (BYOEPS) untuk mengganti agen Trend Micro Deep Security default dengan solusi keamanan titik akhir Anda sendiri, atau lisensi Trend Micro. Jika Anda sudah memiliki lisensi hemat biaya untuk produk selain Trend Micro Deep Security, atau tim yang menyediakan EPS Anda, atau jika Anda ingin menggunakan alat EPS tertentu, gunakan BYOEPS dalam instans Anda.

BYOEPS bekerja di tingkat akun. Instance Anda di akun menggunakan BYOEPS atau EPS default yang dikelola AMS:

- multi-account landing zone (MALZ): Anda menunjuk akun aplikasi yang menggunakan BYOEPS atau EPS terkelola.
- single-account landing zone (SALZ): Akun AMS Anda menggunakan BYOEPS atau EPS terkelola.

BYOEPS, mengurangi AWS tagihan Anda dengan biaya untuk Trend Micro Deep Security. Anda terus dikenakan biaya untuk EPS karena EPS yang dikelola AMS masih diperlukan untuk melindungi EC2 instans yang dibuat dan dikelola AMS yang diperlukan untuk manajemen akses (benteng, dan host manajemen). Untuk menghitung dampak biaya total, Anda harus memperhitungkan biaya lisensi untuk alat baru Anda, dan biaya pengelolaan EPS pada tingkat layanan yang Anda butuhkan.

Penggunaan BYOEPS mengubah peran dan tanggung jawab AMS untuk manajemen keamanan:

- R adalah singkatan dari pihak yang bertanggung jawab yang melakukan pekerjaan untuk mencapai tugas.
- C adalah singkatan dari konsultasikan; pihak yang pendapatnya dicari, biasanya sebagai ahli materi pelajaran; dan dengan siapa ada komunikasi bilateral.
- Saya singkatan dari Informed; sebuah pihak yang diinformasikan tentang kemajuan, seringkali hanya pada penyelesaian tugas atau deliverable.

Manajemen keamanan	Pelanggan	AWS Managed Services
Mempertahankan lisensi EPS Terkelola yang valid untuk EC2 instance AMS Shared Services	R	C
Konfigurasi EPS Terkelola untuk EC2 instance AMS Shared Services	I	R
Memperbarui EPS Terkelola untuk EC2 instance AMS Shared Services	I	R
Memantau malware pada EC2 contoh AMS Shared Services	I	R
Mempertahankan dan memperbarui tanda tangan virus untuk EC2 instance AMS Shared Services	I	R
Memulihkan instans yang terinfeksi malware untuk EC2 instance AMS Shared Services	C	R

Ketika Anda menggunakan BYOEPS, Anda kehilangan salah satu kontrol keamanan yang ditawarkan oleh AMS. Anda masih memiliki manajemen keamanan yang disediakan melalui alat seperti Amazon GuardDuty, Amazon Macie, dan kontrol proses, seperti ulasan konfigurasi IAM. Penggunaan BYOEPS tidak memengaruhi sertifikasi dan pengesahan kepatuhan AMS. Namun, banyak kerangka kerja keamanan dan sertifikasi memiliki persyaratan untuk perlindungan dari malware dan kode berbahaya. Untuk membantu menjaga akun Anda tetap aman dan sesuai, evaluasi kontrol yang direncanakan untuk memastikan bahwa kontrol tersebut memenuhi persyaratan keamanan untuk sertifikasi kepatuhan beban kerja Anda.

Aktifkan BYOEPS untuk akun Anda

Proses untuk menghidupkan BYOEPS berisi tiga tahap dan menggunakan beberapa RFCs Tinjau informasi berikut untuk mempelajari tentang tiga tahap yang diperlukan untuk mengaktifkan BYOEPS. Kemudian, koordinasikan dengan CSDM Anda untuk mengaktifkan BYOEPS untuk akun Anda.

Topik

- [Tahap 1: Prasyarat](#)
- [Tahap 2: Aktifkan BYOEPS di akun Anda](#)
- [Tahap 3: Migrasi instans](#)

Tahap 1: Prasyarat

- Profil EC2 instans Amazon default adalah `customer-mc-ec2-instance-profile`. Jika Anda menggunakan profil EC2 instans Amazon yang berbeda selain profil default, izinkan `ssm:GetParameter` tindakan untuk `/ams/end-point-security` sumber daya ke profil EC2 instans Anda.

Jika Anda tidak dapat memperbarui profil EC2 instans, kirimkan RFC yang menentukan profil instans yang perlu Anda perbarui.

- Pahami ruang lingkup perubahan ini.

Penerapan melalui tipe perubahan otomatis AMS (CT) memungkinkan Anda menentukan AML yang digunakan dalam pembuatan.

Untuk menggunakan BYOEPS dengan akun yang menggunakan EPS yang dikelola AMS, Anda harus bekerja dengan AMS untuk menghapus instans Trend Micro dari EC2 instans tersebut, dan memperbarui kode AMS (misalnya, skrip boot) pada instance tersebut. Tindakan ini mungkin

memerlukan reboot, jadi ini adalah praktik terbaik untuk melakukan tindakan ini sebagai bagian dari jendela pemeliharaan. Hubungi CSDM Anda untuk mengidentifikasi jendela pemeliharaan untuk melakukan aktivitas ini dan membuat rencana migrasi. Untuk rencana migrasi, pertimbangkan pertanyaan-pertanyaan berikut:

1. Berapa banyak contoh yang Anda butuhkan untuk bermigrasi? Bagilah jumlah total instance menjadi batch inkremental yang lebih kecil.
 2. Bagaimana Anda akan membagi instance dalam batch? Misalnya, Anda dapat membagi berdasarkan grup sumber daya dan membuat daftar untuk dibagikan dengan tim operasi AMS.
 3. Berapa banyak waktu yang dibutuhkan setiap batch? Berapa total waktu yang dibutuhkan? Pertimbangkan bahwa Anda mungkin ingin menginstal perkakas EPS pilihan Anda di jendela pemeliharaan yang sama. Berapa banyak waktu yang dibutuhkan?
- CSDM Anda membagikan rencana migrasi dengan tim operasi AMS. Jika armada instans Anda di atas 50, maka bekerjalah dengan CSDM Anda untuk membuat acara yang direncanakan menggunakan proses manajemen acara yang direncanakan (PEM). Untuk informasi selengkapnya, lihat [Manajemen acara yang direncanakan di AWS Managed Services](#)

Operasi AMS berkoordinasi dengan CSDM Anda dan menyarankan RFCs cara mengirimkan sesuai dengan jendela pemeliharaan Anda, berdasarkan jumlah instans di akun Anda.

- Perbarui otomatisasi atau proses peluncuran EC2 instans menggunakan kustom atau AMS AMIs untuk menggunakan AMS yang AMIs dirilis setelah Desember 2020.

Tahap 2: Aktifkan BYOEPS di akun Anda

Saat Anda menggunakan BYOEPS di akun Anda, tanggung jawab yang dimiliki AMS untuk manajemen keamanan berubah. Konsultasikan dengan tim keamanan dan platform cloud Anda sebelum Anda mengaktifkan BYOEPS.

Untuk meminta BYOEPS untuk akun Anda, kirimkan pembaruan “MOO” RFC (Manajemen | Lainnya | Lainnya | Pembaruan) dengan ct-0xdawir96cy7k, dengan detail berikut:

Please enable BYOEPS for this account/these accounts
Account IDs: *IDs for the accounts for BYOEPS.*

AMS menerapkan pembaruan penyimpanan parameter ke akun dan memperbarui profil [instans Amazon EC2 IAM](#).

 Note

- Akun dengan peluncuran instans baru yang menggunakan AMS terbaru AMIs dapat melewati instalasi agen Trend Micro. AMIs lebih tua dari Desember 2020 tidak mendukung fitur BYOEPS. Perbarui otomatisasi yang menggunakan yang lama AMIs untuk menggunakan AMS terbaru AMIs dengan dukungan fitur BYOEPS.
- Untuk penanganan EC2 instans yang ada, lihat Tahap 3: Migrasi instans

Tahap 3: Migrasi instans

Gunakan salah satu opsi berikut untuk memigrasikan instans Anda, tergantung pada kasus penggunaan Anda. Jika Anda tidak yakin opsi mana yang harus dipilih, hubungi CA atau CSDM Anda.

Akun dengan EC2 instans yang menggunakan EPS yang dikelola AMS

Selama jendela pemeliharaan, selaras dengan perencanaan dari Tahap 1, tindakan berikut dilakukan pada setiap instance yang perlu di-onboard ke BYOEPS:

- Dilakukan oleh AMS: Perbarui kode AMS (skrip boot, modul, dan sebagainya) ke versi terbaru. Ini diperlukan karena skrip boot AMS lama tidak memiliki dukungan fitur BYOEPS dan menginstal ulang agen Trend Micro di setiap boot. Juga, hapus instalasi Trend Micro Agent.
- Dilakukan oleh Anda: Instal dan konfigurasi alat EPS pilihan Anda.

 Important

Trend Micro Agent memberikan perlindungan malware. Pastikan Anda memasang pengganti yang sesuai untuk mengamankan instans Anda.

Untuk membuat perubahan ini dikirimkan RFCs dengan jenis perubahan ct-2iz9nvw8zlhst, [Trend Micro DSM | Hapus Agen Trend Micro](#) EPS (Review Required), dalam batch.

Akun tanpa EC2 instans yang menggunakan EPS yang dikelola AMS

Akun dengan peluncuran instans baru yang menggunakan AMS terbaru AMIs dapat melewati instalasi agen Trend Micro. AMIs lebih tua dari Desember 2020 tidak mendukung fitur BYOEPS.

Perbarui otomatisasi yang menggunakan yang lama AMIs untuk menggunakan AMS terbaru AMIs dengan dukungan fitur BYOEPS.

Tambahkan agen Anda pada EC2 instans

Anda dapat menggunakan Pola AMS untuk menyebarkan agen alat seperti CrowdStrike atau Qualys, Kirim permintaan layanan untuk bantuan.

Menerima pemberitahuan AMS

Komunikasi antara Anda dan AMS terjadi karena berbagai alasan:

- RFC yang dibuat oleh AMS yang memerlukan persetujuan Anda
- Kasus AMS dibuat untuk menyelidiki RFC yang Anda buat yang gagal
- Acara yang dibuat oleh monitoring alerts
- Pemberitahuan layanan penambalan yang memberi tahu Anda tentang penambalan yang akan datang
- Permintaan layanan dan laporan insiden
- Laporan CRM bulanan
- Pengumuman AWS penting sesekali (CSDM Anda menghubungi Anda jika ada tindakan di pihak Anda yang diperlukan)

Semua pemberitahuan ini dikirim ke informasi kontak default (email akun root) yang Anda berikan AMS saat Anda masuk. Karena sulit untuk memperbarui email individual, kami sarankan Anda menggunakan email grup yang dapat diperbarui di pihak Anda. Semua pemberitahuan yang dikirimkan kepada Anda juga diterima oleh operasi AMS dan dianalisis sebelum membuat tanggapan.

Layanan pemberitahuan AMS menyediakan dua cara tambahan untuk mengatur kontak untuk pemberitahuan:

- Tandai sumber daya Anda dengan tag kontak (tag Nilai Kunci adalah informasi kontak) dan berikan tag Nama Kunci ke CSDM Anda. Alarm pada sumber daya tersebut akan dikirim ke kontak yang disediakan dalam Nilai Kunci, selain kontak akun yang dibuat saat orientasi. Ini sangat berguna bagi pemilik aplikasi. Untuk informasi selengkapnya, lihat [Pemberitahuan peringatan berbasis tag](#).
- (Diperlukan saat orientasi) Kirim ke daftar kontak bernama CSDM Anda untuk pemberitahuan berbasis non-sumber daya. Misalnya, Anda mungkin memiliki daftar bernama "SecurityContacts" dan yang lain bernama "OperationsContacts", dan sebagainya. AMS menambahkan daftar ke

layanan notifikasi, dan alarm yang berlaku untuk konteks daftar tersebut dikirim ke kontak tersebut. Ini sangat berguna untuk masalah organisasi.

Fitur perutean peringatan lanjutan ini aktif untuk sebagian besar CloudWatch alarm penting seperti kegagalan EC2 instans Amazon, Amazon Elastic Block Store (Amazon EBS) pemanfaatan kapasitas volume - Penggunaan Root, penggunaan NonRoot Amazon EBS, pemanfaatan Memori Tinggi, penggunaan High Swap, dan Pemanfaatan CPU Tinggi untuk Amazon. EC2

Selain itu, ketika Anda mengajukan permintaan layanan, atau laporan insiden, Anda memiliki opsi untuk menambahkan "Email CC" (sangat disarankan) dan alamat email tersebut menerima pemberitahuan tentang permintaan layanan atau insiden.

Important

Sementara alamat email CC yang disediakan dalam permintaan layanan dan laporan insiden menerima pemberitahuan email komunikasi, pemberitahuan lain, seperti pemberitahuan patch, muncul di daftar Permintaan Layanan Anda (email juga dikirim ke kontak default), tanpa pemberitahuan eksplisit kepada Anda bahwa Anda memiliki komunikasi yang menunggu perhatian Anda. Inilah sebabnya mengapa kami sangat menyarankan untuk menambahkan email CC di mana Anda bisa, dan menyiapkan email kontak default sebagai grup di mana semua orang yang menggunakan AMS adalah anggota.

Selain itu, Anda dapat meminta pemberitahuan khusus untuk yang baru AMIs, untuk perubahan status RFC, dan untuk perubahan konfigurasi di akun AMS Anda. Layanan notifikasi opsional ini akan dibahas selanjutnya.

Pemberitahuan AMS AMI dengan SNS

AMS menyediakan layanan notifikasi AMI. Anda dapat menggunakannya untuk berlangganan topik Amazon Simple Notification Service (SNS) Amazon yang memberi tahu Anda saat pembaruan AMS AMI telah dirilis. Anda dapat memilih untuk menerima pemberitahuan hanya untuk AMS yang AMIs Anda gunakan, atau Anda dapat mendaftar untuk menerima pemberitahuan pembaruan untuk semua AMS AMIs. Untuk informasi selengkapnya tentang topik SNS, lihat [Apa itu Layanan Pemberitahuan Sederhana Amazon?](#)

Setiap kali AMIs dirilis, kami mengirim pemberitahuan kepada pelanggan tentang topik yang sesuai; bagian ini menjelaskan cara berlangganan pemberitahuan AMS AMI.

Contoh pesan

```
{
  "Type" : "Notification",
  "MessageId" : "example messageId",
  "TopicArn" : "arn:aws:sns:us-east-1:591688410472:customer-ams-windows2019",
  "Subject" : "New AMS AMIs are Now Available",
  "Message" : "{\"v1\": {\"Message\": \"A new version of the AMS Amazon Machine Images has
been released. You are now able to launch new EC2 stacks from these AMIs.
Please use this time to update any dependencies such as CloudFormation or Autoscaling
groups. Release Notes Windows - Contains latest Windows Patches:
Microsoft Windows Server 2008 R2 Datacenter - (KB2819745, KB3018238, KB4507004,
KB4507437) Microsoft Windows Server 2016 Datacenter Security Enhancedn - (KB4509091,
KB4507459)
Microsoft Windows Server 2016 Datacenter - (KB4509091, KB4507459) Microsoft Windows
Server 2012 R2 Security Enhancedn - (KB3191564, KB3003057, KB3013172, KB3185319,
KB4504418,
KB4506996, KB4507463) Microsoft Windows Server 2012 R2 Standardn - (KB3003057,
KB3013172, KB3185319, KB4504418, KB4506996, KB4507463) Linux - Contains latest Linux
patches -
All AMIs now force domainjoin-cli leave before domainjoin-cli join for better
stability in the domain join process.\"\", \"images\":
{\"images\": {\"image_name\": \"customer-ams-windows2019-2021.08-1\", \"image_id\":
\"ami-05dfa45396fddaa5e\"}}, \"region\": \"us-east-1\"}}\",
\"Timestamp\" : \"2021-09-03T19:05:57.882Z\",
\"SignatureVersion\" : \"1\",
\"Signature\" : \"example sig\",
\"SigningCertURL\" : \"example url\",
\"UnsubscribeURL\" : \"example url\"
}
```

Kemungkinan topik AMS AMI untuk berlangganan:

- SEMUA: Gunakan `customer-ams-all-amis`. Langganan topik ini memberi tahu Anda ketika salah satu AMS AMIs diperbarui.
- AMS AWS Linux AMIs: Untuk Amazon Linux, gunakan `customer-ams-amazon1` dan `customer-ams-amazon1-security-enhanced`. Untuk Amazon Linux 2, gunakan `customer-ams-amazon2` dan `customer-ams-amazon2-security-enhanced`.
- AMS SUSE Linux AMIs: Gunakan `customer-ams-sles12` atau `customer-ams-sles15`.
- AMS AWS RedHat AMIs: Gunakan `customer-ams-rhel8`, `customer-ams-rhel8-security-enhanced`, `customer-ams-rhel7`, `customer-ams-rhel7-security-enhanced`.

- AMS AWS CentOS AMIs: Gunakancustomer-ams-centos7,customer-ams-centos7-security-enhanced.
- AMS Ubuntu AMIs: Gunakancustomer-ams-ubuntu18.
- AMS AWS Windows AMIs: Gunakan customer-ams-windows2019customer-ams-windows2019-security-enhanced,customer-ams-windows2016,customer-ams-windows2016-security-enhanced,customer-ams-windows2012,,customer-ams-windows2012r2,customer-ams-windows2012r2-security-enhanced,customer-ams-windows2022.

Untuk berlangganan pemberitahuan AMI baru AMS dengan menggunakan konsol Amazon SNS:

1. [Buka konsol Amazon SNS ke Dasbor.](#)
2. Di sudut kanan atas, ubah ke Wilayah AWS untuk langganan AMIs Anda.
3. Di panel navigasi kiri, pilih Langganan, lalu pilih Buat langganan.
4. Saat diminta, berikan informasi berikut:
 - a. Topik ARN: `arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}` di mana REGION adalah Wilayah AWS yang dipilih (tempat notifikasi SNS dibuat) dan AMS_AMI_NAME adalah AMI yang Anda inginkan notifikasi. Contoh:
 - Untuk berlangganan notifikasi AMS Amazon Linux baru AMIs di AWS Region us-east-1, gunakan Topik ARN = ini. `arn:aws:sns:us-east-1:287847593866:customer-ams-amazon1`
 - Untuk berlangganan pemberitahuan AMS Window Server 2016 baru AMIs di AWS Region us-west-2, gunakan Topik ini ARN = `arn:aws:sns:us-west-2:287847593866:customer-ams-windows2016`
 - b. Untuk Protokol, pilih Email.
 - c. Untuk Titik Akhir, ketik alamat email yang bisa Anda gunakan untuk menerima notifikasi. Kami merekomendasikan daftar distribusi daripada email individu.
5. Pilih Buat langganan.
6. Saat Anda menerima email konfirmasi dengan baris subjek “Pemberitahuan AWS - Konfirmasi Langganan”, buka email dan pilih Konfirmasi langganan untuk menyelesaikan langganan Anda.

Note

Anda tidak terbatas pada email untuk Protokol. [Untuk informasi tentang protokol lain yang dapat diterima dan cara menggunakannya, lihat berlangganan.](#)

Untuk berhenti berlangganan pemberitahuan AMI baru AMS dengan menggunakan konsol AWS SNS:

1. [Buka konsol Amazon SNS ke Dasbor.](#)
2. Di bilah navigasi, ubah ke Wilayah AWS pilihan Anda. Anda harus menggunakan Wilayah AWS tempat Anda ingin menerima pemberitahuan untuk yang terkait AMIs.
3. Di panel navigasi, pilih Langganan, pilih langganan, lalu pilih Tindakan -> Hapus langganan.
4. Saat diminta konfirmasi, pilih Hapus.

Untuk berlangganan pemberitahuan AMS New AMI menggunakan Deployment | Ingestion | Stack from CloudFormation Template | Create (ct-36cn2avfrj9v):

1. Untuk berlangganan AmazonLinuxSubscription, membuat dan menyimpan file JSON parameter eksekusi; contoh ini menamainya CreateSubscribeAmiParams .json:

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "AmazonLinuxSubscription": {
      "Type": "AWS::SNS::Subscription",
      "Properties": {
        "TopicArn": "arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}",
        "Protocol": "email",
        "Endpoint": "username@yourdomain.com"
      }
    }
  }
}
```

2. Buat dan simpan file JSON parameter RFC dengan konten berikut; contoh ini menamainya CreateSubscribeAmiRfc file.json:

```
{
```

```
"ChangeTypeId": "ct-36cn2avfrrj9v",  
"ChangeTypeVersion": "1.0",  
"Title": "cfn-ingest-subscribe-ami"  
}
```

3. Buat RFC, tentukan CreateSubscribeAmiRfc file dan file: CreateSubscribeAmiParams

```
aws amscm create-rfc --cli-input-json file://CreateSubscribeAmiRfc.json --  
execution-parameters file://CreateSubscribeAmiParams.json
```

Anda menerima ID RFC baru dalam respons dan dapat menggunakannya untuk mengirimkan dan memantau RFC. Sampai Anda mengirimkannya, RFC tetap dalam kondisi pengeditan dan tidak dimulai.

Untuk contoh pembuatan AMIs, lihat [Membuat AMI](#).

Untuk informasi tentang mengonsumsi AMIs secara terprogram, lihat [EC2 stack: creating](#).

Pemberitahuan layanan

AMS mengirimkan permintaan layanan keluar, atau pemberitahuan layanan, saat Anda perlu menindaklanjuti, atau mengetahui, sesuatu yang dapat memengaruhi akun atau sumber daya Anda, termasuk:

- Dampak infrastruktur: AMS mengirimkan pemberitahuan layanan ketika ada layanan AWS yang mendasari yang memengaruhi infrastruktur Anda, dan Anda perlu mengambil tindakan sebelum tanggal tertentu, atau Anda mungkin mengalami pemadaman.
- EC2 Masalah perangkat keras: AMS mengirimkan pemberitahuan layanan untuk masalah EC2 perangkat keras yang mengharuskan Anda me-reboot EC2 instance sebelum tanggal tertentu, atau memberi tahu Anda bahwa AMS akan me-reboot instance untuk Anda. Ini adalah pemberitahuan penting karena reboot dapat menyebabkan pemadaman dan Anda harus merespons dengan tanggal yang dapat diterima, atau membuat RFC dengan ct-09qbhy7kvtxqw, untuk me-reboot instance sendiri. Pemberitahuan layanan seperti ini secara otomatis ditutup dalam lima hari jika Anda tidak merespons.

Pemberitahuan perubahan status RFC

AMS menawarkan pemberitahuan untuk perubahan status RFC melalui email dan CloudWatch Acara:

- Email melalui Konsol AMS: Ada opsi di halaman kedua wizard Buat RFC, di mana Anda dapat menambahkan hingga lima alamat email untuk diberi tahu saat status RFC berubah.
- CloudWatch Acara: Anda dapat mengonfigurasi aturan dan target yang berbeda untuk CloudWatch Acara untuk menerima pemberitahuan untuk setiap perubahan status RFC.

Notifikasi email

Anda dapat menambahkan alamat email untuk menerima perubahan status RFC ke RFC yang Anda buat di konsol AMS, atau dengan menggunakan AMS API/CLI.

Di konsol AMS, gunakan opsi Pemberitahuan email, di halaman kedua wizard Buat RFC:

Di AMS API/CLI, tambahkan baris seperti ini ke bagian parameter RFC RFC Anda (jangan tambahkan baris ke bagian parameter run):

```
--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}\"
```

Perilaku notifikasi bervariasi tergantung jenis penjadwalan RFC:

- Terjadwal RFCs menerima pemberitahuan email pada: Dikirim, Dijadwalkan,, Selesai InProgress, Ditolak, Dibatalkan, Ditolak Otomatis, atau Dibatalkan Otomatis.
- ASAP RFCs menerima pemberitahuan email tentang: Dikirim,, Selesai InProgress, Ditolak, Dibatalkan AutoRejected, atau Dibatalkan Otomatis.

Note

- Pemberitahuan email dikirim dari alamat ini: `no-reply@managedservices.amazonaws.com`.
- Karakter khusus dan URLs judul RFC Anda disunting dalam email yang kami kirim. Ini adalah tindakan pengamanan.

CloudWatch Pemberitahuan acara

AMS menawarkan pemberitahuan push untuk perubahan Status RFC melalui CloudWatch Acara. Untuk mendapatkan notifikasi ini:

1. Buat topik dan langganan tempat pemberitahuan akan dikirim. Anda dapat memberi nama topik apa yang Anda sukai; untuk informasi tentang melakukan hal ini, lihat [SNS Topic and Subscription: Creating](#).
2. Kirim RFC dengan Manajemen | Lainnya | Lainnya | Buat jenis perubahan dan sertakan topik SNS dan langganan dalam permintaan pemberitahuan perubahan status RFC.

Saat Anda mengirimkan permintaan Manajemen | Lainnya | RFC lainnya untuk fitur ini, Anda dapat menentukan perubahan status RFC yang ingin Anda beri tahu dan jenis perubahan apa, dan menyetel filter lainnya. Misalnya, Anda mungkin ingin meminta pemberitahuan hanya jika jenis perubahan Akses Admin adalah EventType = RfcSubmitted dan EventType = RfcUpdated.

Ini adalah templat pemberitahuan CloudWatch acara yang dapat Anda terima (dengan semua nilai yang mungkin):

```
{
  "source ": "aws.managedservices",
  "detail-type": "AMS RFC State Change",
  "detail": {
    "ActionState": "null | AwsActionPending | AwsOperatorAssigned |
CustomerActionPending | NotApplicable | NoActionPending",
    "ActualExecutionTimeRange": {
      "StartTime": "null | Actual Start Time",
      "EndTime": "null | Actual End Time"
    },
    "AutomationStatus": "Automated | Manual",
    "AwsAccountId": "AWS Account ID",
    "AwsApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending
| Rejected | Approved",
    "ChangeTypeId": "Change_Type_ID",
    "ChangeTypeVersion": "Change_Type_Version",
    "CreatedTime": "Created_Time",
    "CustomerApprovalStatus": "null | SubmissionPending | NotRequired |
ApprovalPending | Rejected | Approved",
    "EventType": "RfcActionStateUpdated | RfcApproved | RfcAutoRejected |
RfcCanceled | RfcCompleted | RfcCreated | RfcInProgress | RfcRejected | RfcSubmitted |
RfcUpdated",
```



```

    "LastModifiedTime": "Last_Updated_Time",
    "LastSubmittedTime": "null | Last_Submitted_Time",
    "RequestedExecutionTimeRange": {
        "StartTime": "null | Expected_Start_Time",
        "EndTime": "null | Expected_End_Time"
    },
    "RfcId": "RFC_ID",
    "Status": "Editing | PendingApproval | Scheduled | Rejected | Canceled |
ExecutionLock | InProgress | Success | Failure",
    "Title": "Title"
  }
}

```

Status RFC yang didukung berubah (EventType), seperti yang muncul di notifikasi CloudWatch Peristiwa yang sebenarnya adalah:

- RfcActionStateUpdated (tidak ada opsi konsol AMS): RFC di salah satu status, dijelaskan kemudian, berubah.
- RfcApproved (tidak ada opsi konsol AMS): RFC lulus validasi operator and/or AMS sistem dan telah disetujui untuk diselesaikan.
- RfcAutoRejected (Auto-Rejected): RFC gagal validasi sistem atau operator AMS dan telah ditolak.
- RfcCanceled (Dibatalkan atau Dibatalkan Otomatis): RFC dibatalkan oleh pengirim atau operator AMS.
- RfcCompleted (Selesai): Parameter RFC run telah selesai, termasuk UserData.
- RfcCreated (tidak ada opsi konsol AMS): RFC berhasil dibuat (JSON dan parameter yang dikirimkan valid).
- RfcInProgress (InProgress): Proses RFC masih berlangsung.
- RfcRejected (Ditolak): Sistem gagal RFC atau validasi operator AMS telah ditolak.
- RfcSubmitted (Dikirim): RFC telah diserahkan dan sedang menjalani validasi sistem.
- RfcUpdated (tidak ada opsi konsol AMS): RFC telah diperbarui secara manual oleh operator AMS.

Selain itu, Anda dapat mengirim pemberitahuan CloudWatch Acara (CWE) ke salah satu tujuan yang didukung dan membangun sistem Anda sendiri di atas pemberitahuan otomatis ini:

- EC2 Contoh Amazon
- AWS Lambda fungsi

- Aliran di Amazon Kinesis Data Streams
- Aliran pengiriman di Amazon Data Firehose
- Grup log di Amazon CloudWatch Logs
- Tugas-tugas Amazon ECS
- Run Command Systems Manager
- Otomatisasi Systems Manager
- AWS Batch pekerjaan
- State machine Step Functions
- Pipa di CodePipeline
- CodeBuild proyek
- Templat penilaian Amazon Inspector
- Topik Amazon SNS
- Antrean Amazon SQS
- Target bawaan: panggilan EC2 CreateSnapshot EC2 RebootInstances API, panggilan API, panggilan EC2 StopInstances API, dan panggilan EC2 TerminateInstances API.
- Bus acara default dari akun AWS lain

Note

Kami mengirimkan pemberitahuan CloudWatch Acara untuk perubahan status RFC, dengan upaya terbaik.

Menyiapkan DNS pribadi dan publik

Selama orientasi, AMS menyiapkan layanan DNS pribadi untuk komunikasi antara sumber daya terkelola Anda dan AMS.

Anda dapat menggunakan AMS Route 53 untuk mengelola nama DNS internal untuk sumber daya aplikasi Anda (server web, server aplikasi, database, dan sebagainya) tanpa mengekspos informasi ini ke Internet publik. Ini menambahkan lapisan keamanan tambahan, dan juga memungkinkan Anda untuk gagal dari sumber daya primer ke sumber daya sekunder (sering disebut “flip”) dengan memetakan nama DNS ke alamat IP yang berbeda.

Setelah Anda membuat sumber daya DNS pribadi menggunakan Deployment | Komponen tumpukan lanjutan | DNS (pribadi) | Buat (ct-0c38gftq56zj6) atau Deployment | Komponen tumpukan lanjutan | DNS (publik) | Buat (ct-0vzsr2nyraedl), Anda dapat menggunakan Manajemen | Komponen tumpukan lanjutan | DNS (pribadi) | Pembaruan (ct-1d55pi44ff21u) dan Manajemen | Komponen tumpukan lanjutan | DNS (publik) | Perbarui (ct-1hzofpphabs3i), untuk mengonfigurasi tambahan, atau memperbarui set rekaman yang ada. CTs Untuk akun multi-account landing zone (MALZ), sumber daya DNS yang dibuat di akun aplikasi VPCs dapat dibagikan dengan akun layanan bersama VPC untuk mempertahankan DNS terpusat menggunakan AMS AD.

MALZ

Grafik berikut menggambarkan kemungkinan konfigurasi DNS untuk AMS Zona Pendaratan Multi-Akun. Ini menggambarkan pengaturan DNS hybrid antara AMS dan jaringan pelanggan biasa. Catatan Nama Canonical (CNAME) di server DNS jaringan pelanggan diteruskan ke AMS AD DNS di akun layanan bersama dengan penerusan bersyarat yang memiliki CNAME AMS FQDN diteruskan ke catatan A.

SALZ

Grafik berikut menggambarkan kemungkinan konfigurasi DNS untuk single-account landing zone (SALZ). Ini menunjukkan pengaturan DNS hybrid antara AMS dan jaringan pelanggan biasa. CNAME di server DNS jaringan pelanggan diteruskan ke AMS AD DNS dengan penerusan bersyarat yang memiliki CNAME AMS FQDN diteruskan ke catatan A.

SALZ Route53 DNS

Grafik berikut menggambarkan kemungkinan konfigurasi DNS untuk single-account landing zone (SALZ). Ini menunjukkan pengaturan DNS hybrid antara AMS dan jaringan pelanggan biasa. CNAME di server DNS jaringan pelanggan diteruskan ke AMS AD DNS dengan penerusan bersyarat yang memiliki CNAME AMS FQDN diteruskan ke catatan A. Ini juga memanfaatkan Route53 untuk lalu lintas jaringan keluar sehingga aplikasi apa pun di akun dapat memiliki Resolusi DNS di akun dengan ketersediaan tertinggi.

Route53 mengaktifkan jalur Resolusi:

- Instance yang mencoba menyelesaikan nama AMS MAD -> VPC +2 (AmazonProvidedRoute53/DNS) -> Forwarder Bersyarat dievaluasi -> Aturan Forwarder Bersyarat Route53 MAD cocok -> Route53 Outbound resolver -> DNS AD Terkelola

- Instance yang mencoba menyelesaikan nama pelanggan on-prem -> VPC +2 (AmazonProvidedRoute53/DNS) -> Forwarder Bersyarat dievaluasi -> Aturan Forwarder Bersyarat Route53 On-prem cocok --> Route53 Outbound resolver -> Pelanggan on-prem DNS
- Instance mencoba menyelesaikan nama Internet -> VPC +2 (AmazonProvidedRoute53/DNS) -> Forwarder Bersyarat dievaluasi -> Tidak ada forwarder yang cocok -> Layanan DNS Internet

Untuk informasi selengkapnya, lihat [Menggunakan DNS dengan VPC Anda dan Bekerja dengan Zona Hosting Pribadi](#).

Manajemen lalu lintas jalan keluar AMS

Secara default, rute dengan CIDR tujuan 0.0.0.0/0 untuk subnet pribadi AMS dan aplikasi pelanggan memiliki gateway terjemahan alamat jaringan (NAT) sebagai target. Layanan AMS, TrendMicro dan patching, adalah komponen yang harus memiliki akses keluar ke Internet sehingga AMS dapat menyediakan layanannya, dan TrendMicro dan sistem operasi dapat memperoleh pembaruan.

AMS mendukung pengalihan lalu lintas keluar ke internet melalui perangkat jalan keluar yang dikelola pelanggan selama:

- Ini bertindak sebagai proxy implisit (misalnya, transparan).

and

- Ini memungkinkan dependensi AMS HTTP dan HTTPS (tercantum di bagian ini) untuk memungkinkan penambalan dan pemeliharaan infrastruktur terkelola AMS yang sedang berlangsung.

Beberapa contohnya adalah:

- Gateway transit (TGW) memiliki rute default yang menunjuk ke firewall lokal yang dikelola pelanggan melalui koneksi AWS Direct Connect di akun Jaringan Zona Pendaratan Multi-Akun.
- TGW memiliki rute default yang menunjuk ke titik akhir AWS di VPC keluar Zona Pendaratan Multi-Akun yang memanfaatkan AWS PrivateLink, menunjuk ke proxy yang dikelola pelanggan di akun AWS lain.

- TGW memiliki rute default yang menunjuk ke firewall yang dikelola pelanggan di akun AWS lain, dengan koneksi site-to-site VPN sebagai lampiran ke Multi-Account Landing Zone TGW.

AMS telah mengidentifikasi dependensi HTTP dan HTTPS AMS yang sesuai, dan mengembangkan serta menyempurnakan dependensi ini secara berkelanjutan. Lihat [egressMgmt.zip](#). Seiring dengan file JSON, ZIP berisi README.

Note

- Informasi ini tidak komprehensif - beberapa situs eksternal yang diperlukan tidak tercantum di sini.
- Jangan gunakan daftar ini di bawah daftar penolakan atau strategi pemblokiran.
- Daftar ini dimaksudkan sebagai titik awal untuk set aturan penyaringan jalan keluar, dengan harapan bahwa alat pelaporan akan digunakan untuk menentukan dengan tepat di mana lalu lintas aktual menyimpang dari daftar.

Untuk meminta informasi tentang memfilter lalu lintas jalan keluar, kirim email ke CSDM Anda: ams-csdm@amazon.com.

Menerapkan sumber daya IAM di AMS Advanced

AMS menyebarkan sumber daya IAM di aplikasi multi-akun landing zone (MALZ) dan akun landing zone (SALZ) akun tunggal dengan dua cara:

- Penyediaan IAM Otomatis: Kemampuan ini di AMS memungkinkan Anda mengirimkan jenis perubahan buat, pembaruan, atau hapus untuk peran IAM atau penyediaan kebijakan, tanpa tinjauan operator, dan dengan pemeriksaan validasi IAM dan AMS berjalan secara otomatis.

Kemampuan ini harus diaktifkan secara eksplisit dengan Manajemen | Akun terkelola | Penyediaan IAM Otomatis AMS dengan izin baca-tulis | Mengaktifkan (perlu [ditinjau](#)) [jenis perubahan \(ct-1706xvvk6j9hf\)](#). Untuk mempelajari selengkapnya, lihat [AMS Penyediaan IAM Otomatis](#). Setelah Penyediaan IAM Otomatis AMS diaktifkan, Anda memiliki akses ke Buat, Perbarui, dan Hapus jenis perubahan untuk mengelola sumber daya IAM Anda.

- Tinjau tipe perubahan IAM yang diperlukan: Jenis perubahan ini, Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | [Buat entitas atau kebijakan](#)

[\(diperlukan tinjauan\)](#) (ct-3dpg8mdd9jn1r), memerlukan tinjauan operator AMS, yang terkadang membutuhkan waktu beberapa hari untuk diselesaikan jika klarifikasi diperlukan.

Note

Metode apa pun yang digunakan, peran IAM disediakan ke akun atau akun yang relevan dan, setelah peran tersebut disediakan, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

AMS Penyediaan IAM Otomatis

AWS Managed Services (AMS) mendukung validasi dan penyediaan otomatis untuk sumber daya IAM termasuk peran dan kebijakan yang menggunakan AMS Advanced request for change (RFCs) dan new change types (). CTs Sebelumnya, permintaan ini melalui proses semi-otomatis yang terkadang menghasilkan waktu tunggu yang lama. Sekarang, Anda dapat menggunakan AMS Automated IAM Provisioning untuk menyediakan sumber daya IAM dan mendapatkan hasilnya lebih cepat.

Cara Kerja Penyediaan IAM Otomatis di AMS

Penyediaan IAM Otomatis bergantung pada pemeriksaan run-time otomatis untuk IAM untuk memvalidasi perubahan pada sumber daya IAM. Pemeriksaan otomatis ini, yang dilakukan saat jenis perubahan Buat, Perbarui, atau Hapus dijalankan, mencegah sumber daya IAM yang terlalu permisif atau memiliki pola tidak aman agar tidak diterapkan ke akun Anda. Ini memungkinkan Anda untuk mencocokkan tingkat ketelitian dalam ulasan IAM dengan keahlian tim Anda. Kami menyarankan tim yang baru mengenal layanan cloud dan memerlukan pemeriksaan manual untuk semua perubahan sumber daya IAM menggunakan jenis perubahan yang diperlukan tinjauan yang ada: Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | [Buat entitas atau kebijakan](#) (diperlukan tinjauan), (ct-3dpg8mdd9jn1r). Tim dengan AWS keahlian dan kontrol lingkungan mereka dapat menggunakan Penyediaan IAM Otomatis untuk mempercepat penerapan mereka. Anda dapat menggunakan fitur ini untuk melakukan validasi melalui pemeriksaan run-time otomatis atau untuk melakukan validasi dan penyediaan sumber daya IAM setelah validasi berhasil.

Important

AWS Managed Services telah secara proaktif menerapkan daftar [pemeriksaan runtime](#) validasi yang mencegah pembuatan sumber daya atau kebijakan IAM dengan izin dan

ketentuan tertentu. Untuk deskripsi hak istimewa dan ketentuan ini, lihat [Menerapkan sumber daya IAM di AMS Advanced](#). Jenis perubahan otomatis [ct-1n9gfnog5x7fl](#), [ct-1e0xmuy1diafq](#), dan [ct-17cj84y7632o6](#), [memungkinkan](#) pengguna yang mahir dalam mengelola sumber IAM untuk menyediakan peran dan kebijakan IAM yang memungkinkan tindakan di luar hak [Read Only](#).

Selain itu, Anda dapat menggunakan peran yang dibuat melalui jenis perubahan otomatis [ct-1n9gfnog5x7fl](#), [ct-1e0xmuy1diafq](#), dan [ct-17cj84y7632o6](#) untuk membuat sumber daya baru. Namun, sumber daya tidak dapat mengikuti standar penamaan AMS dan bukan bagian dari tumpukan AMS standar. AMS menyediakan dukungan operasional dan keamanan dari sumber daya spesifik tersebut berdasarkan upaya terbaik.

Meskipun proses manual dan otomatis bertujuan untuk menegakkan standar keamanan kami, penting untuk dicatat bahwa ada perbedaan dalam pemeriksaan di antara keduanya. Penyediaan otomatis memungkinkan fleksibilitas yang lebih besar dalam membuat dan memperbarui peran dan kebijakan; oleh karena itu, mereka tidak sama. Disarankan agar organisasi Anda meninjau dengan cermat [pemeriksaan runtime](#) validasi yang tercantum dalam Panduan Pengguna AMS untuk memastikan bahwa pemeriksaan tersebut selaras dengan harapan dan persyaratan organisasi Anda.

Aliran validasi

Aliran validasi dan penyediaan

Note

Fitur ini cocok untuk tim yang berpengalaman AWS dan sumber daya IAM, dan kami tidak merekomendasikannya untuk tim yang baru. AWS Proses validasi otomatis dirancang untuk menangkap sebagian besar kesalahan dan sangat membantu tim untuk mendapatkan ulasan cepat untuk perubahan IAM, ketika mereka memahami izin yang mereka butuhkan. Untuk menggunakan jenis perubahan baru dengan aman dan efektif, kami menyarankan Anda untuk memiliki pemahaman yang baik tentang AWS IAM, dan [pemeriksaan run-time](#) yang ditawarkan oleh jenis perubahan untuk menentukan apakah mereka cocok untuk tim Anda.

Orientasi ke Penyediaan IAM Otomatis AMS di AMS

[Untuk menggunakan jenis perubahan baru, pertama-tama aktifkan Penyediaan IAM Otomatis AMS dengan mengirimkan RFC menggunakan jenis perubahan berikut: Manajemen | Akun terkelola | Penyediaan IAM Otomatis AMS dengan izin baca-tulis | Aktifkan \(diperlukan tinjauan\) \(ct-1706xvvk6j9hf\)](#). AWS mengharuskan organisasi Anda melalui proses manajemen risiko keamanan pelanggan (CSRM) untuk memastikan bahwa penggunaan jenis perubahan ini selaras dengan kebijakan organisasi Anda. Tim AWS operasi bekerja dengan Anda untuk mendapatkan persetujuan eksplisit dari kontak tim keamanan Anda dalam bentuk penerimaan risiko sebagai bagian dari tinjauan yang diperlukan. Untuk mempelajari lebih lanjut, lihat proses [manajemen risiko pelanggan \(CSRM\) RFC](#).

Setelah RFC mengaktifkan AMS Automated IAM Provisioning dengan fitur izin baca-tulis berhasil, AMS mengaktifkan jenis perubahan Penyediaan IAM Otomatis AMS di akun yang digunakan untuk mengirimkan RFC yang diaktifkan. Untuk mengonfirmasi bahwa akun telah mengaktifkan Penyediaan IAM Otomatis AMS, periksa peran tersebut pada konsol IAM. `AWSTManagedServicesIAMProvisionAdminRole`

Sebagai bagian dari orientasi, AMS menyediakan IAM Access Analyzer di Wilayah AWS akun yang sama untuk memanfaatkan kemampuan pratinjau aksesnya. IAM Access Analyzer membantu mengidentifikasi sumber daya di organisasi dan akun Anda yang dibagikan dengan entitas eksternal, memvalidasi kebijakan IAM terhadap tata bahasa kebijakan dan praktik terbaik, dan menghasilkan kebijakan IAM berdasarkan aktivitas akses di log Anda. AWS CloudTrail Untuk mempelajari lebih lanjut, lihat [Menggunakan AWS Identity and Access Management Access Analyzer](#).

Setelah onboard, akan `AWSTManagedServicesIAMProvisionAdminRole` diterapkan ke akun yang diaktifkan. Jika Anda memilih untuk menggunakan peran ini melalui federasi SAFL, maka Anda harus memasukkan peran tersebut ke solusi federasi Anda.

Sebagai bagian dari orientasi, Anda dapat meminta untuk memperbarui `IAMProvision AdminRole` kebijakan kepercayaan `AWSTManaged Layanan` untuk memberikan peran IAM lain ARN untuk mengambil peran ini menggunakan. `AWS Security Token Service`

Menggunakan Penyediaan IAM Otomatis AMS di AMS

Anda dapat membuat RFCs dengan jenis perubahan Penyediaan IAM Otomatis AMS berikut.

 Note

- Hanya penyediaan peran dan kebijakan yang didukung.

Saat memperbarui peran, CT Pembaruan menggantikan daftar nama sumber daya Amazon (ARNs) kebijakan terkelola yang ada dan dokumen kebijakan “asumsikan peran”, dengan daftar kebijakan terkelola yang disediakan ARNs dan dokumen kebijakan “asumsikan peran”. Dalam pembaruan sebagian; misalnya, menambahkan atau menghapus ARN dalam daftar kebijakan terkelola yang ada ARNs, menambahkan atau menghapus pernyataan kebijakan individual ke dokumen kebijakan “asumsikan peran” tidak diperbolehkan. Demikian pula, saat memperbarui kebijakan, CT Pembaruan menggantikan dokumen kebijakan yang ada dan tidak mengizinkan penambahan atau penghapusan pernyataan kebijakan individual dalam dokumen kebijakan yang ada.

- Ketika opsi “validasi saja” dipilih, pemeriksaan run-time dilakukan tanpa menyediakan entitas atau kebijakan IAM apa pun. Terlepas dari temuan apa pun, status RFC adalah “sukses”. Status “sukses” menunjukkan validasi yang berhasil terhadap entitas atau kebijakan IAM yang disediakan.

- Deployment | Komponen Stack Lanjutan | Identity and Access Management (IAM) | [Buat entitas atau kebijakan \(izin baca-tulis\) \(ct-1n9gfnog5x7fl\)](#): Entitas atau kebijakan IAM baru divalidasi dan disediakan secara otomatis.
- Manajemen | Komponen Stack Lanjutan | Identity and Access Management (IAM) | [Perbarui entitas atau kebijakan \(izin baca-tulis\) \(ct-1e0xmuy1diafq\)](#): Entitas atau kebijakan IAM yang ada diperbarui dan divalidasi secara otomatis.
- Manajemen | Komponen Stack Tingkat Lanjut | Identity and Access Management (IAM) | [Hapus entitas atau kebijakan \(izin baca-tulis\) \(ct-17cj84y7632o6\)](#): Entitas atau kebijakan IAM yang sudah ada yang disediakan menggunakan entitas pembuat otomatis atau jenis perubahan kebijakan dihapus.

Anda hanya dapat memanggil tiga sebelumnya CTs menggunakan peran IAM khusus:.

AWSManagedServicesIAMProvisionAdminRole Peran ini hanya tersedia di akun yang telah di-onboard ke fitur menggunakan Manajemen | Akun terkelola | Izin baca-tulis Penyediaan IAM Otomatis AMS | [Aktifkan](#) (diperlukan peninjauan) (ct-1706xvbk6j9hf).

 Important

Jenis perubahan Buat, Perbarui, dan Hapus selalu terlihat di akun Anda, tetapi tidak diaktifkan secara default. Jika Anda mencoba mengirimkan RFC menggunakan salah satu jenis perubahan ini tanpa terlebih dahulu mengaktifkan fitur Penyediaan IAM Otomatis AMS, maka kesalahan “tidak sah” akan ditampilkan.

Keterbatasan:

- Buat CT memungkinkan Anda membuat peran atau kebijakan IAM dengan izin untuk membuat AWS sumber daya. Namun, AWS sumber daya yang dibuat oleh peran dan kebijakan ini tidak dikelola oleh AMS. Ini adalah praktik terbaik untuk mematuhi kontrol organisasi Anda untuk membatasi pembuatan peran atau kebijakan tersebut.
- CT Pembaruan tidak dapat mengubah peran dan kebijakan IAM yang dibuat dengan CFN Ingest, Mode Perubahan Langsung, Mode Pengembang, atau, dalam beberapa kasus, melalui manual AMS Advanced yang ada atau otomatis. CTs
- CT Hapus tidak dapat menghapus peran atau kebijakan yang ada yang tidak dibuat dengan CT Pembuatan Penyediaan IAM Otomatis AMS.
- Penyediaan IAM Otomatis AMS dengan fitur izin baca-tulis tidak didukung dalam peran Mode Perubahan Langsung. Ini berarti Anda tidak dapat menyediakan atau memperbarui peran dan kebijakan IAM dengan izin baca-tulis menggunakan peran ini.
- Penyediaan IAM Otomatis AMS dengan izin baca-tulis Buat, Perbarui, dan Hapus jenis perubahan tidak kompatibel dengan Konektor. ServiceNow

Pemeriksaan runtime untuk Penyediaan IAM Otomatis AMS di AMS

Penyediaan IAM Otomatis memanfaatkan pemeriksaan dari AWS Identity and Access Management Access Analyzer, dan melakukan pemeriksaan dan validasi tambahan terhadap kebijakan batas AMS. AMS mendefinisikan pemeriksaan dan validasi tambahan berdasarkan praktik terbaik IAM, pengalaman mengoperasikan beban kerja pelanggan di cloud, dan pengalaman evaluasi manual AMS IAM kolektif.

Anda dapat melihat temuan pemeriksaan waktu proses kebijakan dalam output request for change (RFC). Temuan termasuk pengidentifikasi sumber daya, lokasi dalam and/or kebijakan peran yang menghasilkan temuan, dan pesan yang menguraikan pemeriksaan bahwa entitas atau sumber daya

IAM gagal lulus. Temuan ini membantu Anda membuat kebijakan yang fungsional dan sesuai dengan praktik terbaik keamanan.

 Note

Penyediaan IAM Otomatis mencoba untuk spesifik tentang lokasi dalam entitas atau definisi kebijakan yang gagal lulus pemeriksaan. Bergantung pada jenisnya, lokasi mungkin menyertakan nama sumber daya atau ARN, atau indeks dalam array. Misalnya, pernyataan untuk membantu Anda menyesuaikan entitas atau kebijakan untuk hasil yang sukses.

Untuk pengalaman Penyediaan IAM Otomatis AMS yang lancar, adalah praktik terbaik untuk menggunakan opsi “validasi saja” untuk menjalankan pemeriksaan validasi hingga tidak ada temuan dari pemeriksaan validasi yang dilaporkan dalam output RFC. Saat pemeriksaan validasi melaporkan tidak ada temuan, pilih Buat salinan dari Konsol AMS untuk membuat salinan RFC yang ada dengan cepat. Saat Anda siap untuk menyediakan, di bagian Parameter, alihkan nilai Validasi saja dari Ya ke Tidak, lalu lanjutkan.

Ini adalah pemeriksaan run-time yang dilakukan oleh Penyediaan IAM Otomatis AMS untuk memastikan bahwa sumber daya IAM Anda aman:

 Note

Untuk menyediakan kebijakan IAM yang berisi tindakan yang ditolak oleh jenis perubahan otomatis ini, Anda harus mengikuti proses manajemen risiko keamanan pelanggan (CSRM) RFC. Gunakan jenis perubahan berikut: Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat entitas atau kebijakan (diperlukan tinjauan) (ct-3dpg8mdd9jn1r).

- Pemeriksaan dan validasi kebijakan IAM Access Analyzer: Lihat juga referensi pemeriksaan kebijakan Access Analyzer dan validasi [kebijakan IAM Access Analyzer](#).
- Pemeriksaan kebijakan batas izin AMS: Tindakan pada serangkaian layanan yang ditolak secara default. Untuk informasi selengkapnya, lihat [Pemeriksaan batas izin Penyediaan IAM Otomatis](#).
- Pemeriksaan kebijakan batas izin yang ditentukan pelanggan: Tindakan terbatas tambahan pada serangkaian layanan yang ditolak. Untuk informasi selengkapnya, lihat [Pemeriksaan batas izin Penyediaan IAM Otomatis](#).

- Pemeriksaan kustom yang ditentukan AMS: Pemeriksaan yang mengidentifikasi berbagai kebijakan atau pola akses yang tidak aman dan terlalu permisif dalam entitas atau kebijakan IAM yang diminta, dan menolak permintaan jika ditemukan. Untuk selengkapnya, lihat [Elemen kebijakan AWS JSON: Principal](#).

Temuan	Deskripsi
Peran tersebut dapat diakses dari akun eksternal yang berada di luar zona kepercayaan Anda.	Temuan ini mengacu pada prinsip yang tercantum dalam kebijakan kepercayaan peran yang berada di luar zona kepercayaan Anda. Zona kepercayaan didefinisikan sebagai akun tempat peran dibuat atau AWS organisasi tempat akun tersebut berada. Entitas yang bukan milik akun atau AWS Organisasi yang sama adalah entitas eksternal. Untuk menyelesaikan temuan ini, tinjau ID akun di prinsipal ARNs dan pastikan bahwa ID tersebut milik Anda dan merupakan akun bawaan AMS.
Peran tersebut dapat diakses oleh entitas eksternal yang dimiliki oleh akun <i>External_Account_ID</i> yang tidak dimiliki oleh akun pemilik pelanggan AMS. <i>Account_ID</i>	Temuan ini dihasilkan jika kebijakan kepercayaan peran menyertakan ARN utama yang memiliki ID akun yang tidak dimiliki oleh Anda dan akun bawaan AMS. Untuk mengatasi temuan ini, hapus prinsipal tersebut dari kebijakan kepercayaan peran.
ID pengguna kanonik bukan prinsip yang didukung dalam kebijakan kepercayaan IAM.	Prinsipal kanonik tidak IDs didukung dalam kebijakan kepercayaan IAM. Untuk menyelesaikan temuan, hapus prinsipal tersebut dari kebijakan kepercayaan peran.
Peran tersebut dapat diakses oleh identitas web eksternal yang berada di luar zona kepercayaan Anda.	Temuan ini dihasilkan jika kebijakan kepercayaan peran memungkinkan penyedia identitas Web eksternal (iDP) selain SAMP iDP. Untuk mengatasi temuan ini, tinjau kebijakan kepercayaan peran dan hapus pernyataan

Temuan	Deskripsi
Peran tersebut dapat diakses melalui federasi SAMP; namun, penyedia identitas SAMP (IDP) yang disediakan tidak ada.	yang memungkinkan sts:AssumeRoleWithWebIdentity operasi. Temuan ini dihasilkan jika kebijakan kepercayaan peran berisi SAMP IDP yang tidak ada di akun Anda. Untuk menyelesaikannya, pastikan Anda semua IDP SAMP yang terdaftar ada di akun Anda.
Kebijakan berisi tindakan istimewa yang setara dengan administrator atau akses pengguna daya. Pertimbangkan untuk mengurangi ruang lingkup izin ke layanan, tindakan, atau sumber daya tertentu. Jika elemen kebijakan lanjutan seperti NotAction atau NotResource digunakan, pastikan bahwa mereka tidak memberikan akses lebih dari yang Anda inginkan, terutama dalam pernyataan Izinkan.	Ini adalah praktik keamanan terbaik AWS Identity and Access Management untuk hanya memberikan izin yang diperlukan untuk melakukan tugas saat Anda menetapkan izin dengan kebijakan IAM. Lakukan ini dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak istimewa paling sedikit. Temuan ini dihasilkan ketika otomatisasi mendeteksi kebijakan memberikan izin luas dan tidak mematuhi prinsip hak istimewa yang paling rendah. Untuk menyelesaikan temuan, tinjau dan kurangi izin.
Pernyataan berisi tindakan istimewa untuk <i>Service_Name</i>. Pertimbangkan untuk mengecualikan tindakan ini dengan pernyataan penolakan. Lihat referensi kebijakan batas dalam dokumentasi AMS untuk daftar tindakan istimewa.	AMS mengidentifikasi tindakan tertentu untuk layanan tertentu sebagai berisiko dan memerlukan peninjauan dan penerimaan risiko lebih lanjut oleh tim keamanan pelanggan. Temuan ini dihasilkan ketika otomatisasi mendeteksi kebijakan yang diberikan yang memberikan izin tersebut. Untuk mengatasi temuan ini, tolak tindakan ini dalam kebijakan Anda. Untuk daftar tindakan, lihat kebijakan batas AMS. Untuk detail tentang kebijakan batas AMS, lihat. Pemeriksaan batas izin Penyediaan IAM Otomatis AMS

Temuan	Deskripsi
Pernyataan memberikan akses ke RFC Change Types yang memiliki hak istimewa: ct-1n9gfnog5x7fl, ct-1e0xmuy1diafq, dan ct-17cj84y7632o6 untuk layanan. <i>Service_Name</i> Pertimbangkan untuk mencakup izin untuk jenis perubahan tertentu atau mengecualikan jenis perubahan ini dengan pernyataan penolakan.	Temuan ini dihasilkan jika kebijakan memberika n izin untuk melakukan tindakan terkait RFC menggunakan jenis perubahan Penyediaa n IAM Otomatis (). CTs CTs Ini tunduk pada penerimaan risiko dan hanya boleh digunakan melalui peran onboard. Jadi, Anda tidak bisa memberikan izin untuk ini CTs. Untuk mengatasi temuan ini, tolak tindakan RFC menggunakan ini CTs.
Pernyataan berisi tindakan istimewa yang tidak mencakup sumber daya Anda untuk layanan. <i>Service_Name</i> Pertimbangkan untuk melingkupi tindakan ke sumber daya tertentu atau mengecualikan sumber daya dengan awalan namespace AMS. Jika wildcard digunakan, pastikan mereka membatasi ruang lingkup sumber daya Anda.	Temuan ini dihasilkan jika kebijakan memberika n tindakan istimewa yang tidak mencakup sumber daya Anda dari layanan yang diberikan . Kartu liar sering membuat kebijakan yang terlalu permisif yang membawa serangkaian sumber daya atau tindakan yang luas ke dalam ruang lingkup izin. Untuk mengatasi temuan ini, kurangi cakupan izin ke sumber daya yang Anda miliki atau kecualikan sumber daya yang ada di namespace AMS. Untuk daftar awalan namespace AMS, lihat kebijakan batas dalam dokumentasi AMS. Perhatikan bahwa tidak semua awalan berlaku untuk semua layanan. Untuk detail tentang kebijakan batas AMS, lihat. Pemeriksaan batas izin Penyediaan IAM Otomatis AMS
Id akun atau Nama Sumber Daya Amazon (ARN) tidak valid.	Temuan ini dihasilkan jika ada ARN atau ID akun yang ditentukan dalam kebijakan atau kebijakan kepercayaan peran tidak valid. Untuk meninjau sumber daya ARN yang valid untuk layanan, lihat Referensi Otorisasi Layanan. Pastikan bahwa ID akun adalah nomor 12 digit dan akun tersebut aktif. AWS

Temuan	Deskripsi
Penggunaan wildcard (*) untuk id akun di ARN dibatasi..	Temuan ini dihasilkan jika kartu liar (*) ditentukan di bidang ID akun ARN. Kartu liar di bidang ID akun cocok dengan akun apa pun dan berpotensi memberikan izin yang tidak diinginkan ke sumber daya. Untuk mengatasi ini, ganti kartu liar dengan ID akun tertentu.
Akun sumber daya tertentu yang tidak dimiliki oleh akun <i>Account_ID</i> pemilik pelanggan AMS yang sama.	Temuan ini dihasilkan jika ID akun yang ditentukan dalam ARN sumber daya bukan milik Anda dan tidak dikelola oleh AMS. Untuk mengatasi hal ini, pastikan bahwa semua sumber daya (sebagaimana ditentukan oleh ARN mereka dalam kebijakan) milik akun Anda yang dikelola oleh AMS.
Nama peran ada di namespace terbatas AMS.	Temuan ini dihasilkan jika Anda mencoba membuat peran dengan nama yang dimulai dengan awalan cadangan AMS. Untuk mengatasi hal ini, gunakan nama untuk peran yang khusus untuk kasus penggunaan Anda. Untuk daftar awalan cadangan AMS, lihat awalan cadangan AMS
Nama kebijakan ada di namespace terbatas AMS.	Temuan ini dihasilkan jika Anda mencoba membuat kebijakan dengan nama yang dimulai dengan awalan cadangan AMS. Untuk mengatasi hal ini, gunakan nama untuk kebijakan yang khusus untuk kasus penggunaan Anda. Untuk daftar awalan cadangan AMS, lihat awalan cadangan AMS .

Temuan	Deskripsi
ID sumber daya di ARN berada di namespace terbatas AMS.	Temuan ini dihasilkan jika Anda mencoba membuat kebijakan yang memberikan izin ke sumber daya bernama yang ada di namespace AMS. Untuk mengatasinya, pastikan Anda mencakup izin ke sumber daya Anda atau menolak izin ke sumber daya yang ada di namespace AMS. Untuk informasi selengkapnya tentang ruang nama AMS, lihat ruang nama yang dibatasi AMS .
Kasus variabel kebijakan tidak valid. Perbarui variabel ke <i>Variable_Names</i> .	Temuan ini dihasilkan jika mencoba membuat kebijakan yang berisi variabel kebijakan global IAM dalam kasus yang salah. Untuk mengatasi hal ini, gunakan kasus yang benar untuk variabel global dalam kebijakan Anda. Untuk daftar variabel global, lihat kunci konteks kondisi AWS global . Untuk informasi selengkapnya tentang variabel kebijakan, lihat elemen kebijakan IAM: Variabel dan tag
Pernyataan berisi tindakan istimewa yang tidak dicakup ke kunci KMS Anda. Pertimbangkan untuk mencantumkan izin ini ke kunci tertentu atau mengecualikan kunci yang dimiliki AMS.	Temuan ini dihasilkan jika kebijakan berisi izin yang tidak dicakup ke kunci KMS tertentu yang Anda miliki. Untuk mengatasinya, lingkup izin ke kunci tertentu atau kecualikan kunci yang dimiliki AMS. Kunci yang dimiliki AMS memiliki set alias tertentu. Untuk daftar alias kunci yang dimiliki AMS, lihat Pemeriksaan batas izin Penyediaan IAM Otomatis AMS .

Temuan	Deskripsi
Pernyataan berisi tindakan istimewa yang tidak dicakup ke alias kunci KMS Anda. Pertimbangkan untuk mencantumkan izin ini ke kunci atau alias Anda, atau kecualikan alias kunci milik AMS.	Temuan ini dihasilkan jika kebijakan berisi izin yang tidak tercakup ke alias kunci KMS tertentu yang Anda miliki. Untuk mengatasinya, lingkup izin ke kunci tertentu atau kecualikan kunci yang dimiliki AMS. Kunci yang dimiliki AMS memiliki set alias tertentu. Untuk daftar alias kunci yang dimiliki AMS, lihat Pemeriksaan batas izin Penyediaan IAM Otomatis AMS.
Pernyataan berisi tindakan istimewa yang tidak tercakup secara memadai ke kunci KMS Anda menggunakan <code>kms:ResourceAliasesCondition</code>. Pertimbangkan untuk menggunakan nama alias tertentu bersama dengan operator set yang sesuai untuk kunci kondisi. Jika wildcard digunakan dalam nama alias pastikan mereka membatasi ruang lingkup ke set terbatas kunci KMS Anda.	Temuan ini dihasilkan jika Anda melingkupi izin ke kunci KMS Anda menggunakan kondisi dan tidak menggunakan <code>kms:ResourceAliases</code> untuk menutupi alias untuk kunci KMS Anda. Atau, jika kunci <code>kms:ResourceAliases</code> kondisi memiliki nilai yang juga menyertakan alias kunci KMS milik AMS. Untuk mengatasinya, perbarui kondisi untuk mengurangi izin hanya ke alias kunci KMS Anda atau kecualikan alias untuk kunci KMS milik AMS. Untuk daftar alias kunci yang dimiliki AMS, lihat Pemeriksaan batas izin Penyediaan IAM Otomatis AMS.
Peran harus memiliki <code>customer_deny_policy</code> terlampir. Sertakan kebijakan ARN dalam daftar kebijakan yang dikelola. ARNs	Temuan ini dihasilkan jika peran yang Anda buat tidak <code>customer_deny_policy</code> melekat padanya. Untuk mengatasi hal ini, sertakan <code>customer_deny_policy</code> dalam ARNs daftar kebijakan terkelola.

Temuan	Deskripsi
Kebijakan AWS terkelola terlalu permisif atau memberikan izin yang dibatasi oleh kebijakan batas AMS.	Temuan ini dihasilkan jika ManagedPolicyArns nilai untuk peran berisi kebijakan terkelola AMS yang menyediakan akses penuh atau tingkat administrator ke layanan yang relevan. Untuk mengatasi hal ini, tinjau penggunaan kebijakan AWS terkelola dan gunakan kebijakan yang memberikan izin ruang lingkup atau tentukan kebijakan Anda sendiri yang mengikuti prinsip hak istimewa paling sedikit.
Kebijakan terkelola pelanggan berada di namespace AMS terbatas.	Temuan ini dihasilkan jika ada kebijakan yang dikelola pelanggan dengan nama yang diawali di AWS namespace dilampirkan ke peran. Untuk mengatasinya, hapus kebijakan dari ManagedPolicyArns daftar peran tersebut.
Customer_deny_policy tidak dapat dilepaskan dari peran. Sertakan kebijakan ARN dalam daftar kebijakan yang dikelola. ARNs	Temuan ini dihasilkan jika terlepas dari peran selama pembaruan. customer_deny_policy Untuk mengatasi ini, tambahkan customer_deny_policy ke ManagedPolicyArns bidang peran dan coba lagi.
Kebijakan yang dikelola pelanggan disediakan di luar layanan AMS Change Management atau tanpa validasi sebelumnya.	Temuan ini dihasilkan jika satu atau lebih kebijakan yang dikelola pelanggan ARNs yang ada dilampirkan pada suatu peran dan kebijakan tidak disediakan melalui layanan AMS Change Management (melalui RFC). Misalnya, Mode Pengembang atau Mode Perubahan Langsung memungkinkan pelanggan untuk menyediakan kebijakan IAM tanpa RFC. Untuk mengatasi hal ini, hapus kebijakan terkelola pelanggan ARNs dari ManagedPolicyArns daftar peran tersebut.

Temuan	Deskripsi
Jumlah kebijakan terkelola yang diberikan ARNs melebihi kebijakan terlampir per kuota peran.	Temuan ini dihasilkan jika jumlah total kebijakan terkelola yang melekat pada peran melebihi kuota kebijakan per peran. Untuk informasi selengkapnya tentang kuota IAM, lihat kuota IAM dan AWS STS, persyaratan nama , dan batas karakter. Gunakan informasi ini untuk mengurangi jumlah kebijakan yang Anda lampirkan pada peran tersebut.
Ukuran kebijakan kepercayaan ({trust_policy}) melebihi kuota ukuran kebijakan peran dari {size}.	Temuan ini dihasilkan jika ukuran dokumen kebijakan peran asumsi melebihi kuota ukuran kebijakan. Untuk informasi selengkapnya tentang kuota IAM, lihat kuota IAM dan AWS STS, persyaratan nama , dan batas karakter.
Pernyataan berisi semua tindakan mutatif untuk Amazon S3. Pertimbangkan untuk melingkupi izin ini hanya untuk tindakan yang diperlukan. Jika kartu liar digunakan, pastikan mereka mencakup serangkaian tindakan mutatif yang terbatas.	Temuan ini dihasilkan jika kebijakan yang diberikan memberikan semua izin mutatif Amazon Simple Storage Service terlepas dari satu atau beberapa sumber daya. Untuk mengatasinya, sertakan hanya tindakan mutatif Amazon S3 yang diperlukan terhadap bucket Anda.
Pernyataan berisi tindakan istimewa yang tidak diizinkan terhadap bucket apa pun di Amazon S3. Pertimbangkan untuk menambahkan pernyataan yang menyangkal tindakan ini.	Temuan ini dihasilkan jika kebijakan memberikan tindakan istimewa pada ember apa pun. Untuk daftar tindakan istimewa, lihat Pemeriksaan batas izin Penyediaan IAM Otomatis AMS . Untuk menyelesaikan temuan ini, hapus, atau tolak tindakan ini dalam kebijakan Anda.

Temuan	Deskripsi
Pernyataan berisi tindakan istimewa yang tidak dicakup ke bucket Anda di Amazon S3. Pertimbangkan untuk menyertakan bucket Anda atau mengecualikan bucket dengan awalan namespace AMS. Jika kartu liar digunakan, pastikan kartu tersebut cocok dengan ember di ruang nama Anda.	Temuan ini dihasilkan jika kebijakan memberikan tindakan Amazon S3 yang tidak tercakup ke bucket Anda saja. Ini sering terjadi jika kartu liar digunakan saat menentukan sumber daya bucket. Untuk mengatasinya, tentukan nama bucket atau ARNs yang Anda miliki atau kecualikan bucket yang memiliki awalan namespace AMS.
Pernyataan berisi tindakan istimewa yang tidak dicakup ke bucket Anda di Amazon S3. Pertimbangkan untuk menghindari penggunaan kartu liar (*) yang mencakup semua ember di akun.	Temuan ini dihasilkan jika kebijakan memberikan tindakan Amazon S3 yang tidak tercakup dalam bucket Anda. Ini sering terjadi jika kartu liar digunakan saat menentukan sumber daya bucket. Untuk mengatasinya, tentukan nama bucket atau ARNs yang Anda miliki atau kecualikan bucket yang memiliki awalan namespace AMS.
Pernyataan berisi wildcard sumber daya yang dicakup ke semua bucket Amazon S3, termasuk bucket dan bucket yang tidak ada yang tidak Anda miliki. Pertimbangkan untuk melingkupi izin menggunakan kunci kondisi dan <code>s3:ResourceAccount</code> kondisi.	Temuan ini dihasilkan jika kebijakan memberikan izin ke ember yang ditentukan menggunakan kartu liar. Penggunaan kartu liar sering kali membawa ember yang tidak ada atau non-pemilik dalam ruang lingkup. Untuk mengatasi hal ini, gunakan kondisi dan kunci <code>aws:ResourceAccount</code> kondisi untuk cakupan izin ke bucket dalam akun saat ini saja. Untuk detail selengkapnya, lihat Batasi akses ke bucket Amazon S3 yang dimiliki oleh akun tertentu. AWS

Temuan	Deskripsi
Pernyataan berisi elemen <code>NotResource</code> kebijakan, yang dapat dicakup ke sejumlah besar ember, termasuk ember dan ember yang tidak ada yang tidak Anda miliki. Pertimbangkan untuk melingkupi izin menggunakan kunci kondisi dan <code>s3:ResourceAccount</code> kondisi.	Temuan ini dihasilkan jika kebijakan menggunakan elemen <code>NotResources</code> kebijakan untuk menentukan sumber daya bucket. Penggunaan <code>NotResource</code> elemen mungkin mencakup sejumlah besar ember, termasuk ember yang tidak ada atau non-pemilik. Untuk mengatasi hal ini, gunakan kondisi dan kunci <code>aws:ResourceAccount</code> kondisi untuk cakupan izin ke bucket hanya dalam akun saat ini.
Pernyataan berisi tindakan Amazon S3 ke bucket <code>Bucket_Name</code> yang tidak ada, tidak dimiliki oleh akun <code>Account_ID</code>, atau nama berisi kartu liar yang mungkin dicakup ke sejumlah besar ember, termasuk ember dan ember yang tidak ada yang tidak Anda miliki. Pertimbangkan untuk melingkupi izin menggunakan kondisi dan kunci kondisi <code>s3:ResourceAccount</code>	Temuan ini dihasilkan jika kebijakan memberikan izin ke ember yang tidak ada, tidak dimiliki oleh Anda, atau memiliki kartu liar dalam nama ember yang mencakup sejumlah besar ember dan akses tidak dicakup ke akun saat ini saja. Untuk mengatasi hal ini, gunakan kondisi dan kunci <code>aws:ResourceAccount</code> kondisi untuk cakupan izin ke bucket dalam akun saat ini saja.
Pernyataan berisi tindakan Amazon S3 ke bucket <code>Bucket_Name</code> yang tidak ada, tidak dimiliki oleh akun <code>Account_ID</code>, atau namanya berisi kartu liar yang mungkin dicakup ke sejumlah besar ember, termasuk ember dan ember yang tidak ada yang tidak Anda miliki. Akses tidak dibatasi menggunakan <code>s3:ResourceAccount</code> atau akun sumber daya tertentu dalam kondisi bukan milik Anda.	Temuan ini dihasilkan jika kebijakan memberikan izin ke ember yang tidak ada, tidak dimiliki oleh Anda, atau memiliki kartu liar dalam nama ember yang mencakup sejumlah besar ember dan akses hanya dicakup ke akun tertentu. Namun, akun yang ditentukan dalam kunci <code>aws:ResourceAccount</code> kondisi bukan milik Anda dan dikelola oleh AMS. Untuk mengatasinya, perbarui kunci <code>aws:ResourceAccount</code> kondisi dan atur ID akun yang sesuai yang Anda miliki dan dikelola oleh AMS.

Temuan	Deskripsi
Pernyataan berisi tindakan istimewa yang tidak tercakup pada instans Anda untuk Amazon. EC2 Pertimbangkan untuk melingkupi tindakan ke instance tertentu ARNs atau mengecualikan instance yang memiliki kunci tag Nama dengan nilai di awalan namespace AMS. Jika kartu liar digunakan, pastikan mereka cocok dengan ruang nama yang Anda miliki.	Temuan ini dihasilkan jika kebijakan memberika n tindakan istimewa terhadap EC2 instans Amazon yang dimiliki AMS. Instance AMS ditandai dengan kunci tag Nama dengan nilai di namespace AMS. Untuk mengatasi hal ini, tentukan resource Anda atau kecualikan instance AMS dengan kondisi yang memiliki <code>aws:ResourceTag/Name</code> kunci yang mengecualikan nilai dalam namespace AMS menggunakan operator <code>StringNotLike</code>
Pernyataan berisi tindakan istimewa yang tidak dicakup ke sumber daya Anda di AWS Systems Manager penyimpanan parameter. Pertimbangan untuk menentukan ARNs parameter Anda atau mengecualikan parameter dengan awalan namespace AMS. Jika kartu liar digunakan, pastikan mereka hanya mencakup parameter Anda.	Temuan ini dihasilkan jika kebijakan memberika n izin ke parameter yang tidak Anda miliki. Ini biasanya ketika kartu liar digunakan atau parameter dengan awalan namespace AMS terdaftar di bawah sumber daya dalam pernyataan kebijakan. Untuk mengatasi nya, tentukan parameter yang ada di dalam namespace Anda atau kecualikan parameter AMS dengan pernyataan penolakan.
Pernyataan berisi tindakan istimewa terhadap sumber daya di AWS Systems Manager. Pertimbangkan untuk mencantumkan izin untuk hanya membaca tindakan atau tindakan terhadap sumber daya Anda.	Temuan ini dihasilkan jika kebijakan memberika n izin selain penyimpanan parameter atau tindakan hanya-baca terhadap sumber daya Systems Manager. Untuk mengatasi temuan ini, kurangi izin untuk tindakan hanya-baca atau penyimpanan parameter saja.

Temuan	Deskripsi
Pernyataan berisi tindakan istimewa yang tidak dicakup ke {message} <i>Service_Name</i> yang Anda miliki. Pertimbangkan untuk mencakup izin ini ke jenis sumber daya tertentu sebagaimana mestinya atau mengecualikan sumber daya yang dimiliki AMS. Jika kartu liar digunakan, pastikan mereka cocok <i>Resources</i>.	Temuan ini dihasilkan jika kebijakan mengizinkan tindakan istimewa yang tidak diberikan terhadap sumber daya Anda, terutama untuk sumber daya bernama. Untuk mengatasi temuan ini, tinjau daftar sumber daya Anda dan lihat apakah daftar tersebut hanya mencakup sumber daya yang ada di ruang nama Anda. Atau kecualikan sumber daya yang ada di namespace AMS.
Pernyataan berisi tindakan penandaan {<i>Service_Name</i>} yang tidak dicakup ke nilai tertentu untuk kunci tag Nama. Pertimbangkan untuk mencatat tindakan ini dengan menyetel kunci <code>aws:RequestTag/Name</code> kondisi dengan nilai di namespace Anda atau batasi tindakan ini dengan menyetel kunci <code>aws:RequestTag/Name</code> kondisi dengan <code>StringNotLike</code> operator dengan nilai di awalan namespace AMS.	Temuan ini dihasilkan jika kebijakan memberikan izin penandaan untuk layanan tertentu dan izin tidak dicakup ke kunci/nilai tag tertentu. Untuk melihat kunci atau nilai apa yang dapat digunakan dalam tindakan tag, misalnya, saat membuat permintaan untuk melakukan tindakan, gunakan <code>aws:RequestTag/tag</code> key kondisi. Jadi, untuk mengatasinya, gunakan kunci kondisi ini untuk membatasi kunci atau nilai di ruang nama Anda. Atau, tolak kunci Name tag (<code>aws:RequestTag/Name</code>) dengan nilai di namespace AMS.
Kesalahan internal memvalidasi kebijakan kepercayaan peran IAM.	Temuan ini dihasilkan ketika otomatisasi CT mengalami kesalahan dalam melakukan validasi pada kebijakan kepercayaan peran IAM melalui layanan IAM Access Analyzer. Untuk mengatasi ini, kirim ulang RFC. Jika kesalahan berlanjut, hubungi Operasi AMS untuk memecahkan masalah kesalahan.

Temuan	Deskripsi
Kesalahan internal memvalidasi kebijakan terkelola pelanggan.	Temuan ini dihasilkan ketika otomatisasi CT mengalami kesalahan saat melakukan pembatalan pada kebijakan yang dikelola pelanggan melalui layanan IAM Access Analyzer. Untuk mengatasi ini, kirim ulang RFC. Jika kesalahan berlanjut, hubungi Operasi AMS untuk memecahkan masalah kesalahan.
Access analyzer tidak ditemukan di <i>Wilayah AWS</i> . Tidak dapat melakukan pemeriksaan pratinjau akses untuk kebijakan kepercayaan peran.	Temuan ini dihasilkan ketika sumber daya IAM Access Analyzer tidak ditemukan di file. Wilayah AWS Hubungi Operasi AMS untuk memecahkan masalah dan membuat sumber daya IAM Access Analyzer di Wilayah AWS.
Kebijakan kepercayaan yang tidak valid untuk peran <i>Role_Name</i>	Temuan ini dihasilkan bila diberikan peran IAM berisi kebijakan kepercayaan yang tidak valid. Untuk menyelesaikan meninjau kebijakan kepercayaan untuk memverifikasi bahwa itu valid.
IAM Access Analyzer mengalami kesalahan internal. Gagal membuat pratinjau akses untuk peran <i>Role_Name</i>	Temuan ini dihasilkan ketika otomatisasi menemukan kesalahan saat membuat pratinjau akses untuk peran melalui IAM Access Analyzer. Untuk mengatasi ini, kirim ulang RFC. Jika kesalahan berlanjut, hubungi Operasi AMS untuk memecahkan masalah kesalahan.

Temuan	Deskripsi
Gagal membuat pratinjau akses untuk kebijakan kepercayaan peran <i>RoLe_Name</i>	Temuan ini dihasilkan ketika otomatisasi menemukan kesalahan saat membuat pratinjau akses untuk peran melalui IAM Access Analyzer. Untuk mengatasi ini, kirim ulang RFC. Jika kesalahan berlanjut, hubungi Operasi AMS untuk memecahkan masalah kesalahan.
Kesalahan internal memvalidasi SAMP iDP yang terdaftar.	Temuan ini dihasilkan ketika otomatisasi menemukan kesalahan saat memvalidasi SAMP yang disediakan yang IdPs tercantum dalam kebijakan kepercayaan peran. Untuk mengatasi ini, kirim ulang RFC. Jika kesalahan berlanjut, hubungi Operasi AMS untuk memecahkan masalah kesalahan.
Kesalahan internal memvalidasi izin terhadap AWS Key Management Service	Temuan ini dihasilkan saat otomatisasi mengalami kesalahan saat memvalidasi izin AWS KMS utama dalam kebijakan yang disediakan. Untuk mengatasi ini, kirim ulang RFC. Jika kesalahan berlanjut, hubungi Operasi AMS untuk memecahkan masalah kesalahan.
Kesalahan internal memvalidasi kebijakan ARNs terkelola yang terdaftar.	Temuan ini dihasilkan ketika otomatisasi menemukan kesalahan saat memvalidasi kebijakan terkelola yang terdaftar. ARNs Untuk mengatasi ini, kirim ulang RFC. Jika kesalahan berlanjut, hubungi Operasi AMS untuk memecahkan masalah kesalahan.

Temuan	Deskripsi
Kesalahan internal memvalidasi <code>customer_deny_policy</code> lampiran default.	Temuan ini dihasilkan ketika otomatisasi menemukan kesalahan saat memvalidasi bahwa <code>customer_deny_policy</code> itu melekat pada peran. Untuk mengatasi ini, kirim ulang RFC. Jika kesalahan berlanjut, hubungi Operasi AMS untuk memecahkan masalah kesalahan.
Kesalahan internal memvalidasi argumen kebijakan terkelola untuk peran tersebut <i>Role_Name</i>	Temuan ini dihasilkan ketika otomatisasi menemukan kesalahan saat memvalidasi kebijakan terkelola ARNs untuk peran tersebut. Untuk mengatasi ini, kirim ulang RFC. Jika kesalahan berlanjut, hubungi Operasi AMS untuk memecahkan masalah kesalahan.
Kesalahan internal memvalidasi <i>Policy_name</i> terhadap kebijakan batas yang ditentukan pelanggan <code>AWSTransferAccelerationCustomerBoundaryPolicy</code>	Temuan ini dihasilkan ketika otomatisasi mengalami kesalahan saat memvalidasi kebijakan yang membuat daftar penolakan kustom Anda. Untuk mengatasi ini, kirim ulang RFC. Jika kesalahan berlanjut, hubungi Operasi AMS untuk memecahkan masalah kesalahan.
Kebijakan batas yang ditentukan pelanggan <code>AWSTransferAccelerationCustomerBoundaryPolicy</code> ada di akun. Namun, kebijakan tersebut berisi pernyataan <code>allow</code> yang memberikan izin. Kebijakan hanya boleh berisi pernyataan penolakan.	Temuan ini dihasilkan ketika kebijakan yang berisi daftar penolakan kustom Anda menyertakan pernyataan yang memberikan izin. Meskipun daftar penolakan kustom ada di dalam akun Anda sebagai kebijakan yang dikelola IAM, itu tidak dapat digunakan untuk manajemen izin. Kebijakan hanya boleh berisi pernyataan penolakan yang menunjukkan bahwa Anda ingin Penyediaan IAM Otomatis AMS memvalidasi dan menolak tindakan tersebut dalam kebijakan IAM Anda yang dibuat oleh Penyediaan IAM Otomatis AMS.

Temuan	Deskripsi
Pernyataan berisi tindakan istimewa yang ditentukan oleh organisasi Anda untuk <i>Service_Name</i> . Pertimbangkan untuk mengecualikan tindakan ini dengan pernyataan penolakan. Lihat kebijakan yang disebutkan di akun Anda untuk referensi ke daftar tindakan yang dibatasi.	Temuan ini dihasilkan ketika otomatisasi mendeteksi tindakan apa pun dalam kebijakan Anda yang Anda tetapkan dalam daftar penolakan khusus. Untuk menyelesaikan temuan, tinjau pernyataan kebijakan Anda dan hapus tindakan apa pun yang ditentukan dalam daftar penolakan kustom Anda atau tambahkan pernyataan penolakan yang menyangkal tindakan tersebut.
Peran itu harus <i>POLICY_ARN</i> melekat. Sertakan kebijakan ARN dalam daftar kebijakan yang dikelola. ARNs	Temuan ini dihasilkan jika peran yang Anda buat tidak <i>POLICY_ARN</i> melekat padanya. Untuk mengatasi ini, sertakan <i>POLICY_ARN</i> di ManagedPolicyArns bidang peran dan coba lagi.
Tidak <i>POLICY_ARN</i> bisa terlepas dari peran. Sertakan kebijakan ARN dalam daftar kebijakan yang dikelola. ARNs	Temuan ini dihasilkan jika terlepas dari peran selama pembaruan. <i>POLICY_ARN</i> Untuk mengatasi ini, tambahkan <i>POLICY_ARN</i> ke ManagedPolicyArns bidang peran dan coba lagi.

Pemeriksaan batas izin Penyediaan IAM Otomatis AMS

Pemeriksaan batas izin AMS membantu Anda mematuhi kebijakan batas izin default yang disediakan oleh AMS. Kebijakan ini adalah daftar tindakan yang ditolak oleh Penyediaan IAM Otomatis AMS. Kebijakan penyediaan yang berisi tindakan terbatas ini memerlukan penerimaan risiko eksplisit tambahan. Unduh kebijakan di sini: [boundary-policy.zip](#).

Gunakan pemeriksaan kebijakan batas izin yang ditentukan pelanggan untuk menyesuaikan tindakan penolakan di luar default kebijakan batas izin AMS. Saat Anda melakukan onboard ke Penyediaan IAM Otomatis AMS menggunakan jenis perubahan berikut: Manajemen | Akun terkelola | Penyediaan IAM Otomatis AMS dengan izin baca-tulis | [Aktifkan \(diperlukan tinjauan\) \(ct-1706xvvk6j9hf\)](#), Anda dapat menyertakan daftar tindakan penolakan khusus yang menentukan tindakan terbatas tambahan.

Anda dapat memperbarui daftar tindakan tolak menggunakan jenis perubahan: Manajemen | Akun terkelola | Penyediaan IAM otomatis dengan izin baca-tulis | [Perbarui daftar penolakan khusus](#) (ct-2r9xvd3sdsic0). Anda harus menggunakan peran IAM khusus `AWSTrafficManagerIAMProvisionAdminRole` untuk menjalankan jenis perubahan ini.

 Note

- Anda harus memberikan daftar lengkap tindakan penolakan untuk setiap pembaruan. Daftar sebelumnya diganti dengan daftar baru.
- Daftar tindakan penolakan harus berisi hanya tindakan yang harus ditolak. Izinkan tindakan tidak didukung.
- Daftar tindakan penolakan berada di dalam akun sebagai kebijakan terkelola IAM bernama `AWSTrafficManagerIAMProvisionCustomerBoundaryPolicy`. Kebijakan tidak boleh dilampirkan pada peran apa pun.
- Istilah batas izin yang digunakan untuk menunjukkan tindakan yang ditolak dalam Penyediaan IAM Otomatis AMS memiliki arti kontekstual yang berbeda dibandingkan dengan batas izin IAM. Batas izin IAM menetapkan izin maksimum yang dapat diberikan kebijakan saat runtime ke entitas IAM. Untuk informasi selengkapnya tentang batas izin IAM, lihat [Jenis kebijakan di Panduan Pengguna AWS Identity and Access Management](#). Batas izin dalam Penyediaan IAM Otomatis AMS mencegah Anda menyediakan kebijakan IAM yang berisi serangkaian izin tertentu, misalnya, daftar tindakan yang ditolak.

Pemecahan masalah AMS Automated IAM Provisioning findings dan error

Ada tiga cara Anda mungkin mengalami masalah saat menggunakan Penyediaan IAM Otomatis AMS:

- Kesalahan RFC: Ini dapat terjadi karena berbagai alasan; misalnya, input yang salah. Untuk informasi selengkapnya, lihat [Memecahkan masalah kesalahan RFC di AMS](#).
- Kesalahan SSM: Ini dapat terjadi karena berbagai alasan; misalnya, pemformatan yang buruk. Untuk informasi selengkapnya, lihat [Pemecahan Masalah Otomasi Systems Manager](#).
- Temuan pemeriksaan validasi: Ini terjadi ketika salah satu dari banyak pemeriksaan validasi yang menjalankan Penyediaan IAM Otomatis menemukan masalah. Untuk daftar pemeriksaan validasi, dan tindakan yang disarankan untuk diperbaiki, lihat [Pemeriksaan runtime untuk Penyediaan IAM Otomatis AMS di AMS](#).

Menyetel izin di AMS dengan peran dan profil IAM

AMS menggunakan AWS Identity and Access Management (IAM) untuk mengelola pengguna, kredensi keamanan seperti kunci akses, dan izin yang mengontrol AWS sumber daya mana yang dapat diakses pengguna dan aplikasi. AMS menyediakan peran pengguna IAM default dan profil EC2 instans Amazon default (yang menyertakan pernyataan yang memungkinkan akses sumber daya ke peran pengguna IAM default).

Meminta peran pengguna IAM baru atau profil instans

AMS menggunakan peran IAM untuk menetapkan izin pengguna melalui layanan federasi Anda dan profil instans IAM sebagai wadah untuk peran IAM tersebut.

Anda dapat meminta peran IAM khusus dengan Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat entitas atau kebijakan (diperlukan tinjauan) jenis perubahan (ct-3dpd8mdd9jn1r), atau profil instans IAM dengan Manajemen | Aplikasi | Profil instans IAM | Buat Manajemen | Aplikasi | Profil instance IAM | Buat (ulasan diperlukan) jenis perubahan (ct-0ixp4ch2tiu04). Lihat deskripsi masing-masing di bagian ini.

Note

AMS memiliki kebijakan IAM, `customer_deny_policy` yang memblokir ruang nama dan tindakan berbahaya. Kebijakan ini dilampirkan ke semua peran pelanggan AMS secara default dan jarang menjadi masalah bagi pengguna. Pengguna IAM dan permintaan peran Anda tidak menyertakan kebijakan ini, tetapi penyertaan otomatis permintaan `customer_deny_policy` dalam peran IAM membantu AMS menerapkan profil instans IAM baru dengan lebih cepat. Anda dapat meminta pengecualian `customer_deny_policy` kebijakan. Namun, permintaan ini akan melalui tinjauan keamanan yang berat dan kemungkinan akan ditolak karena alasan keamanan.

Batasi izin dengan pernyataan kebijakan peran IAM

AMS menggunakan peran IAM untuk menetapkan izin pengguna melalui layanan federasi Anda.

Zona Pendaratan Akun Tunggal AMS: Lihat [SALZ: Peran Pengguna IAM Default](#).

AMS Zona Pendaratan Multi-Akun: Lihat [MALZ: Peran Pengguna IAM Default](#).

Peran IAM adalah entitas IAM yang mendefinisikan serangkaian izin untuk membuat permintaan layanan. AWS Peran IAM tidak terkait dengan pengguna atau grup tertentu. Sebaliknya, entitas tepercaya mengambil peran, seperti pengguna IAM, aplikasi, atau AWS layanan seperti Amazon EC2. Untuk informasi lebih lanjut, lihat [Peran IAM](#).

Anda dapat mencatat kebijakan yang diinginkan untuk pengguna yang mengasumsikan peran pengguna AMS IAM dengan menggunakan operasi API AWS Security Token Service (STS) [AssumeRole](#) dengan meneruskan kebijakan IAM yang lebih ketat di bawah bidang permintaan. Policy

Contoh pernyataan kebijakan yang dapat Anda gunakan untuk membatasi akses CT disediakan berikutnya.

Dengan menggunakan grup Active Directory (AD) yang dikonfigurasi, dan operasi AWS Security Token Service (STS) API [AssumeRole](#), Anda dapat menetapkan izin untuk pengguna atau grup tertentu, termasuk membatasi akses ke jenis perubahan tertentu (CTs). Anda dapat menggunakan pernyataan kebijakan yang ditunjukkan di bawah ini untuk membatasi akses CT dengan berbagai cara.

Pernyataan tipe perubahan AMS di profil instans IAM default yang memungkinkan akses ke semua panggilan AMS API (amscm dan amsskms) dan semua jenis perubahan:

```
{
  "Sid": "AWSManagedServicesFullAccess",
  "Effect": "Allow",
  "Action": [
    "amscm:*",
    "amsskms:*"
  ],
  "Resource": [
    "*"
  ]
}
```

1. Pernyataan untuk mengizinkan akses dan semua tindakan hanya untuk dua yang ditentukan CTs, di mana “Tindakan” adalah operasi AMS API (salah satu amscm atau amsskms), dan “Sumber Daya” mewakili jenis perubahan IDs dan nomor versi yang ada:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "amscm:*",
      "Resource": [
        "arn:aws:amscm:*:*:changetype/ct-ID1:1.0",
        "arn:aws:amscm:*:*:changetype/ct-ID2:1.0"
      ]
    }
  ]
}
```

2. Pernyataan untuk mengizinkan akses untuk CreateRfc, UpdateRfc, dan hanya SubmitRfc pada dua yang ditentukan CTs:
3. Pernyataan untuk mengizinkan akses untuk CreateRfc, UpdateRfc, dan SubmitRfc pada semua yang tersedia CTs:
4. Pernyataan untuk menolak akses untuk semua tindakan pada CT terbatas dan mengizinkan yang lain CTs:

Batasi izin dengan profil instans Amazon EC2 IAM

Profil instans IAM adalah wadah untuk peran IAM yang dapat Anda gunakan untuk meneruskan informasi peran ke EC2 instans Amazon saat instance dimulai.

Saat ini ada satu profil instans default AWS Managed Services (AMS) `customer-mc-ec2-instance-profile`, yang memberikan izin ke aplikasi yang berjalan pada instance, bukan kepada pengguna yang masuk ke instance. Anda mungkin ingin memodifikasi profil instance default, atau membuat yang baru, jika Anda ingin memberikan akses instance ke sesuatu, tanpa memberikan akses instance lain juga. Anda dapat meminta profil instans IAM baru dengan Management | Applications | IAM instance profile | Create change type (ct-0ixp4ch2tiu04). Saat mengirimkan RFC, Anda dapat membuat profil instans Anda sendiri dan memasukkannya sebagai InstanceProfileDescription, atau Anda bisa memberi tahu AMS (menggunakan bidang yang sama)

tentang perubahan apa yang Anda inginkan. Karena ini adalah CT Manual, AMS harus menyetujui perubahan dan akan menghubungi Anda tentang hal itu.

Jika Anda tidak terbiasa dengan kebijakan Amazon IAM, lihat [Ikhtisar Kebijakan IAM untuk informasi penting](#). Ada juga posting blog yang bagus, [Mengungkap Izin Tingkat Sumber Daya EC2 Amazon](#). Perhatikan bahwa AMS saat ini tidak mendukung kontrol akses berbasis Sumber Daya, tetapi mendukung kontrol tingkat Sumber Daya menggunakan kebijakan peran IAM (untuk penjelasan perbedaannya, lihat [Layanan yang Berfungsi dengan IAM.AWS](#)

AMS Zona Pendaratan Akun Tunggal:

Untuk melihat tabel izin yang diberikan oleh profil instans AMS IAM default, buka Profil Instans [EC2 IAM](#).

Aturan klaim AD FS dan setelan SAMP

ActiveDirectory Aturan klaim Federation Services (AD FS) dan pengaturan SAMP untuk AWS Managed Services (AMS)

Untuk step-by-step petunjuk terperinci tentang cara menginstal dan mengonfigurasi AD FS, lihat [Mengaktifkan Federasi ke AWS Menggunakan Windows Active Directory, ADFS, dan SAMP 2.0](#).

Konfigurasi aturan klaim ADFS

Jika Anda sudah memiliki implementasi ADFS, konfigurasikan berikut:

- Mengandalkan kepercayaan partai
- Aturan klaim

Langkah-langkah aturan kepercayaan dan klaim pihak yang mengandalkan diambil dari [Mengaktifkan Federasi ke AWS Menggunakan Windows Active Directory, AD FS, dan blog SAMP 2.0](#)

- Aturan klaim:
 - Nameid: Konfigurasi per posting blog
 - RoleSessionName: Konfigurasikan sebagai berikut
 - Nama aturan klaim: **RoleSessionName**
 - Toko atribut: **Active Directory**
 - Atribut LDAP: **SAM-Account-Name**

- Jenis Klaim Keluar: **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`**
- Dapatkan Grup AD: Konfigurasi per [posting blog](#)
- Klaim peran: Konfigurasikan sebagai berikut

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^\d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =  
  RegExReplace(c.Value, "AWS-([^\d]{12})-", "arn:aws:iam:$1:saml-provider/  
  customer-readonly-saml,arn:aws:iam:$1:role/"));
```

Konsol web

Anda dapat mengakses konsol Web AWS dengan menggunakan tautan di bawah ini menggantikan **[ADFS-FQDN]** FQDN implementasi ADFS Anda.

`https://[ADFS-FQDN]/.aspx adfs/ls/IdpInitiatedSignOn`

Departemen TI Anda dapat menerapkan tautan di atas ke populasi pengguna melalui Kebijakan Grup.

Akses API dan CLI dengan SAMP

Cara mengkonfigurasi akses API dan CLI dengan SAMP.

Paket python bersumber dari posting blog di bawah ini:

- NTLM: [Cara Menerapkan API Federasi dan Akses CLI Menggunakan SAMP 2.0 dan AD FS](#)
- Formulir: [Cara Menerapkan Solusi Umum untuk API/CLI Akses Federasi Menggunakan SAMP 2.0](#)
- PowerShell: [Cara Mengatur Akses API Federasi ke AWS dengan Menggunakan Windows PowerShell](#)

Konfigurasi skrip

1. Menggunakan Notepad ++, ubah wilayah default ke wilayah yang benar
2. Menggunakan Notepad ++, nonaktifkan verifikasi SSL untuk lingkungan pengujian dan dev

3. Menggunakan Notepad ++, konfigurasi idpentryurl

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?  
loginToRp=urn:amazon:webservices
```

Konfigurasi Windows

Petunjuk di bawah ini adalah untuk paket python. Kredensi yang dihasilkan akan berlaku selama 1 jam.

1. [Unduh dan instal python \(2.7.11\)](#)

2. [Unduh dan instal alat AWS CLI](#)

3. Instal AMS CLI:

- a. Unduh file zip yang dapat didistribusikan AMS yang disediakan oleh manajer pengiriman layanan cloud (CSDM) Anda dan unzip.

Beberapa direktori dan file tersedia.

- b. Buka Managed Cloud Distributables -> CLI -> Windows atau Managed Cloud Distributables -> CLI -> Linux/macOS direktori, tergantung pada sistem operasi Anda, dan:

Untuk Windows, jalankan penginstal yang sesuai (metode ini hanya berfungsi pada sistem Windows 32 atau 64 bit):

- 32 Bit: ManagedCloud API_x86.msi
- 64 Bit: ManagedCloud API_x64.msi

Untuk Mac/Linux, jalankan file bernama: MC_CLI.sh. Anda dapat melakukan ini dengan menjalankan perintah ini: `sh MC_CLI.sh`. Perhatikan bahwa direktori `amscm` dan `amsskms` dan isinya harus berada di direktori yang sama dengan file `MC_CLI.sh`.

- c. Jika kredensi perusahaan Anda digunakan melalui federasi dengan AWS (konfigurasi default AMS), Anda harus menginstal alat manajemen kredensi yang dapat mengakses layanan federasi Anda. Misalnya, Anda dapat menggunakan AWS Security Blog [Cara Menerapkan API Federasi dan Akses CLI Menggunakan SAMP 2.0 dan AD FS](#) untuk bantuan mengonfigurasi alat manajemen kredensi Anda.
- d. Setelah instalasi, jalankan `aws amscm help` dan `aws amsskms help` untuk melihat perintah dan opsi.

4. Unduh skrip SAMP yang diperlukan

Unduh ke c:\aws\scripts

5. [Unduh PIP](#)

Unduh ke c:\aws\downloads

6. Menggunakan PowerShell, instal PIP

```
<pythondir>. \ python.exe c:\aws\downloads\get -pip.py
```

7. Menggunakan PowerShell, instal modul boto

```
<pythondir\ scripts>pip instal boto
```

8. Menggunakan PowerShell, menginstal modul permintaan

```
permintaan<pythondir\ scripts> pemasangan pip
```

9. Menggunakan PowerShell, menginstal modul keamanan permintaan

```
<pythondir\ scripts>permintaan pemasangan pip [keamanan]
```

10. Menggunakan PowerShell, instal modul beautifulsoup

```
<pythondir\ scripts>pip install beautifulsoup4
```

11. Menggunakan PowerShell, buat folder bernama .aws di profil pengguna (%userprofile%\ .aws)

```
mkdir .aws
```

12. Menggunakan PowerShell, buat file kredensi di folder.aws

```
Kredensi Baru-Item -type file —force
```

File kredensial tidak boleh memiliki ekstensi file

Nama file harus semua huruf kecil dan memiliki kredensial nama

13. Buka file kredensial dengan notepad dan tempel di data berikut, tentukan wilayah yang benar

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

14. Menggunakan PowerShell, skrip SAMP dan logon

```
<pythondir>. \ python.exe c:\aws\scripts\samlapi.py
```

Nama Pengguna: [NAMA PENGGUNA] @upn

Pilih peran yang ingin Anda asumsikan

Konfigurasi Linux

Kredensi yang dihasilkan akan berlaku selama 1 jam.

1. Menggunakan WinSCP, transfer skrip SAMP
2. Menggunakan WinSCP, transfer sertifikat Root CA (abaikan untuk pengujian dan dev)
3. Tambahkan ROOT CA ke sertifikat root terpercaya (abaikan untuk pengujian dan dev)

```
$ openssl x509 -inform der -in [certname] .cer -out certificate.pem (abaikan untuk pengujian dan dev)
```

Tambahkan konten certificate.pem ke akhir file/etc/ssl/certs/ca-bundle.crt ((abaikan untuk test dev)

4. Buat folder.aws di rumah/ec2-user 5

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

5. Menggunakan WinSCP, transfer file kredensial ke folder.aws
6. Instal modul boto

```
$ sudo pip instal boto
```

7. Instal modul permintaan

```
Permintaan instal $ sudo pip
```

8. Instal modul beautifulsoup

```
$ sudo pip instal beautifulsoup4
```

9. Salin skrip ke rumah/ec2-user

Tetapkan izin yang diperlukan

Jalankan skrip: `samlapi.py`

Batasi dengan ACL jaringan

Network Access Control List (NACL) adalah lapisan keamanan opsional untuk VPC Anda yang bertindak sebagai firewall untuk mengontrol lalu lintas masuk dan keluar dari satu atau lebih subnet. Anda dapat mengatur jaringan ACLs dengan aturan yang mirip dengan grup keamanan Anda untuk menambahkan lapisan keamanan tambahan ke VPC Anda. Untuk informasi selengkapnya tentang perbedaan antara grup keamanan dan jaringan ACLs, lihat [Perbandingan grup keamanan dan jaringan ACLs](#).

Namun, di AMS Managed Multi-Account Landing Zone, agar AMS dapat mengelola dan memantau infrastruktur secara efektif, penggunaan NACLs terbatas pada cakupan berikut:

- NACLs tidak didukung di akun Inti Zona Pendaratan Multi-Akun, yaitu akun Manajemen, Jaringan, Layanan Bersama, Logging, dan Keamanan.
- NACLs didukung di akun Aplikasi Zona Pendaratan Multi-Akun selama hanya digunakan sebagai daftar “Tolak” dan memiliki “Izinkan Semua” untuk memungkinkan pemantauan AMS dan operasi manajemen.

Dalam lingkungan multi-akun skala besar, Anda juga dapat memanfaatkan fitur seperti firewall jalan keluar terpusat untuk mengontrol lalu lintas keluar dan/atau tabel perutean Transit AWS Gateway di Zona Pendaratan Multi-Akun AMS untuk memisahkan lalu lintas jaringan di antara mereka. VPCs

AMS di Outposts

[AWS Outposts](#) adalah solusi perangkat keras terkelola yang memperluas zona pendaratan terkelola AMS ke pusat data pelanggan. Dengan dukungan AMS AWS Outposts, pelanggan yang mencari keahlian cloud, penghematan biaya, dan platform standar yang ditawarkan oleh AMS, tidak lagi terbatas pada sumber daya hosting di dalamnya. Wilayah AWS Dengan AMS aktif AWS Outposts, pelanggan dengan persyaratan lokal sekarang dapat memodernisasi AWS, sambil menikmati layanan patching, backup, provisioning, manajemen insiden, kontinuitas bisnis, dan pengoptimalan biaya yang ditawarkan oleh AMS.

Setelah AWS Outposts diaktifkan di akun AMS Multi-Account Landing Zone atau Single-Account Landing Zone, Anda dapat mengikuti proses manajemen perubahan AMS yang ada untuk menyediakan dan mengelola AWS sumber daya. Infrastruktur yang di-host AMS dapat dikelola dengan menentukan subnet spesifik Anda AWS Outposts. AWS Outposts siklus hidup dapat dikelola secara langsung di AWS Outposts konsol menggunakan peran layanan penyediaan AWS Outposts mandiri.

Untuk informasi tentang peran tersebut, lihat [AWS Outposts](#).

AWS Outposts instalasi dan manajemen operasional

Orientasi ke AMS pada AWS Outposts proses terdiri dari:

1. Perencanaan Outposts
2. Validasi Pesanan
3. Outposts Onboarding ke AMS
4. Manajemen Siklus Hidup

AWS Outposts perencanaan

Selama AWS Outposts perencanaan, Anda mengidentifikasi AMS pada kasus AWS Outposts penggunaan dan melibatkan pemangku kepentingan utama, termasuk tim akun AMS dan AWS Outposts perwakilan Anda, untuk menyelaraskan strategi kapasitas.

1. Setelah kasus penggunaan yang memerlukan AMS aktif AWS Outposts telah diidentifikasi, libatkan tim akun AMS Anda untuk mendiskusikan perencanaan kapasitas.
2. Setelah persyaratan AWS Outposts kapasitas Anda ditentukan, tim akun AMS Anda melibatkan tim AWS Outposts layanan untuk mendiskusikan rencana AWS Outposts orientasi, peran, dan tanggung jawab. Selama waktu ini, AWS Outposts satu titik kontak (SPOC) diberikan kepada Anda. AWS Outposts SPOC membantu dalam menyelesaikan persyaratan ukuran AWS Outposts .

AWS Outposts validasi pesanan

Selama validasi pesanan, Anda membuat AWS Outposts situs, dan memesan kapasitas yang Anda butuhkan langsung di AWS Outposts konsol atau melalui perwakilan AWS Outposts akun Anda.

Setelah Anda, tim akun AMS, tim diselaraskan, Anda dapat meminta peran layanan yang AWS Outposts disediakan sendiri menggunakan ID tipe perubahan ct-3qe6io8t6jtny, untuk membuat situs dan memesan langsung di konsol. AWS Outposts AWS Outposts AWS Outposts

Atau, Anda dapat bekerja melalui AWS Outposts SPOC untuk membuat Situs Pos Luar dan pesanan. AWS Outposts SPOC Anda tetap memberikan pembaruan status kepada Anda dan tim akun AMS selama validasi situs dan pesanan, dan AWS Outposts penginstalan.

AWS Outposts orientasi ke AMS

Setelah AWS Outposts unit diaktifkan di VPC terkelola AMS, Anda dapat meminta monitor dibuat untuk melacak ketersediaan, kapasitas, pengecualian, dan konektivitas jaringan untuk perangkat keras Outposts Anda. Dengan mengikuti langkah-langkah penerapan pemantauan yang dijelaskan selanjutnya, AWS Outposts perangkat keras Anda dipantau secara aktif oleh AMS.

1. Setelah Anda AWS Outposts diinstal dan diaktifkan, Anda dapat meminta pemantauan AWS Outposts-spesifik dengan mengirimkan template berikut dengan RFC menggunakan Manajemen | Lainnya | Lainnya | Buat (ct-1e1xtak34nx76) jenis perubahan. Operasi AMS memastikan bahwa AWS Outposts subnet dilacak dalam perkakas internal AMS.

- AWS Outposts ID
- Subnet CIDR
- AWS Outposts Alarm yang disarankan:
 - InstanceFamilyCapacityAvailabilityAlert
 - InstanceTypeCapacityAvailabilityAlert
 - EBSVolumeTypeCapacityAvailabilityAlert
 - CapacityExceptionsAlert
 - Connect Langsung ConnectionAlert
- Untuk setiap peringatan di atas, tentukan parameter berikut:
 - Statistik (“Rata-rata” direkomendasikan. Pilihan lain termasuk jumlah, maksimum, minimum, jumlah sampel dan p90)
 - Periode (“5 menit” dianjurkan. Pilihan lain termasuk 10 dan 30 detik, 1, 5, dan 15 menit, 1 dan 6 jam, dan 1 hari)
 - Jenis ambang batas (“Statis” direkomendasikan. “Anomali” juga merupakan pilihan.)
 - Kondisi (“Setiap kali jumlah panggilan lebih besar dari”, “sama dengan”, “kurang dari” juga merupakan opsi.)

- Nilai Kondisi (" 25% "dikonfigurasi secara default. Bilangan bulat positif lainnya diperbolehkan.)
- Topik pemberitahuan (topik operasi AMS ditetapkan secara otomatis. Namun topik lain, atau kustom, juga dapat ditambahkan.)

2. Dukungan Monitoring dan Operasional

- Operasi AMS memantau AWS Outposts metrik untuk pemutusan jaringan atau kegagalan komponen. Operasi AMS menyediakan layanan respons pertama untuk AWS Outposts masalah, dan meningkatkan, jika diperlukan, ke dukungan atau EC2 dukungan Premium.
- Operasi AMS tersedia untuk mengatasi masalah yang terkait dengan AWS Outposts unit Anda.

3. Ketika status EC2 instans atau pemeriksaan status sistem gagal, operasi AMS mengikuti proses yang ada untuk membawa instance kembali online. Jika restart gagal atau AWS Outposts kapasitas tidak mencukupi, maka anggota tim operasi AMS akan memberi tahu Anda secara langsung untuk menentukan langkah selanjutnya.

AWS Outposts manajemen siklus hidup

AWS Outposts Setelah onboard ke akun AMS Anda, Anda akan diberi tahu jika ketersediaan, kapasitas, atau pengecualian jaringan, terjadi. Anda dapat menonaktifkan AWS Outposts langsung melalui AWS Outposts konsol atau AWS Outposts SPOC.

Anda dapat mengelola AWS Outposts langsung di AWS Outposts konsol menggunakan peran AWS Outposts layanan penyedia layanan mandiri atau mode pengembang. Anda juga dapat meminta AWS Outposts melalui CSDM Anda, atau titik kontak AWS Outposts tunggal, (SPOC).

Ketersediaan tinggi AWS Outposts dapat dicapai dengan menerapkan dua atau lebih. AWS Outposts Mengonfigurasi dua atau lebih AWS Outposts memungkinkan opsi multi-availability zone untuk instans Amazon Relational Database Service Anda.

Menyediakan sumber daya terkelola AMS di AWS Outposts

Penyediaan AWS sumber daya yang dihosting di AWS Outposts (misalnya, Amazon, Amazon EMR, EC2 Amazon EKS, Amazon ECS, Amazon EBS, dan Amazon S3) di akun AMS (Zona Pendaratan Akun Tunggal, Zona Pendaratan Multi-Akun, dan Akun Akselerasi) tunduk pada tingkat dukungan AMS yang sama dengan sumber daya di. Wilayah AWS Anda dapat menggunakan manajemen perubahan AMS, layanan penyedia layanan mandiri, atau mode pengembang untuk membuat dan memodifikasi sumber daya yang dibuat. AWS Outposts

Saat ini, semua jenis instans (M5/m5d, C5/C5d, R5/R5d, i3en, G4dn), Amazon Elastic Block Store, Amazon Elastic Container Service, Amazon Elastic Kubernetes Service, Amazon EMR, Amazon Relational Database Service, Application Load Balancers, dan proxy App Mesh Envoy tersedia langsung di DBs AWS Outposts. Sumber daya ini memenuhi syarat untuk dukungan operasi AMS yang sama dengan sumber daya di wilayah yang ada.

Keterbatasan AMS pada AWS Outposts

- Dukungan operasional untuk sumber daya yang AWS Outposts di-host bergantung pada konektivitas jaringan yang konsisten. AWS Outposts pemutusan jaringan mencegah operasi AMS agar tidak dapat memecahkan masalah insiden atau masalah apa pun yang terjadi pada unit yang terputus. AWS Outposts Untuk AMS tentang kontinjensi tingkat AWS Outposts layanan, lihat [Perjanjian Tingkat AWS Layanan \(\) SLAs](#) yang diperbarui.
- Amazon Relational Database Service:
 - Jenis perubahan RDS create (ct-2z60dyvto9g6c), secara default, memungkinkan Multi-AZ dan memerlukan grup subnet DB. Grup subnet DB memerlukan dua subnet dalam dua Availability Zones (AZ) terpisah. Jika Anda hanya memiliki satu AWS Outposts, membuat grup subnet DB adalah masalah karena hanya AWS Outposts ditetapkan ke satu AZ. Untuk menghindari batasan ini, ikuti petunjuk ini:
 1. Minta grup subnet DB melalui RFC dengan Manajemen | Lainnya | CT lainnya, dan tentukan subnet pada AWS Outposts
 2. Buat templat CFN khusus untuk menerapkan RDS AWS Outposts, dan tentukan grup subnet yang dibuat pada langkah sebelumnya. Untuk mempelajari lebih lanjut tentang melakukan hal ini, lihat [Sumber daya khusus](#).
 3. Minta agar AMS menerapkan template CFN yang berisi instans RDS target melalui CT cerap AMS CFN (ct-36cn2avfrrj9v).
 4. Perhatikan bahwa saat ini, RDS for AWS Outposts tidak menyediakan metrik dan log karena keterbatasan Layanan RDS.
 - Workload ingest (WIGs): Linux WIGs hanya berfungsi jika pra- WIGs EC2 instance berada di non-subnet. AWS Outposts Alasannya adalah karena Linux WIGs membuat WIGs node di subnet dari EC2 instance pertama menggunakan m4.large, secara default. Karena AWS Outposts tidak memiliki tipe instance WIGs itu, tidak dapat meluncurkan node pekerjaannya. Solusi untuk ini adalah membuat EC2 instance awal di AWS Outposts non-subnet, kemudian instance target dapat dibuat pada AWS Outposts. Selain itu, saat ini, hanya tipe EC2 instans berbasis Nitro termasuk C5, C5d, M5, M5d, R5, R5d, G4, dan I3en yang didukung. AWS Outposts

- Amazon Elastic Block Store (EBS): Buat EBS Volume CT (ct-16xg8qguovg2w) tidak berfungsi, karena volume dibuat bukan karena kami AWS Outposts tidak memberikan nomor sumber daya Amazon (ARN) AWS sebagai parameter input ke CT. AWS Outposts
- Konektivitas jaringan: Konektivitas jaringan adalah tanggung jawab Anda per AWS Outposts tim.
- Brownfield dan pengambilalihan akun: AWS Outposts diaktifkan di akun non-AMS tidak dapat dialihkan ke AMS, karena sifat AWS Outposts penagihan dan persyaratan dukungan perusahaan.

AMS tentang AWS Outposts kepatuhan

AMS tentang AWS Outposts pengesahan kepatuhan

AWS Outposts pesawat kontrol telah dibuktikan memenuhi syarat HIPAA, kepatuhan PCI dan ISO. Namun, AMS di pesawat AWS Outposts kontrol belum dibuktikan. AWS Outposts Untuk alasan ini, pelanggan didorong untuk mengejar pengesahan kepatuhan AMS pada AWS Outposts lingkungan.

Untuk mengontrol pembuatan sumber daya di unit Outpost, pelanggan didorong untuk memisahkan akses pengembang ke Outpost, untuk mencegah kelebihan akses pengembang di akun terkelola AMS standar.

Beban Kerja Terkelola AMS yang membutuhkan kepatuhan FedRAMP

Yang terpenting, akun manajemen AMS harus terlebih dahulu dinilai untuk kepatuhan terhadap peraturan, karena data bidang kontrol akan mengalir keluar dari akun manajemen AMS AWS Outposts ke akun manajemen.

Jika sertifikasi FedRAMP diperlukan dan struktur akun AMS sesuai, maka Anda disarankan untuk menggunakan vendor pusat data yang sudah memiliki sertifikasi yang diperlukan dan memiliki semua alat tautan layanan (atau sudah mengenkripsi data jalan keluar).

Terakhir, perlindungan data tambahan dapat diberlakukan dengan bekerja sama dengan tim akun Anda untuk menyebarkan SCP yang membatasi data ke AWS Outposts dan mencegah pembuatan sumber daya di wilayah apa pun di akun yang menghosting Outpost.

Dampak pada kepatuhan yang ada untuk akun AMS

Penggunaan akun AWS Outposts tidak perlu diuji ulang untuk kepatuhan selama tidak ada data yang diatur yang dikonsumsi dan akun dipisahkan secara logis. Akun manajemen AMS dapat mengelola akun yang tidak diatur dan diatur selama lintas akun authentication/authorization dan

arus data masuk/keluar dipisahkan di antaranya. VPCs Oleh karena itu, meskipun akun Outpost yang tidak sesuai dan akun aplikasi yang sesuai ada berada di organisasi yang sama (termasuk layanan bersama, jaringan, logging, master, layanan AMS keamanan), akun aplikasi kepatuhan masih mempertahankan kepatuhan karena data dipisahkan secara logis.

AMS pada AWS Outposts FAQs

Kasus penggunaan mana yang memenuhi syarat untuk dukungan AMS? AWS Outposts

AMS on AWS Outposts dapat dimanfaatkan oleh perusahaan yang membutuhkan model operasi cloud yang terbukti memiliki beban kerja yang membutuhkan latensi rendah (misalnya, manajemen robot pabrik dan migrasi mainframe), komputasi tepi (misalnya, workstation jarak jauh dan perampingan data tepi), dan beban transfer data yang besar.

Mengapa saya harus menggunakan fitur ini?

AMS menyediakan pemantauan AWS Outposts perangkat keras dan respons pertama terhadap masalah AWS Outposts perangkat keras apa pun. Selain itu, fitur dukungan berikut untuk semua sumber daya terkelola yang dihosting di AWS Outposts:

- Logging, Monitoring, Guardrails, dan Manajemen Acara
- Manajemen Kontinuitas
- Keamanan dan Manajemen Akses
- Manajemen Patch
- Manajemen Perubahan
- Manajemen Penyediaan Otomatis dan Layanan Mandiri
- Manajemen Insiden dan Masalah
- Pelaporan (Pelaporan untuk AWS Outposts perangkat keras pada awalnya tidak akan didukung dengan AMS aktif AWS Outposts)
- Manajemen Permintaan Layanan
- Mode Pengembang
- Support Perusahaan

Bagaimana cara menggunakan fitur ini?

AWS Outposts Perencanaan: Selama AWS Outposts perencanaan, Anda telah mengidentifikasi AMS pada kasus AWS Outposts penggunaan dan akan melibatkan pemangku kepentingan

utama, termasuk tim akun AMS dan AWS Outposts perwakilan, untuk menyelaraskan strategi kapasitas.

Validasi pesanan: Selama validasi pesanan, Anda membuat AWS Outposts situs, dan memesan kapasitas yang diperlukan langsung di AWS Outposts konsol, atau melalui perwakilan AWS Outposts akun Anda.

AWS Outposts orientasi ke AMS: Setelah AWS Outposts unit diaktifkan di VPC dikelola AMS, Anda dapat meminta agar AWS Outposts onboard ke akun AMS Anda dengan mengirimkan permintaan untuk perubahan (RFC) menggunakan templat di Panduan Pengguna AMS (). [AWS Outposts](#) Operasi AMS kemudian membuat subnet dan monitor untuk Outpost Anda menggunakan input yang disediakan pada RFC.

Manajemen siklus hidup: Setelah dimasukkan AWS Outposts ke akun AMS Anda, Anda akan diberi tahu tentang ketersediaan, kapasitas, atau pengecualian jaringan apa pun. Anda dapat menonaktifkan AWS Outposts langsung melalui AWS Outposts konsol atau titik kontak AWS Outposts tunggal Anda (SPOC).

Apa batasan AMS AWS Outposts?

Kasus penggunaan residensi data (misalnya, undang-undang pelokalan data khusus negara, dll.) belum divalidasi untuk AMS. AWS Outposts

AWS Outposts diaktifkan di akun non-AMS tidak dapat dialihkan ke AMS, karena sifat AWS Outposts penagihan dan persyaratan Dukungan Perusahaan.

AWS Outposts pesawat kontrol telah dibuktikan memenuhi syarat HIPAA, kepatuhan PCI dan ISO. Namun, AMS di pesawat AWS Outposts kontrol belum dibuktikan. AWS Outposts Untuk alasan ini, pelanggan didorong untuk mengejar pengesahan kepatuhan AMS pada AWS Outposts lingkungan.

Dapatkah saya memilih keluar dari fitur ini?

Penyediaan AWS Outposts ke lingkungan AMS Anda adalah opsional. Setelah diterapkan ke akun AMS Anda, AWS Outposts dapat dideprovisioned melalui AWS Outposts konsol kapan saja, jika tidak lagi diperlukan.

Bagaimana AMS akan AWS Outposts ditagih?

Peningkatan AWS Outposts biaya AMS akan diterapkan di tingkat Grup B.

Bagaimana Perjanjian Tingkat Layanan AMS akan berubah untuk mengakomodasi AWS Outposts?

Manajemen insiden akan bergantung pada AWS Outposts ketersediaan. AWS Outposts ketersediaan tergantung pada ketersediaan jaringan pelanggan, yang merupakan tanggung jawab pelanggan. AWS Outposts ketersediaan juga tergantung pada uptime AWS Outposts perangkat keras, yang bergantung pada Perjanjian Tingkat AWS Outposts Layanan.

Lihat juga [AWS Outposts FAQs](#).

Menggunakan tag di AMS

Topik

- [Penandaan otomatis infrastruktur AMS](#)
- [Tag yang direkomendasikan AMS](#)
- [Menandai catatan pembaruan massal](#)

Memberikan tag bisa sangat berharga. Untuk informasi mendalam, baca [Menandai Sumber Daya Amazon EC2](#) Anda.

RFCs yang membuat instance, seperti bucket Amazon S3 atau AWS Elastic Load Balancer (ELB), umumnya menyediakan skema yang memungkinkan Anda menambahkan hingga tujuh tag (pasangan kunci/nilai); Anda dapat menambahkan lebih banyak tag ke bucket S3 Anda dengan mengirimkan Manajemen | Komponen tumpukan lanjutan | Penyimpanan Amazon S3 | Perbarui CT. Amazon EC2, Amazon EFS, Amazon RDS, dan skema multi-tier (HA Two-Tiered dan HA One-Tiered) memungkinkan hingga lima puluh tag. Tag ditentukan di ExecutionParameters bagian skema.

Saat menggunakan konsol AMS, Anda harus mengaktifkan tampilan konfigurasi tambahan untuk menambahkan tag.

Tip

Banyak skema CT memiliki Name bidang Description dan di dekat bagian atas skema. Bidang tersebut digunakan untuk memberi nama komponen tumpukan atau tumpukan, mereka tidak memberi nama sumber daya yang Anda buat. Beberapa skema menawarkan parameter untuk memberi nama sumber daya yang Anda buat, dan beberapa tidak. Misalnya, skema CT untuk EC2 tumpukan Create Amazon tidak menawarkan parameter untuk

menamai EC2 instance Amazon. Untuk melakukannya, Anda harus membuat tag dengan kunci "Nama" dan nilai dari nama yang Anda inginkan. Jika Anda tidak membuat tag seperti itu, EC2 instance Amazon Anda akan ditampilkan di EC2 konsol Amazon tanpa atribut nama.

Apakah ada batasan tag? Ya:

- Tag peka terhadap huruf besar dan kecil.
- Panjang kunci maksimum adalah 128 karakter Unicode.
- Panjang nilai maksimum adalah 256 karakter Unicode.
- Jumlah maksimum tanda per sumber daya adalah 50.
- Prefiks yang dicadangkan adalah `aws:`.
- AWS Nama dan nilai tag yang dihasilkan secara otomatis diberi `aws:` awalan, yang tidak dapat Anda tetapkan. Nama tag yang ditentukan pengguna memiliki prefiks `user:` dalam laporan alokasi biaya.
- Gunakan setiap kunci hanya sekali untuk setiap sumber daya. Jika Anda mencoba menggunakan kunci yang sama dua kali pada sumber daya yang sama, permintaan Anda ditolak.
- Karakter yang diizinkan adalah huruf Unicode, spasi putih, angka, dan karakter khusus berikut: `+ - =. _:/`

Jenis AWS sumber daya apa yang mendukung tag? Lihat [Sekarang Mengatur AWS Sumber Daya Anda dengan Menggunakan hingga 50 Tag per Sumber Daya](#).

Penandaan otomatis infrastruktur AMS

AMS dapat menandai semua sumber daya yang dibuat oleh AMS untuk tujuan manajemen, di akun landing zone (MALZ) multi-akun dan single-account landing zone (SALZ) Anda melalui request for change (RFC) dengan Deployment | Advanced stack components | Tag | Create (review required) change type (ct-0176f0n99vcps). Ini dapat membantu Anda dalam mengidentifikasi sumber daya yang dibuat oleh AMS untuk tujuan manajemen.

AMS dapat secara otomatis mengidentifikasi sumber daya yang dibuat AMS berdasarkan standar penamaan dan memeriksa apakah sumber daya memiliki kunci dan nilai tag berikut - "AppName", "AppId AMSResource", dan "EnvironmentType". Jika kunci tag tidak ada, atau nilainya kosong, kunci tag tersebut dapat dibuat secara otomatis oleh AMS dengan nilai tag "". AMSInfrastructure

Anda dapat menyesuaikan tag yang Anda inginkan pada sumber daya yang dibuat AMS berdasarkan standar penandaan organisasi Anda. Anda dapat menyertakan kunci tag dan nilai tag Anda sendiri saat mengirimkan permintaan ke AMS. Ikuti standar penamaan AWS tag ini: [Menandai Praktik Terbaik](#)

 Note

Untuk akun MALZ, penandaan khusus infrastruktur AMS hanya didukung pada akun Aplikasi. Penandaan khusus pada akun inti saat ini tidak didukung.

Jika nama kunci tag yang Anda berikan di RFC Anda, sudah ada di sumber daya, maka nilai tag akan diganti dengan nilai tag baru yang Anda berikan di RFC.

Total panjang pasangan kunci tag: nilai tidak boleh melebihi 256 karakter.

Sertakan informasi berikut di RFC Anda dengan Deployment | Advanced stack components | Tag | Create (review required) change type (ct-0176f0n99vcps) untuk menandai resource yang dibuat AMS.

1. Daftar akun landing zone multi-akun atau akun landing zone single-account tempat Anda ingin menandai sumber daya buatan AMS untuk tujuan pengelolaan.
2. Diperlukan nama kunci tag dan nilai tag (jika diperlukan). Secara default, AMS dapat menandai dengan nama kunci tag sebagai "EnvironmentType" dan nilai tag sebagai "". AMSInfrastructure [Jika Anda memerlukan nama kunci tag dan nilai tag khusus, ikuti standar penamaan AWS tag: Menandai Praktik Terbaik](#)

Sumber daya ini saat ini didukung oleh penandaan infrastruktur AMS:

```
API Gateway
Amazon CloudFront
Amazon DynamoDB
Amazon EBS
Amazon EC2
Amazon OpenSearch Service
Amazon Quantum Ledger Database (QLDB)
Amazon Redshift
Amazon RDS
Amazon S3 (specific buckets only*)
Amazon Simple Queue Service (SQS)
```

Amazon Simple Notification Service (SNS)

Amazon VPC AWS Certificate Manager AWS CloudFormation AWS CloudTrail AWS CodeBuild
AWS CodePipeline AWS Elastic Beanstalk AWS Lambda AWS Secrets Manager AWS Service
Catalog AWS Systems Manager AWS WAF Regional
Elastic Load Balancing

```
* "arn:aws:s3:::awssms-a*-patch-data-*", "arn:aws:s3::ams-a*-log-management-*", "arn:aws:s3::cf-templates-*", "arn:aws:s3::mc-a*", "arn:aws:s3::ams-aa*-backup-reports-*", "arn:aws:s3::ams-a*- *- ", "arn:aws:s3::ams-a*- *- ", "arn:aws:s3::ams-a*-release-assets-*", "arn:aws:s3::ams-a*-release-assets-*", "arn:aws:s3::ams-a*-release-assets-*", "arn:aws:s3::ams-a*-release-assets-*", "arn:aws:s3::ams-a*-release-assets-*", "arn:aws:s3:: -*", "arn:aws:s3:: *" patch-data-customer-reports patch-data-raw patch-data-reporting sms-cfn-drift-remediation sms-reporting-data-a
```

Tag yang direkomendasikan AMS

AMS merekomendasikan tag berikut pada sumber daya yang didukung. Tag berbintang (*) sangat disarankan.

 Note

Anda dapat menggunakan tag untuk menjadwalkan penambalan. Untuk selengkapnya, lihat [AMS Advanced Patch Orchestrator: model patching berbasis tag](#).

Awalan cadangan AMS

Atribut sumber daya AMS harus sesuai dengan pola tertentu; misalnya, nama profil instans IAM, BackupVault nama, nama tag, dan sebagainya, tidak boleh dimulai dengan awalan cadangan AMS. Awalan yang dicadangkan tersebut adalah:

```
*/aws_reserved/*
ams-*
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
```



```

AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion

```

Tag yang direkomendasikan AMS

Tombol tanda	Nilai yang didukung	Catatan
AppName*	Tidak dibatasi.	Identifikasi aplikasi yang akan berada di, atau memerlukan akses ke, sumber daya. Ini memfasilitasi pelacakan dan komunikasi antara AMS dan Anda.
AppId*		
EnvironmentType *		Membedakan antara pembangunan, pengujian, dan infrastruktur produksi sebagai lingkungan untuk sumber daya.

Tombol tanda	Nilai yang didukung	Catatan
OwnerTeamEmail *	Alamat email daftar distribusi	Identifikasi alamat email daftar distribusi untuk tim yang bertanggung jawab atas sumber daya. Email tidak boleh berupa email pribadi; itu harus berupa email anonim seperti daftar distribusi.
ComplianceFramework	Tidak dibatasi	Identifikasi kontrol dan kebijakan mana yang harus diterapkan pada sumber daya.
CostCenter		Identifikasi pusat biaya atau unit bisnis yang terkait dengan sumber daya (biasanya untuk alokasi biaya dan pelacakan).
Customer		Digunakan oleh pelanggan AMS yang memiliki sumber daya dari beberapa pelanggan (sub-pelanggan AMS). Untuk mengelompokkan sumber daya di lingkungan yang dikelola ke dalam pelanggan spesifik yang mereka layani. Identifikasi klien tertentu pada kelompok sumber daya atau layanan tertentu.
DataClassification		Identifikasi tingkat kerahasiaan data tertentu yang didukung sumber daya. Identifikasi kontrol dan kebijakan mana yang harus diterapkan pada sumber daya.
HoursOfOperation		Identifikasi tanggal atau waktu sumber daya harus dimulai, dihentikan, dihapus, atau diputar.

Tombol tanda	Nilai yang didukung	Catatan
OwnerTeam		Identifikasi tim yang bertanggung jawab atas sumber daya. Memfasilitasi komunikasi dengan tim yang bertanggung jawab atas sumber daya.
Patch Group	Anda memiliki dua opsi: - Anda dapat mengirimkan permintaan layanan dengan informasi yang diuraikan dalam AMS Advanced Patch Orchestrator: model patching berbasis tag, dan AMS membuat patch pada sumber daya yang Anda tentukan, dan menggunakan informasi yang Anda berikan, tag untuk Anda. Patch Group - Jika Anda telah membuat Patch Group tag pada sumber daya Anda, nilai yang didukung tidak dibatasi.	Sumber daya apa yang harus disertakan dalam jendela pemeliharaan tambalan otomatis.
ProjectId	Tidak dibatasi	Identifikasi proyek yang didukung sumber daya.

Tombol tanda	Nilai yang didukung	Catatan
SupportPriority	Salah satu dari enam kemungkinan akronim untuk Kerahasiaan, Integritas, atau Ketersediaan; urutan akronim adalah prioritas. Misalnya, I.C.A. berarti urutannya adalah Integritas, Kerahasiaan, Ketersediaan. Nilai lain yang dapat diterima adalah C.I.A., C.A.I., I.A.C., A.C.I., dan A.I.C.	Identifikasi jenis dukungan mana yang harus diprioritaskan: Kerahasiaan, Integritas, atau Ketersediaan.

Menandai catatan pembaruan massal

Catatan ini untuk digunakan dengan Tag | [Pembaruan Massal dan Tag | Pembaruan Massal \(Review Required\)](#) mengubah jenis penelusuran contoh.

Catatan tentang tag pembaruan massal:

- Layanan yang didukung:
 - Untuk [Tag | Pembaruan Massal \(Diperlukan Ulasan\)](#): Semua.
 - Untuk [Tag | Pembaruan Massal](#):
 - Auto Scaling
 - Amazon EC2
 - Penyeimbang Beban Elastis
 - Amazon RDS
 - Bucket Amazon S3
- Untuk menghasilkan file nilai yang dipisahkan koma (CSV), masuk ke Resource Groups > Tag Editor di AWS konsol, temukan sumber daya yang ingin Anda tag, lalu ekspor ke file CSV. Untuk informasi selengkapnya, lihat [Mengekspor Hasil ke CSV](#).

CATATAN: Sebaiknya gunakan URL S3 yang telah ditandatangani sebelumnya untuk menyediakan lokasi objek CSV.

- Harus ada kolom dengan header Service, Type, dan Identifier. Kolom ini wajib.
- Ubah nama kolom Identifier menjadi ID.
- Nilai untuk kolom Service, Type, dan Identifier (diubah menjadi ID) adalah seperti yang disediakan oleh Editor Tag di bawah Resource Groups.
- Jika sumber daya yang akan diberi tag tidak tersedia di bawah Editor Tag, gunakan Amazon Resource Name (ARN) sumber daya untuk kolom Identifier (diubah menjadi ID) dan biarkan Layanan dan Jenis kosong.
- Header kolom tag yang akan ditambahkan atau dimodifikasi harus memiliki format Tag: **TagKey**.
- Header kolom tag yang akan dihapus harus memiliki format Untag: **TagKey**.
- Setiap baris adalah untuk sumber daya yang akan ditandai atau tidak ditandai.
- Jika tag akan ditambahkan ke sumber daya, tentukan nilai tag di bawah **TagKey** kolom Tag: yang sesuai.
- Jika tag akan dihapus dari sumber daya, tentukan Benar di bawah **TagKey** kolom Untag: yang sesuai.
- Jika Tag: **TagKey** atau Untag: **TagKey** tidak berlaku untuk sumber daya, tambahkan tanda hubung (-) ke kolom masing-masing atau kosongkan.

CATATAN: Untag mengganti Tag - ini karena, tidak seperti Tag, Untag perlu ditambahkan secara manual ke file CSV, jadi kami menganggap tujuannya adalah untuk menghapus, bukan memodifikasi, tag.

- Setiap kolom tambahan yang tidak sesuai dengan kriteria diabaikan.

Important

Ekspor Editor Tag mengisi matriks semua tag terhadap semua sumber daya, tag yang hilang diisi dengan nilai 'tidak ditandai'. Menggunakan kembali CSV ekspor ini sebagai input ke RFC menghasilkan semua tag yang sebelumnya hilang dibuat, dengan nilai literal 'tidak ditandai'.

Note

Untuk informasi tentang mengekspor tag ke file CSV, lihat [Temukan Sumber Daya untuk Ditandai -> Ekspor Hasil ke CSV](#).

AWS Managed Services Resource Scheduler

Gunakan AWS Managed Services (AMS) Resource Scheduler untuk menjadwalkan mulai dan berhenti otomatis AutoScaling grup, EC2 instans Amazon, dan instans RDS di akun Anda. Ini membantu mengurangi biaya infrastruktur di mana sumber daya tidak dimaksudkan untuk berjalan 24/7. Solusinya dibangun di atas [Penjadwal Instance AWS](#), tetapi berisi fitur dan penyesuaian tambahan khusus untuk kebutuhan AMS.

Note

Secara default, Penjadwal Sumber Daya AMS tidak berinteraksi dengan sumber daya yang bukan bagian dari AWS CloudFormation tumpukan. Sumber daya harus menjadi bagian dari tumpukan yang dimulai dengan “stack-”, “sc-” atau “SC-”. Untuk menjadwalkan sumber daya yang bukan bagian dari CloudFormation tumpukan, Anda dapat memperbarui parameter tumpukan Resource Scheduler `ScheduleNonStackResources` ke `Yes`.

Penjadwal Sumber Daya AMS menggunakan periode dan jadwal:

- Periode menentukan waktu saat Resource Scheduler berjalan, seperti waktu mulai, waktu akhir, dan hari dalam sebulan.
- Jadwal berisi periode yang ditentukan, bersama dengan konfigurasi tambahan, seperti jendela pemeliharaan SSM, zona waktu, pengaturan hibernasi, dan sebagainya; dan tentukan kapan sumber daya harus dijalankan, mengingat aturan periode yang dikonfigurasi.

Anda dapat mengonfigurasi periode dan jadwal ini menggunakan tipe perubahan otomatis (CTs) AMS Resource Scheduler.

Untuk detail selengkapnya tentang setelan yang tersedia untuk Penjadwal Sumber Daya AMS, lihat dokumentasi Penjadwal AWS Instance terkait di komponen [Solusi](#). Untuk tampilan arsitektur solusi, lihat dokumentasi Penjadwal AWS Instance yang sesuai di [Architecture overview.html](#).

Menerapkan Penjadwal Sumber Daya AMS

Untuk menerapkan Penjadwal Sumber Daya AMS, gunakan tipe perubahan otomatis (CT): `Deployment | AMS Resource Scheduler | Solution | Deploy (ct-0ywnhc8e5k9z5)` untuk memunculkan RFC yang kemudian menyebarkan solusi di akun Anda. Setelah RFC dijalankan, CloudFormation tumpukan yang berisi sumber daya Penjadwal Sumber Daya AMS dengan konfigurasi default, secara otomatis disediakan ke akun Anda. Untuk selengkapnya tentang jenis perubahan Resource Scheduler, lihat [Penjadwal Sumber Daya AMS](#).

Note

Untuk mengetahui apakah Penjadwal Sumber Daya AMS sudah digunakan di akun Anda, periksa konsol AWS Lambda untuk akun tersebut dan cari fungsi Scheduler. AMSResource

Setelah Penjadwal Sumber Daya AMS disediakan di akun Anda, kami sarankan Anda meninjau konfigurasi default dan, jika diperlukan, menyesuaikan konfigurasi seperti kunci tag, zona waktu, layanan terjadwal, dan sebagainya, berdasarkan preferensi Anda. Untuk detail tentang penyesuaian yang disarankan, lihat [Menyesuaikan Penjadwal Sumber Daya AMS](#), selanjutnya.

Untuk membuat konfigurasi kustom, atau hanya mengonfirmasi konfigurasi Resource Scheduler,

Menyesuaikan Penjadwal Sumber Daya AMS

Sebaiknya Anda menyesuaikan properti berikut dari Penjadwal Sumber Daya AMS menggunakan pemutakhiran jenis perubahan Penjadwal Sumber Daya AMS, lihat Penjadwal [Sumber Daya AMS](#).

- **Nama tag:** Nama tag yang akan digunakan Resource Scheduler untuk mengaitkan jadwal instance dengan sumber daya. Nilai defaultnya adalah Jadwal.
- **Layanan Terjadwal:** Daftar layanan yang dipisahkan koma yang dapat dikelola oleh Resource Scheduler. Nilai default adalah “ec2, rds, autoscaling”. Nilai yang valid adalah “ec2”, “rds” dan “autoscaling”
- **Zona waktu default:** Tentukan zona waktu default untuk Resource Scheduler yang akan digunakan. Nilai defaultnya adalah UTC.
- **Gunakan CMK:** Daftar Amazon KMS Customer Managed Key (CMK) yang dipisahkan koma ARNs yang dapat diberikan izin kepada Resource Scheduler.
- **Penggunaan LicenseManager:** Daftar Manajer AWS Lisensi yang dipisahkan koma ARNs untuk Penjadwal Sumber Daya tersebut dapat diberikan izin untuk.

 Note

AMS dapat, dari waktu ke waktu, merilis fitur dan perbaikan agar AMS Resource Scheduler tetap up to date di akun Anda. Ketika ini terjadi, penyesuaian apa pun yang Anda buat pada Penjadwal Sumber Daya AMS dipertahankan.

Menggunakan Penjadwal Sumber Daya AMS

Untuk mengonfigurasi Penjadwal Sumber Daya AMS setelah solusi diterapkan, gunakan Penjadwal Sumber Daya otomatis CTs untuk membuat, menghapus, memperbarui, dan menjelaskan (mendapatkan detail tentang) periode Penjadwal Sumber Daya AMS (waktu saat Resource Scheduler berjalan) dan jadwal (periode yang dikonfigurasi dan opsi lainnya). Untuk contoh penggunaan jenis perubahan Penjadwal Sumber Daya AMS, lihat [Penjadwal Sumber Daya AMS](#).

Untuk memilih sumber daya yang akan dikelola oleh Penjadwal Sumber Daya AMS, setelah penerapan dan pembuatan jadwal, Anda menggunakan AMS Tag Create CTs untuk menandai grup Auto Scaling, tumpukan Amazon RDS, dan sumber daya EC2 Amazon dengan kunci tag yang Anda berikan selama penerapan, dan jadwal yang ditentukan sebagai nilai tag. Setelah sumber daya ditandai, sumber daya dijadwalkan untuk memulai atau berhenti sesuai jadwal Resource Scheduler yang ditentukan.

Tidak ada biaya tambahan untuk menggunakan Penjadwal Sumber Daya AMS. Namun solusinya menggunakan beberapa Layanan AWS dan Anda dikenakan biaya untuk sumber daya ini saat digunakan. Untuk detail selengkapnya, lihat [Ikhtisar arsitektur](#).

Untuk memilih keluar dari Penjadwal Sumber Daya AMS:

- Untuk memilih keluar atau menonaktifkan sementara: Kirim RFC menggunakan Manajemen otomatis | Penjadwal Sumber Daya AMS | Status | Nonaktifkan jenis perubahan (ct-14v49adibs4db)
- Untuk penghapusan permanen: Kirim Manajemen | Lainnya | Lainnya | Pembaruan (diperlukan tinjauan) (ct-0xdawir96cy7k) RFC meminta penghapusan dari sistem otomatisasi rilis Resource Scheduler

Penaksir biaya Penjadwal Sumber Daya AMS

Untuk melacak penghematan biaya, AMS Resource Scheduler menampilkan komponen yang menghitung perkiraan penghematan biaya per jam untuk sumber daya Amazon EC2 dan RDS yang

dikelola oleh penjadwal. Data penghematan biaya ini kemudian diterbitkan sebagai CloudWatch metrik (AMS/ResourceScheduler) untuk membantu Anda melacaknya. Estimator penghematan biaya hanya memperkirakan penghematan pada jam kerja instans. Ini tidak memperhitungkan biaya lain, seperti biaya transfer data yang terkait dengan sumber daya.

Estimator penghematan biaya diaktifkan dengan Resource Scheduler. Ini berjalan setiap jam dan mengambil data biaya dan penggunaan dari AWS Cost Explorer. Dari data itu menghitung biaya rata-rata per jam untuk setiap jenis instans dan kemudian memproyeksikan biaya untuk sehari penuh jika berjalan tanpa dijadwalkan. Penghematan biaya adalah perbedaan antara biaya yang diproyeksikan dan biaya yang dilaporkan aktual dari Cost Explorer untuk hari tertentu.

Misalnya, jika instance A dikonfigurasi dengan Resource Scheduler untuk dijalankan dari jam 9 pagi sampai jam 5 sore, yaitu delapan jam pada hari tertentu. Cost Explorer melaporkan biaya sebagai \$1 dan penggunaan sebagai 8. Oleh karena itu, biaya rata-rata per jam adalah \$0,125. Jika instance tidak dijadwalkan dengan Resource Scheduler, maka instance akan berjalan 24 jam pada hari itu. Dalam hal ini, biayanya adalah $24 \times 0,125 = \$3$. Resource Scheduler membantu Anda mencapai penghematan biaya \$2.

Agar estimator penghematan biaya dapat mengambil biaya dan penggunaan hanya untuk sumber daya yang dikelola oleh Resource Scheduler dari Cost Explorer, kunci tag yang digunakan Resource Scheduler untuk menargetkan sumber daya perlu diaktifkan sebagai tag alokasi Biaya di Dasbor Penagihan. Jika akun milik suatu organisasi, kunci tag harus diaktifkan di akun Manajemen organisasi. [Untuk informasi tentang hal ini, lihat Mengaktifkan Tag Alokasi Biaya yang Ditentukan Pengguna dan Tag Alokasi Biaya yang Ditentukan Pengguna](#)

Setelah kunci tag diaktifkan sebagai Tag Alokasi Biaya, AWS penagihan mulai melacak biaya dan penggunaan sumber daya yang dikelola oleh Resource Scheduler, dan setelah data tersebut tersedia, estimator penghematan biaya mulai menghitung penghematan biaya dan mempublikasikan data di bawah namespace metrik diAMS/ResourceScheduler. CloudWatch

Kiat penaksir biaya

Estimator Penghematan Biaya tidak menerima diskon seperti instans cadangan, rencana tabungan, dan sebagainya, menjadi pertimbangan dalam perhitungannya. Estimator mengambil biaya penggunaan dari Cost Explorer dan menghitung biaya rata-rata per jam untuk sumber daya. Untuk detail selengkapnya, lihat [Memahami Kumpulan Data AWS Biaya Anda: Lembar Cheat](#)

Agar estimator penghematan biaya dapat mengambil biaya dan penggunaan hanya untuk sumber daya yang dikelola oleh Resource Scheduler dari Cost Explorer, kunci tag yang digunakan Resource

Scheduler untuk menargetkan sumber daya perlu diaktifkan sebagai tag Alokasi Biaya di Dasbor Penagihan. Jika akun milik suatu organisasi, kunci tag harus diaktifkan di akun manajemen organisasi. Untuk informasi tentang hal ini, lihat Tag [Alokasi Biaya yang Ditentukan Pengguna](#). Jika tag alokasi biaya tidak diaktifkan, estimator tidak dapat menghitung penghematan dan menerbitkan metrik, bahkan jika itu diaktifkan.

Praktik terbaik Penjadwal Sumber Daya AMS

Menjadwalkan Instans Amazon EC2

- Perilaku mematikan instance harus disetel ke stop dan bukan `terminate`. Ini telah disetel sebelumnya ke stop untuk instance yang dibuat dengan jenis perubahan otomatis AMS Amazon EC2 Create (`ct-14027q0sjyt1h`) dan dapat disetel untuk instans Amazon yang dibuat dengan konsumsi, dengan menyetel properti ke `EC2 AWS CloudFormation InstanceInitiatedShutdownBehavior stop` Jika instance telah mematikan perilaku yang disetel `terminate`, maka instance akan berakhir ketika Resource Scheduler menghentikannya dan penjadwal tidak akan dapat memulainya kembali.
- EC2 Instans Amazon yang merupakan bagian dari grup Auto Scaling tidak diproses secara individual oleh Penjadwal Sumber Daya AMS, meskipun diberi tag.
- Jika volume root instans target dienkripsi dengan kunci master pelanggan (CMK) KMS, `kms:CreateGrant` izin tambahan perlu ditambahkan ke peran IAM Resource Scheduler Anda, agar penjadwal dapat memulai instance tersebut. Izin ini tidak ditambahkan ke peran secara default untuk meningkatkan keamanan. Jika Anda memerlukan izin ini, kirimkan RFC dengan Management | AMS Resource Scheduler | Solution | Update tipe perubahan, dan tentukan daftar KMS yang dipisahkan koma. ARNs CMKs

Penjadwalan grup Auto Scaling

- Penjadwal Sumber Daya AMS memulai atau menghentikan penskalaan otomatis grup Auto Scaling, bukan instance individual dalam grup. Artinya, penjadwal mengembalikan ukuran grup Auto Scaling (mulai) atau menetapkan ukuran ke 0 (berhenti).
- Tag `AutoScaling` grup dengan tag yang ditentukan dan bukan instance dalam grup.
- Selama berhenti, Penjadwal Sumber Daya AMS menyimpan nilai kapasitas Minimum, Diinginkan, dan Maksimum grup Auto Scaling dan menetapkan Kapasitas Minimum dan yang Diinginkan ke 0. Selama start, scheduler mengembalikan ukuran grup Auto Scaling seperti saat berhenti. Oleh karena itu, instans grup Auto Scaling harus menggunakan konfigurasi kapasitas yang sesuai

sehingga penghentian dan peluncuran ulang instans tidak memengaruhi aplikasi apa pun yang berjalan di grup Auto Scaling.

- Jika grup Auto Scaling diubah (kapasitas minimum atau maksimum) selama periode berjalan, penjadwal menyimpan ukuran grup Auto Scaling baru dan menggunakannya saat memulihkan grup di akhir jadwal berhenti.

Menjadwalkan instans Amazon RDS

- Penjadwal dapat mengambil snapshot sebelum menghentikan instance RDS (tidak berlaku untuk cluster Aurora DB). Fitur ini diaktifkan secara default dengan parameter AWS CloudFormation template Create RDS Instance Snapshot disetel ke true. Snapshot disimpan hingga saat berikutnya instans Amazon RDS dihentikan dan snapshot baru dibuat.

Scheduler dapat menggunakan instans start/stop Amazon RDS yang merupakan bagian dari cluster atau database Amazon RDS Aurora atau dalam konfigurasi multi availability zone (Multi-AZ). Namun, periksa batasan Amazon RDS saat penjadwal tidak dapat menghentikan instans Amazon RDS, terutama instans Multi-AZ. Untuk menjadwalkan Aurora Cluster untuk memulai atau berhenti gunakan parameter template Schedule Aurora Clusters (defaultnya benar). Cluster Aurora (bukan instance individual dalam cluster) harus diberi tag dengan kunci tag yang ditentukan selama konfigurasi awal dan nama jadwal sebagai nilai tag untuk menjadwalkan cluster tersebut.

Setiap instans Amazon RDS memiliki jendela pemeliharaan mingguan di mana setiap perubahan sistem diterapkan. Selama jendela pemeliharaan, Amazon RDS akan secara otomatis memulai instance yang telah dihentikan selama lebih dari tujuh hari untuk menerapkan pemeliharaan. Perhatikan bahwa Amazon RDS tidak akan menghentikan instance setelah acara pemeliharaan selesai.

Penjadwal memungkinkan menentukan apakah akan menambahkan jendela pemeliharaan yang disukai dari instans Amazon RDS sebagai periode berjalan ke jadwalnya. Solusinya akan memulai instance di awal jendela pemeliharaan dan menghentikan instance di akhir jendela pemeliharaan jika tidak ada periode berjalan lainnya yang menentukan bahwa instance harus berjalan, dan jika acara pemeliharaan selesai.

Jika acara pemeliharaan tidak selesai pada akhir jendela pemeliharaan, instance akan berjalan hingga interval penjadwalan setelah acara pemeliharaan selesai.

 Note

Penjadwal tidak memvalidasi bahwa sumber daya dimulai atau dihentikan. Itu membuat panggilan API dan melanjutkan. Jika panggilan API gagal, ia mencatat kesalahan untuk penyelidikan.

AWS Systems Manager di AMS Lanjutan

AWS Systems Manager Dokumen (dokumen SSM) mendefinisikan tindakan yang dilakukan Systems Manager pada sumber daya Anda AWS. Systems Manager mencakup lebih dari selusin dokumen pra-konfigurasi yang dapat Anda gunakan dengan menentukan parameter saat runtime. Dokumen menggunakan JavaScript Object Notation (JSON) atau YAMM, dan dokumen tersebut menyertakan langkah-langkah dan parameter yang Anda tentukan.

AWS Managed Services (AMS) adalah penerbit tepercaya untuk dokumen SSM. Dokumen SSM yang dimiliki oleh AMS hanya dibagikan dengan akun AMS onboard, selalu dimulai dengan awalan cadangan (AWSManagedLayanan-*), dan muncul di konsol Systems Manager, seperti yang dimiliki oleh. AWS Proses AMS untuk pengembangan dan penerbitan dokumen SSM mengikuti praktik AWS terbaik dan memerlukan beberapa tinjauan sejawat sepanjang siklus hidup dokumen. Untuk informasi selengkapnya tentang praktik AWS terbaik untuk berbagi dokumen SSM, lihat [Praktik terbaik untuk dokumen SSM bersama](#).

Dokumen SSM AMS Advanced yang tersedia

Dokumen SSM AMS Advanced tersedia secara eksklusif untuk pelanggan AMS Advanced, dan digunakan untuk mengotomatiskan alur kerja operasional untuk mengoperasikan akun Anda.

Untuk melihat dokumen AMS Advanced SSM yang tersedia dari AWS Management Console:

1. [Buka Systems Managerconsole di AWS Systems Manager konsol](#).
2. Pilih Berbagi dengan saya.
3. Di bilah pencarian, filter berdasarkan awalan nama Dokumen, lalu Sama dengan, dan atur nilainya ke AWSManagedLayanan -.

Untuk petunjuk AWS CLI, lihat [Menggunakan dokumen SSM bersama](#).

Versi dokumen SSM AMS Advanced

Dokumen SSM mendukung pembuatan versi. Dokumen SSM AMS Advanced tidak dapat dimodifikasi dari akun pelanggan dan tidak dapat dibagikan ulang. Mereka dikelola dan dikelola secara terpusat oleh AMS Advanced untuk mengoperasikan akun.

Nomor versi ditambahkan dengan setiap pembaruan dokumen secara spesifik Wilayah AWS. Saat Wilayah baru tersedia, konten dokumen yang sama di dua Wilayah dapat memiliki nomor versi yang berbeda; ini tipikal dan tidak berarti perilaku mereka akan berbeda. Jika Anda ingin membandingkan dua dokumen AMS Advanced SSM, sebaiknya bandingkan hash mereka dengan CLI AWS :

```
aws ssm describe-document \
--name AWSManagedServices-DOCUMENTNAME \
--output text --query "Document.Hash"
```

Dua dokumen SSM identik jika hash mereka cocok.

Harga Systems Manager di AMS

Tidak ada biaya yang terkait dengan akses dokumen AMS Advanced SSM. Biaya runtime bervariasi berdasarkan jenis dokumen SSM, langkah-langkahnya, dan durasi runtime. Untuk informasi lebih lanjut, lihat [AWS Systems Manager harga](#).

Akun AMS offboard

AMS menawarkan bantuan off-boarding untuk akun landing zone satu akun dan multi-akun landing zone.

AMS tidak membatalkan pembagian apa pun AMIs dari Anda selama offboarding untuk menghindari dampak bagi setiap depedensi Anda. Jika Anda ingin menghapus AMS AMIs dari akun Anda, Anda dapat menggunakan `cancel-image-launch-permission` API untuk menyembunyikan spesifik AMIs. Misalnya, Anda dapat menggunakan skrip di bawah ini untuk menyembunyikan semua AMS AMIs yang dibagikan dengan akun Anda sebelumnya:

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
do
aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

Anda harus menginstal AWS CLI v2 agar skrip dapat dijalankan tanpa kesalahan apa pun. Untuk langkah-langkah penginstalan AWS CLI, lihat [Menginstal atau memperbarui AWS CLI versi terbaru](#). Untuk detail tentang `cancel-image-launch-permission` perintah, lihat [cancel-image-launch-permission](#).

Note

Tanggal penghentian layanan adalah hari terakhir bulan kalender setelah berakhirnya periode pemberitahuan penghentian 30 hari yang diperlukan. Jika akhir periode pemberitahuan penghentian yang diperlukan jatuh setelah hari ke-20 bulan kalender, maka tanggal penghentian layanan adalah hari terakhir dari bulan kalender berikutnya. Berikut ini adalah contoh skenario untuk tanggal penghentian.

- Jika pemberitahuan penghentian diberikan pada 12 April, maka pemberitahuan 30 hari berakhir pada 12 Mei. Tanggal penghentian layanan adalah 31 Mei.
- Jika pemberitahuan penghentian diberikan pada 29 April, maka pemberitahuan 30 hari berakhir pada 29 Mei. Tanggal penghentian layanan adalah 30 Juni.

Topik

- [Offboard dari akun landing zone akun tunggal AMS](#)
- [Offboard dari akun landing zone multi-akun AMS](#)

Offboard dari akun landing zone akun tunggal AMS

AMS menawarkan bantuan off-boarding dalam waktu 30 hari sebelum penghentian AMS.

Anda harus meminta bantuan off-boarding setidaknya 7 hari sebelum bantuan tersebut dapat diberikan. Bantuan off-boarding dapat ditawarkan dalam dua bentuk:

- Serah terima kontrol: AMS mentransfer kembali kontrol akun kepada Anda bersama dengan kredensi akses untuk semua aplikasi yang dikelola AMS, atau
- Pengakhiran sumber daya untuk penutupan akun: AMS menghapus semua data di lingkungan yang dikelola AMS dan membatalkan ketentuan sumber daya aktif apa pun di akun. Saat mengirimkan permintaan offboarding, pelanggan dapat meminta AMS:
 - Menghapus atau menyimpan objek data (termasuk log) yang disimpan di bucket Amazon S3
 - Hapus atau simpan ember Amazon S3

- Hapus atau pertahankan titik AWS Backup pemulihan

 Important

Permintaan spesifik lainnya (tergantung pada masuk akal) harus dikomunikasikan ke AMS sebelum inisialisasi offboarding.

Prasyarat Opsional (jika diperlukan):

 Note

Sebelum permintaan offboarding, pelanggan dapat meminta bantuan AMS untuk mentransfer data Anda dalam format yang ada menggunakan AWS Snowball Edge atau media lain yang AWS berinteraksi dengannya.

Selain backup data, data pelanggan berikut dapat diberikan sebagai bagian dari bantuan offboarding:

- Data yang disimpan dalam layanan penyimpanan termasuk log
- Skema jenis perubahan khusus pelanggan
- CloudFormation template untuk skema jenis perubahan

Jika aktivitas off-boarding tidak selesai setelah penghentian AMS, kami menyerahkan kontrol akun untuk memungkinkan Anda menyelesaikan aktivitas yang tertunda.

Fungsi	Apa yang dihapus	Dampak	Tindakan yang dibutuhkan
Pemantauan, Pencatatan, Peringatan	Pemantauan AMS dihapus MMS (Managed Monitoring System) berhenti berlangganan	AMS tidak lagi memiliki akses atau visibilitas ke sumber daya dan lingkungan Anda.	Kontinjensi untuk layanan yang dihapus dan berhenti berlangganan dimiliki oleh Anda.

Fungsi	Apa yang dihapus	Dampak	Tindakan yang dibutuhkan
	Resource Tagger dan Alarm Manager dihapus CloudWatch Peringatan dasar tetap ada di sumber daya yang ada GuardDuty dan Macie: Kepemilikan kembali kepada Anda		
Manajemen Backup	Otomatisasi Cadangan AMS dihapus meskipun AWS Backup layanan tetap tersedia untuk digunakan. Brankas cadangan dan data disimpan kecuali penghapusan diminta.	AMS tidak lagi memantau pekerjaan cadangan atau melakukan tindakan restorasi selama insiden. Alarm dan peringatan dinonaktifkan. Penghapusan peran cadangan IAM dan kunci KMS membuat cadangan AMS Anda tidak dapat dioperasikan.	Paket Cadangan AMS harus dikonfigurasi ulang. Semua kepemilikan pemantauan dan remediasi kembali kepada Anda.
Otomatisasi AMS untuk manajemen layanan	Runbook otomatisasi AWS SSM yang dikurasi AMS, Amazon Simple Notification Service (SNS), dan fungsi Lambda tidak lagi tersedia. AWS	Tidak ada akses AMS ke akun Anda. Semua otomatisasi dinonaktifkan.	Semua otomatisasi termasuk fungsi SSM, SNS, dan Lambda perlu dibuat ulang, jika diperlukan.

Fungsi	Apa yang dihapus	Dampak	Tindakan yang dibutuhkan
Kepatuhan	Visibilitas AMS ke dalam dan pemantauan untuk semua GuardDuty dan AWS Config aturan dihapus, meskipun aturan ini tetap ada di akun.	Semua pemantauan, pelaporan, dan remediasi dari Amazon GuardDuty dan AWS Config Aturan tidak lagi dikelola oleh AMS.	Pemantauan dan remediasi untuk semua alat keamanan dan kepatuhan yang akan diasumsikan oleh Anda.
Agen on-instance	Akses ke Resource Scheduler, Resource Tagger, atau konfigurasi instans otomatis untuk menginstal agen yang diperlukan dalam EC2 instans Anda akan dihapus.	CloudWatch dan Agen SSM pada instance dibiarkan di tempatnya dengan konfigurasi yang ada, namun AMS tidak lagi membantu konfigurasi ini.	Anda mengelola penandaan dan konfigurasi on-instance CloudWatch dan agen SSM.

Fungsi	Apa yang dihapus	Dampak	Tindakan yang dibutuhkan
Infrastruktur patch dan pelaporan	AMS tidak lagi mengelola aktivitas sebelum dan sesudah penambalan, dan akses serta visibilitas ke layanan ini dihapus.	AMS tidak lagi membuat snapshot instance sebelum menambal, tidak lagi menginstal dan memantau instalasi patch, dan tidak lagi memberi tahu Anda tentang hasilnya. Laporan dan bucket S3 “audit” tertinggal di akun Anda sesuai permintaan Anda. AMS tidak lagi menghasilkan laporan metrik layanan.	Anda mempertahankan garis dasar Patch dan snapshot yang dibuat di masa lalu. Selain itu, konfigurasi jendela pemeliharaan patch tetap ada tetapi tambalan tidak lagi diinstal atau diperbaiki oleh AMS. Semua pelaporan metrik operasional infrastruktur sekarang menjadi tanggung jawab Anda.
Manajemen proses	Semua akun dilepas dari manajemen layanan yang disediakan untuk insiden, termasuk permintaan layanan, masalah, dan perubahan, manajemen.	Semua gangguan layanan yang sebelumnya diperbaiki oleh AMS melalui insiden dan permintaan layanan, dan perubahan lingkungan, serta investigasi Root Cause, dikelola lebih lama oleh AMS.	Anda mendapatkan kembali kepemilikan penuh atas semua manajemen proses.

Offboard dari akun landing zone multi-akun AMS

Ada dua jenis AWS akun yang dapat Anda lepaskan dari landing zone multi-akun AMS Advanced:

- Akun aplikasi

- Akun inti

Untuk melepaskan semua akun dari landing zone AMS Multi-akun Anda, Anda harus melepaskan semua akun Aplikasi sebelum Anda melepaskan akun Core.

Untuk mengambil alih dan melanjutkan beban kerja pengoperasian di akun Aplikasi atau Inti offboard, pastikan Anda meninjau dokumentasi ini dengan tim akun AMS Anda. Dokumentasi ini menguraikan perubahan yang dilakukan AMS selama proses offboard.

Tugas yang harus diselesaikan untuk melanjutkan pengoperasian akun offboarded

Tugas berikut diperlukan untuk melanjutkan pengoperasian akun yang Anda offboard dari landing zone multi-akun AMS:

- Aktifkan mode Pengembang: Untuk mendapatkan lebih banyak izin ke akun Anda, aktifkan mode Pengembang sebelum Anda keluar dari akun Aplikasi dari AMS. Saat Anda mengaktifkan mode Pengembang, Anda dapat lebih mudah membuat perubahan yang diperlukan untuk mempersiapkan offboarding. Jangan mencoba menghapus atau memodifikasi sumber daya infrastruktur AMS. Jika Anda menghapus sumber daya infrastruktur AMS, AMS mungkin tidak dapat berhasil keluar dari akun Anda. Untuk informasi tentang cara mengaktifkan mode Pengembang, lihat [Memulai mode AMS Advanced Developer](#).

Jika Anda tidak dapat menyelesaikan perubahan yang diperlukan untuk mempersiapkan offboarding setelah Anda mengaktifkan mode Pengembang, hubungi tim akun AMS Anda untuk mendiskusikan persyaratan Anda.

- Pilih metode alternatif untuk akses EC2 tumpukan: Setelah Anda melepaskan akun Aplikasi dari AMS, Anda tidak dapat menggunakannya RFCs untuk mengakses sumber daya tumpukan Anda. Tinjau [Perubahan offboarding](#), lalu pilih metode akses alternatif sehingga Anda mempertahankan akses ke tumpukan Anda. Untuk informasi selengkapnya, lihat [Alternatif Akses](#).

Akun Aplikasi AMS Offboard

Untuk melepaskan akun Aplikasi dari lingkungan landing zone multi-akun Anda, selesaikan langkah-langkah berikut untuk setiap akun:

1. Verifikasi bahwa tidak ada yang terbuka RFCs di akun. Untuk informasi selengkapnya, lihat [Buat, kloning, perbarui, temukan, dan batalkan RFCs](#).

2. Verifikasi bahwa Anda dapat mengakses alamat email pengguna utama atau root untuk akun tersebut.
3. Dari akun Aplikasi, kirimkan RFC dengan Akun Aplikasi [Konfirmasi jenis perubahan offboarding](#) (ct-2wlfo2jxj2rkj). Di RFC, tentukan akun Aplikasi ke offboard.
4. Dari akun Manajemen, kirimkan RFC dengan akun [Manajemen | Akun Aplikasi Offboard](#) (ct-0vdiy51oyrhbm) jenis perubahan. Di RFC, tentukan akun Aplikasi ke offboard. Juga, tunjukkan apakah Anda ingin menghapus atau mempertahankan lampiran gateway transit ke landing zone.
5. Untuk memastikan penagihan AMS dihentikan, beri tahu CSDM bahwa Anda telah melakukan offboard akun.

Hal berikut terjadi setelah akun Aplikasi di-offboard:

- Semua komponen dipisahkan dari layanan AMS, tetapi sumber daya yang Anda buat tetap ada di akun. Anda dapat memilih untuk menyimpan atau menutup akun AMS yang di-offboard.
- Akun inti dan akun Aplikasi lainnya yang tersisa berfungsi normal setelah akun Aplikasi di-offboard.
- Penagihan AMS dihentikan, tetapi AWS penagihan tidak dihentikan sampai Anda menutup akun. Untuk informasi selengkapnya, lihat [Apa yang perlu Anda ketahui sebelum menutup akun Anda](#).
- Jika akun ditutup, maka akun tersebut terlihat di organisasi Anda di suspended negara bagian selama 90 hari. Setelah 90 hari, akun yang ditutup dihapus secara permanen dan tidak lagi terlihat di organisasi Anda.
- Setelah akun ditutup, Anda masih dapat masuk dan mengajukan kasus dukungan atau kontak Dukungan selama 90 hari.
- Setelah 90 hari, konten apa pun yang tersisa di akun dihapus secara permanen dan AWS layanan yang tersisa dihentikan.

FAQ offboarding akun aplikasi

T: Dapatkah saya menggunakan peran IAM federasi saya untuk terus mengakses akun Aplikasi yang saya offboard dari landing zone multi-akun AMS saya?

Ya. [Peran default AWS Identity and Access Management \(IAM\)](#) yang dibuat AMS tetap tersedia di akun setelah AMS offboarding. Namun, peran dan kebijakan ini dirancang untuk digunakan dengan manajemen akses AMS. Untuk menyediakan akses yang diperlukan bagi pengguna Anda, Anda mungkin perlu menyebarkan sumber daya IAM Anda sendiri.

T: Bagaimana cara mendapatkan akses penuh ke akun Aplikasi yang saya offboard dari landing zone multi-akun AMS saya?

Akun Aplikasi Offboarded dipindahkan ke Unit Organisasi Usang (OU) dalam struktur akun. AWS Organizations Langkah ini mengangkat pembatasan akses SCP yang sebelumnya memblokir akses pengguna root. Untuk selengkapnya tentang cara mengatur ulang kredensi pengguna root, lihat [Menyetel ulang kata sandi pengguna root yang hilang atau terlupakan](#).

T: Perubahan apa yang dilakukan selama offboarding akun Aplikasi?

Untuk informasi tentang tindakan yang dilakukan AMS saat layanan keluar dari akun, lihat [Perubahan offboarding](#).

T: Dapatkah saya melepaskan akun Aplikasi tanpa melepaskannya dari gateway transit?

Ya. Gunakan [akun Manajemen | Akun Aplikasi Offboard](#) (ct-0vdiy51oyrhbm) ubah jenis untuk mengirimkan RFC, dan tentukan parameternya sebagai `DeleteTransitGatewayAttachment` `False`

T: Berapa lama waktu yang dibutuhkan untuk melepaskan akun Aplikasi?

Bila Anda menggunakan [akun Manajemen | Akun Aplikasi Offboard](#) (ct-0vdiy51oyrhbm) mengubah jenis, selesai dalam waktu 1 jam. RFCs

T: Apakah wajib saya menutup akun offboarded?

Tidak. Penutupan akun setelah offboarding AMS tidak wajib. Selama proses offboarding, AMS menghapus akses dan pengelolaannya atas AWS akun Anda, tetapi akun dan sumber daya Anda di dalam akun tetap ada. Penting untuk dicatat bahwa setelah AMS offboarding, Anda bertanggung jawab penuh untuk mengelola dan memelihara AWS akun dan sumber daya Anda. AMS tidak bertanggung jawab atas masalah, insiden, atau gangguan layanan apa pun yang mungkin terjadi di akun Anda setelah proses offboarding selesai. Untuk informasi selengkapnya, lihat [Bagaimana cara menutup AWS akun saya?](#) .

T: Jika saya mengajukan permintaan penutupan akun, apakah semua sumber daya yang ada segera dihapus?

Tidak. Penutupan akun tidak menghentikan sumber daya Anda. Sumber daya di akun secara otomatis berakhir 90 hari setelah permintaan penutupan. Penagihan AMS berhenti, tetapi penagihan AWS sumber daya tidak berhenti sampai Anda menutup akun. Untuk informasi selengkapnya, lihat [Apa yang perlu Anda ketahui sebelum menutup akun Anda](#).

T: Dapatkah saya menjadwalkan offboarding akun Aplikasi?

Ya. Anda dapat menjadwalkan RFCs untuk berjalan pada waktu tertentu. Namun, [Akun Aplikasi | Konfirmasi offboarding](#) RFC harus diselesaikan sebelum Anda dapat menjadwalkan [akun Manajemen | Akun Aplikasi Offboard](#) RFC. Untuk informasi selengkapnya, lihat [penjadwalan RFC](#).

Akun aplikasi offboarding RACI

- R: Pihak yang bertanggung jawab. Pihak yang bertanggung jawab untuk menyelesaikan tugas yang tercantum.
- A: Pihak yang bertanggung jawab. Partai yang menyetujui tugas yang diselesaikan.
- C: Pihak yang dikonsultasikan. Sebuah pihak yang pendapatnya dicari, biasanya sebagai ahli materi pelajaran, dan dengan siapa ada komunikasi bilateral.
- I: Pesta yang diinformasikan. Sebuah pihak yang diinformasikan tentang kemajuan, seringkali hanya pada penyelesaian tugas atau deliverable.

Aktifitas	Pelang	AWS Managed Services (AMS)
Prasyarat		
Verifikasi akses ke alamat email root untuk setiap ID AWS akun yang akan di-offboard	R	C
Tinjau dokumentasi AMS tentang tindakan pelanggan yang direkomen dasikan dan siapkan akun untuk offboarding AMS	R	C
Jika diperlukan, kirimkan RFC untuk mengaktifkan mode Pengembang guna menyiapkan akun untuk offboarding AMS	R	I
Jika diperlukan, pilih metode alternatif untuk akses EC2 tumpukan.	R	I
Offboarding		
Kirim RFCs untuk mengonfirmasi dan meminta offboarding akun Aplikasi	R	I

Aktifitas	Pelang	AWS Managed Services (AMS)
Komponen AMS offboard dari akun Aplikasi	I	R
Beri tahu AMS CSDM tentang akun offboard untuk menghentikan penagihan AMS	R	I
Pasca offboarding		
Setel ulang kata sandi akun pengguna root dan verifikasi akses root di akun offboard	R	C
Tutup akun atau ikuti panduan AMS tentang tindakan pelanggan yang direkomendasikan dalam dokumentasi offboarding AMS untuk terus mengoperasikan akun	R	C

Akun Offboard Core

Untuk melakukan offboard multi-account landing zone Core, selesaikan langkah-langkah berikut:

1. Verifikasi bahwa semua akun Aplikasi di landing zone telah di-offboard dari AMS.
2. Verifikasi bahwa Anda tidak memiliki akun terbuka RFCs . Untuk informasi selengkapnya, lihat [Buat, kloning, perbarui, temukan, dan batalkan RFCs](#).
3. Verifikasi bahwa Anda dapat mengakses alamat email pengguna utama atau root untuk semua akun Core. Untuk informasi selengkapnya, lihat [Akun Zona Pendaratan Multi-Akun](#).
4. Verifikasi bahwa Anda dapat mengakses nomor telepon pengguna utama atau root untuk akun manajemen. Gunakan peran AWSManagedServicesBillingRole IAM untuk memperbarui nomor telepon. Untuk informasi selengkapnya, lihat [Bagaimana cara memperbarui nomor telepon yang terkait dengan AWS akun saya?](#) .
5. Masuk ke akun manajemen landing zone AMS Anda dan kirimkan permintaan layanan AMS. Dalam permintaan layanan, tentukan untuk melepaskan seluruh landing zone Anda.

Berikut ini terjadi setelah akun Core di-offboard:

- Semua komponen dipisahkan dari layanan AMS, tetapi beberapa AWS sumber daya tetap ada di akun. Anda dapat memilih untuk menyimpan atau menutup akun Inti yang di-offboard AMS.
- Penagihan AMS dihentikan, tetapi AWS penagihan tidak dihentikan sampai Anda menutup akun. Untuk informasi selengkapnya, lihat [Apa yang perlu Anda ketahui sebelum menutup akun Anda](#).
- Jika akun ditutup, maka akun tersebut terlihat di organisasi Anda di suspended negara bagian selama 90 hari. Setelah 90 hari, akun anggota yang ditutup dihapus secara permanen dan tidak lagi terlihat di organisasi Anda.
- Setelah akun ditutup, Anda masih dapat masuk dan mengajukan kasus dukungan atau kontak Dukungan selama 90 hari.
- Setelah akun ditutup selama 90 hari, konten apa pun yang tersisa di akun dihapus secara permanen, dan AWS layanan yang tersisa dihentikan.

FAQ offboarding akun inti

T: Dapatkah saya menggunakan peran IAM federasi saya untuk terus mengakses akun Core offboard?

Ya. [Peran default AWS Identity and Access Management \(IAM\)](#) yang dibuat AMS tetap tersedia di akun offboard. Namun, peran dan kebijakan ini dirancang untuk digunakan dengan manajemen akses AMS. Untuk menyediakan akses yang diperlukan bagi pengguna Anda, Anda mungkin perlu menyebarkan sumber daya IAM Anda sendiri.

T: Bagaimana cara mendapatkan akses penuh ke akun Manajemen, Layanan Bersama, Jaringan, atau akun [MALZ non-aplikasi lainnya setelah melakukan offboarding dari landing zone multi-akun AMS](#)?

Setelah offboarding, ikuti petunjuk di [Mengatur ulang kata sandi pengguna root yang hilang atau terlupakan](#) untuk menggunakan kredensial pengguna utama (root) untuk mengakses akun Core selain akun manajemen. Tidak seperti jenis akun lainnya, akun manajemen mempertahankan perangkat otentikasi multi-faktor (MFA) yang tidak dapat diakses yang terkait dengan pengguna root untuk mencegah penggunaan. Untuk mendapatkan kembali akses root, Anda harus mengikuti proses pemulihan [perangkat MFA yang hilang](#).

T: Perubahan apa yang dilakukan selama offboarding akun Core?

Untuk informasi tentang tindakan yang dilakukan AMS saat layanan keluar dari akun, lihat [Perubahan offboarding](#).

T: Berapa lama waktu yang dibutuhkan offboarding akun Core untuk diselesaikan?

Proses offboarding akun Core biasanya memakan waktu hingga 30 hari untuk diselesaikan. Namun, untuk memastikan bahwa semua langkah yang diperlukan diselesaikan dengan benar, Anda harus memulai permintaan offboarding setidaknya 7 hari sebelum offboarding dimulai. Untuk memfasilitasi transisi yang mudah, rencanakan terlebih dahulu dan kirimkan permintaan offboarding Anda terlebih dahulu.

T: Bagaimana cara mengelola komponen bersama setelah AMS offboarding?

AMS Managed Active Directory dan komponen infrastruktur layanan bersama lainnya dirancang untuk akses operator AMS. Anda mungkin perlu memperbarui grup keamanan Amazon Elastic Compute Cloud (Amazon EC2), kebijakan kontrol AWS Organizations layanan (SCP), atau membuat perubahan lain untuk mempertahankan akses penuh ke komponen ini.

T: Dapatkah saya menutup akun Core offboard?

Secara default, akun Aplikasi memiliki beberapa dependensi pada akun MALZ Core, seperti AWS Organizations keanggotaan, konektivitas jaringan gateway transit, dan resolusi DNS melalui AMS Managed Active Directory. Setelah Anda menyelesaikan ketergantungan ini, Anda dapat menonaktifkan dan menutup akun Core offboard. Untuk informasi selengkapnya, lihat [Akun Zona Pendaratan Multi-Akun](#).

Akun inti offboarding RACI

- R: Pihak yang bertanggung jawab. Pihak yang bertanggung jawab untuk menyelesaikan tugas yang tercantum.
- A: Pihak yang bertanggung jawab. Partai yang menyetujui tugas yang diselesaikan.
- C: Pihak yang dikonsultasikan. Sebuah pihak yang pendapatnya dicari, biasanya sebagai ahli materi pelajaran, dan dengan siapa ada komunikasi bilateral.
- I: Pesta yang diinformasikan. Sebuah pihak yang diinformasikan tentang kemajuan, seringkali hanya pada penyelesaian tugas atau deliverable.

Aktifitas	Pelang	AWS Managed Services (AMS)
Prasyarat		
Verifikasi akses ke alamat email root untuk setiap ID akun AWS yang akan di-offboard	R	C
Verifikasi akses ke dan perbarui nomor telepon pengguna root untuk akun manajemen	R	C
Tinjau dokumentasi AMS tentang tindakan pelanggan yang direkomen dasikan dan siapkan akun untuk offboarding AMS	R	C
Offboarding		
Kirim permintaan layanan untuk meminta offboarding landing zone	R	I
Komponen AMS offboard dari akun Core	I	R
Pasca offboarding		
Setel ulang kata sandi akun pengguna root dan verifikasi akses root di akun offboard	R	C
Tutup akun atau ikuti panduan AMS tentang tindakan pelanggan yang direkomendasikan dalam dokumentasi offboarding AMS untuk terus mengoperasikan akun	R	C

Perubahan offboarding

Tabel berikut menjelaskan tindakan yang dilakukan AMS untuk offboarding landing zone multi-akun, potensi dampak, dan tindakan yang direkomendasikan.

Komponen	Jenis akun	Tindakan yang diambil untuk offboard	Dampak potensial	Tindakan pelanggan yang direkomen dasikan
Manajeme akses	Akun aplikasi	Setelah offboarding, akses tumpukan RFCs untuk just-in-time, akses terikat waktu tidak dapat lagi dikirimkan untuk mengakses EC2 tumpukan melalui host benteng AMS AMS tidak lagi mengelola komponen terkait akses pada tumpukan EC2 sumber daya yang ada (agen Terbuka PBIS, skrip gabungan domain)	Tidak dapat menggunakan benteng AMS melalui RFS untuk mengakses instans EC2 EC2 instance yang diluncurkan dari non-AMS yang disediakan AMIs tidak digabungkan ke domain Direktori Aktif Terkelola Jika tidak dihapus, skrip peluncuran AMS di tumpukan sumber daya yang ada mungkin menghasilkan kesalahan karena dependensi AMS yang hilang, dan mencegah bergabung kembali ke domain yang berbeda	Gunakan metode alternatif untuk mengakses EC2 instance (lihat Alternatif Akses) Hapus skrip peluncuran AMS dari tumpukan EC2 sumber daya yang ada (lihat Nonaktifkan skrip EC2 peluncuran AMS)
Manajeme akses (lanjutan)	Akun inti	Jika Anda bermigrasi dari PBIS Open ke PBIS Enterprise (AD Bridge), maka AMS tidak lagi	Jika lisensi PBIS Enterprise diizinkan kedaluwarsa, kredensil Active	Jika Anda bermigrasi ke PBIS Enterprise (AD Bridge), putuskan apakah

Komponen	Jenis akun	Tindakan yang diambil untuk offboard	Dampak potensial	Tindakan pelanggan yang direkomen dasikan
		memperbarui lisensi setelah offboarding akun inti	Directory tidak valid untuk tumpukan instans berbasis Linux yang ada EC2	akan mempertahankan lisensi atau menonaktifkan (lihat PBIS Open/Enterprise (Jembatan AD))
Penebang, Pemantauan, Incident/Event Manajeme	Aplikasi dan akun Inti	Komponen AMS yang akan diterapkan Peringatan dari pemantauan dasar di AMS dihapus CloudWatch Alarm Amazon yang digunakan tetap ada tetapi tidak lagi membuat insiden AMS AWS Config otorisasi agregasi dari AMS dan akun keamanan MALZ Core dihapus AWS Config aturan tetap diterapkan dan Amazon GuardDuty tetap diaktifkan, tetapi tidak lagi membuat insiden AMS	Sumber daya yang baru dibuat tidak memiliki pemantauan dasar AMS dan alarm diterapkan Alarm metrik infrastruktur dan peristiwa keamanan tidak lagi menghasilkan insiden AMS AWS Config tidak lagi dikumpulkan dalam akun pusat	Tentukan, tangkap, dan analisis metrik operasi untuk melihat peristiwa beban kerja dan mengambil tindakan yang tepat. Menerapkan alur kerja peringatan yang diperlukan untuk terus menerapkan pemantauan operasional dan alarm yang diperlukan pada sumber daya baru dan untuk menerima peringatan keamanan dari dan AWS Config Amazon. GuardDuty

Komponen	Jenis akun	Tindakan yang diambil untuk offboard	Dampak potensial	Tindakan pelanggan yang direkomen dasikan
Manajeme kontinuit as (Backup dan Restore)	Akun aplikasi	AMS tidak lagi memantau pekerjaan pencadangan atau melakukan permintaan pencadangan dan pemulihan Brankas cadangan default AMS, kunci enkripsi cadangan, dan peran cadangan tetap ada	Kegagalan operasi Backup mungkin tidak diperhatikan	Pantau dan tinjau konfigurasi rencana cadangan
Manajeme tambalan	Aplikasi dan akun Inti	AMS tidak lagi memantau operasi penambalan untuk eksekusi yang berhasil atau melakukan penambalan manual AMS tidak lagi memperbaiki komponen infrastruktur AMS Garis dasar tambalan yang disediakan AMS dipertahankan Runbook otomatisasi AWS Systems Manager patch yang disediakan AMS tidak dibagikan dan tidak lagi tersedia untuk digunakan	Kegagalan operasi penambalan mungkin tidak diperhatikan Konfigurasi patch yang ada yang bergantung pada AMS yang disediakan runbook Systems Manager Automation harus dikonfigurasi ulang untuk melanjutkan tanpa gangguan	Tinjau dan konfigurasi ulang konfigurasi patching sesuai kebutuhan

Komponen	Jenis akun	Tindakan yang diambil untuk offboard	Dampak potensial	Tindakan pelanggan yang direkomendasikan
Manajemen jaringan	Akun aplikasi	Jika ditentukan, lampiran gateway transit di akun Aplikasi offboard akan dihapus	Akun Aplikasi Offboarded tidak dapat lagi menggunakan gateway transit untuk mengakses layanan bersama, seperti Direktori Aktif Terkelola atau akun Aplikasi lainnya	Tentukan DeleteTransitGatewayAttachment False untuk mempertahankan konektivitas gateway transit
Manajemen keamanan	Akun aplikasi	Akun terlepas dari konsol Trend Micro DSM pusat. Selain itu, agen endpoint tidak lagi meneruskan peringatan melalui proses insiden AMS Agen Trend Micro tetap diinstal tetapi tidak lagi dikelola atau diperbarui oleh AMS AMS menyediakan kustomisasi AMI yang menerapkan agen Trend Micro tidak lagi dikelola atau diperbarui oleh AMS	EC2 deteksi malware titik akhir instance mungkin tidak diperhatikan Agen mikro Trend tidak digunakan pada EC2 instance yang diluncurkan dari non-AMS yang disediakan AMIs	Pertimbangkan opsi untuk melanjutkan atau menghentikan Trend Micro (lihat Trend Micro Deep Security)

Komponen	Jenis akun	Tindakan yang diambil untuk offboard	Dampak potensial	Tindakan pelanggan yang direkomen dasikan
Manajeme keamanan (cont'd)	Akun inti	Infrastruktur Trend Micro DSM dibiarkan di dalam akun Layanan Bersama tetapi tidak lagi dikelola atau diperbarui oleh AMS Trend Micro DSM tidak lagi meneruskan peringatan melalui proses insiden AMS	EC2 deteksi malware titik akhir instance mungkin luput dari perhatian EC2 perlindungan titik akhir instance mungkin terpengaruh jika infrastruktur tidak dipertahankan (pembaruan definisi, lisensi, dan sebagainya)	Putuskan apakah akan melanjutkan atau menghentikan Trend Micro (lihat Trend Micro Deep Security)
Manajeme perubahan	Aplikasi dan akun Inti	Konsol dan API AMS RFC dihapus Kebijakan kontrol layanan kustom AMS (SCPs) yang berisi pembatasan akses tingkat akun terlepas selama offboarding akun Aplikasi, dan dihapus selama offboarding akun Core	Anda harus menggunakan AWS API bawaan untuk membuat sumber daya baru, mengubah sumber daya yang ada, atau memperbarui AWS CloudFormation tumpukan yang ada Pembatasan akses tidak lagi diberlakukan di tingkat akun melalui AMS yang disediakan SCPs	Pastikan bahwa peran pengguna menyediakan akses yang cukup untuk menggunakan AWS layanan Buat SCPs untuk memberikan batasan izin tingkat akun

Komponen	Jenis akun	Tindakan yang diambil untuk offboard	Dampak potensial	Tindakan pelanggan yang direkomendasikan
Gambar dan otomatisasi OS AMS untuk manajemen layanan	Aplikasi dan akun Inti	AMS tidak lagi menyediakan dukungan pada kustomisasi dan meluncuran skrip yang disertakan dalam AMS yang disediakan EC2 AMIs AMS yang disediakan EC2 AMIs tetap tersedia di akun offboard Anda Runbook Otomasi Systems Manager yang disediakan AMS tidak dibagikan dan tidak lagi tersedia untuk digunakan	Setelah offboarding, AMS disediakan AMIs diluncurkan dengan AWS CloudFormation send cfn-signal FAILURE karena dependensi yang hilang pada komponen AMS Proses operasional yang bergantung pada AMS yang disediakan runbook Systems Manager Automation mungkin gagal	Tinjau dan perbarui proses pembuatan atau operasional apa pun yang bergantung pada AMS yang disediakan AMIs atau runbook Otomasi Systems Manager
Infrastruktur layanan bersama	Akun inti	Akses AMS dihapus dan AMS tidak lagi mengelola komponen bersama, termasuk AMS Managed Active Directory AWS Transit Gateway, dan AWS Organizations	Kehilangan manajemen atas infrastruktur bersama	Setel ulang akses admin ke AMS Managed Active Directory dan asumsikan pengelolaan komponen layanan bersama

Komponen	Jenis akun	Tindakan yang diambil untuk offboard	Dampak potensial	Tindakan pelanggan yang direkomen dasikan
Pelaporan	Aplikasi dan akun Inti	AMS tidak lagi mengumpulkan detail akun atau tingkat sumber daya untuk pelaporan agregat	Hilangnya wawasan tentang metrik operasional dan bisnis (cakupan cadangan dan penambalan, manajemen perubahan, dan aktivitas insiden)	Ganti pelaporan data agregat yang diperlukan di seluruh akun dengan solusinya sendiri
Tim akun AMS dan meja layanan	Aplikasi dan akun Inti	Tim akun AMS (CSDM, CA) dan meja layanan operasi AMS tidak lagi mendukung akun offboard	Hilangnya dukungan operasional dengan keahlian dalam arsitektur landing zone multi-akun yang dirancang AMS dan komponen terkait	Pastikan bahwa ada personel yang memadai dan keakraban dengan struktur akun dan sumber daya untuk mendukung operasi di lingkungan

Alternatif Akses

Berikut ini adalah metode alternatif untuk mempertahankan akses ke EC2 tumpukan Anda setelah Anda melepaskan akun AMS:

- Gunakan Pengelola Sesi untuk mengakses EC2 instance dengan izin yang ditinggikan tanpa memerlukan benteng atau akses jaringan masuk. Untuk informasi selengkapnya, lihat [AWS Systems Manager Session Manager](#).
- Bergabunglah kembali EC2 instance ke domain Active Directory yang berbeda dengan kredensi domain baru. Jika Anda menggunakan AWS Directory Service, lihat [Menggabungkan EC2 instance ke AWS Managed Microsoft AD direktori Anda](#).
- Gunakan akun pengguna lokal yang Anda buat melalui salah satu metode akses lain atau melalui [AWS Systems Manager Run Command](#).

Nonaktifkan skrip EC2 peluncuran AMS

Sistem operasi Linux

Gunakan manajer paket distribusi Anda untuk menghapus instalasi `ams-modules` paket. Misalnya, untuk Amazon Linux 2 gunakan `remove ams-modules`.

Sistem operasi Windows

Untuk menonaktifkan skrip EC2 peluncuran di Windows, selesaikan langkah-langkah berikut:

1. Windows Server 2008/2012/2012r2/2016/2019:

Menonaktifkan atau menghapus tugas terjadwal Managed Services Startup dari Task Scheduler. Untuk membuat daftar tugas terjadwal, jalankan `Get-ScheduledTask -TaskName '*Ec2*'` perintah.

Server Windows 2022:

Hapus [tugas EC2 Launch v2](#). Tugas ini berjalan `Initialize-AMSBoot` secara bertahap di `postReady` `C:\AmazonProgramData\EC2 Launch\config\agent-config.yml` pada instance. Berikut ini adalah cuplikan dari sebuah contoh: `agent-config.yml`

```
{
  "task": "executeScript",
  "inputs": [
    {
      "frequency": "always",
      "type": "powershell",
      "runAs": "localSystem"
    }
  ]
}
```

2. (Opsional) Hapus isi file berikut:

```
C:\Program Files\WindowsPowerShell\Modules\AWSManagedServices.*
C:\Windows\System32\WindowsPowerShell\v1.0\Modules
\AWSManagedServices.Build.Utilities\*
```

PBIS Open/Enterprise (Jembatan AD)

Untuk menentukan apakah Anda menggunakan edisi PBIS Open atau PBIS Enterprise (AD Bridge), jalankan perintah berikut dalam instance yang EC2 dikelola Linux:

```
yum info | grep pbis
```

Berikut ini adalah contoh output yang menunjukkan PBIS Enterprise (AD Bridge):

```
Name      : pbis-enterprise
From repo  : pbise
Name      : pbis-enterprise-devel
Repo      : pbise
Description : The pbis-enterprise-devel package includes the development
```

PBIS Terbuka

PBIS Open adalah produk usang yang BeyondTrust tidak lagi mendukung. Untuk informasi selengkapnya, lihat dokumentasi [BeyondTrust pbis-open](#).

Jembatan AD (Perusahaan PBIS)

Anda dapat melakukan salah satu hal berikut:

- Perbarui lisensi dan lanjutkan pengoperasian AD Bridge. Hubungi BeyondTrust untuk mendiskusikan lisensi dan dukungan.
- Hentikan penggunaan AD Bridge. Jalankan perintah Shell berikut untuk menghapus paket PBIS-Enterprise dari instance yang dikelola Linux. Untuk informasi selengkapnya, lihat BeyondTrust dokumentasi [Tinggalkan Domain dan Hapus Instalasi Agen Jembatan AD](#).

```
$ sudo /opt/pbis/bin/uninstall.sh purge
```

Tinggalkan domain Active Directory yang dikelola AMS tanpa menghapus agen PBIS

Anda memiliki opsi untuk meninggalkan Direktori Aktif terkelola AMS tanpa menghapus agen PBIS. Gunakan salah satu solusi berikut, tergantung pada sistem operasi Anda:

Linux operating systems

Gunakan PBIS dari AD terkelola AMS untuk menjalankan perintah shell berikut untuk berhenti bergabung dengan instance Linux EC2 . Untuk informasi selengkapnya, lihat dokumentasi [BeyondTrust pbis-open](#) atau [BeyondTrust AD Bridge](#), tergantung pada versi yang Anda gunakan.

```
$ sudo /opt/pbis/bin/domainjoin-cli leave
```

Anda mungkin melihat pesan kesalahan yang mirip dengan berikut ini:

```
Error: LW_ERROR_KRB5_REALM_CANT_RESOLVE [code 0x0000a3e1]  
Cannot resolve network address for KDC in requested realm
```

Jika kesalahan ini terjadi, maka jalankan perintah berikut untuk menghapus registri penyedia AD dan memulai ulang lwsmd layanan:

```
$ /opt/pbis/bin/regshell dir '[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers  
\ActiveDirectory\DomainJoin]'
```

Gunakan output ID direktori yang Anda terima dari perintah sebelumnya (misalnya, **A123EXAMPLE.AMAZONAWS.COM**) untuk menjalankan perintah berikut:

```
$ /opt/pbis/bin/regshell delete_tree \  
'[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin  
\DIRECTORYID]'
```

```
$ /etc/pbis/redhat/lwsmd restart
```

```
$ /opt/pbis/bin/lwsm restart lwreg
```

Windows operating systems

```
# Collect hostname and domain name using:  
  
Test-ComputerSecureChannel -verbose  
  
# Disjoin computer from the domain:  
  
netdom remove hostname /domain:domain name /force
```

 Note

Pastikan untuk menonaktifkan atau menghapus tugas terjadwal Startup Managed Services seperti yang disebutkan di [Nonaktifkan skrip EC2 peluncuran AMS](#).

Trend Micro Deep Security

Gunakan salah satu opsi berikut untuk melanjutkan atau menghentikan penggunaan Trend Micro Deep Security:

Lanjutkan penggunaan

- (Jika offboarding seluruh MALZ) Setelah offboarding akun Core, sambungkan kembali akun Aplikasi offboard ke Trend Micro Deep Security Manager (DSM) yang ada dan pertahankan lisensi di akun Layanan bersama. Untuk informasi selengkapnya, lihat [Menambahkan akun AWS cloud](#) dan [Memeriksa informasi lisensi Anda](#).
 1. Masuk ke akun layanan bersama dan arahkan ke konsol Secrets Manager.
 2. Ambil kredensial admin konsol DSM yang disimpan di jalur. `/ams/eps/`
 3. Masuk ke konsol DSM di <https://dsm.sentinel.int>.
 4. Pilih Gunakan Peran Lintas Akun, lalu masukkan `arn:aws:iam::ACCOUNTID:role/mc_eps_cross_account_role`. Ganti ACCOUNTID dengan ID akun Aplikasi offboarded.
 5. Pilih Berikutnya.
 6. Tunggu beberapa menit hingga DSM memproses penemuan akun dan menunjukkan bahwa sinkronisasi berhasil.
- Sambungkan kembali akun Aplikasi offboard ke instalasi Trend Micro DSM baru. Untuk informasi selengkapnya, lihat [Mengaktifkan dan melindungi agen](#) dan [Aktifkan agen](#).
- Sambungkan kembali akun Aplikasi offboard ke Trend Micro Cloud One. Untuk informasi selengkapnya, lihat [Memigrasi dari Deep Security ke Workload Security](#) dan [Migrate dari DSM lokal](#).

Hentikan penggunaan

- Copot pemasangan Trend Micro Deep Security Agents dari akun Aplikasi offboard. Untuk informasi selengkapnya, lihat [Menghapus Instalasi Deep Security](#).

Ubah mode manajemen

AWS Managed Services (AMS) menggunakan mode manajemen perubahan untuk perubahan pagar pembatas di AMS Advanced. Mode manajemen perubahan membantu Anda mempertahankan standar operasional yang tinggi untuk lingkungan, dan untuk mengendalikan risiko dan mencegah dampak buruk. AMS Advanced memiliki mode berbeda yang memberikan tingkat kontrol dan risiko yang berbeda. Semua mode, kecuali mode yang dikelola pelanggan, dikelola oleh AMS. Berikut ini adalah mode manajemen perubahan yang tersedia:

- Mode RFC (sebelumnya mode CM Standar): Menyediakan sistem “permintaan untuk perubahan” (RFC) dan jenis perubahan kustom AMS () CTs
- Mode Perubahan Langsung: Sama seperti mode RFC ditambah penggunaan AWS APIs dan konsol untuk membuat sumber daya yang dikelola AMS
- AWS Service Catalog di AMS: Mirip dengan mode Direct Change, tetapi alih-alih menggunakan sistem manajemen perubahan AMS (RFCs), Anda menggunakan AWS Service Catalog untuk membuat sumber daya yang kemudian dikelola AMS.
- Mode pengembang: Sama seperti mode Perubahan Langsung, hanya sumber daya yang Anda buat dengan AWS APIs dan konsol yang tidak dikelola AMS—Anda bertanggung jawab atas pengelolaannya
- Mode Penyediaan Layanan Mandiri (SSP): Sama seperti mode Pengembang kecuali tidak ada akses ke sistem manajemen perubahan AMS (tidak) RFCs
- Mode Terkelola Pelanggan: AMS memberi Anda landing zone multi-akun tetapi semua manajemen sumber daya adalah tanggung jawab Anda

Sistem manajemen perubahan AWS Managed Services (AMS), menggunakan Change Management (CM) API, menyediakan operasi untuk membuat dan mengelola request for change (RFCs) untuk akun multi-account landing zone (MALZ) dan single-account landing zone (SALZ).

Permintaan untuk perubahan (RFC) adalah permintaan yang dibuat oleh Anda atau AMS melalui antarmuka AMS untuk membuat perubahan pada lingkungan terkelola Anda dan menyertakan ID tipe perubahan (CT) untuk operasi tertentu.

AMS change management (CM) API menyediakan operasi untuk membuat dan mengelola permintaan untuk change (RFCs). Anda dapat membuat, memperbarui, mengirimkan, menyetujui, menolak, dan membatalkan. RFCs Operator AMS dapat membuat, memperbarui, mengirimkan, menyetujui, menolak, membatalkan, dan menandai RFCs sebagai ditutup.

Untuk daftar awalan cadangan AMS yang tidak digunakan dalam tag atau nama lain, lihat [Awalan cadangan](#).

Untuk informasi tentang setiap jenis perubahan, termasuk skema dan contoh, lihat [Referensi Jenis Perubahan AMS](#).

 Note

Semua panggilan API manajemen perubahan direkam di AWS CloudTrail. Untuk informasi selengkapnya, lihat [Mengakses log Anda](#).

Ikhtisar mode

Gunakan informasi ini untuk membantu Anda memilih mode AWS Managed Services (AMS) yang sesuai untuk hosting aplikasi Anda, berdasarkan kombinasi fleksibilitas dan tata kelola preskriptif yang Anda inginkan untuk mencapai hasil bisnis Anda.

Audiens yang dituju untuk informasi ini adalah:

- Tim pelanggan yang bertanggung jawab atas strategi dan tata kelola landing zone mereka. Informasi ini akan membantu tim menyusun fondasi landing zone yang dikelola AMS, dengan mode AMS yang ingin mereka tawarkan kepada pelanggan internal dan eksternal mereka.
- Pemilik bisnis dan aplikasi ditugaskan untuk memigrasikan aplikasi mereka ke AMS. Informasi ini akan membantu merencanakan migrasi aplikasi, dengan mode AMS yang sesuai untuk aplikasi migrate/host mereka. Catatan, aplikasi yang sama dapat di-host di lebih dari satu mode AMS selama fase siklus hidup Siklus Hidup Pengembangan Perangkat Lunak (SDLC) yang berbeda.
- Mitra AMS bertugas membimbing pelanggan tentang berbagai opsi untuk membangun dan bermigrasi ke AMS.

Informasi ini paling berguna selama fase dasar menyiapkan platform yang dikelola AMS Anda, dan ketika Anda beralih dari fondasi ke fase migrasi perjalanan adopsi cloud Anda, tepat setelah orientasi ke AMS selesai dan Anda berfokus pada tata kelola dan operasi aplikasi.

Jenis mode dan akun di AMS

Mode AWS Managed Services (AMS) dapat didefinisikan sebagai cara berinteraksi dengan layanan AMS di bawah kerangka tata kelola khusus untuk setiap mode. Perbedaan landing zone, multi-account landing zone atau MALZ dan single-account landing zone atau SALZ dicatat.

Note

Untuk detail tentang penerapan aplikasi dan memilih mode AMS yang tepat, lihat [mode AMS dan aplikasi atau beban kerja](#).

Untuk kasus penggunaan dunia nyata dari berbagai mode, lihat [Kasus penggunaan dunia nyata untuk mode AMS](#)

Tabel berikut memberikan deskripsi mode per layanan AMS.

Fitur AMS	Mode RFC (sebelumnya mode CM Standar) / OOD *	Mode Ubah Langsung	AWS Service Catalog	Penyediaan layanan mandiri/Mode pengembang	Pelanggan Dikelola
Konfigurasi Zona Pendaratan	MALZ dan SALZ	MALZ dan SALZ		MALZ dan SALZ	
Manajemen Perubahan	Mengubah penjadwalan, meninjau perubahan manual, dan mengubah catatan	Sama seperti mode RFC untuk perubahan berisiko tinggi seperti IAM atau grup keamanan		Tidak ada	
Logging, Monitorin	Ya (sumber daya yang didukung)			Tidak	

Fitur AMS	Mode RFC (sebelumnya mode CM Standar) / OOD *	Mode Ubah Langsung	AWS Service Catalog	Penyediaa n layanan mandiri/Mode pengembang	Pelanggan Dikelola
g, Guardrails, dan Manajemen Acara					
Manajemen kontinuitas	Ya (sumber daya yang didukung)			Tidak berlaku/Tidak	Tidak
Manajemen keamanan	Kontrol keamanan tingkat instans dan kontrol tingkat akun			Kontrol tingkat akun	Kontrol tingkat AWS Org
Manajemen tambalan	Ya			Tidak berlaku/Tidak	Tidak
Insiden dan manajemen masalah	Respons dan resolusi SLA untuk sumber daya yang didukung AMS			Respon SLA untuk sumber daya yang dihasilkan	Tidak
Pelaporan	Ya			Tidak	
Manajemen permintaan layanan	Ya			Hanya permintaan Support	Tidak

* Operations On Demand (OOD) memiliki penawaran untuk pelanggan yang menggunakan mode RFC untuk mengelola perubahan mereka melalui sumber daya khusus. Untuk detail selengkapnya, lihat [katalog penawaran Operations on Demand dan hubungi](#) manajer pengiriman layanan cloud (CSDM) Anda.

Note

[Mode Penyediaan Layanan Mandiri di AMS](#) dan [Mode Pengembang AMS Lanjutan](#) mungkin keduanya tampak cocok untuk aplikasi yang memiliki arsitektur kompleks yang berakar pada Layanan AWS asli. Saat merancang beban kerja, Anda membuat trade-off antara keunggulan operasional dan kelincahan, berdasarkan konteks bisnis Anda. Ini adalah cara yang baik untuk berpikir tentang memilih mode SSP atau mode Pengembang untuk aplikasi Anda. Pemilihan juga dapat berubah berdasarkan fase SDLC aplikasi. Misalnya: Ketika aplikasi siap produksi, maka mode SSP mungkin opsi yang lebih tepat karena pagar pembatas AMS yang lebih ketat dalam mode ini. Pagar pembatas diberlakukan dalam bentuk kontrol pencegahan seperti kontrol perubahan berbasis RFC untuk pembaruan IAM dan pada tingkat OU aplikasi. SCPs Keputusan bisnis ini dapat mendorong prioritas rekayasa Anda. Anda dapat mengoptimalkan untuk meningkatkan fleksibilitas bagi pemilik aplikasi dalam fase “pra-prod” dengan mengorbankan tata kelola dan dukungan operasional.

Arsitektur MALZ dan mode AMS terkait

AMS multi-account landing zone (MALZ) memberi Anda opsi untuk secara otomatis menyediakan akun aplikasi (atau akun sumber daya) di bawah Unit Organisasi (OU) default: OU yang Dikelola Pelanggan, OU Terkelola, atau OU Pengembangan. Infrastruktur yang disediakan dalam akun aplikasi yang dibuat di bawah masing-masing OUs ini tunduk pada mode AMS spesifik yang ditawarkan oleh yayasan tersebut. OUs Adalah umum untuk menemukan campuran dua atau lebih mode di akun aplikasi yang sama. Misalnya: Mode RFC dan mode SSP dapat hidup berdampingan dalam akun terkelola AMS yang menghosting arsitektur pipeline yang terdiri dari API Gateway dan Lambda untuk fungsi pemicu, dan, S3 EC2, dan SQS untuk konsumsi dan orkestrasi. Dalam hal ini, mode SSP akan berlaku untuk Lambda dan API Gateway.

Gambar 1 menyajikan bagaimana mode yang berbeda ditawarkan melalui fondasi OUs di AMS. Saat meminta akun aplikasi baru di AMS, Anda harus memilih OU untuk akun tersebut.

Arsitektur MALZ dan mode AMS terkait

AMS memanfaatkan dasar OUs berdasarkan praktik terbaik AWS sebagai cara untuk mengelola akun secara logis menggunakan Kebijakan Kontrol Layanan (SCP). Ini berfungsi sebagai cara untuk menegakkan kerangka tata kelola dengan setiap mode AMS. Setiap tata kelola dan pagar pembatas keamanan (dalam bentuk SCPs) yang diterapkan pada yayasan OUs juga diterapkan

secara otomatis. custom/child OUs Tambahan SCPs dapat diminta untuk anak OUs. Penting untuk dipahami bahwa akun aplikasi tidak sama dengan mode. Mode diterapkan pada infrastruktur yang disediakan dalam akun dan menentukan tanggung jawab operasional antara AMS dan pelanggan.

Gambar 1: Arsitektur MALZ dan mode AMS terkait

Note

“Pembatasan” menyiratkan bahwa Anda dapat meminta kebijakan khusus untuk ini OUs, kebijakan tersebut disetujui oleh AMS atas case-by-case dasar untuk memastikan kebijakan tersebut tidak mengganggu kemampuan AMS untuk memberikan keunggulan operasional. Untuk daftar rinci pagar pembatas AMS, lihat [AMS Guardrails](#) di panduan pengguna.

Mode dan aplikasi AMS atau beban kerja

Pertimbangkan persyaratan operasional dan tata kelola untuk aplikasi Anda saat memilih mode yang tepat, baik dengan meminta akun aplikasi baru atau menghosting aplikasi di akun aplikasi yang ada. Pemilihan mode AMS yang sesuai untuk setiap aplikasi atau beban kerja tergantung pada faktor-faktor berikut:

- Jenis fungsi siklus hidup SDLC yang akan disediakan lingkungan (misalnya, kotak pasir dengan perubahan yang tidak dimoderasi, UAT dengan beberapa perubahan yang sering, produksi dengan perubahan minimal dan sangat diatur)
- Kebijakan tata kelola yang diperlukan (ditegakkan melalui SCPs di tingkat OU)
- Model Operasional (jika Anda ingin memiliki tanggung jawab operasional atau ingin mengalihdayakannya ke AMS)
- Hasil bisnis yang diinginkan, seperti waktu untuk beroperasi di cloud, dan biaya operasi.

Note

Untuk deskripsi jenis mode per layanan AMS, lihat [Jenis mode dan akun di AMS](#). Untuk kasus penggunaan dunia nyata dari berbagai mode, lihat [Kasus penggunaan dunia nyata untuk mode AMS](#)

Tabel berikut menguraikan pertimbangan utama bagi pemilik aplikasi untuk membantu memutuskan mode AMS yang paling sesuai. Pemilik aplikasi harus menyertakan fase penilaian sebelum migrasi aplikasi untuk sepenuhnya memahami mode mana yang berlaku untuk aplikasi spesifik mereka. Contoh: Untuk aplikasi berbasis layanan cloud-native atau arsitektur tanpa server, opsi terbaik adalah mulai membangun dan mengulangi dalam mode Pengembang dan menerapkan Infrastruktur akhir sebagai Kode menggunakan mode AMS Managed — SSP. Dalam hal ini, pemfaktoran ulang ringan mungkin diperlukan untuk memastikan bahwa CloudFormation templat apa pun yang dibuat untuk penerapan otomatis memenuhi pedoman konsumsi yang ditetapkan oleh AMS. Selain itu, izin IAM apa pun harus disetujui oleh AMS Security untuk memastikan mereka mengikuti model hak istimewa paling sedikit.

Mode AMS yang dipilih untuk meng-host aplikasi, dapat membantu Anda membangun model operasi cloud yang Anda inginkan.

Note

Lebih dari satu model operasi cloud dapat ada dalam satu Zona Pendaratan Terkelola AMS berdasarkan berbagai mode AMS yang dipilih untuk meng-host aplikasi.

Masalah keputusan	Mode CM standar/OD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaa n layanan mandiri	Mode pengembangan	Pelanggan Dikelola

Kesiapan operasional

Logging, Monitoring dan Manajemen Acara	AMS bertanggung jawab atas semua infrastruktur yang dikelola	Pelanggan yang bertanggung jawab atas Layanan Penyediaa n Layanan Mandiri (SSP)	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembangan di luar	Pelanggan yang bertanggung jawab

Masalah keputusan	Mode CM standar/OD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaa n layanan mandiri	Mode pengembangan	Pelanggan Dikelola
					sistem AMS CM	
Manajemen Kontinuitas	Tanggung jawab AMS untuk melaksanakan rencana cadangan yang dipilih oleh pelanggan			Pelanggan yang bertanggung jawab atas Layanan Penyediaa n Layanan Mandiri (SSP)	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembangan di luar sistem AMS CM	
Manajemen Akses Tingkat Instans	Dikelola AMS melalui kepercayaan AD satu arah dengan domain on-prem. Memerlukan infrastruktur terkelola untuk bergabung dengan domain AMS			Tidak berlaku	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembangan di luar sistem AMS CM	

Masalah keputusan	Mode CM standar/OD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaa n layanan mandiri	Mode pengembangan	Pelanggan Dikelola
Manajemen Keamanan dan Manajemen Akses Tingkat Akun	Tanggung jawab AMS untuk semua akun terkelola			AMS bertanggung jawab atas semua akun yang dikelola	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembangan di luar sistem AMS CM	
Manajemen Patch	Tanggung jawab AMS untuk semua akun terkelola			Pelanggan yang bertanggung jawab atas Layanan Penyediaa n Layanan Mandiri (SSP)	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembangan di luar sistem AMS CM	

Masalah keputusan	Mode CM standar/OD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaa n layanan mandiri	Mode pengembangan	Pelanggan Dikelola
Manajemen Perubahan	Tanggung jawab AMS untuk semua akun terkelola			Pelanggan yang bertanggung jawab atas Layanan Penyediaa n Layanan Mandiri (SSP)	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembangan di luar sistem AMS CM	
Manajemen Penyediaa n	Preskriptif dan standar untuk opsi penyediaa n yang ditawarkan di AMS	Fleksibil itas untuk langsung menggunak an AWS service API untuk AWS Service Catalog mengikuti standar preskriptif AMS	Fleksibil itas untuk langsung menggunak an AWS service API mengikuti standar preskriptif AMS	Fleksibil itas untuk langsung menggunak an layanan AWS APIs untuk layanan SSP	Fleksibil itas untuk langsung menggunak an AWS service API untuk penyediaa n	

Masalah keputusan	Mode CM standar/OD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaa n layanan mandiri	Mode pengembangan	Pelanggan Dikelola
Manajemen Insiden dan Audit	Tanggung jawab AMS untuk semua akun terkelola				Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembangan di luar AMS Change Management System	
GuardRails Infrastruktur Bersama (Jaringan) dan Kerangka Keamanan	Memanfaatkan Akun Inti AMS yang preskriptif dan standar					Memanfaat kan Akun Inti AMS yang fleksibel dan dipesan lebih dahulu
Kesiapan aplikasi						

Masalah keputusan	Mode CM standar/OD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembangan	Pelanggan Dikelola
Aplikasi refactoring	Diperlukan refactoring ringan				Diperlukan refactoring ringan (jika disediakan menggunakan AMS Standard CM)	Tidak perlu refactoring
Support untuk layanan AWS	Terbatas pada apa yang didukung oleh AMS					Tidak terbatas
Pertimbangan bisnis						
Saatnya kesiapan operasional	Tiga sampai enam bulan			6 bulan+tergantung pada kompetensi operasi aplikasi pelanggan		6-18 bulan tergantung pada infrastruktur pelanggan dan kompetensi operasi aplikasi
Biaya	\$\$\$\$			\$\$\$	\$\$	\$

Masalah keputusan	Mode CM standar/OD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembangan	Pelanggan Dikelola
Contoh aplikasi	Server web dengan tumpukan 3 tingkat, aplikasi dengan kepatuhan dan persyaratan peraturan			Server web menggunakan API Gateway, aplikasi kontainer yang memanfaatkan ECS/EKS	Mengiterasi/mengoptimalkan aplikasi Data Lake yang menggunakan Lambda, Glue, Athena, dll	De-sentralisasi accounts/applications seperti kotak pasir, aplikasi yang dikelola pihak ketiga

* Operations On Demand (OOD) memiliki penawaran untuk pelanggan yang menggunakan mode CM Standar untuk mengelola perubahan mereka melalui sumber daya khusus. Untuk detail selengkapnya, lihat [katalog penawaran Operations on Demand dan hubungi](#) manajer pengiriman layanan cloud (CSDM) Anda.

Note

Perbandingan harga antara mode SSP dan mode Pengembang mengasumsikan bahwa layanan AWS yang sama disediakan.

Membandingkan Mode AMS dengan tujuan bisnis dan TI

Seperti yang ditunjukkan, jika Anda mencari model tata kelola yang sangat terkontrol dan terstandarisasi untuk aplikasi Anda, maka mode Perubahan Standar yang dikelola AMS, AWS Service Catalog, atau Direct Change adalah yang paling cocok. Jika Anda memerlukan model tata kelola yang dipesan lebih dahulu dengan fokus pada inovasi aplikasi tanpa perlu kesiapan operasional, pilih mode Customer Managed. Dengan mode Customer Managed, Anda bisa membutuhkan waktu lebih lama untuk mengoperasikan aplikasi Anda karena Anda memikul tanggung jawab untuk menetapkan orang, proses, dan alat untuk mendukung kemampuan

operasional seperti Manajemen Insiden, Manajemen Konfigurasi, Manajemen Penyediaan, Manajemen Keamanan, Manajemen Patch, dll.

Kasus penggunaan dunia nyata untuk mode AMS

Periksa ini untuk membantu menentukan cara menggunakan mode AMS.

- Gunakan Kasus 1, keharusan bisnis untuk menurunkan biaya dengan keluar pusat data yang sensitif terhadap waktu: Perusahaan dengan acara bisnis yang menarik, seperti pintu keluar pusat data, tertarik untuk menghosting ulang aplikasi on-prem mereka di cloud. Sebagian besar inventaris on-prem terdiri dari server Windows dan Linux dengan campuran versi sistem operasi. Dengan melakukan itu, pelanggan juga ingin memanfaatkan penghematan biaya yang pindah ke penawaran cloud dan meningkatkan postur teknis dan keamanan aplikasi mereka. Pelanggan ingin bergerak cepat tetapi belum memiliki keahlian operasi cloud internal yang dibangun. Pelanggan harus menemukan keseimbangan refactoring, terlalu banyak refactoring dapat berisiko terhadap garis waktu yang ketat. Namun, dengan beberapa refactoring, seperti memperbarui versi OS dan mengoptimalkan database, aplikasi dapat mencapai tingkat kinerja berikutnya. Dalam contoh ini, pelanggan dapat memilih mode RFC yang dikelola AMS untuk meng-host kembali sebagian besar aplikasi mereka. AMS menyediakan operasi infrastruktur, sekaligus memandu tim operasi pelanggan tentang praktik terbaik dalam pengoperasian cloud dengan aman.

AWS Service Catalog yang dikelola AMS dan mode Perubahan Langsung yang dikelola AMS memberi pelanggan fleksibilitas ekstra sambil mencapai hasil dan sasaran bisnis yang sama. Selain itu, pelanggan dapat menggunakan penawaran AMS Operations On Demand (OOD) untuk memiliki insinyur operasi AMS khusus untuk memprioritaskan pelaksanaan permintaan perubahan (RFCs).

Saat membongkar tugas operasional infrastruktur yang tidak terdiferensiasi (patching, backup, manajemen akun, dll) ke AMS, pelanggan dapat terus fokus pada pengoptimalan aplikasi mereka dan meningkatkan tim internal mereka pada operasi cloud. AMS memberikan laporan bulanan kepada pelanggan tentang penghematan biaya, dan membuat rekomendasi tentang pengoptimalan sumber daya. Dalam kasus penggunaan ini, jika ada end-of-life aplikasi yang di-host pada versi OS lama seperti Windows 2003 dan 2008, bahwa pelanggan memutuskan untuk tidak memfaktorkan ulang, itu juga dapat dimigrasikan ke AMS dan dihosting di akun yang memanfaatkan mode Dikelola Pelanggan.

- Gunakan Kasus 2, membangun data lake dengan Lambda, Glue, Athena dalam batas AMS yang aman: Perusahaan ingin menyiapkan Data Lake untuk memenuhi kebutuhan pelaporan untuk beberapa aplikasi di AMS. Pelanggan ingin menggunakan bucket S3 untuk penyimpanan

kumpulan data dan AWS Athena untuk melakukan kueri terhadap kumpulan data untuk setiap laporan. S3 dan AWS Athena akan digunakan di akun AMS Managed terpisah. Akun dengan S3 juga memiliki layanan lain seperti Glue, Lambda, dan Step Functions untuk membangun pipeline konsumsi data. Glue, Lambda, Athena, dan Step Functions dianggap sebagai layanan Penyediaan Layanan Mandiri (SSP) dalam hal ini. Pelanggan juga menyebarkan EC2 instance di akun yang bertindak sebagai server ad hoc tooling/scripting . Pelanggan memulai dengan meminta AMS untuk mengaktifkan layanan SSP di akun AMS Managed mereka. AMS memberikan peran IAM untuk setiap layanan yang dapat diasumsikan oleh pelanggan, setelah peran tersebut dimasukkan ke dalam solusi federasi pelanggan. Untuk kemudahan manajemen, pelanggan juga dapat menggabungkan kebijakan untuk peran IAM terpisah menjadi satu peran khusus, sehingga mengurangi kebutuhan untuk beralih peran saat bekerja di antara layanan AWS. Setelah peran diaktifkan di akun, pelanggan dapat mengonfigurasi layanan sesuai kebutuhan mereka. Namun, pelanggan harus bekerja dengan sistem manajemen perubahan AMS untuk meminta izin tambahan, tergantung pada kasus penggunaannya.

Misalnya, untuk akses ke Glue Crawler, izin tambahan diperlukan oleh Glue. Izin tambahan juga akan diperlukan untuk membuat sumber acara untuk Lambda. Pelanggan akan bekerja dengan AMS untuk memperbarui peran IAM guna memungkinkan akses lintas akun bagi Athena untuk menanyakan bucket S3. Pembaruan untuk peran layanan atau peran terkait layanan juga akan diperlukan melalui manajemen perubahan AMS agar Lambda memanggil layanan Step Functions, dan Glue untuk membaca dan menulis ke semua bucket S3. AMS bekerja dengan pelanggan untuk memastikan bahwa model akses hak istimewa paling sedikit diikuti dan perubahan IAM yang diminta tidak terlalu permisif dan membuka lingkungan terhadap risiko yang tidak perlu. Tim data lake pelanggan menghabiskan waktu merencanakan semua izin IAM yang diperlukan untuk layanan khusus untuk arsitektur pelanggan dan meminta AMS untuk mengaktifkannya. Ini karena semua perubahan IAM diproses secara manual dan menjalani peninjauan dari tim AMS Security. Waktu untuk memproses permintaan ini harus diperhitungkan dalam jadwal penerapan aplikasi.

Karena layanan SSP beroperasi di akun, pelanggan dapat meminta dukungan dan melaporkan masalah melalui manajemen insiden AMS dan permintaan layanan. Namun, AMS tidak akan secara aktif memantau metrik kinerja dan konkurensi untuk Lambda, atau metrik pekerjaan untuk Glue. Adalah tanggung jawab pelanggan untuk memastikan pencatatan dan pemantauan yang tepat diaktifkan untuk layanan SSP. EC2 Instance dan bucket S3 di akun dikelola sepenuhnya oleh AMS.

- Gunakan Kasus 3, penyiapan pipeline penerapan CI/CD yang cepat dan fleksibel di AMS: Seorang pelanggan ingin menyiapkan pipeline CI/CD berbasis Jenkins untuk menyebarkan pipeline kode ke semua akun aplikasi di AMS. Pelanggan mungkin merasa paling cocok untuk meng-host pipeline

CICD ini dalam mode Perubahan Langsung (DCM) yang dikelola AMS atau mode Pengembang yang dikelola AMS karena memberi mereka fleksibilitas untuk mengatur server Jenkins dengan konfigurasi khusus yang diperlukan EC2, dengan izin IAM yang diinginkan untuk mengakses dan ember S3 yang menampung repositori artefak. CloudFormation Meskipun ini juga dapat dilakukan dalam mode RFC yang dikelola AMS, tim pelanggan perlu membuat beberapa manual untuk peran IAM RFCs untuk mengulangi set izin yang disetujui yang paling tidak permisif, yang ditinjau secara manual oleh AMS. DCM memungkinkan pelanggan untuk mencapai tujuan operasional mereka di AWS sambil menghindari kebutuhan untuk membuat beberapa manual RFCs untuk peran IAM, saat menggunakan mode RFC yang dikelola AMS, untuk mengulangi serangkaian izin yang disetujui yang paling tidak permisif, yang ditinjau secara manual oleh AMS. Ini akan membutuhkan waktu serta pendidikan di pihak pelanggan untuk meningkatkan proses dan alat AMS. Bekerja dengan mode Pengembang, pelanggan dapat memulai dengan “peran pengembang” untuk menyediakan infrastruktur menggunakan AWS asli APIs. Cara tercepat dan paling fleksibel untuk mengatur pipeline ini adalah dengan menggunakan mode AMS Managed-Developer. Mode pengembang memberikan cara tercepat dan termudah, sambil mengorbankan integrasi operasional, sementara DCM kurang fleksibel tetapi memberikan tingkat dukungan operasional yang sama dengan mode RFC.

- Gunakan Kasus 4, model operasi yang dipesan lebih dahulu dalam yayasan AMS: Seorang pelanggan melihat keluar pusat data berdasarkan tenggat waktu dan salah satu aplikasi perusahaan mereka sepenuhnya dikelola oleh MSP pihak ketiga, termasuk operasi aplikasi dan operasi infrastruktur. Dengan asumsi bahwa pelanggan tidak memiliki waktu dalam jadwal untuk memfaktorkan ulang aplikasi ini sehingga dapat dioperasikan oleh AMS, mode Customer Managed adalah opsi yang cocok. Pelanggan dapat memanfaatkan pengaturan otomatis dan cepat dari Zona Pendaratan yang dikelola AMS. Mereka dapat memanfaatkan manajemen akun terpusat yang mengontrol penjual akun dan konektivitas melalui akun jaringan terpusat. Ini juga menyederhanakan penagihan mereka dengan mengkonsolidasikan biaya untuk semua akun yang dikelola pelanggan melalui akun Pembayar AMS. Pelanggan memiliki fleksibilitas untuk mengatur model manajemen akses yang dipesan lebih dahulu dengan MSP terpisah dari manajemen akses standar yang digunakan untuk akun Terkelola AMS. Dengan cara ini, menggunakan mode Customer Managed, mereka dapat mengatur lingkungan yang dikelola AMS sambil memenuhi persyaratan bisnis mereka untuk mengosongkan lingkungan di prem mereka. Dalam hal ini, jika pelanggan juga memiliki aplikasi berbasis Windows yang mereka migrasi ke cloud, dan memilih untuk memindahkannya ke akun Customer Managed, pelanggan bertanggung jawab untuk membuat model operasi cloud. Ini bisa rumit, mahal, dan memakan waktu tergantung pada kemampuan pelanggan untuk mengubah proses TI tradisional dan melatih orang. Pelanggan dapat

menghemat waktu dan biaya dengan “mengangkat dan memindahkan” beban kerja tersebut ke akun AMS Managed dan menurunkan operasi infrastruktur ke AMS.

Note

Pelanggan terkadang merasa perlu untuk memindahkan akun aplikasi antara kerangka tata kelola mode RFC atau SSP dan mode Pengembang. Misalnya, pelanggan dapat meng-host aplikasi dalam mode terkelola AMS sebagai bagian dari migrasi lift and shift awal, tetapi lembur ingin menulis ulang aplikasi untuk mengoptimalkannya untuk layanan AWS cloud-native. Mereka dapat mengubah mode akun pra-prod dari RFC yang dikelola AMS ke mode Pengembang yang dikelola AMS, memberi mereka fleksibilitas dan kelincahan untuk penyediaan infrastruktur. Namun, setelah perubahan penyediaan infrastruktur dibuat menggunakan “peran pengembang”, infrastruktur yang sama tidak dapat dipindahkan kembali ke mode RFC yang dikelola AMS. Ini karena AMS tidak dapat menjamin operasi infrastruktur yang disediakan di luar sistem manajemen perubahan AMS. Pelanggan mungkin perlu membuat akun aplikasi baru yang menawarkan mode RFC yang dikelola AMS dan kemudian menerapkan kembali konfigurasi infrastruktur yang “dioptimalkan” melalui CloudFormation templat atau kustom yang dimasukkan ke dalam akun yang dikelola AMS AMIs . Ini adalah cara bersih untuk menerapkan konfigurasi siap produksi. Setelah digunakan, aplikasi akan berada di bawah tata kelola dan operasi AMS preskriptif. Hal yang sama berlaku untuk beralih mode antara mode Customer Managed dan AMS-managed.

Modus RFC

Mode RFC adalah mode default untuk pelanggan rencana operasi AMS Advanced. Ini mencakup sistem manajemen perubahan dengan permintaan perubahan atau RFCs dan katalog jenis perubahan yang akan digunakan untuk meminta penambahan atau perubahan yang Anda butuhkan ke akun Anda. Sistem manajemen perubahan ini memberikan tingkat keamanan dalam membatasi siapa yang dapat melakukan perubahan pada akun Anda.

Untuk detail tentang jenis perubahan AMS Advanced, lihat [Apa itu Jenis Perubahan AMS?](#) .

Untuk detail tentang orientasi ke AMS Advanced, lihat [AWS Managed Services Onboarding Introduction](#).

Untuk contoh penelusuran jenis perubahan, lihat bagian “Informasi Tambahan” untuk jenis perubahan yang relevan di bagian AMS Advanced Change Type Reference Change Type [by Classification](#).

 Note

Mode RFC sebelumnya disebut “Mode Manajemen Ubah” atau “Mode CM Standar.”

Topik

- [Pelajari tentang RFCs](#)
- [Apa itu jenis perubahan?](#)
- [Memecahkan masalah kesalahan RFC di AMS](#)

Pelajari tentang RFCs

Permintaan perubahan, atau RFCs, bekerja dengan cara dua kali lipat. Pertama, ada parameter yang diperlukan untuk RFC itu sendiri. Ini adalah opsi di CreateRfc API. Dan kedua, ada parameter yang diperlukan untuk aksi RFC (parameter eksekusi). Untuk mempelajari CreateRfc opsi, lihat [CreateRfc](#) bagian Referensi AMS API. Opsi ini biasanya muncul di area Konfigurasi tambahan pada halaman Buat RFC.

Anda dapat membuat dan mengirimkan RFC dengan CreateRfc API, `aws amscm create-rfc` CLI, atau menggunakan konsol AMS Buat halaman RFC. Untuk tutorial tentang membuat RFC, lihat [Buat RFC](#).

Topik

- [Apa itu RFCs?](#)
- [Mengautentikasi saat menggunakan AMS API/CLI](#)
- [Memahami ulasan keamanan RFC](#)
- [Memahami klasifikasi tipe perubahan RFC](#)
- [Memahami tindakan RFC dan status aktivitas](#)
- [Memahami kode status RFC](#)
- [Memahami pembaruan RFC CTs dan deteksi drift CloudFormation template](#)
- [Jadwal RFCs](#)
- [Menyetujui atau menolak RFCs](#)

- [Minta periode berjalan terbatas RFC](#)
- [Buat, kloning, perbarui, temukan, dan batalkan RFCs](#)
- [Gunakan konsol AMS dengan RFCs](#)
- [Pelajari tentang parameter RFC umum](#)
- [Mendaftar untuk email harian RFC](#)

Apa itu RFCs?

Permintaan perubahan, atau RFC, adalah cara Anda membuat perubahan di lingkungan yang dikelola AMS, atau meminta AMS untuk membuat perubahan atas nama Anda. Untuk membuat RFC, Anda memilih dari jenis perubahan AMS, pilih parameter RFC (seperti jadwal), lalu kirimkan permintaan menggunakan konsol AMS atau perintah [CreateRfc](#) API dan [SubmitRfc](#).

RFC berisi dua spesifikasi, satu untuk RFC itu sendiri, dan satu untuk parameter tipe perubahan (CT). Pada baris perintah, Anda dapat menggunakan perintah Inline RFC, atau `CreateRfc` template standar dalam format JSON, yang Anda isi dan kirimkan bersama dengan file skema CT JSON yang Anda buat (berdasarkan parameter CT). Nama CT adalah deskripsi informal dari CT. CSIO (kategori, subkategori, item, operasi) adalah deskripsi yang lebih formal dari CT. Hanya ID CT yang harus ditentukan saat membuat RFC.

AMS memberi tahu Anda ketika perubahan telah berhasil diselesaikan (Sukses) atau tidak berhasil (Kegagalan).

Note

Untuk informasi tentang pemecahan masalah kegagalan RFC, lihat [Memecahkan masalah kesalahan RFC di AMS](#)

Grafik berikut menggambarkan alur kerja RFC yang dikirimkan oleh Anda.

Mengautentikasi saat menggunakan AMS API/CLI

Saat Anda menggunakan AMS API/CLI, Anda harus mengautentikasi dengan kredensi sementara. Untuk meminta kredensial keamanan sementara untuk pengguna federasi, cal,, [AssumeRoleWithSALL](#) [GetFederationTokenAssumeRole](#), atau [AssumeRoleWithWebIdentity](#) AWS security token service (STS). APIs

Pilihan umum adalah SAFL. Setelah disiapkan, Anda menambahkan argumen ke setiap operasi yang Anda panggil. Sebagai contoh: `aws --profile saml amscm list-change-type-categories`.

Pintasan untuk profil SAFL 2.0 adalah mengatur variabel profil di awal masing-masing API/CLI dengan `set AWS_DEFAULT_PROFILE=saml` (untuk Windows; untuk Linux itu akan `export AWS_DEFAULT_PROFILE=saml`). Untuk informasi tentang menyetel variabel lingkungan CLI, lihat [Mengonfigurasi Antarmuka Baris Perintah AWS](#), Variabel Lingkungan.

Memahami ulasan keamanan RFC

Proses persetujuan manajemen perubahan AWS Managed Services (AMS) memastikan bahwa kami melakukan tinjauan keamanan terhadap perubahan yang kami buat di akun Anda.

AMS mengevaluasi semua permintaan untuk perubahan (RFCs) terhadap standar teknis AMS. Setiap perubahan yang mungkin menurunkan postur keamanan akun Anda dengan menyimpang dari standar teknis, akan melalui tinjauan keamanan. Selama tinjauan keamanan, AMS menyoroti risiko yang relevan dan, dalam kasus risiko keamanan tinggi atau sangat tinggi, petugas keamanan resmi Anda menerima atau menolak RFC. Semua perubahan juga dievaluasi untuk menilai dampak buruk pada kemampuan AMS untuk beroperasi. Jika potensi dampak buruk ditemukan, maka tinjauan dan persetujuan tambahan diperlukan dalam AMS.

Standar teknis AMS

Standar Teknis AMS menentukan kriteria keamanan minimum, konfigurasi, dan proses untuk menetapkan keamanan dasar akun Anda. Standar ini harus diikuti oleh AMS dan Anda.

Setiap perubahan yang berpotensi menurunkan postur keamanan akun Anda dengan menyimpang dari standar teknis, akan melalui proses Penerimaan Risiko, di mana risiko yang relevan disorot oleh AMS dan diterima atau ditolak oleh petugas keamanan yang berwenang dari pihak Anda. Semua perubahan tersebut juga dievaluasi untuk menilai apakah akan ada dampak buruk pada kemampuan AMS untuk mengoperasikan akun dan, jika demikian, ulasan dan persetujuan tambahan diperlukan dalam AMS.

Proses manajemen risiko keamanan pelanggan (CSRM) RFC

Ketika seseorang dari organisasi Anda meminta perubahan pada lingkungan terkelola Anda, AMS meninjau perubahan tersebut untuk menentukan apakah permintaan tersebut dapat memperburuk postur keamanan akun Anda dengan berada di luar standar teknis. Jika permintaan menurunkan

postur keamanan akun, AMS memberi tahu kontak tim keamanan Anda dengan risiko yang relevan, dan mengeksekusi perubahan; atau, jika perubahan tersebut menimbulkan risiko keamanan yang tinggi atau sangat tinggi di lingkungan, AMS meminta persetujuan eksplisit dari kontak tim keamanan Anda dalam bentuk penerimaan risiko (dijelaskan selanjutnya). Proses Penerimaan Risiko Pelanggan AMS dirancang untuk:

- Memastikan risiko diidentifikasi dan dikomunikasikan dengan jelas kepada pemilik yang tepat
- Minimalkan risiko yang teridentifikasi terhadap lingkungan Anda
- Mendapatkan dan mendokumentasikan persetujuan dari kontak keamanan yang ditunjuk yang memahami profil risiko organisasi Anda
- Mengurangi overhead operasional yang sedang berlangsung untuk risiko yang teridentifikasi

Cara mengakses standar teknis dan risiko tinggi atau sangat tinggi

Kami telah membuat dokumentasi Standar Teknis AMS tersedia untuk referensi Anda dalam <https://console.aws.amazon.com/artifact> sebagai laporan. Gunakan dokumentasi Standar Teknis AMS untuk memahami apakah perubahan akan memerlukan penerimaan risiko dari kontak keamanan resmi Anda sebelum mengirimkan permintaan perubahan (RFC).

Temukan laporan Standar Teknis dengan menelusuri “Standar Teknis AWS Managed Services (AMS)” di bilah pencarian tab AWS Artifact Laporan setelah masuk dengan default `AWSServiceCatalogChangeManagementRole`.

Note

Dokumen standar teknis AMS dapat diakses oleh `Customer_ReadOnly_Role` di landing zone akun tunggal. Di landing zone multi-akun, yang `AWSServiceCatalogAdminRole` digunakan oleh admin keamanan dan `AWSServiceCatalogChangeManagementRole` digunakan oleh tim aplikasi, dapat digunakan untuk mengakses dokumen. Jika tim Anda menggunakan peran kustom, buat `Other | Other RFC` untuk meminta akses dan kami akan memperbarui peran kustom yang ditentukan.

Memahami klasifikasi tipe perubahan RFC

Jenis perubahan yang Anda gunakan saat mengirimkan RFC dibagi menjadi dua kategori besar:

- **Deployment:** Klasifikasi ini untuk membuat sumber daya.

- **Manajemen:** Klasifikasi ini untuk memperbarui atau menghapus sumber daya. Kategori Manajemen juga berisi jenis perubahan untuk mengakses instance, mengenkripsi atau berbagi, dan memulai, menghentikan AMIs, me-reboot, atau menghapus tumpukan.

Memahami tindakan RFC dan status aktivitas

`RfcActionState`(API)/Status Aktivitas (konsol) membantu Anda memahami status intervensi manusia, atau tindakan, pada RFC. Digunakan terutama untuk manual RFCs, `RfcActionState` membantu Anda memahami kapan ada tindakan yang diperlukan oleh Anda atau operasi AMS, dan membantu Anda melihat kapan Operasi AMS secara aktif mengerjakan RFC Anda. Ini memberikan peningkatan transparansi ke dalam tindakan yang diambil pada RFC selama siklus hidupnya.

`RfcActionState`Definisi (API)/Status Aktivitas (konsol):

- `AwsOperatorAssigned`: Operator AWS secara aktif mengerjakan RFC Anda.
- `AwsActionPending`: Respons atau tindakan dari AWS diharapkan.
- `CustomerActionPendingRespons` atau tindakan dari pelanggan diharapkan.
- `NoActionPending`: Tidak ada tindakan yang diperlukan dari AWS atau pelanggan.
- `NotApplicable`: Status ini tidak dapat diatur oleh operator AWS atau pelanggan, dan hanya digunakan untuk RFCs yang dibuat sebelum fungsionalitas ini dirilis.

Status tindakan RFC berbeda tergantung pada apakah jenis perubahan yang dikirimkan memerlukan peninjauan manual dan penjadwalan disetel ke ASAP atau tidak.

- `ActionState`Perubahan RFC selama peninjauan, persetujuan, dan dimulainya jenis perubahan manual dengan penjadwalan yang ditangguhkan:
 - Setelah Anda mengirimkan manual, terjadwal, RFC, `ActionState` secara otomatis berubah `AwsActionPending` untuk menunjukkan bahwa operator perlu meninjau dan menyetujui RFC.
 - Ketika operator mulai secara aktif meninjau RFC Anda, `ActionState` perubahan menjadi `AwsOperatorAssigned`
 - Ketika operator menyetujui RFC Anda, Status RFC berubah menjadi Terjadwal, dan `ActionState` secara otomatis berubah menjadi `NoActionPending`
 - Ketika waktu mulai yang dijadwalkan dari RFC tercapai, Status RFC berubah menjadi `InProgress`, dan `ActionState` secara otomatis berubah `AwsActionPending` untuk menunjukkan bahwa operator perlu ditugaskan untuk meninjau RFC.

- Ketika operator mulai aktif menjalankan RFC, mereka mengubah ActionState ke `AwsOperatorAssigned`.
- Setelah selesai, Operator menutup RFC. Ini secara otomatis mengubah ActionState ke `NoActionPending`.

Important

- Status tindakan tidak dapat diatur oleh Anda. Mereka diatur secara otomatis berdasarkan perubahan dalam RFC, atau diatur secara manual oleh operator AMS.
- Jika Anda menambahkan korespondensi ke RFC, secara otomatis ActionState diatur ke `AwsActionPending`.
- Ketika RFC dibuat, secara otomatis ActionState diatur ke `NoActionPending`.
- Ketika RFC dikirimkan, secara otomatis ActionState diatur ke `AwsActionPending`.
- Ketika RFC Ditolak, Dibatalkan, atau dilengkapi dengan status Sukses atau Kegagalan, secara otomatis ActionState diatur ulang ke `NoActionPending`.
- Status tindakan diaktifkan untuk otomatis dan manual RFCs, tetapi sebagian besar penting untuk manual RFCs karena jenis tersebut RFCs sering memerlukan komunikasi.

Tinjau contoh kasus penggunaan status tindakan RFC

Kasus Penggunaan: Visibilitas pada Proses RFC Manual

- Setelah Anda mengirimkan RFC manual, status tindakan RFC secara otomatis berubah `AwsActionPending` untuk menunjukkan bahwa operator perlu meninjau dan menyetujui RFC. Ketika operator mulai secara aktif meninjau RFC Anda, status tindakan RFC berubah menjadi `AwsOperatorAssigned`.
- Pertimbangkan RFC manual yang telah disetujui dan dijadwalkan dan siap untuk mulai berjalan. Setelah status RFC berubah `InProgress`, status tindakan RFC secara otomatis berubah menjadi `AwsActionPending`. Ini berubah lagi menjadi `AwsOperatorAssigned` setelah operator mulai aktif menjalankan RFC.
- Ketika RFC manual selesai (ditutup sebagai “Sukses” atau “Kegagalan”), status Tindakan RFC berubah `NoActionPending` untuk menunjukkan bahwa tidak ada tindakan lebih lanjut yang diperlukan baik dari pelanggan atau operator.

Kasus penggunaan: korespondensi RFC

- Ketika RFC manual `Pending Approval`, Operator AMS mungkin memerlukan informasi lebih lanjut dari Anda. Operator akan memposting korespondensi ke RFC dan mengubah status tindakan RFC menjadi `CustomerActionPending` Saat Anda merespons dengan menambahkan korespondensi RFC baru, status tindakan RFC secara otomatis berubah menjadi `AwsActionPending`
- Ketika RFC otomatis atau manual gagal, Anda dapat menambahkan korespondensi ke detail RFC, menanyakan kepada Operator AMS mengapa RFC gagal. Ketika korespondensi Anda ditambahkan, status tindakan RFC secara otomatis diatur ke `AwsActionPending` Saat operator AMS mengambil RFC untuk melihat korespondensi Anda, status tindakan RFC berubah menjadi `AwsOperatorAssigned` Ketika operator merespons dengan menambahkan korespondensi RFC baru, status tindakan RFC dapat diatur `CustomerActionPending`, menunjukkan bahwa ada respons lain dari pelanggan yang diharapkan, atau `NoActionPending`, yang menunjukkan bahwa tidak ada respons dari pelanggan yang diperlukan atau diharapkan.

Memahami kode status RFC

Kode status RFC membantu Anda melacak permintaan Anda. Anda dapat mengamati kode status ini selama RFC berjalan di output CLI, atau dengan menyegarkan halaman daftar RFC di konsol.

Anda juga dapat melihat kode untuk RFC di halaman detail untuk RFC itu, yang mungkin terlihat seperti ini:

Anda mungkin melihat RFC dalam daftar yang tidak Anda kirimkan. Ketika operator AMS menggunakan CT internal saja, mereka mengirimkannya dalam RFC dan ditampilkan dalam daftar RFC Anda. Untuk informasi selengkapnya, lihat [Jenis perubahan hanya internal](#).

Important

Anda dapat meminta pemberitahuan perubahan status RFC. Untuk detailnya, lihat [Pemberitahuan Perubahan Status RFC](#).

Kode status RFC

Berhasil	Kegagalan
Pengeditan: RFC telah dibuat tetapi tidak dikirimkan	Ditolak: ditolak RFCs biasanya karena gagal validasi; misalnya, sumber daya yang tidak dapat digunakan, yaitu subnet, ditentukan
PendingApproval /Dikirim: RFC telah diserahkan dan sistem menentukan apakah memerlukan persetujuan, dan mendapatkan persetujuan itu, jika diperlukan	Dibatalkan: RFCs biasanya dibatalkan karena tidak lulus validasi sebelum waktu mulai yang dikonfigurasi berlalu
Disetujui oleh AWS/Disetujui oleh pelanggan : RFC telah disetujui. Otomatis RFCs disetujui oleh AWS, manual RFCs disetujui oleh Operator dan, terkadang, pelanggan	Kegagalan: RFC telah gagal; lihat output untuk alasan kegagalan, dan operasi AMS secara otomatis membuat tiket masalah dan berkomunikasi dengan Anda sesuai kebutuhan StatusReason
Dijadwalkan: RFC telah lulus sintaks dan pemeriksaan persyaratan dan dijadwalkan untuk berjalan	
InProgress: RFC sedang dijalankan, perhatikan RFCs bahwa penyediaan banyak sumber daya atau telah berjalan lama UserData, membutuhkan waktu lebih lama untuk dijalankan	
Dieksekusi: RFC telah dijalankan	
Sukses/Berhasil: RFC telah berhasil diselesaikan	

 Note

Dibatalkan atau ditolak RFCs dapat dikirimkan kembali menggunakan [UpdateRfc](#); lihat juga. [Perbarui RFCs](#)

Jika RFC melewati semua kondisi yang diperlukan (misalnya, semua parameter yang diperlukan ditentukan), status berubah menjadi PendingApproval (bahkan otomatis CTs memerlukan

persetujuan, yang terjadi secara otomatis jika sintaks dan pemeriksaan parameter lulus). Jika tidak lulus, statusnya berubah menjadi `Rejected`. `StatusReason` memberikan informasi tentang penolakan; `ExecutionOutput` bidang memberikan informasi tentang persetujuan dan penyelesaian. Kode kesalahan meliputi:

- `InvalidRfcStateException`: RFC berada dalam status yang tidak mengizinkan operasi yang dipanggil. Misalnya, jika RFC telah pindah ke status Kirim, itu tidak dapat lagi dimodifikasi.
- `InvalidRfcScheduleException`: `StartTime`, `EndTime`, atau `TimeoutInMinutes` parameter dilanggar.
- `InternalServerError`: Kesulitan dengan sistem ditemui.
- `InvalidArgumentException`: Parameter salah ditentukan; misalnya, nilai yang tidak dapat diterima digunakan.
- `ResourceNotFoundException`: Nilai, seperti ID tumpukan, tidak dapat ditemukan.

Jika waktu mulai dan akhir yang dijadwalkan yang diminta (juga dikenal sebagai jendela jalankan perubahan) terjadi sebelum perubahan disetujui, status RFC akan berubah menjadi `Canceled`. Jika perubahan disetujui, status RFC berubah menjadi `Scheduled`. Jendela change run untuk ASAP RFCs adalah waktu yang dikirimkan ditambah `ExpectedExecutionDuration` nilai untuk CT.

Kapan saja sebelum kedatangan jendela run perubahan, perubahan terjadwal (dikirimkan dengan a `RequestedStartTime` di CLI) dapat dimodifikasi atau dibatalkan. Jika perubahan yang dijadwalkan diubah, maka harus dikirimkan kembali.

Ketika waktu mulai perubahan tiba (dijadwalkan atau ASAP) dan setelah persetujuan selesai, status berubah `InProgress` dan tidak ada modifikasi yang dapat dilakukan. Jika perubahan selesai dalam jendela run perubahan yang ditentukan, status berubah menjadi `Success`. Jika ada bagian dari perubahan yang gagal, atau jika perubahan masih berlangsung saat jendela run change berakhir, status akan berubah menjadi `Failure`.

Note

Selama `InProgress`, `Success`, atau `Failure` mengubah status, RFC tidak dapat dimodifikasi atau dibatalkan.

Diagram berikut mengilustrasikan status RFC dari panggilan `CreateRFC` hingga resolusi.

Memahami pembaruan RFC CTs dan deteksi drift CloudFormation template

Sumber daya yang disediakan di AMS menggunakan templat yang dimodifikasi AWS CloudFormation . Jika sumber daya memiliki parameter yang diubah secara langsung melalui Konsol AWS Manajemen layanan, maka catatan CloudFormation pembuatan sumber daya tersebut menjadi tidak sinkron. Jika ini terjadi dan Anda mencoba menggunakan jenis perubahan pembaruan AMS untuk memperbarui sumber daya di AMS, AMS mereferensikan konfigurasi sumber daya asli dan berpotensi menyetel ulang parameter yang diubah. Reset ini mungkin merusak, jadi AMS melarang RFCs dengan jenis perubahan pembaruan jika ada perubahan konfigurasi AMS tambahan yang terdeteksi.

Untuk daftar jenis perubahan pembaruan, gunakan filter konsol.

Remediasi drift FAQs

Pertanyaan dan jawaban tentang remediasi drift AMS. Ada dua jenis perubahan yang dapat Anda gunakan untuk memulai remediasi drift, satu adalah mode eksekusi = manual atau “review required,” yang lainnya adalah mode eksekusi = otomatis.

Sumber daya yang didukung remediasi drift (ct-3kinq0u4l33zf)

Ini adalah sumber daya yang didukung oleh tipe perubahan remediasi drift, (ct-3kinq0u4l33zf).

Untuk perbaikan sumber daya apa pun, gunakan jenis perubahan “diperlukan tinjauan” (ct-34sxfo53yuzah) sebagai gantinya.

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
```



```
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

Jenis perubahan remediasi drift

Pertanyaan dan jawaban tentang penggunaan jenis perubahan remediasi drift AMS.

Untuk daftar sumber daya yang didukung untuk fitur remediasi drift, lihat. [Sumber daya yang didukung remediasi drift \(ct-3king0u4l33zf\)](#)

 Important

Remediasi drift memodifikasi and/or parameter template tumpukan dan wajib untuk memperbarui repositori template lokal Anda atau otomatisasi apa pun yang memperbarui tumpukan ini untuk menggunakan templat dan parameter tumpukan terbaru. Menggunakan and/or parameter template lama tanpa sinkronisasi dapat menyebabkan perubahan merusak pada sumber daya yang mendasarinya.

Tidak diperlukan tinjauan, otomatis, CT (ct-3king0u4l33zf) hanya mendukung remediasi 10 sumber daya per RFC. Untuk memulihkan sumber daya yang tersisa dalam batch 10 buat yang baru RFCs sampai semua sumber daya diperbaiki.

Jenis perubahan remediasi drift mana yang harus saya gunakan?

Kami merekomendasikan untuk menggunakan CT otomatis (ct-3king0u4l33zf) tanpa ulasan saat:

- Anda mencoba melakukan pembaruan ke sumber daya tumpukan yang ada menggunakan CT otomatis dan RFC ditolak sebagai tumpukan. DRIFTED
- Anda menggunakan Update CT di masa lalu dan gagal karena tumpukannya DRIFTED. Anda tidak perlu mencoba pembaruan lagi dan dapat menggunakan ulasan yang diperlukan, manual, CT sebagai gantinya.

Kami merekomendasikan penggunaan tinjauan yang diperlukan, CT manual (ct-34sxfo53yuzah) hanya jika jenis sumber daya yang hanyut tidak didukung oleh remediasi drift tidak diperlukan tinjauan, otomatis, CT (ct-3king0u4l33zf), atau ketika remediasi drift tidak diperlukan tinjauan, otomatis, CT gagal.

Perubahan apa yang dilakukan pada tumpukan selama remediasi?

Remediasi memerlukan pembaruan ke and/or parameter template tumpukan tergantung pada properti yang hanyut. Remediasi juga memperbarui kebijakan tumpukan tumpukan selama remediasi dan mengembalikan kebijakan tumpukan ke nilai sebelumnya setelah remediasi selesai.

Bagaimana kita bisa melihat perubahan yang dilakukan pada and/or parameter template tumpukan?

Dalam menanggapi RFC, ringkasan perubahan disediakan dengan informasi berikut:

- **ChangeSummaryJson:** Berisi ringkasan perubahan and/or Parameter Template Stack sebagai bagian dari remediasi drift. Remediasi dilakukan dalam beberapa fase. Ringkasan perubahan ini terdiri dari perubahan untuk fase individu. Jika Remediasi berhasil periksa perubahan fase terakhir. Lihat **ExecutionPlan** di JSON untuk fase yang dieksekusi secara berurutan. Misalnya, **RestoreReferences** bagian saat hadir selalu dieksekusi di akhir dan berisi JSON untuk perubahan pasca remediasi. Jika remediasi dijalankan dalam **DryRun** mode, tidak satu pun dari perubahan ini akan diterapkan ke tumpukan.
- **PreRemediationStackTemplateAndConfigurationJson:** Berisi snapshot konfigurasi CloudFormation Stack termasuk Template, Parameter, Output, StackPolicyBody sebelum remediasi dipicu pada tumpukan.

Apa yang harus saya lakukan setelah remediasi dilakukan?

Important

Anda perlu memperbarui repositori template lokal Anda, atau otomatisasi apa pun, yang akan memperbarui tumpukan yang diperbaiki, dengan templat dan parameter terbaru yang disediakan dalam ringkasan RFC. Hal ini sangat penting untuk melakukan ini karena menggunakan and/or parameter template lama dapat menyebabkan perubahan destruktif lebih lanjut pada sumber daya stack.

Apakah aplikasi saya akan diterapkan selama remediasi ini?

Remediasi adalah proses offline yang dilakukan hanya pada konfigurasi CloudFormation tumpukan. Tidak ada pembaruan yang dilakukan pada sumber daya yang mendasarinya.

Dapatkah saya terus menggunakan Manajemen | Lainnya | Lainnya RFCs untuk melakukan pembaruan sumber daya setelah perbaikan?

Kami menyarankan agar Anda selalu melakukan pembaruan untuk menumpuk sumber daya menggunakan Pembaruan otomatis yang tersedia CTs. Jika Pembaruan yang tersedia CTs tidak mendukung kasus penggunaan Anda, gunakan Manajemen | Lainnya | Permintaan lainnya.

Apakah remediasi membuat sumber daya baru di tumpukan?

Remediasi tidak membuat sumber daya baru di tumpukan. Namun, remediasi membuat output baru dan memperbarui bagian [metadata](#) template tumpukan untuk menyimpan ringkasan remediasi untuk referensi Anda.

Akankah remediasi selalu berhasil?

Remediasi memerlukan analisis dan validasi konfigurasi template yang cermat untuk menentukan apakah itu dapat dilakukan. Dalam skenario di mana validasi ini gagal, proses remediasi dihentikan dan tidak ada perubahan yang dilakukan pada template tumpukan atau parameter. Selain itu, remediasi hanya dapat dilakukan pada jenis sumber daya yang didukung.

Bagaimana saya bisa melakukan pembaruan untuk menumpuk sumber daya jika remediasi tidak berhasil?

Anda dapat menggunakan Manajemen | Lainnya | Lainnya | Perbarui CT (ct-0xdawir96cy7k) untuk meminta perubahan. AMS memantau skenario tersebut dan bekerja untuk meningkatkan solusi remediasi.

Dapatkah saya memulihkan tumpukan yang memiliki tipe sumber daya yang didukung dan tidak didukung?

Ya. Namun, remediasi dilakukan hanya jika jenis sumber daya yang didukung ditemukan DRIFTED di tumpukan. Jika ada jenis sumber daya yang tidak didukung DRIFTED, remediasi tidak akan dilanjutkan.

Dapatkah saya meminta remediasi untuk tumpukan yang dibuat melalui non-CFN Ingest? CTs

Ya. Remediasi dapat dilakukan pada tumpukan terlepas dari jenis perubahan yang digunakan untuk membuat tumpukan.

Dapatkah saya mengetahui perubahan yang akan dilakukan pada tumpukan sebelum perbaikan?

Ya. Kedua jenis perubahan menyediakan DryRunopsi yang dapat Anda gunakan untuk meminta perubahan yang akan dilakukan jika tumpukan diperbaiki. Namun, perubahan remediasi akhir mungkin berbeda tergantung pada penyimpangan yang ada pada tumpukan pada saat remediasi.

Jadwal RFCs

Fitur Penjadwalan memungkinkan Anda memilih waktu mulai untuk RFCs. Opsi berikut tersedia di fitur Penjadwalan:

- Jalankan perubahan ini secepatnya: AMS menjalankan RFC segera setelah disetujui. Sebagian CTs besar disetujui secara otomatis. Gunakan opsi ini jika tidak ingin RFC dimulai pada waktu tertentu.
- Jadwalkan perubahan ini: Tetapkan hari, waktu, dan zona waktu agar RFC berjalan. Untuk jenis perubahan otomatis, ini adalah praktik terbaik untuk meminta waktu mulai yang setidaknya 10 menit setelah Anda berencana untuk mengirimkan RFC. Untuk meninjau jenis perubahan yang diperlukan, Anda harus meminta waktu mulai setidaknya 24 jam setelah Anda berencana mengirimkan RFC. Jika RFC tidak disetujui oleh waktu mulai yang dikonfigurasi, maka RFC ditolak.

Tetapkan jadwal RFC

Untuk menjadwalkan RFC, gunakan salah satu metode berikut:

Jalankan perubahan ini secepatnya:

- Konsol: Jangan lakukan apa-apa. Ini menggunakan jadwal RFC default.
- API atau CLI: Hapus `RequestedEndTime` opsi `RequestedStartTime` dan dalam operasi Buat RFC.

ASAP “diperlukan peninjauan” ditolak RFCs secara otomatis jika tidak disetujui dalam waktu tiga puluh hari sejak pengajuan.

Jadwalkan perubahan ini:

- Konsol: Pilih tombol Jadwalkan perubahan radio ini. Area waktu mulai terbuka. Ketik secara manual dalam sehari atau gunakan widget kalender untuk memilih hari. Masukkan waktu, dalam UTC, dinyatakan dalam format ISO 8601, dan gunakan daftar drop-down untuk memilih lokasi. Secara default, AMS menggunakan format ISO 8601 Z atau:MM: YYYYMMDDThhmmss YYYY-MM-DDThh SSZ, salah satu format diterima.

Note

Waktu Akhir Default adalah 4 jam dari waktu Mulai yang Anda masukkan. Untuk mengatur Waktu Akhir perubahan terjadwal Anda melebihi 4 jam, gunakan API atau CLI untuk menjalankan perubahan.

- API atau CLI: Kirim nilai untuk RequestedStartTime dan RequestedEndTime parameter dalam operasi Buat RFC. Melewati konfigurasi RequestedEndTime tidak menghentikan proses untuk jenis perubahan otomatis yang telah dimulai. Untuk jenis perubahan “wajib ditinjau”, jika RequestedEndTime tercapai saat penelitian Operasi AMS masih berlangsung, dan Anda berkomunikasi dengan AMS, maka Anda dapat meminta ekstensi, atau Anda mungkin diminta untuk mengirimkan ulang RFC.

Tip

Untuk contoh pembacaan waktu UTC, lihat UTC di situs web [Time-is](#). Contoh format ISO 8601 untuk date/time nilai 2016-12-05 pada 2:20pm: 2016-12-05T 14:20:00 Z atau 20161205T142000Z.

Jika Anda memberikan...

- hanya aRequestedStartTime, RFC dianggap dijadwalkan dan RequestedEndTime diisi menggunakan nilai ExecutionDurationInMinutes
- hanya aRequestedEndTime, kami melempar InvalidArgumentException.
- keduanya RequestedStartTime dan RequestedEndTime, kami menimpa RequestedEndTime dengan waktu mulai yang ditentukan ditambah ExecutionDurationInMinutes nilainya.
- baik RequestedStartTime maupun RequestedEndTime, kami mempertahankan nilai-nilai itu sebagai nol dan RFC diperlakukan sebagai ASAP RFC.

Note

Untuk semua yang dijadwalkan RFCs, waktu akhir yang tidak ditentukan ditulis sebagai waktu yang ditentukan RequestedStartTime ditambah ExpectedExecutionDurationInMinutes atribut dari jenis perubahan yang dikirimkan. Misalnya, jika “60” (menit), dan yang ditentukan RequestedStartTime

adalah 2016-12-05T14:20:00Z (5 Desember 2016 pukul 4:20 pagi), waktu akhir yang sebenarnya akan ditetapkan ke 5 Desember 2016 pukul 5:20 pagi. ExpectedExecutionDurationInMinutes Untuk menemukan tipe perubahan tertentu, jalankan perintah ini: ExpectedExecutionDurationInMinutes

```
aws amscm --profile saml get-change-type-version --  
change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.  
{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Gunakan opsi Prioritas RFC

Gunakan opsi Prioritas dalam jenis `execution mode = manual` perubahan untuk mengingatkan Operasi AMS tentang urgensi permintaan.

Opsi prioritas di `execution mode = manual`:

Tentukan prioritas RFC manual sebagai Tinggi, Sedang, atau Rendah. RFCs diklasifikasikan sebagai Tinggi ditinjau dan disetujui sebelum RFCs diklasifikasikan sebagai Medium, tunduk pada tujuan tingkat layanan RFC (SLOs) dan waktu pengajuannya. RFCs dengan Prioritas rendah atau tidak ada prioritas yang ditentukan diproses sesuai urutan yang dikirimkan.

Menyetujui atau menolak RFCs

RFCs diserahkan dengan persetujuan yang diperlukan (manual) CTs harus disetujui oleh Anda atau AMS. Pra-persetujuan CTs diproses secara otomatis. Untuk informasi selengkapnya, lihat [Persyaratan persetujuan CT](#).

Note

Saat menggunakan “review required” CTs, AMS merekomendasikan agar Anda menggunakan opsi Penjadwalan ASAP (pilih ASAP di konsol, biarkan waktu mulai dan berakhir kosong di API/CLI) karena ini CTs memerlukan operator AMS untuk memeriksa RFC, dan mungkin berkomunikasi dengan Anda sebelum dapat disetujui dan dijalankan. Jika Anda menjadwalkan ini RFCs, pastikan untuk mengizinkan setidaknya 24 jam. Jika persetujuan tidak terjadi sebelum waktu mulai yang dijadwalkan, RFC ditolak secara otomatis.

Jika RFC yang diperlukan persetujuan berhasil dikirimkan oleh AMS, maka RFC tersebut harus disetujui secara eksplisit oleh Anda. Atau, jika Anda mengirimkan RFC yang diperlukan persetujuan, maka itu harus disetujui oleh AMS. Jika Anda diminta untuk menyetujui RFC yang dikirimkan AMS, maka email atau komunikasi lain yang telah ditentukan dikirimkan kepada Anda untuk meminta persetujuan. Komunikasi termasuk ID RFC. Setelah komunikasi dikirim, lakukan salah satu hal berikut:

- Menyetujui atau Menolak Konsol: Gunakan halaman detail RFC untuk RFC yang relevan:
- API/CLI Approve: [ApproveRfc](#) menandai perubahan sebagai disetujui. Tindakan harus diambil oleh pemilik dan operator, jika keduanya diperlukan. Berikut ini adalah contoh CLI menyetujui perintah. Dalam contoh berikut, ganti RFC_ID dengan ID RFC yang sesuai.

```
aws amscm approve-rfc --rfc-id RFC_ID
```

- API/CLI Reject: [RejectRfc](#) menandai perubahan sebagai ditolak. Berikut ini adalah contoh perintah CLI reject. Dalam contoh berikut, ganti RFC_ID dengan ID RFC yang sesuai.

```
aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
```

Minta periode berjalan terbatas RFC

Sebelumnya dikenal sebagai hari pemadaman, Anda dapat meminta untuk membatasi periode waktu tertentu. Tidak ada perubahan yang dapat dijalankan selama waktu-waktu tersebut.

Untuk menetapkan periode berjalan terbatas, gunakan operasi [UpdateRestrictedExecutionTimes](#) API dan tetapkan periode waktu tertentu, di UTC. Periode yang Anda tentukan mengesampingkan periode sebelumnya yang ditentukan. Jika Anda mengirimkan RFC selama waktu berjalan terbatas yang ditentukan, pengiriman gagal dengan kesalahan Jadwal RFC Tidak Valid. Anda dapat menentukan hingga 200 periode waktu terbatas. Secara default, tidak ada periode terbatas yang ditetapkan. Berikut ini adalah contoh perintah permintaan (dengan otentikasi SAM dikonfigurasi):

```
aws amscm --profile saml update-restricted-execution-times --restricted-execution-times='[{"TimeRange":{"StartTime":"2018-01-01T12:00:00Z","EndTime":"2018-01-01T12:00:01Z"}}]'
```

Anda juga dapat melihat RestrictedExecutionTimes setelah Anda saat ini dengan menjalankan operasi [ListRestrictedExecutionTimes](#) API. Contoh:

```
aws amscm --profile saml list-restricted-execution-times
```

Jika Anda ingin mengirimkan RFC selama waktu eksekusi terbatas yang ditentukan, tambahkan `RestrictedExecutionTimesOverride` dengan nilai `OverrideRestrictedTimeRanges`, dan kemudian kirimkan RFC seperti biasa. Ini adalah praktik terbaik untuk hanya menggunakan metode ini untuk RFC kritis atau darurat. Untuk informasi selengkapnya, lihat referensi API untuk [SubmitRfc](#).

Buat, kloning, perbarui, temukan, dan batalkan RFCs

Contoh berikut memandu Anda melalui berbagai operasi RFC.

Topik

- [Buat RFC](#)
- [Kloning RFCs \(buat ulang\) dengan konsol AMS](#)
- [Perbarui RFCs](#)
- [Menemukan RFCs](#)
- [Batalkan RFCs](#)

Buat RFC

Membuat RFC dengan konsol

Berikut ini adalah halaman pertama proses RFC Create di konsol AMS, dengan kartu Quick terbuka dan Browse change types aktif:

Berikut ini adalah halaman pertama proses RFC Create di konsol AMS, dengan Pilih berdasarkan kategori aktif:

Cara kerjanya:

1. Arahkan ke halaman Buat RFC: Di panel navigasi kiri konsol AMS klik RFCs untuk membuka halaman RFCs daftar, lalu klik Buat RFC.
2. Pilih jenis perubahan populer (CT) di tampilan default Jelajahi jenis perubahan, atau pilih CT dalam tampilan Pilih menurut kategori.

- Jelajahi berdasarkan jenis perubahan: Anda dapat mengklik CT populer di area Buat cepat untuk segera membuka halaman Jalankan RFC. Perhatikan bahwa Anda tidak dapat memilih versi CT yang lebih lama dengan pembuatan cepat.

Untuk mengurutkan CTs, gunakan area Semua jenis perubahan dalam tampilan Kartu atau Tabel. Di kedua tampilan, pilih CT dan kemudian klik Buat RFC untuk membuka halaman Jalankan RFC. Jika berlaku, opsi Buat dengan versi yang lebih lama muncul di sebelah tombol Buat RFC.

- Pilih berdasarkan kategori: Pilih kategori, subkategori, item, dan operasi dan kotak detail CT terbuka dengan opsi untuk Membuat dengan versi yang lebih lama jika berlaku. Klik Buat RFC untuk membuka halaman Jalankan RFC.
3. Pada halaman Jalankan RFC, buka area nama CT untuk melihat kotak detail CT. Subjek diperlukan (ini diisi untuk Anda jika Anda memilih CT Anda di tampilan jenis perubahan Jelajahi). Buka area konfigurasi tambahan untuk menambahkan informasi tentang RFC.

Di area konfigurasi Eksekusi, gunakan daftar drop-down yang tersedia atau masukkan nilai untuk parameter yang diperlukan. Untuk mengkonfigurasi parameter eksekusi opsional, buka area konfigurasi tambahan.

4. Setelah selesai, klik Jalankan. Jika tidak ada kesalahan, halaman RFC berhasil dibuat ditampilkan dengan detail RFC yang dikirimkan, dan output Run awal.
5. Buka area parameter Jalankan untuk melihat konfigurasi yang Anda kirimkan. Segarkan halaman untuk memperbarui status eksekusi RFC. Secara opsional, batalkan RFC atau buat salinannya dengan opsi di bagian atas halaman.

Membuat RFC dengan CLI

Cara kerjanya:

1. Gunakan Inline Create (Anda mengeluarkan `create-rfc` perintah dengan semua RFC dan parameter eksekusi disertakan), atau Template Create (Anda membuat dua file JSON, satu untuk parameter RFC dan satu untuk parameter eksekusi) dan mengeluarkan `create-rfc` perintah dengan dua file sebagai input. Kedua metode tersebut dijelaskan di sini.
2. Kirim `aws amscm submit-rfc --rfc-id ID` perintah RFC: dengan ID RFC yang dikembalikan.

Pantau `aws amscm get-rfc --rfc-id ID` perintah RFC:.

Untuk memeriksa versi jenis perubahan, gunakan perintah ini:

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=CT_ID
```

Note

Anda dapat menggunakan CreateRfc parameter apa pun dengan RFC apa pun apakah itu bagian dari skema untuk jenis perubahan atau tidak. Misalnya, untuk mendapatkan pemberitahuan ketika status RFC berubah, tambahkan baris ini, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}\"` ke bagian parameter RFC dari permintaan (bukan parameter eksekusi). Untuk daftar semua CreateRfc parameter, lihat [Referensi AMS Change Management API](#).

BUAT SEBARIS:

Keluarkan perintah create RFC dengan parameter eksekusi yang disediakan sebaris (tanda kutip saat memberikan parameter eksekusi sebaris), lalu kirimkan ID RFC yang dikembalikan. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini::

```
aws amscm create-rtc --change-type-id "CT_ID" --change-type-version "VERSION" --title
"TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

TEMPLATE MEMBUAT:

Note

Contoh pembuatan RFC ini menggunakan tipe perubahan tumpukan Load Balancer (ELB).

1. Temukan CT yang relevan. Perintah berikut mencari ringkasan klasifikasi CT untuk yang berisi “ELB” di Nama Item dan membuat output dari Kategori, Item, Operasi, dan ChangeType ID dalam bentuk tabel (Subkategori untuk keduanya). `Advanced stack components`

```
aws amscm list-change-type-classification-summaries --query
"ChangeTypeClassificationSummaries[?contains(Item,'ELB')].
[Category,Item,Operation,ChangeTypeId]" --output table
```

CtSummaries				
Deployment	Load balancer (ELB) stack	Create	ct-123h45t6uz7jl	
Management	Load balancer (ELB) stack	Update	ct-01tm873rsebx9	

2. Temukan versi terbaru dari CT:

ChangeTypeId dan ChangeTypeVersion: ID tipe perubahan untuk panduan ini adalah ct-123h45t6uz7jl (buat ELB), untuk mengetahui versi terbaru, jalankan perintah ini:

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=ct-123h45t6uz7jl
```

3. Pelajari opsi dan persyaratannya. Perintah berikut output skema ke file JSON bernama .json. CreateElbParams

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
"ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. Memodifikasi dan menyimpan parameter eksekusi file JSON. Contoh ini menamai file CreateElbParams .json.

Untuk CT penyediaan, termasuk dalam skema dan harus diserahkan dalam parameter eksekusi. StackTemplateId

Untuk TimeoutInMinutes, berapa menit yang diizinkan untuk pembuatan tumpukan sebelum RFC gagal, pengaturan ini tidak akan menunda eksekusi RFC, tetapi Anda harus memberikan waktu yang cukup (misalnya, jangan tentukan "5"). Nilai yang valid adalah "60" hingga "360," untuk CTs dengan jangka panjang UserData: Buat EC2 dan Buat ASG. Kami merekomendasikan maksimum yang diizinkan "60" untuk semua penyediaan CTs lainnya.

Berikan ID VPC tempat Anda ingin tumpukan dibuat; Anda bisa mendapatkan ID VPC dengan perintah CLI. `aws amsskms list-vpc-summaries`

```
{
  "Description":      "ELB-Create-RFC",
  "VpcId":            "VPC_ID",
  "StackTemplateId":  "stm-sdhopv000000000000",
```

```

"Name": "MyElbInstance",
"TimeoutInMinutes": 60,
"Parameters": {
  "ELBSubnetIds": ["SUBNET_ID"],
  "ELBHealthCheckHealthyThreshold": 4,
  "ELBHealthCheckInterval": 5,
  "ELBHealthCheckTarget": "HTTP:80/",
  "ELBHealthCheckTimeout": 60,
  "ELBHealthCheckUnhealthyThreshold": 5,
  "ELBScheme": false
}
}

```

5. Keluarkan template RFC JSON ke file di folder Anda saat ini bernama CreateElbRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. Ubah dan simpan CreateElbRfc file.json. Karena Anda membuat parameter eksekusi dalam file terpisah, hapus ExecutionParameters baris. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```

{
  "ChangeTypeVersion": "2.0",
  "ChangeTypeId": "ct-123h45t6uz7jl",
  "Title": "Create ELB"
}

```

7. Buat RFC. Perintah berikut menentukan file parameter eksekusi dan file template RFC:

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-parameters file://CreateElbParams.json
```

Anda menerima ID RFC baru dalam respons dan dapat menggunakannya untuk mengirimkan dan memantau RFC. Sampai Anda mengirimkannya, RFC tetap dalam kondisi pengeditan dan tidak dimulai.

Kiat

Note

Anda dapat menggunakan AMS API/CLI untuk membuat RFC tanpa membuat file JSON RFC atau file JSON parameter eksekusi CT. Untuk melakukan ini, Anda menggunakan `create-rfc` perintah dan menambahkan parameter RFC dan eksekusi yang diperlukan ke perintah, ini disebut “Buat Sebaris”. Perhatikan bahwa semua penyediaan CTs telah terkandung dalam `execution-parameters` blok `Parameters` array dengan parameter untuk sumber daya. Parameter harus memiliki tanda kutip yang lolos dengan garis miring belakang (`\`).

Metode terdokumentasi lainnya untuk membuat RFC disebut “Template Create.” Di sinilah Anda membuat file JSON untuk parameter RFC dan file JSON lain untuk parameter eksekusi, dan mengirimkan dua file dengan perintah. `create-rfc` File-file ini dapat berfungsi sebagai template dan digunakan kembali untuk masa depan RFCs.

Saat membuat RFCs dengan template, Anda dapat menggunakan perintah untuk membuat file JSON dengan konten yang Anda inginkan dengan mengeluarkan perintah seperti yang ditunjukkan. Perintah membuat file bernama “`parameters.json`” dengan konten yang ditampilkan; Anda juga bisa menggunakan perintah ini untuk membuat file RFC JSON.

Kloning RFCs (buat ulang) dengan konsol AMS

Anda dapat menggunakan konsol AMS untuk mengkloning RFC yang ada.

Untuk mengkloning, atau membuat ulang, RFC menggunakan konsol AMS, ikuti langkah-langkah berikut:

1. Temukan RFC yang relevan. Dari navigasi kiri, klik RFCs.

RFCs Dasbor terbuka.

2. Gulir halaman sampai Anda menemukan RFC yang ingin Anda kloning. Gunakan opsi Filter untuk mempersempit daftar. Pilih RFC yang ingin Anda kloning.

Halaman detail RFC terbuka.

3. Klik Buat Salinan.

Halaman Buat permintaan untuk perubahan terbuka dengan semua opsi yang ditetapkan seperti pada RFC asli.

4. Buat perubahan yang Anda inginkan. Untuk mengatur opsi tambahan, ubah opsi Basic ke Advanced. Setelah Anda mengatur semua opsi, pilih Kirim.

Halaman detail RFC aktif terbuka dengan ID RFC baru untuk RFC kloning dan RFC kloning muncul di dasbor RFC.

Perbarui RFCs

Anda dapat mengirimkan ulang RFC yang telah ditolak atau yang belum dikirimkan, dengan memperbarui RFC dan kemudian mengirimkannya, atau mengirimkannya kembali. Perhatikan bahwa sebagian besar ditolak karena RFCs yang ditentukan `RequestedStartTime` telah berlalu sebelum pengiriman atau yang `TimeoutInMinutes` ditentukan tidak memadai untuk menjalankan RFC (karena `TimeoutInMinutes` tidak memperpanjang RFC yang berhasil, kami sarankan untuk selalu menyetel ini ke setidaknya "60" dan hingga "360" untuk Amazon atau grup Auto Scaling EC2 Amazon dengan jangka panjang). EC2 UserData Bagian ini menjelaskan cara menggunakan versi CLI dari `UpdateRfc` perintah untuk memperbarui RFC dengan parameter RFC baru, atau parameter baru menggunakan JSON stringified atau file parameter yang diperbarui.

Contoh ini menjelaskan penggunaan AMS `UpdateRfc` API versi CLI (lihat [Perbarui RFC](#)). Meskipun ada jenis perubahan untuk memperbarui beberapa sumber daya (DNS pribadi dan publik, tumpukan penyeimbang beban, dan konfigurasi tambalan tumpukan), tidak ada CT untuk memperbarui RFC.

Kami menyarankan Anda mengirimkan satu `UpdateRfc` operasi pada satu waktu. Jika Anda mengirimkan beberapa pembaruan, misalnya pada tumpukan DNS, pembaruan mungkin gagal mencoba memperbarui DNS secara bersamaan.

DATA YANG DIPERLUKAN: `RfcId`: RFC yang Anda perbarui.

DATA OPSIONAL `ExecutionParameters`:: Kecuali Anda memperbarui bidang yang tidak `wajibDescription`, seperti, Anda akan mengirimkan parameter eksekusi yang dimodifikasi untuk mengatasi masalah yang menyebabkan RFC ditolak atau dibatalkan. Semua nilai non-null yang dikirimkan menimpa nilai-nilai tersebut di RFC asli.

1. Temukan RFC yang ditolak atau dibatalkan yang relevan, Anda dapat menggunakan perintah ini (Anda dapat mengganti nilainya dengan `Canceled`):

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
```

2. Anda dapat memodifikasi salah satu parameter RFC berikut:

```
{
  "Description": "string",
  "ExecutionParameters": "string",
  "ExpectedOutcome": "string",
  "ImplementationPlan": "string",
  "RequestedEndTime": "string",
  "RequestedStartTime": "string",
  "RfcId": "string",
  "RollbackPlan": "string",
  "Title": "string",
  "WorstCaseScenario": "string"}
```

Contoh perintah memperbarui bidang Deskripsi:

```
aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
--region us-east-1
```

Contoh perintah memperbarui ExecutionParameters VpcId bidang:

```
aws amscm update-rfc --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id
"RFC_ID" --region us-east-1
```

Contoh perintah memperbarui RFC dengan file parameter eksekusi yang berisi pembaruan; lihat contoh file parameter eksekusi di langkah 2 dari: [EC2 stack | Buat](#):

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --
rfc-id "RFC_ID" --region us-east-1
```

3. Kirim ulang RFC menggunakan submit-rfc dan ID RFC yang sama dengan yang Anda miliki saat RFC pertama kali dibuat:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Jika RFC berhasil, Anda tidak menerima konfirmasi atau pesan kesalahan di baris perintah.

4. Untuk memantau status permintaan dan untuk melihat Output Eksekusi, jalankan perintah berikut.

```
aws amscm get-rfc --rfc-id RFC_ID
```

Menemukan RFCs

Temukan permintaan perubahan (RFC) dengan konsol

Untuk menemukan RFC menggunakan konsol AMS, ikuti langkah-langkah berikut.

Note

Prosedur ini hanya berlaku untuk yang dijadwalkan RFCs, RFCs yaitu, yang tidak menggunakan opsi ASAP.

1. Dari navigasi kiri, klik RFCs.

RFCs Dasbor terbuka.

2. Gulir daftar atau gunakan opsi Filter untuk memperbaiki daftar.

Daftar RFC berubah per kriteria filter.

3. Pilih tautan Subjek untuk RFC yang Anda inginkan.

Halaman detail RFC terbuka untuk RFC itu dengan informasi termasuk ID RFC.

4. Jika ada banyak RFCs di dasbor, Anda dapat menggunakan opsi Filter untuk mencari berdasarkan RFC:

- Subjek: Baris subjek, atau judul (dalam API/CLI) diberikan kepada RFC saat dibuat.
- ID RFC: Pengidentifikasi untuk RFC.
- Status aktivitas: Jika Anda mengetahui status RFC, Anda dapat memilih antara `AwsOperatorAssigned` arti operator sedang melihat RFC, yang `AwsActionPending` berarti bahwa operator AMS harus melakukan sesuatu sebelum eksekusi RFC dapat dilanjutkan atau `CustomerActionPending` artinya Anda perlu mengambil beberapa tindakan sebelum eksekusi RFC dapat dilanjutkan.
- Status: Jika Anda mengetahui status RFC, Anda dapat memilih antara:
 - Dijadwalkan: RFCs yang dijadwalkan.
 - Dibatalkan: RFCs yang dibatalkan.
 - Sedang berlangsung: RFCs sedang berlangsung.
 - Sukses: RFCs yang dieksekusi dengan sukses.
 - Ditolak: RFCs yang ditolak.

- Pengeditan: RFCs yang sedang diedit.
- Kegagalan: RFCs itu gagal.
- Persetujuan yang tertunda: RFCs yang tidak dapat dilanjutkan sampai AMS atau Anda menyetujui. Biasanya, ini menunjukkan bahwa Anda perlu menyetujui RFC. Anda akan mendapatkan pemberitahuan layanan ini di daftar Permintaan Layanan Anda.
- Ubah jenis: Pilih Kategori, Subkategori, Item, dan Operasi, dan ID jenis perubahan diambil untuk Anda.
- Waktu mulai yang diminta atau Waktu akhir yang diminta: Opsi filter ini memungkinkan Anda memilih Sebelum atau Setelah, lalu masukkan Tanggal dan, secara opsional, Waktu (hh: mm dan zona waktu). Filter ini beroperasi dengan sukses hanya pada jadwal RFCs (tidak ASAP RFCs).
- Status: Baik Dijadwalkan, Dibatalkan, Sedang berlangsung, Sukses, Ditolak, Mengedit, atau Kegagalan.
- Subjek: Subjek (atau judul, jika RFC dibuat dengan API/CLI) yang Anda berikan RFC.
- Ubah tipe ID: Gunakan pengenal untuk jenis perubahan yang dikirimkan dengan RFC.

Pencarian memungkinkan Anda untuk menambahkan filter, seperti yang ditunjukkan pada gambar berikut.

5. Klik tautan Subjek untuk RFC yang Anda inginkan.

Halaman detail RFC terbuka untuk RFC itu dengan informasi termasuk ID RFC.

Menemukan permintaan perubahan (RFC) dengan CLI

Anda dapat menggunakan beberapa filter untuk menemukan RFC.

Untuk memeriksa versi jenis perubahan, gunakan perintah ini:

```
aws amscm list-change-type-version-summaries --filter  
Attribute=ChangeTypeId,Value=CT_ID
```

Note

Anda dapat menggunakan `CreateRfc` parameter apa pun dengan RFC apa pun apakah itu bagian dari skema untuk jenis perubahan atau tidak. Misalnya, untuk mendapatkan

pemberitahuan ketika status RFC berubah, tambahkan baris ini, `--notification`
`"{"Email": {"EmailRecipients" : ["email@example.com"]}}"` ke bagian parameter RFC dari permintaan (bukan parameter eksekusi). Untuk daftar semua `CreateRfc` parameter, lihat [Referensi AMS Change Management API](#).

Jika Anda tidak menuliskan ID RFC, dan perlu menemukannya nanti, Anda dapat menggunakan sistem manajemen perubahan AMS (CM) untuk mencarinya dan mempersempit hasilnya dengan filter atau kueri.

1. [ListRfcSummaries](#) Operasi CM API memiliki filter. Anda dapat [Memfilter](#) hasil berdasarkan `Attribute` dan `Value` digabungkan dalam operasi AND logis, atau berdasarkan `Attribute`, `aCondition`, dan `Values`.

Penyaringan RFC

Atribut	Nilai valid	Ketentuan yang valid	Kondisi default	Catatan
ActualEndTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , "20170101T000000Z")	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua
ActualStartTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , "20170101T000000Z")	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara

Atribut	Nilai valid	Ketentuan yang valid	Kondisi default	Catatan
				harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua
AutomationStatusId	Manual, Otomatis	Setara	Setara	Hanya ada dua status otomatisasi
ChangeTypeId	Setiap ID jenis perubahan yang valid; misalnya, ct-123h45t6uz7jl	Setara	Setara	Menemukan Jenis Perubahan atau CSIO
ChangeTypeVersion	Setiap ID tipe perubahan yang valid; misalnya, 1.0	Setara	Setara	Menemukan Jenis Perubahan atau CSIO
CreatedBy	String apa pun (panjang maksimum yang diizinkan adalah 2048 karakter)	Contains	Contains	CreatedBy Bidang RFC berisi ARN pengguna yang membuatnya

Atribut	Nilai valid	Ketentuan yang valid	Kondisi default	Catatan
CreatedTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , “20170101 T000000Z”)	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua
LastModifiedTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , “20170101 T000000Z”)	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua

Atribut	Nilai valid	Ketentuan yang valid	Kondisi default	Catatan
LastSubmittedTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , “20170101 T000000Z”)	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua
RequestedEndTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , “20170101 T000000Z”)	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua

Atribut	Nilai valid	Ketentuan yang valid	Kondisi default	Catatan
RequestedStartTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , “20170101 T000000Z”)	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua
RfcStatusId	Dibatalkan, Mengedit, Kegagalan , InProgress, Ditolak PendingApproval, Dijadwalkan, Sukses	Setara	Setara	Segarkan daftar RFC di konsol AMS atau jalankan GetRfc
Judul	Setiap judul RFC yang valid	Contains	Contains	Ekspresi reguler di setiap bidang individu tidak didukung. Pencarian yang tidak peka huruf besar/kecil

Contoh:

Untuk menemukan semua IDs yang RFCs terkait dengan SQS (di mana SQS terkandung dalam bagian Item CT), Anda dapat menggunakan perintah ini:

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name, `SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

Yang mengembalikan sesuatu seperti ini:

```

-----
|                               ListRfcSummaries                               |
+-----+-----+-----+-----+-----+-----+
|Deployment| Advanced Stack Components      |SQS   |Create |ct-123h45t6uz7jl|
|Management| Monitoring & Notification    |SQS   |Update |ct-123h45t6uz7jl|
+-----+-----+-----+-----+-----+-----+

```

Filter lain yang tersedia `list-rfc-summaries` adalah `AutomationStatusId`, untuk mencari RFCs yang otomatis atau manual:

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

Filter lain yang tersedia `list-rfc-summaries` adalah `Title` (Subjek di konsol):

```
Attribute=Title,Value=RFC-TITLE
```

Contoh struktur permintaan baru di JSON yang mengembalikan RFCs where:

- (Judul BERISI frasa "Windows 2012" ATAU "Amazon Linux") DAN
- (RfcStatusId SAMA DENGAN "Sukses" ATAU "InProgress") DAN
- (20170101T000000Z <= <= 20170103T000000Z) DAN (<= 20170103T000000Z)
RequestedStartTime ActualEndTime

```

{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    }
  ],
  {

```

```

    "Attribute": "RequestedStartTime",
    "Values": ["20170101T000000Z", "20170103T000000Z"],
    "Condition": "Between"
  },
  {
    "Attribute": "ActualEndTime",
    "Values": ["20170103T000000Z"],
    "Condition": "Before"
  }
]
}

```

Note

Dengan lebih lanjutFilters, AMS bermaksud untuk menghentikan bidang berikut dalam rilis mendatang:

- Nilai: Bidang Nilai adalah bagian dari bidang Filter. Gunakan bidang Nilai yang mendukung fungsionalitas yang lebih canggih.
- RequestedEndTimeRange: Gunakan bagian RequestedEndTime dalam bidang Filter yang mendukung fungsionalitas yang lebih canggih
- RequestedStartTimeRange: Gunakan bagian RequestedStartTime dalam bidang Filter yang mendukung fungsionalitas yang lebih canggih.

[Untuk informasi tentang penggunaan kueri CLI, lihat Cara Memfilter Output dengan Opsi --query dan referensi bahasa kueri, Spesifikasi. JMESPath](#)

2. Jika Anda menggunakan konsol AMS:

Pergi ke halaman RFCsdaftar. Jika diperlukan, Anda dapat memfilter pada Subjek RFC, yang Anda masukkan sebagai RFC Title saat Anda membuatnya.

Kiat

Note

Prosedur ini hanya berlaku untuk yang dijadwalkan RFCs, RFCs yaitu, yang tidak menggunakan opsi ASAP.

Batalkan RFCs

Anda dapat membatalkan RFC menggunakan Konsol atau AMS API/CLI.

Untuk membatalkan RFC dengan konsol, temukan RFC di daftar RFC Anda, buka, klik Batal.

Data yang Diperlukan:

- Reason: Mengapa Anda membatalkan RFC.
 - RfcId: RFC yang Anda batalkan.
1. Biasanya Anda akan membatalkan RFC segera setelah mengirimkannya (jadi ID RFC harus berguna); jika tidak, Anda tidak akan dapat membatalkannya kecuali Anda menjadwalkannya dan itu sebelum waktu mulai yang ditentukan. Jika Anda perlu menemukan ID RFC, Anda dapat menggunakan perintah ini (Anda dapat mengganti Value dengan PendingApproval RFC yang disetujui secara manual):

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
```

2. Contoh perintah untuk membatalkan RFC:

```
aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --region us-east-1
```

Gunakan konsol AMS dengan RFCs

Konsol AMS menyediakan fitur untuk membantu Anda berhasil membuat dan mengirimkan RFCs.

Gunakan halaman Daftar RFC (Konsol)

Halaman RFCsdaftar konsol AMS memberi Anda opsi berikut:

- Pencarian RFC tingkat lanjut melalui Filter. Untuk informasi, lihat [Menemukan RFCs](#).
- Menemukan terakhir kali RFC Dimodifikasi. Nilai ini menunjukkan bahwa terakhir kali status RFC diubah.
- Melihat detail RFC dengan Subjek RFC. Memilih tautan ini membuka halaman detail untuk RFC itu.
- Melihat status RFC. Untuk informasi, lihat [Memahami kode status RFC](#)

Gunakan RFC quick create (konsol)

Gunakan kartu cepat RFC, atau daftar tabel, atau pilih jenis perubahan RFCs berdasarkan klasifikasi.

Untuk mempelajari selengkapnya, lihat [Buat RFC](#).

Tambahkan korespondensi dan lampiran RFC (konsol)

Anda dapat menambahkan korespondensi ke RFC setelah dikirimkan dan sebelum disetujui; misalnya, saat berada dalam keadaan "PendingApproval". Setelah RFC disetujui (dalam keadaan "Terjadwal" atau "InProgress"), korespondensi tidak dapat ditambahkan, karena dapat ditafsirkan sebagai perubahan pada permintaan. Setelah RFC selesai (dalam keadaan "Dibatalkan", "Ditolak", "Sukses", atau "Kegagalan"), korespondensi sekali lagi diaktifkan, meskipun korespondensi dinonaktifkan setelah RFC ditutup selama lebih dari 30 hari.

 Note

Setiap korespondensi dibatasi hingga 5.000 karakter.

Batasan untuk lampiran:

- Hanya tiga lampiran per korespondensi.
- Batasi lima puluh lampiran per RFC.
- Setiap lampiran harus berukuran kurang dari 5 MB.
- Hanya file teks yang diterima seperti plaintext (.txt), nilai yang dipisahkan koma (.), JSON (.csv), atau YAMB (.json). .yaml Dalam kasus format YAMAL, file harus dilampirkan menggunakan ekstensi .yaml file.

 Note

File teks yang memiliki konten XMLdilarang. Jika Anda memiliki konten XMLuntuk dibagikan dengan AMS, gunakan permintaan layanan.

- Nama file dibatasi hingga 255 karakter, dengan hanya angka, huruf, spasi, tanda hubung (-), garis bawah (_), dan titik (.).
- Memperbarui dan menghapus lampiran pada RFC saat ini tidak didukung.

Untuk menambahkan korespondensi dan lampiran ke RFC, ikuti langkah-langkah berikut:

1. Di konsol AMS, pada halaman detail RFC untuk RFC, temukan bagian Korespondensi di bagian bawah halaman.

Sebelum korespondensi apa pun:

Setelah beberapa korespondensi:

2. Untuk menambahkan korespondensi baru, ketik pesan Anda di kotak teks Balas. Untuk melampirkan file yang terkait dengan korespondensi, pilih Tambahkan Lampiran, lalu pilih file yang Anda inginkan.
3. Setelah selesai, pilih Kirim.

Korespondensi baru, bersama dengan tautan ke file terlampir, muncul di daftar korespondensi di halaman detail RFC.

Konfigurasikan pemberitahuan email RFC (konsol)

Halaman pembuatan Permintaan Perubahan konsol AMS memberi Anda opsi untuk menambahkan alamat email guna menerima pemberitahuan perubahan status RFC:

Selain itu, Anda dapat menambahkan alamat email untuk pemberitahuan ke jenis perubahan apa pun, misalnya:

```
aws amscm create-rfc --change-type-id <Change type ID>
                        --change-type-version 1.0 --title "TITLE"
                        --notification "{\"Email\": {\"EmailRecipients\" :
[\"email@example.com\"]}}\""
```

Tambahkan baris serupa (`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}\"`) ke setiap jenis perubahan inline atau permintaan template di bagian parameter RFC dari permintaan, bukan bagian parameter.

Pelajari tentang parameter RFC umum

Berikut ini adalah parameter RFC yang harus Anda kirimkan, dan parameter yang biasa digunakan di RFCs:

- Ubah informasi jenis: `ChangeTypeId` dan `ChangeTypeVersion`. Dengan daftar jenis perubahan IDs dan nomor versi, lihat [Mengubah Referensi Jenis](#).

Jalankan `list-change-type-classification-summaries` di CLI dengan query argumen untuk mempersempit hasil. Misalnya, mempersempit hasil untuk mengubah jenis yang berisi "Akses" dalam Item nama.

```
aws amscm list-change-type-classification-summaries --query
  "ChangeTypeClassificationSummaries [?contains (Item, 'access')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

Jalankan `get-change-type-version` dan tentukan ID tipe perubahan. Perintah berikut mendapatkan versi CT untuk `ct-2tylseo8rxfsc`.

```
aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
```

- Judul: Nama untuk RFC; ini menjadi Subjek RFC di daftar RFC konsol AMS dan Anda dapat mencarinya dengan `GetRfc` perintah dan filter `Title`
- Penjadwalan: Jika Anda menginginkan RFC terjadwal, Anda harus menyertakan `RequestedEndTime` parameter `RequestedStartTime` dan, atau gunakan opsi Jadwalkan konsol perubahan ini. Untuk ASAP RFC (yang berjalan segera setelah disetujui), saat menggunakan CLI, `RequestedStartTime` tinggalkan `RequestedEndTime` dan `null`. Saat menggunakan konsol, terima opsi ASAP.

Jika `RequestedStartTime` terlewatkan, RFC ditolak.

- Penyediaan CTs: Parameter eksekusi, atau pengaturan khusus `Parameters` yang diperlukan untuk menyediakan sumber daya. Mereka sangat bervariasi tergantung pada CT.
- Non-penyediaan CTs: CTs yang tidak menyediakan sumber daya, seperti akses CTs atau Lainnya | Lainnya, atau menghapus tumpukan, memiliki parameter eksekusi minimal dan tidak ada blok. `Parameters`
- Beberapa RFCs juga mengharuskan Anda menentukan `TimeoutInMinutes`, atau berapa menit yang diizinkan untuk pembuatan tumpukan sebelum RFC gagal. Nilai yang valid adalah 60 (menit) hingga 360, untuk jangka panjang `UserData`. Jika eksekusi tidak dapat diselesaikan sebelum

TimeoutInMinutes terlampaui, RFC gagal. Namun, pengaturan ini tidak menunda eksekusi RFC.

- RFCs yang membuat instance, seperti bucket S3 atau ELB, umumnya menyediakan skema yang memungkinkan Anda menambahkan hingga tujuh tag (pasangan kunci/nilai). Anda dapat menambahkan lebih banyak tag ke bucket S3 Anda dengan mengirimkan RFC menggunakan Deployment | Advanced stack components | Tag | Create change type (ct-3cx7we852p3af). EC2, EFS, RDS, dan skema multi-tier (HA Two-Tiered dan HA One-Tiered) memungkinkan hingga lima puluh tag. Tag ditentukan di ExecutionParameters bagian skema. Memberikan tag bisa sangat berharga. Untuk informasi selengkapnya, lihat [Menandai EC2 Sumber Daya Amazon Anda](#).

Saat menggunakan konsol AMS, Anda harus membuka area konfigurasi tambahan untuk menambahkan tag.

Tip

Banyak skema CT memiliki Name bidang Description dan di dekat bagian atas skema. Bidang tersebut digunakan untuk memberi nama komponen tumpukan atau tumpukan, mereka tidak memberi nama sumber daya yang Anda buat. Beberapa skema menawarkan parameter untuk memberi nama sumber daya yang Anda buat, dan beberapa tidak. Misalnya, skema CT untuk EC2 tumpukan Create tidak menawarkan parameter untuk menamai EC2 instance. Untuk melakukannya, Anda harus membuat tag dengan kunci "Nama" dan nilai dari nama yang Anda inginkan. Jika Anda tidak membuat tag seperti itu, EC2 instance Anda akan ditampilkan di EC2 konsol tanpa atribut name.

Gunakan opsi AWS Wilayah RFC

Titik akhir AMS API dan CLI (amscmdanamsskms) ada di us-east-1. Jika Anda berfederasi dengan Security Assertion Markup Language (SAMP), maka skrip diberikan kepada Anda saat orientasi yang mengatur Wilayah Anda ke us-east-1. AWS Jika Anda menggunakan SAMP, maka Anda tidak perlu menentukan --region opsi saat Anda mengeluarkan perintah. Jika SAMP Anda dikonfigurasi untuk menggunakan us-east-1 tetapi akun Anda tidak berada di Wilayah itu, maka Anda harus menentukan Wilayah AWS yang diboard akun saat Anda mengeluarkan perintah lain (misalnya,). AWS aws s3

 Note

Sebagian besar contoh perintah yang disediakan dalam panduan ini tidak menyertakan --region opsi.

Mendaftar untuk email harian RFC

Anda dapat mendaftar untuk email harian yang merangkum aktivitas RFC di akun Anda selama 24 jam terakhir menggunakan fitur RFC digest. Fitur RFC digest adalah proses efisien yang mengurangi jumlah notifikasi email yang Anda terima terkait akun Anda. RFCs Intisari RFC dapat mengurangi kemungkinan Anda melewatkan tindakan yang menunggu respons Anda.

Untuk mengaktifkan fitur RFC digest, hubungi AMS Cloud Service Delivery Manager (CSDM). CSDM berlangganan Anda. Anda dapat meminta hingga 20 alamat email (atau alias) untuk disertakan dalam daftar email intisari RFC Anda. Jadwal email saat ini ditetapkan pada pukul 09:00 UTC-8.

Untuk mematikan fitur RFC digest, hubungi CSDM Anda dengan permintaan Anda.

Jika Anda tidak mengatur intisari RFC dan menginginkan pemberitahuan mengenai Anda RFCs, atau jika Anda ingin informasi lebih rinci tentang Anda RFCs daripada apa yang disediakan oleh intisari RFC, gunakan Sistem Manajemen Perubahan untuk mengatur pemberitahuan CloudWatch Acara atau pemberitahuan email untuk setiap RFC individu yang Anda inginkan informasi. Untuk informasi tentang cara menyiapkan notifikasi RFC, lihat Pemberitahuan [Perubahan Status RFC](#).

Topik yang terkandung dalam intisari RFC meliputi:

- Persetujuan Pelanggan Tertunda: Daftar RFCs yang PendingApprovalberstatus, menunggu persetujuan Anda
- Balasan Pelanggan Tertunda: Daftar RFCs yang menunggu balasan Anda pada korespondensi RFC
- Persetujuan atau Balasan AWS RFCs yang Tertunda: Daftar yang menunggu di AMS untuk balasan atau persetujuan
- Selesai: Daftar RFCs dalam status Sukses, Kegagalan, Dibatalkan dan Ditolak

Berikut ini adalah contoh RFC digest:

Apa itu jenis perubahan?

Jenis perubahan mengacu pada tindakan yang dilakukan oleh permintaan perubahan (RFC) AWS Managed Services (AMS) dan mencakup tindakan perubahan itu sendiri, dan jenis perubahan — manual vs otomatis. AMS memiliki banyak koleksi jenis perubahan yang tidak digunakan oleh layanan web Amazon lainnya. Anda menggunakan jenis perubahan ini saat mengirimkan permintaan untuk perubahan (RFC) untuk menyebarkan, atau mengelola, atau mendapatkan akses ke, sumber daya.

Topik

- [Otomatis dan manual CTs](#)
- [Persyaratan persetujuan CT](#)
- [Ubah versi tipe](#)
- [Buat jenis perubahan](#)
- [Perbarui jenis perubahan](#)
- [Jenis perubahan hanya internal](#)
- [Ubah skema tipe](#)
- [Mengelola izin untuk jenis perubahan](#)
- [Menyunting informasi sensitif dari jenis perubahan](#)
- [Menemukan jenis perubahan, menggunakan opsi kueri](#)

Otomatis dan manual CTs

Batasan pada jenis perubahan adalah apakah mereka otomatis atau manual, ini adalah `AutomationStatusId` atribut tipe perubahan, yang disebut mode Eksekusi di konsol AMS.

Jenis perubahan otomatis memiliki hasil dan waktu eksekusi yang diharapkan dan dijalankan melalui sistem otomatis AMS, umumnya dalam waktu satu jam atau kurang (ini sangat tergantung pada sumber daya apa yang disediakan CT). Jenis perubahan manual jarang terjadi, tetapi diperlakukan berbeda karena mengharuskan operator AMS bertindak pada RFC sebelum dapat dijalankan. Itu terkadang berarti berkomunikasi dengan pengirim RFC, jadi, jenis perubahan manual memerlukan waktu yang bervariasi untuk menyelesaikannya.

Untuk semua yang dijadwalkan RFCs, waktu akhir yang tidak ditentukan ditulis sebagai waktu yang ditentukan `RequestedStartTime` ditambah `ExpectedExecutionDurationInMinutes`

atribut dari jenis perubahan yang dikirimkan. Misalnya, jika "60" (menit), dan yang ditentukan RequestedStartTime adalah 2016-12-05T14:20:00Z (5 Desember 2016 pukul 4:20 pagi), waktu akhir yang sebenarnya akan ditetapkan ke 5 Desember 2016 pukul 5:20 pagi. ExpectedExecutionDurationInMinutes Untuk menemukan tipe perubahan tertentu, jalankan perintah ini: ExpectedExecutionDurationInMinutes

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --  
query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Note

Dijadwalkan RFCs dengan mode Eksekusi = Manual, di Konsol, harus diatur untuk berjalan setidaknya 24 jam di masa mendatang. Peringatan ini tidak berlaku untuk AMS API/CLI, tetapi masih penting untuk menjadwalkan manual RFCs setidaknya 8 jam ke depan.

Note

Saat menggunakan "review required" CTs, AMS merekomendasikan agar Anda menggunakan opsi Penjadwalan ASAP (pilih ASAP di konsol, biarkan waktu mulai dan berakhir kosong di API/CLI) karena ini CTs memerlukan operator AMS untuk memeriksa RFC, dan mungkin berkomunikasi dengan Anda sebelum dapat disetujui dan dijalankan. Jika Anda menjadwalkan ini RFCs, pastikan untuk mengizinkan setidaknya 24 jam. Jika persetujuan tidak terjadi sebelum waktu mulai yang dijadwalkan, RFC ditolak secara otomatis.

AMS bertujuan untuk menanggapi CT manual dalam waktu empat jam, dan akan berkorespondensi sesegera mungkin, tetapi bisa memakan waktu lebih lama bagi RFC untuk benar-benar dijalankan.

Untuk daftar yang Manual dan memerlukan tinjauan AMS, lihat file CSV Ubah Jenis, yang tersedia di halaman Sumber Daya Pengembang di Konsol. CTs

YouTube Video: [Bagaimana cara menemukan jenis perubahan otomatis untuk AMS RFCs?](#)

Untuk menemukan mode Eksekusi untuk CT di konsol AMS, Anda harus menggunakan opsi pencarian jenis perubahan Jelajahi. Hasilnya menunjukkan mode eksekusi dari jenis perubahan yang cocok atau jenis perubahan.

Untuk menemukan tipe perubahan tertentu dengan menggunakan AMS CLI, jalankan perintah ini:

AutomationStatus

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --  
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

Anda juga dapat mencari jenis perubahan di [Referensi Jenis Perubahan AMS](#), yang menyediakan informasi tentang semua jenis perubahan AMS.

 Note

AMS saat API/CLI ini bukan bagian dari AWSAPI/CLI. To access the AMS API/CLI, Anda mengunduh AMS SDK melalui konsol AMS.

Persyaratan persetujuan CT

AMS CTs selalu memiliki dua kondisi persetujuan, **AwsApproval** dan **CustomerApproval** untuk menunjukkan apakah RFC memerlukan AMS atau Anda, atau siapa pun, untuk menyetujui eksekusi.

Kondisi persetujuan agak terkait dengan mode eksekusi; untuk detailnya, lihat [Otomatis dan manual CTs](#).

Untuk mengetahui kondisi persetujuan untuk CT, Anda dapat melihat di [AMS Change Type Reference](#), atau menjalankannya [GetChangeTypeVersion](#). Keduanya juga akan memberi Anda mode CT **AutomationStatusId** atau Eksekusi.

Anda dapat menyetujui RFCs dengan menggunakan konsol AMS atau dengan perintah berikut:

```
aws amscm approve-rfc --rfc-id RFC_ID
```

Kondisi persetujuan CT

Jika kondisi persetujuan CT adalah	Hal ini membutuhkan persetujuan dari	Dan
<code>AwsApprovalId: Required</code>	Sistem tipe perubahan AMS,	Tidak ada tindakan yang diperlukan. Kondisi ini khas untuk otomatis CTs.
<code>AwsApprovalId: NotRequiredIfSubmitter</code>	Sistem jenis perubahan AMS dan tidak ada orang lain, jika RFC yang dikirimkan adalah untuk akun yang diserahkan,	Tidak ada tindakan yang diperlukan. Kondisi ini khas untuk manual CTs karena akan selalu ditinjau oleh operator AMS.
<code>CustomerApprovalId: NotRequired</code>	Sistem tipe perubahan AMS,	Jika RFC melewati pemeriksaan sintaks dan parameter, itu disetujui secara otomatis.
<code>CustomerApprovalId: Required</code>	Sistem tipe perubahan AMS dan Anda,	Pemberitahuan dikirimkan kepada Anda, dan Anda harus secara eksplisit menyetujui RFC, baik dengan menanggapi pemberitahuan, atau menjalankan operasi. ApproveRfc
<code>CustomerApprovalId: NotRequiredIfSubmitter</code>	Sistem tipe perubahan AMS dan tidak ada orang lain, jika Anda mengirimkan RFC.	Jika RFC melewati pemeriksaan sintaks dan parameter, itu disetujui secara otomatis.

Jika kondisi persetujuan CT adalah	Hal ini membutuhkan persetujuan dari	Dan
Insiden Keamanan Mendesak atau Patch	AMS	Apakah auto disetujui dan diimplementasikan.

Ubah versi tipe

Jenis perubahan diberi versi dan versi berubah saat pembaruan besar dibuat untuk jenis perubahan.

Setelah memilih jenis perubahan menggunakan konsol AMS, Anda memiliki opsi untuk membuka area konfigurasi tambahan dan memilih versi jenis perubahan. Anda juga dapat menentukan versi jenis perubahan pada baris API/CLI perintah. Anda mungkin ingin melakukan ini karena berbagai alasan, termasuk:

- Anda tahu bahwa versi jenis perubahan Pembaruan yang Anda inginkan harus cocok dengan versi jenis Buat perubahan yang Anda gunakan untuk membuat sumber daya yang sekarang ingin Anda perbarui. Misalnya, Anda mungkin memiliki instance Elastic Load Balancer (ELB) yang dibuat dengan ELB Create change type versi 1. Untuk memperbaruinya, pilih ELB Update versi 1.
- Anda ingin menggunakan versi jenis perubahan yang memiliki opsi berbeda di dalamnya daripada jenis perubahan terbaru. Kami tidak merekomendasikan hal ini karena pembaruan AMS mengubah jenis terutama untuk alasan keamanan dan kami menyarankan Anda untuk selalu memilih versi terbaru.

Buat jenis perubahan

Buat jenis perubahan dicocokkan version-to-version dengan jenis perubahan Perbarui. Artinya, versi tipe perubahan yang Anda gunakan untuk menyediakan sumber daya harus sesuai dengan versi jenis perubahan Perbarui yang akan Anda gunakan nanti untuk memodifikasi sumber daya tersebut. Misalnya, jika Anda membuat bucket S3 dengan Create S3 Bucket change type versi 2.0, dan kemudian ingin mengirimkan RFC untuk memodifikasi bucket S3 tersebut, Anda harus menggunakan Update S3 Bucket change type versi 2.0 juga, meskipun ada jenis perubahan Update S3 Bucket dengan versi 3.0.

Sebaiknya simpan catatan ID tipe perubahan dan versi yang Anda gunakan saat menyediakan sumber daya dengan tipe Buat perubahan jika nanti Anda ingin menggunakan jenis perubahan Pembaruan untuk memodifikasinya.

Perbarui jenis perubahan

AMS menyediakan jenis perubahan Pembaruan untuk memperbarui sumber daya yang dibuat dengan tipe Buat perubahan. Jenis perubahan Perbarui harus dicocokkan version-to-version dengan jenis Buat perubahan yang awalnya digunakan untuk menyediakan sumber daya.

Sebaiknya simpan catatan ID tipe perubahan dan versi yang Anda gunakan saat menyediakan sumber daya agar mudah memperbaruinya.

YouTube Video: [Bagaimana cara menggunakan pembaruan CTs untuk mengubah sumber daya di akun AWS Managed Services \(AMS\)?](#)

Jenis perubahan hanya internal

Anda dapat melihat jenis perubahan yang hanya untuk penggunaan internal. Ini agar Anda tahu tindakan apa yang dapat atau dilakukan AMS. Jika ada jenis perubahan internal saja yang ingin Anda miliki untuk digunakan, kirimkan permintaan layanan.

Misalnya, ada Manajemen | Pemantauan dan pemberitahuan | penindasan CloudWatch alarm | Perbarui CT yang hanya internal. AMS menggunakannya untuk menyebarkan pembaruan infrastruktur (seperti menambal) untuk mematikan pemberitahuan alarm yang mungkin dipicu oleh pembaruan secara keliru. Ketika CT ini dikirimkan, Anda akan melihat RFC untuk CT dalam daftar RFC Anda. CT internal apa pun yang digunakan dalam RFC akan muncul di daftar RFC Anda.

Ubah skema tipe

Semua jenis perubahan menyediakan skema JSON untuk masukan Anda dalam pembuatan, modifikasi, atau akses, sumber daya. Skema menyediakan parameter, dan deskripsinya, bagi Anda untuk membuat permintaan perubahan (RFC).

Keberhasilan eksekusi RFC menghasilkan output eksekusi. Untuk penyediaan RFCs, output eksekusi menyertakan “stack_id” yang mewakili tumpukan CloudFormation dan dapat dicari di konsol. CloudFormation Output eksekusi terkadang menyertakan output ID dari instance yang dibuat dan ID tersebut dapat digunakan untuk mencari instance di konsol AWS yang sesuai. <stack-xxxx> Misalnya, output eksekusi Create ELB CT menyertakan “stack_id” yang dapat dicari CloudFormation dan

mengeluarkan nilai `key=ELB` = yang dapat dicari di konsol Amazon untuk Elastic Load Balancing. EC2

Mari kita periksa skema CT. Ini adalah skema untuk CodeDeploy Application Create, skema yang cukup kecil. Beberapa skema memiliki Parameter area yang sangat luas.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv000000000000",
      "type": "string",
      "enum": ["stm-sft6rv000000000000"]
    },
    "Name": {
      "description": "A name for the stack or stack component
;
this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "Tags": {
      "description": "Up to seven tags (key/value pairs) to
categorize the resource.",
```

Bagian pertama dari skema memberikan informasi kepada AMS tentang jenis perubahan yang diminta.

```

    "type": "array",
    "items": {
      "type": "object",
      "properties": {
        "Key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 127
        },
        "Value": {
          "type": "string",
          "minLength": 1,
          "maxLength": 255
        }
      },
      "additionalProperties": false,
      "required": [
        "Key",
        "Value"
      ]
    },
    "minItems": 1,
    "maxItems": 7
  },
  "TimeoutInMinutes": {
    "description": "The maximum amount of time, in minutes,
to
    allow for execution of the change. This will not prolong
execution,
    but the RFC fails if the change is not completed in the
specified time.
    Valid values are 60 up to 360, for long-running
UserData.",
    "type": "number",
    "minimum": 0,
    "maximum": 60
  },
  "Parameters": {
    "description": "Specifications for the stack.",
    "type": "object",
    "properties": {
      "CodeDeployApplicationName": {
        "description": "The name of an AWS CodeDeploy
application.",

```

TimeoutInMinutes
Parameter ini memungkinkan Anda untuk menunjukkan waktu batas untuk menjalankan jenis perubahan. Nilai yang valid adalah 60 hingga 360, untuk jangka panjang UserData.

Bagian Parameter adalah tempat Anda menentukan pengaturan untuk sumber daya yang Anda buat, atau tindakan yang Anda minta.

Bagian “properti tambahan” memberi

```
        "type": "string",
        "minLength": 1,
        "maxLength": 100,
        "pattern": "^[a-zA-Z0-9._+=,e-]{1,100}$"
      }
    },
    "additionalProperties": false,
    "required": [
      "CodeDeployApplicationName"
    ]
  }
},
"additionalProperties": false,
"required": [
  "Description",
  "VpcId",
  "StackTemplateId",
  "Name",
  "TimeoutInMinutes",
  "Parameters"
]
}
```

tahu Anda parameter apa yang diperlukan dan mana yang opsional.

Note

Skema ini memungkinkan hingga tujuh tag; namun, EFS EC2, RDS, dan skema pembuatan multi-tier memungkinkan hingga 50 tag.

Mengelola izin untuk jenis perubahan

Anda dapat menggunakan kebijakan khusus untuk membatasi jenis perubahan (CTs) yang tersedia untuk grup atau pengguna yang berbeda.

Untuk mempelajari lebih lanjut tentang melakukan hal ini, lihat bagian Panduan Pengguna AMS [Menyetel Izin](#).

Menyunting informasi sensitif dari jenis perubahan

Skema jenis perubahan AMS menawarkan atribut parameter,

"metadata": "ams:sensitive": "true" yang digunakan untuk parameter yang berisi informasi

sensitif, seperti kata sandi. Ketika atribut ini disetel, masukan yang diberikan dikaburkan. Perhatikan bahwa Anda tidak dapat menyetel atribut parameter ini; namun, jika Anda bekerja dengan AMS untuk membuat tipe perubahan dan memiliki parameter yang ingin dikaburkan pada input, Anda dapat meminta ini.

Menemukan jenis perubahan, menggunakan opsi kueri

Contoh ini menunjukkan cara menggunakan Konsol AMS untuk menemukan jenis perubahan yang sesuai untuk RFC yang ingin Anda kirimkan.

Anda dapat menggunakan konsol atau API/CLI untuk menemukan perubahan jenis ID (CT) atau versi. Ada dua metode, baik pencarian atau memilih klasifikasi. Untuk kedua jenis pilihan, Anda dapat mengurutkan pencarian dengan memilih Paling sering digunakan, Paling baru digunakan, atau Alfabetis.

YouTube Video: [Bagaimana cara membuat RFC menggunakan AWS Managed Services CLI dan di mana saya dapat menemukan Skema CT?](#)

Di konsol AMS, pada halaman RFCs-> Buat RFC:

- Dengan Browse by change type yang dipilih (default), baik:
 - Gunakan area Quick create untuk memilih dari AMS yang paling populer CTs. Klik pada label dan halaman Jalankan RFC terbuka dengan opsi Subjek diisi otomatis untuk Anda. Selesaikan opsi yang tersisa sesuai kebutuhan dan klik Jalankan untuk mengirimkan RFC.
 - Atau, gulir ke bawah ke Semua jenis perubahan area dan mulai mengetik nama CT di kotak opsi, Anda tidak harus memiliki nama jenis perubahan yang tepat atau lengkap. Anda juga dapat mencari CT dengan mengubah jenis ID, klasifikasi, atau mode eksekusi (otomatis atau manual) dengan memasukkan kata-kata yang relevan.

Dengan tampilan Kartu default yang dipilih, kartu CT yang cocok muncul saat Anda mengetik, pilih kartu dan klik Buat RFC. Dengan tampilan Tabel dipilih, pilih CT yang relevan dan klik Buat RFC. Kedua metode membuka halaman Run RFC.

- Atau, dan untuk menjelajahi pilihan jenis perubahan, klik Pilih berdasarkan kategori di bagian atas halaman untuk membuka serangkaian kotak opsi drop-down.
- Pilih Kategori, Subkategori, Item, dan Operasi. Kotak informasi untuk jenis perubahan itu muncul panel muncul di bagian bawah halaman.
- Saat Anda siap, tekan Enter, dan daftar jenis perubahan yang cocok akan muncul.

- Pilih jenis perubahan dari daftar. Kotak informasi untuk jenis perubahan itu muncul di bagian bawah halaman.
- Setelah Anda memiliki jenis perubahan yang benar, pilih Buat RFC.

Note

AMS CLI harus diinstal agar perintah ini berfungsi. Untuk menginstal AMS API atau CLI, buka halaman Sumber Daya Pengembang konsol AMS. Untuk materi referensi tentang AMS CM API atau AMS SKMS API, lihat bagian Sumber Informasi AMS di Panduan Pengguna. Anda mungkin perlu menambahkan `--profile` opsi untuk otentikasi; misalnya, `aws amsskms ams-cli-command --profile SAML`. Anda mungkin juga perlu menambahkan `--region` opsi karena semua perintah AMS kehabisan `us-east-1`; misalnya, `aws amscm ams-cli-command --region=us-east-1`

Note

Titik akhir AMS API/CLI (`amscm` dan `amsskms`) berada di Wilayah AWS N. Virginia, `us-east-1`. Bergantung pada cara autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan `--profile saml`, jika itu adalah metode otentikasi Anda.

Untuk mencari jenis perubahan menggunakan AMS CM API (lihat [ListChangeTypeClassificationSummaries](#)) atau CLI:

Anda dapat menggunakan filter atau kueri untuk mencari. `ListChangeTypeClassificationSummaries` Operasi memiliki opsi [Filter](#) untuk `Category`, `Subcategory`, `Item`, dan `Operation`, tetapi nilainya harus sama persis dengan nilai yang ada. Untuk hasil yang lebih fleksibel saat menggunakan CLI, Anda dapat menggunakan opsi. `--query`

Ubah jenis penyaringan dengan AMS CM API/CLI

Atribut	Nilai valid	Kondisi valid/default	Catatan
ChangeTypeId	String apa pun yang mewakili ChangeTypeId (Misalnya: ct-abc123xyz7890)	Setara	Untuk jenis perubahan IDs, lihat Referensi Ubah Jenis . Untuk jenis perubahan IDs, lihat Menemukan Jenis Perubahan atau CSIO.
Kategori	Teks bentuk bebas apa pun	Contains	Ekspresi reguler di setiap bidang individu tidak didukung. Pencarian yang tidak peka huruf besar/kecil
Subkategori			
Item			
Operasi			

- Berikut adalah beberapa contoh klasifikasi jenis perubahan daftar:

Perintah berikut mencantumkan semua kategori jenis perubahan.

```
aws amscm list-change-type-categories
```

Perintah berikut mencantumkan subkategori milik kategori tertentu.

```
aws amscm list-change-type-subcategories --category CATEGORY
```

Perintah berikut mencantumkan item milik kategori dan subkategori tertentu.

```
aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
```

- Berikut adalah beberapa contoh pencarian jenis perubahan dengan kueri CLI:

Perintah berikut mencari ringkasan klasifikasi CT untuk yang berisi "S3" di Nama item dan membuat output dari kategori, subkategori, item, operasi, dan mengubah ID tipe dalam bentuk tabel.

```
aws amscm list-change-type-classification-summaries --query
  "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

```
+-----+
|          ListChangeTypeClassificationSummaries          |
+-----+-----+-----+-----+-----+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+-----+-----+-----+-----+-----+
```

3. Anda kemudian dapat menggunakan ID tipe perubahan untuk mendapatkan skema CT dan memeriksa parameternya. Perintah berikut output skema ke file JSON bernama `creates3params.schema.json`.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
--query "ChangeTypeVersion.ExecutionInputSchema" --output text >
CreateS3Params.schema.json
```

[Untuk informasi tentang penggunaan kueri CLI, lihat Cara Memfilter Output dengan Opsi `--query` dan referensi bahasa kueri, Spesifikasi JMESPath](#)

4. Setelah Anda memiliki ID tipe perubahan, kami sarankan untuk memverifikasi versi untuk jenis perubahan untuk memastikan itu adalah versi terbaru. Gunakan perintah ini untuk menemukan versi untuk jenis perubahan tertentu:

```
aws amscm list-change-type-version-summaries --filter
  Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

Untuk menemukan tipe perubahan tertentu, jalankan perintah ini: `AutomationStatus`

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

Untuk menemukan tipe perubahan tertentu, jalankan perintah ini:

`ExpectedExecutionDurationInMinutes`

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h  
--query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Memecahkan masalah kesalahan RFC di AMS

Banyak kegagalan RFC penyediaan AMS dapat diselidiki melalui dokumentasi. CloudFormation Lihat [Pemecahan Masalah AWS CloudFormation](#): Kesalahan Pemecahan Masalah

Saran pemecahan masalah tambahan disediakan di bagian berikut.

Kesalahan RFC “Manajemen” di AMS

AMS “Manajemen” Jenis perubahan kategori (CTs) memungkinkan Anda untuk meminta akses ke sumber daya serta mengelola sumber daya yang ada. Bagian ini menjelaskan beberapa masalah umum.

Kesalahan akses RFC

- Pastikan Username dan FQDN yang Anda tentukan di RFC sudah benar dan ada di domain. Untuk bantuan menemukan FQDN Anda, lihat [Menemukan](#) FQDN Anda.
- Pastikan ID tumpukan yang Anda tentukan untuk akses adalah tumpukan EC2 -related. Tumpukan seperti ELB dan Amazon Simple Storage Service (S3) bukan kandidat untuk RFCs akses, sebagai gantinya, gunakan peran akses baca saja untuk mengakses sumber daya tumpukan ini. Untuk bantuan menemukan ID tumpukan, lihat [Menemukan tumpukan IDs](#)
- Pastikan ID tumpukan yang Anda berikan sudah benar dan milik akun yang relevan.

Untuk bantuan terkait kegagalan akses RFC lainnya, lihat [Manajemen akses](#).

YouTube Video: [Bagaimana cara mengajukan Request for Change \(RFC\) dengan benar untuk menghindari penolakan dan kegagalan?](#)

Kesalahan penjadwalan CT RFC (manual)

Sebagian besar jenis perubahan adalah ExecutionMode = Otomatis, tetapi beberapa ExecutionMode = Manual dan itu memengaruhi cara Anda menjadwalkannya untuk menghindari kegagalan RFC.

Dijadwalkan RFCs dengan ExecutionMode =Manual, harus diatur untuk mengeksekusi setidaknya 24 jam di masa mendatang jika Anda menggunakan Konsol AMS untuk membuat RFC. Peringatan ini

tidak berlaku untuk AMS API/CLI, tetapi masih penting untuk menjadwalkan Manual RFCs setidaknya 8 jam ke depan.

AMS bertujuan untuk menanggapi CT manual dalam waktu empat jam, dan akan berkorespondensi sesegera mungkin, tetapi bisa memakan waktu lebih lama bagi RFC untuk benar-benar dieksekusi.

Menggunakan RFCs dengan pembaruan manual CTs

Operasi AMS menolak Manajemen | Lainnya | Lainnya RFCs untuk pembaruan tumpukan, ketika ada jenis perubahan Pembaruan untuk jenis tumpukan yang ingin Anda perbarui.

Kesalahan tumpukan hapus RFC

Kegagalan tumpukan penghapusan RFC: Jika Anda menggunakan Manajemen | Tumpukan standar | Tumpukan | Hapus CT, Anda akan melihat peristiwa terperinci di AWS CloudFormation Konsol untuk tumpukan dengan nama tumpukan AMS. Anda dapat mengidentifikasi tumpukan Anda dengan memeriksanya terhadap nama yang ada di Konsol AMS. AWS CloudFormation Konsol memberikan rincian lebih lanjut tentang penyebab kegagalan.

Sebelum menghapus tumpukan, Anda harus mempertimbangkan bagaimana tumpukan dibuat. Jika Anda membuat tumpukan menggunakan AMS CT dan tidak menambahkan atau mengedit sumber daya tumpukan, Anda dapat menghapusnya tanpa masalah. Namun, itu adalah ide yang baik untuk Anda menghapus sumber daya yang ditambahkan secara manual dari tumpukan sebelum mengirimkan tumpukan hapus RFC terhadapnya. Misalnya, jika Anda membuat tumpukan menggunakan tumpukan penuh CT (HA Two Tier), itu termasuk grup keamanan - SG1. Jika Anda kemudian menggunakan AMS untuk membuat grup keamanan lain - SG2, dan mereferensikan yang baru SG2 di SG1 dibuat sebagai bagian dari tumpukan penuh, dan kemudian menggunakan CT tumpukan hapus untuk menghapus tumpukan, tidak SG1 akan dihapus seperti yang direferensikan oleh SG2.

Important

Menghapus tumpukan dapat memiliki konsekuensi yang tidak diinginkan dan tidak terduga. AMS lebih suka *tidak* menghapus tumpukan atau menumpuk sumber daya atas nama pelanggan karena alasan ini. Perhatikan, AMS hanya akan menghapus sumber daya atas nama Anda (melalui Manajemen yang dikirimkan | Lainnya | Lainnya | Jenis perubahan pembaruan) yang tidak mungkin dihapus menggunakan jenis perubahan yang sesuai, otomatis, untuk dihapus. Pertimbangan tambahan:

- Jika sumber daya diaktifkan untuk 'hapus perlindungan', AMS dapat membantu membuka blokir ini jika Anda mengirimkan Manajemen | Lainnya | Lainnya | Perbarui jenis perubahan dan, setelah perlindungan penghapusan dihapus, Anda dapat menggunakan CT otomatis untuk menghapus sumber daya tersebut.
- Jika ada beberapa sumber daya dalam tumpukan, dan Anda hanya ingin menghapus sebagian dari sumber daya tumpukan, gunakan jenis perubahan CloudFormation Pembaruan (lihat [CloudFormation Ingest Stack: Update](#)). Anda juga dapat mengirimkan Manajemen | Lainnya | Lainnya | Perbarui jenis perubahan dan insinyur AMS dapat membantu Anda menyusun set perubahan, jika diperlukan.
- Jika ada masalah dalam menggunakan CT CloudFormation Pembaruan karena drift, AMS dapat membantu jika Anda mengirimkan Manajemen | Lainnya | Lainnya | Pembaruan untuk menyelesaikan penyimpangan (sejauh yang didukung oleh CloudFormation Layanan AWS) dan memberikan ChangeSet yang kemudian dapat Anda validasi dan jalankan menggunakan CT, Management/Custom Stack/Stack From CloudFormation Template/ Approve Changeset, dan Pembaruan otomatis.

AMS mempertahankan pembatasan di atas untuk membantu memastikan tidak ada penghapusan sumber daya yang tidak terduga atau tidak terduga.

Untuk informasi selengkapnya, lihat [Pemecahan Masalah AWS CloudFormation: menghapus tumpukan gagal](#).

Kesalahan DNS pembaruan RFC

Beberapa RFCs untuk memperbarui zona yang dihosting DNS dapat gagal, beberapa tanpa alasan. Membuat beberapa RFCs sekaligus untuk memperbarui zona yang dihosting DNS (pribadi atau publik) dapat menyebabkan beberapa RFCs gagal karena mereka mencoba memperbarui tumpukan yang sama pada saat yang bersamaan. Manajemen perubahan AMS menolak atau gagal RFCs yang tidak dapat memperbarui tumpukan karena tumpukan sudah diperbarui oleh RFC lain. AMS merekomendasikan agar Anda membuat satu RFC sekaligus dan menunggu RFC berhasil sebelum menaikkan yang baru untuk tumpukan yang sama.

Kesalahan entitas IAM RFC

AMS menyediakan sejumlah peran dan profil IAM default ke dalam akun AMS yang dirancang untuk memenuhi kebutuhan Anda. Namun, Anda mungkin perlu meminta sumber daya IAM tambahan sesekali.

Proses untuk mengirimkan RFCs permintaan sumber daya IAM kustom mengikuti alur kerja standar untuk manual RFCs, tetapi proses persetujuan juga mencakup tinjauan keamanan untuk memastikan kontrol keamanan yang tepat ada. Oleh karena itu, prosesnya biasanya memakan waktu lebih lama daripada manual lainnya RFCs. Untuk mengurangi waktu siklus ini RFCs, ikuti panduan berikut.

Untuk informasi tentang apa yang kami maksud dengan tinjauan IAM dan cara memetakannya ke Standar Teknis dan proses Penerimaan Risiko kami, lihat [Memahami ulasan keamanan RFC](#).

Permintaan sumber daya IAM umum:

- Jika Anda meminta kebijakan yang berkaitan dengan aplikasi utama yang kompatibel dengan cloud, misalnya CloudEndure, lihat CloudEndure kebijakan IAM AMS yang telah disetujui sebelumnya: Buka paket file Contoh Zona Pendaratan [WIGs Cloud Endure](#) dan buka file `customer_cloud_endure_policy.json`

Note

Jika Anda menginginkan kebijakan yang lebih permisif, diskusikan kebutuhan Anda dengan Anda CloudArchitect/CSDM dan dapatkan, jika diperlukan, AMS Security Review and Signoff sebelum mengirimkan RFC yang menerapkan kebijakan tersebut.

- Jika Anda ingin mengubah sumber daya yang digunakan oleh AMS di akun Anda secara default, sebaiknya Anda meminta salinan sumber daya yang dimodifikasi, bukan perubahan pada yang sudah ada.
- Jika Anda meminta izin untuk pengguna manusia (alih-alih melampirkan izin ke pengguna) lampirkan izin ke peran, lalu berikan izin kepada pengguna untuk mengambil peran tersebut. Untuk detail tentang hal ini, lihat [Akses konsol AMS Advanced sementara](#).
- Jika Anda memerlukan izin luar biasa untuk migrasi sementara atau alur kerja, berikan tanggal akhir untuk izin tersebut dalam permintaan Anda.
- Jika Anda telah mendiskusikan subjek permintaan Anda dengan tim keamanan Anda, berikan bukti persetujuan mereka kepada CSDM Anda dengan sedetail mungkin.

Jika AMS menolak IAM RFC, kami memberikan alasan yang jelas untuk penolakan tersebut. Misalnya, kami mungkin menolak permintaan pembuatan kebijakan IAM dan menjelaskan kebijakan yang tidak pantas. Dalam hal ini, Anda dapat membuat perubahan yang diidentifikasi dan mengirimkan kembali permintaan. Jika kejelasan tambahan tentang status permintaan diperlukan, kirimkan permintaan layanan, atau hubungi CSDM Anda.

Daftar berikut menjelaskan risiko umum yang AMS coba mitigasi saat kami meninjau IAM Anda. RFCs Jika IAM RFC Anda memiliki salah satu risiko ini, itu dapat mengakibatkan penolakan RFC. Dalam kasus di mana Anda memerlukan pengecualian, AMS meminta persetujuan dari tim keamanan Anda. Untuk mencari pengecualian seperti itu, koordinasikan dengan CSDM Anda.

Note

AMS dapat, dengan alasan apa pun, menolak perubahan apa pun pada sumber daya IAM di dalam akun. Untuk masalah mengenai penolakan RFC, hubungi Operasi AMS melalui permintaan layanan, atau hubungi CSDM Anda.

- Eskalasi hak istimewa, seperti izin yang memungkinkan Anda mengubah izin Anda sendiri, atau untuk mengubah izin sumber daya lain di dalam akun. Contoh:
 - Penggunaan `iam:PassRole` dengan peran lain yang lebih istimewa.
 - Izin untuk kebijakan `attach/detach` IAM dari peran atau pengguna.
 - Modifikasi kebijakan IAM di akun.
 - Kemampuan untuk melakukan panggilan API dalam konteks infrastruktur manajemen.
- Izin untuk mengubah sumber daya atau aplikasi yang diperlukan untuk menyediakan layanan AMS kepada Anda. Contoh:
 - Modifikasi infrastruktur AMS seperti benteng, host manajemen, atau infrastruktur EPS.
 - Penghapusan fungsi AWS Lambda manajemen log, atau aliran log.
 - Penghapusan atau modifikasi aplikasi CloudTrail pemantauan default.
 - Modifikasi Direktori Layanan Direktori Aktif (AD).
 - Menonaktifkan alarm CloudWatch (CW).
 - Modifikasi prinsip, kebijakan, dan ruang nama yang digunakan di akun sebagai bagian dari landing zone.
- Penyebaran infrastruktur di luar praktik terbaik, seperti izin yang memungkinkan pembuatan infrastruktur dalam keadaan yang membahayakan keamanan informasi Anda. Contoh:

- Pembuatan bucket S3 publik, atau tidak terenkripsi, atau berbagi volume EBS secara publik.
- Penyediaan alamat IP publik.
- Modifikasi kelompok keamanan untuk memungkinkan akses luas.
- Izin yang terlalu luas yang dapat menyebabkan dampak aplikasi, seperti izin yang dapat mengakibatkan kehilangan data, kehilangan integritas, konfigurasi yang tidak tepat, atau gangguan layanan untuk infrastruktur Anda dan aplikasi di dalam akun. Contoh:
 - Menonaktifkan, atau mengarahkan, lalu lintas jaringan melalui suka atau. APIs `ModifyNetworkInterfaceAttribute` `UpdateRouteTable`
 - Menonaktifkan infrastruktur terkelola dengan melepaskan volume dari host yang dikelola.
- Izin untuk layanan bukan bagian dari deskripsi layanan AMS dan tidak didukung oleh AMS.

Layanan yang tidak tercantum dalam deskripsi Layanan AMS tidak dapat digunakan di akun AMS. Untuk meminta dukungan untuk fitur atau layanan, silakan hubungi CSDM Anda.

- Izin yang tidak memenuhi tujuan yang Anda nyatakan karena terlalu murah hati, atau terlalu konservatif, atau diterapkan pada sumber daya yang salah. Contoh:
 - Permintaan `s3:PutObject` izin ke bucket S3 yang memiliki enkripsi KMS wajib, tanpa `KMS:Encrypt` izin ke kunci yang relevan.
 - Izin yang berkaitan dengan sumber daya yang tidak ada di akun.
 - IAM RFCs di mana deskripsi RFC tampaknya tidak cocok dengan permintaan.

Kesalahan RFC “Penerapan”

AMS “Deployment” Jenis perubahan kategori (CTs) memungkinkan Anda untuk meminta berbagai sumber daya yang didukung AMS ditambahkan ke akun Anda.

Sebagian besar AMS CTs yang membuat sumber daya didasarkan pada AWS CloudFormation templat. Sebagai pelanggan, Anda memiliki akses hanya-baca ke semua layanan AWS termasuk AWS CloudFormation, Anda dapat dengan cepat mengidentifikasi AWS CloudFormation tumpukan yang mewakili tumpukan Anda berdasarkan deskripsi tumpukan menggunakan AWS CloudFormation Konsol. Tumpukan yang gagal kemungkinan akan berada dalam keadaan `DELETE_COMPLETE`. Setelah Anda mengidentifikasi AWS CloudFormation tumpukan, peristiwa akan menunjukkan sumber daya spesifik yang gagal dibuat, dan mengapa.

Menggunakan CloudFormation dokumentasi untuk memecahkan masalah

Sebagian besar penyediaan AMS RFCs menggunakan CloudFormation templat dan dokumentasi tersebut dapat membantu pemecahan masalah. Lihat dokumentasi untuk AWS CloudFormation template itu:

- Buat kegagalan penyeimbang beban aplikasi: [AWS::ElasticLoadBalancingV2::LoadBalancer \(Application Load Balancer\)](#)
- Buat grup penskalaan Otomatis: [AWS::AutoScaling::AutoScalingGroup \(Grup Auto Scaling\)](#)
- Buat cache memcache: [AWS::ElastiCache::CacheCluster \(Cache Cluster\)](#)
- Buat cache Redis: [AWS::ElastiCache::CacheCluster \(Cache Cluster\)](#)
- [Buat DNS Hosted Zone \(digunakan dengan Create DNS private/public\): AWS::Route53::HostedZone \(R53 Hosted Zone\)](#)
- [Buat DNS Record Set \(digunakan dengan Create DNS private/public\): AWS::Route53::RecordSet \(Resource Record Set\)](#)
- Buat EC2 tumpukan: [AWS::EC2::Instance \(Elastic Compute Cloud\)](#)
- Buat Sistem File Elastis (EFS): [AWS::EFS::FileSystem \(Sistem File Elastis\)](#)
- Buat Load balancer: [AWS::ElasticLoadBalancing::LoadBalancer \(Elastic Load Balancer\)](#)
- Buat RDS DB: [AWS::RDS::DBInstance \(Database Relasional\)](#)
- Buat Amazon S3: [AWS::S3::Bucket \(Layanan Penyimpanan Sederhana\)](#)
- Buat Antrian: [AWS::SQS::Queue \(Layanan Antrian Sederhana\)](#)

RFC membuat kesalahan AMIs

Amazon Machine Image (AMI) adalah templat yang berisi konfigurasi perangkat lunak (misalnya, sistem operasi, server aplikasi, dan aplikasi). Dari AMI, Anda meluncurkan instance, yang merupakan salinan AMI yang berjalan sebagai server virtual di cloud. AMIs sangat berguna, dan diperlukan untuk membuat EC2 instance atau grup Auto Scaling; namun, Anda harus mematuhi beberapa persyaratan:

- Instance yang Anda tentukan `Ec2InstanceId` harus dalam keadaan berhenti agar RFC berhasil. Jangan gunakan instans Auto Scaling group (ASG) untuk parameter ini karena ASG akan menghentikan instance yang dihentikan.
- Untuk membuat AMS Amazon Machine Image (AMI), Anda harus memulai dengan instance AMS. Sebelum Anda dapat menggunakan instance untuk membuat AMI, Anda harus menyiapkannya

dengan memastikan bahwa instans tersebut dihentikan dan tidak bergabung dari domainnya.

Untuk detailnya, lihat [Membuat Gambar Mesin Amazon Standar Menggunakan Sysprep](#)

- Nama yang Anda tentukan untuk AMI baru harus unik di dalam akun atau RFC gagal. Cara melakukannya dijelaskan dalam [AMI | Buat](#), dan untuk detail selengkapnya, lihat dan [AWS AMI Design](#).

Note

Untuk informasi tambahan tentang persiapan pembuatan AMI, lihat [AMI | Buat](#).

RFCs membuat EC2s atau ASGs kesalahan

Untuk EC2 atau kegagalan ASG dengan batas waktu, AMS menyarankan Anda mengonfirmasi apakah AMI yang digunakan disesuaikan. Jika ya, silakan lihat langkah-langkah pembuatan AMI yang disertakan dalam panduan ini (lihat [AMI | Buat](#)) untuk memastikan bahwa AMI dibuat dengan benar. Kesalahan umum saat membuat AMI kustom adalah tidak mengikuti langkah-langkah dalam panduan untuk mengganti nama atau memanggil Sysprep.

RFCs membuat kesalahan RDS

Kegagalan Amazon Relational Database Service (RDS) dapat terjadi karena berbagai alasan karena Anda dapat menggunakan banyak mesin yang berbeda saat membuat RDS, dan setiap mesin memiliki persyaratan dan keterbatasannya sendiri. [Sebelum mencoba membuat tumpukan AMS RDS, tinjau nilai parameter AWS RDS dengan cermat, lihat Membuat DBInstance](#)

Untuk mempelajari lebih lanjut tentang Amazon RDS secara umum, termasuk rekomendasi ukuran, lihat Dokumentasi Layanan [Amazon Relational Database Service](#).

RFCs membuat kesalahan Amazon S3

Satu kesalahan umum saat membuat bucket penyimpanan S3 adalah tidak menggunakan nama unik untuk bucket. Jika Anda mengirimkan bucket S3 Create CT dengan nama yang sama dengan yang dikirimkan sebelumnya, itu akan gagal karena bucket S3 sudah ada dengan itu. BucketName ini akan dirinci di AWS CloudFormation Konsol, di mana Anda akan melihat bahwa peristiwa tumpukan menunjukkan bahwa nama bucket sudah digunakan.

Validasi RFC versus kesalahan eksekusi

Kegagalan RFC dan pesan terkait berbeda dalam pesan keluaran pada halaman detail RFC konsol AMS untuk RFC yang dipilih:

- Alasan Kegagalan Validasi hanya tersedia di Bidang Status
- Alasan Kegagalan Eksekusi tersedia di Output Eksekusi serta Bidang Status.

Pesan kesalahan RFC

Ketika Anda menemukan kesalahan berikut untuk jenis perubahan yang tercantum (CTs), Anda dapat menggunakan solusi ini untuk membantu Anda menemukan sumber masalah dan memperbaikinya.

```
{"errorMessage":"An error has occurred during RFC execution. We are investigating the issue.", "errorType":"InternalError"}
```

Jika Anda memerlukan bantuan lebih lanjut setelah merujuk pada opsi pemecahan masalah berikut, maka libatkan AMS melalui korespondensi RFC atau buat permintaan layanan. Lihat [Korespondensi dan Lampiran RFC \(Konsol\)](#) dan [Membuat Permintaan Layanan di AMS untuk detail selengkapnya](#).

Kesalahan konsumsi beban kerja (WIGS)

Note

Alat validasi untuk Windows dan Linux dapat diunduh dan dijalankan langsung di server lokal Anda, serta EC2 instance di AWS. Hal ini dapat ditemukan melalui Panduan Pengembang Aplikasi AMS Advanced [Migrating workloads: Linux pre-ingestion validation](#) dan [Migrating workloads: Windows pre-ingestion validation](#).

- Pastikan EC2 instance ada di akun AMS target. Misalnya, jika Anda telah membagikan AMI dari akun non-AMS ke akun AMS, Anda harus membuat EC2 instance di akun AMS dengan AMI bersama sebelum dapat mengirimkan RFC Workload Ingest.
- Periksa untuk melihat apakah grup keamanan yang dilampirkan pada instance memiliki lalu lintas jalan keluar yang diizinkan. Agen SSM harus dapat terhubung ke titik akhir publiknya.

- Periksa untuk melihat apakah instance memiliki izin yang tepat untuk terhubung dengan agen SSM. Izin ini disertakan dengan `customer-mc-ec2-instance-profile`, Anda dapat memeriksanya di EC2 konsol:

EC2 kesalahan penghentian tumpukan contoh

- Periksa untuk melihat apakah instance sudah dalam keadaan berhenti atau dihentikan.
- Jika EC2 instans sedang online dan Anda melihat `InternalError` kesalahan, maka kirimkan permintaan layanan untuk diselidiki AMS.
- Perhatikan bahwa Anda tidak dapat menggunakan tipe perubahan Management | Advanced stack components | EC2 instance stack | `Stop ct-3mvvt2zkyveqj` untuk menghentikan instance Auto Scaling group (ASG). Jika Anda perlu menghentikan instans ASG, maka kirimkan permintaan layanan.

EC2 instance stack membuat kesalahan

`InternalError` Pesannya berasal dari CloudFormation; alasan status `CREATION_FAILED`. Anda dapat menemukan detail tentang kegagalan tumpukan dalam peristiwa CloudWatch tumpukan dengan mengikuti langkah-langkah berikut:

- Di konsol AWS Management, Anda dapat melihat daftar peristiwa tumpukan saat tumpukan dibuat, diperbarui, atau dihapus. Dari daftar ini, temukan peristiwa kegagalan dan kemudian lihat alasan status untuk peristiwa tersebut.

Alasan status mungkin berisi pesan kesalahan dari AWS CloudFormation atau dari layanan tertentu yang dapat membantu Anda memahami masalah tersebut.

- Untuk informasi selengkapnya tentang melihat peristiwa tumpukan, lihat [Melihat Data dan Sumber Daya AWS CloudFormation Stack di AWS Management Console](#).

EC2 kesalahan pemulihan volume instance

AMS membuat RFC pemecahan masalah internal saat pemulihan volume EC2 instans gagal. Ini dilakukan karena pemulihan volume EC2 instans merupakan bagian penting dari pemulihan bencana (DR) dan AMS membuat RFC pemecahan masalah internal ini untuk Anda secara otomatis.

Saat RFC pemecahan masalah internal dibuat, spanduk ditampilkan memberi Anda tautan ke RFC. Pemecahan masalah internal RFC ini memberi Anda lebih banyak visibilitas ke kegagalan RFC dan, daripada mengirimkan percobaan ulang yang RFCs mengarah ke kesalahan yang sama, atau membuat Anda secara manual menjangkau AMS untuk kegagalan ini, Anda dapat melacak perubahan Anda dan mengetahui bahwa kegagalan sedang dikerjakan oleh AMS. Ini juga mengurangi metrik time-to-recovery (TTR) untuk perubahannya karena Operator AMS secara proaktif bekerja pada kegagalan RFC alih-alih menunggu permintaan Anda.

Cara mendapatkan bantuan dengan RFC

Anda dapat menghubungi AMS untuk mengidentifikasi akar penyebab kegagalan Anda. Jam kerja AMS adalah 24 jam sehari, 7 hari seminggu, 365 hari setahun.

AMS menyediakan beberapa jalan bagi Anda untuk meminta bantuan atau membuat permintaan layanan.

- Untuk meminta informasi atau saran, atau akses ke layanan TI yang dikelola AMS, atau meminta layanan tambahan dari AMS, gunakan konsol AMS dan kirimkan permintaan layanan. Untuk detailnya, lihat [Membuat Permintaan Layanan](#). Untuk informasi umum tentang permintaan layanan AMS, lihat [Manajemen Permintaan Layanan](#).
- Untuk melaporkan masalah kinerja layanan AWS atau AMS yang memengaruhi lingkungan terkelola Anda, gunakan konsol AMS dan kirimkan laporan insiden. Untuk detailnya, lihat [Melaporkan Insiden](#). Untuk informasi umum tentang manajemen insiden AMS, lihat [Respons insiden](#).
- Untuk pertanyaan spesifik tentang bagaimana Anda atau sumber daya atau aplikasi Anda bekerja dengan AMS, atau untuk meningkatkan insiden, kirim email ke satu atau beberapa hal berikut:
 1. Pertama, jika Anda tidak puas dengan permintaan layanan atau tanggapan laporan insiden, kirimkan email ke CSDM Anda: ams-csdlm@amazon.com
 2. Selanjutnya, jika eskalasi diperlukan, Anda dapat mengirim email ke Manajer Operasi AMS (tetapi CSDM Anda mungkin akan melakukannya): ams-opsmanager@amazon.com
 3. Eskalasi lebih lanjut akan ke Direktur AMS: ams-director@amazon.com
 4. Akhirnya, Anda selalu dapat menghubungi AMS VP: ams-vp@amazon.com

Mode Perubahan Langsung di AMS

Topik

- [Memulai dengan mode Perubahan Langsung](#)
- [Keamanan dan kepatuhan](#)
- [Ubah manajemen dalam mode Perubahan Langsung](#)
- [Membuat tumpukan menggunakan mode Perubahan Langsung](#)
- [Kasus penggunaan Mode Perubahan Langsung](#)

AWS Managed Services (AMS) Direct Change mode (DCM) memperluas manajemen perubahan AMS Advanced dengan menyediakan AWS akses asli ke akun AMS Advanced Plus dan Premium untuk menyediakan dan memperbarui AWS sumber daya. Dengan DCM, Anda memiliki opsi untuk menggunakan AWS API asli (konsol atau CLI/SDK) atau permintaan manajemen perubahan AMS Advanced untuk perubahan (RFCs), dan dalam kedua kasus sumber daya dan perubahannya sepenuhnya didukung oleh AMS, termasuk pemantauan, tambalan, cadangan, manajemen respons insiden. Sumber daya yang disediakan melalui DCM terdaftar di sistem manajemen pengetahuan layanan AMS (SKMS), bergabung dengan domain Active Directory yang dikelola AMS (bila berlaku), dan menjalankan agen manajemen AMS. Gunakan perkakas yang ada (misalnya, AWS SDK CloudFormation, dan CDK) untuk mengembangkan dan menerapkan tumpukan yang dikelola AMS. CloudFormation

 Note

Mode Perubahan Langsung tidak menghapus manajemen perubahan AMS RFCs. Anda memiliki akses penuh ke AMS RFCs dengan DCM.

[Tonton video Akash untuk mempelajari lebih lanjut \(6:30\)](#)

Memulai dengan mode Perubahan Langsung

Mulailah dengan memeriksa prasyarat dan kemudian mengirimkan permintaan perubahan (RFC) di akun AMS Advanced Anda yang memenuhi syarat.

1. Konfirmasikan bahwa akun yang ingin Anda gunakan dengan DCM memenuhi persyaratan:
 - Akun tersebut adalah AMS Advanced Plus atau Premium.
 - Akun tidak mengaktifkan Service Catalog. Saat ini kami tidak mendukung akun orientasi ke DCM dan Service Catalog secara bersamaan. Jika Anda sudah onboard ke Service Catalog tetapi tertarik dengan DCM, diskusikan kebutuhan Anda dengan manajer pengiriman layanan

cloud (CSDM) Anda. Jika Anda memutuskan untuk beralih dari Service Catalog ke DCM, offboard Service Catalog, untuk melakukan itu, sertakan permintaan dalam permintaan perubahan di bawah ini. Untuk detail tentang Service Catalog di AMS, lihat [AMS dan Service Catalog](#).

2. Kirim permintaan perubahan (RFC) menggunakan Manajemen | Akun terkelola | Mode Perubahan Langsung | Aktifkan jenis perubahan (ct-3rd4781c2nnhp). Untuk contoh panduan, lihat [Mode Perubahan Langsung | Aktifkan](#).

Setelah CT diproses, peran IAM yang telah ditentukan sebelumnya, `AWSManagedServicesCloudFormationAdminRole` dan `AWSManagedServicesUpdateRole` disediakan dalam akun yang ditentukan.

3. Tetapkan peran yang sesuai untuk pengguna yang memerlukan akses DCM menggunakan proses federasi internal Anda.

Note

Anda dapat menentukan sejumlah SAMLIdentity Penyedia, AWS Layanan, dan Entitas IAM (Peran, Pengguna, dll) untuk mengambil peran. Anda harus memberikan setidaknya satu: `SAMLIdentityProviderARNs`, `IAMEntityARNs`, atau `AWSServicePrincipals`. Untuk informasi lebih lanjut, konsultasikan dengan departemen IAM perusahaan Anda atau dengan arsitek cloud AMS (CA) Anda.

Mode Perubahan Langsung peran dan kebijakan IAM

Saat mode Perubahan Langsung diaktifkan di akun, entitas IAM baru ini diterapkan:

`AWSManagedServicesCloudFormationAdminRole`: Peran ini memberikan akses ke CloudFormation konsol, membuat dan memperbarui CloudFormation tumpukan, melihat laporan drift, dan membuat dan mengeksekusi CloudFormation ChangeSets Akses ke peran ini dikelola melalui penyedia SAMP Anda.

Kebijakan terkelola yang diterapkan dan dilampirkan pada peran `AWSManagedServicesCloudFormationAdminRole` adalah:

- Akun aplikasi AMS Advanced multi-account landing zone (MALZ)
- `AWSManagedServices_CloudFormationAdminPolicy1`

- `AWSManagedServices_CloudFormationAdminPolicy2`
- Kebijakan ini mewakili izin yang diberikan kepada `AWSManagedServicesCloudFormationAdminRole` Anda dan mitra menggunakan kebijakan ini untuk memberikan akses ke peran yang ada di akun dan mengizinkan peran tersebut untuk meluncurkan dan memperbarui CloudFormation tumpukan di akun. Ini mungkin memerlukan pembaruan kebijakan kontrol layanan AMS (SCP) tambahan untuk mengizinkan entitas IAM lainnya meluncurkan CloudFormation tumpukan.
- Akun landing zone (SALZ) akun AMS Advanced single-account
 - `AWSManagedServices_CloudFormationAdminPolicy1`
 - `AWSManagedServices_CloudFormationAdminPolicy2`
 - `cdk-legacy-mode-s3-akses` [kebijakan in-line]
 - `AWS ReadOnlyAccess` kebijakan

`AWSManagedServicesUpdateRole`: Peran ini memberikan akses terbatas ke layanan hilir AWS . APIs Peran ini diterapkan dengan kebijakan terkelola yang menyediakan operasi API yang bermutasi dan tidak bermutasi, tetapi secara umum membatasi operasi mutasi (seperti `Create/Delete/PUT`), terhadap layanan tertentu seperti IAM, KMS,, VPC, sumber daya dan konfigurasi infrastruktur `AMSGuardDuty`, dan sebagainya. Akses ke peran ini dikelola melalui penyedia SAMP Anda.

Kebijakan terkelola yang diterapkan dan dilampirkan pada peran `AWSManagedServicesUpdateRole` adalah:

- Akun aplikasi landing zone multi-akun AMS tingkat lanjut
 - `AWSManagedServicesUpdateBasePolicy`
 - `AWSManagedServicesUpdateDenyPolicy`
 - `AWSManagedServicesUpdateDenyProvisioningPolicy`
 - `AWSManagedServicesUpdateEC2dan RDSPolicy`
 - `AWSManagedServicesUpdateDenyActionsOnAMSInfraKebijakan`
- Akun landing zone akun tunggal AMS Advanced
 - `AWSManagedServicesUpdateBasePolicy`
 - `AWSManagedServicesUpdateDenyProvisioningPolicy`
 - `AWSManagedServicesUpdateEC2dan RDSPolicy`
 - `AWSManagedServicesUpdateDenyActionsOnAMSInfraKebijakan1`

- `AWSManagedServicesUpdateDenyActionsOnAMSInfraKebijakan2`

Selain itu, `AWSManagedServicesUpdateRole` peran kebijakan terkelola juga memiliki kebijakan AWS terkelola yang `ViewOnlyAccess` melekat padanya.

Keamanan dan kepatuhan

Keamanan dan kepatuhan adalah tanggung jawab bersama antara AMS Advanced dan Anda, sebagai pelanggan kami. Mode AMS Advanced Direct Change tidak mengubah tanggung jawab bersama ini.

Keamanan dalam mode Perubahan Langsung

AMS Advanced menawarkan nilai tambahan dengan landing zone preskriptif, sistem manajemen perubahan, dan manajemen akses. Saat menggunakan mode Perubahan Langsung, model tanggung jawab ini tidak berubah. Namun, Anda harus mewaspadai risiko tambahan.

Peran “Perbarui” Mode Perubahan Langsung (lihat [Mode Perubahan Langsung peran dan kebijakan IAM](#)) memberikan izin tinggi yang memungkinkan entitas mengaksesnya, untuk membuat perubahan pada sumber daya infrastruktur layanan yang didukung AMS dalam akun Anda. Dengan izin yang tinggi, beragam risiko ada tergantung pada sumber daya, layanan, dan tindakan, terutama dalam situasi di mana perubahan yang salah dibuat karena pengawasan, kesalahan, atau kurangnya kepatuhan terhadap proses internal dan kerangka kontrol Anda.

Sesuai Standar Teknis AMS, risiko berikut telah diidentifikasi dan rekomendasi dibuat sebagai berikut. Informasi terperinci tentang Standar Teknis AMS tersedia melalui AWS Artifact. Untuk mengakses AWS Artifact, hubungi CSDM Anda untuk instruksi atau pergi ke [Memulai](#) dengan. AWS Artifact

AMS-STD-001: Penandaan

Standar	Apakah itu rusak	Risiko	Rekomendasi
Semua sumber daya yang dimiliki AMS harus memiliki pasangan nilai kunci berikut	Ya. Istirahat untuk CloudFormation CloudTrail,, EFS OpenSearch,, CloudWatch Logs,	Penandaan sumber daya AMS yang salah dapat berdampak buruk pada operasi pelaporan, peringatan	Akses harus dibatasi untuk membuat perubahan apa pun pada persyaratan penandaan default

Standar	Apakah itu rusak	Risiko	Rekomendasi
Semua tag milik AMS selain yang tercantum di atas harus memiliki awalan seperti AMS* atau dalam kasus. MC* upper/lower/mix	SQS, SSM, Tagging api - karena layanan ini tidak mendukung aws : TagsKey kondisi untuk membatasi penandaan untuk namespace AMS. Standar yang diberikan dalam tabel AMS-STD-003, berikut, menyatakan bahwa Anda dapat mengubah, Lingkungan dan Appld AppName, tetapi tidak untuk sumber daya milik AMS. Tidak dapat dicapai melalui izin IAM.	n, dan penambalan sumber daya Anda, di sisi AMS.	AMS untuk siapa pun selain tim AMS.
Tag apa pun pada tumpukan milik AMS tidak boleh dihapus berdasarkan permintaan perubahan Anda.	Ya. CloudFormation tidak mendukung aws : TagsKey kondisi untuk membatasi tag untuk namespace AMS.		

Standar	Apakah itu rusak	Risiko	Rekomendasi
Anda tidak diizinkan untuk menggunakan konvensi penamaan tag AMS di infrastruktur Anda seperti yang disebutkan dalam tabel AMS-STD-002, selanjutnya.	Ya. Istirahat untuk CloudFormation CloudTrail, Amazon Elastic File System (EFS), OpenSearch, CloudWatch Log, Amazon Simple Queue Service (SQS), Amazon EC2 Systems Manager (SSM), API Tagging; layanan ini tidak <code>aws:TagsKey</code> mendukung kondisi untuk membatasi penandaan pada namespace AMS.		

AMS-STD-002: Identity and Access Management (IAM)

Standar	Apakah itu rusak	Risiko	Rekomendasi
4.7 Tindakan, yang melewati proses manajemen perubahan (RFC), tidak boleh diizinkan seperti memulai atau menghentikan instance, pembuatan bucket S3 atau instans RDS, dan sebagainya. Akun mode pengembang	Ya. Tujuan tindakan layanan mandiri memungkinkan Anda melakukan tindakan melewati sistem AMS RFC.	Model akses aman adalah aspek teknis inti AMS dan pengguna IAM untuk konsol atau akses terprogram menghindari kontrol akses ini. Akses pengguna IAM tidak dipantau oleh manajemen perubahan AMS.	Pengguna IAM harus dibatasi waktu dan diberikan izin berdasarkan hak istimewa paling sedikit dan. need-to-know

Standar	Apakah itu rusak	Risiko	Rekomendasi
dan layanan mode Penyediaan Layanan Mandiri (SSPS) dikecualikan selama tindakan dilakukan dalam batas-batas peran yang ditugaskan.		Akses CloudTrail hanya login.	

AMS-STD-003: Keamanan Jaringan

Standar	Apakah itu rusak	Risiko	Rekomendasi
S2. IP elastis pada EC2 instans harus digunakan hanya dengan perjanjian penerimaan risiko formal, atau dengan kasus penggunaan yang valid oleh tim internal.	Ya. Tindakan layanan mandiri memungkinkan Anda untuk mengaitkan dan memisahkan alamat IP elastis (EIP).	Menambahkan IP elastis ke sebuah instance memaparkannya ke Internet. Hal ini meningkatkan risiko pengungkapan informasi dan aktivitas yang tidak sah.	Blokir lalu lintas yang tidak perlu ke instans itu melalui grup keamanan, dan verifikasi bahwa grup keamanan Anda dilampirkan dengan instans untuk memastikan bahwa itu memungkinkan lalu lintas hanya sesuai kebutuhan untuk alasan bisnis.
S14. VPC Peering dan koneksi endpoint antar akun milik pelanggan yang sama dapat diizinkan.	Ya. Tidak mungkin melalui kebijakan IAM.	Lalu lintas yang meninggalkan akun AMS Anda tidak dipantau setelah keluar dari batas akun.	Kami merekomendasikan mengintip hanya dengan akun AMS yang Anda miliki. Jika kasus penggunaan Anda mengharuskan ini, gunakan grup

Standar	Apakah itu rusak	Risiko	Rekomendasi
			keamanan dan tabel rute untuk membatasi rentang lalu lintas, sumber daya, dan jenis apa yang dapat keluar melalui koneksi yang relevan.
Basis AMS AMIs dapat dibagi antara akun yang dikelola AMS dan tidak dikelola selama kami dapat memverifikasi bahwa akun tersebut dimiliki oleh organisasi yang sama. AWS		AMIs mungkin berisi data sensitif dan mungkin terpapar ke akun yang tidak diinginkan.	Bagikan hanya AMIs dengan akun yang dimiliki oleh organisasi Anda atau validasi kasus penggunaan dan informasi akun sebelum berbagi di luar organisasi.

AMS-STD-007: Penebangan

Standar	Apakah itu rusak	Risiko	Rekomendasi
19. Setiap log dapat diteruskan dari satu akun AMS ke akun AMS lain dari pelanggan yang sama.	Ya. Potensi ketidakamanan untuk log pelanggan karena verifikasi akun pelanggan berada di organisasi yang sama tidak dapat dicapai melalui kebijakan IAM.	Log mungkin berisi data sensitif dan mungkin terpapar ke akun yang tidak diinginkan.	Bagikan log hanya dengan akun yang dikelola oleh AWS Org Anda, atau validasi kasus penggunaan dan informasi akun sebelum berbagi di luar organisasi Anda. Kami dapat memverifikasi ini melalui berbagai
20. Setiap log dapat diteruskan dari AMS ke akun non-AMS hanya jika akun non-AMS dimiliki oleh pelanggan			

Standar	Apakah itu rusak	Risiko	Rekomendasi
AMS yang sama (dengan mengonfirmasi bahwa mereka berada di bawah AWS Organizations akun yang sama atau dengan mencocokkan domain email dengan nama perusahaan pelanggan dan akun terkait PAYER) menggunakan alat internal.			cara, periksa dengan manajer pengirim layanan cloud (CSDM) Anda.

Bekerja dengan tim otorisasi dan otentikasi internal Anda untuk mengontrol izin ke peran mode Perubahan Langsung yang sesuai.

Kepatuhan dalam mode Perubahan Langsung

Mode Perubahan Langsung kompatibel dengan beban kerja produksi dan non-produksi. Anda bertanggung jawab untuk memastikan kepatuhan terhadap standar kepatuhan apa pun (misalnya, PHI, HIPAA, PCI), dan untuk memastikan bahwa penggunaan mode Perubahan Langsung sesuai dengan kerangka kerja dan standar kontrol internal Anda.

Ubah manajemen dalam mode Perubahan Langsung

Manajemen perubahan adalah proses yang digunakan AMS Advanced untuk mengimplementasikan permintaan perubahan. Permintaan untuk perubahan (RFC) adalah permintaan yang dibuat oleh Anda, atau AMS Advanced melalui antarmuka AMS Advanced untuk membuat perubahan pada lingkungan terkelola Anda dan menyertakan ID AMS Advanced change type (CT) untuk operasi tertentu. Untuk informasi selengkapnya, lihat [Mengubah manajemen](#).

Note

Mode Perubahan Langsung tidak menghapus manajemen perubahan AMS RFCs, Anda masih memiliki akses penuh ke AMS RFCs dengan DCM.

Mode Perubahan Langsung AMS (DCM) memperluas manajemen perubahan AMS Advanced dengan menyediakan AWS akses asli ke akun AMS Advanced Plus dan Premium untuk menyediakan dan memperbarui AWS sumber daya. Pengguna yang telah diberikan izin mode Perubahan Langsung melalui peran IAM, dapat menggunakan akses AWS API asli ke penyediaan dan membuat perubahan pada sumber daya di akun AMS Advanced mereka. Pengguna masih dapat menggunakan manajemen perubahan AMS Advanced RFCs menggunakan peran IAM yang sama. Dalam kedua kasus, sumber daya dan perubahannya sepenuhnya didukung oleh AMS, termasuk pemantauan, tambalan, cadangan, manajemen respons insiden. Pengguna yang tidak memiliki peran yang sesuai dalam akun ini harus menggunakan proses RFC manajemen perubahan AMS Advanced untuk melakukan perubahan.

Ubah kasus penggunaan manajemen

Untuk alasan keamanan, beberapa perubahan pada AMS Advanced hanya dapat dilakukan melalui proses Change Management Request for Change (RFC).

AWSManagedServicesCloudFormationAdminRoleIni terbatas pada tindakan yang diambil melalui CloudFormation (CFN). Untuk selengkapnya tentang cara membuat tumpukan melalui DCM, lihat [Membuat tumpukan menggunakan mode Perubahan Langsung](#). AWSManagedServicesUpdateRoleIni dibatasi untuk tindakan berikut.

[Misalnya penelusuran untuk setiap jenis perubahan, termasuk jenis perubahan Manajemen | Akun terkelola | Mode Perubahan Langsung | Aktifkan \(ct-3rd4781c2nnhp\)](#), lihat bagian “Informasi Tambahan” untuk jenis perubahan yang relevan di bagian AMS Advanced Change Type Reference [Change Type by Classification](#).

Layanan	Tindakan
AWS Key Management Service (AWS KMS)	Perbarui
AWS Certificate Manager	Buat
AWS Identity and Access Management (IAM)	Setiap

Layanan	Tindakan
AWS VPN	Setiap
Penjadwal Sumber Daya AMS	
AWS Backup	Buat rencana cadangan
Konsumsi Beban Kerja AMS () WIGs	Setiap
Penyaringan Jalan Masuk AMS (Palo Alto Terkelola)	
Perubahan akun AMS Advanced MALZ	
Amazon GuardDuty	
Akses Stack Tingkat Lanjut AMS	Setiap
Volume Amazon Elastic Block Store (EBS)	Hapus
Enkripsi default Amazon Elastic Block Store (EBS)	Aktifkan enkripsi default
Amazon Elastic Compute Cloud (Amazon EC2)	Ubah nama host
Amazon Machine Image (AMI)	Hapus, bagikan
Grup EC2 Keamanan Amazon	Setiap
AMS SSPS Tingkat Lanjut	
AWS Microsoft AD yang dikelola	
Mode pengembang AMS Lanjutan	
Amazon Simple Storage Service (Amazon S3)	Buat kebijakan bucket S3
AWS Systems Manager	Buat

Membuat tumpukan menggunakan mode Perubahan Langsung

Ada dua persyaratan saat meluncurkan tumpukan dalam CloudFormation menggunakan `AWSManagedServicesCloudFormationAdminRole`, agar tumpukan dikelola oleh AMS:

- Template harus berisi `fileAmsStackTransform`.
- Nama tumpukan harus dimulai dengan awalan `stack-` diikuti oleh string alfanumerik 17 karakter.

Note

Agar berhasil menggunakan `AmsStackTransform`, Anda harus mengakui bahwa template tumpukan Anda berisi `CAPABILITY_AUTO_EXPAND` kemampuan agar AWS CloudFormation (CFN) membuat atau memperbarui tumpukan. Anda melakukan ini dengan meneruskan `CAPABILITY_AUTO_EXPAND` sebagai bagian dari permintaan `create-stack` Anda. CFN menolak permintaan jika kemampuan ini tidak diakui ketika disertakan dalam template. `AmsStackTransform` Konsol CFN memastikan bahwa Anda melewati kemampuan ini jika Anda memiliki transformasi di template Anda, tetapi ini dapat dilewatkan ketika Anda berinteraksi dengan CFN melalui mereka. APIs

Anda harus meneruskan kemampuan ini setiap kali Anda menggunakan panggilan API CFN berikut:

- [CreateChangeSet](#)
- [CreateStack](#)
- [UpdateStack](#)

Saat membuat atau memperbarui tumpukan dengan DCM, validasi dan augmentasi CFN Ingest dan Pembaruan CTs Tumpukan yang sama dilakukan di tumpukan, untuk informasi selengkapnya lihat Pedoman [AWS CloudFormation Ingest](#), Praktik Terbaik, dan Batasan. Pengecualian untuk ini adalah bahwa grup keamanan default AMS (SGs) tidak akan dilampirkan ke instance atau EC2 instance yang berdiri sendiri di grup Auto Scaling (). ASGs Saat Anda membuat CloudFormation template, dengan EC2 instance yang berdiri sendiri atau ASGs, Anda dapat melampirkan default. SGs

Note

Peran IAM sekarang dapat dibuat dan dikelola dengan.
`AWSManagedServicesCloudFormationAdminRole`

Default AMS SGs memiliki aturan masuk dan keluar yang memungkinkan instans berhasil diluncurkan dan diakses nanti melalui SSH atau RDP oleh operasi AMS dan Anda. Jika Anda menemukan bahwa grup keamanan default AMS terlalu permisif, Anda dapat membuat sendiri SGs dengan aturan yang lebih ketat dan melampirkannya ke instans Anda, asalkan masih memungkinkan Anda dan operasi AMS untuk mengakses instans selama insiden.

Grup keamanan default AMS adalah sebagai berikut:

- `SentinelDefaultSecurityGroupPrivateOnly`: Dapat diakses di template CFN melalui parameter SSM ini `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- `SentinelDefaultSecurityGroupPrivateOnlyEgressAll`: Dapat diakses di template CFN melalui parameter SSM ini `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

Transformasi AMS

Tambahkan `Transform` pernyataan ke CloudFormation template Anda. Ini menambahkan CloudFormation makro yang memvalidasi dan mendaftarkan tumpukan dengan AMS pada waktu peluncuran.

Contoh JSON

```
"Transform": {
  "Name": "AmsStackTransform",
  "Parameters": {
    "StackId": {"Ref" : "AWS::StackId"}
  }
}
```

Contoh YAMM

```
Transform:
  Name: AmsStackTransform
```

Parameters:
 StackId: !Ref 'AWS::*StackId*'

Tambahkan juga Transform pernyataan saat memperbarui template tumpukan yang ada.

Contoh JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
  "Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

Contoh YAMM

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
```

```
Default: HelloWorldTopic
Resources:
  SnsTopic:
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Ref TopicName
```

Nama tumpukan

Nama tumpukan harus dimulai dengan awalan `stack-` diikuti oleh string alfanumerik 17 karakter. Ini untuk menjaga kompatibilitas dengan sistem AMS lain yang beroperasi pada tumpukan AMS IDs.

Berikut ini adalah contoh cara untuk menghasilkan tumpukan yang kompatibel IDs:

Bash:

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python:

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

PowerShell:

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17 | %
{[char]$_}) )
```

Kasus penggunaan Mode Perubahan Langsung

Berikut ini adalah kasus penggunaan untuk Mode Perubahan Langsung:

Penyediaan dan manajemen sumber daya melalui AWS CloudFormation

- Integrasikan perkakas dan proses CloudFormation berbasis yang ada.

Manajemen dan pembaruan sumber daya yang sedang berlangsung

- Perubahan atom kecil dengan risiko rendah.

- Perubahan yang seharusnya berjalan melalui RFC manual atau otomatis.
- Perangkat yang membutuhkan akses AWS API asli.
- Peran DCM dapat digunakan jika Anda berada dalam tahap migrasi. Tim migrasi memanfaatkan izin di DCM untuk membuat atau memodifikasi tumpukan.
- Peran DCM dapat digunakan dalam CI/CD pipeline untuk membangun baru AMIs, membuat tugas Amazon ECS, dan sebagainya.

Mode Pengembang AMS Lanjutan

Topik

- [Memulai mode AMS Advanced Developer](#)
- [Keamanan dan kepatuhan dalam mode Pengembang](#)
- [Ubah manajemen dalam mode Pengembang](#)
- [Penyediaan infrastruktur dalam mode Pengembang AMS](#)
- [Kontrol Detektif dalam mode Pengembang AMS](#)
- [Pencatatan, pemantauan, dan manajemen acara dalam mode Pengembang AMS](#)
- [Manajemen insiden dalam mode Pengembang AMS](#)
- [Manajemen tambalan dalam mode Pengembang AMS](#)
- [Manajemen kontinuitas dalam mode Pengembang AMS](#)
- [Keamanan dan manajemen akses dalam mode Pengembang AMS](#)

Mode pengembang AWS Managed Services (AMS) menggunakan izin yang ditingkatkan di akun AMS Advanced Plus dan Premium untuk menyediakan dan memperbarui sumber daya AWS di luar proses manajemen perubahan AMS Advanced. Mode AMS Advanced Developer melakukan ini dengan memanfaatkan panggilan AWS API native dalam AMS Advanced Virtual Private Cloud (VPC), memungkinkan Anda merancang dan mengimplementasikan infrastruktur dan aplikasi di lingkungan terkelola Anda.

Saat menggunakan akun yang mengaktifkan mode Pengembang, manajemen kontinuitas, manajemen tambalan, dan manajemen perubahan disediakan untuk sumber daya yang disediakan melalui proses manajemen perubahan AMS Advanced atau dengan menggunakan AMS Amazon Machine Image (AMI). Namun, fitur manajemen AMS ini tidak ditawarkan untuk sumber daya yang disediakan melalui native. AWS APIs

Anda bertanggung jawab untuk memantau sumber daya infrastruktur yang disediakan di luar proses manajemen perubahan AMS Advanced. Mode pengembang kompatibel dengan beban kerja produksi dan non-produksi. Dengan izin yang tinggi, Anda memiliki tanggung jawab yang meningkat untuk memastikan kepatuhan terhadap kontrol internal.

 Important

Sumber daya yang Anda buat menggunakan mode Pengembang dapat dikelola oleh AMS Advanced hanya jika dibuat menggunakan proses manajemen perubahan AMS Advanced.

Mode pengembang adalah salah satu mode AMS Advanced yang dapat Anda gunakan. Lihat informasi yang lebih lengkap di [Ikhtisar mode](#).

Memulai mode AMS Advanced Developer

Pelajari berbagai akun AMS Advanced dengan mode AMS Advanced Developer dan cara mengimplementasikan mode Developer dengan sukses.

Topik

- [Sebelum Anda memulai dengan mode AMS Developer](#)
- [Prasyarat untuk mode Pengembang AMS](#)
- [Cara menerapkan mode AMS Advanced Developer](#)
- [Izin mode Pengembang AMS Lanjutan](#)

Sebelum Anda memulai dengan mode AMS Developer

Sebelum menerapkan mode Developer, ada beberapa hal yang harus Anda ketahui.

AMS Advanced tidak dapat mengelola tumpukan atau sumber daya yang ada di DevMode akun yang dibuat di luar proses manajemen perubahan AMS Advanced melalui request for change (RFCs). Namun, saat akun masuk DevMode, AMS Advanced terus mengelola sumber daya yang disediakan melalui proses manajemen perubahan AMS Advanced dengan RFCs

Anda tidak dapat memulai dengan DevMode akun dan kemudian menutupnya ke akun aplikasi AMS Advanced-managed.

Prasyarat untuk mode Pengembang AMS

Berikut ini adalah prasyarat untuk menerapkan mode Pengembang:

- Anda harus menjadi pelanggan AMS Advanced dengan setidaknya satu akun AMS Advanced Plus atau Premium onboard.
- Akun apa pun yang Anda gunakan harus berupa akun AMS Advanced Plus atau Premium.
- Zona Pendaratan Multi-Akun (MALZ): Anda harus menggunakan peran yang `AWSManagedServicesDevelopmentRole` telah ditentukan AWS Identity and Access Management (IAM). Anda meminta peran ini. Bagian selanjutnya menjelaskan cara memperoleh izin mode Pengembang.
- Single-Account Landing Zone (SALZ): Anda harus menggunakan peran yang `customer_developer_role` telah ditentukan AWS Identity and Access Management (IAM). Anda meminta peran ini. Bagian selanjutnya menjelaskan cara memperoleh izin mode Pengembang.

Cara menerapkan mode AMS Advanced Developer

Anda menerapkan mode Developer dengan meminta agar akun AMS Advanced Anda yang memenuhi syarat disediakan dengan peran IAM yang telah ditentukan sebelumnya:

- MALZ: `AWSManagedServicesDevelopmentRole`
- SALZ: `customer_developer_role`

Anda kemudian menetapkan peran tersebut ke pengguna yang relevan di jaringan federasi Anda.

AMS Advanced merekomendasikan agar Anda memastikan bahwa penggunaan mode Developer sesuai dengan kerangka kerja dan standar kontrol internal Anda karena mode Pengembang menciptakan dua vektor perubahan: Manajemen perubahan AMS Advanced untuk sumber daya yang dikelola AMS Advanced dan federasi peran yang dikelola pelanggan untuk sumber daya yang Anda, sebagai pelanggan kami, kelola. Meskipun proses AMS Advanced tetap sesuai dengan deklarasi kami, proses pelanggan dan kerangka kerja kontrol mungkin perlu diperbarui.

Untuk mengimplementasikan mode Developer di akun AMS Advanced

1. Konfirmasikan akun yang ingin Anda gunakan dengan mode Pengembang memenuhi persyaratan yang tercantum di [Prasyarat untuk mode Pengembang AMS](#).

2. Kirim permintaan perubahan (RFC) menggunakan tipe perubahan (CT) Manajemen | Akun terkelola | Mode pengembang | Aktifkan (diperlukan tinjauan). Untuk contoh cara menggunakan CT ini, lihat [Mode Pengembang | Aktifkan \(Review Required\)](#).

Setelah CT diproses, peran IAM yang telah ditentukan, (AWSManagedServicesDevelopmentRole untuk MALZ, **customer_developer_role** untuk SALZ), disediakan di akun yang diminta.

3. Tetapkan peran yang sesuai kepada pengguna yang memerlukan akses mode Pengembang menggunakan proses federasi internal Anda.

AMS Advanced menyarankan Anda membatasi akses untuk mencegah penyediaan, atau perubahan pada, sumber daya yang tidak diinginkan atau tidak disetujui.

Izin mode Pengembang AMS Lanjutan

Peran yang telah ditentukan sebelumnya (AWSManagedServicesDevelopmentRole untuk MALZ, **customer_developer_role** untuk SALZ), memberikan izin untuk membuat sumber daya infrastruktur aplikasi dalam VPC AMS Advanced, termasuk peran IAM, sekaligus membatasi akses ke komponen layanan bersama yang dioperasikan oleh AMS Advanced (misalnya, host manajemen, pengontrol domain, Trend Micro EPS, benteng, dan layanan AWS yang tidak didukung). Peran ini juga membatasi akses ke log Layanan AWS Lanjutan Amazon GuardDuty, AWS Organizations, AWS Directory Service APIs, dan AMS.

Meskipun peran memungkinkan Anda membuat peran IAM tambahan, batas izin yang sama yang disertakan dalam akses mode Pengembang diberlakukan pada peran IAM apa pun yang dibuat oleh AWSManagedServicesDevelopmentRole

Keamanan dan kepatuhan dalam mode Pengembang

Keamanan dan kepatuhan adalah tanggung jawab bersama antara AMS Advanced dan Anda sebagai pelanggan kami. Mode AMS Advanced Developer mengalihkan tanggung jawab bersama kepada Anda atas sumber daya yang disediakan di luar proses manajemen perubahan atau disediakan melalui manajemen perubahan tetapi diperbarui dengan izin mode Pengembang. Untuk informasi selengkapnya tentang tanggung jawab bersama, lihat [AWS Managed Services](#).

Peringatan:

- DevMode memungkinkan Anda dan tim resmi Anda untuk melewati deny-by-default prinsip-prinsip inti keamanan AMS. Keuntungan, swalayan, lebih sedikit waktu menunggu AMS harus ditimbang

terhadap kerugiannya, siapa pun dapat melakukan tindakan tak terduga dan destruktif tanpa sepengetahuan tim keamanan mereka. Jenis perubahan otomatis untuk mengaktifkan mode Dev dan mode Perubahan Langsung diekspos, dan setiap orang yang berwenang di organisasi Anda dapat menjalankannya CTs dan mengaktifkan mode ini.

- Anda bertanggung jawab untuk mengelola izin eksekusi CT dari basis pengguna Anda.
- AMS tidak mengelola izin eksekusi CT

Rekomendasi:

- Lindungi
 - Pelanggan dapat mencegah akses ke CT ini melalui izin, lihat [Membatasi izin dengan pernyataan](#) kebijakan peran IAM
 - Mencegah akses ke CT ini dengan menerapkan proxy seperti sistem ITSM
 - Memanfaatkan kebijakan kontrol layanan (SCPs) yang mencegah kebijakan dan perilaku sesuai kebutuhan, lihat Perpustakaan Kontrol [Pencegahan dan Detektif AMS](#)
- Mendeteksi
 - Pantau RFC Anda untuk ini CTs (Aktifkan mode pengembang ct-1opjmhuddw194 dan mode perubahan langsung, Aktifkan ct-3rd4781c2nnhp) dieksekusi dan merespons sesuai
 - Tinjau and/or audit akun Anda untuk keberadaan sumber daya IAM untuk mengidentifikasi akun tersebut di mana mode Pengembang atau mode Perubahan Langsung telah diterapkan
- Menanggapi
 - Hapus akun dalam mode Pengembang sesuai kebutuhan

Keamanan dalam mode Pengembang

AMS Advanced menawarkan nilai tambahan dengan landing zone preskriptif, sistem manajemen perubahan, dan manajemen akses. Saat menggunakan mode Pengembang, nilai keamanan AMS Advanced dipertahankan dengan menggunakan konfigurasi akun yang sama dari akun AMS Advanced standar yang menetapkan jaringan pengerasan keamanan AMS Advanced dasar. Jaringan dilindungi oleh batas izin yang diberlakukan dalam peran (AWSManagedServicesDevelopmentRole untuk MALZ, **customer_developer_role** untuk SALZ), yang membatasi pengguna untuk memecah perlindungan parameter yang ditetapkan saat akun disiapkan.

Misalnya, pengguna dengan peran dapat mengakses Amazon Route 53 tetapi zona host internal AMS Advanced dibatasi. Batas izin yang sama diberlakukan pada peran IAM yang dibuat oleh `AWSManagedServicesDevelopmentRole`, menegakkan batasan izin pada yang membatasi pengguna untuk memecah perlindungan parameter `AWSManagedServicesDevelopmentRole` yang ditetapkan saat akun di-onboard ke AMS Advanced.

Kepatuhan dalam mode Pengembang

Mode pengembang kompatibel dengan beban kerja produksi dan non-produksi. Anda bertanggung jawab untuk memastikan kepatuhan terhadap standar kepatuhan apa pun (misalnya, PHI, HIPAA, PCI), dan untuk memastikan bahwa penggunaan mode Pengembang sesuai dengan kerangka kerja dan standar pengendalian internal Anda.

Ubah manajemen dalam mode Pengembang

Manajemen perubahan adalah proses yang digunakan layanan AMS Advanced untuk mengimplementasikan permintaan perubahan. Permintaan untuk perubahan (RFC) adalah permintaan yang dibuat oleh Anda atau AMS Advanced melalui antarmuka AMS Advanced untuk membuat perubahan pada lingkungan terkelola Anda dan menyertakan ID tipe perubahan (CT) untuk operasi tertentu. Untuk informasi selengkapnya, lihat [Ubah mode manajemen](#).

Manajemen perubahan tidak diberlakukan di akun AMS Advanced di mana izin mode Pengembang diberikan. Pengguna yang telah diberikan izin mode Pengembang dengan peran IAM (`AWSManagedServicesDevelopmentRole` untuk MALZ, **customer_developer_role** untuk SALZ), dapat menggunakan akses AWS API asli ke penyedia dan membuat perubahan pada sumber daya di akun AMS Advanced mereka. Pengguna yang tidak memiliki peran yang sesuai dalam akun ini harus menggunakan proses manajemen perubahan AMS Advanced untuk melakukan perubahan.

Important

Sumber daya yang Anda buat menggunakan mode Pengembang dapat dikelola oleh AMS Advanced hanya jika dibuat menggunakan proses manajemen perubahan AMS Advanced. Permintaan untuk perubahan yang dikirimkan ke AMS Advanced untuk sumber daya yang dibuat di luar proses manajemen perubahan AMS Advanced ditolak oleh AMS Advanced karena harus ditangani oleh Anda.

Pembatasan API layanan penyediaan layanan mandiri

Semua layanan mandiri AMS Advanced didukung dengan mode Pengembang. Akses ke layanan yang disediakan sendiri tunduk pada batasan yang diuraikan di masing-masing bagian panduan pengguna untuk masing-masing. Jika layanan yang disediakan sendiri tidak tersedia dengan peran mode Pengembang, Anda dapat meminta peran yang diperbarui melalui jenis perubahan mode Pengembang.

Layanan berikut tidak menyediakan akses penuh ke layanan APIs:

Layanan Penyediaan Mandiri Dibatasi dalam mode Pengembang

Layanan	Catatan
Amazon API Gateway	Semua APIs panggilan Gateway diperbolehkan kecuali <code>SetWebACL</code> .
Penskalaan Otomatis Aplikasi	Hanya dapat mendaftarkan atau membatalkan pendaftaran target yang dapat diskalakan, dan menempatkan atau menghapus kebijakan penskalaan.
AWS CloudFormation	Tidak dapat mengakses atau memodifikasi CloudFormation tumpukan yang memiliki nama yang diawali dengan <code>mc-</code>
AWS CloudTrail	Tidak dapat mengakses atau memodifikasi CloudTrail sumber daya yang memiliki nama yang diawali dengan <code>ams-</code> and/or <code>mc-</code> .
Amazon Cognito (Kolam Pengguna)	Tidak dapat mengaitkan token perangkat lunak. Tidak dapat membuat kumpulan pengguna, pekerjaan impor pengguna, server sumber daya, atau penyedia identitas.
AWS Directory Service	Hanya AWS Directory Service tindakan berikut yang diperlukan oleh Connect dan WorkSpaces layanan. Semua tindakan

Layanan	Catatan
	Directory Service lainnya ditolak oleh kebijakan batas izin mode Pengembang: • <code>ds:AuthorizeApplication</code> • <code>ds:CreateAlias</code> • <code>ds:CreateIdentityPoolDirectory</code> • <code>ds>DeleteDirectory</code> • <code>ds:DescribeDirectories</code> • <code>ds:GetAuthorizedApplicationDetails</code> • <code>ds:ListAuthorizedApplications</code> • <code>ds:UnauthorizeApplication</code> Dalam akun landing zone akun tunggal, kebijakan batas secara eksplisit menolak akses ke direktori terkelola AMS Advanced yang digunakan oleh AMS Advanced untuk mempertahankan akses ke akun yang diaktifkan mode pengembang.
Amazon Elastic Compute Cloud	Tidak dapat mengakses Amazon EC2 APIs yang berisi <code>string:DhcpOptions</code>, <code>Gateway</code>, <code>Subnet</code>, <code>VPC</code>, dan <code>VPN</code>. Tidak dapat mengakses atau memodifikasi EC2 sumber daya Amazon yang memiliki tag yang diawali dengan <code>AMS</code>, <code>mcManagement</code>, <code>HostASG</code>, and/or <code>sentinel</code>.

Layanan	Catatan
Amazon EC2 (Laporan)	Hanya akses tampilan yang diberikan (tidak dapat memodifikasi). Catatan: Amazon EC2 Reports sedang bergerak. Item menu Laporan akan dihapus dari menu navigasi EC2 konsol Amazon. Untuk melihat laporan EC2 penggunaan Amazon setelah dihapus, gunakan konsol AWS Billing dan Manajemen Biaya.
AWS Identity and Access Management (IAM)	Tidak dapat menghapus batas izin yang ada, atau mengubah kebijakan kata sandi pengguna IAM. Tidak dapat membuat atau memodifikasi sumber daya IAM kecuali Anda menggunakan peran IAM yang benar (<code>AWSManagedServicesDevelopmentRole</code> untuk MALZ, customer_developer_role untuk SALZ)). Tidak dapat mengubah sumber daya IAM yang diawali dengan: <code>ams,,mc,customer_deny_policy</code> . and/or <code>sentinel</code> Saat membuat sumber daya IAM baru (peran, pengguna, atau grup), batas izin (MALZ:AWSManagedServicesDevelopmentRolePermissionsBoundary , SALZ:ams-app-infra-permissions-boundary) harus dilampirkan.
AWS Key Management Service (AWS KMS)	Tidak dapat mengakses atau memodifikasi kunci KMS yang dikelola lanjutan AMS.
AWS Lambda	Tidak dapat mengakses atau memodifikasi AWS Lambda fungsi yang diawali dengan AMS.

Layanan	Catatan
CloudWatch Log	Tidak dapat mengakses aliran CloudWatch log yang nama diawali dengan:mc,aws,lambda. and/or AMS
Amazon Relational Database Service (Amazon RDS)	Tidak dapat mengakses atau memodifikasi database Amazon Relational Database Service (Amazon RDS) DBs () yang memiliki nama yang diawali dengan:. mc -
AWS Resource Groups	Hanya dapat mengaksesGet,List, dan tindakan API Grup Search Sumber Daya.
Amazon Route 53	Tidak dapat mengakses atau memodifikasi sumber daya Route53 AMS yang dikelola lanjutan.
Amazon S3	Tidak dapat mengakses bucket Amazon S3 yang memiliki nama yang diawali dengan:ams - *,,, ams atau. ms - a mc - a
AWS Security Token Service	Satu-satunya API layanan token keamanan yang diizinkan adalahDecodeAuthorizationMessage .
Amazon SNS	Tidak dapat mengakses topik SNS yang memiliki nama yang diawali dengan:AMS-,Energon-Topic , atau. MMS-Topic
AWS Systems Manager (SSM)	Tidak dapat mengubah parameter SSM yang diawali denganams,mc, atau. svc Tidak dapat menggunakan SSM API SendCommand terhadap EC2 instans Amazon yang memiliki tag yang diawali dengan atau. ams mc

Layanan	Catatan
AWS Menandai	Anda hanya memiliki akses ke tindakan API AWS Tagging yang diawali dengan. Get
AWS Lake Formation	Tindakan AWS Lake Formation API berikut ditolak: • lakeformation:DescribeResource • lakeformation:GetDataLakeSettings • lakeformation:DeregisterResource • lakeformation:RegisterResource • lakeformation:UpdateResource • lakeformation:PutDataLakeSettings
Amazon Elastic Inference	Anda hanya dapat memanggil aksi Elastic Inference API. elastic-inference:Connect Izin ini termasuk dalam customer_sagemaker_admin_policy yang dilampirkan pada customer_sagemaker_admin_role . Tindakan ini memberi Anda akses ke akselerator Elastic Inference.
AWS Shield	Tidak ada akses ke salah satu layanan APIs atau konsol ini.
Layanan Alur Kerja Sederhana Amazon	Tidak ada akses ke salah satu layanan APIs atau konsol ini.

Penyediaan infrastruktur dalam mode Pengembang AMS

Pengguna yang tidak memiliki peran IAM mode

PengembangAWSManagedServicesDevelopmentRole, di akun tempat mode

Pengembang diaktifkan, diharuskan mengikuti proses manajemen perubahan AMS Advanced yang memanfaatkan AMS Advanced. AMIs Pengguna dengan peran yang benar (MALZ:AWSManagedServicesDevelopmentRole, SALZ:customer_developer_role) dapat menggunakan sistem manajemen perubahan AMS Advanced dan AMS Advanced AMIs tetapi tidak diharuskan melakukannya.

Note

AWS AMI, yang belum diproses melalui konsumsi beban kerja AMS Advanced, atau dibuat di akun AMS Advanced, tidak akan menyertakan konfigurasi AMS Advanced-required.

Kontrol Detektif dalam mode Pengembang AMS

Bagian ini telah disunting karena berisi informasi sensitif terkait keamanan AMS. Informasi ini tersedia melalui Dokumentasi konsol AMS. Untuk mengakses Artifact AWS, Anda dapat menghubungi CSDM Anda untuk mendapatkan petunjuk atau membuka [Memulai dengan Artifact AWS](#).

Pencatatan, pemantauan, dan manajemen acara dalam mode Pengembang AMS

Pencatatan, pemantauan, dan manajemen peristiwa tidak tersedia untuk sumber daya yang disediakan di luar proses manajemen perubahan AMS Advanced, atau untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang.

Manajemen insiden dalam mode Pengembang AMS

Tidak ada perubahan waktu respons insiden. Resolusi insiden adalah upaya terbaik untuk sumber daya yang disediakan di luar proses manajemen perubahan, atau sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang.

Note

Perjanjian tingkat layanan AMS (SLA) tidak berlaku untuk sumber daya yang dibuat atau diperbarui di luar sistem manajemen perubahan AMS (permintaan untuk perubahan atau

RFCs), termasuk mode Pengembang; oleh karena itu, sumber daya yang diperbarui atau dibuat dalam mode Pengembang secara otomatis terdegradasi ke P3 dan dukungan AMS adalah upaya terbaik.

Manajemen tambalan dalam mode Pengembang AMS

Manajemen tambalan tidak tersedia untuk sumber daya yang disediakan di luar proses manajemen perubahan AMS Advanced, atau untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang. Waktu penambalan:

- Untuk pembaruan keamanan kritis: Dalam waktu 10 hari kerja setelah rilis oleh vendor untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang.
- Untuk pembaruan penting: Dalam waktu 2 bulan setelah rilis oleh vendor untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang.

Manajemen kontinuitas dalam mode Pengembang AMS

Manajemen kontinuitas tidak tersedia untuk sumber daya yang disediakan di luar proses manajemen perubahan AMS Advanced, atau untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang.

Waktu inisiasi pemulihan lingkungan dapat memakan waktu hingga 12 jam untuk sumber daya yang disediakan di luar proses manajemen perubahan AMS Advanced, atau untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang.

Keamanan dan manajemen akses dalam mode Pengembang AMS

Perlindungan anti-malware adalah tanggung jawab Anda atas sumber daya yang disediakan di luar proses manajemen perubahan AMS Advanced, atau untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang. Akses ke instans Amazon Elastic Compute Cloud (Amazon EC2) yang tidak disediakan melalui manajemen perubahan AMS Advanced mungkin dikontrol oleh pasangan kunci alih-alih menyediakan akses gabungan.

Mode Penyediaan Layanan Mandiri di AMS

Mode AWS Managed Services (AMS) Self-Service Provisioning (SSP) menyediakan akses penuh ke AWS layanan native dan kemampuan API di akun terkelola AMS. Anda mengakses layanan melalui peran standar, cakupan bawah,. AWS Identity and Access Management AMS menyediakan permintaan layanan dan manajemen insiden. Peringatan, pemantauan, pencatatan, tambalan, cadangan, dan manajemen perubahan adalah tanggung jawab Anda. Dalam banyak kasus, layanan Penyediaan Layanan Mandiri (SSPS) dikelola sendiri, atau tanpa server, dan tidak memerlukan manajemen tugas operasional tertentu seperti patching. Anda mendapat manfaat dari penggunaan layanan ini dalam batas lingkungan yang ditentukan oleh pagar pembatas AMS dan setiap perubahan IAM (termasuk peran terkait layanan, peran layanan, peran lintas akun, atau pembaruan kebijakan) perlu disetujui oleh Operasi AMS untuk menjaga keamanan dasar platform. Anda dapat memanfaatkan AWS CloudFormation template untuk mengotomatiskan penerapan layanan ini, tetapi ini tidak didukung untuk semua layanan SSP.

Important

Gunakan mode SSP di akun AWS Managed Services (AMS) Anda untuk mengakses dan menggunakan AWS layanan, dengan batasan sebagaimana disebutkan.

Ada beberapa Layanan AWS yang dapat Anda gunakan tanpa manajemen AMS, di akun AMS Anda. Layanan mode Penyediaan Layanan Mandiri, atau singkatnya SSPS, cara menambahkannya ke akun AMS Anda dan FAQs untuk masing-masing, dijelaskan di bagian ini.

Layanan penyediaan layanan mandiri ditawarkan apa adanya, dan Anda bertanggung jawab untuk mengelolanya. AMS tidak memberikan peringatan, pemantauan, pencatatan, atau penambalan untuk sumber daya yang terkait dengan layanan tersebut. AMS menyediakan peran IAM yang memungkinkan Anda menggunakan layanan di akun AMS Anda dengan aman. AMS SLAs tidak berlaku.

Untuk sumber daya yang Anda sediakan melalui layanan mandiri, AMS menyediakan manajemen insiden, kontrol detektif dan pagar pembatas, pelaporan, sumber daya yang ditunjuk (Cloud Service Delivery Manager dan Cloud Architect), keamanan dan akses, serta dukungan teknis melalui permintaan layanan. Selain itu, jika berlaku, Anda bertanggung jawab atas manajemen kontinuitas, manajemen patch, pemantauan infrastruktur, dan manajemen perubahan untuk sumber daya yang disediakan atau dikonfigurasi di luar sistem manajemen perubahan AMS.

Memulai dengan mode SSP di AMS

Penyediaan layanan mandiri adalah salah satu mode AMS untuk multi-account landing zone (MALZ) yang dapat Anda gunakan. Untuk informasi selengkapnya, lihat [Ikhtisar mode](#).

Untuk menyediakan kemampuan penyediaan layanan mandiri, AMS telah menciptakan peran IAM yang ditingkatkan dengan batas izin untuk membatasi perubahan yang tidak diinginkan dari akses langsung. Layanan AWS Peran tidak mencegah semua perubahan dan Anda harus mematuhi kontrol internal dan kebijakan kepatuhan Anda, dan memvalidasi bahwa semua yang Layanan AWS digunakan memenuhi sertifikasi yang diperlukan. Ini adalah mode penyediaan swalayan. Untuk detail tentang persyaratan AWS kepatuhan, lihat [AWS Kepatuhan](#).

Untuk menambahkan layanan penyediaan layanan mandiri ke akun Aplikasi landing zone multi-akun Anda, gunakan Manajemen AWS | layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (CT), baik CT yang diperlukan peninjauan atau CT otomatis, seperti yang diinstruksikan untuk layanan.

Note

Untuk meminta agar AMS menyediakan layanan penyediaan layanan mandiri tambahan, ajukan permintaan layanan.

Gunakan AMS SSP untuk menyediakan Amazon API Gateway di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon API Gateway secara langsung di akun terkelola AMS Anda. [Amazon API Gateway](#) adalah layanan yang dikelola sepenuhnya yang memudahkan pengembang untuk membuat, menerbitkan, memelihara, memantau, dan mengamankan APIs pada skala apa pun. Dengan menggunakan REST, AWS Management Console Anda dapat membuat REST dan WebSocket APIs bertindak sebagai pintu depan bagi aplikasi untuk mengakses data, logika bisnis, atau fungsionalitas dari layanan back-end Anda, seperti beban kerja yang berjalan di Amazon Elastic Compute Cloud ([Amazon EC2](#)), kode yang berjalan, aplikasi web apa pun [AWS Lambda](#), atau aplikasi komunikasi real-time.

API Gateway menangani semua tugas yang terlibat dalam menerima dan memproses hingga ratusan ribu panggilan API bersamaan, termasuk manajemen lalu lintas, otorisasi dan kontrol akses, pemantauan, dan manajemen versi API. API Gateway tidak memiliki biaya minimum atau

biaya startup. Anda hanya membayar untuk panggilan API yang Anda terima dan jumlah data yang ditransfer keluar dan, dengan model harga berjenjang API Gateway, Anda dapat mengurangi biaya saat skala penggunaan API Anda. Untuk mempelajari selengkapnya, lihat [Amazon API Gateway](#).

FAQ: API Gateway di AMS

T: Bagaimana cara meminta akses ke Amazon API Gateway di akun AMS saya?

Minta akses ke API Gateway dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_apigateway_author_role` dan `customer_apigateway_cloudwatch_role`. Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon API Gateway di akun AMS saya?

- Konfigurasi API Gateway terbatas pada sumber daya tanpa AMS - atau MC - awalan untuk mencegah modifikasi apa pun pada infrastruktur AMS.
- CREATE hak istimewa untuk VPCLink dinonaktifkan untuk mencegah pembuatan Elastic Load Balancer yang tidak diatur. Jika VPCLinks diperlukan, lihat [Application Load Balancer | Buat](#).

T: Apa prasyarat atau dependensi untuk menggunakan Amazon API Gateway di akun AMS saya?

Itu tergantung pada jenis API Gateway yang ingin Anda terapkan. Ini bisa menjadi layanan mandiri, tetapi juga dapat meminta akses ke layanan yang ada (misalnya, penyeimbang beban jaringan).

Gunakan AMS SSP untuk menyediakan Alexa for Business di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Alexa for Business secara langsung di akun terkelola AMS Anda. Alexa for Business adalah layanan yang memungkinkan organisasi dan karyawan Anda menggunakan Alexa untuk menyelesaikan lebih banyak pekerjaan. Dengan Alexa for Business, Anda dapat menggunakan Alexa sebagai asisten cerdas Anda untuk menjadi lebih produktif di ruang rapat, di meja Anda, dan bahkan dengan perangkat Alexa yang sudah Anda gunakan di rumah atau saat bepergian. Manajer TI dan fasilitas dapat menggunakan Alexa for Business untuk mengukur dan meningkatkan pemanfaatan ruang pertemuan yang ada di tempat kerja mereka.

Untuk mempelajari lebih lanjut, lihat [Alexa for Business](#).

Alexa for Business di AWS Managed Services FAQ

T: Bagaimana cara meminta akses ke Alexa for Business di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_alex_console_role` A juga `customer_alex_device_setup_user` dibuat untuk Device Setup Tool yang disediakan oleh Alexa for Business; Alat Pengaturan Perangkat ini kemudian dapat digunakan untuk mengatur perangkat Anda. Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

Gateway Alexa for Business memungkinkan Anda menghubungkan Alexa for Business ke titik akhir Cisco Webex dan Poly Group Series untuk mengontrol rapat dengan suara Anda. Perangkat lunak gateway berjalan pada perangkat keras lokal Anda dan dengan aman proksi arahan konferensi dari Alexa for Business ke titik akhir Cisco Anda. Gateway membutuhkan dua pasang AWS kredensial untuk berkomunikasi dengan Alexa for Business. Kami menyediakan dua pengguna IAM akses terbatas: `customer_alex_gateway_installer_user` dan `customer_alex_gateway_execution_user` untuk gateway Alexa for Business Anda, satu untuk menginstal gateway dan satu untuk mengoperasikan gateway; ini dapat diminta dengan mengirimkan RFC dengan Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat entitas atau kebijakan (diperlukan tinjauan) jenis perubahan (ct-3dpg8mdd9dd9jn1r).

Note

Untuk menghasilkan laporan penggunaan dan mengirimkannya ke Amazon S3, tentukan nama bucket Amazon S3 di RFC layanan yang disediakan sendiri.

T: Apa batasan untuk menggunakan Alexa for Business di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Alexa for Business tersedia dengan peran layanan mandiri Alexa for Business.

T: Apa prasyarat atau dependensi untuk menggunakan Alexa for Business di akun AMS saya?

- Jika Anda bermaksud menggunakan WPA2 Enterprise Wi-Fi untuk menyiapkan perangkat bersama, tentukan jenis keamanan jaringan ini di Alat Pengaturan Perangkat, yang AWS Private Certificate Authority diperlukan.

- AMS hanya membuat kunci rahasia yang dimulai dengan namespace “A4B”. Ini hanya terbatas pada namespace ini.

T: Apa fungsi Alexa for Business yang membutuhkan terpisah? RFCs

Untuk mendaftarkan perangkat Alexa Voice Service (AVS) dengan Alexa for Business, berikan akses ke pembuat perangkat bawaan Alexa. Untuk melakukan ini, peran IAM perlu dibuat di konsol Alexa for Business yang dapat digunakan menggunakan Management | Other | Other | Other change type. Hal ini memungkinkan pembuat perangkat AVS untuk mendaftarkan dan mengelola perangkat dengan Alexa for Business atas nama Anda.

Gunakan AMS SSP untuk menyediakan Amazon AppStream 2.0 di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon AppStream 2.0 (AppStream 2.0) secara langsung di akun terkelola AMS Anda. AppStream 2.0 memungkinkan Anda memindahkan aplikasi desktop Anda ke AWS, tanpa menulis ulang. Anda dapat menginstal aplikasi Anda pada AppStream 2.0, mengatur konfigurasi peluncuran, dan membuat aplikasi Anda tersedia untuk pengguna. AppStream 2.0 menawarkan berbagai pilihan opsi mesin virtual sehingga Anda dapat memilih jenis instans yang paling sesuai dengan kebutuhan aplikasi Anda, dan mengatur parameter skala otomatis sehingga Anda dapat dengan mudah memenuhi kebutuhan pengguna akhir Anda. AppStream 2.0 memungkinkan Anda untuk meluncurkan aplikasi di jaringan Anda sendiri, yang berarti aplikasi Anda dapat berinteraksi dengan AWS sumber daya yang ada.

Amazon AppStream 2.0 memungkinkan Anda menginstal, menguji, dan memperbarui aplikasi dengan cepat dan mudah menggunakan pembuat gambar. Aplikasi apa pun yang berjalan di Microsoft Windows Server 2012 R2, Windows Server 2016, atau Windows Server 2019 didukung, dan Anda tidak perlu melakukan modifikasi apa pun. Ketika pengujian selesai, Anda dapat mengatur konfigurasi peluncuran aplikasi, pengaturan pengguna default, dan mempublikasikan gambar Anda untuk diakses pengguna.

Untuk mempelajari lebih lanjut, lihat [AppStream 2.0](#).

AppStream 2.0 di AWS Managed Services FAQ

T: Bagaimana cara meminta akses ke AppStream 2.0 di akun AMS saya?

Minta akses ke AppStream 2.0 dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-3qe6io8t6jtny) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_appstream_console_role`

A juga `customer_appstream_stream_role` digunakan untuk streaming aplikasi yang mengharuskan pengguna untuk diautentikasi menggunakan kredensial login Active Directory mereka.

Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AppStream 2.0 di akun AMS saya?

- Fungsionalitas berikut harus dikonfigurasi oleh tim Dukungan AMS, dan memerlukan spesifik RFCs. Instruksi tentang meminta fungsionalitas tambahan dapat ditemukan di bagian 4.
 - Membuat dan Streaming dari Titik Akhir VPC Antarmuka.
 - Support untuk titik akhir Amazon S3 untuk folder rumah dan persistensi pengaturan aplikasi di jaringan pribadi.
 - Membuat dan memilih peran IAM yang akan tersedia di semua instance streaming armada.
 - Bergabung dengan armada AppStream 2.0 dan pembuat gambar domain Microsoft Active Directory.
 - Membuat Laporan Penggunaan Kustom AppStream 2.0.
 - Custom branding saat ini tidak didukung.

T: Apa prasyarat atau dependensi untuk menggunakan AppStream 2.0 di akun AMS saya?

Saat mengirimkan RFC ke onboard AppStream 2.0, sertakan nama bucket Amazon S3 yang akan digunakan untuk laporan penggunaan 2.0. AppStream Nama bucket ditambahkan ke `customer-appstream-usagereports-policy` yang dibuat saat AppStream 2.0 di-onboard.

T: Fungsionalitas AppStream 2.0 apa yang membutuhkan terpisah RFCs?

- Untuk memilih titik akhir VPC antarmuka untuk AppStream 2.0, kirimkan Manajemen | Lainnya | Lainnya | Perbarui jenis perubahan RFC untuk membuat titik akhir VPC di akun Anda. Untuk langkah-langkah untuk membuat titik akhir khusus untuk AppStream 2.0, lihat [Membuat dan Streaming dari Titik Akhir VPC Antarmuka](#) di AppStream panduan pengguna 2.0.
- Support untuk titik akhir Amazon S3 untuk folder rumah dan persistensi pengaturan aplikasi di jaringan pribadi dapat dikonfigurasi dengan meminta titik akhir VPC Amazon S3 dengan Manajemen | Lainnya | Lainnya | Lainnya | Buat jenis perubahan RFC. RFC harus menyertakan bucket Amazon S3 target yang menghosting konten folder beranda, atau pengaturan aplikasi

bucket Amazon S3, masing-masing. RFC ini akan memberikan AppStream 2.0 izin yang diperlukan untuk mengakses titik akhir VPC Amazon S3. Untuk langkah-langkah untuk membuat titik akhir khusus untuk streaming, lihat [Menggunakan Titik Akhir VPC Amazon S3 untuk Folder Rumah dan Persistensi Pengaturan Aplikasi](#) dalam panduan pengguna 2.0. AppStream

- Untuk membuat dan memilih peran IAM yang akan tersedia di semua instance streaming armada, kirimkan Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat entitas atau kebijakan (review required) change type (ct-3dpd8mdd9jn1r) RFC yang meminta peran IAM dengan kebijakan yang diperlukan. Nama peran IAM harus selalu dimulai dengan awalan: "customer_appstream".
- Armada Amazon AppStream 2.0 dan pembuat gambar dapat digabungkan ke domain di Microsoft Active Directory dengan mengirimkan Manajemen | Lainnya | Lainnya | Perbarui jenis perubahan RFC untuk pembuatan Akun Layanan di Active Directory (AD). Izin minimal yang diperlukan untuk bergabung dengan Microsoft Active Directory didefinisikan dalam dokumentasi AppStream 2.0 di [Pemberian Izin untuk Membuat dan Mengelola Objek Komputer Direktori Aktif](#).
- Untuk membuat Laporan Penggunaan AppStream 2.0 kustom, kirimkan Manajemen | Lainnya | Lainnya | Buat jenis perubahan RFC yang meminta berikut:
 - "AppStreamUsageReports" Pembuatan tumpukan CFN
 - "customer_appstream_usagereports_role" disediakan di akun
 - Juga, berikan detail berikut:
 - Berikan ekspresi CRON untuk menjadwalkan Crawler run. Secara default adalah 23:00 UTC setiap hari.
 - Bucket Amazon S3 ARN akan digunakan untuk hasil kueri Athena. Bucket ini harus memiliki awalan: `aws-athena-query-results`
 - Bucket Amazon S3 ARN untuk Log Laporan Penggunaan AppStream 2.0.

Setelah peran disediakan, masukkan peran ke dalam solusi federasi Anda dan login, lalu akses dan AWS GlueAWS Glue Athena untuk membuat laporan kustom menggunakan peran laporan penggunaan. Untuk detail tentang menggunakan Laporan Penggunaan AppStream 2.0, lihat [Membuat Laporan Kustom dan Menganalisis Data Penggunaan AppStream 2.0](#), dalam dokumentasi AppStream 2.0.

Gunakan AMS SSP untuk menyediakan Amazon Athena di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Athena (Athena) secara langsung di akun terkelola AMS Anda. Athena adalah layanan kueri interaktif

yang membantu Anda menganalisis data di Amazon S3 menggunakan SQL standar. Athena tidak memiliki server, sehingga tidak ada infrastruktur untuk dikelola dan Anda hanya membayar untuk mengkueri yang Anda jalankan. Anda mengarahkan ke data Anda di Amazon S3, menentukan skema, dan mulai melakukan kueri menggunakan SQL standar. Sebagian besar hasil disampaikan dalam hitungan detik. Dengan Athena, tidak perlu pekerjaan kompleks extract-transform-load (ETL) untuk mempersiapkan data Anda untuk analisis. Ini membuatnya mudah bagi siapa pun dengan keterampilan SQL untuk menganalisis kumpulan data skala besar dengan cepat. Untuk mempelajari lebih lanjut, lihat [Amazon Athena](#).

FAQ: Athena di AMS

T: Bagaimana cara meminta akses ke Amazon Athena di akun AMS saya?

Minta akses ke Athena dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_athena_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Athena di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Athena tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Athena di akun AMS saya?

Athena memiliki ketergantungan besar pada AWS Glue layanan, karena menggunakan data catalog/metastore yang dibuat dengan AWS Glue. Oleh karena itu, AWS Glue izin disertakan dalam Athena RFC yang sukses.

Peran tersebut `customer_athena_console_role` memiliki prasyarat untuk ember Amazon S3. Untuk membuat bucket baru, gunakan CT otomatis `ct-1a68ck03fn98r` (Deployment | Advanced stack components | S3 storage | Create). Saat Anda menggunakan CT otomatis ini untuk membuat bucket S3 untuk Athena, nama bucket harus dimulai dengan awalan `athena-query-results-`*

Gunakan AMS SSP untuk menyediakan Amazon Bedrock di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon Bedrock secara langsung di akun dikelola AMS Anda. Amazon Bedrock adalah layanan yang dikelola sepenuhnya yang membuat model foundation berkinerja tinggi (FMs) dari startup AI terkemuka dan AWS tersedia untuk Anda gunakan melalui API terpadu. Anda dapat memilih dari

berbagai model pondasi untuk menemukan model yang paling cocok untuk kasus penggunaan Anda. Amazon Bedrock juga menawarkan serangkaian kemampuan yang luas untuk membangun aplikasi AI generatif dengan keamanan, privasi, dan AI yang bertanggung jawab. Menggunakan Amazon Bedrock, Anda dapat dengan mudah bereksperimen dengan dan mengevaluasi model dasar teratas untuk kasus penggunaan Anda, menyesuaikannya secara pribadi dengan data Anda menggunakan teknik seperti fine-tuning dan Retrieval Augmented Generation (RAG), dan membangun agen yang menjalankan tugas menggunakan sistem perusahaan dan sumber data Anda.

Dengan pengalaman tanpa server Amazon Bedrock, Anda dapat memulai dengan cepat, menyesuaikan model foundation secara pribadi dengan data Anda sendiri, serta mengintegrasikan serta menerapkannya dengan mudah dan aman ke dalam aplikasi Anda menggunakan alat AWS tanpa harus mengelola infrastruktur apa pun. Untuk informasi lebih lanjut, lihat [Amazon Bedrock](#).

FAQ: Batuan Dasar Amazon di AMS

T: Bagaimana cara meminta akses ke Amazon Bedrock di akun AMS saya?

Untuk meminta akses ke Amazon Bedrock, kirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) ubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_bedrock_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Bedrock di akun AMS saya?

- Basis pengetahuan Amazon Bedrock tidak didukung secara default sebagai bagian dari peran SSPS karena ketergantungannya pada OpenSearch Amazon Service Serverless yang saat ini tidak didukung di AMS.
- Bedrock Studio tidak didukung karena ketergantungannya pada layanan yang tidak didukung seperti Amazon. DataZone

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Bedrock di akun AMS saya?

- Langganan model pihak ketiga yang memerlukan AWS Marketplace izin harus dilakukan oleh peran default (`AWSManagedServicesAdminRole` di MALZ dan `Customer_ReadOnly_Role` di SALZ). Ini karena peran default menyertakan AWS Marketplace izin.
- Jika enkripsi data digunakan, maka Anda harus memberikan ARN AWS KMS kunci saat Anda meminta pembuatan peran konsol. Selain itu, ember Amazon S3 yang digunakan harus memiliki “batuan dasar” dalam namanya.

Gunakan AMS SSP untuk menyediakan Amazon CloudSearch di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses CloudSearch kapabilitas Amazon secara langsung di akun terkelola AMS Anda. Amazon CloudSearch adalah layanan terkelola di AWS Cloud yang Anda gunakan agar hemat biaya untuk menyiapkan, mengelola, dan menskalakan solusi pencarian untuk situs web atau aplikasi Anda. Amazon CloudSearch mendukung 34 bahasa dan fitur pencarian populer seperti penyorotan, pelengkapan otomatis, dan pencarian geospasial. Untuk mempelajari lebih lanjut, lihat [Amazon CloudSearch](#).

Note

AWS telah menutup akses pelanggan baru ke Amazon CloudSearch, efektif 25 Juli 2024. Pelanggan Amazon CloudSearch yang sudah ada dapat terus menggunakan layanan seperti biasa. AWS terus berinvestasi dalam peningkatan keamanan, ketersediaan, dan kinerja untuk Amazon CloudSearch, tetapi kami tidak berencana untuk memperkenalkan fitur baru. Untuk memahami perbedaan antara Amazon CloudSearch dan Amazon OpenSearch Service, dan bagaimana Anda dapat beralih ke OpenSearch Layanan, hubungi arsitek cloud (CA) Anda untuk mendapatkan panduan. Untuk informasi selengkapnya tentang transisi ke OpenSearch Layanan, lihat [Transisi dari layanan Amazon ke CloudSearch Amazon OpenSearch Service](#).

FAQ Amazon CloudSearch di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon CloudSearch di akun AMS saya?

Minta akses ke Amazon CloudSearch dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_csearch_admin_role` dan `customer_csearch_dev_role`. Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon CloudSearch di akun AMS saya?

Fungsionalitas penuh Amazon CloudSearch tersedia di akun AMS Anda. Semua solusi database yang didukung AMS saat ini didukung di Amazon. CloudSearch Perhatikan bahwa, saat ini, DynamoDB adalah satu-satunya solusi database AWS terkelola yang tidak dapat diindeks.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon CloudSearch di akun AMS saya?

Amazon CloudSearch bergantung pada Amazon S3 yang bekerja dengan Penyedia Identitas untuk menganalisis data input secara otomatis dan menentukan bidang tabel. Akses ke Amazon S3 tidak disediakan dengan RFC ini, dan harus diminta secara terpisah dalam permintaan layanan.

Menggunakan AMS SSP untuk menyediakan Amazon CloudWatch Synthetics di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon CloudWatch Synthetics secara langsung di akun terkelola AMS Anda. Anda dapat menggunakan Amazon CloudWatch Synthetics untuk membuat 'kenari' untuk memantau titik akhir Anda dan API

Canary adalah skrip yang dapat dikonfigurasi, ditulis dalam Node.js atau Python, yang berjalan sesuai jadwal. Mereka membuat fungsi Lambda di akun Anda yang menggunakan Node.js atau Python sebagai kerangka kerja. Canary bekerja di atas protokol HTTP maupun HTTPS. Canary memeriksa ketersediaan dan latensi titik akhir Anda dan dapat menyimpan data waktu buka dan tangkapan layar UI. Mereka memantau REST Anda APIs, URLs, dan konten situs web, dan mereka dapat memeriksa perubahan yang tidak sah dari phishing, injeksi kode, dan skrip lintas situs.

Canary mengikuti rute yang sama dan melakukan tindakan yang sama sebagai pelanggan, sehingga memungkinkan Anda untuk terus memverifikasi pengalaman pelanggan Anda bahkan ketika Anda tidak memiliki lalu lintas pelanggan pada aplikasi Anda. Dengan menggunakan canary, Anda dapat menemukan masalah sebelum para pelanggan Anda menemukannya. Untuk mempelajari lebih lanjut, lihat [Amazon CloudWatch: Menggunakan pemantauan sintetis](#).

FAQ Amazon CloudWatch Synthetics di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon CloudWatch Synthetics di akun AMS saya?

Minta akses ke Amazon CloudWatch Synthetics dengan mengirimkan RFC dengan Management | AWS service | Self-provisioned service | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: 'customer_cw_synthetics_console_role' dan 'customer_cw_synthetics_canary_lambda_role'. Setelah disediakan di akun Anda, Anda harus mengaktifkan peran 'customer_cw_synthetics_console_role' dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon CloudWatch Synthetics di akun AMS saya?

Tidak ada batasan untuk penggunaan Amazon CloudWatch Synthetics di akun AMS Anda. Membuat peran untuk kenari di luar peran layanan yang disediakan AMS 'customer_cw_synthetics_canary_lambda_role' dilarang.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon CloudWatch Synthetics di akun AMS saya?

Canary membuat dan menggunakan bucket Amazon CloudWatch Synthetics S3 default: cw-syn-results "- -" *`${accountnumber} ${default-region}`*

Gunakan AMS SSP untuk menyediakan kumpulan pengguna Amazon Cognito di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas kumpulan pengguna Amazon Cognito secara langsung di akun terkelola AMS Anda. Kumpulan pengguna Amazon Cognito menyediakan direktori pengguna aman yang menskalakan hingga ratusan juta pengguna. Sebagai layanan yang dikelola sepenuhnya, kumpulan pengguna Amazon Cognito dapat diatur tanpa khawatir tentang infrastruktur server yang berdiri. Layanan ini memungkinkan Anda mengelola kumpulan pengguna akhir yang dapat Anda gunakan untuk berintegrasi dengan aplikasi internal Anda. Layanan ini memberi Anda alternatif untuk database yang disesuaikan atau direktori pengguna akhir untuk aplikasi web atau seluler. Pada saat yang sama, kumpulan pengguna Amazon Cognito menyediakan serangkaian fungsi lengkap dari layanan direktori seperti kebijakan kata sandi, otentikasi multi faktor, pemulihan kata sandi, dan pendaftaran sendiri ke layanan. Ini juga memungkinkan aplikasi untuk menggabungkan akses di layanan publik populer lainnya seperti OpenID, Facebook, Amazon atau Google.

Amazon Cognito dibagi menjadi dua produk utama. Kumpulan pengguna Amazon Cognito dan Penyedia Identitas Amazon Cognito. Bagian ini berfokus pada kumpulan pengguna Amazon Cognito, yang menyediakan akses ke AWS layanan lain seperti Amazon S3 atau DynamoDB. Layanan ini memungkinkan Anda menggunakan kumpulan pengguna Amazon Cognito, atau penyedia identitas pihak ketiga, untuk menyediakan akses ke AWS layanan. Ini juga menyediakan akses ke AWS layanan menggunakan akses tamu anonim. Karena sifat kuat dari kumpulan pengguna Amazon Cognito, itu akan dikelola secara manual case-by-case berdasarkan layanan manual operasi, untuk menghindari potensi kerusakan keamanan ke akun. Untuk mempelajari lebih lanjut, lihat [Kumpulan Pengguna Amazon Cognito](#).

Kumpulan pengguna Amazon Cognito di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke kumpulan pengguna Amazon Cognito di akun AMS saya?

Implementasi kumpulan pengguna Amazon Cognito di AMS adalah proses 2 langkah:

1. Kirim Manajemen | Lainnya | Lainnya | Buat (ct-1e1xtak34nx76) ubah jenis dan minta pembuatan kumpulan pengguna Amazon Cognito di Akun AMS Anda. Sertakan informasi berikut:
 - AWS Wilayah.
 - Nama untuk Kumpulan Pengguna Cognito.
 - Jika Anda ingin menggunakan Amazon Simple Email Service (Amazon SES) untuk mengirim pesan dan notifikasi alih-alih layanan email Cognito internal default, maka pelanggan harus memberikan alamat email yang sudah divalidasi untuk Layanan Amazon SES di akun. Alamat ini akan digunakan untuk bidang “Dari” dan “BALAS-KE” dari pesan. Mereka juga harus menunjukkan Wilayah tempat Amazon SES diaktifkan (us-east-1, eu-west-1 atau us-west-2).
 - Jika Anda ingin menggunakan pesan SMS untuk kata sandi dan verifikasi satu kali, maka pelanggan harus menunjukkannya.
2. Minta akses pengguna dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_cognito_admin_role` dan `customer_cognito_importjob_role`. Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda. Peran ini memungkinkan Anda mengelola kumpulan pengguna Amazon Cognito, mengelola pengguna dan grup di kolam, membuat pekerjaan impor untuk pengguna, memodifikasi pesan notifikasi dan langganan, mengaitkan aplikasi ke kumpulan pengguna, mengelola sendiri menambahkan layanan federasi ke kolam, dan menghapus kumpulan yang sudah dibuat.

T: Apa batasan untuk menggunakan kumpulan pengguna Amazon Cognito di akun AMS saya?

Anda tidak akan dapat membuat kumpulan pengguna Amazon Cognito. Tindakan itu memerlukan pembuatan peran IAM untuk memanfaatkan layanan yang digunakan oleh Amazon Cognito, seperti Amazon SES dan Amazon Simple Notification Service (Amazon SNS).

T: Apa prasyarat atau dependensi untuk menggunakan kumpulan pengguna Amazon Cognito di akun AMS saya?

Jika Anda ingin menggunakan Amazon SES untuk mengirim pesan dan pemberitahuan melalui email ke kumpulan pengguna Anda, mereka seharusnya sudah mengaktifkan layanan Amazon SES di akun, dan sudah memvalidasi alamat email yang harus digunakan di bidang “DARI” dan

“BALAS-KE” dari email yang dikirim. Untuk informasi selengkapnya tentang memvalidasi alamat email menggunakan Amazon SES, lihat [Memverifikasi Alamat Email di Amazon SES](#).

Gunakan AMS SSP untuk menyediakan Amazon Comprehend di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Comprehend secara langsung di akun terkelola AMS Anda. Amazon Comprehend adalah layanan pemrosesan bahasa alami (NLP) yang menggunakan pembelajaran mesin untuk menemukan wawasan dan hubungan dalam teks, tidak diperlukan pengalaman pembelajaran mesin. Amazon Comprehend menggunakan pembelajaran mesin untuk membantu Anda menemukan wawasan dan hubungan dalam data tidak terstruktur Anda. Layanan mengidentifikasi bahasa teks; mengekstrak frasa kunci, tempat, orang, merek, atau peristiwa; memahami seberapa positif atau negatif teks itu; menganalisis teks menggunakan tokenisasi dan bagian pidato; dan secara otomatis mengatur kumpulan file teks berdasarkan topik. Anda juga dapat menggunakan kemampuan AutoML di Amazon Comprehend untuk membuat kumpulan entitas kustom atau model klasifikasi teks yang disesuaikan secara unik dengan kebutuhan organisasi Anda. Untuk mempelajari lebih lanjut, lihat [Amazon Comprehend](#).

FAQ Amazon Comprehend di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon Comprehend di akun AMS saya?

Konsol Amazon Comprehend dan peran akses data dapat diminta melalui pengajuan dua Layanan AMS: RFCs

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_comprehend_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Comprehend di akun AMS saya?

Buat fungsionalitas Peran IAM Baru melalui konsol Amazon Comprehend dibatasi. Jika tidak, fungsionalitas penuh Amazon Comprehend tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Comprehend di akun AMS saya?

Amazon S3 dan AWS Key Management Service (AWS KMS) diperlukan untuk menggunakan Amazon Comprehend, jika bucket Amazon S3 dienkripsi dengan kunci. AWS KMS

Menggunakan AMS SSP untuk menyediakan Amazon Connect di akun AMS

Note

Setelah mempertimbangkan dengan cermat, kami memutuskan untuk mengakhiri dukungan untuk Amazon Connect Voice ID, efektif 20 Mei 2026. Amazon Connect Voice ID tidak akan lagi menerima pelanggan baru mulai 20 Mei 2025. Sebagai pelanggan lama dengan akun yang mendaftar untuk layanan sebelum 20 Mei 2025, Anda dapat terus menggunakan fitur ID Suara Amazon Connect. Setelah 20 Mei 2026, Anda tidak akan lagi dapat menggunakan Amazon Connect Voice ID.

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Connect secara langsung di akun terkelola AMS Anda. Amazon Connect adalah pusat kontak cloud omnichannel yang membantu perusahaan menyediakan layanan pelanggan yang unggul dengan biaya lebih rendah. Amazon Connect memberikan pengalaman yang mulus di seluruh suara dan obrolan untuk pelanggan dan agen. Ini termasuk satu set alat untuk perutean berbasis keterampilan, analitik real-time dan historis yang kuat, dan alat manajemen easy-to-use intuitif — semuanya dengan harga. pay-as-you-go

Anda dapat membuat satu atau beberapa instance instance pusat kontak virtual di akun landing zone multi-akun AMS atau akun landing zone akun tunggal. Anda dapat menggunakan penyedia identitas SAMP 2.0 yang ada untuk akses agen atau menggunakan dukungan asli Amazon Connect untuk manajemen siklus hidup pengguna.

Selain itu, Anda dapat mengklaim nomor telepon free/direct panggilan tol untuk setiap instans Amazon Connect dari konsol Amazon Connect. Anda dapat membuat alur kontak yang kaya untuk mencapai pengalaman dan perutean pelanggan yang diinginkan menggunakan antarmuka pengguna easy-to-use grafis. Alur kontak dapat memanfaatkan AWS Lambda fungsi untuk diintegrasikan dengan penyimpanan data lokal dan API. Anda juga dapat mengaktifkan streaming data menggunakan Kinesis Streams dan Firehose.

Rekaman panggilan, transkrip obrolan, dan laporan, disimpan dalam bucket Amazon S3 yang dienkripsi menggunakan kunci. AWS KMS Log alur kontak dapat disimpan ke grup CloudWatch log.

Untuk mempelajari lebih lanjut, lihat [Amazon Connect](#).

FAQ Amazon Connect di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon Connect di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_connect_console_role` dan `customer_connect_user_role`. Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Connect di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Connect tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Connect di akun AMS saya?

- Anda harus membuat AWS KMS Key dan bucket Amazon S3 menggunakan AMS standar RFCs; bucket Amazon S3 diperlukan untuk menyimpan rekaman panggilan dan transkrip obrolan.
- Jika Anda ingin mengintegrasikan dengan Active Directory (AD), AD Connector diperlukan untuk integrasi antara instans Amazon Connect yang dihosting AMS dan layanan direktori lokal Anda. AD Connector dapat dikonfigurasi di akun Anda dengan meminta RFC 'Manajemen | Lainnya | Lainnya'.
- Anda dapat mengaktifkan layanan mandiri opsional berikut berdasarkan persyaratan alur kontak Anda.
 - AWS Lambda: Anda dapat menggunakan fungsi Lambda untuk memperluas alur kontak guna memanfaatkan penyimpanan data lokal yang ada atau. APIs Anda dapat menggunakan layanan Lambda yang disediakan sendiri untuk membuat fungsi Lambda.
 - Amazon Kinesis Data Streams: Anda dapat membuat aliran data untuk mengaktifkan streaming Data ke aplikasi eksternal. Anda dapat melakukan streaming catatan jejak kontak atau Acara Agen.
 - Amazon Kinesis Data Firehose: Anda dapat membuat Data Firehose untuk mengalirkan catatan jejak kontak volume tinggi ke aplikasi eksternal.
 - Amazon Lex: Anda dapat memanfaatkan Amazon Lex Chatbots untuk menciptakan arus kontak cerdas yang memanfaatkan layanan Amazon Alexa untuk pengalaman dan otomatisasi pelanggan yang kaya.
- T: Bagaimana cara saya meminta untuk menambahkan daftar negara untuk panggilan keluar atau masuk?

Untuk menambahkan daftar negara untuk panggilan keluar atau masuk, kirimkan permintaan layanan ke AMS.

Menggunakan AMS SSP untuk menyediakan Amazon Data Firehose di akun AMS

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Data Firehose secara langsung di akun terkelola AMS Anda. Firehose adalah cara termudah untuk memuat data streaming secara andal ke dalam data lake, penyimpanan data, dan alat analitik. Ini dapat menangkap, mengubah, dan memuat data streaming ke Amazon S3, Amazon Redshift, OpenSearch Amazon Service, dan Splunk², memungkinkan analitik hampir real-time dengan alat intelijen bisnis dan dasbor yang sudah Anda gunakan saat ini. Ini adalah layanan yang dikelola sepenuhnya yang secara otomatis menskalakan agar sesuai dengan throughput data Anda dan tidak memerlukan administrasi berkelanjutan. Ini juga dapat mengumpulkan, mengompres, mengubah, dan mengenkripsi data sebelum memuatnya, meminimalkan jumlah penyimpanan yang digunakan di tempat tujuan dan meningkatkan keamanan. Untuk mempelajari lebih lanjut, lihat [Apa itu Amazon Data Firehose?](#)

FAQ Firehose di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Data Firehose di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_kinesis_firehose_user_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan Firehose di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Data Firehose tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Firehose di akun AMS saya?

Peran IAM terkait layanan baru harus diminta untuk setiap aliran pengiriman. Anda juga dapat menggunakan kembali satu peran terkait layanan untuk semua aliran dengan memperbarui kebijakan

peran dengan izin sumber daya yang diperlukan (termasuk ember S3/Kunci KMS/Fungsi Lambda/aliran Kinesis).

Setelah Anda mengirimkan RFC untuk menambahkan Firehose, insinyur Operasi AMS akan menghubungi Anda melalui Permintaan Layanan untuk sumber daya yang ingin Anda sambungkan dengan Firehose Data (misalnya AWS KMS, Aliran S3, Lambda, dan Kinesis). ARNs

Gunakan AMS SSP untuk menyediakan Amazon DevOps Guru di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon DevOps Guru secara langsung di akun terkelola AMS Anda. Amazon DevOps Guru adalah layanan operasi yang dikelola sepenuhnya yang memudahkan pengembang dan operator untuk meningkatkan kinerja dan ketersediaan aplikasi mereka. DevOpsGuru memungkinkan Anda membongkar tugas administratif yang terkait dengan mengidentifikasi masalah operasional sehingga Anda dapat dengan cepat menerapkan rekomendasi untuk meningkatkan aplikasi Anda. DevOpsGuru menciptakan wawasan reaktif yang dapat Anda gunakan untuk meningkatkan aplikasi Anda sekarang. Ini juga menciptakan wawasan proaktif untuk membantu Anda menghindari masalah operasional yang mungkin memengaruhi aplikasi Anda di masa mendatang. DevOpsGuru menerapkan pembelajaran mesin untuk menganalisis data operasional dan metrik aplikasi serta peristiwa Anda untuk mengidentifikasi perilaku yang menyimpang dari pola operasi normal. Anda akan diberitahu ketika DevOps Guru mendeteksi masalah operasional atau risiko. Untuk setiap masalah, DevOps Guru menyajikan rekomendasi cerdas untuk mengatasi masalah operasional masa depan saat ini dan yang diprediksi.

Untuk mempelajari lebih lanjut, lihat [Apa itu Amazon DevOps Guru](#).

FAQ Amazon DevOps Guru di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon DevOps Guru di akun AMS saya?

Untuk meminta akses, kirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_devopsguru_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon DevOps Guru di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon DevOps Guru tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan DevOps Amazon Guru di akun AMS saya?

Tidak ada prasyarat. DevOpsGuru memanfaatkan AWS layanan berikut: Amazon CloudWatch Logs, RDS Insights, AWS X-Ray, AWS Lambda dan. AWS CloudTrail

Gunakan AMS SSP untuk menyediakan Amazon DocumentDB (dengan kompatibilitas MongoDB) di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon DocumentDB (dengan kompatibilitas MongoDB) secara langsung di akun terkelola AMS Anda. Amazon DocumentDB (dengan kompatibilitas MongoDB) adalah layanan database dokumen yang cepat, terukur, sangat tersedia, dan dikelola sepenuhnya yang mendukung beban kerja MongoDB. Amazon DocumentDB memberi Anda kinerja, skalabilitas, dan ketersediaan yang Anda butuhkan saat mengoperasikan beban kerja MongoDB yang penting dalam skala besar. Amazon DocumentDB mengimplementasikan Apache 2.0 open source MongoDB 3.6 API dengan meniru tanggapan yang diharapkan klien MongoDB dari server MongoDB, memungkinkan Anda untuk menggunakan driver dan alat MongoDB yang ada dengan Amazon DocumentDB. Di Amazon DocumentDB, penyimpanan dan komputasi dipisahkan, memungkinkan masing-masing untuk menskalakan secara independen, dan Anda dapat meningkatkan kapasitas baca hingga jutaan permintaan per detik dengan menambahkan hingga 15 replika baca latensi rendah, terlepas dari ukuran data Anda. Amazon DocumentDB dirancang untuk ketersediaan 99,99% dan mereplikasi enam salinan data Anda di tiga Availability Zone (). AWS AZs Anda dapat menggunakan AWS Database Migration Service (DMS) secara gratis (selama enam bulan) untuk memigrasikan database EC2 MongoDB Amazon Elastic Compute Cloud (Amazon) lokal atau Amazon Elastic Compute Cloud (Amazon) ke Amazon DocumentDB tanpa waktu henti. Untuk mempelajari lebih lanjut, lihat [Amazon DocumentDB \(dengan kompatibilitas MongoDB\)](#).

FAQ Amazon DocumentDB di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon DocumentDB di akun AMS saya?

Konsol Amazon DocumentDB dan peran akses data dapat diminta melalui pengajuan dua RFCs AMS, akses konsol, dan akses data:

Minta akses ke Amazon DocumentDB dengan mengirimkan RFC dengan Manajemen AWS | layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_documentdb_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon DocumentDB di akun AMS saya?

Amazon DocumentDB memerlukan izin khusus Amazon RDS. Karena AMS sepenuhnya mengelola Amazon RDS, peran IAM untuk Amazon DocumentDB mencakup beberapa batasan tindakan di Amazon RDS. Pembatasan berikut berlaku:

- Akses ke `DeleteDBInstance` dan `DeleteDBCluster` APIs telah dibatasi. Untuk menggunakan penghapusan tersebut APIs, kirimkan RFC dengan Manajemen | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Perbarui entitas atau kebijakan (diperlukan tinjauan) jenis perubahan (ct-27tuth19k52b4).
- Anda tidak dapat menambah atau menghapus tag dari instans Amazon RDS.
- Anda tidak dapat membuat instans Amazon DocumentDB Anda menjadi publik.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon DocumentDB di akun AMS saya?

Amazon S3 dan AWS KMS diperlukan untuk menggunakan Amazon DocumentDB, jika bucket Amazon S3 dienkripsi dengan kunci. AWS KMS

Gunakan AMS SSP untuk menyediakan Amazon DynamoDB di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon DynamoDB (DynamoDB) secara langsung di akun terkelola AMS Anda. Amazon DynamoDB adalah nilai kunci dan database dokumen yang memberikan kinerja milidetik satu digit pada skala apa pun. Ini adalah database multi-wilayah, multi-aktif yang dikelola sepenuhnya dengan keamanan bawaan, pencadangan dan pemulihan, dan caching dalam memori untuk aplikasi skala internet. Untuk mempelajari selengkapnya, lihat [Amazon DynamoDB](#).

Amazon DynamoDB Accelerator (DAX) adalah layanan caching write-through yang dirancang untuk memudahkan proses menambahkan cache ke tabel DynamoDB. DAX ditujukan untuk aplikasi yang memerlukan pembacaan performa tinggi.

FAQ DynamoDB di AWS Managed Services

T: Bagaimana cara meminta akses ke DynamoDB dan DAX di akun AMS saya?

Minta akses ke DynamoDB dan DAX dengan mengirimkan RFC dengan Manajemen AWS | layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran dan kebijakan IAM berikut ke akun Anda:

- Nama peran DynamoDB: `customer_dynamodb_role`

Nama peran layanan DAX: `customer_dax_service_role`

- Nama kebijakan DynamoDB: `customer_dynamodb_policy`

Kebijakan layanan DAX: `customer_dax_service_policy`

Setelah disediakan di akun Anda, Anda harus memasukkan solusi `customer_dynamodb_role` dalam federasi Anda.

T: Apa batasan untuk menggunakan DynamoDB di akun AMS saya?

Semua fungsi DynamoDB didukung termasuk DynamoDB Accelerator (DAX).

Saat membuat alarm untuk tabel tertentu, nama alarm harus diawali dengan “pelanggan*”; misalnya, `customer-employee-table-high-put-latency`

Saat membuat topik Amazon SNS untuk DynamoDB, itu harus diberi nama: `dynamodb`

Untuk menghapus topik Amazon SNS yang dibuat oleh DynamoDB, kirimkan Manajemen | Lainnya | Lainnya | Perbarui jenis perubahan RFC.

T: Apa prasyarat atau dependensi untuk menggunakan DynamoDB di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan DynamoDB di akun AMS Anda.

Gunakan AMS SSP untuk menyediakan Amazon Elastic Container Registry di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Elastic Container Registry (Amazon ECR) Registry ECR) secara langsung di akun terkelola AMS Anda. Amazon Elastic Container Registry adalah registri kontainer [Docker](#) yang dikelola sepenuhnya yang memudahkan pengembang untuk menyimpan, mengelola, dan menyebarkan gambar kontainer Docker. Amazon ECR terintegrasi dengan [Amazon Elastic Container Service \(Amazon ECS\)](#), [menyederhanakan pengembangan](#) Anda ke alur kerja produksi. Amazon ECR menghilangkan kebutuhan untuk mengoperasikan repositori kontainer Anda sendiri atau khawatir tentang penskalaan infrastruktur yang mendasarinya. Amazon ECS meng-host gambar Anda dalam arsitektur yang sangat tersedia dan dapat diskalakan, memungkinkan Anda untuk menyebarkan kontainer secara andal untuk aplikasi Anda. Integrasi dengan AWS Identity and Access Management (IAM) menyediakan kontrol tingkat sumber daya dari setiap repositori. Dengan Amazon ECR, tidak

ada biaya atau komitmen di muka. Anda hanya membayar untuk jumlah data yang Anda simpan di repositori dan data yang ditransfer ke Internet.

Untuk mempelajari lebih lanjut, lihat [Amazon Elastic Container Registry](#).

FAQ Amazon Elastic Container Registry di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon ECR di akun AMS saya?

Minta akses ke Amazon ECR dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_ecr_console_role`, dan `customer_ecr_poweruser_instance_profile` dengan kebijakan IAM terkait, `customer_ecr_console_policy` dan `customer_ecr_poweruser_instance_profile_policy`, masing-masing. Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon ECR di akun AMS saya?

Ada batasan seputar ruang nama AMS untuk penggunaan Amazon ECR di akun AMS Anda. Gambar kontainer mungkin tidak diawali dengan “AMS-” atau “Sentinel-”.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon ECR di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Amazon ECR di akun AMS Anda.

Menggunakan AMS SSP untuk menyediakan EC2 Image Builder di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Image Builder EC2 secara langsung di akun terkelola AMS Anda. EC2 Image Builder adalah AWS layanan yang dikelola sepenuhnya yang membuatnya lebih mudah untuk mengotomatiskan pembuatan, pengelolaan, dan penyebaran gambar server yang disesuaikan, aman, dan up-to-date “emas” yang sudah diinstal sebelumnya dan dikonfigurasi sebelumnya dengan perangkat lunak dan pengaturan untuk memenuhi standar TI tertentu.

Anda dapat menggunakan AWS Management Console, AWS CLI, atau APIs untuk membuat gambar khusus di akun Anda AWS . Saat Anda menggunakan AWS Management Console, wizard Amazon EC2 Image Builder memandu Anda melalui langkah-langkah untuk:

- Berikan artefak awal

- Tambah dan hapus perangkat lunak
- Sesuaikan pengaturan dan skrip
- Jalankan tes yang dipilih
- Mendistribusikan gambar ke AWS Wilayah

Gambar yang Anda buat dibuat di akun Anda dan dapat dikonfigurasi untuk tambalan sistem operasi secara berkelanjutan. Untuk mempelajari lebih lanjut, lihat [EC2 Image Builder](#).

EC2 FAQ Image Builder di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke EC2 Image Builder di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. Melalui RFC ini, peran IAM berikut akan disediakan di akun Anda: `customer_ec2_imagebuilder_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk EC2 Image Builder?

AMS tidak mendukung penggunaan Default Layanan untuk konfigurasi infrastruktur. Anda dapat membuat konfigurasi infrastruktur baru atau menggunakan yang sudah ada.

AMS saat ini tidak mendukung pembuatan resep wadah.

T: Apa prasyarat atau dependensi untuk mengaktifkan Image Builder? EC2

- EC2 Peran terkait layanan Image Builder: Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat resource Image Builder pertama di AWS Management Console, AWS CLI, atau AWS API, Image Builder membuat peran terkait layanan untuk Anda.
- Instans yang digunakan untuk membuat gambar dan menjalankan pengujian menggunakan Image Builder harus memiliki akses ke layanan Systems Manager. Agen SSM akan diinstal pada gambar sumber jika belum ada, dan akan dihapus sebelum gambar dibuat.
- AWS IAM: Peran IAM yang Anda kaitkan dengan profil instans harus memiliki izin untuk menjalankan komponen build dan test yang disertakan dalam image Anda. Kebijakan peran IAM berikut harus dilampirkan ke peran IAM yang terkait dengan profil instans: `EC2InstanceProfileForImageBuilder` dan `AmazonSSMManagedInstanceCore` Nama peran IAM harus berisi `*imagebuilder*` kata kunci.

- Jika Anda mengonfigurasi logging, profil instance yang ditentukan dalam konfigurasi infrastruktur Anda harus memiliki `s3:PutObject` izin untuk bucket target (`arn:aws:s3:::{bucket-name}/*`). Misalnya:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::{bucket-name}/*"
    }
  ]
}
```

- Buat topik SNS dengan nama 'imagebuilder' untuk menerima peringatan dan pemberitahuan dari Image Builder. EC2

Gunakan AMS SSP untuk menyediakan Amazon ECS AWS Fargate di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses Amazon ECS pada AWS Fargate kemampuan langsung di akun terkelola AMS Anda. AWS Fargate adalah teknologi yang dapat Anda gunakan dengan Amazon ECS untuk menjalankan kontainer (lihat [Kontainer AWS](#) aktif) tanpa harus mengelola server atau cluster instans Amazon EC2 . Dengan AWS Fargate, Anda tidak lagi harus menyediakan, mengonfigurasi, atau menskalakan, kelompok mesin virtual untuk menjalankan kontainer. Anda tidak perlu memilih jenis server, memutuskan kapan akan menskalakan kluster Anda, atau mengoptimalkan paket kluster.

Untuk mempelajari lebih lanjut, lihat [Amazon ECS di AWS Fargate](#).

FAQ Amazon ECS di Fargate di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon ECS di Fargate di akun AMS saya?

Minta akses ke Amazon ECS di Fargate dengan mengirimkan RFC dengan Manajemen AWS | layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_ecs_fargate_console_role` (jika tidak ada peran IAM yang ada disediakan untuk mengaitkan kebijakan ECS),,,`customer_ecs_fargate_events_service_role`, `customer_ecs_task_execution_service_role` dan. `customer_ecs_codedeploy_service_role` `AWSServiceRoleForApplicationAutoScaling_ECSService` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon ECS di Fargate di akun AMS saya?

- Pemantauan dan pencatatan tugas Amazon ECS dianggap sebagai tanggung jawab Anda karena aktivitas tingkat kontainer terjadi di atas hypervisor, dan kemampuan logging dibatasi oleh Amazon ECS di Fargate. Sebagai pengguna Amazon ECS di Fargate, kami menyarankan Anda mengambil langkah-langkah yang diperlukan untuk mengaktifkan login pada tugas Amazon ECS Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan Driver Log awslogs untuk](#) Kontainer Anda.
- Keamanan dan perlindungan malware di tingkat kontainer juga dianggap sebagai tanggung jawab Anda. Amazon ECS di Fargate tidak menyertakan Trend Micro atau komponen keamanan jaringan yang telah dikonfigurasi sebelumnya.
- Layanan ini tersedia untuk akun landing zone multi-akun dan single-account landing zone AMS.
- Amazon ECS [Service Discovery](#) dibatasi secara default dalam peran yang disediakan sendiri karena izin yang ditingkatkan diperlukan untuk membuat zona host pribadi Route 53. Untuk mengaktifkan Service Discovery pada layanan, kirimkan Manajemen | Lainnya | Lainnya | Perbarui jenis perubahan. Untuk memberikan informasi yang diperlukan untuk mengaktifkan Penemuan Layanan untuk Layanan Amazon ECS Anda, lihat [manual Penemuan Layanan](#).
- AMS saat ini tidak mengelola atau membatasi gambar yang digunakan untuk menyebarkan ke kontainer ke Amazon ECS Fargate. Anda akan dapat menyebarkan gambar dari Amazon ECR, Docker Hub, atau repositori gambar pribadi lainnya. Oleh karena itu, kami menyarankan agar gambar publik atau gambar yang tidak aman tidak digunakan, karena dapat mengakibatkan aktivitas berbahaya di akun.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon ECS di Fargate di akun AMS saya?

- Berikut ini adalah dependensi Amazon ECS di Fargate; namun, tidak ada tindakan tambahan yang diperlukan untuk mengaktifkan layanan ini dengan peran yang Anda sediakan sendiri:

- CloudWatch log
 - CloudWatch acara
 - CloudWatch alarm
 - CodeDeploy
 - App Mesh
 - Cloud Map
 - Route 53
- Bergantung pada kasus penggunaan Anda, berikut ini adalah sumber daya yang diandalkan Amazon ECS, dan mungkin diperlukan sebelum menggunakan Amazon ECS di Fargate di akun Anda:
 - Grup keamanan untuk digunakan dengan layanan Amazon ECS. Anda dapat menggunakan Deployment | Advanced stack components | Security Group | Create (auto) (ct-3pc215bnwb6p7), atau, jika grup keamanan Anda memerlukan aturan khusus, gunakan Deployment | Advanced stack components | Security Group | Create (review required) (ct-1oxx2g2d7hc90). Catatan: Grup keamanan yang Anda pilih dengan Amazon ECS harus dibuat khusus untuk Amazon ECS tempat layanan atau kluster Amazon ECS berada. Anda dapat mempelajari lebih lanjut di bagian Grup Keamanan di [Menyiapkan dengan Amazon ECS](#) dan [Keamanan di Amazon Elastic Container Service](#).
 - Aplikasi load balancer (ALB), network load balancer (NLB), classic load balancer (ELB) untuk load balancing antar tugas.
 - Grup Sasaran untuk ALBs.
 - Sumber daya mesh aplikasi (misalnya, Router Virtual, Layanan Virtual, Node Virtual) untuk diintegrasikan dengan Amazon ECS Cluster Anda.
 - Saat ini, tidak ada cara bagi AMS untuk secara otomatis mengurangi risiko yang terkait dengan izin grup keamanan pendukung saat dibuat di luar jenis perubahan AMS standar. Kami menyarankan Anda meminta grup keamanan tertentu untuk digunakan dengan kluster Fargate Anda untuk membatasi kemungkinan menggunakan grup keamanan yang tidak ditunjuk untuk digunakan dengan Amazon ECS.

Gunakan AMS SSP untuk menyediakan Amazon EKS AWS Fargate di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses Amazon EKS pada AWS Fargate kemampuan langsung di akun terkelola AMS Anda. AWS Fargate adalah teknologi yang menyediakan kapasitas komputasi sesuai permintaan dan berukuran tepat untuk kontainer (untuk memahami kontainer, lihat [Apa itu Kontainer?](#)). Dengan AWS Fargate, Anda tidak perlu lagi menyediakan, mengonfigurasi, atau menskalakan grup mesin virtual untuk menjalankan kontainer. Dengan begitu, Anda tidak perlu memilih jenis server, memutuskan kapan untuk skala simpul grup Anda, atau mengoptimalkan kluster packing.

Amazon Elastic Kubernetes Service (Amazon EKS) mengintegrasikan AWS Fargate Kubernetes dengan menggunakan kontroler yang AWS dibangun menggunakan model upstream yang dapat diperluas yang disediakan oleh Kubernetes. Pengontrol ini berjalan sebagai bagian dari bidang kontrol Kubernetes yang dikelola Amazon EKS dan bertanggung jawab untuk menjadwalkan pod Kubernetes asli ke Fargate. Pengendali Fargate termasuk penjadwal baru yang berjalan dengan penjadwal Kubernetes default selain beberapa pengendali masuk urusan mutasi dan validasi. Ketika Anda memulai pod yang memenuhi kriteria untuk berjalan di Fargate, pengendali Fargate yang berjalan di kluster akan mengenali, memperbarui, dan menjadwalkan pod ke Fargate.

Untuk mempelajari lebih lanjut, lihat [Amazon EKS di AWS Fargate Sekarang Tersedia Secara Umum](#) dan [Panduan Praktik Terbaik Amazon EKS untuk Keamanan](#) (termasuk “Rekomendasi” seperti “Tinjau dan cabut akses anonim yang tidak perlu” dan banyak lagi).

Tip

AMS memiliki tipe perubahan, Deployment | Komponen tumpukan lanjutan | Manajemen Identitas dan Akses (IAM) | Buat penyedia OpenID Connect (ct-30ecvfi3tq4k3), yang dapat Anda gunakan dengan Amazon EKS. Sebagai contoh, lihat [Identity and Access Management \(IAM\) | Membuat Penyedia OpenID Connect](#).

FAQ Amazon EKS AWS Fargate aktif di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon EKS di Fargate di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda.

- `customer_eks_fargate_console_role`.

Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

- Peran layanan ini memberi Amazon EKS di Fargate izin untuk memanggil AWS layanan lain atas nama Anda:
 - `customer_eks_pod_execution_role`
 - `customer_eks_cluster_service_role`

T: Apa batasan untuk menggunakan Amazon EKS di Fargate di akun AMS saya?

- Membuat EC2 nodegroup yang [dikelola](#) atau [dikelola sendiri](#) tidak didukung di AMS. Jika Anda memiliki persyaratan untuk menggunakan node EC2 pekerja, hubungi AMS Cloud Service Delivery Manager (CSDM) atau Cloud Architect (CA).
- AMS tidak menyertakan Trend Micro atau komponen keamanan jaringan yang telah dikonfigurasi sebelumnya untuk gambar kontainer. Anda diharapkan untuk mengelola layanan pemindaian gambar Anda sendiri untuk mendeteksi gambar kontainer berbahaya sebelum penerapan.
- EKSCluster tidak didukung karena saling ketergantungan. CloudFormation
- Selama pembuatan kluster, Anda memiliki izin untuk menonaktifkan pencatatan bidang kontrol cluster. Untuk informasi selengkapnya, lihat [Amazon EKS mengontrol pencatatan pesawat](#). Kami menyarankan agar Anda mengaktifkan semua pencatatan API, Otentikasi, dan Audit penting pada pembuatan kluster.
- Selama pembuatan kluster, akses titik akhir kluster untuk kluster Amazon EKS secara default menjadi publik; untuk informasi selengkapnya, lihat kontrol akses titik akhir kluster [Amazon EKS](#). Kami menyarankan agar titik akhir Amazon EKS disetel ke pribadi. Jika titik akhir diperlukan untuk akses publik, maka itu adalah praktik terbaik untuk mengaturnya ke publik hanya untuk rentang CIDR tertentu.
- AMS tidak memiliki metode untuk memaksa dan membatasi gambar yang digunakan untuk menyebarkan ke wadah di Amazon EKS Fargate. Anda dapat menerapkan gambar dari Amazon ECR, Docker Hub, atau repositori gambar pribadi lainnya. Oleh karena itu, ada risiko menyebarkan citra publik yang mungkin melakukan aktivitas berbahaya di akun.
- Menerapkan kluster EKS melalui cloud development kit (CDK) atau CloudFormation Ingest tidak didukung di AMS.
- Anda harus membuat grup keamanan yang diperlukan menggunakan [ct-3pc215bnwb6p7 Deployment | Komponen tumpukan lanjutan | Grup keamanan](#) | Buat dan referensi dalam file

manifes untuk pembuatan ingress. Ini karena peran tersebut `customer-eks-alb-ingress-controller-role` tidak diizinkan untuk membuat grup keamanan.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon EKS di Fargate di akun AMS saya?

Untuk menggunakan layanan ini, dependensi berikut harus dikonfigurasi:

- [Untuk autentikasi terhadap layanan, baik KUBECTL maupun aws-iam-authenticator harus diinstal; untuk informasi selengkapnya, lihat Mengelola otentikasi klaster.](#)
- Kubernetes mengandalkan konsep yang disebut “akun layanan.” Untuk memanfaatkan fungsionalitas akun layanan di dalam klaster kubernetes di EKS, Manajemen | Lainnya | Lainnya | Pembaruan RFC diperlukan dengan masukan berikut:
 - [Diperlukan] Nama Cluster Amazon EKS
 - [Diperlukan] Namespace Amazon EKS Cluster tempat akun layanan (SA) akan digunakan.
 - [Diperlukan] Nama Amazon EKS Cluster SA.
 - [Wajib] Nama Kebijakan IAM dan permissions/document untuk dikaitkan.
 - [Diperlukan] Nama Peran IAM diminta.
 - [Opsional] URL penyedia OpenID Connect. Untuk informasi selengkapnya, lihat
 - [Mengaktifkan peran IAM untuk akun layanan di klaster Anda](#)
 - [Memperkenalkan peran IAM berbutir halus untuk akun layanan](#)
- Kami menyarankan agar aturan Config dikonfigurasi dan dipantau
 - Titik akhir klaster publik
 - Pencatatan API yang dinonaktifkan

Anda bertanggung jawab untuk memantau dan memulihkan aturan Config ini.

Jika Anda ingin menerapkan [pengontrol ALB Ingress](#), kirimkan Management | Other | Other Update RFC untuk menyediakan peran IAM yang diperlukan untuk digunakan dengan pod ALB Ingress Controller. Input berikut diperlukan untuk membuat sumber daya IAM untuk dikaitkan dengan ALB Ingress Controller (sertakan ini dengan RFC Anda):

- [Diperlukan] Nama Cluster Amazon EKS
- [Opsional] URL penyedia OpenID Connect

- [Opsional] Namespace Amazon EKS Cluster tempat layanan pengontrol masuk penyeimbang beban aplikasi (ALB) akan diterapkan. [default: kube-sistem]
- [Opsional] Nama akun layanan Amazon EKS Cluster (SA). [default: aws-load-balancer-controller]

Jika Anda ingin mengaktifkan enkripsi rahasia amplop di cluster Anda (yang kami sarankan), berikan kunci KMS yang ingin IDs Anda gunakan, di bidang deskripsi RFC untuk menambahkan layanan (Manajemen | layanan | Layanan yang disediakan sendiri | Tambahkan (AWS ct-1w8z66n899dct). Untuk mempelajari lebih lanjut tentang enkripsi amplop, lihat [Amazon EKS menambahkan enkripsi amplop untuk rahasia dengan AWS KMS](#).

Gunakan AMS SSP untuk menyediakan Amazon EMR di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon EMR secara langsung di akun terkelola AMS Anda. Amazon EMR adalah platform cloud big data terkemuka di industri untuk memproses sejumlah besar data menggunakan alat open source seperti Apache Spark, Apache Hive, Apache, Apache Flink, Apache Hudi, dan Presto HBase. Dengan Amazon EMR, Anda dapat menjalankan analisis skala Petabyte dengan biaya kurang dari setengah biaya solusi lokal tradisional dan lebih dari 3x lebih cepat daripada Apache Spark standar. Untuk pekerjaan jangka pendek, Anda dapat memutar dan memutar cluster dan membayar per detik untuk instance yang digunakan. Untuk beban kerja yang berjalan lama, Anda dapat membuat klaster yang sangat tersedia yang secara otomatis menskalakan untuk memenuhi permintaan.

Anda dapat membuat satu atau beberapa instance klaster EMR Amazon di akun landing zone multi-akun AMS atau akun landing zone akun tunggal untuk mendukung klaster EMR Amazon sementara dan persisten. Anda juga dapat mengaktifkan otentikasi Kerberos untuk mengaktifkan autentikasi pengguna dari domain Active Directory lokal.

Anda dapat memanfaatkan beberapa penyimpanan data dengan kluster EMR Amazon untuk mendukung alat dan pustaka Hadoop khusus kasus penggunaan. Cluster EMR Amazon dapat dibuat menggunakan instans OnDemand atau Spot dan mengonfigurasi penskalaan otomatis untuk mengelola kapasitas dan mengurangi biaya.

File log cluster dapat diarsipkan ke bucket Amazon S3 untuk logging dan debugging. Anda juga dapat mengakses antarmuka web yang dihosting di klaster EMR Amazon untuk mendukung persyaratan administrasi hadoop atau pengalaman buku catatan bagi pelanggan.

Untuk mempelajari lebih lanjut, lihat [Amazon EMR](#).

FAQ Amazon EMR di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon EMR di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:

- `customer_emr_cluster_instance_profile`
- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

Setelah disediakan di akun Anda, Anda harus memasukkan `customer_emr_console_role` di solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon EMR di akun AMS saya?

Saat membuat Amazon EMR di EC2 cluster dari konsol AWS, kami menyarankan Anda untuk menggunakan opsi Create Cluster — Advanced. Cluster EMR Amazon harus dibuat dengan menambahkan tag dengan Kunci "for-use-with-amazon-emr-managed-policies" dengan Nilai "benar". Pilih konfigurasi berikut di opsi Keamanan:

- Pilih peran khusus untuk klaster Anda:
 - Peran EMR: `customer_emr_cluster_service_role`
 - EC2 Profil Contoh: `customer_emr_cluster_instance_profile`
 - Peran Auto Scaling: `customer_emr_cluster_autoscaling_role`
- EC2 Grup keamanan:
 - Master: `ams-emr-master-security -grup`
 - Inti & Tugas: `ams-emr-worker-security -grup`
 - Akses Layanan: `ams-emr-serviceaccess-security -group`

T: Apa prasyarat atau dependensi untuk menggunakan Amazon EMR di akun AMS saya?

AMS membuat grup keamanan default untuk master, pekerja, dan node layanan EMR Amazon.

Template peluncuran dan grup keamanan yang akan digunakan dengan cluster EMR Amazon harus memiliki kunci tag "for-use-with-amazon-emr-managed-policies" dengan nilai "true".

Profil instans cluster Amazon EMR default memungkinkan akses ke sumber daya seperti bucket s3 dan tabel dynamodb dengan namanya yang berisi "emr". Anda dapat meminta kebijakan IAM tambahan untuk menggunakan sumber daya tambahan apa pun yang akan digunakan dengan Amazon EMR. Sumber daya ARN berikut dapat digunakan dengan pekerjaan EMR Amazon menggunakan `customer_emr_cluster_instance_profile`:

- `arn:aws:dynamodb: *:*:tabel/*emr*`
- `arn:aws:kinesis: *:*:stream/*emr*`
- `arn:aws:sns: *:*: *emr*arn:aws:sqs: *:*: *emr*`
- `arn:aws:sqs: *:*: *emr*`
- `arn:aws:sqs: *:*:AWS- -* ElasticMapReduce`
- `arn:aws:sdb: *:*:domain: *emr*`
- `arn:aws:s3: ::*emr*`

Jika otentikasi kerberos diperlukan untuk cluster EMR Amazon:

- Berikan nama ranah yang akan digunakan untuk setiap kluster EMR Amazon kerberisasi dan alamat IP Direktori Aktif di lokasi.
- Persyaratan infrastruktur:

Multi-Account Landing Zone (MALZ): Kirim RFC untuk membuat akun aplikasi Terkelola baru atau VPC baru di akun aplikasi yang ada.

Single-Account Landing Zone (SALZ): Kirim RFC untuk membuat subnet baru di VPC Anda.

- Konfigurasi kepercayaan yang masuk untuk ranah kluster di Active Directory di lokasi.
- Kirim RFC untuk mengonfigurasi zona DNS untuk ranah di AD Terkelola.
- Konfigurasi Realm:

MALZ: Kirim Manajemen | Lainnya | Lainnya | Perbarui (ct-0xdawir96cy7k) RFC untuk memperbarui opsi VPC DHCP yang disetel untuk menggunakan nama ranah untuk akhiran nama domain.

SALZ: Kirim Manajemen | Lainnya | Lainnya | Perbarui (ct-0xdawir96cy7k) RFC untuk menghasilkan AMI EMR Amazon baru untuk menggunakan ranah khusus untuk akhiran nama domain.

Untuk menyebarkan Amazon EMR studio, `customer_emr_cluster_service_role` peran tersebut memiliki prasyarat untuk bucket Amazon Simple Storage Service. Untuk membuat bucket, gunakan CT otomatis `ct-1a68ck03fn98r` (Deployment | Advanced stack components | S3 storage | Create). Saat Anda menggunakan CT otomatis ini untuk membuat bucket Amazon S3 untuk Amazon EMR, nama bucket harus dimulai dengan awalan. `customer-emr-*` Dan, Anda harus membuat bucket di AWS Wilayah yang sama dengan cluster EMR Amazon.

Gunakan AMS SSP untuk menyediakan Amazon EventBridge di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses EventBridge kapabilitas Amazon secara langsung di akun terkelola AMS Anda. Amazon EventBridge adalah layanan bus acara tanpa server yang memudahkan untuk menghubungkan aplikasi Anda dengan data dari berbagai sumber. EventBridge memberikan aliran data real-time dari aplikasi Anda sendiri, aplikasi Software-as-a-Service (SaaS), AWS dan layanan dan rute data tersebut ke target seperti. AWS Lambda Anda dapat mengatur aturan perutean untuk menentukan ke mana harus mengirim data Anda untuk membangun arsitektur aplikasi yang bereaksi secara real time ke semua sumber data Anda. EventBridge memungkinkan Anda membangun arsitektur berbasis peristiwa, yang digabungkan dan didistribusikan secara longgar.

Untuk mempelajari lebih lanjut, lihat [Amazon EventBridge](#).

EventBridge di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke EventBridge akun AMS saya?

Meminta akses EventBridge dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_eventbridge_role` dan `customer_eventbridge_scheduler_execution_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

Peran eksekusi, `customer_eventbridge_scheduler_execution_role` adalah peran IAM yang diasumsikan oleh EventBridge Scheduler untuk berinteraksi dengan orang lain Layanan AWS

atas nama Anda. Kebijakan izin yang dilampirkan pada peran ini memberikan akses EventBridge Scheduler untuk memanggil target.

 Note

Secara default, EventBridge Scheduler menggunakan kunci yang AWS dimiliki EventBridge untuk mengenkripsi data. Untuk menggunakan kunci yang dikelola pelanggan EventBridge untuk mengenkripsi data, kirimkan RFC menggunakan Layanan Manajemen | AWS | Layanan yang disediakan sendiri | [Tambahkan \(perlu ditinjau\) jenis perubahan \(ct-3qe6io8t6jtny\)](#) untuk penyediaan layanan.

T: Apa batasan penggunaan EventBridge di akun AMS saya?

Anda harus mengirimkan AMS RFCs dan membuat sumber daya berikut: Peran layanan untuk memicu pekerjaan batch, antrian SQS, CodeBuild CodePipeline, dan perintah SSM.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? EventBridge

Anda harus meminta peran EventBridge layanan dengan RFC menggunakan Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat entitas atau kebijakan (perlu ditinjau) mengubah jenis (ct-3dpd8mdd9jn1r) sebelum menggunakan untuk memicu EventBridge sumber daya lain, seperti, Lambda, Amazon SNS, Amazon SQS, atau Amazon Sumber daya AWS log. AWS Batch CloudWatch Tentukan layanan yang akan dipanggil saat meminta peran layanan Anda. Untuk mempelajari tentang izin yang diperlukan untuk memanggil target, lihat [Menggunakan Kebijakan Berbasis Sumber Daya](#) untuk. EventBridge

EventBridge terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS dalam EventBridge. CloudTrail harus diaktifkan dan diizinkan untuk menyimpan file log ke ember S3. Catatan: Semua akun AMS telah CloudTrail diaktifkan, jadi tidak diperlukan tindakan.

T: Peran `customer_eventbridge_scheduler_execution_role` memiliki prasyarat untuk Key (opsional, jika digunakan untuk enkripsi). AWS Key Management Service Bagaimana cara mengadopsi AWS KMS CMKs enkripsi data saat istirahat/transit?

Secara default, EventBridge Scheduler mengenkripsi metadata peristiwa dan data pesan yang disimpan di bawah kunci yang AWS dimiliki (enkripsi saat istirahat). EventBridge Scheduler juga

mengkripsi data yang melewati antara EventBridge Scheduler dan layanan lainnya menggunakan Transport Layer Security (TLS) (enkripsi dalam perjalanan).

Jika kasus penggunaan khusus Anda mengharuskan Anda mengontrol dan mengaudit kunci enkripsi yang melindungi data Anda di EventBridge Scheduler, Anda dapat menggunakan kunci yang dikelola pelanggan.

Anda harus meminta RFC menggunakan Management | Layanan AWS | Self-provisioned service | Tambahkan (perlu ditinjau) jenis perubahan sebelum menggunakan Amazon EventBridge untuk memasukkan izin. AWS KMS

Gunakan AMS SSP untuk menyediakan Amazon Forecast di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Forecast (Forecast) secara langsung di akun terkelola AMS Anda. Amazon Forecast adalah layanan yang dikelola sepenuhnya yang menggunakan pembelajaran mesin untuk memberikan perkiraan yang sangat akurat.

Note

AWS telah menutup akses pelanggan baru ke Amazon Forecast, efektif 29 Juli 2024. Amazon Forecast pelanggan lama dapat terus menggunakan layanan seperti biasa. AWS terus berinvestasi dalam peningkatan keamanan, ketersediaan, dan kinerja untuk Amazon Forecast, tetapi AWS tidak berencana untuk memperkenalkan fitur baru. Jika Anda ingin menggunakan Amazon Forecast, hubungi CSDM Anda sehingga mereka dapat memandu Anda lebih lanjut mengenai cara [Transisi penggunaan Amazon Forecast Anda ke Amazon Canvas](#). SageMaker

Berdasarkan teknologi yang sama yang digunakan di Amazon.com, Forecast menggunakan pembelajaran mesin untuk menggabungkan data deret waktu dengan variabel tambahan untuk membangun prakiraan. Forecast tidak memerlukan pengalaman pembelajaran mesin untuk memulai. Anda hanya perlu memberikan data historis, ditambah data tambahan apa pun yang Anda yakini dapat memengaruhi perkiraan Anda. Misalnya, permintaan untuk warna kemeja tertentu dapat berubah dengan musim dan lokasi toko. Hubungan yang kompleks ini sulit ditentukan sendiri, tetapi pembelajaran mesin sangat cocok untuk mengenalinya. Setelah Anda memberikan data

Anda, Forecast akan secara otomatis memeriksanya, mengidentifikasi apa yang bermakna, dan menghasilkan model peramalan yang mampu membuat prediksi yang hingga 50% lebih akurat daripada melihat data deret waktu saja.

Untuk mempelajari lebih lanjut, lihat [Amazon Forecast](#).

FAQ Amazon Forecast di AWS Managed Services

T: Bagaimana cara meminta akses ke Forecast di akun AMS saya?

Minta akses ke AWS Firewall Manager dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_forecast_admin_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan Forecast di akun AMS saya?

Akses bucket S3 default hanya memungkinkan Anda mengakses bucket dengan pola penamaan 'customer-forecast-*'. Jika Anda memiliki konvensi penamaan sendiri untuk bucket data, diskusikan penamaan bucket dan penyiapan akses terkait dengan Cloud Architect (CA) Anda. Misalnya:

- Anda dapat menentukan peran layanan Amazon Forecast spesifik Anda dengan penamaan seperti 'AmazonForecast- ExecutionRole -*' dan terkait akses bucket S3 yang tepat. Lihat peran Layanan - AmazonForecast-ExecutionRole-Admin dan kebijakan IAM - `customer_forecast_default_s3_access_policy`, di konsol IAM.
- Anda mungkin perlu mengaitkan akses bucket S3 terkait ke peran federasi IAM. Lihat kebijakan IAM - `customer_forecast_default_s3_access_policy`, di konsol IAM.

T: Apa prasyarat atau dependensi untuk menggunakan Forecast di akun AMS saya?

- Bucket Amazon S3 yang tepat harus dibuat sebelum menggunakan Forecast. Terutama, akses bucket S3 default adalah dengan pola penamaan 'customer-forecast-*'
- Jika Anda ingin menggunakan pola penamaan pada bucket S3 selain 'customer-forecast-*', Anda harus membuat peran layanan baru dengan izin akses S3 di bucket:
 1. Peran layanan baru yang akan dibuat dengan penamaan 'AmazonForecast- ExecutionRole - {suffix}'.
 2. Kebijakan IAM baru yang akan dibuat yang mirip dengan `customer_forecast_default_s3_access_policy` dan dikaitkan dengan peran layanan baru dan peran admin federasi terkait (misalnya 'customer_forecast_admin_role')

T: Bagaimana cara meningkatkan keamanan data saat menggunakan Amazon Forecast?

- Untuk enkripsi data saat istirahat, Anda dapat menggunakan AWS KMS untuk menyediakan CMK yang dikelola pelanggan untuk melindungi penyimpanan data di layanan Amazon S3:
 - Aktifkan enkripsi default pada bucket dengan kunci penyediaan dan siapkan kebijakan bucket untuk menerima enkripsi AWS KMS data sambil meletakkan data.
 - Aktifkan peran layanan Amazon Forecast 'AmazonForecast- ExecutionRole -*' dan peran admin federasi (misalnya 'customer_forecast_admin_role ') sebagai pengguna kunci. AWS KMS
- Untuk enkripsi data dalam perjalanan, Anda dapat mengatur protokol HTTPS, yang diperlukan saat mentransfer objek pada kebijakan bucket Amazon S3.
- Pembatasan lebih lanjut pada kontrol akses, aktifkan kebijakan bucket untuk akses yang disetujui untuk peran layanan Amazon Forecast 'AmazonForecast- ExecutionRole -*' dan peran admin (misalnya 'customer_forecast_admin_role ').

T: Apa praktik terbaik saat menggunakan Amazon Forecast?

- Anda harus memiliki pemahaman yang baik tentang praktik klasifikasi data Anda dan memetakan kebutuhan keamanan data terkait saat menggunakan bucket S3 dengan Amazon Forecast.
- Untuk konfigurasi bucket Amazon S3, kami sangat menyarankan Anda untuk mengaktifkan penegakan HTTPS dalam kebijakan bucket S3 Anda.
- Anda harus mengetahui peran admin 'customer_forecast_admin_role' mendukung akses permissif (Get/Delete/Putobjek S3) di bucket Amazon S3 dengan penamaan 'customer-forecast-*'.

CATATAN: Jika Anda memerlukan kontrol akses berbutir halus untuk beberapa tim, ikuti praktik berikut:

- Tentukan identitas IAM akses berbasis tim Anda (peran/pengguna) dengan akses hak istimewa paling sedikit ke bucket Amazon S3 terkait.
- Buat AWS KMS CMKs hibah team/project berbasis akses yang tepat ke identitas IAM yang sesuai. (akses pengguna dan 'AmazonForecast- ExecutionRole - {team/project}').
- Siapkan enkripsi default bucket S3 dengan yang dibuat AWS KMS CMKs.
- Terapkan lalu lintas API S3 dengan protokol HTTPS pada kebijakan bucket S3.
- Menerapkan konfigurasi bucket S3 untuk akses yang disetujui untuk identitas IAM terkait (akses pengguna dan 'AmazonForecast- ExecutionRole - {team/project}' ke bucket.
- Jika Anda ingin menggunakan 'customer_forecast_admin_role' untuk tujuan umum, pertimbangkan poin yang tercantum sebelumnya untuk melindungi bucket S3.

T: Di mana informasi kepatuhan tentang Amazon Forecast?

Lihat [AWS layanan Program Kepatuhan](#).

Gunakan AMS SSP untuk menyediakan Amazon FSx di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses FSx kapabilitas Amazon secara langsung di akun terkelola AMS Anda. Amazon FSx menyediakan sistem file pihak ketiga yang dikelola sepenuhnya. Amazon FSx memberi Anda kompatibilitas asli sistem file pihak ketiga dengan set fitur untuk beban kerja seperti penyimpanan berbasis Windows, komputasi kinerja tinggi (HPC), pembelajaran mesin, dan otomatisasi desain elektronik (EDA). Amazon FSx mengotomatiskan tugas administrasi yang memakan waktu seperti penyediaan perangkat keras, konfigurasi perangkat lunak, penambalan, dan pencadangan. Amazon FSx mengintegrasikan sistem file dengan AWS layanan cloud-native, membuatnya lebih berguna untuk serangkaian beban kerja yang lebih luas.

Amazon FSx memberi Anda dua sistem file untuk dipilih: Amazon untuk Windows File Server FSx untuk aplikasi berbasis Windows dan Amazon untuk Lustre FSx untuk beban kerja intensif komputasi. Untuk mempelajari lebih lanjut, lihat [Amazon FSx](#).

FAQ Amazon FSx di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon FSx di akun AMS saya?

Meminta akses ke Amazon FSx dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_fsx_admin_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon FSx di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh dari layanan ini tersedia.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon FSx di akun AMS saya?

Tidak ada prasyarat. Namun, untuk konfigurasi lanjutan seperti Multi-AZ, Anda harus menginstal dan mengelola layanan Replikasi DFS dan DFS Namespaces. Untuk informasi selengkapnya, lihat [Menerapkan Sistem File Multi-AZ](#).

T: Bagaimana cara mengintegrasikan sistem FSx file Amazon saya dengan iklan terkelola landing zone multi-akun saya?

Saat membuat sistem FSx file Amazon, Anda dapat menentukan MALZ Managed AD sebagai 'Direktori Aktif Microsoft AWS Terkelola' untuk Otentikasi Windows. Untuk informasi selengkapnya lihat, [Menggunakan Amazon FSx dengan AWS Directory Service Microsoft Active Directory](#)

Anda juga harus membagikan iklan Terkelola ke akun aplikasi terlebih dahulu. Lakukan ini dengan mengirimkan RFC dengan Management | Directory Service | Directory | Share directory change type (ct-369odosk0pd9w).

T: Pengguna mana yang termasuk dalam grup AWS Delegated FSx Administrators?

Hanya administrator server file TI. Grup ini memiliki hak akses penuh di semua berbagi file.

T: Haruskah saya menggunakan file share default, share, yang dibuat saat FSx sistem disediakan?

Tidak, kami tidak menyarankan menggunakan berbagi file default, bagikan, seperti yang disediakan. Ini memberikan Akses Penuh ke Semua Orang, yang melanggar prinsip hak istimewa paling sedikit. Sebagai gantinya, buat berbagi file khusus yang lebih kecil yang sesuai dengan kebutuhan bisnis Anda.

T: Bagaimana cara membuat pembagian file khusus untuk organisasi tertentu dalam bisnis saya?

Lihat [Berbagi File](#) untuk petunjuk cara membuat berbagi file kustom. Batasi akses pada setiap berbagi file menggunakan prinsip hak istimewa paling sedikit.

Gunakan AMS SSP untuk menyediakan Amazon FSx untuk OpenZFS di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses Amazon FSx untuk kemampuan OpenZFS secara langsung di akun terkelola AMS Anda. FSx untuk OpenZFS adalah layanan penyimpanan file yang dikelola sepenuhnya yang memudahkan pemindahan data yang berada di ZFS lokal atau server file berbasis Linux lainnya ke AWS tanpa mengubah kode aplikasi atau cara Anda mengelola data. Ini menawarkan penyimpanan file yang sangat andal, terukur, berkinerja, dan kaya fitur yang dibangun di atas sistem file OpenZFS open-source, menyediakan fitur dan kemampuan sistem file OpenZFS yang sudah dikenal dengan kelincahan, skalabilitas, dan kesederhanaan layanan yang dikelola sepenuhnya. AWS Untuk pengembang yang membangun aplikasi cloud-native, ia menawarkan penyimpanan sederhana dan berkinerja tinggi dengan kemampuan yang kaya untuk bekerja dengan data.

FSx untuk sistem file OpenZFS dapat diakses secara luas dari Linux, Windows, dan instance komputasi macOS dan kontainer menggunakan protokol NFS standar industri (v3, v4.0, v4.1, v4.2).

Didukung oleh prosesor AWS Graviton dan teknologi AWS disk dan jaringan terbaru (termasuk jaringan Datagram AWS Scalable Reliable dan sistem AWS Nitro), FSx untuk OpenZFS memberikan hingga 1 juta IOPS dengan latensi ratusan mikrodetik. Dengan dukungan lengkap untuk fitur OpenZFS seperti point-in-time snapshot instan dan kloning data, FSx untuk OpenZFS memudahkan Anda mengganti server file lokal Anda dengan AWS penyimpanan yang menyediakan kemampuan sistem file yang sudah dikenal dan menghilangkan kebutuhan untuk melakukan kualifikasi panjang dan mengubah atau merancang ulang aplikasi atau alat yang ada. Dan, dengan menggabungkan kekuatan kemampuan manajemen data OpenZFS dengan kinerja tinggi dan efisiensi biaya dari teknologi AWS terbaru, FSx untuk OpenZFS memungkinkan Anda membangun dan menjalankan aplikasi intensif data berkinerja tinggi.

Sebagai layanan yang dikelola sepenuhnya, FSx untuk OpenZFS memudahkan peluncuran, menjalankan, dan menskalakan sistem file yang dikelola sepenuhnya AWS yang menggantikan server file yang Anda jalankan di tempat sambil membantu memberikan kelincahan yang lebih baik dan biaya yang lebih rendah. Dengan FSx untuk OpenZFS, Anda tidak perlu lagi khawatir tentang pengaturan dan penyediaan server file dan volume penyimpanan, mereplikasi data, menginstal dan menambal perangkat lunak server file, mendeteksi dan mengatasi kegagalan perangkat keras, dan melakukan backup secara manual. Ini juga menyediakan integrasi yang kaya dengan AWS layanan lain, seperti AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS), Amazon CloudWatch, dan AWS CloudTrail.

Amazon FSx memberi Anda dua sistem file untuk dipilih: Amazon untuk Windows File Server FSx untuk aplikasi berbasis Windows dan Amazon untuk Lustre FSx untuk beban kerja intensif komputasi. Untuk mempelajari lebih lanjut, lihat [Amazon FSx](#).

FAQ Amazon FSx untuk OpenZFS di AWS Managed Services

T: Bagaimana cara meminta akses untuk digunakan FSx untuk OpenZFS di akun AMS saya?

Minta akses ke Amazon FSx OpenZFS dengan mengirimkan RFC dengan Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_fsx_ontap_admin_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan FSx OpenZFS di akun AMS saya?

Mengganti grup keamanan pada antarmuka jaringan FSx elastis Amazon (ENIs) mengharuskan Anda mengirimkan Manajemen | Lainnya | Lainnya | Pembaruan RFCs karena grup keamanan merupakan perimeter penting untuk lingkungan AMS. Itu satu-satunya batasan.

T: Apa prasyarat atau dependensi yang digunakan untuk OpenZFS di akun AMS saya FSx ?

Tidak ada prasyarat. Namun, Anda harus [Gunakan AMS SSP untuk menyediakan Amazon FSx di akun AMS Anda](#) menginstal.

Gunakan AMS SSP untuk menyediakan Amazon FSx untuk NetApp ONTAP di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses Amazon FSx untuk kemampuan NetApp ONTAP secara langsung di akun terkelola AMS Anda. Amazon FSx untuk NetApp ONTAP adalah layanan yang dikelola sepenuhnya yang menyediakan penyimpanan file yang sangat andal, terukur, berkinerja, dan kaya fitur yang dibangun di atas NetApp sistem file ONTAP yang populer. Ini menyediakan fitur, kinerja, kemampuan, dan sistem NetApp file APIs yang sudah dikenal dengan kelincahan, skalabilitas, dan kesederhanaan yang dikelola sepenuhnya. Layanan AWS

Amazon FSx untuk NetApp ONTAP menyediakan penyimpanan file bersama yang kaya fitur, cepat, dan fleksibel yang dapat diakses secara luas dari instans komputasi Linux, Windows, dan macOS yang berjalan di dalam atau di tempat. AWS FSx untuk ONTAP menawarkan penyimpanan SSD berkinerja tinggi dengan latensi sub-milidetik, dan membuatnya cepat dan mudah untuk mengelola data Anda dengan memungkinkan Anda memotret, mengkloning, dan mereplikasi file Anda dengan mengklik tombol. Ini juga secara otomatis meningkatkan data Anda ke penyimpanan elastis berbiaya lebih rendah, menghilangkan kebutuhan untuk menyediakan atau mengelola kapasitas dan memungkinkan Anda mencapai tingkat kinerja SSD untuk beban kerja Anda sambil hanya membayar penyimpanan SSD untuk sebagian kecil data Anda. Ini menyediakan penyimpanan yang sangat tersedia dan tahan lama dengan cadangan yang dikelola sepenuhnya dan dukungan untuk pemulihan bencana lintas wilayah, dan mendukung keamanan data populer dan aplikasi anti-virus yang membuatnya lebih mudah untuk melindungi dan mengamankan data Anda. Bagi pelanggan yang menggunakan NetApp ONTAP lokal, FSx ONTAP adalah solusi ideal untuk memigrasi, mencadangkan, atau mem-burst aplikasi berbasis file Anda dari lokal ke lokasi AWS tanpa perlu mengubah kode aplikasi atau cara Anda mengelola data.

Sebagai layanan yang dikelola sepenuhnya, Amazon FSx untuk NetApp ONTAP memudahkan peluncuran dan skala penyimpanan file bersama yang andal, berkinerja, dan aman di cloud. Dengan Amazon FSx untuk NetApp ONTAP, Anda tidak perlu lagi khawatir tentang pengaturan dan penyediaan server file dan volume penyimpanan, mereplikasi data, menginstal dan menambal perangkat lunak server file, mendeteksi dan mengatasi kegagalan perangkat keras, mengelola failover dan fallback, dan melakukan backup secara manual. Ini juga menyediakan integrasi yang

kaya dengan yang lain Layanan AWS, seperti AWS Identity and Access Management, Amazon WorkSpaces, AWS Key Management Service, dan AWS CloudTrail.

Amazon FSx memberi Anda dua sistem file untuk dipilih: Amazon untuk Windows File Server FSx untuk aplikasi berbasis Windows dan Amazon untuk Lustre FSx untuk beban kerja intensif komputasi. Untuk mempelajari lebih lanjut, lihat [Amazon FSx](#).

FAQ Amazon FSx untuk NetApp ONTAP di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon FSx untuk NetApp ONTAP di akun AMS saya?

Minta akses ke Amazon FSx untuk NetApp ONTAP dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_fsx_ontap_admin_role`. Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan Amazon FSx untuk NetApp ONTAP di akun AMS saya?

Mengganti grup keamanan di Amazon FSx untuk antarmuka jaringan elastis NetApp ONTAP (ENIs) mengharuskan Anda mengirimkan Manajemen | Lainnya | Lainnya | Pembaruan RFCs karena grup keamanan merupakan perimeter penting untuk lingkungan AMS. Itu satu-satunya batasan.

T: Apa prasyarat atau dependensi untuk menggunakan FSx Amazon NetApp untuk ONTAP di akun AMS saya?

Tidak ada prasyarat. Namun, Anda harus [Gunakan AMS SSP untuk menyediakan Amazon FSx di akun AMS Anda](#) menginstal.

Gunakan AMS SSP untuk menyediakan Amazon Inspector Classic di akun AMS Anda

Note

Pemberitahuan akhir dukungan: Pada 20 Mei 2026, AWS akan mengakhiri dukungan untuk Amazon Inspector Classic. Setelah 20 Mei 2026, Anda tidak akan lagi dapat mengakses konsol Amazon Inspector Classic atau sumber daya Amazon Inspector Classic. Amazon Inspector Classic tidak akan lagi tersedia untuk akun baru, dan akun yang belum menyelesaikan penilaian dalam enam bulan terakhir. Untuk semua akun lain, akses akan tetap berlaku hingga 20 Mei 2026, setelah itu Anda tidak lagi dapat mengakses konsol

Amazon Inspector Classic atau sumber daya Amazon Inspector Classic. Untuk informasi selengkapnya, lihat [bagian akhir dukungan Amazon Inspector Classic](#).

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Inspector Classic secara langsung di akun terkelola AMS Anda. Amazon Inspector Classic adalah layanan penilaian keamanan otomatis yang membantu meningkatkan keamanan dan kepatuhan aplikasi yang digunakan. AWS Amazon Inspector Classic secara otomatis menilai aplikasi untuk eksposur, kerentanan, dan penyimpangan dari praktik terbaik. Setelah melakukan penilaian, Amazon Inspector Classic menghasilkan daftar rinci temuan keamanan yang diprioritaskan berdasarkan tingkat keparahan. Temuan ini dapat ditinjau secara langsung atau sebagai bagian dari laporan penilaian terperinci, yang tersedia melalui konsol Amazon Inspector Classic atau API. Untuk mempelajari lebih lanjut, lihat [Amazon Inspector Classic](#).

FAQ Amazon Inspector di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon Inspector Classic di akun AMS saya?

Minta akses ke Amazon Inspector Classic dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran `customer_inspector_admin_role` IAM ke akun Anda. Peran tersebut mencakup `AmazonInspectorFullAccess` kebijakan AWS yang dikelola. Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Inspector Classic di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Inspector Classic tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Inspector Classic di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Amazon Inspector Classic di akun AMS Anda.

Gunakan Amazon Inspector baru di AMS

Anda sekarang dapat menggunakan Amazon Inspector baru di akun AMS Anda.

Untuk Amazon Inspector Classic, `customer-inspector-admin-role-ssm-inspector-agent-policy` dan diperlukan `AmazonInspectorFullAccess`. Namun, telah ada pembaruan untuk peran `SSPcustomer-inspector-admin-role`, yang sekarang mencakup tambahan.

policyAmazonInspector2FullAccess Kebijakan baru ini memungkinkan izin API untuk Amazon Inspector versi baru.

Gunakan AMS SSP untuk menyediakan Amazon Kendra di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Kendra secara langsung di akun terkelola AMS Anda. Amazon Kendra adalah layanan pencarian cerdas yang menggunakan pemrosesan bahasa alami dan algoritme pembelajaran mesin canggih untuk mengembalikan jawaban spesifik atas pertanyaan pencarian dari data Anda. Tidak seperti pencarian berbasis kata kunci tradisional, Amazon Kendra menggunakan kemampuan pemahaman semantik dan kontekstualnya untuk menentukan apakah dokumen relevan dengan kueri penelusuran. Amazon Kendra mengembalikan jawaban spesifik untuk pertanyaan, sehingga pengalaman Anda hampir berinteraksi dengan ahli manusia. Amazon Kendra sangat skalabel, mampu memenuhi tuntutan kinerja, terintegrasi erat dengan AWS layanan lain seperti Amazon S3 dan Amazon Lex, dan menawarkan keamanan tingkat perusahaan. Untuk mempelajari lebih lanjut, lihat [Amazon Kendra](#).

FAQ Amazon Kendra di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon Kendra di akun AMS saya?

Untuk meminta akses ke Amazon Inspector Classic, kirimkan RFC dengan Management | AWS service | Self-provisioned service | Tambahkan (ct-3qe6io8t6jtny) jenis perubahan. RFC ini menyediakan peran `customer_kendra_console_role` IAM ke akun Anda. Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Kendra di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Kendra tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Kendra di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk memulai dengan Amazon Kendra. Namun, tergantung pada kasus penggunaan spesifik Anda, Anda mungkin memerlukan akses ke AWS layanan lain.

Gunakan SSP AMS untuk menyediakan Amazon Kinesis Data Streams di akun AMS

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Kinesis Data Streams (KDS) secara langsung di akun terkelola AMS Anda. Amazon Kinesis Data Streams adalah layanan streaming data real-time yang sangat skalabel, dan tahan lama. KDS dapat terus

menangkap gigabyte data per detik dari ratusan ribu sumber seperti clickstream situs web, aliran peristiwa database, transaksi keuangan, umpan media sosial, log TI, dan peristiwa pelacakan lokasi. Data yang dikumpulkan tersedia dalam milidetik untuk memungkinkan kasus penggunaan analitik real-time seperti dasbor waktu nyata, deteksi anomali waktu nyata, harga dinamis, dan banyak lagi. Untuk mempelajari selengkapnya, lihat [Amazon Kinesis Data Streams](#).

FAQ Kinesis Data Streams di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Kinesis Data Streams di akun AMS saya?

Meminta akses ke Amazon Kinesis Data Streams dengan mengirimkan RFC dengan Manajemen | Layanan AWS | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_kinesis_data_streaming_user_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Kinesis Data Streams di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Kinesis Data Streams tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Kinesis Data Streams di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Amazon Kinesis Data Streams di akun AMS Anda.

Gunakan AMS SSP untuk menyediakan Amazon Kinesis Video Streams di akun AMS

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Kinesis Video Streams (KVS) secara langsung di akun terkelola AMS Anda. Amazon Kinesis Video Streams membantu Anda mengalirkan video dengan aman dari AWS perangkat yang terhubung ke analitik, pembelajaran mesin (ML), pemutaran, dan pemrosesan lainnya. Kinesis Video Streams secara otomatis menyediakan, dan menskalakan secara elastis, semua infrastruktur yang diperlukan untuk menyerap data video streaming dari jutaan perangkat. Ini juga tahan lama menyimpan, mengenkripsi, dan mengindeks data video di aliran Anda, dan memungkinkan Anda untuk mengakses data Anda melalui `easy-to-use APIs` Kinesis Video Streams memungkinkan Anda memutar video untuk dilihat langsung dan sesuai permintaan, dan dengan cepat membangun aplikasi yang memanfaatkan

visi komputer dan analitik video melalui integrasi dengan Amazon Rekognition Video, dan pustaka untuk kerangka kerja HTML seperti Apache,, dan OpenCV. MxNet TensorFlow Untuk mempelajari selengkapnya, lihat [Amazon Kinesis Video Streams](#).

FAQ Amazon Kinesis Video Streams di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Kinesis Video Streams di akun AMS saya?

Minta akses ke Amazon Kinesis Video Streams dengan mengirimkan RFC dengan AWS Manajemen | layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_kinesis_video_streaming_user_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Kinesis Video Streams di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Kinesis Video Streams tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Kinesis Video Streams di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Amazon Kinesis Video Streams di akun AMS Anda.

Gunakan AMS SSP untuk menyediakan Amazon Lex di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Lex secara langsung di akun terkelola AMS Anda. Amazon Lex adalah layanan untuk membangun antarmuka percakapan ke dalam aplikasi apa pun menggunakan suara dan teks. Amazon Lex menyediakan fungsionalitas pembelajaran mendalam lanjutan dari pengenalan suara otomatis (ASR) untuk mengonversi ucapan menjadi teks, dan pemahaman bahasa alami (NLU) untuk mengenali maksud teks, untuk memungkinkan Anda membangun aplikasi dengan pengalaman pengguna yang sangat menarik dan interaksi percakapan yang hidup. Dengan Amazon Lex, teknologi pembelajaran mendalam yang sama yang mendukung Amazon Alexa sekarang tersedia untuk pengembang mana pun, memungkinkan Anda untuk dengan cepat dan mudah membangun bahasa alami, bot percakapan, atau chatbot percakapan yang canggih dan mudah. Untuk mempelajari lebih lanjut, lihat [Amazon Lex](#).

FAQ Amazon Lex di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Lex di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_lex_author_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Lex di akun AMS saya?

Integrasi Amazon Lex dengan Lambda terbatas pada fungsi Lambda tanpa awalan “AMS-”, untuk mencegah modifikasi apa pun pada infrastruktur AMS.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Lex di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Amazon Lex di akun AMS Anda.

Gunakan AMS SSP untuk menyediakan Amazon MQ di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon MQ secara langsung di akun terkelola AMS Anda. Amazon MQ adalah layanan broker pesan terkelola untuk Apache ActiveMQ yang membantu Anda mengatur dan mengoperasikan broker pesan di cloud. Broker pesan memungkinkan sistem perangkat lunak yang berbeda, sering menggunakan bahasa pemrograman yang berbeda dan pada platform yang berbeda, untuk berkomunikasi dan bertukar informasi. Amazon MQ mengurangi beban operasional Anda dengan mengelola penyediaan, penyiapan, dan pemeliharaan ActiveMQ, broker pesan sumber terbuka yang populer. Menghubungkan aplikasi Anda saat ini ke Amazon MQ menggunakan standar industri APIs dan protokol untuk pengiriman pesan, termasuk JMS, NMS, AMQP, STOMP, MQTT, dan WebSocket. Menggunakan standar berarti, dalam banyak kasus, tidak perlu menulis ulang kode pesan apa pun saat Anda bermigrasi. AWS Untuk mempelajari lebih lanjut, lihat [Apa itu Amazon MQ?](#)

FAQ Amazon MQ di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon MQ di akun AMS saya?

Pemanfaatan Amazon MQ di akun AMS Anda adalah proses dua langkah:

1. Menyediakan Broker Amazon MQ. Untuk melakukan ini, kirimkan Template CFN, dengan Broker MQ Amazon disertakan, melalui RFC dengan Deployment | Ingestion | Stack CloudFormation from Template | Buat jenis perubahan (ct-36cn2avfrj9v), atau kirimkan RFC dengan Manajemen | Lainnya | Lainnya | Buat jenis perubahan (ct-1e1xtak34nx76) mengubah jenis yang meminta Amazon MQ Broker disediakan di akun Anda.
2. Akses konsol Amazon MQ. Setelah Amazon MQ Broker disediakan, dapatkan akses ke konsol Amazon MQ dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_mq_console_role`

Setelah peran disediakan di akun Anda, Anda harus memasukkannya ke dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon MQ di akun AMS saya?

Fungsionalitas penuh Amazon MQ tersedia di akun AMS Anda; namun, penyediaan Broker MQ Amazon tidak tersedia melalui kebijakan karena izin tinggi yang diperlukan. Lihat di atas untuk detail tentang cara menyediakan broker Amazon MQ di akun Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon MQ di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Amazon MQ di akun AMS Anda.

Menggunakan AMS SSP untuk menyediakan Amazon Managed Service untuk Apache Flink di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses Amazon Managed Service untuk kemampuan Apache Flink secara langsung di akun terkelola AMS Anda. Layanan Terkelola untuk Apache Flink adalah cara termudah untuk menganalisis data streaming, mendapatkan wawasan yang dapat ditindaklanjuti, dan menanggapi kebutuhan bisnis dan pelanggan Anda secara real time. Amazon Managed Service untuk Apache Flink mengurangi kompleksitas membangun, mengelola, dan mengintegrasikan aplikasi streaming dengan layanan lain. AWS Pengguna SQL dapat dengan mudah menanyakan data streaming atau membangun seluruh aplikasi streaming menggunakan templat dan editor SQL interaktif. Pengembang Java dapat dengan cepat membangun aplikasi streaming canggih menggunakan pustaka dan AWS integrasi Java open source untuk mengubah dan menganalisis data secara real time. Amazon Managed Service untuk Apache Flink menangani semua yang diperlukan untuk menjalankan aplikasi real-time Anda secara terus menerus dan menskalakan secara otomatis agar sesuai dengan volume dan throughput data masuk Anda. Dengan Amazon Managed Service untuk Apache Flink, Anda hanya membayar sumber daya

yang digunakan aplikasi streaming Anda. Tidak ada biaya minimum atau biaya pengaturan. Untuk mempelajari selengkapnya, lihat [Amazon Managed Service untuk Apache Flink](#).

Layanan Terkelola untuk Apache Flink di AWS Managed Services FAQ

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Managed Service untuk Apache Flink di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_kinesis_analytics_application_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Managed Service untuk Apache Flink di akun AMS saya?

- Konfigurasi terbatas pada sumber daya tanpa awalan 'AMS-' atau 'MC-' untuk mencegah modifikasi apa pun pada infrastruktur AMS.
- Izin untuk menghapus atau membuat Kinesis Data Streams atau Firehose baru telah dihapus dari kebijakan. Kami memiliki kebijakan lain yang memungkinkan itu.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Kinesis Data Streams di akun AMS saya?

Ada beberapa dependensi:

- Amazon Managed Service untuk Apache Flink mengharuskan Kinesis Data Streams atau Firehose harus dibuat sebelum mengonfigurasi aplikasi dengan Managed Service for Apache Flink.
- Izin kebijakan berbasis sumber daya harus menunjukkan sumber data input tertentu.

Gunakan AMS SSP untuk menyediakan Amazon Managed Streaming for Apache Kafka di akun AMS

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon Managed Streaming for Apache Kafka (Amazon MSK) secara langsung di akun terkelola AMS Anda. Amazon Managed Streaming for Apache Kafka adalah layanan data streaming yang AWS

dikelola sepenuhnya sehingga memudahkan Anda untuk membangun dan menjalankan aplikasi yang menggunakan Apache Kafka untuk memproses data streaming tanpa perlu menjadi ahli dalam mengoperasikan cluster Apache Kafka. Amazon MSK mengelola penyediaan, konfigurasi, dan pemeliharaan cluster Apache Kafka dan node Apache untuk Anda. ZooKeeper Amazon MSK juga menunjukkan metrik kinerja utama Apache Kafka di Konsol. AWS

Amazon MSK menyediakan beberapa tingkat keamanan untuk kluster Apache Kafka Anda, termasuk isolasi jaringan VPC, AWS IAM untuk otorisasi API bidang kontrol, enkripsi saat istirahat, enkripsi TLS dalam perjalanan, otentikasi sertifikat berbasis TLS, otentikasi diamankan oleh. SASL/SCRAM AWS Secrets Manager Untuk mempelajari lebih lanjut, lihat [Amazon MSK](#).

FAQ Amazon MSK di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon MSK di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini memberikan kebijakan dan peran IAM berikut ke akun Anda:

- `customer-msk-admin-policy.json`
- `AmazonMSKFullAccess`
- `customer-msk-admin-role.json`

Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon MSK?

Agar Amazon MSK dapat mengirimkan log broker ke tujuan yang Anda konfigurasi, pastikan bahwa `AmazonMSKFullAccess` kebijakan tersebut dilampirkan ke peran IAM Anda. Jadi izin akses penuh sudah ada.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon MSK?

Sebelum membuat cluster MSK Anda, Anda harus memiliki VPC dan subnet di dalam VPC itu. Secara default, AMS memiliki ini sebagai bagian dari pembuatan [VPC AMS](#) default.

Untuk mempelajari tentang batasan MSK Amazon, lihat Batas [MSK Amazon](#).

Gunakan SSP AMS untuk menyediakan Layanan Terkelola Amazon untuk Prometheus di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon Managed Service for Prometheus (AMP) secara langsung di akun terkelola AMS Anda. Amazon Managed Service for Prometheus adalah layanan pemantauan tanpa server yang kompatibel dengan Prometheus untuk metrik kontainer yang memudahkan pemantauan lingkungan kontainer dengan aman dalam skala besar. Dengan Amazon Managed Service for Prometheus, Anda dapat menggunakan model data Prometheus sumber terbuka dan bahasa kueri yang sama yang Anda gunakan saat ini untuk memantau kinerja beban kerja kontainer Anda, dan juga menikmati peningkatan skalabilitas, ketersediaan, dan keamanan tanpa harus mengelola infrastruktur yang mendasarinya.

Amazon Managed Service for Prometheus secara otomatis menskalakan konsumsi, penyimpanan, dan kueri metrik operasional saat beban kerja meningkat dan turun. Ini terintegrasi dengan layanan AWS keamanan untuk memungkinkan akses cepat dan aman ke data. Untuk informasi selengkapnya, lihat [Apa itu Layanan Terkelola Amazon untuk Prometheus?](#)

Layanan Terkelola Amazon untuk Prometheus di AWS Managed Services FAQ

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Managed Service untuk Prometheus di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer-prometheus-console-role` Setelah disediakan di akun Anda, Anda harus memasukkan `customer-prometheus-console-role` peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Layanan Terkelola Amazon untuk Prometheus di akun AMS saya?

Semua fitur didukung.

T: Apa prasyarat atau dependensi untuk menggunakan Layanan Terkelola Amazon untuk Prometheus di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk memulai Layanan Terkelola Amazon untuk Prometheus. Namun, tergantung pada kasus penggunaan spesifik Anda, Anda mungkin memerlukan akses ke AWS layanan lain.

Menggunakan AMS SSP untuk menyediakan Amazon Personalize di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon Personalisasi secara langsung di akun terkelola AMS Anda. Amazon Personalize adalah layanan pembelajaran mesin yang memudahkan pengembang untuk membuat rekomendasi individual bagi pelanggan yang menggunakan aplikasi mereka.

Pembelajaran mesin semakin banyak digunakan untuk meningkatkan keterlibatan pelanggan dengan mendukung rekomendasi produk dan konten yang dipersonalisasi, hasil pencarian yang disesuaikan, dan promosi pemasaran yang ditargetkan. Namun, mengembangkan kemampuan pembelajaran mesin yang diperlukan untuk menghasilkan sistem rekomendasi canggih ini telah berada di luar jangkauan sebagian besar organisasi saat ini karena kompleksitasnya. Amazon Personalize memungkinkan pengembang tanpa pengalaman pembelajaran mesin sebelumnya untuk dengan mudah membangun kemampuan personalisasi canggih ke dalam aplikasi mereka, menggunakan teknologi pembelajaran mesin yang disempurnakan dari penggunaan bertahun-tahun di Amazon.com.

Dengan Amazon Personalize, Anda menyediakan aliran aktivitas dari aplikasi Anda — klik, tampilan halaman, pendaftaran, pembelian, dan sebagainya — serta inventaris item yang ingin Anda rekomendasikan, seperti artikel, produk, video, atau musik. Anda juga dapat memilih untuk memberikan Amazon Personalize dengan informasi demografis tambahan dari pengguna Anda seperti usia, atau lokasi geografis. Amazon Personalize akan memproses dan memeriksa data, mengidentifikasi apa yang berarti, memilih algoritme yang tepat, serta melatih serta mengoptimalkan model personalisasi yang disesuaikan untuk data Anda. Semua data yang dianalisis oleh Amazon Personalize dijaga kerahasiaan dan aman, dan hanya digunakan untuk rekomendasi khusus Anda. Anda dapat mulai menyajikan rekomendasi yang dipersonalisasi melalui panggilan API sederhana. Anda hanya membayar untuk apa yang Anda gunakan, dan tidak ada biaya minimum dan tidak ada komitmen di muka.

Untuk mempelajari selengkapnya, lihat [Amazon Personalize](#).

FAQ Personalisasi Amazon di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon Personalize di akun AMS saya?

Minta akses dengan mengirimkan tipe perubahan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny), dan Anda perlu menentukan bucket S3 mana yang berisi data yang akan digunakan oleh personalisasi untuk menghasilkan rekomendasi. AWS RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_personalize_console_role` dan `customer_personalize_service_role`

- Setelah `customer_personalize_console_role` disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda. Anda juga dapat melampirkan `customer_personalize_console_policy` ke peran lain yang ada selain `Customer_ReadOnly_Role`.
- Setelah `customer_personalize_service_role` diberikan ke akun Anda, maka Anda dapat merujuk ARN-nya saat membuat grup dataset baru.

Pada saat ini, Operasi AMS juga akan menerapkan peran layanan ini di akun Anda: `aws_code_pipeline_service_role_policy`.

T: Apa batasan untuk menggunakan Amazon Personalize di akun AMS saya?

Konfigurasi Amazon Personalize terbatas pada sumber daya tanpa awalan 'ams-' atau 'mc-', untuk mencegah modifikasi apa pun pada infrastruktur AMS.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Personalize di akun AMS saya?

- Jika bucket S3 tempat data disimpan dienkripsi, ID kunci KMS harus disediakan, sehingga kami dapat mengizinkan peran yang digunakan oleh Amazon Personalize untuk mendekripsi bucket.

Amazon Personalize tidak mendukung kunci KMS S3 default. Jika diperlukan untuk menggunakan KMS, buat kunci kustom dan tambahkan kebijakan berikut dengan membuka RFC dengan jenis perubahan Kunci KMS | Buat (Review Required):

JSON

```
{
  "Version": "2012-10-17",
  "Id": "key-consolepolicy-3",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
```

```

        "Service": "personalize.amazonaws.com"
      },
      "Action": "kms:*",
      "Resource": "*"
    }
  ]
}

```

- Bucket S3 harus dibuat dengan kebijakan bucket berikut. Lakukan ini dengan mengirimkan RFC dengan jenis perubahan S3 Storage | Create Policy. Kebijakan ini memungkinkan Amazon Personalize untuk mengakses data; bucket tersebut akan berisi data yang akan digunakan oleh Amazon Personalize.

JSON

```

{
  "Version": "2012-10-17",
  "Id": "PersonalizeS3BucketAccessPolicy",
  "Statement": [
    {
      "Sid": "PersonalizeS3BucketAccessPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "personalize.amazonaws.com"
      },
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}

```


Gunakan AMS SSP untuk menyediakan Amazon QuickSight di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses QuickSight kapabilitas secara langsung di akun terkelola AMS Anda. QuickSight adalah layanan intelijen bisnis yang cepat dan bertenaga cloud yang memberikan wawasan kepada semua orang di organisasi Anda. Sebagai layanan yang dikelola sepenuhnya, Anda QuickSight dapat dengan mudah membuat dan menerbitkan dasbor interaktif yang menyertakan wawasan pembelajaran mesin (ML). Untuk mempelajari lebih lanjut, lihat [Amazon QuickSight](#).

QuickSight di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke QuickSight akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_quicksight_console_admin_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan QuickSight di akun AMS saya?

- AWS pengaturan sumber daya QuickSight tidak akan dapat diakses oleh Anda karena ketergantungan kebijakan IAM. Namun, tim AMS mengaktifkan setiap sumber daya untuk Anda sebagai tanggapan atas permintaan Anda untuk mengaktifkan layanan.
- Akses sumber daya untuk pengguna individu dan grup tidak didukung dalam model ini karena fitur ini memungkinkan pengguna untuk mengubah izin IAM yang dapat membahayakan infrastruktur AMS.
- Kemampuan untuk mengundang identitas IAM dari dalam tidak QuickSight didukung karena risiko yang terlibat mengubah objek IAM.
- QuickSight layanan menawarkan dua edisi: Enterprise dan Standard. Keduanya menyediakan opsi masuk tunggal (SSO) yang didukung di AMS. Namun, Enterprise Edition memiliki opsi untuk berintegrasi QuickSight dengan Active Directory (AD). QuickSight pada AMS tidak mendukung integrasi dengan AD karena ketidakcocokan antara struktur akun AMS dan persyaratan kepercayaan. QuickSight

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? QuickSight

- Ketika AMS menerima RFC ini untuk ditambahkan QuickSight, Anda akan dikirim permintaan layanan untuk informasi tambahan; berikan mereka yang berikut:
 - QuickSight nama akun (misalnya, *CustomerName*-quicksight)
 - QuickSight Edisi (Standar versus Perusahaan)
 - AWS Wilayah tempat mengaktifkan QuickSight layanan (default ke Wilayah AMS AWS Anda).
 - Alamat email notifikasi untuk QuickSight akun.
 - (Opsional) Bucket S3 tempat file data yang akan dianalisis berada.
 - VPC dan subnet IDs yang terhubung untuk QuickSight mendukung fitur untuk menambahkan koneksi VPC, yang memungkinkan konektivitas pribadi antara QuickSight dan sumber daya di dalam akun.

Operator AMS melakukan proses pendaftaran atas nama Anda dan mengonfigurasi dua QuickSight fungsi:

- [Penemuan otomatis](#) ke sumber data.
- [Koneksi VPC](#).

 Note

Tindakan ini perlu dilakukan oleh operator AMS karena izin IAM dan VPC yang ditinggikan diperlukan selama proses masuk.

Gunakan AMS SSP untuk menyediakan Amazon Rekognition di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Rekognition secara langsung di akun terkelola AMS Anda. Amazon Rekognition memudahkan untuk menambahkan analisis gambar dan video ke aplikasi Anda menggunakan teknologi pembelajaran mendalam yang terbukti, sangat skalabel, dan tidak memerlukan keahlian pembelajaran mesin untuk digunakan. Dengan Amazon Rekognition, Anda dapat mengidentifikasi objek, orang, teks, adegan, dan aktivitas dalam gambar dan video, serta mendeteksi konten yang tidak pantas. Amazon Rekognition juga menyediakan analisis wajah dan kemampuan pencarian wajah yang sangat akurat yang dapat Anda gunakan untuk mendeteksi, menganalisis, dan membandingkan wajah untuk

berbagai macam verifikasi pengguna, penghitungan orang, dan kasus penggunaan keselamatan publik.

Dengan Label Kustom Amazon Rekognition, Anda dapat mengidentifikasi objek dan adegan dalam gambar yang spesifik untuk kebutuhan bisnis Anda. Misalnya, Anda dapat membuat model untuk mengklasifikasikan suku cadang mesin tertentu di jalur perakitan Anda atau untuk mendeteksi tanaman yang tidak sehat. Amazon Rekognition Custom Labels menangani pengembangan model angkat berat untuk Anda, jadi tidak diperlukan pengalaman pembelajaran mesin. Anda hanya perlu menyediakan gambar objek atau adegan yang ingin Anda identifikasi, dan layanan menangani sisanya.

Untuk mempelajari lebih lanjut, lihat [Amazon Rekognition](#).

FAQ Rekognition Amazon di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Rekognition di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_rekognition_console_role` & `customer_rekognition_service_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Rekognition di akun AMS saya?

Fungsionalitas penuh Amazon Rekognition tersedia dengan peran layanan Amazon Rekognition yang disediakan sendiri.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Rekognition di akun AMS saya?

Jika Anda menggunakan Kinesis Video Streams yang menyediakan video streaming sumber untuk pemroses aliran Video Rekognition Amazon atau aliran data sebagai tujuan untuk menulis data ke Kinesis Data Streams, silakan berikan AMS saat membuat RFC. `kinesisStreamName`

Gunakan AMS SSP untuk menyediakan Amazon SageMaker AI di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon SageMaker AI secara langsung di akun terkelola AMS Anda. SageMaker AI memberi setiap

pengembang dan ilmuwan data kemampuan untuk membangun, melatih, dan menerapkan model pembelajaran mesin dengan cepat. Amazon SageMaker AI adalah layanan yang dikelola sepenuhnya yang mencakup seluruh alur kerja pembelajaran mesin untuk memberi label dan menyiapkan data Anda, memilih algoritme, melatih model, menyetel dan mengoptimalkannya untuk penerapan, membuat prediksi, dan mengambil tindakan. Model Anda dapat berproduksi lebih cepat dengan usaha yang jauh lebih sedikit dan biaya lebih rendah. Untuk mempelajari lebih lanjut, lihat [Amazon SageMaker AI](#).

SageMaker FAQ AI di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke SageMaker AI di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_sagemaker_admin_role` dan peran layanan. `AmazonSageMaker-ExecutionRole-Admin` Setelah SageMaker AI disediakan di akun Anda, Anda harus memasukkan `customer_sagemaker_admin_role` peran tersebut dalam solusi federasi Anda. Peran layanan tidak dapat diakses oleh Anda secara langsung; layanan SageMaker AI menggunakannya saat melakukan berbagai tindakan seperti yang dijelaskan di sini: [Melewati Peran](#).

T: Apa batasan untuk menggunakan SageMaker AI di akun AMS saya?

- Kasus penggunaan berikut tidak didukung oleh peran AMS Amazon SageMaker AI IAM:
 - SageMaker AI Studio tidak didukung saat ini.
 - SageMaker AI Ground Truth untuk mengelola tenaga kerja pribadi tidak didukung karena fitur ini memerlukan akses yang terlalu permisif ke sumber daya Amazon Cognito. Jika mengelola tenaga kerja pribadi diperlukan, Anda dapat meminta peran IAM khusus dengan izin gabungan SageMaker AI dan Amazon Cognito. Jika tidak, sebaiknya gunakan tenaga kerja publik (didukung oleh Amazon Mechanical Turk), AWS Marketplace atau penyedia layanan, untuk pelabelan data.
- Membuat Titik Akhir VPC untuk mendukung panggilan API ke layanan SageMaker AI (`aws.sagemaker.{region}.notebook`, `com.amazonaws.{region}.sagemaker.api` & `com.amazonaws.{region}.sagemaker.runtime`) tidak didukung karena izin tidak dapat dicakup ke layanan terkait AI saja. SageMaker Untuk mendukung kasus penggunaan ini, kirimkan Manajemen | Lainnya | RFC lainnya untuk membuat titik akhir VPC terkait.

- SageMaker Penskalaan otomatis titik akhir AI tidak didukung karena SageMaker AI memerlukan DeleteAlarm izin pada sumber daya (“*”) apa pun. Untuk mendukung penskalaan otomatis titik akhir, kirimkan Manajemen | Lainnya | RFC lainnya untuk mengatur penskalaan otomatis untuk titik akhir AI. SageMaker

T: Apa prasyarat atau dependensi untuk menggunakan SageMaker AI di akun AMS saya?

- Kasus penggunaan berikut memerlukan konfigurasi khusus sebelum digunakan:
 - Jika bucket S3 akan digunakan untuk menyimpan artefak dan data model, maka Anda harus meminta bucket S3 yang diberi nama dengan kata kunci yang diperlukan (“”, “Sagemaker”, SageMaker “sagemaker” atau “aws-glue”) dengan Deployment | Komponen tumpukan lanjutan | Penyimpanan S3 | Buat RFC.
 - Jika Elastic File Store (EFS) akan digunakan, maka penyimpanan EFS harus dikonfigurasi dalam subnet yang sama, dan diizinkan oleh grup keamanan.
 - Jika sumber daya lain memerlukan akses langsung ke layanan SageMaker AI (notebook, API, runtime, dan sebagainya), maka konfigurasi harus diminta oleh:
 - Mengirimkan RFC untuk membuat grup keamanan untuk titik akhir (Deployment | Advanced stack components | Security group | Create (auto)).
 - Mengirimkan Manajemen | Lainnya | Lainnya | Buat RFC untuk menyiapkan titik akhir VPC terkait.

T: Apa konvensi penamaan yang didukung untuk sumber daya yang **customer_sagemaker_admin_role** dapat diakses secara langsung? (Berikut ini adalah untuk memperbarui dan menghapus izin; jika Anda memerlukan konvensi penamaan tambahan yang didukung untuk sumber daya Anda, hubungi AMS Cloud Architect untuk konsultasi.)

- Sumber daya: Melewati AmazonSageMaker-ExecutionRole-* peran
 - Izin: Peran layanan yang disediakan sendiri SageMaker AI mendukung penggunaan peran layanan SageMaker AI (AmazonSageMaker-ExecutionRole-*) Anda dengan AWS Glue,, dan. AWS RoboMaker AWS Step Functions
- Sumber Daya: Rahasia tentang AWS Secrets Manager
 - Izin: Jelaskan, Buat, Dapatkan, Perbarui rahasia dengan AmazonSageMaker-* awalan.
 - Izin: Jelaskan, Dapatkan rahasia saat tag SageMaker sumber daya disetel ke true.
- Sumber Daya: Repositori di AWS CodeCommit

- Izin: Buat/hapus repositori dengan awalan. `AmazonSageMaker-`*
- Izin: Git Pull/Push pada repositori dengan awalan berikut,,, dan. `*sagemaker*` `*SageMaker*` `*Sagemaker*`
- Sumber Daya: Repositori Amazon ECR (Amazon Elastic Container Registry)
 - Izin: Izin: Setel, hapus kebijakan repositori, dan unggah gambar kontainer, saat konvensi penamaan sumber daya berikut digunakan,. `*sagemaker*`
- Sumber daya: ember Amazon S3
 - Izin: Dapatkan, Letakkan, Hapus objek, batalkan objek S3 unggahan multibagian saat sumber daya memiliki awalan berikut:,, dan. `*SageMaker*` `*Sagemaker*` `*sagemaker*` `aws-glue`
 - Izin: Dapatkan objek S3 saat SageMaker tag disetel ke. `true`
- Sumber Daya: Grup CloudWatch Log Amazon
 - Izin: Buat Grup Log atau Streaming, Letakkan Acara Log, Daftar, Perbarui, Buat, Hapus pengiriman log dengan awalan berikut:. `/aws/sagemaker/*`
- Sumber daya: Amazon CloudWatch Metric
 - Izin: Masukkan data metrik saat awalan berikut digunakan:`AWS/SageMaker,,,AWS/SageMaker/`, `aws/SageMaker` `aws/SageMaker/``aws/sagemaker`, `aws/sagemaker/` dan. `/aws/sagemaker/`.
- Sumber Daya: CloudWatch Dasbor Amazon
 - Izin: Create/Delete dasbor saat awalan berikut digunakan:. `customer_*`
- Sumber daya: Topik Amazon SNS (Layanan Pemberitahuan Sederhana)
 - Izin: Subscribe/Create topik saat awalan berikut digunakan:`*sagemaker*`,, `*SageMaker*` dan. `*Sagemaker*`

Q: Apa perbedaan antara **AmazonSageMakerFullAccess** dan **customer_sagemaker_admin_role**?

The `customer_sagemaker_admin_role` with the `customer_sagemaker_admin_policy` memberikan izin yang hampir sama dengan `AmazonSageMakerFullAccess` kecuali:

- Izin untuk terhubung dengan AWS RoboMaker, Amazon Cognito, dan AWS Glue sumber daya.
- SageMaker Penskalaan otomatis titik akhir AI. Anda harus mengirimkan RFC dengan Manajemen | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Perbarui entitas atau kebijakan (diperlukan tinjauan) jenis perubahan (ct-27tuth19k52b4) untuk meningkatkan izin

penskalaan otomatis sementara, atau secara permanen, karena penskalaan otomatis memerlukan akses permisif pada layanan. CloudWatch

T: Bagaimana cara mengadopsi kunci terkelola AWS KMS pelanggan dalam enkripsi data saat istirahat?

Anda harus memastikan bahwa kebijakan kunci telah diatur dengan benar pada kunci yang dikelola pelanggan sehingga pengguna atau peran IAM terkait dapat menggunakan kunci. Untuk informasi selengkapnya, lihat [dokumen Kebijakan AWS KMS Utama](#).

Gunakan AMS SSP untuk menyediakan Amazon Simple Email Service di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon Simple Email Service (Amazon SES) langsung di akun terkelola AMS Anda. Amazon Simple Email Service adalah layanan pengiriman email berbasis cloud yang dirancang untuk membantu pemasar digital dan pengembang aplikasi, mengirim email pemasaran, pemberitahuan, dan transaksional.

Anda dapat menggunakan antarmuka SMTP atau salah satu AWS SDKs untuk mengintegrasikan Amazon SES langsung ke aplikasi yang ada. Anda juga dapat mengintegrasikan kemampuan pengiriman email Amazon SES ke dalam perangkat lunak yang sudah Anda gunakan, seperti sistem tiket dan klien email.

Untuk mempelajari selengkapnya, lihat [Amazon Simple Email Service](#).

FAQ Amazon SES di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon SES di akun AMS saya?

Meminta akses ke Amazon SES dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_ses_admin_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon SES di akun AMS saya?

- Anda harus mengonfigurasi kebijakan bucket S3 agar Amazon SES dapat memublikasikan peristiwa ke bucket.

- Anda harus menggunakan default (AWS SES), atau mengonfigurasi, kunci CMK untuk mengizinkan Amazon SES mengenkripsi email dan mendorong peristiwa ke sumber daya layanan lain seperti Amazon S3, Amazon SNS, Lambda, dan Firehose, milik akun.

T: Apa batasan untuk menggunakan Amazon SES di akun AMS saya?

Anda harus meningkatkan RFCs untuk membuat sumber daya berikut:

- Pengguna SMTP dan peran layanan IAM dengan PutEvents izin, ke aliran Kinesis Firehose.
- Anda harus membuat AWS sumber daya baru seperti bucket S3, aliran Firehose, topik SNS dengan menggunakan jenis perubahan AMS agar aturan Amazon SES dan tujuan set konfigurasi dapat berfungsi dengan sumber daya tersebut.
- Kredensi SMTP. Untuk meminta kredensi SMTP baru, gunakan Ubah Jenis (Manajemen | Lainnya | Lainnya | Buat). AMS membuat kredensial dan menambahkannya ke Secrets Manager untuk Anda.

Gunakan AMS SSP untuk menyediakan Amazon Simple Workflow Service di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Simple Workflow Service (Amazon SWF) secara langsung di akun terkelola AMS Anda. Amazon Simple Workflow Service membantu pengembang membangun, menjalankan, dan menskalakan pekerjaan latar belakang yang memiliki langkah paralel atau berurutan. Anda dapat menganggap Amazon SWF sebagai pelacak status dan koordinator tugas yang dikelola sepenuhnya di Cloud. Jika langkah aplikasi Anda membutuhkan waktu lebih dari 500 milidetik untuk diselesaikan, Anda perlu melacak status pemrosesan, atau Anda perlu memulihkan atau mencoba lagi jika tugas gagal, Amazon SWF dapat membantu Anda. Untuk mempelajari selengkapnya, lihat [Amazon Simple Workflow Service](#).

FAQ Amazon SWF di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon SWF di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_swf_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon SWF di akun AMS saya?

InvokeFunctionIzin Lambda telah disertakan dalam layanan ini, namun AMS `customer_deny_policy` yang ditambahkan ke semua peran pelanggan AMS secara eksplisit menolak akses ke fungsi AMS Lambda dan sumber daya milik AMS. Untuk menandai atau menghapus tag sumber daya dalam Amazon SWF, kirimkan Manajemen | Lainnya | Jenis Perubahan Lainnya.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon SWF di akun AMS saya?

Amazon SWF bergantung pada AWS Lambda layanan, oleh karena itu, izin untuk memanggil Lambda telah diberikan sebagai bagian dari peran ini dan tidak ada izin tambahan yang diperlukan untuk memanggil Lambda dari Amazon SWF. Jika tidak, tidak ada prasyarat untuk menggunakan Amazon SWF.

Gunakan AMS SSP untuk menyediakan Amazon Ttract di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Textract secara langsung di akun terkelola AMS Anda. Amazon Textract adalah layanan pembelajaran mesin yang dikelola sepenuhnya yang secara otomatis mengekstrak teks cetak, tulisan tangan, dan data lain dari dokumen yang dipindai yang melampaui pengenalan karakter optik sederhana (OCR) untuk mengidentifikasi, memahami, dan mengekstrak data dari formulir dan tabel. Untuk mempelajari lebih lanjut, lihat [Amazon Texttract](#).

FAQ Amazon Texttract di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta Amazon Texttract untuk disiapkan di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun

Anda: `customer_textract_console_role`, `customer_textract_human_review_execution_role` dan `customer_ec2_textract_instance_profile` Setelah disediakan di akun Anda, Anda harus memasukkan peran `customer_textract_console_role` dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Ttract di akun AMS saya?

Tidak ada batasan untuk penggunaan Amazon Ttract di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Ttract di akun AMS saya?

Anda harus meminta pembuatan bucket S3 dengan mengirimkan Deployment RFC | Komponen tumpukan lanjutan | S3 storage | Create (ct-1a68ck03fn98r).

Gunakan SSP AMS untuk menyediakan Amazon Transcribe di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Transcribe secara langsung di akun terkelola AMS Anda. Amazon Transcribe adalah layanan pengenalan suara otomatis yang dikelola sepenuhnya dan dilatih terus menerus yang secara otomatis menghasilkan transkrip teks berstempel waktu dari file audio. Amazon Transcribe memudahkan pengembang untuk menambahkan speech-to-text kemampuan ke aplikasi mereka. Data audio hampir tidak mungkin bagi komputer untuk mencari dan menganalisis. Oleh karena itu, pidato yang direkam perlu dikonversi menjadi teks sebelum dapat digunakan dalam aplikasi. Secara historis, pelanggan harus bekerja dengan penyedia transkripsi yang mengharuskan mereka menandatangani kontrak mahal dan sulit untuk diintegrasikan ke dalam tumpukan teknologi mereka untuk menyelesaikan tugas ini. Banyak dari penyedia ini menggunakan teknologi usang yang tidak beradaptasi dengan baik untuk skenario yang berbeda, seperti audio telepon dengan kesetiaan rendah yang umum di pusat kontak, yang menghasilkan akurasi yang buruk.

Amazon Transcribe menggunakan proses pembelajaran mendalam yang disebut Automatic Speech Recognition (ASR) untuk mengubah ucapan menjadi teks, dengan cepat dan akurat. Amazon Transcribe dapat digunakan untuk mentranskripsikan panggilan layanan pelanggan, mengotomatiskan teks dan subtitling tertutup, dan menghasilkan metadata untuk aset media guna membuat arsip yang dapat dicari sepenuhnya. Anda dapat menggunakan Amazon Transcribe Medical untuk menambahkan speech-to-text kemampuan medis ke aplikasi dokumentasi klinis. Untuk mempelajari lebih lanjut, lihat [Amazon Transcribe](#).

FAQ Amazon Transcribe di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta Amazon Transcribe disiapkan di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_transcribe_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan Amazon Transcribe di akun AMS saya?

Anda harus menggunakan 'customer-transcribe*' sebagai awalan untuk bucket Anda saat bekerja dengan transcribe, kecuali RA dan ditentukan lain.

Anda tidak dapat membuat peran IAM dalam transkrip Amazon.

Anda tidak dapat menggunakan bucket S3 yang dikelola layanan untuk data keluaran di SSPS default (jika diperlukan, hubungi CA akun Anda).

Anda harus mengirimkan Penerimaan Risiko jika ingin menggunakan Kunci KMS yang dikelola pelanggan yang tidak termasuk dalam namespace AMS.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Transcribe di akun AMS saya?

S3 harus memiliki akses ke bucket dengan nama 'customer-transcribe*'. KMS diperlukan untuk menggunakan Amazon Transcribe jika bucket S3 Anda dienkripsi dengan kunci KMS. Jika ember tidak perlu dienkripsi "KMStranscribelzinkan" dapat dihapus.

Gunakan AMS SSP untuk menyediakan Amazon WorkSpaces di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses WorkSpaces kapabilitas secara langsung di akun terkelola AMS Anda. WorkSpaces memungkinkan Anda menyediakan desktop Microsoft Windows atau Amazon Linux virtual berbasis cloud untuk pengguna Anda, yang dikenal sebagai WorkSpaces WorkSpaces menghilangkan kebutuhan untuk mendapatkan dan menyebarkan perangkat keras atau menginstal perangkat lunak yang kompleks. Anda dapat dengan cepat menambahkan atau menghapus pengguna saat kebutuhan Anda berubah. Pengguna mengaksesnya WorkSpaces dengan menggunakan aplikasi klien dari perangkat yang didukung atau, untuk Windows WorkSpaces, browser web, dan mereka masuk dengan menggunakan kredensial Active Directory (AD) lokal yang ada.

Untuk mempelajari lebih lanjut, lihat [Amazon WorkSpaces](#).

WorkSpaces di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke WorkSpaces akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM

berikut ke akun Anda: `customer_workspaces_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan WorkSpaces di akun AMS saya?

Fungsionalitas penuh Workspaces tersedia dengan peran layanan Amazon yang WorkSpaces disediakan sendiri.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? WorkSpaces

- WorkSpaces dibatasi oleh AWS Wilayah; oleh karena itu, AD Connector harus dikonfigurasi di AWS Wilayah yang sama tempat WorkSpaces instans di-host.

Pelanggan dapat terhubung WorkSpaces ke AD pelanggan menggunakan salah satu dari dua metode berikut:

1. Menggunakan konektor AD untuk otentikasi proxy ke layanan Active Directory lokal (lebih disukai):

Konfigurasi Konektor Direktori Aktif (AD) di akun AMS Anda sebelum mengintegrasikan WorkSpaces instans Anda dengan layanan direktori lokal. Konektor AD bertindak sebagai proxy bagi pengguna AD yang ada (dari domain Anda) untuk terhubung WorkSpaces menggunakan kredensial AD lokal yang ada. Ini lebih disukai karena WorkSpaces secara langsung bergabung dengan domain on-prem pelanggan, yang bertindak sebagai Resource dan User forest, yang mengarah ke kontrol yang lebih besar di sisi pelanggan.

Untuk informasi selengkapnya, lihat [Praktik Terbaik untuk Menerapkan Amazon WorkSpaces \(Skenario 1\)](#).

2. Menggunakan Konektor AD dengan AWS Microsoft AD, VPC Layanan Bersama, dan kepercayaan satu arah ke lokal:

Anda juga dapat mengautentikasi pengguna dengan direktori lokal dengan terlebih dahulu membuat kepercayaan keluar satu arah dari AD yang dikelola AMS ke AD lokal. WorkSpaces akan bergabung dengan AMS-managed AD menggunakan AD Connector. WorkSpaces Izin akses kemudian akan didelegasikan ke WorkSpaces instans melalui AD yang dikelola AMS, tanpa perlu membangun kepercayaan dua arah dengan lingkungan lokal Anda. Dalam skenario ini, hutan Pengguna akan berada di AD pelanggan dan hutan Sumber Daya akan berada di AD yang dikelola AMS (perubahan pada AD yang dikelola AMS dapat diminta melalui RFC). Perhatikan bahwa konektivitas antara WorkSpaces VPC dan VPC Layanan Bersama MALZ yang menjalankan AD yang dikelola AMS dibuat melalui Transit Gateway.

Untuk informasi selengkapnya, lihat [Praktik Terbaik untuk Menerapkan Amazon WorkSpaces \(Skenario 6\)](#).

 Note

[AD Connector](#) dapat dikonfigurasi dengan mengirimkan [Management | Other | Other | Other | Create change type RFC](#) dengan detail konfigurasi AD prasyarat; untuk informasi selengkapnya, lihat [Membuat AD Connector](#). Jika metode 2 digunakan untuk membuat hutan Sumber Daya di AD yang dikelola AMS, kirimkan Manajemen lain | Lainnya | Lainnya | Lainnya | Buat jenis perubahan RFC di akun layanan bersama AMS dengan menjalankan AD yang dikelola AMS.

Gunakan SSP AMS untuk menyediakan layanan Kode AMS di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas layanan Kode AMS secara langsung di akun terkelola AMS Anda. Layanan AMS Code adalah bundling eksklusif dari layanan manajemen kode AWS sebagaimana dirinci selanjutnya. Anda dapat memilih untuk menerapkan semua layanan di AMS dengan layanan Kode AMS, atau Anda dapat menerapkannya di AMS satu per satu.

Layanan Kode AMS mencakup layanan berikut:

- AWS CodeCommit: Layanan [kontrol sumber](#) yang dikelola sepenuhnya yang menampung repositori berbasis Git yang aman. Itu membuatnya sehingga tim dapat berkolaborasi dalam kode dalam ekosistem yang aman dan sangat skalabel. CodeCommit menghilangkan kebutuhan untuk mengoperasikan sistem kontrol sumber Anda sendiri atau khawatir tentang penskalaan infrastrukturnya. Anda dapat menggunakan CodeCommit untuk menyimpan apa pun dengan aman dari kode sumber ke biner dan bekerja dengan mulus dengan alat Git Anda yang ada. Untuk mempelajari selengkapnya, lihat [AWS CodeCommit](#)

Untuk menerapkan ini di akun AMS Anda secara independen dari layanan Kode AMS, lihat [Gunakan SSP AMS untuk menyediakan AWS CodeCommit di akun AMS Anda](#).

- AWS CodeBuild: Layanan integrasi berkelanjutan yang dikelola sepenuhnya yang mengkompilasi kode sumber, menjalankan pengujian, dan menghasilkan paket perangkat lunak yang siap digunakan. Dengan CodeBuild, Anda tidak perlu menyediakan, mengelola, dan menskalakan

server build Anda sendiri. CodeBuild menskalakan terus menerus dan memproses beberapa build secara bersamaan, sehingga build Anda tidak dibiarkan menunggu dalam antrian. Anda dapat memulai dengan cepat menggunakan lingkungan build yang dikemas sebelumnya, atau Anda dapat membuat lingkungan build khusus yang menggunakan alat build Anda sendiri. Dengan CodeBuild, Anda dikenakan biaya per menit untuk sumber daya komputasi yang Anda gunakan. Untuk mempelajari selengkapnya, lihat [AWS CodeBuild](#)

Untuk menerapkan ini di akun AMS Anda secara independen dari layanan Kode AMS, lihat [Gunakan SSP AMS untuk menyediakan AWS CodeBuild di akun AMS Anda](#).

- AWS CodeDeploy: Layanan penyebaran terkelola penuh yang mengotomatiskan penerapan perangkat lunak ke berbagai layanan komputasi seperti Amazon EC2 dan server lokal Anda. AWS CodeDeploy membantu Anda merilis fitur baru dengan cepat, membantu Anda menghindari downtime selama penerapan aplikasi, dan menangani kompleksitas memperbarui aplikasi Anda. Anda dapat menggunakan AWS CodeDeploy untuk mengotomatiskan penerapan perangkat lunak, menghilangkan kebutuhan akan operasi manual yang rawan kesalahan. Skala layanan agar sesuai dengan kebutuhan penerapan Anda. Untuk mempelajari selengkapnya, lihat [AWS CodeDeploy](#)

Untuk menerapkan ini di akun AMS Anda secara independen dari layanan Kode AMS, lihat [Gunakan SSP AMS untuk menyediakan AWS CodeDeploy di akun AMS Anda](#).

- AWS CodePipeline: Layanan [pengiriman berkelanjutan](#) yang dikelola sepenuhnya yang membantu Anda mengotomatiskan saluran pipa rilis untuk pembaruan aplikasi dan infrastruktur yang cepat dan andal. CodePipeline mengotomatiskan fase build, test, dan deploy dari proses rilis Anda setiap kali ada perubahan kode, berdasarkan model rilis yang Anda tentukan. Ini memungkinkan Anda untuk dengan cepat dan andal memberikan fitur dan pembaruan. Anda dapat dengan mudah mengintegrasikan AWS CodePipeline dengan layanan pihak ketiga seperti GitHub atau dengan plugin kustom Anda sendiri. Dengan AWS CodePipeline, Anda hanya membayar untuk apa yang Anda gunakan. Tidak ada biaya di muka atau komitmen jangka panjang. Untuk mempelajari selengkapnya, lihat [AWS CodePipeline](#)

Untuk menerapkan ini di akun AMS Anda secara independen dari layanan Kode AMS, lihat [Gunakan SSP AMS untuk menyediakan AWS CodePipeline di akun AMS Anda](#).

Layanan Kode AMS di AWS Managed Services FAQ

T: Bagaimana cara meminta akses ke layanan Kode AMS di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM

berikut ke akun Anda: `customer_code_suite_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda. Pada saat ini Operasi AMS juga akan menerapkan `customer_codebuild_service_role`, `customer_codedeploy_service_role`, peran `aws_code_pipeline_service_role` layanan di akun Anda untuk CodeBuild, CodeDeploy dan CodePipeline layanan. Jika izin IAM tambahan untuk diperlukan untuk diperlukan, kirimkan permintaan layanan AMS: `customer_codebuild_service_role`

Note

Anda juga dapat menambahkan layanan ini secara terpisah; untuk informasi, lihat [Gunakan SSP AMS untuk menyediakan AWS CodeBuild di akun AMS Anda](#), [Gunakan SSP AMS untuk menyediakan AWS CodeDeploy di akun AMS Anda](#), dan [Gunakan SSP AMS untuk menyediakan AWS CodePipeline di akun AMS Anda](#), masing-masing.

T: Apa batasan untuk menggunakan layanan Kode AMS di akun AMS saya?

- AWS CodeCommit: Fitur pemicu CodeCommit dinonaktifkan mengingat hak terkait untuk membuat topik SNS. Autentikasi langsung terhadap CodeCommit dibatasi; pengguna harus mengautentikasi dengan Credential Helper. Beberapa perintah KMS juga dibatasi: `kms: Enkripsi`, `kms: Dekripsi`, `kms: ReEncrypt`, `kms: GenerateDataKey` dan `kms: GenerateDataKeyWithoutPlaintext` `kms: DescribeKey`
- CodeBuild: Untuk akses admin AWS CodeBuild konsol, izin dibatasi pada tingkat sumber daya; misalnya, CloudWatch tindakan dibatasi pada sumber daya tertentu dan `iam: PassRole` izin dikontrol.
- CodeDeploy: Saat ini CodeDeploy mendukung penerapan hanya di EC2 Amazon/On-premise. Penerapan di ECS dan Lambda melalui tidak didukung. CodeDeploy
- CodePipeline: CodePipeline fitur, tahapan, dan penyedia terbatas pada hal-hal berikut:
 - Tahap Penerapan: Amazon S3 dan AWS CodeDeploy
 - Tahap Sumber: Amazon S3, Bit Bucket AWS CodeCommit, dan GitHub
 - Build Stage: AWS CodeBuild dan Jenkins
 - Tahap Persetujuan: Amazon SNS
 - Tahap Uji: AWS CodeBuild, Jenkins, Pengujian UI Ghost Inspector BlazeMeter, Beban StormRunner Fokus Mikro, Pemantauan API Runscope
 - Panggilan Panggilan: Step Functions dan Lambda

Note

Operasi AMS menyebarkan `customer_code_pipeline_lambda_policy` di akun Anda; itu harus dilampirkan dengan peran eksekusi Lambda untuk tahap pemanggilan Lambda. Berikan nama `service/execution` peran Lambda yang Anda inginkan agar kebijakan ini ditambahkan. Jika tidak ada `service/execution` peran Lambda khusus, maka AMS membuat peran baru bernama `customer_code_pipeline_lambda_execution_role`, yaitu salinan dari peran Lambda `customer_lambda_basic_execution_role`. `customer_code_pipeline_lambda_policy`

T: Apa prasyarat atau dependensi untuk menggunakan layanan Kode AMS di akun AMS saya?

- **CodeCommit:** Jika bucket S3 dienkripsi dengan AWS KMS kunci, S3 dan AWS KMS harus digunakan. AWS CodeCommit
- **CodeBuild:** Jika izin IAM tambahan diperlukan untuk peran AWS CodeBuild layanan yang ditentukan, minta izin tersebut melalui permintaan layanan AMS.
- **CodeDeploy:** Tidak ada.
- **CodePipeline:** Tidak ada. AWS layanan yang didukung—AWS CodeCommit AWS CodeBuild,, AWS CodeDeploy—harus diluncurkan sebelum, atau bersamaan dengan, peluncuran. CodePipeline Namun ini dilakukan oleh insinyur AMS.

Gunakan SSP AMS untuk menyediakan AWS Amplify di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Amplify kapabilitas secara langsung di akun terkelola AMS Anda. AWS Amplify Ini adalah solusi lengkap yang memungkinkan pengembang web dan seluler frontend untuk dengan mudah membangun, menghubungkan, dan meng-host aplikasi fullstack. Amplify memberikan fleksibilitas untuk memanfaatkan luasnya AWS layanan saat kasus penggunaan Anda berkembang. Amplify menyediakan produk untuk membangun aplikasi iOS, Android, Flutter, Web, dan React Native fullstack. Untuk mempelajari selengkapnya, lihat [AWS Amplify](#).

AWS Amplify di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara saya meminta AWS Amplify untuk disiapkan di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_amplify_console_role` Setelah disediakan ke akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

Selain itu, Anda harus memberikan Penerimaan Risiko karena AWS Amplify memiliki izin mutasi infrastruktur. Untuk melakukan ini, bekerja dengan Cloud Service Delivery Manager (CSDM) Anda.

T: Apa batasan penggunaan AWS Amplify di akun AMS saya?

Anda harus menggunakan `'amplify*'` sebagai awalan untuk bucket Anda saat bekerja dengan Amplify, kecuali RA dan ditentukan lain.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Amplify

Tidak ada prasyarat untuk penggunaan di akun AMS Anda. AWS Amplify

Hanya lingkungan Malz: Peran bawaan bawaan untuk Amplify adalah `"customer_amplify_console_role"`. Untuk menggunakan peran kustom, pertama-tama gunakan entitas IAM. Kemudian, buat RFC tambahan untuk menambahkan peran kustom Anda ke daftar izin Kebijakan Kontrol Layanan untuk Akun Aplikasi.

Gunakan AMS SSP untuk menyediakan AWS AppSync

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS AppSync kapabilitas secara langsung di akun terkelola AMS Anda. AWS AppSync menyederhanakan pengembangan aplikasi dengan memungkinkan Anda membuat API fleksibel untuk mengakses, memanipulasi, dan menggabungkan data dengan aman dari satu atau beberapa sumber data. AWS AppSync adalah layanan terkelola yang menggunakan GraphQL untuk memudahkan aplikasi mendapatkan data yang tepat yang mereka butuhkan.

Dengan AWS AppSync, Anda dapat membangun aplikasi yang dapat diskalakan, termasuk yang memerlukan pembaruan waktu nyata, pada berbagai sumber data seperti penyimpanan data NoSQL, database relasional, APIs HTTP, dan sumber data kustom Anda. AWS Lambda Untuk aplikasi seluler dan web, AWS AppSync juga menyediakan akses data lokal saat perangkat offline, dan sinkronisasi data dengan resolusi konflik yang dapat disesuaikan, saat kembali online. Untuk mempelajari selengkapnya, lihat [AWS AppSync](#).

AWS AppSync di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses AWS AppSync di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_appsync_service_role` dan `customer_appsync_author_role`. Setelah disediakan di akun Anda, Anda harus memasukkan solusi `customer_appsync_author_role` dalam federasi Anda.

T: Apa batasan untuk menggunakan AWS AppSync?

- Saat membuat Sumber Data AppSync pada pelanggan perlu menentukan peran layanan yang dibuat sebelumnya, pembuatan peran baru tidak diperbolehkan dan oleh karena itu akan mengembalikan akses yang ditolak
- AppSync peran dikonfigurasi untuk membatasi izin ke sumber daya yang berisi awalan 'AMS-' atau 'MC-' untuk mencegah modifikasi apa pun pada infrastruktur AMS.

T: Apa prasyarat atau dependensi yang digunakan? AWS AppSync

Layanan ini memungkinkan beberapa layanan lain untuk digunakan sebagai sumber data, Izin dasar untuk menggunakannya seperti itu termasuk dalam peran layanan (`customer_appsync_service_role`), tetapi Anda harus secara manual memilih peran layanan saat menggunakan layanan.

Gunakan SSP AMS untuk menyediakan AWS App Mesh di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS App Mesh kapabilitas secara langsung di akun terkelola AMS Anda. AWS App Mesh menyediakan jaringan tingkat aplikasi untuk memudahkan layanan Anda berkomunikasi satu sama lain di berbagai jenis infrastruktur komputasi. App Mesh menstandarisasi cara layanan Anda berkomunikasi, memberi Anda end-to-end visibilitas dan memastikan ketersediaan tinggi untuk aplikasi Anda.

AWS App Mesh memudahkan menjalankan layanan dengan menyediakan visibilitas yang konsisten dan kontrol lalu lintas jaringan untuk layanan yang dibangun di berbagai jenis infrastruktur komputasi. App Mesh menghilangkan kebutuhan untuk memperbarui kode aplikasi untuk mengubah cara data pemantauan dikumpulkan atau lalu lintas dirutekan antar layanan. App Mesh mengonfigurasi setiap

layanan untuk mengeksport data pemantauan dan mengimplementasikan logika kontrol komunikasi yang konsisten di seluruh aplikasi Anda. Ini memudahkan untuk dengan cepat menentukan lokasi kesalahan yang tepat dan secara otomatis merutekan ulang lalu lintas jaringan ketika ada kegagalan atau ketika perubahan kode perlu digunakan. Untuk mempelajari selengkapnya, lihat [AWS App Mesh](#).

AWS App Mesh di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses AWS App Mesh di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_app_mesh_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS App Mesh?

Fungsionalitas penuh AWS App Mesh tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan? AWS App Mesh

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS App Mesh

Gunakan SSP AMS untuk menyediakan AWS Audit Manager di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Audit Manager secara langsung di akun terkelola AMS Anda. Audit Manager membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda menilai risiko dan kepatuhan terhadap peraturan dan standar industri. Audit Manager mengotomatisasi pengumpulan bukti untuk membuatnya lebih mudah untuk menilai apakah kebijakan, prosedur, dan aktivitas Anda beroperasi secara efektif. Ketika tiba waktunya untuk audit, Audit Manager membantu Anda mengelola tinjauan pemangku kepentingan atas kontrol Anda dan membantu Anda membuat laporan siap audit dengan upaya manual yang jauh lebih sedikit. Untuk mempelajari lebih lanjut, lihat [Audit Manager](#).

AWS Audit Manager di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Audit Manager akun AMS saya?

Anda dapat meminta akses melalui pengajuan Manajemen RFC Layanan | Layanan AWS | AWS Layanan yang disediakan sendiri | Tambah (diperlukan peninjauan) (ct-3qe6io8t6jtny). RFC ini menyediakan peran IAM berikut di akun Anda: `customer-audit-manager-admin-Role`. Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS Audit Manager?

Tidak ada batasan untuk penggunaan AWS Audit Manager di akun AMS Anda. Fungsionalitas AWS Audit Manager penuh untuk disediakan.

T: Apa prasyarat atau dependensi yang digunakan? AWS Audit Manager

1. Anda perlu menyediakan AMS dengan ember s3 tempat Anda reports/assessments ingin tinggal.
2. Jika Anda ingin memiliki enkripsi dengan layanan ini, Anda perlu menyediakan AMS dengan KMS CMK ARN untuk digunakan.
3. Jika Anda ingin mengirim pemberitahuan SNS ke Topik, Anda harus memberikan nama topik atau arn.
4. (Opsional) Ada prasyarat tambahan jika Anda ingin mengaktifkan Organizations sebagai bagian dari landing zone multi-akun Anda di Audit Manager dan Anda menginginkan akun administrator yang didelegasikan: Di kolom deskripsi untuk RFC (Manajemen AWS | layanan | Layanan yang Kompatibel | Tambah), sebutkan bahwa Anda ingin menggunakan akun administrator yang didelegasikan sebagai bagian dari Pengaturan Audit Manager dan berikan rincian di bawah ini:
 - KMS CMK ARN (digunakan untuk mengatur Audit Manager, awalnya)
 - ID akun administrator yang didelegasikan untuk Audit Manager untuk digunakan sebagai bagian dari landing zone multi-akun ini (dapat berupa akun aplikasi MALZ)

Gunakan SSP AMS untuk menyediakan AWS Batch di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Batch kapabilitas secara langsung di akun terkelola AMS Anda. AWS Batch memungkinkan pengembang, ilmuwan, dan insinyur untuk dengan mudah dan efisien menjalankan ratusan ribu pekerjaan komputasi batch AWS. AWS Batch secara dinamis menyediakan kuantitas dan jenis sumber daya komputasi yang optimal (seperti CPU atau instance yang dioptimalkan memori) berdasarkan volume dan persyaratan sumber daya spesifik dari pekerjaan batch yang dikirimkan. Dengan AWS Batch, tidak perlu menginstal dan mengelola perangkat lunak komputasi batch atau cluster server yang Anda

gunakan untuk menjalankan pekerjaan Anda, memungkinkan Anda untuk fokus pada menganalisis hasil dan memecahkan masalah. Untuk mempelajari selengkapnya, lihat [AWS Batch](#).

AWS Batch di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Batch akun AMS saya?

1. Untuk meminta akses ke AWS Batch, kirimkan Manajemen RFC | Layanan AWS | Layanan yang disediakan sendiri | Tambah (ct-1w8z66n899dct). RFC ini menyediakan peran dan kebijakan IAM berikut di akun Anda:

Peran IAM:

- `customer_batch_console_role`
- `customer_batch_ecs_instance_role`
- `customer_batch_events_service_role`
- `customer_batch_service_role`
- `customer_batch_ecs_task_role`

Kebijakan:

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`
- `customer_batch_events_service_role_policy`

2. Setelah disediakan di akun Anda, Anda harus memasukkan peran `customer_batch_console_role` dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS Batch?

Saat membuat Lingkungan Komputasi, Anda harus menandai EC2 instance sebagai “customer_batch” atau “customer-batch”. Jika instance tidak diberi tag, instance tidak akan dihentikan berdasarkan batch saat pekerjaan selesai.

T: Apa prasyarat atau dependensi yang digunakan? AWS Batch

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS Batch

Gunakan SSP AMS untuk menyediakan AWS Certificate Manager di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas AWS Certificate Manager (ACM) secara langsung di akun terkelola AMS Anda. AWS Certificate Manager adalah layanan yang memungkinkan Anda menyediakan, mengelola, dan menyebarkan sertifikat Secure Sockets Layer/Transport Layer Security (SSL/TLS) publik dan pribadi untuk digunakan dengan AWS layanan dan sumber daya internal Anda yang terhubung. SSL/TLS sertifikat digunakan untuk mengamankan komunikasi jaringan dan menetapkan identitas situs web melalui internet serta sumber daya di jaringan pribadi. AWS Certificate Manager menghapus proses manual yang memakan waktu untuk membeli, mengunggah, dan memperbarui SSL/TLS sertifikat.

Dengan AWS Certificate Manager, Anda dapat meminta sertifikat, menerapkannya pada AWS sumber daya yang terintegrasi dengan ACM, seperti Elastic Load Balancers, distribusi CloudFront Amazon, dan pada APIs API Gateway, dan biarkan menangani perpanjangan sertifikat. AWS Certificate Manager Ini juga memungkinkan Anda untuk membuat sertifikat pribadi untuk sumber daya internal Anda dan mengelola siklus hidup sertifikat secara terpusat. Sertifikat publik dan swasta yang disediakan AWS Certificate Manager untuk digunakan dengan layanan terintegrasi ACM gratis. Anda hanya membayar untuk AWS sumber daya yang Anda buat untuk menjalankan aplikasi Anda. Dengan [AWS Private Certificate Authority](#), Anda membayar bulanan untuk pengoperasian AWS Private CA dan untuk sertifikat pribadi yang Anda terbitkan. Untuk mempelajari lebih lanjut, lihat [AWS Certificate Manager - AWS Dokumentasi](#).

FAQ ACM di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Certificate Manager akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_acm_create_role` Anda dapat menggunakan peran ini untuk membuat dan mengelola sertifikat ACM. Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

Sertifikat ACM dapat dibuat menggunakan jenis perubahan berikut, meskipun Anda belum menambahkan peran `customer_acm_create_role` IAM:

- [ACM | Buat Sertifikat Publik](#)
- [ACM | Buat Sertifikat Pribadi](#)
- [Sertifikat ACM dengan tambahan SANs | Buat](#)

T: Apa batasan untuk menggunakan AWS Certificate Manager?

Anda harus mengirimkan Permintaan Perubahan (RFC) ke AMS untuk menghapus atau memodifikasi sertifikat yang ada, karena tindakan tersebut memerlukan akses admin penuh (gunakan Manajemen | Lainnya | Lainnya | Jenis perubahan pembaruan (ct-0xdawir96cy7k). Perhatikan bahwa kebijakan IAM tidak dapat mengecualikan hak berdasarkan nama tag (mc*, ams*, dll). Sertifikat tidak dikenakan biaya, jadi menghapus sertifikat yang tidak digunakan tidak sensitif terhadap waktu.

T: Apa prasyarat atau dependensi untuk menggunakan Certificate Manager?

Nama DNS publik yang ada, dan akses untuk membuat catatan DNS CNAME, tetapi itu tidak perlu di-host di akun terkelola.

Gunakan SSP AMS untuk menyediakan AWS Private Certificate Authority di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Private Certificate Authority kapabilitas secara langsung di akun terkelola AMS Anda. Sertifikat privat digunakan untuk mengidentifikasi dan mengamankan komunikasi antara sumber daya yang terhubung di jaringan pribadi, seperti server, seluler, dan perangkat dan aplikasi IoT. AWS Private CA adalah layanan CA pribadi terkelola yang membantu Anda mengelola siklus hidup sertifikat pribadi Anda dengan mudah dan aman. AWS Private CA memberi Anda layanan CA pribadi yang sangat tersedia tanpa investasi di muka dan biaya pemeliharaan berkelanjutan untuk mengoperasikan CA pribadi Anda sendiri. AWS Private CA memperluas kemampuan manajemen sertifikat ACM ke sertifikat pribadi, memungkinkan Anda untuk membuat dan mengelola sertifikat publik dan swasta secara terpusat. Anda dapat dengan mudah membuat dan menerapkan sertifikat pribadi untuk AWS sumber daya menggunakan AWS Management Console atau ACM API. Untuk EC2 instance, container, perangkat IoT, dan sumber daya lokal, Anda dapat dengan mudah membuat dan melacak sertifikat pribadi dan menggunakan kode otomatisasi sisi klien Anda sendiri untuk menerapkannya. Anda juga memiliki fleksibilitas untuk membuat sertifikat pribadi dan mengelolanya sendiri untuk aplikasi yang memerlukan masa pakai sertifikat khusus, algoritme kunci, atau nama sumber daya Untuk mempelajari lebih lanjut, lihat. [AWS Private CA](#)

AWS Private CA di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses AWS Private CA di akun AMS saya?

Meminta akses melalui pengajuan AWS Layanan RFC (Manajemen | layanan | AWS Layanan yang Kompatibel). Melalui RFC ini peran IAM berikut akan disediakan di akun Anda:.

`customer_acm_pca_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS Private CA?

Saat ini, AWS Resource Access Manager (AWS RAM) tidak dapat digunakan untuk berbagi AWS Private CA lintas akun Anda.

T: Apa prasyarat atau dependensi yang digunakan? AWS Private CA

1. Jika Anda berencana untuk membuat CRL, Anda memerlukan ember S3 untuk menyimpannya. AWS Private CA secara otomatis menyeter CRL di bucket Amazon S3 yang Anda tunjuk dan memperbaruinya secara berkala. Merupakan syarat awal bahwa bucket S3 memiliki kebijakan bucket di bawah ini sebelum Anda dapat menyiapkan CRL. Untuk melanjutkan permintaan ini; buat RFC dengan `ct-0fpj1xa808sh2` (Manajemen | Komponen tumpukan lanjutan | Penyimpanan S3 | Kebijakan pembaruan) sebagai berikut:

- Berikan nama bucket S3 atau ARN.
- Salin kebijakan di bawah ini ke RFC dan ganti `bucket-name` dengan nama bucket S3 yang Anda inginkan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "acm-pca.amazonaws.com"
      },
      "Action": [
```



```

        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation"
    ],
    "Resource": [
        "arn:aws:s3:::bucket-name/*",
        "arn:aws:s3:::bucket-name"
    ]
}
]
}

```

2. Jika bucket S3 di atas dienkripsi, maka Service Principal `acm-pca.amazonaws.com` memerlukan izin untuk mendekripsi. Untuk melanjutkan permintaan ini; buat RFC dengan `ct-3ovo7px2vsa6n` (Manajemen | Komponen tumpukan lanjutan | Kunci KMS | Pembaruan) sebagai berikut:

- Berikan ARN Kunci KMS di mana kebijakan harus diperbarui.
- Salin kebijakan di bawah ini ke RFC dan ganti `bucket-name` dengan nama bucket S3 yang Anda inginkan.

```

{
  "Sid": "Allow ACM-PCA use of the key",
  "Effect": "Allow",
  "Principal": {
    "Service": "acm-pca.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": [
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
        "arn:aws:s3:::bucket_name/audit-report/*",
        "arn:aws:s3:::bucket_name/crl/*"
      ]
    }
  }
}

```

```
}  
}  
}
```

3. AWS Private CA CRLs tidak mendukung pengaturan S3 “Blokir akses publik ke ember dan objek yang diberikan melalui daftar kontrol akses baru (ACLs)”. Anda harus menonaktifkan pengaturan ini dengan akun S3 dan bucket untuk memungkinkan penulisan CRLs seperti yang disebutkan di [Cara membuat dan menyimpan CRL Anda dengan aman untuk ACM Private CA Jika Anda ingin menonaktifkan, buat](#) RFC baru dengan ct-0xdawir96cy7k (Manajemen | Lainnya | Lainnya | Pembaruan) dan lampirkan Penerimaan Risiko. AWS Private CA Jika Anda memiliki pertanyaan tentang penerimaan risiko, hubungi Cloud Architect Anda.

Gunakan SSP AMS untuk menyediakan AWS CloudEndure di akun AMS Anda

Note

Setelah peluncuran yang sukses AWS Application Migration Service, layanan CloudEndure Migrasi sekarang berakhir di semua AWS Wilayah. Kami merekomendasikan penggunaan pelanggan AWS Application Migration Service untuk migrasi lift dan shift ke GovCloud Wilayah dan ke Wilayah Komersil. Untuk informasi, lihat [Apa itu AWS Application Migration Service?](#) .

Jika Anda ingin menggunakan AWS Application Migration Service, hubungi CA Anda sehingga mereka dapat memandu Anda.

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS CloudEndure kapabilitas secara langsung di akun terkelola AMS Anda. AWS CloudEndure migrasi menyederhanakan, mempercepat, dan mengotomatiskan migrasi skala besar dari infrastruktur fisik, virtual, dan berbasis cloud ke infrastruktur. AWS CloudEndure Disaster Recovery (DR) melindungi terhadap downtime dan kehilangan data dari ancaman apa pun, termasuk ransomware dan korupsi server.

AWS CloudEndure di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke CloudEndure akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan Pengguna

IAM berikut ke akun Anda: `customer_cloud_endure_user` Setelah disediakan di akun Anda, kunci akses dan kunci rahasia untuk pengguna dibagikan di AWS Secrets Manager.

Kebijakan ini juga disediakan untuk akun: `customer_cloud_endure_policy` dan `customer_cloud_endure_deny_policy`

Selain itu, Anda harus memberikan Penerimaan Risiko karena solusi CloudEndure DR untuk integrasi aplikasi memiliki izin mutasi infrastruktur. Untuk melakukan ini, bekerja dengan manajer pengiriman layanan cloud (CSDM) Anda.

T: Apa batasan penggunaan CloudEndure di akun AMS saya?

Instans replikasi dan konversi cloud endure hanya dapat diluncurkan di subnet yang Anda tunjukkan.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? CloudEndure Bagikan hal berikut melalui korespondensi dua arah RFC:

- Detail Subnet VPC untuk instans Replikasi dan Konversi yang akan diluncurkan.
- Nama Sumber Daya Amazon Kunci KMS (ARN) jika volume EBS dienkripsi.

Gunakan SSP AMS untuk menyediakan AWS CloudHSM di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS CloudHSM kapabilitas secara langsung di akun terkelola AMS Anda. AWS CloudHSM membantu Anda memenuhi persyaratan kepatuhan perusahaan, kontraktual, dan peraturan untuk keamanan data dengan menggunakan instans Modul Keamanan Perangkat Keras (HSM) khusus di cloud. AWS, dan mitra AWS Marketplace, menawarkan berbagai solusi untuk melindungi data sensitif dalam AWS platform, tetapi untuk beberapa aplikasi dan data yang tunduk pada mandat kontrak atau peraturan untuk mengelola kunci kriptografi, perlindungan tambahan mungkin diperlukan. AWS CloudHSM melengkapi solusi perlindungan data yang ada dan memungkinkan Anda untuk melindungi kunci enkripsi Anda di dalamnya HSMs yang dirancang dan divalidasi dengan standar pemerintah untuk manajemen kunci yang aman. AWS CloudHSM memungkinkan Anda untuk membuat, menyimpan, dan mengelola kunci kriptografi dengan aman yang digunakan untuk enkripsi data dengan cara yang kunci hanya dapat diakses oleh Anda. Untuk mempelajari selengkapnya, lihat [AWS CloudHSM](#).

AWS CloudHSM di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS CloudHSM akun AMS saya?

Pemanfaatan di akun AMS Anda adalah proses dua langkah:

1. Minta AWS CloudHSM cluster. Lakukan ini dengan mengirimkan RFC dengan Manajemen | Lainnya | Lainnya | Buat (ct-1e1xtak34nx76) jenis perubahan. Sertakan detail berikut:
 - AWS Wilayah.
 - VPC ID/ARN. Provide a VPC ID/VPC ARN yang berada di akun yang sama dengan RFC yang Anda kirimkan.
 - Tentukan setidaknya dua Availability Zone untuk cluster.
 - ID EC2 instans Amazon yang akan terhubung ke cluster HSM.
2. Akses AWS CloudHSM konsol. Lakukan ini dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_cloudhsm_console_role`

Setelah peran disediakan di akun Anda, Anda harus memasukkannya ke dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS CloudHSM di akun AMS saya?

Akses ke AWS CloudHSM konsol tidak memberi Anda kemampuan untuk membuat, menghentikan, atau memulihkan kluster Anda. Untuk melakukan hal-hal itu, kirimkan Manajemen | Lainnya | Lainnya | Buat jenis perubahan (ct-1e1xtak34nx76) jenis perubahan.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS CloudHSM

Anda harus mengizinkan lalu lintas TCP menggunakan port 2225 melalui EC2 instans Amazon klien dalam VPC, atau menggunakan Direct Connect VPN untuk server on-premise yang menginginkan akses ke cluster HSM. AWS CloudHSM tergantung pada Amazon EC2 untuk grup keamanan dan antarmuka jaringan. Untuk pemantauan atau audit log, HSM mengandalkan CloudTrail (operasi AWS API) dan CloudWatch Log untuk semua aktivitas perangkat HSM lokal.

T: Siapa yang akan menerapkan pembaruan ke AWS CloudHSM klien dan pustaka perangkat lunak terkait?

Anda bertanggung jawab untuk menerapkan pembaruan perpustakaan dan klien. Anda akan ingin memantau halaman riwayat [versi CloudHSM](#) untuk rilis, dan kemudian menerapkan pembaruan menggunakan peningkatan klien [CloudHSM](#).

Note

Tambahan perangkat lunak untuk alat HSM selalu diterapkan secara otomatis oleh layanan AWS CloudHSM

Gunakan SSP AMS untuk menyediakan AWS CodeBuild di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS CodeBuild kapabilitas secara langsung di akun terkelola AMS Anda. AWS CodeBuild adalah layanan integrasi berkelanjutan yang dikelola sepenuhnya yang mengkompilasi kode sumber, menjalankan pengujian, dan menghasilkan paket perangkat lunak yang siap digunakan. Dengan CodeBuild, Anda tidak perlu menyediakan, mengelola, dan menskalakan server build Anda sendiri. CodeBuild menskalakan terus menerus dan memproses beberapa build secara bersamaan, sehingga build Anda tidak dibiarkan menunggu dalam antrian. Anda dapat memulai dengan cepat menggunakan lingkungan build yang dikemas sebelumnya, atau Anda dapat membuat lingkungan build khusus yang menggunakan alat build Anda sendiri. Dengan CodeBuild, Anda dikenakan biaya per menit untuk sumber daya komputasi yang Anda gunakan. Untuk mempelajari selengkapnya, lihat [AWS CodeBuild](#).

Note

Untuk onboard CodeCommit, CodeBuild CodeDeploy, dan CodePipeline dengan satu RFC, kirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) ubah jenis dan minta tiga layanan:, dan. CodeBuild CodeDeploy CodePipeline Kemudian, ketiga peran, `customer_codebuild_service_role`, `customer_codedeploy_service_role`, dan `aws_code_pipeline_service_role` disediakan di akun Anda. Setelah penyediaan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

CodeBuild di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS CodeBuild akun AMS saya?

Pemanfaatan AWS CodeBuild di akun AMS Anda adalah proses dua langkah:

1. Menyediakan proses build CodeBuild Service Role untuk berkoordinasi dengan bucket AWS S3, Amazon, CloudWatch dan grup Log
2. Minta akses ke CodeBuild konsol

Anda dapat meminta agar keduanya disiapkan di akun AMS Anda dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS CodeBuild di akun AMS saya?

Untuk akses administrator AWS CodeBuild konsol, izin dibatasi pada tingkat sumber daya; misalnya, CloudWatch tindakan dibatasi pada sumber daya tertentu dan `iam:PassRole` izin dikontrol.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? CodeBuild

Jika izin IAM tambahan diperlukan untuk peran AWS CodeBuild layanan yang ditentukan, minta izin tersebut melalui permintaan layanan AMS.

Gunakan SSP AMS untuk menyediakan AWS CodeCommit di akun AMS Anda

Note

AWS telah menutup akses pelanggan baru AWS CodeCommit, efektif 25 Juli 2024. AWS CodeCommit Pelanggan yang sudah ada dapat terus menggunakan layanan seperti biasa. AWS terus berinvestasi dalam keamanan, ketersediaan, dan peningkatan kinerja untuk AWS CodeCommit, tetapi kami tidak berencana untuk memperkenalkan fitur baru. Untuk memigrasikan CodeCommit repositori AWS Git ke penyedia Git lainnya, hubungi arsitek cloud (CA) Anda untuk mendapatkan panduan. Untuk informasi selengkapnya tentang memigrasi repositori Git Anda, lihat [Cara memigrasikan repositori CodeCommit AWS Anda ke penyedia Git lain](#).

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS CodeCommit kapabilitas secara langsung di akun terkelola AMS Anda. AWS CodeCommit adalah layanan [kontrol sumber](#) yang dikelola sepenuhnya yang menampung repositori berbasis Git yang aman. Ini membantu tim untuk berkolaborasi dalam kode dalam ekosistem yang aman dan sangat skalabel.

CodeCommit menghilangkan kebutuhan untuk mengoperasikan sistem kontrol sumber Anda sendiri atau khawatir tentang penskalaan infrastrukturnya. Anda dapat menggunakan CodeCommit untuk menyimpan apa pun dengan aman mulai dari kode sumber hingga binari, dan ini bekerja dengan mulus dengan alat Git Anda yang ada. Untuk mempelajari selengkapnya, lihat [AWS CodeCommit](#).

Note

Untuk onboard CodeCommit, CodeBuild CodeDeploy, dan CodePipeline dengan satu RFC, kirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) ubah jenis dan minta tiga layanan:, dan. CodeBuild CodeDeploy CodePipeline Kemudian, ketiga peran, `customer_codebuild_service_role`, `customer_codedeploy_service_role`, dan `aws_code_pipeline_service_role` disediakan di akun Anda. Setelah penyediaan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

CodeCommit di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke CodeCommit akun AMS saya?

AWS CodeCommit peran konsol dan akses data dapat diminta melalui pengajuan dua AWS Layanan RFCs, akses konsol, dan akses data:

- Minta akses ke AWS CodeCommit dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_codecommit_console_role`. Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

Akses data (seperti Pelatihan dan Daftar Entitas) memerlukan terpisah CTs untuk setiap sumber data yang menentukan sumber data S3 (wajib), bucket keluaran (wajib) dan KMS (opsional). Tidak ada batasan untuk penciptaan lapangan AWS CodeCommit kerja selama semua sumber data telah diberikan peran akses. Untuk meminta akses data, kirimkan RFC dengan Manajemen | Lainnya | Buat (ct-1e1xtak34nx76).

T: Apa batasan penggunaan AWS CodeCommit di akun AMS saya?

Fitur pemicu CodeCommit dinonaktifkan mengingat hak terkait untuk membuat topik SNS. Autentikasi langsung terhadap CodeCommit dibatasi, pengguna harus mengautentikasi dengan Credential

Helper. Beberapa perintah KMS juga dibatasi: `kms:Encrypt`, `kms:Decrypt`, `kms:ReEncrypt`, `kms:GenerateDataKey`, `kms:GenerateDataKeyWithoutPlaintext`, dan `kms:DescribeKey`.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS CodeCommit

Jika bucket S3 dienkripsi dengan kunci KMS, S3 dan KMS harus digunakan. AWS CodeCommit

Gunakan SSP AMS untuk menyediakan AWS CodeDeploy di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS CodeDeploy kapabilitas secara langsung di akun terkelola AMS Anda. AWS CodeDeploy adalah layanan penyebaran terkelola penuh yang mengotomatiskan penerapan perangkat lunak ke berbagai layanan komputasi seperti Amazon EC2, AWS Fargate AWS Lambda, dan server lokal Anda. AWS CodeDeploy membantu Anda merilis fitur baru dengan cepat, membantu Anda menghindari downtime selama penerapan aplikasi, dan menangani kompleksitas memperbarui aplikasi Anda. Anda dapat menggunakan AWS CodeDeploy untuk mengotomatiskan penerapan perangkat lunak, menghilangkan kebutuhan akan operasi manual yang rawan kesalahan. Skala layanan agar sesuai dengan kebutuhan penerapan Anda. Untuk mempelajari selengkapnya, lihat [AWS CodeDeploy](#).

Note

Untuk onboard CodeCommit, CodeBuild CodeDeploy, dan CodePipeline dengan satu RFC, kirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) ubah jenis dan minta tiga layanan: dan. CodeBuild CodeDeploy CodePipeline Kemudian, ketiga peran, `customer_codebuild_service_role`, `customer_codedeploy_service_role`, dan `aws_code_pipeline_service_role` disediakan di akun Anda. Setelah menyediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

CodeDeploy di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke CodeDeploy akun AMS saya?

Meminta akses CodeDeploy dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_codedeploy_console_role`

dan. `customer_codedeploy_service_role` Setelah disediakan di akun Anda, Anda harus memasukkan `customer_codedeploy_console_role` peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan CodeDeploy di akun AMS saya?

Saat ini kami hanya mendukung Platform Komputasi sebagai — EC2 Amazon/On-Premises. Blue/Green Penerapan tidak didukung.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? CodeDeploy

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. CodeDeploy

Gunakan SSP AMS untuk menyediakan AWS CodePipeline di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS CodePipeline kapabilitas secara langsung di akun terkelola AMS Anda. AWS CodePipeline adalah layanan [pengiriman berkelanjutan](#) yang dikelola sepenuhnya yang membantu Anda mengotomatiskan saluran pipa rilis Anda untuk pembaruan aplikasi dan infrastruktur yang cepat dan andal. CodePipeline mengotomatiskan fase build, test, dan deploy dari proses rilis Anda setiap kali ada perubahan kode, berdasarkan model rilis yang Anda tentukan. Ini memungkinkan Anda untuk dengan cepat dan andal memberikan fitur dan pembaruan. Anda dapat dengan mudah mengintegrasikan AWS CodePipeline dengan layanan pihak ketiga seperti GitHub atau dengan plugin kustom Anda sendiri. Dengan AWS CodePipeline, Anda hanya membayar untuk apa yang Anda gunakan. Tidak ada biaya di muka atau komitmen jangka panjang. Untuk mempelajari selengkapnya, lihat [AWS CodePipeline](#).

Note

Untuk onboard CodeCommit, CodeBuild CodeDeploy, dan CodePipeline dengan satu RFC, kirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) ubah jenis dan minta tiga layanan:, dan. CodeBuild CodeDeploy CodePipeline Kemudian, ketiga peran, `customer_codebuild_service_role`, `customer_codedeploy_service_role`, dan `aws_code_pipeline_service_role` disediakan di akun Anda. Setelah menyediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda. CodePipeline di AMS tidak mendukung “ CloudWatch Acara Amazon” untuk Tahap Sumber karena memerlukan izin yang lebih tinggi untuk membuat peran dan kebijakan layanan, yang melewati model hak istimewa paling sedikit dan proses manajemen perubahan AMS.

CodePipeline di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke CodePipeline akun AMS saya?

Minta akses ke CodePipeline dengan mengirimkan permintaan layanan untuk `customer_code_pipeline_console_role` di akun yang relevan. Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

Pada saat ini, Operasi AMS juga akan menerapkan peran layanan ini di akun Anda:
`aws_code_pipeline_service_role_policy`

T: Apa batasan penggunaan CodePipeline di akun AMS saya?

Ya. CodePipeline fitur, tahapan, dan penyedia terbatas pada hal-hal berikut:

1. Tahap Penerapan: Terbatas untuk Amazon S3, dan AWS CodeDeploy
2. Tahap Sumber: Terbatas untuk Amazon S3,, AWS CodeCommit, dan BitBucket GitHub
3. Build Stage: Terbatas untuk AWS CodeBuild, dan Jenkins
4. Tahap Persetujuan: Terbatas untuk Amazon SNS
5. Tahap Uji: Terbatas pada AWS CodeBuild, Jenkins,, Ghost Inspector UI Testing BlazeMeter, Micro StormRunner Focus Load, dan Runscope API Monitoring
6. Panggilan Panggilan: Terbatas untuk Step Functions, dan Lambda

Note

Operasi AMS akan diterapkan `customer_code_pipeline_lambda_policy` di akun Anda; itu harus dilampirkan dengan peran eksekusi Lambda untuk tahap pemanggilan Lambda. Harap berikan nama service/execution peran Lambda yang Anda inginkan agar kebijakan ini ditambahkan. Jika tidak ada service/execution peran Lambda khusus, AMS akan membuat peran baru bernama `customer_code_pipeline_lambda_execution_role`, yang akan menjadi salinan dari peran `LambdaBasicExecutionRole`.
`customer_code_pipeline_lambda_policy`

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? CodePipeline

AWS layanan yang didukung AWS CodeCommit AWS CodeBuild,, AWS CodeDeploy harus diluncurkan sebelum, atau bersamaan dengan, peluncuran CodePipeline.

Gunakan SSP AMS untuk menyediakan AWS Compute Optimizer di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Compute Optimizer kapabilitas secara langsung di akun terkelola AMS Anda. AWS Compute Optimizer merekomendasikan sumber daya AWS Komputasi yang optimal untuk beban kerja Anda untuk mengurangi biaya dan meningkatkan kinerja dengan menggunakan pembelajaran mesin untuk menganalisis metrik pemanfaatan historis. Komputasi penyediaan berlebih (EC2 Amazon ASGs dan) dapat menyebabkan biaya infrastruktur yang tidak perlu dan komputasi yang kurang penyediaan dapat menyebabkan kinerja aplikasi yang buruk. Compute Optimizer membantu Anda memilih jenis instans EC2 Amazon yang optimal, termasuk yang merupakan bagian dari grup Auto EC2 Scaling Amazon, berdasarkan data pemanfaatan Anda. Untuk mempelajari selengkapnya, lihat [AWS Compute Optimizer](#).

FAQ Compute Optimizer di AWS Managed Services

T: Bagaimana cara meminta akses ke Compute Optimizer di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_compute_optimizer_readonly_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Compute Optimizer di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh AWS Compute Optimizer tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Compute Optimizer di akun AMS saya?

- Anda harus mengirimkan RFC (Manajemen | Lainnya | Lainnya | Pembaruan) yang mengizinkan AMS Ops untuk mengaktifkan layanan di akun. Selama penerapan, peran terkait layanan (SLR) dibuat untuk memungkinkan pengumpulan metrik dan pembuatan laporan. SLR diberi label ""`AWSServiceRoleForComputeOptimizer`". Untuk informasi selengkapnya, lihat [Menggunakan Peran Tertaut Layanan](#) untuk AWS Compute Optimizer
- CloudWatch metrik harus diaktifkan untuk metrik berikut:
 - Pemanfaatan CPU: Persentase unit EC2 komputasi Amazon yang dialokasikan yang digunakan pada instance. Metrik ini mengidentifikasi daya pemrosesan yang diperlukan untuk menjalankan aplikasi pada instance yang dipilih.

- Pemanfaatan memori: Jumlah memori yang telah digunakan dalam beberapa cara selama periode sampel. Metrik ini mengidentifikasi memori yang diperlukan untuk menjalankan aplikasi pada instance yang dipilih. Pemanfaatan memori dianalisis hanya untuk sumber daya yang memiliki CloudWatch agen terpadu diinstal pada mereka. Untuk informasi lebih lanjut, lihat [Mengaktifkan Pemanfaatan Memori dengan CloudWatch Agen](#) (hal. 10).
- Jaringan di: Jumlah byte yang diterima pada semua antarmuka jaringan oleh instance. Metrik ini mengidentifikasi volume trafik jaringan yang masuk ke satu instance.
- Jaringan keluar: Jumlah byte yang dikirim pada semua antarmuka jaringan oleh instance. Metrik ini mengidentifikasi volume trafik jaringan keluar dari satu instance.
- Disk lokal input/output (I/O): Jumlah input/output operasi untuk disk lokal. Metrik ini mengidentifikasi kinerja volume root dari sebuah instance

Gunakan SSP AMS untuk menyediakan AWS DataSync di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS DataSync kapabilitas secara langsung di akun terkelola AMS Anda. AWS DataSync memindahkan sejumlah besar data secara online antara penyimpanan lokal dan Amazon S3, Amazon Elastic File System (Amazon Elastic File System) atau Amazon FSx. Tugas manual yang terkait dengan transfer data dapat memperlambat migrasi dan membebani operasi TI. DataSync menghilangkan atau secara otomatis menangani banyak tugas ini, termasuk pekerjaan penyalinan skrip, penjadwalan dan pemantauan transfer, memvalidasi data, dan mengoptimalkan pemanfaatan jaringan. Agen DataSync perangkat lunak terhubung ke penyimpanan Network File System (NFS) dan Server Message Block (SMB) Anda, sehingga Anda tidak perlu memodifikasi aplikasi Anda. DataSync Dapat mentransfer ratusan terabyte dan jutaan file dengan kecepatan hingga 10 kali lebih cepat daripada alat sumber terbuka, melalui internet atau tautan. AWS Direct Connect Anda dapat menggunakan DataSync untuk memigrasikan kumpulan data aktif atau arsip ke AWS, mentransfer data ke cloud untuk analisis dan pemrosesan tepat waktu, atau mereplikasi data AWS untuk kelangsungan bisnis.

Untuk mempelajari selengkapnya, lihat [AWS DataSync](#).

DataSync di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke DataSync akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_datasync_console_role`

Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

Grup CloudWatch log yang digunakan untuk melakukan streaming log tugas adalah “/aws/datasync”.

T: Apa batasan penggunaan DataSync di akun AMS saya?

Fungsionalitas penuh AWS DataSync tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? DataSync

- Amazon S3 (Nama Sumber Daya ARNs Amazon) diperlukan untuk semua bucket S3 yang terkait dengan DataSync tugas yang akan dilakukan menggunakan peran layanan. DataSync `customer_datasync_service_role`
- Endpoint VPC dan grup keamanan untuk DataSync agen harus diminta dengan RFC dengan Manajemen | Lainnya | Lainnya | Buat (ct-1e1xtak34nx76) mengubah jenis sebelum menggunakan VPC Endpoints.
- AWS DataSync agen berjalan di AMS sebagai alat. AWS DataSync Agen ditambah dan diperbarui oleh layanan; untuk detailnya, lihat [AWS DataSync FAQ](#).
- Untuk meluncurkan AWS DataSync agen, kirimkan RFC dengan Manajemen | Lainnya | Lainnya | Buat (ct-1e1xtak34nx76) jenis perubahan, meminta agen disebarkan. Berikan ID AWS DataSync Amazon EC2 AMI, jenis instans, subnet, grup keamanan; dan referensi EC2 keypair Amazon yang ada atau minta pembuatan keypair baru.

 Note

AMS menyediakan AWS DataSync agen secara manual atas nama pelanggan, dan tidak memerlukan proses konsumsi WIGS di Amazon AWS DataSync AMI. EC2

Gunakan SSP AMS untuk menyediakan AWS Device Farm di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Device Farm kapabilitas secara langsung di akun terkelola AMS Anda. AWS Device Farm adalah layanan pengujian aplikasi yang memungkinkan Anda meningkatkan kualitas web dan aplikasi seluler Anda dengan mengujinya di berbagai browser desktop dan perangkat seluler nyata; tanpa harus menyediakan dan mengelola infrastruktur pengujian apa pun. Layanan ini memungkinkan Anda menjalankan pengujian secara bersamaan di beberapa browser desktop atau perangkat nyata untuk

mempercepat eksekusi rangkaian pengujian, serta menghasilkan video dan log untuk membantu Anda mengidentifikasi masalah dengan aplikasi dengan cepat.

Untuk mempelajari selengkapnya, lihat [AWS Device Farm](#).

AWS Device Farm di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke AWS Device Farm akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_devicefarm_role`

Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Device Farm di akun AMS saya?

Akses penuh ke AWS Device Farm layanan disediakan dengan pengecualian menggunakan namespace AMS di tag 'Nama'.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Device Farm

Tidak ada.

Gunakan SSP AMS untuk menyediakan AWS Elastic Disaster Recovery di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Elastic Disaster Recovery kapabilitas secara langsung di akun terkelola AMS Anda. AWS Elastic Disaster Recovery meminimalkan waktu henti dan kehilangan data dengan pemulihan aplikasi berbasis cloud dan lokal yang cepat dan andal menggunakan penyimpanan yang terjangkau, komputasi minimal, dan pemulihan. point-in-time Anda dapat meningkatkan ketahanan TI saat digunakan AWS Elastic Disaster Recovery untuk mereplikasi aplikasi lokal atau berbasis cloud yang berjalan pada sistem operasi yang didukung. Gunakan AWS Management Console untuk mengonfigurasi pengaturan replikasi dan peluncuran, memantau replikasi data, dan meluncurkan instance untuk latihan atau pemulihan.

Untuk mempelajari selengkapnya, lihat [AWS Elastic Disaster Recovery](#).

AWS Elastic Disaster Recovery di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke AWS Elastic Disaster Recovery akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_drs_console_role`

Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Elastic Disaster Recovery di akun AMS saya?

Tidak ada batasan untuk digunakan AWS Elastic Disaster Recovery di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Elastic Disaster Recovery

- Setelah Anda memiliki akses ke peran konsol, Anda harus menginisialisasi layanan Elastic Disaster Recovery untuk membuat peran IAM yang diperlukan dalam akun.
 - Anda harus mengirimkan tipe perubahan Manajemen | Aplikasi | Profil instans IAM | Buat (ulasan diperlukan) ubah jenis ct-0ixp4ch2tiu04 RFC untuk membuat tiruan dari profil instans dan melampirkan kebijakan. `customer-mc-ec2-instance-profile AWSElasticDisasterRecoveryEc2InstancePolicy` Anda harus menentukan mesin mana yang akan dilampirkan kebijakan baru.
 - Jika instance tidak menggunakan profil instance default, AMS dapat melampirkan `AWSElasticDisasterRecoveryEc2InstancePolicy` melalui otomatisasi.
- Anda harus menggunakan kunci KMS milik pelanggan untuk pemulihan lintas akun. Kunci KMS akun sumber harus diperbarui mengikuti kebijakan untuk mengizinkan akses akun target. Untuk informasi selengkapnya, lihat [Berbagi kunci enkripsi EBS dengan akun target](#).
- Kebijakan kunci KMS harus diperbarui untuk memungkinkan izin `customer_drs_console_role` melihat kebijakan jika Anda tidak ingin beralih peran ke tampilan.
- Untuk pemulihan bencana lintas akun dan lintas wilayah, AMS harus menyiapkan akun sumber dan target sebagai Akun Tepercaya dan menerapkan [Failback dan peran dalam ukuran yang tepat.AWS](#) AWS CloudFormation

Gunakan SSP AMS untuk menyediakan AWS Elemental MediaConvert di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Elemental MediaConvert kapabilitas secara langsung di akun terkelola AMS Anda. AWS Elemental MediaConvert adalah layanan transcoding video berbasis file dengan fitur tingkat siaran. Ini

memungkinkan Anda untuk membuat konten video-on-demand (VOD) untuk siaran dan pengiriman multilayar dalam skala besar. Layanan ini menggabungkan kemampuan video dan audio canggih dengan antarmuka dan pay-as-you-go harga layanan web yang sederhana. Dengan AWS Elemental MediaConvert, Anda dapat fokus pada memberikan pengalaman media yang menarik tanpa harus khawatir tentang kompleksitas membangun dan mengoperasikan infrastruktur pemrosesan video Anda sendiri.

Untuk mempelajari selengkapnya, lihat [AWS Elemental MediaConvert](#).

MediaConvert di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke MediaConvert akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_mediaconvert_author_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

Peran kedua akan disediakan, `customer_MediaConvert_Default_Role`, yang digunakan oleh MediaConvert untuk membaca dari bucket S3 sumber dan menulis output ke bucket S3 tujuan, dan juga untuk memanggil gateway API jika Anda memerlukan manajemen hak digital (DRM).

T: Apa batasan penggunaan MediaConvert di akun AMS saya?

Tidak ada batasan untuk penggunaan MediaConvert di AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? MediaConvert

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. MediaConvert

Gunakan SSP AMS untuk menyediakan AWS Elemental MediaLive di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Elemental MediaLive kapabilitas secara langsung di akun terkelola AMS Anda. AWS Elemental MediaLive adalah layanan pemrosesan video langsung tingkat siaran. Ini memungkinkan Anda untuk membuat aliran video berkualitas tinggi untuk pengiriman ke televisi siaran dan perangkat multilayar yang terhubung ke internet, seperti terhubung, tablet, smartphone, dan TVs set-top box. Layanan ini bekerja dengan menyandikan streaming video langsung Anda secara real-time, mengambil sumber video langsung berukuran lebih besar dan mengompresnya menjadi versi yang lebih kecil untuk didistribusikan ke pemirsa Anda. Dengan AWS Elemental MediaLive, Anda dapat dengan mudah mengatur streaming

untuk acara langsung dan saluran 24x7 dengan fitur penyiaran lanjutan, ketersediaan tinggi, dan harga. pay-as-you-go AWS Elemental MediaLive memungkinkan Anda fokus untuk menciptakan pengalaman video langsung yang menarik bagi pemirsa Anda tanpa kerumitan membangun dan mengoperasikan infrastruktur pemrosesan video tingkat siaran.

Untuk mempelajari selengkapnya, lihat [AWS Elemental MediaLive](#).

MediaLive di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke MediaLive akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_medialive_author_role`

Sebagai bagian dari RFC ini, peran kedua diterapkan ke akun Anda; `customer_medialive_service_role` peran, peran ini dapat ditetapkan ke saluran dan input Media Live Anda untuk berinteraksi dengan layanan lain seperti Amazon S3, dan Log. MediaStore CloudWatch

Setelah peran disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan MediaLive di akun AMS saya?

Tidak ada batasan untuk penggunaan MediaLive di AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? MediaLive

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. MediaLive

Gunakan SSP AMS untuk menyediakan AWS Elemental MediaPackage di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Elemental MediaPackage kapabilitas secara langsung di akun terkelola AMS Anda. AWS Elemental MediaPackage andal mempersiapkan dan melindungi video Anda untuk pengiriman melalui internet. Dari satu input video, AWS Elemental MediaPackage buat aliran video yang diformat untuk diputar di ponsel TVs, komputer, tablet, dan konsol game yang terhubung. Ini membuatnya mudah untuk menerapkan fitur video populer untuk pemirsa (start-over, pause, rewind, dan sebagainya.), Seperti yang biasa ditemukan di. DVRs AWS Elemental MediaPackage juga dapat melindungi konten Anda menggunakan Digital Rights Management (DRM). AWS Elemental MediaPackage skala secara

otomatis sebagai respons terhadap pemuatan, sehingga pemirsa Anda akan selalu mendapatkan pengalaman hebat tanpa Anda harus memprediksi secara akurat terlebih dahulu kapasitas yang Anda perlukan.

Untuk mempelajari selengkapnya, lihat [AWS Elemental MediaPackage](#).

MediaPackage di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke AWS Elemental MediaPackage akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_mediapackage_author_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

Peran kedua akan diberikan `customer_mediapackage_service_role`, yang dapat ditetapkan ke saluran Media Live Anda dan input untuk berinteraksi dengan layanan lain seperti S3 dan Secrets Manager.

T: Apa batasan penggunaan MediaPackage di akun AMS saya?

Tidak ada batasan untuk penggunaan MediaPackage di AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? MediaPackage

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. MediaPackage

Gunakan SSP AMS untuk menyediakan AWS Elemental MediaStore di akun AMS Anda

Note

Setelah pertimbangan cermat, AWS telah membuat keputusan untuk berhenti MediaStore, efektif 13 November 2025. Jika Anda adalah pelanggan aktif MediaStore, Anda dapat menggunakan MediaStore seperti biasa hingga 13 November 2025, ketika dukungan untuk layanan akan berakhir. Setelah tanggal ini, Anda tidak akan lagi dapat menggunakan MediaStore atau kemampuan apa pun yang disediakan oleh layanan ini.

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Elemental MediaStore kapabilitas secara langsung di akun terkelola AMS Anda. AWS Elemental MediaStore adalah layanan

AWS penyimpanan yang dioptimalkan untuk media. Ini memberi Anda kinerja, konsistensi, dan latensi rendah yang diperlukan untuk mengirimkan konten video streaming langsung. AWS Elemental MediaStore bertindak sebagai toko asal dalam alur kerja video Anda. Kemampuan kinerjanya yang tinggi memenuhi kebutuhan beban kerja pengiriman media yang paling menuntut, dikombinasikan dengan penyimpanan jangka panjang yang hemat biaya. Untuk mempelajari selengkapnya, lihat [AWS Elemental MediaStore](#).

MediaStore di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke MediaStore akun AMS saya?

Meminta akses MediaStore dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_mediastore_author_role` Sebagai bagian dari RFC ini, peran kedua diterapkan ke akun Anda; `MediaStoreAccessLogs` peran, yang digunakan oleh MediaStore layanan untuk log aktivitas CloudWatch, jika Anda memilih untuk mengaktifkan fitur tersebut. Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

Pada saat ini, Operasi AMS juga akan menerapkan peran layanan ini di akun Anda:

`aws_code_pipeline_service_role_policy`

T: Apa batasan penggunaan MediaStore di akun AMS saya?

Tidak ada batasan untuk penggunaan MediaStore di AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? MediaStore

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. MediaStore

Gunakan SSP AMS untuk menyediakan AWS Elemental MediaTailor di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Elemental MediaTailor kapabilitas secara langsung di akun terkelola AMS Anda. AWS Elemental MediaTailor memungkinkan penyedia video memasukkan iklan yang ditargetkan secara individual ke dalam aliran video mereka tanpa mengorbankan tingkat siaran. `quality-of-service` Dengan AWS Elemental MediaTailor, pemirsa video langsung atau sesuai permintaan Anda masing-masing menerima streaming yang menggabungkan konten Anda dengan iklan yang dipersonalisasi untuk mereka. Tetapi tidak seperti solusi iklan yang dipersonalisasi lainnya, dengan seluruh streaming AWS

Elemental MediaTailor Anda — video dan iklan — disampaikan dengan kualitas video tingkat siaran untuk meningkatkan pengalaman bagi pemirsa Anda. AWS Elemental MediaTailor memberikan pelaporan otomatis berdasarkan metrik pengiriman iklan sisi klien dan server, untuk mengukur tayangan iklan dan perilaku pemirsa secara akurat. Anda dapat dengan mudah memonetisasi acara menonton permintaan tinggi yang tidak terduga tanpa menggunakan biaya di muka. AWS Elemental MediaTailor Ini juga meningkatkan tingkat pengiriman iklan, membantu Anda menghasilkan lebih banyak uang dari setiap video, dan bekerja dengan berbagai jaringan pengiriman konten, server keputusan iklan, dan perangkat klien yang lebih luas.

Untuk mempelajari selengkapnya, lihat [AWS Elemental MediaTailor](#).

MediaTailor di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke MediaTailor akun AMS saya?

Meminta akses MediaTailor dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer-mediatailor-role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan MediaTailor di akun AMS saya?

Tidak ada batasan untuk penggunaan MediaTailor di AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? MediaTailor

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. MediaTailor

Gunakan SSP AMS untuk menyediakan AWS Global Accelerator di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Global Accelerator secara langsung di akun terkelola AMS Anda. Global Accelerator adalah layanan lapisan jaringan di mana Anda membuat akselerator untuk meningkatkan ketersediaan dan kinerja untuk aplikasi internet yang digunakan oleh khalayak global. Untuk mempelajari lebih lanjut, lihat [Akselerator Global](#).

FAQ Akselerator Global di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta Global Accelerator untuk disiapkan di akun AMS saya?

Meminta akses melalui pengajuan AWS Layanan RFC (Manajemen | layanan | AWS Layanan Penyediaan Mandiri). Melalui RFC ini, peran IAM berikut akan disediakan di akun Anda:

`customer_global_accelerator_console_role` Setelah disediakan di akun Anda, Anda harus mengaktifkan peran konsol dalam solusi federasi Anda.

T: Apa batasan penggunaan Global Accelerator di akun AMS saya?

Global Accelerator adalah layanan global yang mendukung titik akhir di beberapa AWS Wilayah, yang tercantum dalam Tabel [AWS Wilayah](#).

T: Apa prasyarat atau dependensi untuk menggunakan Global Accelerator di akun AMS saya?

Saat Anda mengatur akselerator dengan Global Accelerator, Anda mengaitkan alamat IP statis ke titik akhir regional di satu atau beberapa Wilayah. AWS Untuk akselerator standar, titik akhir adalah Network Load Balancer, Application Load Balancer, EC2 instans Amazon, atau alamat IP Elastis. Untuk akselerator perutean khusus, titik akhir adalah subnet virtual private cloud (VPC) dengan satu atau beberapa instance. EC2

Gunakan SSP AMS untuk menyediakan AWS Glue di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Glue kapabilitas secara langsung di akun terkelola AMS Anda. AWS Glue adalah layanan ekstrak, transformasi, dan pemuatan (ETL) yang dikelola sepenuhnya yang membantu Anda mempersiapkan dan memuat data Anda untuk analitik. Anda dapat membuat dan menjalankan pekerjaan ETL dengan beberapa klik di file. AWS Management Console Anda menunjuk AWS Glue ke data yang disimpan AWS, dan AWS Glue menemukan data Anda serta menyimpan metadata terkait (misalnya definisi tabel dan skema) di. AWS Glue Data Catalog Setelah dikatalogkan, data Anda segera dapat dicari, dapat ditanyakan, dan tersedia untuk tindakan ETL. Untuk mempelajari selengkapnya, lihat [AWS Glue](#).

AWS Glue di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara saya meminta AWS Glue untuk disiapkan di akun AMS saya?

Meminta akses AWS Glue dengan mengirimkan RFC dengan Manajemen | Layanan AWS | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:

- `customer_glue_console_role`
- `customer_glue_service_role`

Peran sebelumnya mencakup kebijakan terlampir berikut:

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

Setelah peran disediakan di akun Anda, Anda harus memasukkannya ke dalam solusi federasi Anda.

Untuk akses ke titik akhir Crawler, Jobs, dan Development (peran yang diperlukan untuk kasus penggunaan tertentu), kirimkan RFC dengan Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat entitas atau kebijakan (ct-3dpd8mdd9jn1r).

T: Apa batasan penggunaan AWS Glue di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh AWS Glue tersedia di akun AMS Anda. Untuk lingkungan interaktif tempat Anda dapat membuat dan menguji skrip ETL, gunakan Notebook di Studio. AWS Glue AWS Glue Sesi Interaktif dan Notebook Job adalah fitur tanpa server AWS Glue yang dapat Anda gunakan AWS Glue dan yang memanfaatkan peran layanan. AWS Glue

AWS Glue sebelum 2.0: AWS Glue Notebook adalah sumber daya yang tidak dikelola yang meluncurkan instans EC2 Amazon di akun. Ini adalah praktik terbaik untuk meluncurkan EC2 instans Amazon Anda sendiri dan menginstal perangkat lunak yang diperlukan untuk mendukung lingkungan dan pengembangan notebook. [Untuk informasi lebih lanjut, lihat Tutorial: Mengatur Notebook Apache Zeppelin Lokal untuk Menguji dan Mendebug Skrip ETL dan Menggunakan Titik Akhir Pengembangan untuk Mengembangkan Skrip.](#)

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Glue

AWS Glue memiliki ketergantungan pada Amazon S3 CloudWatch,, CloudWatch dan Log. Dependensi transitif bervariasi berdasarkan sumber data, dan fitur AWS Glue layanan lainnya mungkin berinteraksi dengannya (contoh: Amazon Redshift, Amazon RDS, Athena).

Gunakan SSP AMS untuk menyediakan AWS Lake Formation di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Lake Formation kapabilitas secara langsung di akun terkelola AMS Anda. AWS Lake Formation adalah layanan

yang membuatnya mudah untuk mengatur danau data yang aman dalam beberapa hari. Sebuah danau data adalah repositori terpusat, dikurasi, dan aman yang menyimpan semua data Anda, baik dalam bentuk aslinya dan yang disiapkan untuk analisis. Danau data memungkinkan Anda untuk menguraikan silo data dan menggabungkan berbagai jenis analitik untuk mendapatkan wawasan dan memandu keputusan bisnis yang lebih baik.

Membuat danau data dengan Lake Formation sesederhana mendefinisikan sumber data serta kebijakan akses dan keamanan data apa yang ingin Anda terapkan. Lake Formation kemudian membantu Anda mengumpulkan dan membuat katalog data dari database dan penyimpanan objek, memindahkan data ke danau data Amazon S3 baru Anda, membersihkan dan mengklasifikasikan data Anda menggunakan algoritma machine learning, dan mengamankan akses ke data sensitif Anda. Pengguna Anda dapat mengakses katalog data terpusat (untuk detailnya, lihat [AWS Glue FAQ](#)) yang menjelaskan kumpulan data yang tersedia dan penggunaannya yang sesuai. Pengguna Anda kemudian memanfaatkan kumpulan data ini dengan pilihan layanan analisis dan pembelajaran mesin mereka, seperti [Amazon Redshift](#), [Amazon Athena](#), dan (dalam versi beta) [Amazon EMR](#) untuk Apache Spark. Lake Formation dibangun di atas kemampuan yang tersedia di [AWS Glue](#).

Untuk mempelajari selengkapnya, lihat [AWS Lake Formation](#).

FAQ Lake Formation di AWS Managed Services

T: Bagaimana cara meminta akses ke AWS Lake Formation akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_lakeformation_data_analyst_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

Selain itu, dua peran berikut adalah opsional:

- `customer_lakeformation_admin_role`
- `customer_lakeformation_workflow_role`

Untuk izin admin, Anda dapat memilih untuk onboard peran `customer_lakeformation_admin_role` sebagai bagian dari jenis perubahan SSPS yang sama (ct-3qe6io8t6jtny).

Jika Anda ingin membuat Cetak Biru di AWS Lake Formation Konsol, Anda harus mengirimkan Manajemen | Lainnya | RFC lainnya (ct-1e1xtak34nx76) untuk menyebarkan.

`customer_lakeformation_workflow_role` Di RFC, Anda harus memberikan nama bucket S3 jika bucket adalah sumber saat Blueprints dibuat. Bucket S3 berlaku jika tipe Blueprint adalah, Classic Load Balancer Load AWS CloudTrail Balancer atau Application Load Balancer Load Balancer.

T: Apa batasan penggunaan AWS Lake Formation di akun AMS saya?

Fungsionalitas penuh dari Lake Formation tersedia di AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Lake Formation

Lake Formation terintegrasi dengan AWS Glue layanan, oleh karena itu AWS Glue pengguna hanya dapat mengakses database dan tabel di mana mereka memiliki izin Lake Formation. Selain itu, pengguna AWS Athena dan Amazon Redshift hanya dapat menanyakan database dan tabel AWS Glue tempat mereka memiliki izin Lake Formation.

Gunakan SSP AMS untuk menyediakan AWS Lambda di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Lambda kapabilitas secara langsung di akun terkelola AMS Anda. AWS Lambda memungkinkan Anda menjalankan kode tanpa menyediakan atau mengelola server. Anda hanya membayar untuk waktu komputasi yang Anda konsumsi, tidak ada biaya ketika kode Anda tidak berjalan. Dengan Lambda, Anda dapat menjalankan kode untuk hampir semua jenis aplikasi atau layanan back-end, semuanya tanpa administrasi. Unggah kode Anda dan Lambda menangani semua yang diperlukan untuk menjalankan dan menskalakan kode Anda dengan ketersediaan tinggi. Anda dapat mengatur kode Anda untuk secara otomatis memicu dari AWS layanan lain, atau memanggilnya langsung dari Web atau aplikasi seluler apa pun. Untuk mempelajari selengkapnya, lihat [AWS Lambda](#).

Lambda di AWS Managed Services FAQ

T: Bagaimana cara meminta akses ke AWS Lambda akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_lambda_admin_role` dan `customer_lambda_basic_execution_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Lambda di akun AMS saya?

- Fungsi Lambda dirancang untuk dipanggil oleh sumber peristiwa. Untuk daftar layanan yang dapat digunakan sebagai sumber peristiwa Lambda, lihat [Menggunakan AWS Lambda dengan Layanan Lain](#). Tidak semua layanan ini saat ini tersedia di akun AMS. Jika Anda memerlukan layanan yang tidak tersedia, kerjakan dengan AMS CSDM Anda untuk mengajukan pengecualian.
- [Secara default AMS memberi Anda peran inisiasi Lambda dasar yang berisi izin AWSLambdaBasicExecutionRole dan AWSXrayWriteOnlyAccess izin; untuk selengkapnya, lihat Peran Inisiasi.AWS Lambda](#) Jika Anda memerlukan izin tambahan, seperti kemampuan untuk menyediakan fungsi Lambda dalam VPC AMS Anda, kirimkan RFC ke Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) tipe perubahan.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Lambda

Tidak ada prasyarat atau dependensi untuk memulai AWS Lambda; Namun, tergantung pada kasus penggunaan spesifik Anda, Anda mungkin memerlukan akses ke AWS layanan lain untuk membuat sumber peristiwa, atau izin tambahan untuk fungsi Anda untuk melakukan berbagai tindakan. Jika izin tambahan diperlukan, kirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (perlu ditinjau) jenis perubahan (ct-3qe6io8t6jtny).

T: Apa yang harus saya lakukan untuk menjalankan fungsi Lambda di salah satu akun saya?

Untuk menerapkan fungsi Lambda di akun inti, gunakan pedoman berikut:

- Pastikan SSPS untuk AWS Lambda onboard.
- Tidak ada batasan khusus yang melarang penerapan ini di bawah tanggung jawab AMS, selama sumber daya AMS Anda dilindungi dan sesuai.
- Jika Anda ingin AMS membuat fungsi Lambda, maka Anda harus terlebih dahulu menggunakan peran SSPS yang disediakan. AWS Lambda Kemudian, jika Anda masih menginginkan bantuan AMS untuk menyebarkan atau mendukung fungsi tersebut, hubungi CA Anda dan mulai proses di luar cakupan (OOS).

Gunakan SSP AMS untuk menyediakan AWS License Manager di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS License Manager kapabilitas secara langsung di akun terkelola AMS Anda. AWS License Manager terintegrasi dengan AWS layanan untuk menyederhanakan pengelolaan lisensi di beberapa AWS akun, katalog TI, dan lokal, melalui satu akun. AWS AWS License Manager memungkinkan administrator membuat aturan

lisensi khusus yang meniru persyaratan perjanjian lisensi mereka, dan kemudian memberlakukan aturan ini ketika instance Amazon diluncurkan. EC2 Aturan AWS License Manager memungkinkan Anda membatasi pelanggaran lisensi dengan menghentikan peluncuran instans secara fisik atau dengan memberi tahu administrator tentang pelanggaran tersebut. Untuk mempelajari selengkapnya, lihat [AWS License Manager](#).

License Manager di AWS Managed Services FAQ

Pertanyaan dan jawaban umum:

T: Bagaimana cara saya meminta AWS License Manager untuk disiapkan di akun AMS saya?

Minta akses ke AWS License Manager dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_license_manager_role` Setelah peran IAM License Manager disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS License Manager di akun AMS saya?

Anda dapat mengaitkan AWS License Manager aturan dengan aturan yang AMIs Anda miliki (difilter di bawah “Dimiliki oleh saya”). Jika Anda memilih untuk menerapkan asosiasi batas ke AMI (contoh: hanya dapat mendukung 100 vCPU dari AMI ini) dan menghabiskan batasnya, peluncuran future dengan AMI tersebut diblokir dan mengembalikan kesalahan yang menyatakan “Tidak ada lisensi yang tersedia.” Ini adalah perilaku yang dimaksudkan dari layanan ini (tidak mengizinkan kelelahan lisensi). Jika Anda kehabisan batas tetapi perlu meluncurkan AMI lagi, Anda harus mengubah aturan yang dikonfigurasi AWS License Manager.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS License Manager

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS License Manager

Gunakan SSP AMS untuk menyediakan AWS Migration Hub di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Migration Hub kapabilitas secara langsung di akun terkelola AMS Anda. AWS Migration Hub menyediakan satu lokasi di mana Anda dapat melacak kemajuan migrasi aplikasi di beberapa solusi AWS dan mitra. Menggunakan Migration Hub memungkinkan Anda memilih alat migrasi AWS dan mitra yang paling sesuai dengan kebutuhan Anda, sekaligus memberikan visibilitas ke status migrasi di seluruh

portofolio aplikasi Anda. Migration Hub juga menyediakan metrik dan kemajuan utama untuk aplikasi individual, terlepas dari alat mana yang digunakan untuk memigrasikannya. Ini memungkinkan Anda untuk dengan cepat mendapatkan pembaruan kemajuan di semua migrasi Anda, dengan mudah mengidentifikasi dan memecahkan masalah apa pun, dan mengurangi keseluruhan waktu dan upaya yang dihabiskan untuk proyek migrasi Anda. Untuk mempelajari selengkapnya, lihat [AWS Migration Hub](#).

FAQ Migration Hub di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Migration Hub di akun AMS saya?

Minta akses ke Migration Hub dengan mengirimkan RFC dengan Management | AWS service | Self-provisioned service | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_migrationhub_author_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk Migration Hub?

Tidak ada.

T: Apa prasyarat untuk mengaktifkan Migration Hub?

Tidak ada prasyarat untuk mulai menggunakan Migration Hub di akun AMS Anda. Namun, izin di luar Migration Hub mungkin diperlukan selama pengelolaan layanan, seperti menulis izin ke Amazon S3 untuk mengunggah informasi server.

Gunakan SSP AMS untuk menyediakan AWS Outposts di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Outposts kapabilitas secara langsung di akun terkelola AMS Anda. AWS Outposts adalah layanan yang dikelola sepenuhnya yang memperluas AWS infrastruktur, AWS layanan APIs, dan alat ke hampir semua pusat data, ruang co-lokasi, atau fasilitas lokal untuk pengalaman hybrid yang konsisten. AWS Outposts baik untuk beban kerja yang memerlukan akses latensi rendah ke sistem lokal, pemrosesan data lokal, atau penyimpanan data lokal. Untuk mempelajari selengkapnya, lihat [AWS Outposts](#).

AWS Outposts di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara saya meminta AWS Outposts untuk disiapkan di akun AMS saya?

Minta akses ke AWS Outposts dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_outposts_role` Setelah peran disediakan di akun Anda, Anda harus memasukkannya ke dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Outposts di akun AMS saya?

Tidak ada batasan untuk penggunaan AWS Outposts di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Outposts

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS Outposts

Gunakan SSP AMS untuk menyediakan AWS Resilience Hub di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Resilience Hub kapabilitas secara langsung di akun dikelola AMS Anda. AWS Resilience Hub membantu Anda secara proaktif mempersiapkan dan melindungi AWS aplikasi Anda dari gangguan. Resilience Hub menawarkan penilaian dan validasi ketahanan yang terintegrasi ke dalam siklus hidup pengembangan perangkat lunak Anda untuk mengungkap kelemahan ketahanan. Resilience Hub membantu Anda memperkirakan apakah aplikasi Anda dapat memenuhi target tujuan waktu pemulihan (RTO) dan tujuan titik pemulihan (RPO) atau tidak, dan membantu menyelesaikan masalah sebelum dirilis ke produksi. Setelah menerapkan AWS aplikasi ke dalam produksi, Anda dapat menggunakan Resilience Hub untuk terus melacak postur ketahanan aplikasi Anda. Jika terjadi pemadaman, Resilience Hub mengirimkan pemberitahuan ke operator untuk meluncurkan proses pemulihan terkait.

AWS Resilience Hub di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Resilience Hub akun AMS saya?

Minta akses ke Resilience Hub dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran dan kebijakan IAM berikut ke akun Anda:

IAM role

- `customer_resiliencehub_console_role`
- `customer_resiliencehub_service_role`

Kebijakan

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

Setelah peran disediakan di akun Anda, Anda harus memasukkan peran tersebut `customer_resiliencehub_console_role` dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Resilience Hub di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Resilience Hub tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Resilience Hub

Tidak ada prasyarat atau dependensi untuk menggunakan Resilience Hub di akun AMS Anda.

Gunakan SSP AMS untuk menyediakan AWS Secrets Manager di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Secrets Manager kapabilitas secara langsung di akun terkelola AMS Anda. AWS Secrets Manager membantu Anda melindungi rahasia yang diperlukan untuk mengakses aplikasi, layanan, dan sumber daya TI Anda. Layanan ini memungkinkan Anda untuk dengan mudah memutar, mengelola, dan mengambil kredensial database, kunci API, dan rahasia lainnya sepanjang siklus hidupnya. Pengguna dan aplikasi mengambil rahasia dengan panggilan ke Secrets Manager APIs, menghilangkan kebutuhan untuk hardcode informasi sensitif dalam teks biasa. Secrets Manager menawarkan rotasi rahasia dengan integrasi bawaan untuk Amazon RDS, Amazon Redshift, dan Amazon DocumentDB. Selain itu, layanan ini dapat diperluas ke jenis rahasia lainnya, termasuk kunci API dan OAuth token. Untuk mempelajari selengkapnya, lihat [AWS Secrets Manager](#).

Note

Secara default, operator AMS dapat mengakses rahasia AWS Secrets Manager yang dienkripsi menggunakan AWS KMS kunci default akun (CMK). Jika Anda ingin rahasia Anda

tidak dapat diakses oleh Operasi AMS, gunakan CMK kustom, dengan kebijakan kunci AWS Key Management Service (AWS KMS) yang menentukan izin yang sesuai dengan data yang disimpan dalam rahasia.

FAQ Secrets Manager di AWS Managed Services

T: Bagaimana cara meminta akses ke AWS Secrets Manager akun AMS saya?

Minta akses ke Secrets Manager dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-3qe6io8t6jtny) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_secrets_manager_console_role` dan `customer-rotate-secrets-lambda-role`. `customer_secrets_manager_console_role` ini digunakan sebagai peran Admin untuk menyediakan dan mengelola rahasia, dan `customer-rotate-secrets-lambda-role` digunakan sebagai peran eksekusi Lambda untuk fungsi Lambda yang memutar rahasia. Setelah disediakan di akun Anda, Anda harus memasukkan `customer_secrets_manager_console_role` peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Secrets Manager di akun AMS saya?

Fungsionalitas penuh AWS Secrets Manager tersedia di akun AMS Anda, bersama dengan fungsi rotasi otomatis rahasia. Namun, perhatikan bahwa mengatur rotasi Anda menggunakan 'Buat fungsi Lambda baru untuk melakukan rotasi' tidak didukung karena memerlukan izin yang lebih tinggi untuk membuat AWS CloudFormation tumpukan (Peran IAM dan pembuatan fungsi Lambda), yang melewati proses Manajemen Perubahan. AMS Advanced hanya mendukung 'Gunakan fungsi Lambda yang ada untuk melakukan rotasi' di mana Anda mengelola fungsi Lambda untuk memutar rahasia menggunakan peran Admin Lambda SSPS. AWS AMS Advanced tidak membuat atau mengelola Lambda untuk memutar rahasia.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Secrets Manager

Ruang nama berikut dicadangkan untuk digunakan oleh AMS dan tidak tersedia sebagai bagian dari akses langsung ke: AWS Secrets Manager

- `arn:aws:secretsmanager: *: *:rahasia:ams-shared/*`
- `arn:aws:secretsmanager: *: *:rahasia:dibagikan pelanggan/*`
- `arn:aws:secretsmanager: *: *:rahasia:ams/*`

Berbagi kunci menggunakan Secrets Manager (AMS SSPS)

Berbagi rahasia dengan AMS dalam teks biasa RFC, permintaan layanan, atau laporan insiden, menghasilkan insiden pengungkapan informasi dan AMS menyunting informasi tersebut dari kasus dan meminta Anda membuat ulang kunci.

Anda dapat menggunakan [AWS Secrets Manager](#) (Secrets Manager) di bawah namespace ini, `customer-shared`

Berbagi Kunci menggunakan Secrets Manager FAQ

T: Jenis rahasia apa yang harus dibagikan menggunakan Secrets Manager?

Beberapa contoh adalah kunci yang telah dibagikan sebelumnya untuk pembuatan VPN, kunci rahasia seperti kunci Otentikasi (IAM, SSH), kunci Lisensi, dan Kata Sandi.

T: Bagaimana cara berbagi kunci dengan AMS menggunakan Secrets Manager?

1. Masuk ke konsol AWS Manajemen menggunakan akses federasi Anda dan peran yang sesuai: untuk SALZ, `Customer_ReadOnly_Role` untuk MALZ, `AWSSecretsManagerChangeManagementRole`.
2. Arahkan ke [AWS Secrets Manager konsol](#) dan klik Simpan rahasia baru.
3. Pilih Tipe rahasia lainnya.
4. Masukkan nilai rahasia sebagai teks biasa dan gunakan enkripsi KMS default. Klik Berikutnya.
5. Masukkan nama rahasia dan deskripsi, nama selalu dimulai dengan `customer-shared/`. Misalnya yang dibagikan pelanggan/`mykey2022`. Klik Berikutnya.
6. Biarkan rotasi otomatis dinonaktifkan, Klik Berikutnya.
7. Tinjau dan klik Store untuk menyimpan rahasia.
8. Balas kepada kami dengan nama rahasia melalui permintaan Layanan, RFC, atau laporan insiden, sehingga kami dapat mengidentifikasi dan mengambil rahasia tersebut.

T: Izin apa yang diperlukan untuk berbagi kunci menggunakan Secrets Manager?

SALZ: Cari kebijakan IAM `customer_secrets_manager_shared_policy` terkelola dan verifikasi bahwa dokumen kebijakan sama dengan yang dilampirkan dalam langkah-langkah

pembuatan di bawah ini. Konfirmasikan bahwa kebijakan tersebut dilampirkan pada Peran IAM berikut: `Customer_ReadOnly_Role`.

MALZ: Validasi bahwa `AMSSecretsManagerSharedPolicy`, dilampirkan ke `AWSManagedServicesChangeManagementRole` peran yang memungkinkan Anda `GetSecretValue` melakukan tindakan di namespace. `ams-shared`

Contoh:

```
{
  "Action": "secretsmanager:*",
  "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  ],
  "Effect": "Allow",
  "Sid": "AllowAccessToSharedNameSpaces"
}
```

Note

Izin yang diperlukan diberikan saat Anda menambahkan AWS Secrets Manager sebagai layanan yang disediakan layanan mandiri.

Gunakan SSP AMS untuk menyediakan AWS Security Hub di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Security Hub kapabilitas secara langsung di akun terkelola AMS Anda. AWS Security Hub memberi Anda pandangan komprehensif tentang keadaan keamanan Anda di dalam AWS dan kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub memusatkan dan memprioritaskan temuan keamanan dan kepatuhan dari seluruh AWS akun, layanan, dan mitra pihak ketiga yang didukung untuk membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi. Untuk mempelajari selengkapnya, lihat [AWS Security Hub](#).

FAQ Security Hub di AWS Managed Services

T: Bagaimana cara meminta akses ke AWS Security Hub akun AMS saya?

Meminta akses ke Security Hub dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_securityhub_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Security Hub di akun AMS saya?

Fungsionalitas pengarsipan telah dicatat sebagai potensi keamanan dan risiko operasional dan telah dibatasi sebagai bagian dari peran Keamanan layanan yang disediakan sendiri.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Security Hub

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS Security Hub

Gunakan SSP AMS untuk menyediakan AWS Service Catalog AppRegistry di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AppRegistry kapabilitas secara langsung di akun terkelola AMS Anda. AppRegistry memungkinkan pencarian aplikasi, pelaporan, dan tindakan manajemen dari lokasi pusat. Pembangun jarang membuat aplikasi dalam satu AWS akun. Mereka biasanya memisahkan sumber daya aplikasi berdasarkan fase siklus hidup, seperti pengembangan, pengujian, dan produksi. AppRegistry memungkinkan Anda untuk mengelompokkan dan melihat semua koleksi sumber daya Anda di seluruh AWS akun yang Anda tentukan.

Dengan AppRegistry, Anda dapat menyimpan AWS aplikasi Anda, kumpulan sumber daya yang terkait dengan aplikasi Anda, dan grup atribut aplikasi. Untuk mempelajari lebih lanjut, lihat [Apa itu AppRegistry](#).

FAQ: AWS Service Catalog AppRegistry di AMS

T: Bagaimana cara meminta akses ke AWS Service Catalog AppRegistry akun AMS saya?

Minta akses ke AppRegistry dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer-appregistry-console-role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Service Catalog AppRegistry di akun AMS saya?

Akses penuh ke AppRegistry layanan disediakan dengan pengecualian menggunakan namespace AMS di 'Name' tag.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Service Catalog AppRegistry

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AppRegistry

Gunakan SSP AMS untuk menyediakan AWS Shield Advanced di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Shield Advanced kapabilitas secara langsung di akun terkelola AMS Anda. AWS Shield Advanced adalah layanan perlindungan Distributed Denial of Service (DDoS) terkelola yang melindungi aplikasi yang berjalan. AWS Shield Advanced menyediakan deteksi selalu aktif dan mitigasi inline otomatis yang meminimalkan waktu henti dan latensi aplikasi, sehingga tidak perlu menggunakan Support untuk mendapatkan manfaat dari perlindungan S. AWS DDo Ada dua tingkatan AWS Shield - Standard dan Advanced; AMS menawarkan Shield Advanced. Untuk mempelajari selengkapnya, lihat [Shield Advanced](#).

Semua AWS pelanggan mendapat manfaat dari perlindungan otomatis AWS Shield Standard, tanpa biaya tambahan. AWS Shield Standard bertahan terhadap serangan lapisan DDo S jaringan dan transportasi yang paling umum, sering terjadi, yang menargetkan situs web atau aplikasi Anda. Saat Anda menggunakan AWS Shield Standard Amazon CloudFront dan Amazon Route 53, Anda menerima perlindungan ketersediaan komprehensif terhadap semua serangan infrastruktur yang diketahui (Layer 3 dan 4).

Untuk tingkat perlindungan yang lebih tinggi terhadap serangan yang menargetkan aplikasi Anda yang berjalan di Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), CloudFront Amazon, dan AWS Global Accelerator Amazon Route 53 resource, Anda dapat berlangganan. AWS Shield Advanced

Selain perlindungan lapisan jaringan dan transport yang disertakan AWS Shield Standard, AWS Shield Advanced menyediakan deteksi dan mitigasi tambahan terhadap serangan DDo S yang besar dan canggih, visibilitas mendekati real-time ke dalam serangan, dan integrasi dengan AWS WAF, firewall aplikasi web. AWS Shield Advanced juga memberi Anda akses 24x7 ke Tim AWS Shield Response (SRT) dan perlindungan terhadap lonjakan terkait DDo S di Amazon Elastic Compute Cloud (Amazon), EC2 Elastic Load Balancing (Elastic Load Balancing), Amazon, CloudFront dan Amazon Route 53. AWS Global Accelerator

Pertanyaan Umum tentang Shield Advanced di AWS Managed Services

T: Bagaimana cara meminta akses ke Shield Advanced di akun AMS saya?

Minta akses ke Shield Advanced dengan mengirimkan RFC dengan Management | AWS service | Self-provisioned service | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_shield_role` dan `aws_drt_shield_role`. Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

Setelah peran diterapkan ke akun Anda, Anda dapat menggunakan `customer_shield_role` untuk mengonfirmasi langganan Anda AWS Shield Advanced di akun Anda.

Note

Perhatikan bahwa ada biaya bulanan dan komitmen satu tahun yang terkait dengan penggunaan. AWS Shield Advanced Selain itu, menggunakan AWS Shield Advanced AMS memberi wewenang kepada AMS untuk meningkatkan ke AWS Shield (SRT), yang dapat membuat perubahan pada aturan firewall (AWS WAF) aplikasi web Anda selama insiden penolakan layanan terdistribusi yang meningkat. DDoS Perubahan ini akan dilakukan dalam koordinasi dengan AMS.

T: Apa batasan penggunaan Shield Advanced di akun AMS saya?

Meskipun bukan pembatasan, Anda harus memahami bahwa menggunakan Shield Advanced menyebarkan `aws_drt_shield_role`, yang memungkinkan AWS Shield tim (SRT) untuk membuat perubahan darurat pada AWS WAF aturan di dalam akun AMS selama insiden S meningkat DDoS. Ini direkomendasikan oleh AMS untuk remediasi tercepat serangan DDoS, dan akan terjadi setelah eskalasi AMS ke SRT.

T: Apa prasyarat atau dependensi untuk menggunakan Shield Advanced di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Shield Advanced di akun AMS Anda.

Gunakan SSP AMS untuk menyediakan AWS Snowball Edge di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Snowball Edge secara langsung di akun terkelola AMS Anda. Snowball Edge adalah solusi transportasi

data skala petabyte yang menggunakan perangkat yang dirancang agar aman, untuk mentransfer sejumlah besar data ke dalam dan keluar dari Cloud. AWS Snowball Edge mengatasi tantangan umum dengan transfer data skala besar termasuk biaya jaringan yang tinggi, waktu transfer yang lama, dan masalah keamanan. Anda dapat menggunakan Snowball Edge untuk memigrasikan data analitik, data genomik, pustaka video, repositori gambar, cadangan, dan untuk mengarsipkan bagian dari shutdown pusat data, penggantian tape, atau proyek migrasi aplikasi. Mentransfer data dengan Snowball Edge sederhana, cepat, lebih aman, dan hanya seperlima biaya transfer data melalui Internet berkecepatan tinggi.

Dengan Snowball Edge, Anda tidak perlu menulis kode apa pun atau membeli perangkat keras apa pun untuk mentransfer data Anda. Mulailah dengan menggunakan Konsol AWS Manajemen untuk [Membuat Pekerjaan Impor](#) untuk Snowball, dan perangkat Snowball akan dikirimkan secara otomatis kepada Anda. Setelah tiba, pasang perangkat ke jaringan lokal Anda, unduh dan jalankan Klien Snowball (“Klien”) untuk membuat koneksi, dan kemudian gunakan Klien untuk memilih direktori file yang ingin Anda transfer ke perangkat. Klien kemudian mengenkripsi dan mentransfer file ke perangkat dengan kecepatan tinggi. Setelah transfer selesai dan perangkat siap dikembalikan, label pengiriman E Ink secara otomatis diperbarui dan Anda dapat melacak status pekerjaan dengan Amazon Simple Notification Service (Amazon SNS), pesan teks, atau langsung di Konsol. Untuk mempelajari selengkapnya, lihat [AWS Snowball Edge](#).

FAQ Snowball Edge di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Snowball Edge akun AMS saya?

Implementasi Snowball Edge di AMS adalah proses dua langkah:

1. Kirim Manajemen | Lainnya | Lainnya | Buat (ct-1e1xtak34nx76) ubah jenis dan minta peran layanan untuk Snowball Edge untuk Akun AMS Anda.
2. Minta akses pengguna dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_snowball_console_role`, `customer_snowball_export_role`, dan `customer_snowball_import_role`. Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Snowball Edge di akun AMS saya?

Fungsionalitas penuh AWS Snowball Edge tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Snowball Edge

Anda harus memiliki akun peran layanan seperti yang disebutkan di atas.

Gunakan SSP AMS untuk menyediakan AWS Step Functions di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Step Functions kapabilitas secara langsung di akun terkelola AMS Anda. AWS Step Functions adalah layanan Web yang memungkinkan Anda untuk mengoordinasikan komponen aplikasi terdistribusi dan layanan mikro dengan menggunakan alur kerja visual. Anda membangun aplikasi dari komponen individu yang masing-masing menjalankan fungsi diskrit, atau tugas, memungkinkan Anda untuk menskalakan dan mengubah aplikasi dengan cepat. Step Functions menyediakan cara yang dapat diandalkan untuk mengoordinasikan komponen dan langkah melalui fungsi aplikasi Anda. Step Functions menawarkan konsol grafis untuk memvisualisasikan komponen aplikasi Anda sebagai serangkaian langkah. Ini secara otomatis memicu dan melacak setiap langkah, dan mencoba lagi ketika ada kesalahan, sehingga aplikasi Anda berjalan secara berurutan dan seperti yang diharapkan, setiap saat. Step Functions mencatat status setiap langkah, jadi ketika terjadi kesalahan, Anda dapat mendiagnosis dan melakukan debug masalah dengan cepat. Untuk mempelajari selengkapnya, lihat [AWS Step Functions](#).

FAQ Step Functions di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Step Functions akun AMS saya?

Minta akses ke AWS Step Functions dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_step_functions_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Step Functions di akun AMS saya?

Fungsionalitas penuh AWS Step Functions tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Step Functions

Saat runtime, peran yang digunakan oleh Step Functions harus memiliki akses ke layanan yang digunakan oleh fungsi step. Misalnya, fungsi langkah dapat bergantung pada fungsi Lambda. Seseorang yang membuat fungsi langkah kemungkinan akan membuat fungsi Lambda pada saat yang sama dan harus meminta akses ke layanan itu juga.

Gunakan AMS SSP untuk menyediakan AWS Systems Manager Parameter Store di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan AWS Systems Manager Parameter Store secara langsung di akun terkelola AMS Anda. AWS Systems Manager Parameter Store menyediakan penyimpanan hierarkis yang aman untuk manajemen data konfigurasi dan manajemen rahasia. Anda dapat menyimpan data seperti kata sandi, string database, dan kode lisensi sebagai nilai parameter. Anda dapat menyimpan nilai sebagai teks biasa atau data terenkripsi. Anda kemudian dapat mereferensikan nilai dengan menggunakan nama unik yang Anda tentukan saat Anda membuat parameter. Sangat skalabel, tersedia, dan tahan lama, Parameter Store didukung oleh AWS Cloud. Untuk mempelajari lebih lanjut, lihat [Menyimpan AWS Systems Manager Parameter](#).

Note

Jika Anda ingin menyimpan rahasia khusus dengan manajemen siklus hidup, gunakan [Gunakan SSP AMS untuk menyediakan AWS Secrets Manager di akun AMS Anda](#) alih-alih Parameter Store. Secrets Manager membantu Anda memenuhi persyaratan keamanan dan kepatuhan dengan memungkinkan Anda memutar rahasia secara otomatis. Secrets Manager menawarkan integrasi bawaan untuk MySQL, PostgreSQL, dan Amazon Aurora di Amazon RDS, yang dapat diperluas ke jenis rahasia lain dengan menyesuaikan fungsi Lambda.

AWS Systems Manager FAQ Parameter Store di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Systems Manager Parameter Store di akun AMS saya?

Minta akses ke AWS Systems Manager Parameter Store dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_systemsmanager_parameterstore_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS Systems Manager Parameter Store di akun AMS saya?

Anda diminta untuk menggunakan kunci AWS Terkelola; akses dibatasi dari membuat kunci KMS kustom. Namun, jika kunci khusus diperlukan, kirimkan RFC untuk membuat kunci yang dikelola pelanggan (CMK) menggunakan Deployment | Komponen Tumpukan Tingkat Lanjut | Kunci KMS | Buat jenis perubahan (ct-1d84keiri1jhg) dengan peran IAM ini, sebagai nilai untuk parameter dan. `customer_systemsmanager_parameterstore_console_role`
`IAMPrincipalsRequiringDecryptPermissions`
`IAMPrincipalsRequiringEncryptPermissionsPrincipal` Setelah Kunci KMS dibuat, Anda dapat membuat String Aman menggunakannya.

T: Apa prasyarat atau dependensi untuk menggunakan AWS Systems Manager Parameter Store di akun AMS saya?

Tidak ada prasyarat; Namun, SSM Parameter Store bergantung pada KMS untuk membuat String Aman sehingga Anda dapat mengenkripsi dan mendekripsi Nilai mereka yang disimpan di Parameter Store.

Gunakan SSP AMS untuk menyediakan AWS Systems Manager Otomasi di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan AWS Systems Manager Otomasi secara langsung di akun terkelola AMS Anda. AWS Systems Manager Otomatisasi menyederhanakan tugas pemeliharaan dan penerapan umum instans Amazon Elastic Compute Cloud dan AWS sumber daya lainnya menggunakan runbook, tindakan, dan kuota layanan. Ini memungkinkan Anda untuk membangun, mengeksekusi, dan memantau otomatisasi dalam skala besar. Automasi Systems Manager adalah jenis dokumen Systems Manager yang mendefinisikan tindakan yang dilakukan Systems Manager pada instans terkelola Anda. Runbook yang Anda gunakan untuk melakukan tugas pemeliharaan dan penerapan umum seperti menjalankan perintah atau skrip otomatisasi dalam instance terkelola Anda. Systems Manager menyertakan fitur yang membantu Anda menargetkan grup instans besar dengan menggunakan tag Amazon Elastic Compute Cloud, dan kontrol kecepatan yang membantu Anda meluncurkan perubahan sesuai dengan batas yang Anda tentukan. Runbook ditulis menggunakan JavaScript Object Notation (JSON) atau YAMM. Menggunakan Pembuat Dokumen di konsol Otomatisasi Systems Manager, namun, Anda dapat membuat runbook tanpa harus menulis dalam JSON atau YAML. Atau Anda dapat menggunakan runbook yang disediakan Manajer Sistem dengan langkah-langkah yang telah ditentukan sebelumnya yang sesuai dengan kebutuhan Anda. Untuk mempelajari lebih lanjut, lihat [Bekerja dengan runbook](#) dalam AWS Systems Manager dokumentasi.

Note

Meskipun Systems Manager Automation mendukung 20 jenis tindakan yang dapat digunakan di runbook, sejumlah tindakan terbatas yang dapat Anda gunakan saat membuat runbook untuk digunakan di akun AMS Advanced Anda. Demikian pula, sejumlah runbook yang disediakan Manajer Sistem dapat digunakan baik secara langsung atau dari dalam runbook Anda sendiri. Untuk detailnya, lihat batasan di FAQ berikut.

AWS Systems Manager FAQ Otomasi di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Systems Manager Automation di akun AMS saya?

Minta akses ke AWS Systems Manager Otomasi dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_systemsmanager_automation_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS Systems Manager Otomasi di akun AMS saya?

Anda diminta untuk membuat runbook Anda, dengan serangkaian tindakan yang didukung Systems Manager terbatas untuk otomatisasi, hanya untuk menjalankan and/or skrip perintah dalam instance terkelola Anda. Tindakan yang tersedia untuk Anda bersama dengan batasan apa pun diuraikan seperti di bawah ini.

AWS Systems Manager Batasan Otomasi

Tindakan	Deskripsi	Batasan
<code>aws: assertAwsResource Properti —</code>	Menegaskan status AWS sumber daya atau status acara	Hanya EC2 contoh
<code>aws:aws: cabang —</code>	Jalankan langkah-langkah otomatisasi bersyarat	Tidak ada batasan

Tindakan	Deskripsi	Batasan
AWS: createTags -	Buat tag untuk AWS sumber daya	Hanya untuk runbook otomatisasi SSM yang Anda buat
AWS: ExecuteAutomation -	Jalankan otomatisasi lain	Hanya runbook otomatisasi yang Anda buat
AWS: ExecuteScript -	Jalankan skrip	Hanya skrip yang tidak melakukan panggilan API apa pun ke layanan apa pun
aws:jeda —	Jeda otomatisasi	Tidak ada batasan
AWS: runcommand —	Jalankan perintah pada instance terkelola	Hanya menggunakan dokumen yang disediakan Manajer Sistem - AWS-RunShellScript dan AWS-RunPowerShellScript
aws:tidur —	Tunda otomatisasi	Tidak ada batasan
aws: waitForAws ResourceProperty —	Tunggu properti AWS sumber daya	Hanya EC2 contoh

Anda juga dapat memilih untuk menjalankan perintah atau skrip secara langsung dengan Systems Manager yang disediakan runbook AWS- RunShellScript dan AWS- RunPowerShellScript menggunakan fitur 'Run Command' dari dalam konsol Systems Manager. Anda juga dapat membuat sarang runbook ini di dalam runbook Anda yang melayani validasi pra and/or posting tambahan atau logika otomatisasi kompleks apa pun.

Peran tersebut mematuhi prinsip hak istimewa terkecil dan hanya memberikan izin yang diperlukan untuk membuat, mengeksekusi, dan mengambil detail eksekusi runbook yang bertujuan untuk mengeksekusi and/or skrip perintah dalam instance terkelola Anda. Itu tidak memberikan izin untuk kemampuan lain yang disediakan AWS Systems Manager layanan. Meskipun fitur ini memungkinkan Anda untuk membuat runbook otomatisasi, eksekusi runbook tidak dapat ditargetkan untuk sumber daya yang dimiliki AMS.

T: Apa prasyarat atau dependensi untuk menggunakan AWS Systems Manager Otomasi di akun AMS saya?

Tidak ada prasyarat; Namun, Anda harus memastikan kontrol and/or kepatuhan proses internal Anda dipatuhi saat membuat runbook. Kami juga merekomendasikan untuk menguji runbook secara menyeluruh sebelum menjalankannya terhadap sumber daya produksi.

T: Dapatkah kebijakan Systems Manager **customer_systemsmanager_automation_policy** dilampirkan ke peran IAM lainnya?

Tidak, tidak seperti layanan berkemampuan penyediaan mandiri lainnya, kebijakan ini hanya dapat ditetapkan ke peran default yang disediakan.
`customer_systemsmanager_automation_console_role`

Tidak seperti kebijakan peran SSPS lainnya, kebijakan SSM SSM ini tidak dapat dibagikan dengan peran IAM kustom lainnya, karena layanan AMS ini hanya untuk menjalankan perintah atau skrip otomatisasi dalam instans terkelola Anda. Jika izin ini diizinkan untuk dilampirkan ke peran IAM kustom lainnya, berpotensi dengan izin pada layanan lain, cakupan tindakan yang diizinkan dapat diperluas ke layanan terkelola, dan berpotensi menurunkan postur keamanan akun Anda.

Untuk mengevaluasi setiap permintaan perubahan (RFCs) terhadap standar teknis AMS kami, bekerja sama dengan Arsitek Cloud atau Manajer Pengiriman Layanan Anda masing-masing, lihat [ulasan keamanan RFC](#).

Note

AWS Systems Manager memungkinkan Anda menggunakan runbook yang dibagikan dengan akun Anda. Kami menyarankan Anda berhati-hati dan melakukan pemeriksaan uji tuntas saat menggunakan runbook bersama dan pastikan untuk meninjau konten untuk memahami yang dijalankan command/scripts sebelum menjalankan runbook. Untuk detailnya, lihat [Praktik terbaik untuk dokumen SSM bersama](#).

Gunakan SSP AMS untuk menyediakan AWS Transfer Family di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas (Transfer AWS Transfer Family Family) secara langsung di akun terkelola AMS Anda. AWS Transfer Family adalah AWS layanan yang dikelola sepenuhnya yang memungkinkan Anda mentransfer file melalui

Secure File Transfer Protocol (SFTP), masuk dan keluar dari penyimpanan Amazon Simple Storage Service (Amazon S3). SFTP juga dikenal sebagai Secure Shell (SSH) File Transfer Protocol. SFTP digunakan dalam alur kerja pertukaran data di berbagai industri seperti layanan keuangan, perawatan kesehatan, periklanan, dan ritel, antara lain.

Dengan AWS SFTP, Anda mendapatkan akses ke server SFTP AWS tanpa perlu menjalankan infrastruktur server apa pun. Anda dapat menggunakan layanan ini untuk memigrasikan alur kerja berbasis SFTP AWS sambil mempertahankan klien dan konfigurasi pengguna akhir Anda apa adanya. Pertama-tama Anda mengaitkan nama host Anda dengan titik akhir server SFTP, lalu tambahkan pengguna Anda dan berikan mereka tingkat akses yang tepat. Setelah Anda melakukannya, permintaan transfer pengguna Anda dilayani langsung dari titik akhir server AWS SFTP Anda. Untuk mempelajari selengkapnya [AWS Transfer for SFTP](#), lihat juga [Membuat server berkemampuan SFTP](#).

AWS Transfer for SFTP di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Transfer for SFTP akun AMS saya?

Minta akses ke AWS Transfer for SFTP dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). Melalui RFC ini, peran IAM berikut, dan kebijakan, disediakan di akun Anda:

- `customer_transfer_author_role`. Peran ini dirancang bagi Anda untuk mengelola layanan SFTP melalui konsol.
- `customer_transfer_sftp_server_logging_role`. Peran ini dirancang untuk dilampirkan pada Server SFTP. Hal ini memungkinkan server SFTP untuk menarik log ke dalam CloudWatch.
- `customer_transfer_sftp_user_role`. Peran ini dirancang untuk dilampirkan pada pengguna SFTP. Ini memungkinkan pengguna SFTP untuk berinteraksi dengan bucket S3.
- `policy_customer_transfer_scope_down_policy`. Kebijakan ini adalah kebijakan cakupan bawah yang dapat diterapkan pada Pengguna SFTP untuk membatasi akses mereka pada bucket S3 ke folder rumah mereka.
- `customer_transfer_sftp_efs_user_role`. Peran ini dirancang untuk dilampirkan pada pengguna SFTP. Hal ini memungkinkan pengguna SFTP untuk berinteraksi dengan sistem file EFS.

Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Transfer for SFTP di akun AMS saya?

AWS Transfer untuk konfigurasi SFTP terbatas pada sumber daya tanpa awalan “AMS-” atau “MC-” untuk mencegah modifikasi apa pun pada infrastruktur AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Transfer for SFTP

- Anda harus memiliki bucket Amazon S3 dengan nama yang berisi kata kunci “transfer” sebelum membuat AWS Transfer for SFTP server dan pengguna.
- Untuk menggunakan “Penyedia Identifikasi Pelanggan”, Anda harus menerapkan API Gateway, fungsi Lambda, dan repositori pengguna Anda (AD, Secrets Manager, dan sebagainya). Untuk informasi selengkapnya, lihat [Mengaktifkan otentikasi kata sandi untuk AWS Transfer for SFTP menggunakan AWS Secrets Manager](#) dan [Bekerja dengan Penyedia Identitas](#).

Gunakan SSP AMS untuk menyediakan AWS Transit Gateway di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Transit Gateway kapabilitas secara langsung di akun terkelola AMS Anda. AWS Transit Gateway adalah layanan yang memungkinkan Anda menghubungkan Amazon Virtual Private Cloud (VPCs) dan jaringan lokal Anda ke satu gateway. Saat Anda meningkatkan jumlah beban kerja yang berjalan AWS, Anda harus dapat menskalakan jaringan Anda di beberapa akun dan Amazon VPCs untuk mengikuti pertumbuhannya. Hari ini, Anda dapat menghubungkan pasangan Amazon VPCs menggunakan peering. Namun, mengelola point-to-point konektivitas di banyak Amazon VPCs, tanpa kemampuan untuk mengelola kebijakan konektivitas secara terpusat, dapat menjadi mahal dan rumit secara operasional. Untuk konektivitas lokal, Anda perlu melampirkan AWS VPN ke setiap VPC Amazon individual. Solusi ini dapat memakan waktu untuk membangun dan sulit untuk mengelola ketika jumlah VPCs tumbuh menjadi ratusan. Untuk mempelajari selengkapnya, lihat [AWS Transit Gateway](#).

AWS Transit Gateway di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Transit Gateway akun AMS saya?

Minta akses ke AWS Transit Gateway dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_tgw_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Transit Gateway di akun AMS saya?

Fungsionalitas lengkap AWS Transit Gateway tersedia di akun landing zone akun tunggal AMS Anda kecuali modifikasi tabel rute untuk perutean Transit Gateway. Minta perubahan tabel rute dengan mengirimkan Manajemen | Lainnya | Lainnya | Buat jenis perubahan (ct-1e1xtak34nx76).

 Note

Layanan ini hanya didukung untuk single-account landing zone (SALZ), bukan multi-account landing zone (MALZ).

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Transit Gateway

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS Transit Gateway

Gunakan AMS SSP untuk menyediakan AWS WAF - Firewall Aplikasi Web di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS WAF kapabilitas secara langsung di akun terkelola AMS Anda. AWS WAF adalah firewall aplikasi web (AWS WAF) yang membantu melindungi aplikasi web Anda dari eksploitasi web umum yang dapat memengaruhi ketersediaan aplikasi, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan. AWS WAF memberi Anda kontrol atas lalu lintas mana yang diizinkan, atau diblokir, ke aplikasi web Anda dengan mendefinisikan aturan keamanan web yang dapat disesuaikan. Anda dapat menggunakan AWS WAF untuk membuat aturan kustom yang memblokir pola serangan umum, seperti injeksi SQL atau cross-site scripting; dan aturan yang dirancang untuk aplikasi spesifik Anda.

Untuk mempelajari lebih lanjut, lihat [AWS WAF - Firewall Aplikasi Web](#).

AMS tidak mendukung pemantauan (CloudWatch alarm/acara/peringatan MMS) untuk AWS WAF. Karena sifatnya AWS WAF, Anda harus membuat aturan khusus untuk aplikasi Anda; AMS tidak dapat mengukur dan membuat alarm untuk Anda, tanpa konteks aplikasi Anda. Untuk mempelajari lebih lanjut, lihat [AWS WAF - Firewall Aplikasi Web](#).

AWS WAF di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara saya meminta AWS WAF untuk disiapkan di akun AMS saya?

Meminta akses AWS WAF dengan mengirimkan RFC dengan Manajemen | Layanan AWS | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_waf_role` Setelah peran AWS WAF IAM disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS WAF?

Setelah izin disediakan, Anda memiliki fungsionalitas penuh. AWS WAF

T: Apa prasyarat atau dependensi yang digunakan? AWS WAF

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS WAF

Gunakan SSP AMS untuk menyediakan AWS Well-Architected Tool di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Well-Architected Tool kapabilitas secara langsung di akun terkelola AMS Anda. AWS Well-Architected Tool Ini membantu Anda meninjau keadaan beban kerja Anda dan membandingkannya dengan praktik terbaik AWS arsitektur terbaru. Alat ini didasarkan pada [AWS Well-Architected Framework, yang dikembangkan untuk membantu arsitek](#) cloud membangun infrastruktur aplikasi yang aman, berkinerja tinggi, tangguh, dan efisien. Kerangka kerja ini memberikan pendekatan yang konsisten bagi Anda untuk mengevaluasi arsitektur, telah digunakan dalam puluhan ribu tinjauan beban kerja yang dilakukan oleh tim arsitektur AWS solusi, dan memberikan panduan untuk membantu mengimplementasikan desain yang sesuai dengan kebutuhan aplikasi dari waktu ke waktu. Untuk mempelajari selengkapnya, lihat [AWS Well-Architected Tool](#).

AWS WA Tool di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Well-Architected Tool akun AMS saya?

Meminta akses AWS Well-Architected Tool dengan mengirimkan RFC dengan Manajemen | Layanan AWS | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_well_architected_tool_console_admin_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Well-Architected Tool di akun AMS saya?

Fungsionalitas penuh AWS Well-Architected Tool tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Well-Architected Tool

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS Well-Architected Tool

Gunakan SSP AMS untuk menyediakan AWS X-Ray di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas (AWS X-Ray X-Ray) secara langsung di akun terkelola AMS Anda. AWS X-Ray membantu pengembang menganalisis dan men-debug produksi, aplikasi terdistribusi, seperti yang dibangun menggunakan arsitektur microservices. Dengan X-Ray, Anda dapat memahami kinerja aplikasi dan layanan yang mendasarinya, untuk mengidentifikasi dan memecahkan masalah akar penyebab masalah kinerja dan kesalahan. X-Ray memberikan end-to-end tampilan permintaan saat mereka melakukan perjalanan melalui aplikasi Anda, dan menunjukkan peta komponen dasar aplikasi Anda. Anda dapat menggunakan X-Ray untuk menganalisis kedua aplikasi dalam pengembangan dan produksi, dari aplikasi tiga tingkat sederhana, hingga aplikasi layanan mikro kompleks yang terdiri dari ribuan layanan. Untuk mempelajari selengkapnya, lihat [AWS X-Ray](#).

FAQ X-Ray di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS X-Ray akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_xray_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda. Selain itu, Anda harus memiliki kemampuan `customer_xray_daemon_write_instance_profile` untuk mendorong data dari EC2 instans Amazon Anda ke X-Ray. Profil instance ini dibuat saat Anda menerima file `customer_xray_console_role`.

Anda dapat mengirimkan permintaan layanan ke Operasi AMS untuk menetapkan profil instans yang ada, atau Anda dapat menggunakan profil instans yang dibuat saat Operasi AMS mengaktifkan X-Ray untuk Anda. `customer_xray_daemon_write_policy`

T: Apa batasan penggunaan AWS X-Ray di akun AMS saya?

Fungsionalitas penuh AWS X-Ray tersedia di akun AMS Anda kecuali untuk enkripsi dengan kunci AWS KMS (kunci KMS). AWS X-Ray mengenkripsi semua data jejak secara default. Secara default, X-Ray mengenkripsi jejak dan data terkait saat istirahat. Jika Anda perlu mengenkripsi data saat istirahat dengan kunci, Anda dapat memilih kunci KMS AWS-managed (aws/xray) atau kunci KMS Customer-Managed. Untuk kunci KMS yang Dikelola Pelanggan untuk enkripsi X-Ray, kirimkan Manajemen | Lainnya | Lainnya | Buat jenis perubahan (ct-1e1xtak34nx76).

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS X-Ray

AWS X-Ray memiliki ketergantungan pada Amazon S3 CloudWatch,, CloudWatch dan Log, yang sudah diterapkan di akun AMS. Dependensi transitif bervariasi berdasarkan sumber data dan AWS layanan lain AWS X-Ray yang mungkin berinteraksi dengan fitur (misalnya, Amazon Redshift, Amazon RDS, Athena).

Gunakan AMS SSP untuk menyediakan VM Import/Export di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses VM Import/Export capabilities secara langsung di akun terkelola AMS Anda. VM Import/Export memungkinkan Anda untuk dengan mudah mengimpor gambar mesin virtual dari lingkungan yang ada ke EC2 instans Amazon dan mengekspornya kembali ke lingkungan lokal Anda. Penawaran ini memungkinkan Anda untuk memanfaatkan investasi yang ada di mesin virtual yang telah Anda buat untuk memenuhi persyaratan keamanan, manajemen konfigurasi, dan kepatuhan TI Anda dengan membawa mesin virtual tersebut ke Amazon EC2 sebagai ready-to-use contoh. Anda juga dapat mengeksport instans yang diimpor kembali ke infrastruktur virtualisasi lokal Anda, memungkinkan Anda untuk menyebarkan beban kerja di seluruh infrastruktur TI Anda. Untuk mempelajari lebih lanjut, lihat [Impor/ Ekspor VM](#).

FAQ VM Import/Export di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke VM Import/Export di akun AMS saya?

Minta akses ke VM Import/Export dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini

memberikan kebijakan IAM berikut ke akun Anda: `customer_vmimport_policy` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

Peran tambahan, peran `Import/Export Layanan VM`, diperlukan agar layanan dapat melakukan tindakan di akun Anda.

T: Apa batasan untuk menggunakan VM Import/Export di akun AMS saya?

- Fungsionalitas untuk mengimpor gambar mesin khusus dan volume data keduanya tersedia di AMS VM Impor/Ekspor. Namun, izin ke S3 telah dicakup untuk membatasi tindakan ke bucket yang cocok dengan nama untuk membatasi akses ke informasi `customer-vmimport-*` dalam akun.
- Impor gambar dan snapshot didukung di AMS VM Impor/Ekspor. Namun, fungsi impor instance dan ekspor instance tidak tersedia karena langkah-langkah keamanan.
- Selain itu, fungsionalitas ekspor telah dinonaktifkan untuk mengurangi risiko mengeksport data yang dibatasi dan sensitif.

T: Apa prasyarat atau dependensi untuk menggunakan VM di akun AMS saya? Import/Export

- Anda harus memberikan image disk yang didukung untuk mengimpor ke AWS lingkungan. Untuk selengkapnya, lihat [Import/Export Persyaratan VM](#).
- VM Import/Export tidak dapat diakses melalui AWS konsol. Anda harus mengakses layanan ini melalui AWS CLI Alat AWS untuk PowerShell, atau AWS SDKs. Atau, Anda dapat meminta profil instance dengan mengirimkan jenis perubahan `ct-117rmp64d5mnb: Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat profil instance`. EC2 Profil instance ini memungkinkan alat untuk melakukan perintah dari sebuah instance.

Modus Dikelola Pelanggan

Mode AWS Managed Services (AMS) Customer Managed menyediakan model tata kelola yang fleksibel dan dapat disesuaikan dengan kebutuhan Anda. Ini dapat dianggap sebagai opsi fallback untuk layanan dan aplikasi yang AMS tidak dapat beroperasi untuk Anda. AMS tidak mengoperasikan infrastruktur yang dihosting di akun yang dibuat dalam mode ini. Namun, Anda dapat memanfaatkan manajemen multi-akun terpusat dalam mode ini. Fitur Zona Pendaratan Multi-Akun berikut dapat dimanfaatkan dalam mode ini:

- Penyebaran Akun Otomatis
- Konektivitas melalui Transit Gateway di akun jaringan

- Pustaka Aturan Konfigurasi AMS
- Simpan salinan log di akun logging
- Agregasi peringatan Guard Duty yang dikelola pelanggan ke akun Keamanan
- Tagihan Terkonsolidasi
- Pengaktifan Kebijakan Kontrol Layanan kustom.

Misalnya: Jika Anda ingin menjalankan beban kerja di Ubuntu Pro, yang bukan Sistem Operasi yang dikelola oleh AMS, Anda dapat menggunakan akun yang dikelola pelanggan untuk hosting itu. Anda juga dapat mengkonsolidasikan beban kerja melalui akun yang dikelola pelanggan, untuk memanfaatkan diskon massal pada Instances/Sharing Paket Cadangan yang tersedia melalui berbagi di seluruh organisasi AWS.

Memulai mode Customer Managed

Mode Terkelola Pelanggan AMS tersedia melalui akun Aplikasi landing zone multi-akun khusus.

Untuk detailnya, termasuk cara membuat akun Aplikasi Terkelola Pelanggan, lihat [Akun aplikasi yang Dikelola Pelanggan](#).

AMS dan AWS Service Catalog

Service Catalog di AWS Managed Services (AMS) memungkinkan organisasi untuk membuat dan mengelola katalog layanan teknologi informasi AWS (TI) dan memungkinkan administrator TI untuk membuat, mengelola, dan mendistribusikan katalog produk yang disetujui kepada pengguna akhir di akun mereka, yang kemudian dapat mengakses produk yang mereka butuhkan di portal layanan yang dipersonalisasi. Administrator dapat mengontrol pengguna mana yang memiliki akses ke setiap produk untuk menegakkan kepatuhan terhadap kebijakan bisnis organisasi. Administrator juga dapat mengatur peran sehingga pengguna akhir hanya memerlukan akses IAM ke Service Catalog untuk menyebarkan sumber daya yang disetujui. Service Catalog memungkinkan organisasi Anda mendapatkan keuntungan dari peningkatan kelincahan dan pengurangan biaya karena pengguna akhir hanya dapat menemukan dan meluncurkan produk yang mereka butuhkan dari katalog yang Anda kontrol.

Service Catalog memberi Anda alternatif untuk proses permintaan perubahan (RFC) AMS untuk menyediakan dan memperbarui sumber daya di akun terkelola AMS Anda. AMS mengelola semua tugas operasi infrastruktur yang diperlukan untuk menjalankan AWS dalam skala besar untuk semua sumber daya infrastruktur yang disediakan melalui Service Catalog termasuk keamanan, kepatuhan,

penyediaan, ketersediaan, tambalan, pemantauan, peringatan, pelaporan, respons insiden, dan pengoptimalan biaya. Memanfaatkan Service Catalog di akun terkelola AMS Anda memberi Anda mekanisme untuk mengelola layanan TI yang umum digunakan secara terpusat dan membantu Anda mencapai tata kelola yang konsisten sekaligus memungkinkan pengguna untuk dengan cepat menerapkan hanya layanan TI yang disetujui yang mereka butuhkan ke lingkungan terkelola mereka.

Memulai Service Catalog

Untuk memulai Service Catalog di AMS, kirimkan permintaan layanan melalui konsol AMS untuk meminta akses ke Service Catalog. Setelah mengajukan permintaan, tiga peran IAM akan diterapkan ke akun Anda bersama dengan tumpukan terkelola AMS yang berisi CloudFormation makro yang memanggil AMS Transform (dijelaskan sebelumnya) sehingga kami dapat mendaftarkan produk di sistem kami, dan untuk melakukan operasi terhadap infrastruktur yang disediakan melalui Service Catalog. Tiga peran IAM yang digunakan termasuk peran bagi admin TI untuk mengelola produk sebagai admin Service Catalog; peran bagi pemilik aplikasi dan pengguna akhir untuk mengonfigurasi, meluncurkan, dan mengelola produk; dan peran yang akan digunakan sebagai kendala peluncuran, yang menentukan izin yang akan digunakan oleh Service Catalog saat meluncurkan atau memperbarui produk Anda.

Service Catalog di AMS sebelum Anda mulai

Apakah Service Catalog menggantikan proses AMS request for change (RFC) yang ada?

Di akun di mana Service Catalog diaktifkan, itu akan bertindak sebagai sistem manajemen perubahan tempat Anda menyediakan dan memperbarui layanan TI di akun AMS Anda melalui katalog produk yang telah ditentukan sebelumnya; AMS akan menyediakan portfolio/product katalog default, dan admin TI Anda dapat membuat dan mengonfigurasi milik Anda sendiri. Service Catalog hanya akan mengakui tumpukan yang disediakan melalui Service Catalog. Demikian juga, layanan yang disediakan melalui Service Catalog tidak akan dapat dimodifikasi melalui proses AMS RFC karena modifikasi di luar Service Catalog akan mengalihkan tumpukan dari konfigurasi produk yang disetujui.

Dapatkah saya melihat tumpukan yang disediakan melalui katalog layanan di Konsol AMS?

Ya. Anda dapat melihat semua tumpukan yang disediakan melalui katalog layanan di konsol AMS. Tumpukan yang disediakan melalui katalog layanan mudah diidentifikasi oleh ID tumpukan "SC-". Meskipun tumpukan dapat dilihat di konsol AMS, Anda tidak akan dapat memperbarui melalui proses AMS RFC. Akses ke sistem manajemen perubahan AMS (RFCs) terbatas pada permintaan akses, orkestrasi patch, dan cadangan saja. RFCs

Jika saya menyediakan and/or pembaruan tumpukan melalui Service Catalog, apakah akan ada RFC yang sesuai di Konsol AMS?

Satu-satunya RFC yang akan ditampilkan di konsol AMS adalah RFC untuk mendaftarkan tumpukan dengan AMS saat tumpukan awalnya disediakan. RFC ini diajukan secara otomatis oleh proses validasi AMS yang dipicu saat tumpukan diluncurkan melalui Service Catalog. Semua penyediaan dan perubahan lainnya dilacak secara langsung di Service Catalog dan dapat dilihat di konsol Service Catalog. Selanjutnya, Anda dapat menggunakan fitur Provisioned Product Plan di Service Catalog untuk melihat daftar perubahan yang akan dilakukan pada sumber daya sebelum penyediaan atau pembaruan produk.

Apakah saya harus melakukan sesuatu yang spesifik untuk menyediakan produk di akun terkelola AMS saya?

Ya. Semua produk Service Catalog yang disediakan di akun AMS harus berisi baris JSON ini dalam template CFN yang mendefinisikan produk tersebut:

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

Cuplikan CloudFormation kode ini memicu validasi AMS yang diperlukan sebelum sumber daya dapat disediakan di akun terkelola AMS Anda. Adalah tanggung jawab Anda untuk memasukkan baris kode ini sebagai bagian dari definisi produk. Jika tidak disertakan, penyediaan akan gagal dan pesan kesalahan berikut akan ditampilkan: “Gagal membuat produk. Akun ini dikelola oleh AMS. Semua produk di akun AMS harus memiliki Transform kode AMS di template.

Apakah ada fungsionalitas Service Catalog yang tidak tersedia and/or terbatas untuk pelanggan AMS saat diluncurkan?

Ya, fitur SC berikut tidak tersedia untuk pelanggan AMS pada peluncuran awal:

- Pembuatan Akun melalui Service Catalog
- Kemampuan untuk meluncurkan semua AWS Services melalui Service Catalog ke dalam akun yang dikelola AMS. Ketersediaan AWS Service terbatas pada layanan yang didukung AMS (dikelola dan disediakan sendiri). Untuk informasi selengkapnya tentang layanan yang didukung AMS, lihat deskripsi layanan AMS.
- Konektor Service Catalog IT service manager (ITSM) tidak akan berkomunikasi dengan laporan insiden AMS, dan permintaan layanan.

- Kemampuan untuk memanfaatkan Service Catalog mulai cepat dan arsitektur referensi tanpa modifikasi. Ingat bahwa produk Service Catalog untuk akun AMS harus berisi baris kode JSON ini:

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

dalam template CNF. Perhatikan bahwa baris ini bukan bagian dari CloudFormation template AWS biasa dan harus ditambahkan secara eksplisit.

- Terraform saat ini tidak didukung oleh AMS untuk menyediakan produk Service Catalog.
- Stackset AWS CFN tidak didukung di AMS.
- Anda tidak dapat membuat peran IAM kustom.
- Tindakan Layanan terbatas pada:
 - [AWS- RebootRdsInstance](#)
 - [Instans AWS-Restart EC2](#)
 - [Instans AWS-Mulai EC2](#)
 - [AWS- StartRdsInstance](#)
 - [Instans AWS-Stop EC2](#)
 - [AWS- StopRdsInstance](#)
 - [AWS- CreateImage](#)
 - [AWS- CreateRdsSnapshot](#)
 - [AWS- CreateSnapshot](#)

Note

Saat membuat tindakan layanan, Anda dapat mengonfigurasi peran eksekusi menjadi izin pengguna akhir, peran peluncuran, atau peran IAM khusus yang Anda pilih. Peran eksekusi yang dipilih harus memiliki izin yang cukup untuk melakukan tindakan layanan, dan memiliki peran TrustPolicy yang memungkinkannya diasumsikan oleh Service Catalog, jika tidak, tindakan layanan akan gagal pada saat eksekusi. Sebaiknya gunakan `AWSManagedServicesServiceCatalogLaunchRole`, yang memiliki izin dan kebijakan kepercayaan yang benar untuk digunakan sebagai tindakan layanan.

Untuk apa saya masih perlu menggunakan sistem AMS RFC?

Pada ketersediaan umum (GA) Anda masih perlu menggunakan RFCS untuk menjalankan tindakan berikut:

- Mengkonfigurasi Patch Orchestrator
- Mengkonfigurasi kebijakan Cadangan
- Meminta akses instans
- Membuat dan menetapkan grup keamanan yang berada di luar pedoman AMS.
- Melakukan konsumsi beban kerja (WIGS)
- Membuat Peran IAM

Dapatkah saya menggunakan Service Catalog CLI untuk mengakses Service Catalog di akun terkelola AMS saya?

Ya, Service Catalog APIs tersedia dan diaktifkan melalui CLI. Tindakan dari pengelolaan artefak Service Catalog melalui penyediaan dan penghentian artefak tersebut, tersedia. Untuk informasi selengkapnya, lihat [Sumber Daya AWS Service Catalog](#), atau unduh AWS SDK atau CLI terbaru.

Siapa yang membuat, mengelola, dan mendistribusikan katalog produk yang disetujui pelanggan?

Administrator and/or TI administrator katalog pelanggan, atau sumber daya yang ditetapkan, bertanggung jawab atas pengelolaan katalog Service Catalog dan produk yang disetujui.

Bisakah saya menggunakan AMS AMIs?

AMIs AMS yang dijual setelah Maret 2020 dapat digunakan melalui AWS Service Catalog.

Bagaimana cara bermigrasi ke AMS menggunakan Service Catalog?

Untuk memigrasikan beban kerja Anda ke AMS menggunakan Service Catalog, Anda mulai dengan mengikuti proses [Workload Ingest](#) (WIGs) untuk membuat AMI di AMS. Anda menggunakan AMI yang diproduksi oleh WIGS untuk membuat produk di Service Catalog. Cara melakukannya dirinci di [AWS Service Catalog - Memulai](#).

Menemukan data yang Anda butuhkan (SKMS), AMS

Menemukan data yang Anda perlukan saat menggunakan akun AWS Managed Services (AMS) memanggil sistem manajemen pengetahuan layanan AMS, atau SKMS. AMS.

SKMS adalah singkatan dari sistem manajemen pengetahuan layanan dan mengacu pada semua informasi yang terkait dengan layanan AWS Managed Services (AMS) untuk pelanggan. AMS memiliki API SKMS untuk menemukan data.

Topik

- [Apa itu manajemen pengetahuan layanan?](#)
- [Menemukan VPC IDs di AMS](#)
- [Menemukan subnet IDs di AMS](#)
- [Cari AMI IDs, AMS](#)
- [Temukan grup keamanan \(SG\) IDs, AMS](#)
- [Temukan entitas IAM di AMS](#)
- [Temukan tumpukan IDs di AMS](#)
- [Temukan contoh IDs atau alamat IP di AMS](#)
- [Temukan Nama Sumber Daya Amazon \(ARNs\) di AMS](#)
- [Temukan sumber daya oleh ARN di AMS](#)
- [Temukan pengaturan akun AMS](#)

Apa itu manajemen pengetahuan layanan?

Manajemen pengetahuan layanan adalah penyimpanan semua informasi di akun AMS Anda. Informasi tentang hal-hal berikut diperoleh dari sistem manajemen pengetahuan layanan AMS (SKMS), melalui AMS SKMS API atau melalui AMS Console:

- VPCs
- Subnet terkelola
- Komponen tumpukan dan tumpukan, termasuk EC2 instans Amazon dan sumber daya lainnya
- Gambar Mesin Amazon (AMIs)

Anda dapat menggunakan informasi dari SKMS untuk memahami infrastruktur yang dikelola dan sebagai masukan untuk mengubah permintaan manajemen dan layanan untuk membuat, mengubah, atau menghapus infrastruktur.

 Note

Semua panggilan AMS SKMS API dicatat dalam AWS CloudTrail.

Akses SKMS melalui AMS SKMS API, yang menyediakan operasi untuk menemukan informasi tentang lingkungan (VPCs dan subnet) dan sumber daya aplikasi (tumpukan, instans Amazon, dan gambar EC2 instans atau AMIs) yang dapat digunakan di sana.

VPCs dan gambar contoh disiapkan di akun, dengan izin akses yang diperlukan, selama orientasi. Setelah dibuat, Anda dapat menggunakan sistem manajemen perubahan untuk mengisi tumpukan VPCs yang berfungsi.

Menemukan VPC IDs di AMS

Virtual Private Cloud (VPC) memiliki satu atau lebih subnet. Di AMS VPC Anda ada di Wilayah AWS dan Anda memiliki subnet pribadi dan publik.

Lihat juga [Menemukan subnet IDs di AMS](#).

Beberapa CTs membutuhkan VpcId. Untuk menemukan ID VPC, Anda dapat menggunakan konsol AMS atau API/CLI.

Konsol AMS:

Di panel navigasi, pilih VPCs dan VPC yang relevan. Halaman detail VPC untuk VPC yang dipilih terbuka dengan informasi termasuk ID VPC.

AMS SKMS API ListVpcSummaries atau CLI:

 Note

AMS CLI harus diinstal agar perintah ini berfungsi. Untuk menginstal AMS API atau CLI, buka halaman Sumber Daya Pengembang konsol AMS. Untuk materi referensi tentang AMS CM API atau AMS SKMS API, lihat bagian Sumber Informasi AMS di Panduan Pengguna. Anda

mungkin perlu menambahkan `--profile` opsi untuk otentikasi; misalnya, `aws amsskms ams-cli-command --profile SAML`. Anda mungkin juga perlu menambahkan `--region` opsi karena semua perintah AMS kehabisan `us-east-1`; misalnya, `aws amscm ams-cli-command --region=us-east-1`

 Note

Titik akhir AMS API/CLI (amscm dan amsskms) berada di Wilayah AWS N. Virginia,. us-east-1 Bergantung pada cara autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan --region us-east-1 saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan--profile sam1, jika itu adalah metode otentikasi Anda.

1. Dalam contoh berikut, perintah pertama meminta daftar ringkasan untuk semua yang ada VPCs di akun. Perintah kedua meminta daftar VPCs, dengan filter kueri untuk mencantumkan hanya yang VPCs dibuat pada tahun 2016, dan menampilkan CreatedTime, VpcId, dan Nama.

 Note

Anda dapat memperoleh AMS SKMS CLI melalui halaman Sumber Daya Pengembang di konsol AMS.

```
aws amsskms list-vpc-summaries --output table
```

```

+-----+
|                                     ListVPCSummaries
+-----+
|                                     VPCSummaries
+-----+
| CreatedTime      | 2016-01-15T18:50:11Z
| VpcId           | vpc-01234567890abcdef
| LastModifiedTime | 2016-01-15T18:50:11Z
| Name            | 952444781316-initial-vpc
+-----+
|                                     Visibility

```

Id	PrivateAndPublic
Name	PrivateAndPublic

2. Kali ini dengan kueri:

```
aws amsskms list-VPC-summaries --query "VPCSummaries[?
starts_with(@.CreatedTime,to_string(`2016`))].[CreatedTime, VpcId, Name]" --output
table
```

ListVPCSummaries		
2016-01-15T18:50:11Z	vpc-01234567890abcdef	952444781316-initial-VPC

Menemukan subnet IDs di AMS

Beberapa sumber daya mengharuskan Anda menentukan subnet, atau daftar subnet, pada waktu konfigurasi. Untuk menemukan subnet, Anda dapat menggunakan konsol AMS atau AMS SKMS API/CLI. Note that the AMS SKMS API/CLI bersifat pribadi dan harus diinstal sebelum Anda dapat menggunakannya.

Konsol AMS:

1. Di panel navigasi, pilih VPCs dan VPC yang relevan. Halaman detail VPC untuk VPC yang dipilih terbuka dengan tabel subnet, klik ID subnet untuk membuka halaman detail dan menemukan ID.

AMS SKMS API ListSubnetSummaries atau CLI:

Note

AMS CLI harus diinstal agar perintah ini berfungsi. Untuk menginstal AMS API atau CLI, buka halaman Sumber Daya Pengembang konsol AMS. Untuk materi referensi tentang AMS CM API atau AMS SKMS API, lihat bagian Sumber Informasi AMS di Panduan Pengguna. Anda mungkin perlu menambahkan `--profile` opsi untuk otentikasi; misalnya, `aws amsskms ams-cli-command --profile SAML`. Anda mungkin juga perlu menambahkan `--`

region opsi karena semua perintah AMS kehabisan us-east-1; misalnya. `aws amscm aws-cli-command --region=us-east-1`

Note

Titik akhir AMS API/CLI (amscm dan amsskms) berada di Wilayah AWS N. Virginia,. us-east-1 Bergantung pada cara autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan `--profile saml`, jika itu adalah metode otentikasi Anda.

Untuk menemukan subnet untuk VPC Anda, Anda dapat mencari dengan perintah seperti `list-subnet-summaries` yang ditunjukkan.

Note

Jika Anda mencari subnet yang tidak ada di akun AMS, Anda dapat mencobanya `aws ec2 describe-subnets --region us-west-2`.

1. API/CLI ListSubnetSummaries Operasi SKMS:

Daftar sederhana:

```
aws amsskms list-subnet-summaries
```

Output ke tabel:

```
aws amsskms list-subnet-summaries --output table
```

2. ListSubnetSummaries Operasi SKMS API memiliki parameter untuk mempersempit hasil berdasarkan visibilitas. Selain itu, Anda dapat [Memfilter](#) hasil berdasarkan nama. Jika Anda menggunakan CLI, Anda juga dapat menggunakan `--query` opsi untuk mempersempit output atau mencari sebagian dari nilai. Misalnya, untuk menemukan semua subnet untuk VPC tertentu, Anda dapat menggunakan perintah ini:

```
aws amsskms list-subnet-summaries --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

Yang mengembalikan sesuatu seperti ini:

```
-----
|                               ListSubnetSummaries                               |
+-----+-----+-----+-----+
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
+-----+-----+-----+-----+
```

[Untuk informasi tentang penggunaan kueri CLI, lihat Cara Memfilter Output dengan Opsi --query dan referensi bahasa kueri, Spesifikasi. JMESPath](#)

3. Jika Anda memiliki beberapa VPCs, sertakan filter VPC dalam perintah, dan kemudian jalankan perintah untuk setiap VPC. Misalnya:

```
list-subnet-summaries --filter Attribute=VpcId,Value=vpc-xxxxxxx --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

4. Di AWS, gunakan subnet [deskripsikan](#).

[Untuk informasi tentang penggunaan kueri CLI, lihat Cara Memfilter Output dengan Opsi --query dan referensi bahasa kueri, Spesifikasi.. JMESPath](#)

Nama subnet

Subnet AMS Anda dibuat secara otomatis setelah masukan dikumpulkan dari Anda dan ditambahkan ke sistem. AMS menggunakan rumus untuk membuat nama subnet Anda: A **ACCOUNT_ID** - **SUBNET-TYPE** - **AZ** - **IDENTIFIER**. Jenis subnet akan menjadidmz,shared-services, ataucustomer-application. Jika Anda memiliki lebih dari satu subnet aplikasi pelanggan, pengenal opsional dapat ditambahkan ke nama subnet, setelah ID akun, untuk menunjukkan bahwa subnet adalah subnet “tambahan” atau “cadangan”.

Cari AMI IDs, AMS

Amazon Machine Image, atau AMI, adalah template untuk EC2 instans Amazon, dibuat dari EC2 instans Amazon. AWS menyediakan yang diperbarui AMIs (dengan tambalan, misalnya) setiap bulan; namun, AWS Managed Services (AMS) mengharuskan AMIs yang telah dimodifikasi untuk penggunaan AMS. AMS merilis baru AMIs yang dapat Anda gunakan segera setelah Patch Tuesday setiap bulan.

Amazon Machine Images (AMIs) adalah templat konfigurasi instans yang digunakan untuk membuat EC2 instance di AWS. AMS mengharuskan penggunaan khusus AMIs untuk sumber daya yang dikelola AMS. Jenis perubahan untuk membuat EC2 instance dan grup EC2 Auto Scaling mengharuskan Anda menentukan AMI untuk AMS untuk digunakan sebagai dasar untuk instance yang dibuat oleh tipe perubahan. AMS menyarankan agar Anda selalu memilih AMI terbaru yang tersedia untuk Anda.

Untuk mempelajari selengkapnya AWS AMIs, lihat [Desain AWS AMI](#).

Saat membuat EC2 tumpukan Amazon atau grup Amazon EC2 Auto Scaling untuk akun AMS Anda, Anda harus menentukan AMI berdasarkan. Amild Anda terbatas untuk AMIs itu dimulai dengan “pelanggan-” dan kami menyarankan Anda untuk selalu memilih AMI terbaru.

Untuk menemukan AMI terbaru untuk akun Anda, Anda dapat mencari dengan perintah AMS SKMS CLI atau menggunakan halaman detail konsol AMS untuk VPC yang relevan:

- Gunakan konsol AMS: Tersedia AMIs tercantum di halaman AMI di konsol AMS. Pilih dari AMIs dengan nama yang dimulai dengan “pelanggan-”.
- Gunakan API/CLI ListAmis operasi AMS SKMS.

Note

AMS CLI harus diinstal agar perintah ini berfungsi. Untuk menginstal AMS API atau CLI, buka halaman Sumber Daya Pengembang konsol AMS. Untuk materi referensi tentang AMS CM API atau AMS SKMS API, lihat bagian Sumber Informasi AMS di Panduan Pengguna. Anda mungkin perlu menambahkan `--profile` opsi untuk otentikasi; misalnya, `aws amsskms ams-cli-command --profile SAML`. Anda mungkin juga perlu menambahkan `--region` opsi karena semua perintah AMS kehabisan `us-east-1`; misalnya, `aws amscm ams-cli-command --region=us-east-1`

Berikut adalah contoh CLI dengan query opsi yang membatasi hasil kepada pelanggan: AMIs

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --output table
```

Contoh ini menggunakan filter opsi dengan query opsi untuk menemukan Windows AMIs yang dimulai dengan “pelanggan”:

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --filter Attribute=Platform,Value=windows --output table
```

- [Untuk informasi tentang penggunaan kueri CLI, lihat Cara Memfilter Output dengan Opsi --query dan referensi bahasa kueri, Spesifikasi. JMESPath](#)

Temukan grup keamanan (SG) IDs, AMS

Amazon EC2 membuat dan OpenSearch membuat domain CTs memerlukan ID grup keamanan. Ini akan dalam bentuk sg-02ce123456e7893c7. Akun Anda memiliki setidaknya dua grup keamanan default; lihat [Grup keamanan](#). Selain itu, Anda mungkin memiliki grup keamanan yang Anda buat untuk tujuan tertentu. Untuk menemukan grup keamanan Anda:

- AWS Console: Gunakan konsol EC2 atau VPC untuk melihat semua grup keamanan untuk VPC yang dipilih.
- API/CLI (saat masuk ke akun AMS Anda):

Buat daftar grup keamanan Anda:

```
aws ec2 describe-security-groups
```

Temukan entitas IAM di AMS

Akun Anda memiliki Peran dan Kebijakan IAM default; lihat [Peran pengguna IAM di AMS](#) dan profil instans IAM default; lihat [EC2 Profil instans IAM](#) dengan kebijakan default. Untuk menemukan peran dan kebijakan IAM Anda:

- Konsol: Gunakan konsol IAM untuk melihat semua kebijakan dan peran IAM untuk akun Anda.
- API/CLI (saat masuk ke akun AMS Anda):

Note

AMS CLI harus diinstal agar perintah ini berfungsi. Untuk menginstal AMS API atau CLI, buka halaman Sumber Daya Pengembang konsol AMS. Untuk materi referensi tentang AMS CM API atau AMS SKMS API, lihat bagian Sumber Informasi AMS di Panduan Pengguna. Anda mungkin perlu menambahkan `--profile` opsi untuk otentikasi; misalnya, `aws amsskms ams-cli-command --profile SAML`. Anda mungkin juga perlu menambahkan `--region` opsi karena semua perintah AMS kehabisan `us-east-1`; misalnya, `aws amscm ams-cli-command --region=us-east-1`

Buat daftar peran Anda:

```
aws --profile saml iam list-roles
```

Buat daftar kebijakan Anda:

```
aws --profile saml iam list-role-policies --role-name ROLE_NAME
```

Temukan tumpukan IDs di AMS

Untuk menemukan Stack ID, Anda dapat menggunakan EC2 konsol Amazon, konsol AMS, atau AMS SKMS API/CLI.

Konsol AMS:

- Di panel navigasi, pilih RFCs, lalu klik RFC yang membuat tumpukan. Gunakan opsi filter di bagian atas untuk mengurangi daftar. Halaman detail RFC terbuka dan menyertakan keluaran run dengan ID tumpukan.
- Atau, Anda dapat memilih Tumpukan di panel navigasi untuk membuka halaman daftar tumpukan, dan kemudian halaman melalui daftar tumpukan ke tumpukan yang Anda minati. Metode ini lebih berguna jika Anda mengetahui subjek tumpukan yang Anda cari.

EC2 Konsol Amazon:

Di panel navigasi, pilih Instans atau Load Balancer atau Grup Auto Scaling.

AMS SKMS API ListStackSummaries atau CLI:

Note

AMS CLI harus diinstal agar perintah ini berfungsi. Untuk menginstal AMS API atau CLI, buka halaman Sumber Daya Pengembang konsol AMS. Untuk materi referensi tentang AMS CM API atau AMS SKMS API, lihat bagian Sumber Informasi AMS di Panduan Pengguna. Anda mungkin perlu menambahkan `--profile` opsi untuk otentikasi; misalnya, `aws amsskms ams-cli-command --profile SAML`. Anda mungkin juga perlu menambahkan `--region` opsi karena semua perintah AMS kehabisan `us-east-1`; misalnya, `aws amscm ams-cli-command --region=us-east-1`

Note

Titik akhir AMS API/CLI (`amscm` dan `amsskms`) berada di Wilayah AWS N. Virginia, `us-east-1`. Bergantung pada cara autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan `--profile saml`, jika itu adalah metode otentikasi Anda.

Untuk melihat daftar tumpukan di akun saat ini, jalankan `ListStackSummaries` pengoperasian API SKMS (CLI): `list-stack-summaries`. Untuk mendapatkan informasi lengkap tentang instance stack tertentu, by `StackId`, run `GetStack`.

- Dalam contoh berikut, perintah pertama meminta daftar ringkasan untuk semua instance tumpukan di akun. Perintah kedua meminta daftar instance tumpukan, dengan filter kueri untuk mencantumkan hanya yang dari template tumpukan tertentu, dan menampilkan `VpcId`, Nama, dan `StackId`.

```
aws amsskms list-stack-summaries --output table
```

```
-----
```



```

|                                     ListStackSummaries                                     |
|                                     StackSummaries                                     |
+-----+-----+-----+-----+
| VpcId      | StackId      | StackTemplateId | Name      |
+-----+-----+-----+-----+
| vpc-0123abcd| stack-1fb7fe2212345678| stm-sdhopvbb123456789| Test ELB |
| vpc-0123abcd| stack-8323cc0e12345678| stm-s2b72beb123456789| S3 store |
| vpc-0123abcd| stack-2309fa0712345678| stm-sdhopvbb123456789| ELB      |
| vpc-0123abcd| stack-5e61a70512345678| stm-sdpabqbb123456789| PatchSim |
| vpc-0123abcd| stack-bd0e080d12345678| stm-s2b72beb123456789| CLI demo |
+-----+-----+-----+-----+

```

Untuk informasi tentang penggunaan kueri CLI, lihat [Cara Memfilter Output dengan Opsi --query dan referensi bahasa kueri, Spesifikasi.. JMESPath](#)

Note

Untuk informasi tentang penggunaan instance IDs untuk akses, lihat juga [Mengakses instance menggunakan benteng](#).

Temukan contoh IDs atau alamat IP di AMS

- Untuk meminta akses ke instance, masuk ke instance, atau membuat AMI, Anda harus memiliki ID instans. Untuk sebuah EC2 instance (baik instance mandiri atau bagian dari tumpukan), atau instance database, Anda dapat menemukan ID dalam beberapa cara berbeda:
 - Konsol AMS untuk instance dalam tumpukan ASG: Lihat di halaman detail RFC untuk RFC yang membuat tumpukan. Di bagian Output Eksekusi, Anda akan menemukan ID tumpukan untuk tumpukan ASG dan Anda kemudian dapat pergi ke halaman EC2 Console Auto Scaling Groups dan mencari ID tumpukan itu dan menemukan instance untuk itu. Ketika Anda menemukan instance, pilih dan area terbuka di bagian bawah halaman dengan detail, termasuk alamat IP.
 - Konsol AMS untuk instance mandiri EC2 atau database (DB): Lihat di halaman detail RFC untuk RFC yang membuat instans EC2 stack atau DB. Di bagian Output Eksekusi, Anda akan menemukan ID Instans dan alamat IP.
 - EC2 Konsol AWS:
 1. Di panel navigasi, pilih Instans. Halaman Instances terbuka.

2. Klik contoh yang Anda inginkan ID untuk. Halaman detail instance membuka dan menampilkan ID dan alamat IP.
- Konsol Database AWS:
 1. Pada halaman Beranda, pilih Instans DB. Halaman Instances terbuka.
 2. Filter untuk instance DB yang Anda inginkan ID untuk. Halaman detail instance membuka dan menampilkan ID.
 - AMS CLI/API.

Note

AMS CLI harus diinstal agar perintah ini berfungsi. Untuk menginstal AMS API atau CLI, buka halaman Sumber Daya Pengembang konsol AMS. Untuk materi referensi tentang AMS CM API atau AMS SKMS API, lihat bagian Sumber Informasi AMS di Panduan Pengguna. Anda mungkin perlu menambahkan `--profile` opsi untuk otentikasi; misalnya, `aws amsskms ams-cli-command --profile SAML`. Anda mungkin juga perlu menambahkan `--region` opsi karena semua perintah AMS kehabisan `us-east-1`; misalnya, `aws amscm ams-cli-command --region=us-east-1`

Note

Titik akhir AMS API/CLI (`amscm` dan `amsskms`) berada di Wilayah AWS N. Virginia, `us-east-1` Bergantung pada bagaimana autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan `--profile saml`, jika itu adalah metode otentikasi Anda.

Jalankan perintah berikut untuk mendapatkan detail output eksekusi stack:

```
aws amsskms get-stack --stack-id STACK_ID
```

Outputnya terlihat mirip dengan ini dengan `InstanceID` muncul di dekat bagian bawah, di bawah `Outputs` (nilai yang ditampilkan adalah contoh):

```
{
  "Stack": {
    "StackId": "stack-7fa52bd5eb8240123",
    "Status": {
      "Id": "CreateCompleted",
      "Name": "CreateCompleted"
    },
    "VpcId": "vpc-01234567890abcdef",
    "Description": "Amazon",
    "Parameters": [
      {
        "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
        "Key": "SecurityGroups"
      },
      {
        "Value": "subnet-01234567890abcdef",
        "Key": "InstanceSubnetId"
      },
      {
        "Value": "t2.large",
        "Key": "InstanceType"
      },
      {
        "Value": "ami-01234567890abcdef",
        "Key": "InstanceAmiId"
      }
    ],
    "Tags": [],
    "Outputs": [
      {
        "Value": "i-0b22a22eec53b9321",
        "Key": "InstanceId"
      },
      {
        "Value": "10.0.5.000",
        "Key": "InstancePrivateIP"
      }
    ],
    "StackTemplateId": "stm-s6xvs0000000000000",
    "CreatedTime": "1486584508416",
    "Name": "Amazon"
  }
}
```

}

Temukan Nama Sumber Daya Amazon (ARNs) di AMS

Nama Sumber Daya Amazon (ARN) adalah string yang secara unik mengidentifikasi AWS sumber daya, seperti EC2 instance, bucket S3, akun, fungsi Lambda, dan sebagainya. AWS memerlukan ARN saat Anda ingin menentukan sumber daya secara jelas di semua AWS, seperti dalam kebijakan IAM, tag Amazon Relational Database Service (Amazon RDS), dan panggilan API. ARNs dibangun dari pengidentifikasi yang menentukan layanan, Wilayah, akun, dan informasi lainnya. Ada tiga format ARN:

```
arn:aws:service:region:account-id:resource-id
arn:aws:service:region:account-id:resource-type/resource-id
arn:aws:service:region:account-id:resource-type:resource-id
```

Note

Format yang tepat dari ARN tergantung pada layanan dan jenis sumber daya. [Untuk mempelajari selengkapnya ARNs, lihat Nama Sumber Daya Amazon \(ARNs\) dan Ruang Nama AWS Layanan dan Format ARN.](#)
[Untuk contoh format ARN menurut sumber daya, lihat tabel tipe sumber daya Referensi Otorisasi AWS Layanan.](#)

Menemukan ARN objek AWS bisa jadi sulit. Berikut adalah tiga cara untuk mencoba:

- Konsol layanan AWS: Buka konsol layanan AWS yang relevan, cari sumber daya dan temukan ARN di detail untuk sumber daya.
- AWS API/CLI (Anda harus menginstal AWS CLI terlebih dahulu): Cari layanan yang relevan di [Referensi Perintah AWS CLI](#), lalu, tergantung pada layanan AWS, cari operasi yang relevan, seperti, atau `describeget`, dan sebagainya. Misalnya, untuk semua peran, kebijakan, dan pengguna IAM, Anda bisa mendapatkan ARN dalam output dari CLI dengan:

```
aws iam get-role --role-name EMR_DefaultRole
```

- Buat ARN berdasarkan format yang relevan: Temukan format ARN untuk sumber daya, dengan melihat halaman [Tindakan, sumber daya, dan kondisi untuk layanan AWS, menemukan layanan](#)

[yang relevan, dan kemudian tindakan yang relevan, dan menelusuri ke format ARN sumber](#) daya. Setelah Anda memiliki format, ganti variabel dengan pengaturan yang relevan.

Anda dapat membuat ARN sendiri dengan mengikuti format yang sesuai (format berubah per layanan dan jenis sumber daya) dan mengisi informasi. Berikut adalah beberapa contoh ARN:

- Akun AWS ARN memiliki sintaks berikut:

```
arn:aws:iam::ACCOUNT-ID:root
```

- ARN S3 memiliki hierarki bucket dan objek terkait yang datar:

```
arn:aws:s3:::ams-bucket
```

- EC2 ARN memiliki sub sumber daya seperti gambar, grup keamanan, instance, dan sebagainya. Contoh ini mencakup ID instance di akhir:

```
arn:aws:ec2:us-east-1:123456789012:instance/i-012abcd34efghi56
```

- Lambda ARN memiliki nama fungsi untuk bagian resource-id, dan Anda mungkin perlu menyertakan nomor versi di bagian akhir, seperti yang ditunjukkan dalam contoh ini:

```
arn:aws:lambda:us-east-1:123456789012:function:api-function:1
```

AWS Key Management Service Layanan ini menyediakan informasi ini: [Menemukan ID kunci dan kunci ARN](#).

[Untuk menemukan ARN dari tabel DynamoDB, gunakan CLI tabel deskripsikan DynamoDB.](#)

Untuk melihat temuan orang luar AWS ARNs, lihat [AWS ARN Explained: Amazon](#) Resource Name Guide.

Temukan sumber daya oleh ARN di AMS

Amazon Resource Names (ARNs) mengidentifikasi AWS sumber daya secara unik. [Untuk mempelajari tentang ARNs dan format ARN, lihat Amazon Resource Names \(ARNs\) dan Ruang Nama AWS Layanan dan Format ARN.](#)

 Note

Untuk mendapatkan detail tentang sumber daya dari ARN-nya, Anda harus memiliki akses ke akun yang membuat sumber daya.

Tidak ada jalur langsung AWS untuk mencari semua detail sumber daya dari sumber daya ARN, karena layanan memiliki beberapa jenis sumber daya dengan berbagai informasi terkait. Jika Anda memiliki ARN untuk sumber daya, Anda dapat menentukan:

- AWS Layanan terkait (segmen ARN ketiga) memberi tahu Anda konsol AWS apa yang harus dilihat untuk menemukan sumber daya
- ID sumber daya (segmen ARN keenam atau ketujuh) mengonfirmasi bahwa Anda telah menemukan sumber daya yang tepat

Atau Anda dapat mencari perintah AWS CLI yang tersedia untuk layanan itu di [Referensi Perintah AWS CLI](#) untuk informasi tentang mendapatkan detail tentang sumber daya.

Misalnya, dari ARN berikut, Anda dapat menentukan bahwa layanannya `lambda`, akunnya `123456789012`, jenis sumber dayanya `function`, dan nama fungsinya adalah `TestFunction`

```
arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

Dari sini, Anda dapat meninjau [dokumentasi AWS CLI untuk layanan Lambda](#) untuk mempelajari bagaimana detail lebih lanjut dapat diambil dengan berbagai perintah, seperti `aws lambda get-function` dan `aws lambda get-function-configuration`

Misalnya, Anda dapat menggunakan perintah berikut untuk mendapatkan informasi lebih lanjut tentang fungsi Lambda jika Anda memiliki nama atau ARN:

```
aws lambda get-function-configuration --function-name TestFunction
```

```
aws lambda get-function-configuration --function-name arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

Temukan pengaturan akun AMS

Pengaturan akun yang digunakan untuk membuat AMS RFCs, mengatur jadwal, dan menentukan siapa yang menerima notifikasi.

Beberapa pengaturan dibuat selama orientasi dan memerlukan permintaan layanan untuk diubah. Anda harus mencatat detail akun ini karena Anda akan menggunakannya saat berkomunikasi dengan AMS:

- **Kredensial:** Jika Anda perlu mengambil nama pengguna atau kata sandi AMS Anda, hubungi Administrator TI lokal Anda - AMS menggunakan Direktori Aktif perusahaan Anda.
- **Cloud Service Delivery Manager (CSDM):** Orang ini adalah penghubung Anda dengan AMS dan tersedia untuk menjawab pertanyaan layanan. Anda diberikan informasi kontak orang ini saat orientasi dan harus tetap tersedia untuk semua orang di organisasi Anda yang berinteraksi dengan AMS. Anda dapat mengharapkan untuk menerima laporan bulanan tentang layanan AMS Anda dari orang ini.
- **Akses konsol:** Anda mengakses konsol AMS di URL yang disiapkan khusus untuk akun Anda. Anda bisa mendapatkan URL dari CSDM Anda.
- **AMS CLI:** Anda dapat memperoleh AMS CLI melalui halaman sumber daya Pengembang konsol AMS, atau paket yang dapat didistribusikan yang Anda dapatkan dari CSDM Anda. Setelah Anda memiliki paket yang dapat didistribusikan, ikuti langkah-langkah yang diuraikan dalam [Menginstal atau meningkatkan CLI AMS](#).
- **Jendela pemeliharaan:** Jendela pemeliharaan Anda menentukan kapan penambalan terjadi untuk EC2 instance Anda. AWS Managed Services Maintenance Window (atau Maintenance Window) melakukan aktivitas pemeliharaan untuk AWS Managed Services (AMS) dan berulang pada hari Kamis kedua setiap bulan mulai pukul 15:00 hingga 16:00 Waktu Pasifik. AMS dapat mengubah jendela pemeliharaan dengan pemberitahuan 48 jam. Anda mungkin telah memilih jendela yang berbeda saat onboarding--menyimpan catatan jendela pemeliharaan yang Anda pilih.
- **Pemantauan:** AMS menyediakan satu set CloudWatch metrik secara default, tetapi Anda juga dapat meminta metrik tambahan. Jika Anda melakukannya, catat itu.
- **Log:** Secara default, log Anda disimpan di `ams-a-ACCOUNT_ID-log-management-REGION` di mana **REGION** adalah wilayah tempat log dibuat.
- **Mitigasi:** Saat orientasi, AMS mencatat tindakan mitigasi pilihan Anda jika serangan malware terhadap sumber daya Anda diidentifikasi. Misalnya, hubungi orang-orang tertentu. Pastikan informasi ini tersedia untuk semua orang di organisasi Anda yang berinteraksi dengan AMS.

- Wilayah: Anda dapat melihat halaman detail VPC di konsol AMS. Anda juga dapat menjalankan perintah ini setelah Anda menginstal AMS SKMS CLI (perintah ini menggunakan profil SAFL, hapus jika metode otentikasi Anda berbeda):

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

Important

Note

Titik akhir AMS API/CLI (amscm dan amsskms) berada di Wilayah AWS N. Virginia, us-east-1 Bergantung pada bagaimana autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan `--profile saml`, jika itu adalah metode otentikasi Anda.

Temukan FQDNs di AMS

Jenis perubahan akses AWS Managed Services (AMSCTs) () memerlukan nama domain yang sepenuhnya memenuhi syarat, atau FQDN, dari domain terpercaya AMS Anda, dalam bentuk. C844273800838.amazonaws.com Untuk menemukan AWS FQDN Anda, lakukan salah satu hal berikut:

- AWS Console: Lihat di konsol AWS Directory Service di kolom nama Direktori.
- CLI: Gunakan perintah ini saat masuk ke domain Anda:

Windows (mengembalikan pengguna dan FQDN):

```
whoami /upn
```

atau (DC+DC+DC = FQDN)

```
whoami /fqdn
```


Linux:

```
hostname --fqdn
```

Note

Titik akhir AMS API/CLI (amscm dan amsskms) berada di Wilayah AWS N. Virginia,. us-east-1 Bergantung pada cara autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan `--profile saml`, jika itu adalah metode otentikasi Anda.

Temukan zona ketersediaan (AZs) di AMS

Availability Zone: Semua akun memiliki setidaknya dua zona ketersediaan. Untuk menemukan nama zona ketersediaan Anda secara akurat, Anda harus terlebih dahulu mengetahui ID subnet terkait.

- Konsol AMS: Di panel navigasi klik VPCs, lalu klik VPC yang relevan, jika perlu. Pada halaman VPCs detail, pilih subnet yang relevan dalam tabel subnet untuk membuka halaman detail subnet dengan nama zona ketersediaan terkait.
- AMS SKMS API/CLI:

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

Note

Titik akhir AMS API/CLI (amscm dan amsskms) berada di Wilayah AWS N. Virginia,. us-east-1 Bergantung pada cara autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan `--profile saml`, jika itu adalah metode otentikasi Anda.

Temukan topik SNS di AMS

Topik SNS Anda menentukan siapa yang diberi tahu dalam berbagai keadaan. AMS menyediakan topik SNS untuk notifikasi AMI (lihat notifikasi [AMS AMI dengan SNS](#)), CloudWatch alarm, dan EC2 sumber daya (lihat [Menerima peringatan yang dihasilkan oleh AMS](#)) dan banyak lagi. Untuk menemukan topik SNS Anda yang ada:

- AWS Console: Gunakan konsol SNS untuk melihat semua topik, aplikasi, dan langganan, serta grafik pesan. Juga buat, hapus, berlangganan, dan publikasikan ke topik.
- API/CLI (saat masuk ke akun AMS Anda, memerlukan AWS CLI):

Daftar topik SNS Anda:

```
aws sns list-topics
```

Daftar langganan SNS Anda:

```
aws sns list-subscriptions
```

Note

Titik akhir AMS API/CLI (amscm dan amsskms) berada di Wilayah AWS N. Virginia, us-east-1 Bergantung pada cara autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan `--profile sam1`, jika itu adalah metode otentikasi Anda.

Temukan pengaturan cadangan di AMS

Cadangan dan snapshot dikelola oleh AMS melalui layanan asli. [AWS Backup](#)

Konfigurasi dikelola melalui AWS Backup rencana. Anda dapat memiliki beberapa AWS Backup paket yang mengaitkan sumber daya yang ditandai dengan jadwal cadangan dan kebijakan penyimpanan. Untuk menemukan AWS Backup pengaturan akun AMS Anda, gunakan konsol <https://console.aws.amazon.com/backup>, atau AWS CLI Command Reference [untuk](#) perintah cadangan.

Untuk informasi selengkapnya tentang AMS dan AWS Backup, lihat [Manajemen Kontinuitas](#).

Manajemen akses di AMS

Pelajari cara mengakses sumber daya dengan menggunakan SSH, atau protokol desktop jarak jauh (RDP), dan cara menggunakan bastion.

Sistem manajemen akses AWS Managed Services (AMS) dikonfigurasi selama orientasi. Hanya pengguna dengan peran pengguna AMS IAM, yang digabungkan melalui AMS, yang dapat mengakses sumber daya AMS di akun.

Selain kepercayaan federasi, yang dijelaskan selanjutnya, kelompok keamanan AMS adalah elemen penting dalam akses aplikasi pribadi dan publik. Untuk informasi tentang grup keamanan AMS dan cara mengubahnya, lihat [Grup keamanan](#).

Topik

- [Apa itu Manajemen Akses?](#)
- [Bagaimana dan kapan menggunakan akun pengguna root di AMS](#)
- [Konsol AMS Advanced dan EC2 akses Amazon](#)
- [Mengakses konsol AWS Manajemen dan konsol AMS](#)
- [Mengakses instance menggunakan benteng](#)

Apa itu Manajemen Akses?

Manajemen akses adalah cara AMS melindungi sumber daya Anda dengan hanya mengizinkan akses yang diotorisasi dan diautentikasi. AMS menggunakan peran pengguna IAM dan profil instans default, serta autentikasi multi-faktor, grup keamanan, nama benteng ramah DNS, dan lainnya untuk menjaga sumber daya Anda tetap terlindungi.

AMS berfokus pada tiga jenis akses yang memerlukan manajemen:

- Akses konsol: Dengan memanfaatkan federasi, pengguna di Active Directory akun dapat mengakses konsol menggunakan sistem masuk tunggal (SSO). Jika Anda memiliki otentikasi multi-faktor yang dikonfigurasi untuk akun ini, Anda dapat terus meminta MFA untuk mendapatkan akses ke konsol.
- Akses instans dengan RDP atau SSH: Memanfaatkan kepercayaan Active Directory, pengguna di Active Directory akun yang ada dapat meminta akses ke instance, dan kemudian berhasil mengautentikasi ke bastion dan instance dengan menggunakan kredensi perusahaan yang ada.

Jika Anda memiliki otentikasi multi-faktor yang dikonfigurasi untuk akun tersebut, Anda dapat terus meminta MFA untuk meminta akses ke instans. AMS menggunakan solusi MFA sendiri untuk membatasi akses insinyur AMS ke instance.

- Akses aplikasi: Bervariasi berdasarkan kasus penggunaan.

Topik

- [Mengapa dan kapan AMS mengakses akun Anda](#)

Mengapa dan kapan AMS mengakses akun Anda

AWS Managed Services (AMS) mengelola infrastruktur AWS Anda dan terkadang, karena alasan tertentu, operator dan administrator AMS mengakses akun Anda. Peristiwa akses ini didokumentasikan dalam log AWS CloudTrail (CloudTrail) Anda.

Mengapa, kapan, dan bagaimana AMS mengakses akun Anda dijelaskan dalam topik berikut.

Pemicu akses akun pelanggan AMS

Aktivitas akses akun pelanggan AMS didorong oleh pemicu. Pemicu hari ini adalah AWS tiket yang dibuat dalam sistem manajemen masalah kami sebagai respons terhadap alarm dan peristiwa Amazon CloudWatch (CloudWatch), serta laporan insiden atau permintaan layanan yang Anda kirimkan. Beberapa panggilan layanan dan aktivitas tingkat host dapat dilakukan untuk setiap akses.

Pembenaran akses, pemicu, dan inisiator pemicu tercantum dalam tabel berikut.

Pemicu Akses

Akses	Inisiator	Pemicu
Menambal	AMS	Masalah tambalan
Penyebaran infrastruktur	AMS	Masalah penyebaran
Investigasi masalah internal	AMS	Masalah masalah (masalah yang telah diidentifikasi sebagai sistemik)

Akses	Inisiator	Pemicu
Investigasi dan remediasi peringatan	AMS	Item kerja operasional AWS Systems Manager (SSM OpsItems)
Eksekusi RFC manual	Anda	Masalah Request for Change (RFC). (Non-otomatis RFCs mungkin memerlukan akses AMS ke sumber daya Anda)
Investigasi dan remediasi insiden	Anda	Kasus dukungan masuk (insiden atau permintaan layanan yang Anda kirimkan)
Pemenuhan permintaan layanan masuk	Anda	

Akun pelanggan AMS mengakses peran IAM

Saat dipicu, AMS mengakses akun pelanggan menggunakan peran AWS Identity and Access Management (IAM). Seperti semua aktivitas di akun Anda, peran dan penggunaannya masuk CloudTrail.

Important

Jangan memodifikasi atau menghapus peran ini.

Peran IAM untuk akses AMS ke akun pelanggan

Nama Peran	Jenis Akun (SALZ, Manajemen MALZ, Aplikasi MALZ, dll.)	Deskripsi
ams-service-admin	SALZ, MALZ	Akses otomatisasi layanan AMS dan penerapan infrastruktur otomatis misalnya Patch, Backup, Remediasi Otomatis.

Nama Peran	Jenis Akun (SALZ, Manajemen MALZ, Aplikasi MALZ, dll.)	Deskripsi
ams-application-infra-read-hanya	SALZ, Aplikasi MALZ, Aplikasi Alat MALZ	Operator hanya membaca akses
ams-application-infra-operations		Akses operator untuk incidents/service permintaan
ams-application-infra-admin		Akses Admin AD
ams-primary-read-only	Manajemen MALZ	Operator hanya membaca akses
ams-primary-operations		Akses operator untuk incidents/service permintaan
ams-primary-admin		Akses Admin AD
ams-logging-read-only	Penebangan MALZ	Operator hanya membaca akses
ams-logging-operations		Akses operator untuk incidents/service permintaan
ams-logging-admin		Akses Admin AD
ams-networking-read-only	Jaringan MALZ	Operator hanya membaca akses
ams-networking-operations		Akses operator untuk incidents/service permintaan
ams-networking-admin		Akses Admin AD
ams-shared-services-read-hanya	Layanan Bersama MALZ	Operator hanya membaca akses

Nama Peran	Jenis Akun (SALZ, Manajemen MALZ, Aplikasi MALZ, dll.)	Deskripsi
ams-shared-services-operations		Akses operator untuk incidents/service permintaan
ams-shared-services-admin		Akses Admin AD
ams-security-read-only	Keamanan MALZ	Operator hanya membaca akses
ams-security-operations		Akses operator untuk incidents/service permintaan
ams-security-admin		Akses Admin AD
ams-access-security-analyst	SALZ, Aplikasi MALZ, Aplikasi Alat MALZ, MALZ Core	Akses Keamanan AMS
ams-access-security-analyst-baca-saja		AMS Security, akses hanya baca
Sentinel_ _Peran_ 0 MBHe AdminUser PXHaz RQadu PVc CDc	SALZ	[BreakGlassRole] Digunakan untuk BreakGlass ke akun pelanggan
Sentinel_ _Peran_ S0 0 PowerUser wZuPu ROOI IazDb RI9	SALZ, MALZ	Akses Poweruser ke akun pelanggan untuk eksekusi RFC
Sentinel_ ReadOnlyUser _peran_pd4l6rw9rd0lnlkd5 JOo		ReadOnly akses ke akun pelanggan untuk eksekusi RFC
ams_admin_role		Akses admin ke akun pelanggan untuk eksekusi RFC

Nama Peran	Jenis Akun (SALZ, Manajemen MALZ, Aplikasi MALZ, dll.)	Deskripsi
AWSManagedServices_Provisioning_CustomerStacksRole		Digunakan untuk meluncurkan dan memperbarui tumpukan CFN atas nama pelanggan melalui Ingest CloudFormation
customer_ssm_automation_role		Peran diteruskan oleh eksekusi CT ke SSM Automation untuk eksekusi runbook
ams_ssm_automation_role	SALZ, Aplikasi MALZ, MALZ Core	Peran diteruskan oleh layanan AMS ke SSM Automation untuk eksekusi runbook
ams_ssm_iam_deployment_role	Aplikasi MALZ	Peran yang digunakan oleh katalog IAM
ams_ssm_shared_services_intermediary_role	Layanan Bersama MALZ	Peran yang digunakan oleh aplikasi ams_ssm_automation_role untuk mengeksekusi Dokumen SSM tertentu di akun Layanan Bersama
AmsOpsCenterRole		Digunakan untuk membuat dan memperbarui OpsItems di akun pelanggan
AMSOpsItemAutoExecutionRole	SALZ, MALZ	Digunakan untuk mendapatkan Dokumen SSM, menjelaskan tag sumber daya, memperbarui OpsItems, dan memulai otomatisasi
customer-mc-ec2-instance-profil		Profil EC2 contoh pelanggan default (peran)

Meminta akses instans

Untuk mengakses sumber daya, Anda harus terlebih dahulu mengirimkan permintaan untuk perubahan (RFC) untuk akses tersebut. Ada dua jenis akses yang dapat Anda minta: admin (izin baca/tulis) dan read-only (akses pengguna standar). Akses berlangsung selama delapan jam, secara default. Informasi ini diperlukan:

- Stack ID, atau set stack IDs, untuk instance atau instance yang ingin Anda akses.
- Nama domain yang sepenuhnya memenuhi syarat dari domain tepercaya AMS Anda.
- Nama pengguna Active Directory dari orang yang menginginkan akses.
- ID VPC tempat tumpukan yang ingin Anda akses.

Setelah Anda diberikan akses, Anda dapat memperbarui permintaan sesuai kebutuhan.

Untuk contoh cara meminta akses, lihat [Stack Admin Access | Grant](#) atau [Stack Read-only Access | Grant](#).

Bagaimana dan kapan menggunakan akun pengguna root di AMS

[Pengguna root](#) adalah superuser di dalam AWS akun Anda. AMS memonitor penggunaan root. Kami menyarankan Anda menggunakan root hanya untuk beberapa tugas yang memerlukannya, misalnya: mengubah pengaturan akun Anda, mengaktifkan akses AWS Identity and Access Management (IAM) ke penagihan dan manajemen biaya, mengubah kata sandi root Anda, dan mengaktifkan otentikasi multi-faktor (MFA). Lihat [Tugas yang memerlukan kredensi pengguna root](#) di AWS Identity and Access Management Panduan Pengguna.

Note

MFA diaktifkan selama onboarding AMS Advanced untuk secara khusus melarang akses pengguna root. Akses root di akun yang dikelola AMS berbeda dari AWS akun lain, dan sangat penting untuk keamanan seluruh lingkungan yang dikelola AMS Anda. MFA yang dikonfigurasi adalah MFA virtual dan dilakukan menggunakan perangkat milik AMS. Setelah MFA virtual dikonfigurasi dengan bantuan AMS, token virtual segera dihapus. Ini memastikan bahwa baik Anda maupun AMS tidak mempertahankan kemampuan untuk masuk ke akun sebagai pengguna root. Login root hanya dapat diaktifkan kembali pada permintaan khusus (dijelaskan selanjutnya) dan AMS mengharapkan akses tersebut hanya digunakan jika benar-

benar diperlukan. Untuk informasi tentang MFA, lihat [Amankan Akun Baru dengan Otentikasi Multi-Faktor](#).

Akses root selalu memicu respons tim AMS Security and Operations. AMS memantau panggilan API untuk akses root, dan alarm dipicu jika akses tersebut terdeteksi.

Meminta akses root sedikit berbeda antara jenis akun AMS.

Akses root dengan landing zone akun tunggal AMS Advanced:

Jika Anda memiliki landing zone akun tunggal, hubungi manajer pengiriman layanan cloud (CSDM) dan arsitek cloud (CAs) untuk memberi tahu mereka tentang pekerjaan akses root yang Anda butuhkan. Yang terbaik adalah memberikan pemberitahuan dua puluh empat jam sebelum kegiatan yang diusulkan.

Akses root dengan landing zone multi-akun AMS Advanced:

Untuk aplikasi multi-akun landing zone, Shared Services, Security, atau akun Networking, gunakan tipe perubahan Management | Other | Other (ct-1e1xtak34nx76). Sertakan tanggal, waktu, dan tujuan menggunakan kredensial pengguna root dan jadwalkan RFC untuk memastikan memberikan pemberitahuan dua puluh empat jam sebelum aktivitas yang diusulkan. Gunakan akun Manajemen landing zone multi-akun Anda untuk mengirimkan RFC.

Selain itu, hubungi CSDM Anda dan CAs dua puluh empat jam sebelumnya, untuk memberi tahu mereka tentang pekerjaan akses root yang Anda butuhkan.

Operasi AMS dan respons keamanan terhadap penggunaan root:

AMS menerima alarm saat akun pengguna root digunakan. Jika penggunaan kredensial root tidak terjadwal, mereka menghubungi tim Keamanan AMS, dan tim akun Anda, untuk memverifikasi apakah ini aktivitas yang diharapkan. Jika bukan aktivitas yang diharapkan, AMS bekerja sama dengan tim Keamanan Anda untuk menyelidiki masalah tersebut.

Konsol AMS Advanced dan EC2 akses Amazon

Mengakses konsol AMS Advanced.

Mengakses EC2 instans Amazon Anda.

Kirim permintaan akses:

Masuk ke EC2 instans AMS Amazon Anda:

Mengakses konsol AWS Manajemen dan konsol AMS

Selama orientasi, Anda diberikan login ke konsol AWS Manajemen (dengan hak istimewa terbatas: Anda dapat menulis ke konsol AMS, dan beberapa bidang di halaman informasi pelanggan Anda). Anda dapat mengakses konsol AMS dengan memilih tautan Managed Services di konsol AWS Manajemen. Baik akses federasi atau kredensi bersama (nama pengguna/kata sandi) disiapkan sesuai kesepakatan dengan tim administrasi TI Anda. Untuk pembuatan akun atau grup lebih lanjut, kirimkan permintaan layanan ke AMS.

Untuk informasi tentang mendapatkan akses ke konsol AWS Manajemen, lihat [Bekerja dengan konsol AWS Manajemen](#).

Untuk beberapa tips tentang menggunakan konsol AMS, lihat [Menggunakan konsol AMS](#).

Akses konsol AMS sementara

Jika Anda belum menyiapkan penyedia identitas (misalnya, SAMP) untuk mengautentikasi ke AMS, Anda bisa mendapatkan akses sementara ke konsol AMS. Hubungi CSDM Anda untuk memiliki Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat permintaan perubahan entitas atau kebijakan (ct-3dpd8mdd9jn1r) yang dikirimkan atas nama Anda dengan nilai-nilai berikut:

- **UserName:** Nama untuk entitas pengguna IAM yang Anda buat
- **AccessType:** “Akses konsol”
- **UserPermissions:** “Akses konsol AMS sementara untuk **USERNAME** (orang yang ingin Anda akses sementara)”
- **Pemberitahuan email:** Alamat email Anda, sehingga Anda dapat menyetujui permintaan saat AMS meminta Anda

 Note

RFC untuk akses Konsol AMS sementara ini memerlukan tinjauan keamanan dan penerimaan oleh tim keamanan internal Anda dan AMS Global Security.

Setelah permintaan ini selesai, dan Anda dapat masuk, Anda harus menyetujui RFC yang dibuat, untuk melacak persetujuan dan mengizinkan tim AMS untuk menutup pekerjaan. Untuk menyetujui RFC, temukan di halaman daftar RFC (akan ada tanda Persetujuan Tertunda di sebelahnya), pilih untuk membuka halaman detail RFC untuk RFC itu, lalu pilih Menyetujui. Perhatikan bahwa Anda tidak akan dapat menggunakan AMS sampai RFC disetujui.

Ketika RFC berhasil diselesaikan, operasi AMS memberi Anda pengguna IAM baru dan kata sandi. Kemudian ikuti langkah-langkah ini:

1. Buka konsol AWS Manajemen dan masuk dengan kredensi yang disediakan. Anda akan diminta untuk membuat kata sandi baru. Anda juga harus, setelah login, menyiapkan otentikasi multi-faktor (MFA); untuk mempelajari lebih lanjut tentang melakukan itu, lihat [Menggunakan Multi-Factor Authentication \(MFA\)](#) di. AWS
2. Di konsol AWS Manajemen, ubah ke peran IAM yang disediakan (customer_*CustomerCode*_readonly_user_role).
3. Buka AMS Managed Services Console.

 Note

Akses sementara default hingga enam puluh hari; namun, Anda dapat meminta perpanjangan tiga puluh hari dengan menghubungi CSDM Anda.

Mengakses instance menggunakan benteng

Semua akses ke sumber daya di dalam akun yang dikelola AMS, baik untuk pelanggan maupun operator AMS, dijamin oleh penggunaan host bastion. Kami memelihara benteng RDP Linux dan Windows untuk akses untuk akun AMS Advanced multi-account landing zone (MALZ) dan Single-account landing zone (SALZ) AMS Advanced.

Benteng Anda hanya dapat diakses melalui koneksi pribadi Anda (VPN atau AWS Direct Connect) DX. Selain firewall untuk mencegah lalu lintas masuk, benteng secara teratur disediakan ulang (dengan kredensi yang ada) pada jadwal tetap.

 Note

Untuk informasi tentang memindahkan file ke EC2 instans, lihat [Transfer file: Windows lokal atau PC MAC ke Linux Amazon EC2](#).

MALZ

Anda mengakses instans akun Anda dengan masuk ke instans bastion dengan kredensial Active Directory (AD) Anda. Amazon menggunakan benteng yang terletak di VPC jaringan perimeter (akun jaringan), dan Anda menggunakan benteng pelanggan Anda, yang terletak di subnet Customer Bastions Anda di akun layanan bersama.

Ketika lingkungan AMS Anda awalnya onboard, Anda memiliki dua bastion SSH dan dua benteng RDP tergantung pada pilihan Anda.

SALZ

Anda mengakses instans akun Anda dengan masuk ke instans bastion dengan kredensial Active Directory (AD) Anda. AMS menggunakan benteng yang terletak di subnet jaringan perimeter, dan Anda menggunakan benteng yang terletak di subnet pribadi Anda.

Ketika akun Anda awalnya onboard, Anda memiliki dua benteng RDP dan dua SSH, secara default.

 Note

Sebagai bagian dari landing zone akun tunggal, AMS menyediakan benteng RDP (Windows) dan SSH (Linux) untuk mengakses tumpukan Anda; Namun, Anda dapat memilih apakah Anda hanya menginginkan benteng RDP atau hanya bastion SSH. Untuk meminta agar hanya RDP, atau hanya bastion SSH yang dipertahankan, kirimkan permintaan layanan.

Untuk mengakses instance, Anda perlu:

- Akses diberikan ke tumpukan. Untuk mendapatkan akses yang diberikan ke tumpukan, lihat [Stack Admin Access | Grant](#) atau [Stack Read-Only Access | Grant](#).
- ID tumpukan yang ingin Anda akses sehingga Anda dapat diberikan akses ke instance. Untuk menemukan ID tumpukan, lihat [Temukan tumpukan IDs di AMS](#).
- IP contoh yang ingin Anda akses. Untuk menemukan IP instance, lihat [Temukan contoh IDs atau alamat IP di AMS](#).
- Nama benteng ramah DNS atau IP benteng. Cara menggunakan nama benteng ramah DNS dan cara menemukan IP benteng dijelaskan selanjutnya.

Nama benteng ramah DNS

AWS Managed Services (AMS) menggunakan nama bastion ramah DNS.

MALZ

Untuk multi-account landing zone (MALZ), catatan DNS dibuat untuk bastion di FQDN dari Direktori Aktif yang dikelola AMS. AMS menggantikan benteng Linux dan Windows sesuai kebutuhan. Misalnya, jika ada benteng AMI baru yang harus digunakan, catatan DNS bastion diperbarui secara dinamis untuk menunjuk ke bastion baru yang valid.

1. Untuk mengakses bastion SSH (Linux), gunakan catatan DNS seperti ini:
`sshbastion(1-4).Your_Domain.com`

Misalnya, di mana domain adalah `Your_Domain`:

- `sshbastion1.Your_Domain.com`
- `sshbastion2.Your_Domain.com`
- `sshbastion3.Your_Domain.com`
- `sshbastion4.Your_Domain.com`

2. Untuk mengakses benteng RDP (Windows), gunakan catatan DNS seperti ini:
`rdp-Username.Your_Domain.com`

Misalnya, di mana nama pengguna adalah `alex`, `test`, `demo`, atau `bob`, dan domain adalah `Your_Domain.com`:

- `rdp-alex.Your_Domain.com`
- `rdp-test.Your_Domain.com`

- `rdp-demo.Your_Domain.com`
- `rdp-bob.Your_Domain.com`

SALZ

Single-account landing zone (SALZ) menggantikan benteng Linux dan Windows sesuai kebutuhan. Misalnya, jika ada benteng AMI baru yang harus digunakan, catatan DNS bastion diperbarui secara dinamis untuk menunjuk ke bastion baru yang valid.

1. Untuk mengakses bastion SSH (Linux), gunakan catatan DNS seperti ini:
`sshbastion(1-4).AccountNumber.amazonaws.com`.

Misalnya, di 123456789012 mana nomor akun:

- `sshbastion1.A123456789012.amazonaws.com`
- `sshbastion2.A123456789012.amazonaws.com`
- `sshbastion3.A123456789012.amazonaws.com`
- `sshbastion4.A123456789012.amazonaws.com`

2. Untuk mengakses benteng RDP (Windows), gunakan catatan DNS seperti ini:
`rdpbastion(1-4).ACCOUNT_NUMBER.amazonaws.com`

Misalnya, di 123456789012 mana nomor akun:

- `rdpbastion1.A123456789012.amazonaws.com`
- `rdpbastion2.A123456789012.amazonaws.com`
- `rdpbastion3.A123456789012.amazonaws.com`
- `rdpbastion4.A123456789012.amazonaws.com`

Menghemat biaya pada benteng single-account landing zone (SALZ)

AMS menyediakan dua bastion SSH dan dua benteng RDP dalam konfigurasi default agar Anda dapat terhubung ke EC2 instans Amazon, dan juga menyebarkan dua benteng DMZ dalam konfigurasi default untuk operasi layanan. Benteng menggunakan m4. EC2 instans Amazon besar secara default. Anda memiliki opsi untuk mengubah EC2 instans Amazon yang digunakan untuk bastion ke t3.small, dan menghemat biaya.

Jika Anda menggunakan instans sesuai permintaan, atau instans spot, atau rencana tabungan, Anda harus mempertimbangkan fitur ini, dan menghemat biaya. Jika Anda menggunakan Instans Cadangan, pertimbangkan jika menggunakan instans t3.small dapat menurunkan biaya Anda. Untuk mengubah jenis instans, kirimkan RFC dengan Management | Advanced stack components | EC2 instance stack | Resize (ct-15mazjj88xc69) CT dari akun AMS Anda.

Hubungi manajer pengiriman layanan cloud (CSDM) Anda untuk pertanyaan tambahan, atau untuk memeriksa apakah Anda dapat memanfaatkan fitur ini.

Menggunakan alamat IP bastion

Pelanggan AMS dapat menggunakan bastion SSH dan RDP, baik yang [Nama benteng ramah DNS](#) dijelaskan sebelumnya, atau alamat IP bastion.

Untuk menemukan alamat IP bastion, SSH dan RDP, untuk akun Anda:

1. Hanya untuk landing zone multi-akun: Masuk ke akun Layanan Bersama.
2. Buka EC2 Console dan pilih Running Instances.

Halaman Instances terbuka.

3. Di kotak filter di bagian atas, masukkan ssh-bastion atau rdp-bastion.

Di kotak filter di bagian atas, masukkan customer-ssh atau customer-rdp.

Benteng SSH and/or RDP untuk tampilan akun Anda.

Perhatikan bahwa selain bastion SSH Anda, Anda mungkin melihat benteng jaringan perimeter AMS dalam daftar, yang tidak tersedia untuk ini.

4. Pilih benteng SSH atau RDP. Jika Anda menggunakan komputer Windows dan ingin masuk ke instance Linux, Anda menggunakan bastion SSH. Jika Anda ingin masuk ke instance Windows, Anda menggunakan benteng RDP. Jika Anda menggunakan OS Linux dan ingin masuk ke instance Windows, Anda menggunakan benteng SSH melalui terowongan RDP (ini agar Anda dapat mengakses desktop Windows). Untuk mengakses instance Linux dari OS Linux, Anda menggunakan bastion SSH.

Contoh akses instans di AMS

Contoh-contoh ini menunjukkan cara masuk ke instans di akun AMS Anda dengan menggunakan benteng setelah Anda diberikan akses melalui RFC. Untuk informasi tentang mendapatkan akses yang diberikan, lihat [Meminta akses instans](#).

Note

Untuk informasi tentang memindahkan file ke EC2 instans, lihat [Transfer file: Windows lokal atau PC MAC ke Linux Amazon EC2](#).

Data yang dibutuhkan:

- Nama atau alamat IP yang ramah DNS Bastion: Gunakan nama ramah DNS seperti yang dijelaskan dalam [Nama benteng ramah DNS](#) atau temukan alamat IP benteng seperti yang dijelaskan dalam [Menggunakan alamat IP bastion](#)

Note

EC2 Instans Amazon yang dibuat melalui grup EC2 Auto Scaling Amazon akan memiliki alamat IP yang masuk dan keluar dan Anda harus menggunakan EC2 konsol Amazon Anda untuk menemukan alamat IP tersebut.

- Nama pengguna (misalnya `DOMAIN_FQDN\USERNAME`) dan Kata Sandi: Kredensial untuk akun. `USERNAME` harus nama pengguna Active Directory Anda.

Perhatikan bahwa nama pengguna dalam format `username@customerdomain.com` dapat digunakan tetapi dapat menyebabkan masalah dengan pengaturan PBIS Anda.

- Alamat IP Stack: Temukan ini dengan melihat output run untuk RFC yang Anda kirimkan untuk meluncurkan tumpukan, atau cari alamat IP EC2 instans Amazon di EC2 konsol Amazon. Untuk satu EC2 instance Amazon, Anda juga dapat menggunakan perintah AMS SKMS `ListStackSummaries` untuk menemukan ID tumpukan dan kemudian `GetStack` menemukan alamat IP tumpukan. Untuk referensi AMS SKMS API, lihat tab Laporan di AWS Artifact Console.

Akses alamat IP bastion, baik SSH atau RDP, yang sesuai, dan masuk menggunakan salah satu prosedur berikut.

 Note

Benteng RDP hanya memungkinkan dua koneksi simultan. Jadi, dalam skenario kasus terbaik, hanya 4 admin yang dapat terhubung ke tumpukan windows secara bersamaan. Jika Anda memerlukan lebih banyak koneksi untuk RDP, lihat [Opsi Benteng AMS selama Migrasi Aplikasi/Orientasi di panduan orientasi](#) AMS.

Komputer Linux ke Linux misalnya

Gunakan SSH untuk terhubung ke bastion SSH dan kemudian ke instance Linux.

MALZ

Untuk informasi selengkapnya tentang nama benteng ramah, lihat Benteng [DNS](#).

Untuk terhubung ke instance Linux, Anda harus terlebih dahulu terhubung ke bastion SSH.

1. Buka jendela shell dan masukkan:

```
ssh Domain_FQDN\\Username@SSH_bastion_name  
or SSH_bastion_IP
```

Yang akan terlihat seperti ini jika domain_FQDN Anda adalah "corp.domain.com", nomor akun Anda adalah "123456789123", Your_Domain adalah "amazonaws.com", Anda memilih benteng "4", dan nama pengguna Anda adalah "": JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. Masuk dengan kredensyal Active Directory perusahaan Anda.
3. Ketika disajikan dengan prompt Bash, SSH masuk ke instance, dan kemudian masukkan:

```
ssh Domain_FQDN\\Username@Instance_IP
```

Atau, Anda dapat menggunakan bendera Login (-l):

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

Untuk informasi selengkapnya tentang nama benteng ramah, lihat Benteng [DNS](#).

Untuk terhubung ke instance Linux, Anda harus terlebih dahulu terhubung ke bastion SSH.

1. Buka jendela shell dan masukkan:

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name  
or SSH_BASTION_IP
```

Yang akan terlihat seperti ini jika nomor akun Anda adalah 123456789123, Anda memilih bastion 4, dan nama pengguna Anda adalah: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. Masuk dengan kredensial Active Directory perusahaan Anda.
3. Ketika disajikan dengan prompt Bash, SSH masuk ke instance, dan kemudian masukkan:

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Atau, Anda dapat menggunakan bendera Login (-l):

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Komputer Linux ke instans Windows

Gunakan terowongan SSH dan klien RDP untuk terhubung ke instance Windows dari komputer Linux Anda.

MALZ

Prosedur ini memerlukan klien Remote Desktop Connection untuk Linux; contohnya menggunakan Microsoft Remote Desktop (klien UNIX open source untuk menghubungkan ke Windows Remote Desktop Services). Rdesktop adalah alternatif.

Note

Cara Anda masuk ke instance Windows mungkin berubah berdasarkan klien desktop jarak jauh yang digunakan.

Pertama Anda membuat terowongan SSH, dan kemudian masuk.

Untuk informasi lebih lanjut tentang nama benteng ramah, lihat [Nama benteng ramah DNS](#).

Sebelum Anda memulai:

- Meminta akses ke instans yang ingin Anda sambungkan; untuk informasi, lihat [Permintaan akses](#).
- Pilih nama bastion SSH DNS yang ramah untuk dihubungkan; misalnya:

```
sshbastion(1-4).Your_Domain
```

Yang akan terlihat seperti ini jika domain_fqdn Anda adalah "corp.domain.com", Your_Domain yang dikelola AMS Anda adalah "amazonaws.com", Anda memilih benteng "4", dan nama pengguna Anda adalah "JoeSmith":

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- Temukan alamat IP dari instans yang ingin Anda sambungkan; untuk informasi, lihat [Menemukan ID instans atau alamat IP](#).
1. Siapkan RDP melalui terowongan SSH dari desktop Linux ke instance Windows. Untuk mengeluarkan ssh perintah dengan nilai yang tepat, ada beberapa cara untuk melanjutkan:
 - Di shell Linux, atur variabel, lalu masukkan perintah koneksi SSH:

```
BASTION="sshbastion(1-4).Your_Domain"  
WINDOWS="Windows_Instance_Private_IP"  
AD="AD_Account_Number"  
USER="AD_Username"  
ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
```

Contoh, jika nilai berikut digunakan:

```
BASTION="sshbastion4.A123456789123.amazonaws.com"
```

```
WINDOWS="172.16.3.254"
```

```
AD="ACORP_example"
```

```
USER="john.doe"
```

- Tambahkan nilai variabel langsung ke ssh perintah.

Dalam kedua kasus, inilah permintaan yang dirender (dengan asumsi kumpulan nilai variabel yang sama):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
```

2. Entah: Buka Klien Desktop Jarak Jauh Anda, masukkan alamat dan port loopback, 127.0.0.1:3389, lalu buka koneksi.

Atau, masuk ke instance Windows dari shell desktop Linux baru. Jika Anda menggunakan RDesktop, perintahnya terlihat seperti ini:

```
rdesktop 127.0.0.1:3389
```

Jendela desktop jarak jauh untuk instance Windows muncul di desktop Linux Anda.

Tip

Jika sesi desktop jarak jauh gagal dimulai, verifikasi bahwa konektivitas jaringan ke instance Windows dari bastion SSH diizinkan pada port 3389 dari shell pada langkah 1 (ganti dengan tepat): `private_ip_address_of_windows_instance`

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

Sukses:

```
nc 172.16.0.83 3389 -v -z
    Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
    netstat -anvp | grep 3389
```

```
tcp    0    0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

SALZ

Prosedur untuk landing zone akun tunggal ini memerlukan klien Remote Desktop Connection untuk Linux; contohnya menggunakan Microsoft Remote Desktop (klien UNIX open source untuk menghubungkan ke Windows Remote Desktop Services). Rdesktop adalah alternatif.

Note

Cara Anda masuk ke instance Windows mungkin berubah berdasarkan klien desktop jarak jauh yang digunakan.

Pertama Anda membuat terowongan SSH, dan kemudian masuk.

Untuk informasi lebih lanjut tentang nama benteng ramah, lihat [Nama benteng ramah DNS](#).

Sebelum Anda memulai:

- Meminta akses ke instans yang ingin Anda sambungkan; untuk informasi, lihat [Permintaan akses](#).
- Pilih nama bastion SSH DNS yang ramah untuk dihubungkan; misalnya:

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

Yang akan terlihat seperti ini jika nomor akun Anda 123456789123 dan Anda memilih benteng 4:

```
sshbastion4.A123456789123.amazonaws.com
```

- Temukan alamat IP dari instans yang ingin Anda sambungkan; untuk informasi, lihat [Menemukan ID instans atau alamat IP](#).
1. Siapkan RDP melalui terowongan SSH dari desktop Linux ke instance Windows. Untuk mengeluarkan ssh perintah dengan nilai yang tepat, ada beberapa cara untuk melanjutkan:
 - Di shell Linux, atur variabel, lalu masukkan perintah koneksi SSH:

```
BASTION="sshbastion(1-4).AMSAccountNumber.amazonaws.com"  
WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"  
AD="AD_ACCOUNT_NUMBER"  
USER="AD_USERNAME"  
ssh -L 3389:$WINDOWS:3389 A$AD\\\\"$USER@$BASTION
```

Contoh, jika nilai berikut digunakan:

```
BASTION="sshbastion4.A123456789123.amazonaws.com"
```

```
WINDOWS="172.16.3.254"
```

```
AD="ACORP_example"
```

```
USER="john.doe"
```

- Tambahkan nilai variabel langsung ke ssh perintah.

Dalam kedua kasus, inilah permintaan yang dirender (dengan asumsi kumpulan nilai variabel yang sama):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\n\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. Entah: Buka Klien Desktop Jarak Jauh Anda, masukkan alamat dan port loopback, 127.0.0.1:3389, lalu buka koneksi.

Atau, masuk ke instance Windows dari shell desktop Linux baru. Jika Anda menggunakan RDesktop, perintahnya terlihat seperti ini:

```
rdesktop 127.0.0.1:3389
```

Jendela desktop jarak jauh untuk instance Windows muncul di desktop Linux Anda.

Tip

Jika sesi desktop jarak jauh gagal dimulai, verifikasi bahwa konektivitas jaringan ke instance Windows dari bastion SSH diizinkan pada port 3389 dari shell pada langkah 1 (ganti dengan tepat): `private_ip_address_of_windows_instance`

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

Sukses:

```
nc 172.16.0.83 3389 -v -z
    Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
netstat -anvp | grep 3389
tcp    0      0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

Komputer Windows ke instans Windows

Gunakan klien Windows Remote Desktop Connection untuk terhubung ke instance Windows dari komputer Windows Anda.

MALZ

Untuk informasi lebih lanjut tentang nama benteng ramah, lihat [Nama benteng ramah DNS](#).

1. Buka program Remote Desktop Connection, program Windows standar, dan masukkan nama DNS ramah dari benteng Windows di bidang hostname.
2. Pilih Hubungkan. Remote Desktop Connection mencoba koneksi RDP ke benteng.

Jika berhasil, kotak dialog kredensial terbuka. Untuk mendapatkan akses, gunakan kredensial Active Directory perusahaan Anda, seperti yang Anda lakukan dengan instance Windows.

3. Buka program Remote Desktop Connection di bastion dan masukkan alamat IP instance Windows yang ingin Anda sambungkan (misalnya, 10.0.0.100), lalu pilih Connect. Kredensi Active Directory perusahaan Anda diperlukan lagi sebelum Anda terhubung ke instans Windows.

SALZ

Untuk informasi lebih lanjut tentang nama benteng ramah, lihat [Nama benteng ramah DNS](#).

1. Buka program Remote Desktop Connection, program Windows standar, dan masukkan nama DNS ramah dari benteng Windows di bidang nama host; misalnya `rdpbastion(1-4).AMSAccountNumber.amazonaws.com`, yang akan terlihat seperti ini jika nomor akun Anda 123456789123 dan Anda memilih bastion 4, `rdpbastion4.A123456789123.amazonaws.com`
2. Pilih Hubungkan. Remote Desktop Connection mencoba koneksi RDP ke benteng.

Jika berhasil, kotak dialog kredensial terbuka. Untuk mendapatkan akses, gunakan kredensial Active Directory perusahaan Anda, seperti yang Anda lakukan dengan instance Windows.
3. Buka program Remote Desktop Connection di bastion dan masukkan alamat IP instance Windows yang ingin Anda sambungkan (misalnya, 10.0.0.100), lalu pilih Connect. Kredensial Active Directory perusahaan Anda diperlukan lagi sebelum Anda terhubung ke instans Windows.

Komputer Windows ke Linux misalnya

Untuk RDP ke benteng SSH dari lingkungan Windows, ikuti langkah-langkah ini.

MALZ

Sebelum Anda memulai:

- Meminta akses ke instans yang ingin Anda sambungkan; untuk informasi, lihat [Permintaan akses](#).
- Pilih nama bastion SSH DNS yang ramah untuk dihubungkan; misalnya:

```
sshbastion(1-4).YOUR_DOMAIN
```

Yang akan terlihat seperti ini jika YOUR_DOMAIN adalah myamsaddomain.com” dan Anda memilih benteng 4:

```
sshbastion4.myamsaddomain.com
```

- Temukan alamat IP dari instans yang ingin Anda sambungkan; untuk informasi, lihat [Menemukan ID instans atau alamat IP](#).

Untuk terhubung ke instance Linux dari mesin Windows Anda, Anda harus terlebih dahulu terhubung ke bastion SSH.

Gunakan klien [OpenSSH](#) Windows asli atau instal [Putty](#) di mesin lokal Anda. [Untuk mempelajari lebih lanjut tentang OpenSSH, lihat OpenSSH di Windows.](#)

1. Gunakan Windows asli atau buka PuTTY dan masukkan nama host bastion SSH atau alamat IP bastion SSH. Misalnya, 10.65.2.214 (22 adalah port yang digunakan untuk SSH; itu akan diatur secara default).
2. OpenSSH atau Putty mencoba koneksi SSH ke benteng dan membuka jendela shell.
3. Gunakan kredensial Active Directory perusahaan Anda seperti yang Anda lakukan dengan host RDP untuk mendapatkan akses.
4. Saat disajikan dengan prompt Bash, SSH ke dalam instance. Masukkan:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

Sebelum Anda memulai:

- Meminta akses ke instans yang ingin Anda sambungkan; untuk informasi, lihat [Permintaan akses](#).
- Pilih nama bastion SSH DNS yang ramah untuk dihubungkan; misalnya:

```
sshbastion(1-4).AMSAccountNumber.amazonaws.com
```

Yang akan terlihat seperti ini jika nomor akun Anda 123456789123 dan Anda memilih benteng 4:

```
sshbastion4.A123456789123.amazonaws.com
```

- Temukan alamat IP dari instans yang ingin Anda sambungkan; untuk informasi, lihat [Menemukan ID instans atau alamat IP](#).

Untuk terhubung ke instance Linux dari mesin Windows Anda, Anda harus terlebih dahulu terhubung ke bastion SSH.

Gunakan klien [OpenSSH](#) Windows asli atau instal [Putty](#) di mesin lokal Anda. [Untuk mempelajari lebih lanjut tentang OpenSSH, lihat OpenSSH di Windows.](#)

1. Gunakan Windows asli atau buka PuTTY dan masukkan nama host bastion SSH atau alamat IP bastion SSH. Misalnya, 10.65.2.214 (22 adalah port yang digunakan untuk SSH; itu akan diatur secara default).
2. OpenSSH atau Putty mencoba koneksi SSH ke benteng dan membuka jendela shell.
3. Gunakan kredensial Active Directory perusahaan Anda seperti yang Anda lakukan dengan host RDP untuk mendapatkan akses.
4. Saat disajikan dengan prompt Bash, SSH ke dalam instance. Masukkan:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

Kontrol akses berbasis tim, atau peran, di akun AMS

Skenario: Dua tim aplikasi A, dan B, masing-masing menggunakan satu akun AMS untuk aplikasi mereka “AA”, dan “BB”. Tim A menginginkan akses hanya ke sumber daya untuk aplikasi “AA”, dan tim B hanya menginginkan akses ke sumber daya untuk aplikasi “BB”. Bagaimana cara mengaturnya?

Gunakan alat ITSM mereka untuk mengimplementasikan kontrol akses berbasis tim (TBAC). Misalnya, Anda dapat menggunakan Aplikasi ServiceNow Konektor AMS untuk integrasi dengan AMS APIs. Hubungi CSDM Anda untuk panduan tingkat tinggi implementasi ini.

Konfigurasi instans otomatis di AMS Advanced

Layanan konfigurasi instans otomatis AMS Advanced berjalan setiap hari dan secara otomatis memindai serta memperbarui SSM dan CloudWatch agen serta file konfigurasi pada instans terkelola EC2 Anda. Pembaruan berlaku, sesuai kebutuhan untuk:

- SSM dan agen CloudWatch
- CloudWatch file konfigurasi

[Pembaruan ini memungkinkan AMS mengakses instans yang dikelola AMS, dan mengonfigurasi EC2 instans agar memancarkan log dan metrik yang sesuai.](#)

Topik

- [Prasyarat untuk konfigurasi instans otomatis](#)
- [Instalasi otomatis Agen SSM](#)
- [Perubahan otomatis](#)

Prasyarat untuk konfigurasi instans otomatis

Untuk pelanggan AMS Advanced yang menerapkan instans dengan Manajemen Perubahan, prasyarat berikut harus dipenuhi:

- Agen SSM diinstal, dan dalam keadaan terkelola.
- Instance ditandai sebagai instance terkelola. (`aws:cloudformation:stack-nameTag` memiliki nilai yang dimulai dengan `stack-` atau `sc-`.)

Jika Agen SSM belum diinstal pada instans Anda, Anda dapat menginstalnya menggunakan fitur instalasi otomatis Agen SSM AMS. Untuk informasi selengkapnya, lihat [Instalasi otomatis Agen SSM](#).

Atau, Anda dapat menginstal Agen SSM secara manual. Untuk informasi selengkapnya, lihat berikut ini:

- Linux: [Instal SSM Agent secara manual pada EC2 instans untuk Linux - AWS Systems Manager](#)
- Windows: [Instal SSM Agent secara manual pada EC2 instans untuk Windows Server - AWS Systems Manager](#)

Untuk informasi selengkapnya tentang agen SSM, lihat dokumentasi AWS [Bekerja dengan Agen SSM](#).

Instalasi otomatis Agen SSM

Agar AMS mengelola instans Amazon Elastic Compute Cloud (Amazon EC2), Anda harus menginstal Agen AWS Systems Manager SSM di setiap instans. Jika instans Anda tidak menginstal Agen SSM, Anda dapat menggunakan fitur instalasi otomatis Agen SSM AMS.

Note

- Fitur ini hanya tersedia untuk EC2 instance yang tidak ada dalam grup Auto Scaling dan yang menjalankan sistem operasi Linux yang didukung oleh AMS.
- Fitur instalasi otomatis Agen SSM AMS dinonaktifkan secara default. Untuk mengaktifkannya, hubungi CA atau CSDM Anda.

Prasyarat untuk penggunaan Agen SSM

- Pastikan profil instance yang terkait dengan instance target memiliki salah satu kebijakan berikut (atau izin yang setara seperti yang diizinkan di dalamnya):
 - Amazon SSMManged EC2 InstanceDefaultPolicy
 - Amazon SSMManged InstanceCore
- Pastikan bahwa tidak ada Kebijakan Kontrol Layanan di AWS Organizations tingkat yang secara eksplisit menolak izin yang tercantum dalam kebijakan sebelumnya.

Untuk informasi selengkapnya, lihat [Mengonfigurasi izin instans yang diperlukan untuk Systems Manager](#).

- Untuk memblokir lalu lintas keluar, pastikan titik akhir antarmuka berikut diaktifkan di VPC tempat instance target berada, (ganti “wilayah” di URL dengan tepat):
 - ssm. <region>.amazonaws.com
 - ssmmessages. <region>.amazonaws.com
 - ec2pesan. <region>.amazonaws.com

Untuk informasi selengkapnya, lihat [Meningkatkan keamanan EC2 instans dengan menggunakan titik akhir VPC untuk Systems Manager](#).

Untuk tips umum tentang mengaktifkan atau memecahkan masalah ketersediaan node terkelola, lihat [Solusi 2: Verifikasi bahwa profil instans IAM telah ditentukan untuk instance \(hanya instance\) EC2](#).

 Note

AMS berhenti dan memulai setiap instance sebagai bagian dari proses instalasi otomatis. Ketika sebuah instance dihentikan, data yang disimpan dalam volume penyimpanan instance dan data yang disimpan pada RAM hilang. Untuk informasi selengkapnya, lihat [Apa yang terjadi ketika Anda menghentikan sebuah instance](#).

Minta instalasi otomatis Agen SSM pada instans Anda

Jika akun Anda di-onboard ke AMS Accelerate Patch Add-On, maka konfigurasi jendela pemeliharaan patch (MW) untuk instance tersebut. Agen SSM yang berfungsi diperlukan untuk menyelesaikan proses tambalan. Jika Agen SSM hilang pada sebuah instance, maka AMS mencoba menginstalnya secara otomatis selama jendela pemeliharaan tambalan.

 Note

AMS berhenti dan memulai setiap instance sebagai bagian dari proses instalasi otomatis. Ketika sebuah instance dihentikan, data yang disimpan dalam volume penyimpanan instance dan data yang disimpan pada RAM hilang. Untuk informasi selengkapnya, lihat [Apa yang terjadi ketika Anda menghentikan sebuah instance](#).

Cara kerja instalasi otomatis Agen SSM

AMS menggunakan data EC2 pengguna untuk menjalankan skrip instalasi pada instans Anda. Untuk menambahkan skrip data pengguna dan menjalankannya pada instance Anda, AMS harus menghentikan dan memulai setiap instance.

Jika instans Anda sudah memiliki skrip data pengguna yang ada, AMS akan menyelesaikan langkah-langkah berikut selama proses instalasi otomatis:

1. Membuat cadangan skrip data pengguna yang ada.
2. Mengganti skrip data pengguna yang ada dengan skrip instalasi Agen SSM.
3. Memulai ulang instance untuk menginstal Agen SSM.

4. Menghentikan instance dan mengembalikan skrip asli.
5. Memulai ulang instance dengan skrip asli.

Perubahan otomatis

Layanan konfigurasi instans otomatis AMS Advanced membuat perubahan, sesuai kebutuhan, pada EC2 instans Anda.

Apa yang berubah:

- [Secara otomatis memperbarui kode pada instance Linux](#)
- [Secara otomatis memperbarui PBIS pada instance Linux](#)
- [Secara otomatis memperbarui versi minimum SSM dan agen CloudWatch](#)
- [CloudWatch file konfigurasi, perbarui detail](#)
- [Log yang dikonfigurasi secara otomatis](#)

Secara otomatis memperbarui kode pada instance Linux

AMS secara otomatis memperbarui kode instans pada instance Linux. Ini membantu meningkatkan stabilitas operasional dan keamanan komponen dan lingkungan AMS sama sekali.

FAQ:

Apa yang termasuk dalam On Instance Code (OIC) di Linux?

OIC menyertakan paket ams-toolkit bersama dengan beberapa file konfigurasi dan pekerjaan cron. AMS memerlukan file dan paket ini untuk integrasi (Active Directory, CloudFormation dan dependensi lainnya). Kami memanggang file-file ini ke dalam AMS yang disediakan AMIs atau menginstal ke instance Anda selama konsumsi beban kerja.

Kapan AMS akan memperbarui OIC?

AMS memperbarui OIC saat kami merilis versi baru dengan perbaikan bug atau peningkatan lainnya. Alur kerja untuk memeriksa versi OIC dan pembaruan berjalan setiap hari.

Secara otomatis memperbarui PBIS pada instance Linux

AMS menggunakan modul Power Broker Identity Service (PBIS) untuk menggabungkan instance Linux ke Active Directory yang dikelola AMS.

AMS secara otomatis memperbarui PBIS pada instance Linux.

FAQ:

Kapan AMS akan memperbarui PBIS?

AMS mengaktifkan pembaruan PBIS saat reboot. Jika ada versi PBIS baru yang tersedia, maka AMS mencoba menginstal versi baru selama reboot instance berikutnya.

Bisakah pembaruan PBIS dimatikan?

Anda dapat menonaktifkan pembaruan PBIS di tingkat instans atau akun:

- Tingkat akun: Buat parameter di penyimpanan parameter SSM: Nama: `/ams/skip-pbis-update`, Nilai: `true` (kasus apa pun).

Note

Profil instance harus memiliki izin untuk membaca parameter SSM. Jika flag tidak ada, maka perilaku default adalah menjalankan pembaruan.

- Tingkat instans:
 - Berbasis tag: Tambahkan tag berikut ke instance: Key: `skip_pbis_update`, Value: `true` (kasus apa pun).
 - File Config: Tambahkan flag berikut ke file: `/opt/aws/ams/etc/ams.conf.d/state.ini`
`skip_pbis_update = true`.

Note

Tag memiliki prioritas yang lebih tinggi daripada parameter SSM. Anda dapat mematikan pembaruan PBIS di tingkat akun melalui parameter, tetapi mengubahnya untuk satu (atau beberapa) instance dengan menambahkan tag Key: `skip_pbis_update`, Value: `false`.

Untuk mengonfigurasi salah satu opsi yang dijelaskan, ikuti proses manajemen perubahan standar di lingkungan AMS Anda.

Secara otomatis memperbarui versi minimum SSM dan agen CloudWatch

Versi minimum AMS Advanced (SSM atau CloudWatch agen) adalah versi yang telah diuji oleh tim layanan AMS dan disetujui sebelumnya untuk sistem operasi Anda. Kami mencoba untuk tetap proaktif dan menjalankan versi stabil dan kompatibel terbaru, sehingga nomor versi berubah seiring waktu. Anda dapat menemukan versi minimum saat ini dengan menaikkan permintaan layanan ke AMS.

- Manajemen Agen SSM

Agen SSM Amazon bertanggung jawab untuk menjalankan perintah jarak jauh pada instance. Otomatisasi konfigurasi instans memastikan bahwa Agen SSM menjalankan versi minimum.

- Manajemen Agen Cloudwatch

CloudWatch Agen Amazon bertanggung jawab untuk memancarkan log dan metrik OS. Konfigurasi instans otomatis melakukan hal berikut:

- Jika diperlukan, nonaktifkan agen CloudWatch Log lama dan memigrasikan konfigurasi ke agen terpadu baru CloudWatch
- Jika instans Anda menjalankan Agen CloudWatch Log lama, konfigurasi instans otomatis akan menonaktifkan layanan agen CloudWatch Log lama dan memigrasikan konfigurasinya ke agen terpadu. CloudWatch
- Menyesuaikan CloudWatch konfigurasi Anda untuk memancarkan log dan metrik yang sesuai.

File dan direktori yang terpengaruh:

- Windows
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\ Konfigurasi\
- Linux
 - /opt/aws/amazon-cloudwatch-agent/etc/
 - /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/
 - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

CloudWatch file konfigurasi, perbarui detail

Kami membaca CloudWatch konfigurasi kustom Anda (hanya JSON) dari CloudWatch direktori berikut (lihat direktori yang [direkomendasikan](#)), dan menggabungkannya dengan konfigurasi AMS standar: CloudWatch

- CloudWatch Berkas
 - Pada contoh:
 - Windows
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\ Konfigurasi\
 - %ProgramFiles%\ ModulWindowsPowerShell\ AWSManaged Services.Logging.Utilities\ Files\ Config.json
 - Linux
 - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json
 - Di Amazon S3:
 - Windows:
 - https://ams-configuration-artifacts-REGION_NAME.s3.REGION_NAME.amazonaws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json
 - Linux:
 - https://ams-configuration-artifacts-REGION_NAME.s3.REGION_NAME.amazonaws.com/configurations/cloudwatch/latest/linux-cloudwatch-config.json

Log yang dikonfigurasi secara otomatis

Kami mengonfigurasi instance Anda untuk menulis log berikut.

- Windows:
 - SSMAgentLog Amazon
 - AmazonCloudWatchAgentLog
 - SSMErrorLog Amazon
 - AmazonCloudFormationLog
 - ApplicationEventLog
 - EC2ConfigServiceEventLog

- MicrosoftWindowsAppLockerEXEAndDLLEventLog
- MicrosoftWindowsAppLockerMSIAndScriptEventLog
- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog
- Linux:
 - /var/log/amazon/ssm/amazon-ssm-agent.log
 - /var/log/amazon/ssm/errors.log
 - /var/log/audit/audit.log
 - /var/log/cloud-init-output.log
 - /var/log/cloud-init.log
 - /var/log/cron
 - /var/log/dpkg.log
 - /var/log/maillog
 - /var/log/messages
 - /var/log/secure
 - /var/log/spooler
 - /var/log/syslog
 - /var/log/yum.log
 - /var/log/zypper.log

Pemantauan dan manajemen acara di AMS

Topik

- [Apa itu pemantauan?](#)
- [Apa yang dipantau oleh sistem pemantauan AMS?](#)
- [Cara kerja pemantauan](#)
- [Melihat konfigurasi pemantauan untuk akun AMS](#)
- [Mengubah konfigurasi pemantauan untuk akun AMS](#)
- [Pemberitahuan insiden sadar aplikasi di AMS](#)
- [Menggunakan OpsCenter di AMS](#)
- [Pemberitahuan peringatan dari AMS](#)
- [Membuat CloudWatch alarm tambahan di AMS](#)
- [Membuat CloudWatch metrik dan alarm khusus di AMS](#)
- [Menggunakan CloudWatch Application Insights untuk server .Net dan SQL di AMS](#)
- [Menggunakan Aturan EventBridge Terkelola Amazon di AMS](#)
- [Remediator Tepercaya di AMS](#)

Sistem pemantauan AWS Managed Services (AMS) memantau sumber daya AMS Anda dari kegagalan, penurunan kinerja, dan masalah keamanan. Sistem pemantauan AMS bergantung pada layanan AWS seperti Amazon CloudWatch (CloudWatch), Amazon, Amazon Macie GuardDuty, dan AWS Health. Selain sistem pemantauan, AMS juga menerapkan TrendMicro DeepSecurity perlindungan terhadap malware pada instans Amazon Elastic Compute Cloud (Amazon EC2), untuk informasi tentang default keamanan titik akhir (EPS), lihat. [Keamanan Titik Akhir \(EPS\)](#)

Pemantauan AMS memberikan manfaat ini:

- Garis dasar pemantauan sehingga Anda memiliki tingkat perlindungan default meskipun Anda tidak mengonfigurasi pemantauan lain untuk akun terkelola Anda. Untuk informasi, lihat [Peringatan dari pemantauan dasar di AMS](#).
- Investigasi peringatan untuk menentukan tindakan yang tepat. Misalnya, jika GuardDuty menemukan aktivitas yang menunjukkan upaya brute forcing terhadap EC2 instance Amazon, AMS menganalisis flowlog VPC untuk memahami asal dan konteks aktivitas.

- Remediasi peringatan, bila memungkinkan, untuk mencegah atau mengurangi dampak pada aplikasi Anda. Misalnya, jika Anda menggunakan EC2 instans Amazon mandiri dan gagal dalam pemeriksaan kesehatan Sistem, AMS mencoba memulihkan instance dengan menghentikan dan memulai ulang instans tersebut. Untuk informasi selengkapnya, lihat [Remediasi peringatan otomatis AMS](#).
- Transparansi menjadi peringatan aktif, dan sebelumnya diselesaikan, menggunakan OpsCenter. Misalnya, jika Anda memiliki pemanfaatan CPU tinggi yang tidak terduga pada EC2 instans Amazon, Anda dapat meminta akses ke konsol AWS Systems Manager (termasuk akses ke OpsCenter konsol) dan melihat OpsItem langsung di OpsCenter konsol.

Apa itu pemantauan?

Sistem pemantauan AMS memantau AWS sumber daya Anda untuk kegagalan, penurunan kinerja, dan masalah keamanan. Sebagai akun terkelola, AMS mengonfigurasi dan menyebarkan alarm untuk AWS sumber daya yang berlaku, memantaunya, dan melakukan remediasi bila berlaku.

Sistem pemantauan AMS menghasilkan peringatan berdasarkan konfigurasi pemantauan di akun Anda. Konfigurasi pemantauan akun mengacu pada semua parameter sumber daya di akun yang membuat peringatan; untuk informasi tentang parameter sumber daya, lihat [Peringatan dari pemantauan dasar di AMS](#). Konfigurasi pemantauan akun mencakup definisi CloudWatch Alarm, dan Aturan CloudWatch Peristiwa yang menghasilkan peringatan (alarm atau peristiwa).

Konfigurasi pemantauan dasar adalah kumpulan definisi alarm ([Peringatan dari pemantauan dasar di AMS](#)) yang dikuratori oleh AMS untuk memantau sumber daya di akun terkelola Anda. Konfigurasi pemantauan akun mungkin berbeda dari konfigurasi dasar, sebagai akibat dari perubahan yang diminta oleh Anda.

Pemberitahuan akan segera terjadi, sedang berlangsung, surut, atau potensi kegagalan, penurunan kinerja, atau masalah keamanan yang dihasilkan oleh pemantauan dasar yang dikonfigurasi dalam akun, disebut peringatan. Contoh peringatan adalah CloudWatch Alarm Amazon, CloudWatch Acara Amazon, Acara, atau Layanan Temuan dari AWS seperti Amazon GuardDuty, dan acara, atau peringatan, dari Trend Micro Deep Security.

Peringatan dari layanan AWS terkait keamanan seperti Amazon, GuardDuty Amazon Macie, atau Trend Micro Deep Security disebut peringatan keamanan untuk membedakannya dari jenis peringatan lainnya.

Pemantauan AMS memberikan manfaat ini:

- Kemampuan untuk menyesuaikan alarm sumber daya dasar untuk memenuhi kebutuhan Anda.
- Remediasi otomatis peringatan, bila memungkinkan, untuk mencegah atau mengurangi dampak pada aplikasi Anda. Misalnya, jika Anda menggunakan EC2 instans Amazon mandiri dan gagal dalam pemeriksaan kesehatan sistem, AMS mencoba memulihkan instance dengan menghentikan dan memulai ulang instans tersebut. Untuk informasi selengkapnya, lihat [Remediasi peringatan otomatis AMS](#).
- Transparansi menjadi peringatan aktif, dan sebelumnya diselesaikan, menggunakan OpsCenter. Misalnya, jika Anda memiliki pemanfaatan CPU tinggi yang tidak terduga pada EC2 instans Amazon, Anda dapat meminta akses ke AWS Systems Manager konsol (yang mencakup akses ke OpsCenter konsol) dan melihat OpsItem langsung di OpsCenter konsol.
- Menyelidiki peringatan untuk menentukan tindakan yang tepat.
- Peringatan yang dihasilkan berdasarkan konfigurasi di akun Anda dan AWS layanan yang didukung. Konfigurasi pemantauan akun mengacu pada semua parameter sumber daya di akun yang membuat peringatan. Konfigurasi pemantauan akun mencakup definisi CloudWatch Alarm, dan EventBridge (sebelumnya dikenal sebagai CloudWatch Peristiwa) yang menghasilkan peringatan (alarm atau peristiwa). Untuk informasi selengkapnya tentang parameter sumber daya, lihat [Peringatan dari pemantauan dasar di AMS](#).
- Pemberitahuan tentang kegagalan yang akan terjadi, sedang berlangsung, surut, atau potensi kegagalan; penurunan kinerja; atau masalah keamanan yang dihasilkan oleh pemantauan dasar yang dikonfigurasi dalam akun (dikenal sebagai peringatan). Contoh peringatan termasuk CloudWatch Alarm, Peristiwa, atau Temuan dari layanan AWS, seperti GuardDuty atau AWS Health.

Apa yang dipantau oleh sistem pemantauan AMS?

Sesuai dengan model tanggung jawab layanan bersama AWS Managed Services (AMS), sistem pemantauan AMS memantau infrastruktur AWS Anda. Untuk detail tentang pemantauan dasar di AMS, termasuk sumber daya AWS yang dipantau dan jenis peringatan untuk setiap sumber daya, lihat [Peringatan dari pemantauan dasar di AMS](#). Untuk EC2 instans Amazon, AMS memantau sistem operasi dan menyediakan pemantauan dasar berdasarkan metrik OS seperti pemanfaatan CPU dan penggunaan volume root.

Kami merekomendasikan untuk melengkapi pemantauan AMS dengan pemantauan tambahan menggunakan layanan AWS yang disesuaikan dengan aplikasi Anda. [Untuk panduan tentang pemantauan ketersediaan, lihat bagian “Monitoring and Alarming” di whitepaper Reliability Pillar ini.](#) Anda dapat mengonfigurasi pemantauan Anda sendiri agar sesuai dengan kebutuhan operasional

Anda; bagaimana melakukannya dibahas dalam [Membuat CloudWatch alarm tambahan di AMS](#) dan [Membuat CloudWatch metrik dan alarm khusus di AMS](#).

Pemantauan proaktif Zona Pendaratan Akun Tunggal atas Active Directory Trust di AMS

AMS single-account landing zone (SALZ) memantau status kepercayaan satu arah antara Direktori Aktif Terkelola (AD) di akun terkelola AMS dan domain perusahaan Anda. Kepercayaan satu arah dengan Managed AD sangat penting untuk permintaan akses dan permintaan masuk instans. Dengan pemantauan baru ini, AMS sekarang secara proaktif menanggapi masalah terkait kepercayaan, dan mengurangi waktu rata-rata untuk mendeteksi insiden terkait akses.

Fitur ini diaktifkan secara otomatis di akun AWS Managed Services (AMS) Anda.

Ada dampak biaya yang kecil. Fitur ini menggunakan empat CloudWatch metrik AWS, dan dua CloudWatch alarm AWS untuk satu kepercayaan.

Cara kerja pemantauan

Lihat grafik berikut tentang arsitektur pemantauan di AWS Managed Services (AMS).

Diagram berikut memberikan gambaran tingkat tinggi dari landing zone multi-akun AMS dan alur kerja pemantauan landing zone akun tunggal AMS.

- **Pembuatan:** Pada saat orientasi akun, AMS mengonfigurasi pemantauan dasar (kombinasi alarm (CW), dan aturan acara CW) untuk semua sumber daya yang dibuat di akun terkelola. CloudWatch Konfigurasi pemantauan dasar menghasilkan peringatan ketika alarm CW dipicu atau peristiwa CW dihasilkan.
- **Agregasi:**
 - **Zona Pendaratan Multi-Akun:** Peringatan dihasilkan oleh sumber daya Anda dalam akun Aplikasi dan Unit Organisasi Inti dan dikirim ke sistem pemantauan AMS dengan mengarahkannya melalui akun Keamanan.
 - **Zona Pendaratan Akun Tunggal:** Semua peringatan yang dihasilkan oleh sumber daya Anda dikirim ke sistem pemantauan AMS dengan mengarahkannya ke topik SNS di akun.
 - Anda juga dapat mengonfigurasi cara AMS mengelompokkan EC2 peringatan bersama. AMS mengelompokkan semua peringatan yang terkait dengan EC2 instance yang sama ke dalam

satu insiden, atau membuat satu insiden per peringatan, tergantung pada preferensi Anda. Anda dapat mengubah konfigurasi ini kapan saja dengan bekerja sama dengan Cloud Service Delivery Manager atau Cloud Architect Anda. Ini bekerja dengan cara yang sama apakah Anda menggunakan Zona Pendaratan Multi-Akun atau Zona Pendaratan Akun Tunggal.

- Pemrosesan: AMS menganalisis peringatan dan memprosesnya berdasarkan potensi dampaknya. Peringatan diproses seperti yang dijelaskan selanjutnya.
- Peringatan dengan dampak pelanggan yang diketahui: Ini mengarah pada pembuatan laporan insiden baru dan AMS mengikuti proses manajemen insiden; untuk informasi tentang manajemen insiden, lihat [Tanggapan insiden AMS](#).

Contoh peringatan: EC2 Instans Amazon gagal dalam pemeriksaan kesehatan sistem, AMS mencoba memulihkan instance dengan menghentikan dan memulai ulang instans.

- Peringatan dengan dampak pelanggan yang tidak pasti: Untuk jenis peringatan ini, AMS mengirimkan laporan insiden, dalam banyak kasus meminta Anda untuk memverifikasi dampak sebelum AMS mengambil tindakan. Namun, jika pemeriksaan terkait infrastruktur lewat, AMS tidak mengirimkan laporan insiden kepada Anda.

Misalnya: Peringatan untuk pemanfaatan CPU > 85% selama lebih dari 10 menit pada EC2 instans Amazon tidak dapat segera dikategorikan sebagai insiden karena perilaku ini mungkin diharapkan berdasarkan penggunaan. Dalam contoh ini, AMS Automation melakukan pemeriksaan terkait infrastruktur pada sumber daya. Jika pemeriksaan tersebut lulus, maka AMS tidak mengirim pemberitahuan peringatan, bahkan jika penggunaan CPU melewati 99%. Jika Automation mendeteksi bahwa pemeriksaan terkait infrastruktur gagal pada sumber daya, AMS mengirimkan pemberitahuan peringatan dan memeriksa apakah mitigasi diperlukan. Pemberitahuan peringatan dibahas secara rinci di bagian ini. AMS menawarkan opsi mitigasi dalam notifikasi. Ketika Anda membalas pemberitahuan yang mengonfirmasi bahwa peringatan tersebut merupakan insiden, AMS akan membuat laporan insiden baru dan proses manajemen insiden AMS dimulai. Pemberitahuan layanan yang menerima respons “tidak ada dampak pelanggan,” atau tidak ada respons sama sekali selama tiga hari, ditandai sebagai diselesaikan dan peringatan terkait ditandai sebagai diselesaikan.

- Peringatan tanpa dampak pelanggan: Jika, setelah evaluasi, AMS menentukan bahwa peringatan tidak memiliki dampak pelanggan, maka peringatan ditutup.

Misalnya, AWS Health memberi tahu EC2 instance yang membutuhkan penggantian tetapi instance itu telah dihentikan.

EC2 pemberitahuan yang dikelompokkan misalnya

Anda dapat mengonfigurasi pemantauan AMS untuk mengelompokkan peringatan bersama dari EC2 instance yang sama ke dalam satu insiden. Cloud Service Delivery Manager atau Cloud Architect Anda dapat mengonfigurasinya untuk Anda. Ada empat parameter yang dapat Anda konfigurasi untuk setiap akun yang dikelola AMS.

1. Lingkup: Pilih seluruh akun atau berbasis tag.

- Untuk menentukan konfigurasi yang berlaku untuk setiap EC2 instance di akun tersebut, pilih scope = account-wide.
- Untuk menentukan konfigurasi yang hanya berlaku untuk EC2 instance di akun tersebut dengan tag tertentu, pilih scope = berbasis tag.

2. Aturan pengelompokan: Pilih klasik atau contoh.

- Untuk mengonfigurasi pengelompokan tingkat instans untuk setiap sumber daya di akun Anda, pilih scope = account-wide dan grouping rule = instance.
- Untuk mengonfigurasi sumber daya tertentu di akun Anda agar menggunakan pengelompokan tingkat instans, beri tag pada instance tersebut, lalu pilih scope = tag-based dan grouping rule = instance level.
- Untuk tidak menggunakan pengelompokan instance untuk peringatan di akun Anda, pilih aturan pengelompokan = klasik.

3. Opsi keterlibatan: Pilih tidak ada, hanya laporkan, atau default.

- Agar AMS tidak membuat insiden atau menjalankan otomatisasi untuk alarm dari sumber daya tersebut saat konfigurasi aktif, pilih none.
- Agar AMS tidak membuat insiden atau menjalankan otomatisasi untuk alarm dari sumber daya tersebut saat konfigurasi aktif, dan tidak menjalankan dokumen Systems Manager penyembuhan otomatis tetapi untuk menyertakan catatan peristiwa ini dalam pelaporan Anda, pilih laporan saja. Ini mungkin berguna jika Anda ingin mengurangi volume kasus dukungan insiden yang berinteraksi dengan Anda dan jika beberapa insiden dari beberapa sumber daya tidak memerlukan perhatian segera, misalnya yang ada di akun non-produksi.
- Agar AMS dapat memproses peringatan Anda, menjalankan otomatisasi, dan membuat kasus insiden bila diperlukan, pilih default.

4. Selesaikan setelah: Pilih 24 jam, 48 jam, atau 72 jam. Terakhir, konfigurasi kapan kasus insiden ditutup secara otomatis. Jika waktu dari korespondensi kasus terakhir mencapai nilai Selesaikan setelah yang dikonfigurasi, insiden ditutup.

Notifikasi pemberitahuan

Sebagai bagian dari pemrosesan peringatan, berdasarkan analisis dampak, AWS Managed Services (AMS) membuat insiden dan memulai proses manajemen insiden untuk remediasi, ketika dampak dapat ditentukan. Jika dampak tidak dapat ditentukan, AMS akan mengirimkan pemberitahuan peringatan ke alamat email yang terkait dengan akun Anda melalui pemberitahuan layanan. Dalam beberapa skenario, pemberitahuan peringatan ini tidak dikirim. Misalnya, jika pemeriksaan terkait infrastruktur melewati peringatan pemanfaatan CPU yang tinggi, maka pemberitahuan peringatan tidak dikirimkan kepada Anda. Untuk informasi selengkapnya, lihat diagram pada arsitektur pemantauan AMS untuk proses penanganan peringatan di [Cara kerja pemantauan](#).

Pemberitahuan peringatan berbasis tag

Gunakan tag untuk mengirim pemberitahuan peringatan untuk sumber daya Anda ke alamat email yang berbeda. Ini adalah praktik terbaik untuk menggunakan pemberitahuan peringatan berbasis tag karena pemberitahuan yang dikirim ke satu alamat email dapat menyebabkan kebingungan ketika beberapa tim pengembang menggunakan akun yang sama. Pemberitahuan peringatan berbasis tag tidak terpengaruh oleh [EC2 pemberitahuan yang dikelompokkan misalnya](#) pengaturan yang Anda pilih.

Dengan pemberitahuan peringatan berbasis tag, Anda dapat:

- Kirim peringatan ke alamat email tertentu: Tag sumber daya yang memiliki peringatan yang harus dikirim ke alamat email tertentu dengan, `key = OwnerTeamEmail.value = EMAIL_ADDRESS`
- Kirim peringatan ke beberapa alamat email: Untuk menggunakan beberapa alamat email, tentukan daftar nilai yang dipisahkan koma. Misalnya, `key = OwnerTeamEmail, value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ....` Jumlah total karakter untuk bidang nilai tidak boleh melebihi 260.
- Gunakan kunci tag kustom: Untuk menggunakan kunci tag kustom, berikan nama kunci tag kustom ke CSDM Anda dalam email yang secara eksplisit memberikan persetujuan untuk mengaktifkan notifikasi otomatis untuk komunikasi berbasis tag. Ini adalah praktik terbaik untuk menggunakan strategi penandaan yang sama untuk tag kontak di semua instans dan sumber daya Anda.

Note

Nilai kuncinya `OwnerTeamEmail` tidak harus dalam kasus unta. Namun, tag peka huruf besar/kecil dan praktik terbaik adalah menggunakan format yang disarankan.

Alamat email harus ditentukan secara lengkap, dengan tanda “at” (@) untuk memisahkan bagian lokal dari domain. Contoh alamat email yang tidak valid: *Team.AppATabc.xyz* atau. *john.doe* Untuk panduan umum tentang strategi penandaan Anda, lihat [AWS Menandai sumber daya](#). Jangan menambahkan informasi identitas pribadi (PII) di tag Anda. Gunakan daftar distribusi atau alias sedapat mungkin.

Pemberitahuan peringatan berbasis tag didukung untuk sumber daya dari Layanan Amazon berikut: EC2, Elastic Block Store (EBS), Elastic Load Balancing (ELB), Application Load Balancer (ALB), Network Load Balancer, Relational Database Service (RDS), Elastic File System (EFS), dan VPN. OpenSearch FSx Site-to-Site

Melihat konfigurasi pemantauan untuk akun AMS

Ada dua bagian penting untuk konfigurasi pemantauan akun yang dapat Anda lihat:

- CloudWatch Alarm: Anda dapat melihat semua alarm CW di akun dengan membuka CloudWatch konsol dan memilih berbagai layanan yang menarik.
- CloudWatch Acara:
 - Zona Pendaratan Multi-Akun: CloudWatch Peristiwa yang dipantau di akun dapat ditemukan dengan memfilter semua aturan acara CW dengan string. "ams - "
 - Single-Account Landing Zone: CloudWatch Peristiwa yang dipantau di akun dapat ditemukan dengan memfilter semua aturan acara CW dengan string. "mc - "

Mengubah konfigurasi pemantauan untuk akun AMS

Anda dapat mengubah konfigurasi pemantauan dasar untuk sumber daya Amazon EC2 . Untuk peringatan yang dapat dikonfigurasi, lihat [Peringatan dari pemantauan dasar di AMS](#). Anda dapat mengubah definisi alarm, tujuan alarm, atau memilih keluar dari pemberitahuan alarm untuk monitor dasar sehingga peringatan memenuhi persyaratan operasional aplikasi Anda. Anda dapat meminta salah satu atau semua perubahan yang disebutkan sebelumnya dengan mengirimkan Manajemen | Lainnya | Lainnya | Perbarui CT (ct-0xdawir96cy7k) dengan rincian berikut.

- Instance IDs [opsional, jika tidak disebutkan, semua instance dalam akun berada dalam cakupan]
- CloudWatch nama metrik, misalnya, pemanfaatan CPU/swap free/ IOwait
- Target - ID email/nomor telepon untuk topik SMS/SNS

Untuk mempelajari lebih lanjut tentang jenis perubahan yang dapat Anda minta dalam konfigurasi pemantauan dasar, lihat Dokumentasi [Amazon CloudWatch](#).

Pemberitahuan insiden sadar aplikasi di AMS

Gunakan pemberitahuan insiden otomatis sadar aplikasi untuk menyesuaikan pengalaman komunikasi Anda untuk kasus dukungan yang dibuat AMS atas nama Anda. Saat Anda menggunakan fitur ini, AMS mengambil preferensi beban kerja khusus [AWS Service Catalog AppRegistry](#) untuk memperkaya komunikasi insiden AMS Anda dengan metadata tentang aplikasi Anda dan untuk menyesuaikan tingkat keparahan kasus dukungan yang dibuat oleh AMS atas nama Anda. Untuk menggunakan fitur ini, Anda harus terlebih dahulu menyediakan AWS Service Catalog AppRegistry di akun AMS Anda.

Untuk mempelajari selengkapnya tentang default pemantauan AMS, lihat [Pemantauan dan manajemen acara di AMS](#)

Penyediaan AppRegistry di akun AMS Anda dan buat aplikasi

AppRegistry Layanan ini tersedia dalam mode Penyediaan Layanan Mandiri (SSP) untuk akun AMS Anda. Untuk petunjuk tentang cara meminta akses, lihat [Menggunakan SSP AMS untuk menyediakan AWS Service Catalog AppRegistry di akun AMS Anda](#).

Setelah penyediaan AppRegistry, gunakan salah satu metode berikut untuk membuat aplikasi:

1. AWS konsol: Untuk mempelajari selengkapnya tentang membuat aplikasi AppRegistry melalui AWS console, lihat [Membuat Aplikasi](#) di Panduan AWS Service Catalog AppRegistry Administrator.
2. CloudFormation: Anda dapat menentukan AppRegistry aplikasi Anda seperti Anda mendefinisikan sumber daya lainnya. Untuk informasi selengkapnya, lihat [referensi jenis AWS Service Catalog AppRegistry sumber daya](#) di Panduan AWS CloudFormation Pengguna.

Buat tag untuk mengaktifkan pengayaan kasus

Anda harus menandai aplikasi Anda sebelum AMS dapat mengakses metadata aplikasi. Tabel berikut mencantumkan tag yang diperlukan.

Kunci tanda	Nilai tanda
ams-dikelola	true

Sesuaikan tingkat keparahan kasus dukungan AMS untuk aplikasi Anda

Anda dapat menyesuaikan tingkat keparahan kasus dukungan yang dibuat AMS dengan menentukan seberapa penting aplikasi Anda untuk organisasi Anda. Pengaturan ini dikendalikan oleh grup atribut yang terkait dengan aplikasi Anda di AppRegistry. Nama nama grup atribut harus sesuai dengan pola berikut:

```
AMS.<ApplicationName>.CommunicationOptions
```

Dalam pola sebelumnya, `ApplicationName` harus cocok dengan nama yang digunakan AppRegistry ketika Anda membuat aplikasi.

Contoh konten:

```
{
  "SchemaVersion": "1.0",
  "Criticality": "low"
}
```

SchemaVersion

Ini menentukan versi skema yang Anda gunakan dan subset fitur yang tersedia untuk digunakan.

Versi skema	Fitur
1.0	Tingkat keparahan kasus dukungan yang disesuaikan berdasarkan nilai Kritikalitas

Kritikalitas

Kekritisan aplikasi ini menentukan tingkat keparahan kasus dukungan yang dibuat oleh sistem otomatis AMS.

Nilai valid:

```
low|normal|high|urgent|critical
```

Untuk informasi selengkapnya tentang tingkat keparahan, lihat [SeverityLevel](#) di Referensi AWS Dukungan API.

Wajib: Ya

Tinjau izin yang diperlukan

Untuk menggunakan fitur ini, AMS memerlukan akses ke AWS Identity and Access Management izin berikut:

- saya: ListRoleTags
- saya: ListUserTags
- resourcegroupstaggingapi: GetResources
- servicecatalog-appregistry: GetApplication
- servicecatalog-appregistry: ListAssociatedAttributeGroups
- servicecatalog-appregistry: GetAttributeGroup

Important

Pastikan bahwa tidak ada kebijakan IAM atau kebijakan kontrol layanan (SCP) yang menyangkal tindakan sebelumnya.

Panggilan API dibuat oleh `ams-access-admin` peran. Berikut ini adalah contoh dari apa yang mungkin Anda lihat:

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

Menggunakan OpsCenter di AMS

Tim Operasi AWS Managed Services (AMS) digunakan [AWS Systems Manager OpsCenter](#) untuk mendiagnosis dan memulihkan banyak peringatan yang terkait dengan sumber daya Anda.

Menggunakan OpsCenter mengurangi mean time to resolution (MTTR), sambil memberikan pandangan transparan ke dalam antrian operasional tim operasi AMS.

Dengan OpsCenter, AMS memberi Anda pandangan transparan tentang item pekerjaan operasional, juga dikenal sebagai [OpsItems](#), yang secara aktif dikerjakan oleh tim AMS, selain solusi otomatis.

Untuk mempelajari lebih lanjut tentang OpsCenter dan OpsItems, lihat [AWS Systems Manager OpsCenter](#). Untuk informasi tentang mendapatkan akses ke Konsol AWS Manajemen, lihat [Bekerja dengan AWS Management Console](#). Dari AWS Management Console, Anda dapat menavigasi ke AWS Systems Manager Console, dan OpsCenter; untuk mempelajari lebih lanjut, lihat [AWS Systems Manager Session Manager](#). OpsCenter juga menyediakan API yang dapat Anda gunakan; untuk informasi, lihat [Pelajari Selengkapnya OpsCenter](#).

OpsCenter adalah fitur harga dengan ~ 1000 OpsItems yang harganya di bawah \$10. Untuk informasi, lihat [harga AWS Systems Manager](#).

Pemberitahuan peringatan dari AMS

Sebagai bagian dari pemrosesan peringatan, berdasarkan analisis dampak, AWS Managed Services (AMS) membuat insiden dan memulai proses manajemen insiden untuk remediasi, ketika dampak dapat ditentukan. Jika dampak tidak dapat ditentukan, AMS mengirimkan pemberitahuan peringatan ke alamat email yang terkait dengan akun Anda melalui pemberitahuan layanan; lihat diagram pada arsitektur pemantauan AMS untuk proses penanganan peringatan di [Cara kerja pemantauan](#).

Menerima peringatan yang dihasilkan oleh AMS

AWS Managed Services (AMS) memungkinkan Anda menerima pemberitahuan peringatan untuk EC2 sumber daya Amazon secara langsung untuk mengurangi keterlambatan komunikasi. Untuk menerima EC2 peringatan Amazon secara langsung, berlangganan target Anda (email pilihan) ke topik Amazon SNS Direct-Customer-Alerts menggunakan Manajemen | Pemantauan dan pemberitahuan | SNS | Berlangganan jenis perubahan (ct-3rc19u1k017wu).

Note

Tidak semua lansiran dasar dikirim ke topik Direct-Customer-Alerts secara default. Untuk melihat semua peringatan yang dihasilkan oleh sistem pemantauan AMS, berlangganan topik Amazon SNS untuk sistem pemantauan AMS. Dalam permintaan, minta “Topik Pemantauan AMS”, tentukan saluran berlangganan untuk menerima peringatan (Lambda, Amazon SQS,

HTTP/S, email, atau SMS), dan tentukan titik akhir (misalnya, alamat email, jika Anda memilih protokol email) yang akan menerima peringatan.

Topik pemantauan AMS menerima peringatan yang digunakan oleh layanan bersama AMS, sehingga bisa berisik.

Untuk mempelajari lebih lanjut, lihat bagian [Berlangganan](#) di referensi API Berlangganan Layanan Pemberitahuan Sederhana Amazon.

Untuk daftar peringatan dasar yang disediakan AMS, lihat. [Peringatan dari pemantauan dasar di AMS](#)

Pemberitahuan peringatan berbasis tag di AMS

Gunakan tag untuk mengirim pemberitahuan peringatan untuk sumber daya Anda ke alamat email yang berbeda. Ini adalah praktik terbaik untuk menggunakan pemberitahuan peringatan berbasis tag karena pemberitahuan yang dikirim ke satu alamat email dapat menyebabkan kebingungan ketika beberapa tim pengembang menggunakan akun yang sama.

Important

Pemberitahuan peringatan berbasis tag hanya berfungsi untuk notifikasi yang terkait dengan Amazon EC2, Amazon EBS, Elastic Load Balancing, Network Load Balancer, Application Load Balancer, Amazon RDS, Amazon Redshift, dan. OpenSearch
Jangan menambahkan informasi identitas pribadi (PII) di tag Anda.

Kirim peringatan ke alamat email tertentu

Tag sumber daya yang memiliki peringatan yang harus dikirim ke alamat email tertentu dengan `key = OwnerTeamEmail,value = EMAIL_ADDRESS`.

Kirim peringatan ke beberapa alamat email

Untuk menggunakan beberapa alamat email, tentukan daftar nilai yang dipisahkan koma.

Misalnya, `key = OwnerTeamEmail,value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, . . .` Jumlah total karakter untuk bidang nilai tidak boleh melebihi 260.

Menggunakan kunci tag kustom

Untuk menggunakan kunci tag kustom, berikan nama kunci tag kustom ke CSDM Anda dalam email yang memberikan persetujuan untuk mengaktifkan notifikasi otomatis untuk komunikasi berbasis tag. Ini adalah praktik terbaik untuk menggunakan strategi penandaan yang sama untuk tag kontak di semua instans dan sumber daya Anda.

Alamat email harus ditentukan secara lengkap, dengan tanda “at” (@) untuk memisahkan bagian lokal dari domain. Contoh alamat email yang tidak valid: *Team.AppATabc.xyz* atau. *john.doe* Untuk panduan umum tentang strategi penandaan Anda, lihat [Menggunakan tag](#). Untuk menandai sumber daya yang ada, kirimkan RFC dengan jenis perubahan Deployment | Advanced stack components | Tag | Create (auto) (ct-3cx7we852p3af).

Note

Nilai kunci *OwnerTeamEmail* tidak harus dalam kasus unta. Namun, tag peka huruf besar/kecil dan praktik terbaik adalah menggunakan format yang disarankan.

Remediasi peringatan otomatis AMS

Setelah verifikasi, AWS Managed Services (AMS) secara otomatis memulihkan peringatan tertentu sesuai dengan kondisi dan proses tertentu yang dijelaskan di bagian ini.

Nama peringatan	Deskripsi	Ambang batas	Tindakan
Saluran aman rusak	Broken Secure Channel Alarm dipicu pada EC2 Instans Windows ketika instance kehilangan koneksi dengan AD Domain Controller.	Ambang batas berada di atas nilai yang ditentukan 10 kali dalam 15 menit terakhir.	Remediasi otomatis AMS memvalidasi bahwa instance sedang online di SSM, nama host tidak diduplikasi, dan Objek Komputer AD selaras dengan tumpukan. CloudFormation Remediasi memperbaiki koneksi saluran aman untuk memulihkan akses ke instance.

Nama peringatan	Deskripsi	Ambang batas	Tindakan
Pemeriksaan Status Gagal	Kemungkinan kegagalan perangkat keras atau keadaan kesalahan instance.	Sistem telah mendeteksi status gagal setidaknya sekali dalam 15 menit terakhir.	Remediasi otomatis AMS pertama kali memvalidasi jika instance dapat diakses. Jika instance tidak dapat diakses, maka instance dihentikan dan dimulai ulang. Stop and start memungkinkan instance untuk bermigrasi ke perangkat keras baru yang mendasarinya. Untuk informasi lebih lanjut, lihat bagian berikut "Otomatisasi Remediasi Kegagalan Pemeriksaan EC2 Status."
AMSLinuxDiskUsage	Picu saat penggunaan disk dari 1 titik pemasangan (ruang yang ditentukan pada volume) pada EC2 instans Anda terisi.	Ambang batas berada di atas nilai yang ditentukan 6 kali pada 30 menit terakhir.	Remediasi otomatis AMS pertama menghapus file sementara. Jika itu tidak membebaskan ruang disk yang cukup, itu memperpanjang volume untuk mencegah downtime jika volume menjadi penuh.

Nama peringatan	Deskripsi	Ambang batas	Tindakan
AMSWindowsDiskUsage	Saat penggunaan disk dari 1 titik pemasangan (ruang yang ditentukan pada volume) pada EC2 instans Anda terisi.	Ambang batas berada di atas nilai yang ditentukan 6 kali selama 30 menit terakhir.	Remediasi otomatis AMS pertama menghapus file sementara. Jika itu tidak membebaskan ruang disk yang cukup, itu memperpanjang volume untuk mencegah downtime jika volume menjadi penuh.

Nama peringatan	Deskripsi	Ambang batas	Tindakan
RDS-EVENT-0089	Instans DB telah mengonsumsi lebih dari 90% dari penyimpanan yang dialokasikan.	Penyimpanan lebih dari 90% dialokasikan.	Remediasi otomatis AMS pertama-tama memvalidasi bahwa DB berada dalam keadaan yang dapat dimodifikasi dan tersedia atau penuh penyimpanan. Kemudian mencoba untuk meningkatkan penyimpanan yang dialokasikan, IOPS, dan throughput penyimpanan melalui changeset. CloudFormation Jika stack drift sudah terdeteksi, itu jatuh kembali ke RDS API untuk mencegah downtime. Fitur ini dapat dipilih keluar dengan menambahkan tag berikut ke Instans RDS DB: <pre>"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".</pre>

Nama peringatan	Deskripsi	Ambang batas	Tindakan
RDS-EVENT-0007	Penyimpanan yang dialokasikan untuk instans DB telah habis. Untuk mengatasinya, alokasikan penyimpanan tambahan.	Penyimpanan dialokasikan 100%.	Remediasi otomatis AMS pertama-tama memvalidasi bahwa DB berada dalam keadaan yang dapat dimodifikasi dan tersedia atau penuh penyimpanan. Kemudian mencoba untuk meningkatkan penyimpanan yang dialokasikan, IOPS, dan throughput penyimpanan melalui <code>changeset</code>. <code>CloudFormation</code> Jika <code>stack drift</code> sudah terdeteksi, itu jatuh kembali ke RDS API untuk mencegah downtime. Fitur ini dapat dipilih keluar dengan menambahkan tag berikut ke Instans RDS DB: <pre>"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".</pre>

Nama peringatan	Deskripsi	Ambang batas	Tindakan
RDS-EVENT-0224	Penyimpanan yang dialokasikan yang diminta mencapai atau melebihi ambang penyimpanan maksimum yang dikonfigurasi.	Ambang penyimpanan maksimum untuk instans DB telah habis atau lebih besar dari atau sama dengan penyimpanan yang dialokasikan yang diminta.	Remediasi otomatis AMS pertama-tama memvalidasi bahwa jumlah penyimpanan RDS yang diminta akan melanggar ambang batas penyimpanan maksimal. Jika dikonfirmasi, AMS mencoba meningkatkan ambang penyimpanan maksimal sebesar 30% dengan CloudFormation set perubahan, atau mengarahkan RDS API jika sumber daya tidak disediakan. CloudFormation Fitur ini dapat dipilih keluar dengan menambahkan tag berikut ke Instans RDS DB: <pre>"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".</pre>

Nama peringatan	Deskripsi	Ambang batas	Tindakan
Kapasitas penyimpanan RDS	Kurang dari 1GB tersisa di penyimpanan yang dialokasikan untuk instans DB.	Penyimpanan dialokasikan 99%.	Remediasi otomatis AMS pertama-tama memvalidasi bahwa DB berada dalam keadaan yang dapat dimodifikasi dan tersedia atau penuh penyimpanan. Kemudian mencoba untuk meningkatkan penyimpanan yang dialokasikan, IOPS, dan throughput penyimpanan melalui <code>changeset</code>. <code>CloudFormation</code> Jika <code>stack drift</code> sudah terdeteksi, itu jatuh kembali ke RDS API untuk mencegah downtime. Fitur ini dapat dipilih keluar dengan menambahkan tag berikut ke Instans RDS DB: "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Amazon EC2 Broken Secure Channel: Catatan otomatisasi remediasi

Sebelum remediasi otomatis AWS Managed Services (AMS) melakukan remediasi pada masalah Amazon EC2 Windows Broken Secure Channel, otomatisasi melakukan pra-pemeriksaan berikut dan membuat laporan insiden untuk penyelidikan lebih lanjut:

- Memvalidasi bahwa status SSM EC2 instans Amazon adalah “Online.”
- Memvalidasi apakah EC2 instans Amazon merupakan bagian dari grup Auto Scaling dan apakah semua instance dalam grup Auto Scaling memiliki nama host yang sama.
- Memeriksa apakah EC2 instance Amazon adalah bagian dari CloudFormation tumpukan yang digunakan untuk menyediakannya. Jika instance telah dihapus dari CloudFormation tumpukan, otomatisasi memverifikasi apakah Active Directory Organizational Unit (OU) terkait masih mereferensikan tumpukan.

Setelah validasi di atas berlalu, otomatisasi berlanjut untuk memulihkan saluran Broken Secure.

Langkah-langkah Remediasi:

- Remediasi otomatis mencoba memperbaiki saluran aman antara EC2 instans dan Domain AD, memulihkan akses ke instans.
- Pasca remediasi otomatisasi memeriksa apakah saluran aman dibuat. Jika tidak berhasil, AMS membuat insiden dan melibatkan operasi AMS untuk menyelidiki.

EC2 kegagalan pemeriksaan status: Catatan otomatisasi remediasi

Cara kerja remediasi otomatis AMS dengan masalah kegagalan pemeriksaan EC2 status:

- Jika EC2 instans Amazon Anda tidak dapat dijangkau, instans harus dihentikan dan dimulai lagi sehingga dapat dimigrasikan ke perangkat keras baru dan dipulihkan.
- Jika akar masalahnya ada di dalam OS (perangkat yang hilang di fstab, korupsi kernel, dan sebagainya), otomatisasi tidak dapat memulihkan instance Anda.
- Jika instans Anda termasuk dalam grup Auto Scaling, otomatisasi tidak memerlukan tindakan—tindakan AutoScalingGroup penskalaan menggantikan instance.
- Jika instans Anda mengaktifkan EC2 Auto Recovery, remediasi tidak akan mengambil tindakan.

EC2 otomatisasi remediasi penggunaan volume

Cara kerja remediasi otomatis AWS Managed Services (AMS) dengan masalah penggunaan EC2 volume:

- Otomatisasi pertama memvalidasi jika ekspansi volume diperlukan dan jika dapat dilakukan. Jika ekspansi dianggap tepat, otomatisasi dapat meningkatkan kapasitas volume. Proses otomatis ini menyeimbangkan kebutuhan akan pertumbuhan dengan ekspansi yang terkendali dan terbatas.
- Sebelum memperluas volume, otomatisasi melakukan tugas pembersihan (Windows: Disk Cleaner, Linux: Logrotate+Penghapusan Log Agen Manajer Layanan Sederhana) pada instance untuk mencoba mengosongkan ruang.

Note

Tugas pembersihan tidak dijalankan pada instance keluarga EC2 “T” karena ketergantungan mereka pada kredit CPU untuk fungsionalitas lanjutan.

- Di Linux, otomatisasi hanya mendukung perluasan sistem file tipe EXT2, EXT3, EXT4 dan XFS.
- Pada Windows, otomatisasi hanya mendukung New Technology File System (NTFS) dan Resilient File System (ReFS).
- Otomatisasi tidak memperluas volume yang merupakan bagian dari Logical Volume Manager (LVM) atau array RAID.
- Otomatisasi tidak memperluas volume penyimpanan instance.
- Otomatisasi tidak mengambil tindakan jika volume yang terpengaruh sudah lebih besar dari 2 TiB.
- Ekspansi melalui otomatisasi dibatasi maksimal tiga kali per minggu dan lima kali total selama masa pakai sistem.
- Otomatisasi tidak memperluas volume jika ekspansi sebelumnya terjadi dalam enam jam terakhir.

Ketika aturan ini mencegah otomatisasi mengambil tindakan, AMS menghubungi Anda melalui permintaan layanan keluar untuk menentukan tindakan selanjutnya yang harus diambil.

Otomatisasi remediasi acara penyimpanan rendah Amazon RDS

Cara kerja remediasi otomatis AWS Managed Services (AMS) dengan masalah peristiwa penyimpanan rendah Amazon RDS:

- Sebelum mencoba memperluas penyimpanan instans Amazon RDS, otomatisasi melakukan beberapa pemeriksaan untuk memastikan instans Amazon RDS berada dalam status yang dapat dimodifikasi dan tersedia, atau penuh penyimpanan.
- Di mana CloudFormation stack drift terdeteksi, remediasi terjadi melalui Amazon RDS API.
- Tindakan remediasi tidak berjalan dalam skenario berikut:
 - Status instans Amazon RDS tidak “tersedia” atau “penuh penyimpanan”.
 - Penyimpanan instans Amazon RDS saat ini tidak dapat dimodifikasi (seperti ketika penyimpanan telah dimodifikasi dalam enam jam terakhir).
 - Instans Amazon RDS memiliki penyimpanan auto-scaling yang diaktifkan.
 - Instans Amazon RDS bukan sumber daya dalam CloudFormation tumpukan.
- Remediasi terbatas pada satu ekspansi per enam jam dan tidak lebih dari tiga ekspansi dalam periode empat belas hari bergulir.
- Ketika skenario ini terjadi, AMS menghubungi Anda dengan insiden keluar untuk menentukan tindakan selanjutnya.

Membuat CloudWatch alarm tambahan di AMS

Anda dapat membuat CloudWatch alarm baru menggunakan Penerapan AWS Managed Services (AMS) | Pemantauan dan pemberitahuan | CloudWatch | Buat jenis perubahan alarm.

Important

AMS tidak memantau CloudWatch alarm yang dibuat oleh Anda.

Menggunakan CloudWatch metrik dan alarm khusus untuk EC2 instans Amazon (hanya berfungsi untuk penerapan yang dapat berubah yang tidak bergantung pada pembaruan yang diterapkan ke AMIs grup Auto Scaling):

1. Menghasilkan skrip pemantauan aplikasi dan metrik kustom Anda. Untuk informasi selengkapnya dan akses ke skrip contoh, lihat [Memantau Memori dan Metrik Disk untuk Instans Amazon EC2 Linux](#). Skrip CloudWatch pemantauan Amazon untuk EC2 instans Amazon Linux menunjukkan cara memproduksi dan menggunakan metrik CloudWatch khusus Amazon. Sampel skrip Perl ini terdiri atas contoh yang berfungsi penuh yang melaporkan metrik pemanfaatan memori, swap, dan ruang disk untuk instans Linux.

2. Unggah skrip pemantauan Anda. Untuk mengunggah skrip pemantauan ke grup Auto Scaling atau konfigurasi EC2 instans Amazon, Anda dapat menggunakan UserData saat mengonfigurasi grup Auto Scaling atau instans EC2 Amazon, atau, jika aplikasi Anda digunakan, Anda dapat memodifikasi konfigurasi CodeDeploy dengan Deployment | Applications | application CodeDeploy | Deploy CT (ct-2edc3sd1sqmrb).
3. Publikasikan metrik kustom Anda ke CloudWatch (saat pertama kali memublikasikan titik data untuk metrik kustom baru, metrik tersebut dibuat), lihat [Menerbitkan Metrik Kustom](#).
4. Buat CloudWatch alarm, lihat [Membuat CloudWatch Alarm untuk Instance](#).

 Important

Data pemantauan harus dikirim ke jalur ini [infra/INSTANCE_ID/YOUR_CUSTOM_METRIC]

Untuk mengubah atau menghapus CloudWatch alarm, kirimkan RFC dengan Manajemen | Lainnya | Lainnya | Buat jenis perubahan (ct-1e1xtak34nx76) dengan parameter yang diperlukan untuk menyelesaikan tindakan seperti yang dijelaskan dalam referensi Amazon API. CloudWatch [PutMetricAlarm](#)

Anda dapat menggunakan aliran CloudWatch acara. AMS terintegrasi dengan CloudWatch dan Anda dapat meminta agar panggilan AWS API apa pun memicu CloudWatch peristiwa.

Untuk melakukan ini, kirimkan Manajemen | Lainnya | Lainnya | Perbarui CT (ct-0xdawir96cy7k) dengan panggilan API yang Anda minati. Operator AMS akan berbicara dengan Anda untuk mengumpulkan persyaratan. Untuk mempelajari lebih lanjut, lihat [CloudWatch Dokumentasi Amazon](#).

Untuk mendapatkan akses ke aliran CloudWatch acara, kirimkan Manajemen | Lainnya | Lainnya | Perbarui CT (ct-0xdawir96cy7k) untuk menambahkan pesta ke topik notifikasi SNS. Operator AMS akan berbicara dengan Anda untuk mengumpulkan persyaratan.

Membuat CloudWatch metrik dan alarm khusus di AMS

Anda dapat menyimpan metrik bisnis dan aplikasi Anda di Amazon CloudWatch. Anda dapat melihat grafik, dan menyetel alarm berdasarkan metrik ini, seperti yang dapat Anda lakukan untuk metrik yang CloudWatch sudah disimpan untuk sumber daya AWS Managed Services (AMS) Anda. Untuk mempelajari selengkapnya CloudWatch, lihat [CloudWatch Konsep Amazon](#).

Amazon SNS memungkinkan aplikasi mengirim pesan penting waktu ke beberapa pelanggan melalui mekanisme “push” terhadap AMS Managed Monitoring System atau MMS, topik Amazon SNS (SNS) tempat alarm dipublikasikan; dalam hal ini, MMS dan antrian SQS Anda. Anda dapat menggunakan CloudWatch untuk membuat metrik khusus dan, melalui topik SNS, memiliki alarm AMS Anda dengan tepat. Untuk melakukan ini, ikuti langkah-langkah ini.

Note

Proses ini tidak berfungsi untuk penerapan yang tidak dapat diubah yang mengandalkan pembaruan yang diterapkan AMIs ke grup Auto Scaling, ini cocok untuk penerapan aplikasi yang dapat berubah (bukan ASG).

Menyiapkan metrik khusus dalam batasan AMS Advanced, adalah tugas yang kompleks. Untuk contoh dari CloudWatch, lihat [Contoh: Menghitung kemunculan istilah](#).

1. Buat skrip pemantauan aplikasi dan metrik kustom Anda (seperti contoh kemunculan hitungan). Untuk informasi selengkapnya dan akses ke skrip contoh, lihat [Memantau Memori dan Metrik Disk untuk Instans Amazon EC2 Linux](#).
2. Unggah skrip pemantauan Anda. Untuk mengunggah skrip pemantauan ke grup Auto Scaling atau konfigurasi EC2 instans Amazon, Anda dapat menggunakan UserData saat mengonfigurasi grup Auto Scaling atau instans EC2 Amazon, atau, jika aplikasi Anda digunakan, Anda dapat memodifikasi konfigurasi CodeDeploy dengan Deployment | Applications | application CodeDeploy | Deploy CT (ct-2edc3sd1sqmrb).
3. Publikasikan metrik kustom Anda ke CloudWatch (saat pertama kali memublikasikan titik data untuk metrik kustom baru, metrik tersebut dibuat), lihat [Publikasikan Metrik Kustom](#).
4. Untuk mengintegrasikan metrik pelanggan Anda ke sistem pemantauan aplikasi Anda, minta AMS membuat topik SNS untuk metrik dengan mengirimkan RFC dengan Deployment | Monitoring dan notifikasi | SNS | Buat jenis perubahan (ct-3dfnglm4ombbs).
5. Buat CloudWatch alarm, lihat [Membuat CloudWatch Alarm Amazon](#).

Important

Data pemantauan harus dikirim ke jalur ini [infra/*INSTANCE_ID*/*YOUR_CUSTOM_METRIC*].

Menggunakan CloudWatch Application Insights untuk server .Net dan SQL di AMS

Anda dapat menggunakan Amazon CloudWatch Application Insights untuk menyiapkan monitor untuk sumber daya aplikasi AWS Managed Services (AMS) Anda untuk terus menganalisis data untuk tanda-tanda masalah dengan aplikasi Anda dan mengurangi mean time to repair (MTTR) saat memecahkan masalah aplikasi. Untuk detail tentang Wawasan CloudWatch Aplikasi, lihat [Wawasan CloudWatch Aplikasi untuk.NET dan SQL Server](#).

Important

AMS tidak memantau masalah dari CloudWatch Application Insights karena mereka untuk kode aplikasi yang dikendalikan oleh Anda.

Untuk menggunakan CloudWatch Application Insights, kirimkan RFC dengan Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat entitas atau kebijakan (diperlukan tinjauan) jenis perubahan (ct-3dpd8mdd9jn1r) dengan permintaan untuk membuat peran IAM yang memberi Anda izin untuk mengonfigurasi Wawasan Aplikasi. CloudWatch Ada dua opsi untuk menerima masalah yang diidentifikasi: melalui topik SNS atau dengan target dalam aturan CloudWatch Acara. Di RFC, tentukan yang Anda inginkan. Jika Anda berencana untuk menggunakan aturan CloudWatch Peristiwa, tentukan juga definisi aturan di RFC. Setelah Anda mengatur dengan CloudWatch Application Insights, Anda menerima pemberitahuan tentang potensi masalah termasuk wawasan yang mengarah ke kemungkinan akar penyebab.

Untuk mempelajari cara Anda dapat mengambil peran, lihat Panduan Onboarding AMS [Menggabungkan Direktori Aktif Anda dengan Peran IAM AMS](#).

Menggunakan Aturan EventBridge Terkelola Amazon di AMS

AMS Advanced menggunakan Aturan EventBridge Terkelola Amazon. Aturan Terkelola adalah jenis aturan unik yang terhubung langsung ke AMS. Aturan ini cocok dengan peristiwa yang masuk dan mengirimkannya ke target untuk diproses. Aturan Terkelola telah ditentukan sebelumnya oleh AMS dan menyertakan pola peristiwa yang diperlukan oleh layanan untuk mengelola akun pelanggan, dan kecuali ditentukan lain, hanya layanan pemilik yang dapat menggunakan Aturan Terkelola ini.

Aturan Terkelola AMS ditautkan ke prinsipal `events.managedservices.amazonaws.com` layanan. Aturan Terkelola ini dikelola melalui peran

[AWSServiceRoleForManagedServices_Eventsterkait layanan](#). Untuk menghapus aturan ini diperlukan konfirmasi khusus oleh pelanggan. Untuk informasi selengkapnya, lihat [Menghapus Aturan Terkelola untuk AMS](#).

Untuk informasi selengkapnya tentang aturan, lihat [Aturan](#) di Panduan EventBridge Pengguna Amazon.

Aturan EventBridge Terkelola Amazon yang diterapkan oleh AMS

Aturan yang EventBridge Dikelola Amazon

Nama Aturan	Deskripsi	Definisi
AMSAdvancedCoreRule	Aturan ini meneruskan CloudWatch Alarm Amazon ke Pemantauan AMS. CloudWatch Alarm Acara Amazon memantau CloudWatch Alarm.	<pre>{ { "source": ["aws.cloudwatch"], "detail-type": ["CloudWatch Alarm State Change"], } }</pre>

Membuat Aturan Terkelola untuk AMS

Anda tidak perlu membuat Aturan EventBridge Terkelola Amazon secara manual. Saat Anda melakukan onboard ke AMS di AWS Management Console AWS CLI, the, atau AWS API, AMS membuatnya untuk Anda.

Mengedit Aturan Terkelola untuk AMS

AMS tidak mengizinkan Anda mengedit Aturan Terkelola. Nama dan pola acara untuk setiap Aturan Terkelola telah ditentukan sebelumnya oleh AMS.

Menghapus Aturan Terkelola untuk AMS

Anda tidak perlu menghapus Aturan Terkelola secara manual. Saat Anda keluar dari AMS di AWS Management Console, Management Console AWS CLI, atau AWS API, AMS akan membersihkan resource dan menghapus semua Aturan Terkelola yang dimiliki AMS untuk Anda.

Jika AMS gagal menghapus Aturan Terkelola selama offboarding, Anda juga dapat menggunakan EventBridge konsol Amazon, AWS CLI atau AWS API untuk menghapus Aturan Terkelola secara manual. Untuk melakukan ini, Anda harus terlebih dahulu lepas dari AMS dan melakukan penghapusan paksa Aturan Terkelola.

Remediator Tepercaya di AMS

Trusted Remediator adalah solusi AWS Managed Services yang mengotomatiskan remediasi dan rekomendasi. [AWS Trusted Advisor](#) [AWS Compute Optimizer](#) Trusted Remediator membuat rekomendasi kapan Trusted Advisor dan Compute Optimizer menunjukkan peluang bagi Anda untuk mengurangi biaya, meningkatkan ketersediaan sistem, mengoptimalkan kinerja, atau menutup celah keamanan untuk Anda. Akun AWS Dengan Trusted Remediator, Anda dapat mengatasi rekomendasi keamanan, kinerja, pengoptimalan biaya, toleransi kesalahan, dan batas layanan ini dengan cara yang aman dan terstandarisasi yang menggunakan praktik terbaik yang telah ditetapkan. Trusted Remediator memungkinkan Anda untuk mengkonfigurasi solusi remediasi dan berjalan secara otomatis pada jadwal yang Anda buat, menyederhanakan proses remediasi. Pendekatan yang disederhanakan ini membahas masalah secara konsisten, efisien, dan tanpa intervensi manual.

Manfaat utama Remediator Tepercaya

Berikut ini adalah manfaat utama dari Trusted Remediator:

- Peningkatan keamanan, kinerja, dan pengoptimalan biaya: Remediator Tepercaya membantu Anda meningkatkan postur keamanan keseluruhan akun Anda, mengoptimalkan pemanfaatan sumber daya, dan mengurangi biaya operasional.
- Pengaturan dan konfigurasi swalayan: Anda dapat mengonfigurasi Remediator Tepercaya agar sesuai dengan kebutuhan dan preferensi Anda.
- Trusted Advisor Pemeriksaan otomatis dan perbaikan AWS Compute Optimizer rekomendasi: Setelah konfigurasi, Trusted Remediator secara otomatis menjalankan tindakan remediasi untuk pemeriksaan yang dipilih. Otomatisasi ini menghilangkan kebutuhan akan intervensi manual.
- Implementasi praktik terbaik: Tindakan remediasi didasarkan pada praktik terbaik yang telah ditetapkan, sehingga masalah ditangani dengan cara yang standar dan efektif.

- Eksekusi terjadwal: Anda dapat memilih jadwal remediasi yang sesuai dengan alur kerja day-to-day operasional Anda.

Trusted Remediator memberdayakan Anda untuk secara proaktif mengatasi masalah yang teridentifikasi di AWS lingkungan Anda, membantu Anda mematuhi praktik terbaik dan memelihara infrastruktur cloud yang aman, berkinerja tinggi, dan hemat biaya.

Cara kerja Remediator Tepercaya

Berikut ini adalah ilustrasi alur kerja Remediator Tepercaya:

Trusted Remediator menilai Trusted Advisor dan rekomendasi Compute Optimizer untuk Anda dan membuatnya. Akun AWS Systems Manager [OpsItems](#) OpsCenter Kemudian, Anda dapat menggunakan dokumen otomatisasi Remediator Tepercaya untuk memulihkan OpsItems secara otomatis atau manual. Berikut ini adalah rincian untuk setiap jenis remediasi:

- Remediasi otomatis: Remediator Tepercaya menjalankan dokumen otomatisasi dan memantau jalannya. Setelah dokumen otomatisasi selesai, Remediator Tepercaya menyelesaikan Opsitem.
- Remediasi manual: Remediator Tepercaya menciptakan OpsItem untuk Anda tinjau. Setelah meninjau, Anda dapat membuat RFC otomatis, [Remediator Tepercaya | Finding | Remediate](#), ubah jenis untuk memulihkan sumber daya. Untuk informasi tentang langkah-langkah remediasi manual, lihat [Jalankan remediasi manual di Remediator Tepercaya](#).

Log remediasi disimpan dalam bucket Amazon S3. Anda dapat menggunakan data di bucket S3 untuk membuat QuickSight dasbor khusus untuk pelaporan. AMS juga menyediakan laporan berdasarkan permintaan untuk Remediator Tepercaya. Untuk menerima laporan ini, hubungi CSDM Anda.

Istilah kunci untuk Remediator Tepercaya

Berikut ini adalah istilah yang berguna untuk diketahui ketika Anda menggunakan Trusted Remediator di AMS:

- AWS Trusted Advisor dan AWS Compute Optimizer: Layanan pengoptimalan cloud yang disediakan oleh AWS. Trusted Advisor dan Compute Optimizer memeriksa lingkungan AWS Anda dan memberikan rekomendasi berdasarkan praktik terbaik dalam enam kategori berikut:

- Optimalisasi biaya
- Performa
- Keamanan
- Toleransi kesalahan
- Keunggulan operasional
- Batas layanan

Untuk informasi selengkapnya, lihat [AWS Trusted Advisor](#) dan [AWS Compute Optimizer](#).

- Remediator Terpercaya: Solusi remediasi AMS untuk [Trusted Advisor](#) pemeriksaan dan [AWS Compute Optimizer](#) rekomendasi. Trusted Remediator membantu Anda memulihkan Trusted Advisor pemeriksaan dan rekomendasi Compute Optimizer dengan aman dengan praktik terbaik yang dikenal untuk meningkatkan keamanan, kinerja, dan mengurangi biaya. Trusted Remediator mudah diatur dan dikonfigurasi. Anda mengonfigurasi sekali, dan Trusted Remediator menjalankan remediasi sesuai jadwal pilihan Anda (harian atau mingguan).
- AWS Systems Manager Dokumen SSM: File JSON atau YAMM yang mendefinisikan tindakan yang AWS Systems Manager dilakukan pada sumber daya Anda. AWS Dokumen SSM berfungsi sebagai spesifikasi deklaratif untuk mengotomatiskan tugas operasional di berbagai AWS sumber daya dan instance.
- AWS Systems Manager OpsCenter OpsItem Sumber daya manajemen masalah operasional cloud yang membantu Anda melacak dan menyelesaikan masalah operasional di AWS lingkungan Anda. OpsItems memberikan pandangan terpusat dan sistem manajemen untuk data operasional dan isu-isu di seluruh Layanan AWS dan sumber daya. Masing-masing OpsItem mewakili masalah operasional, seperti risiko keamanan potensial, masalah kinerja, atau insiden operasional.
- Konfigurasi: Konfigurasi adalah seperangkat atribut [yang disimpan di AWS AppConfig, kemampuan AWS Systems Manager](#). Aplikasi Trusted Remediator AWS AppConfig membantu mengonfigurasi remediasi di tingkat akun.
- Mode eksekusi: Mode eksekusi adalah atribut konfigurasi yang menentukan cara menjalankan remediasi untuk setiap hasil Trusted Advisor pemeriksaan. Ada empat mode eksekusi yang didukung: Otomatis, Manual, Bersyarat, Tidak Aktif.
- Penggantian sumber daya: Fitur ini menggunakan tag sumber daya untuk mengganti konfigurasi sumber daya tertentu.
- Log item remediasi: File log di bucket log S3 remediasi Remediator Terpercaya. Log item remediasi dibuat saat remediasi OpsItems dibuat. File log ini berisi remediasi eksekusi manual OpsItems dan remediasi eksekusi otomatis. OpsItems Gunakan file log ini untuk melacak semua item remediasi.

- Log eksekusi remediasi otomatis: File log di bucket log S3 remediasi Remediator Tepercaya. Log eksekusi remediasi otomatis dibuat ketika otomatis menjalankan dokumen SSM selesai. Log ini berisi rincian eksekusi SSM untuk OpsItems remediasi eksekusi otomatis. Gunakan file log ini untuk melacak remediasi otomatis.

Memulai Remediator Tepercaya di AMS

Remediator Tepercaya tersedia di AMS tanpa biaya tambahan. Trusted Remediator mendukung konfigurasi akun tunggal dan multi-akun.

Onboard ke Remediator Tepercaya

Untuk memasukkan akun AMS Anda ke Remediator Tepercaya, kirimkan email ke Cloud Architects atau Cloud Service Delivery Manager (). CSDMs Dalam email, sertakan informasi berikut:

- Akun AWS: Nomor identifikasi akun dua belas digit. Semua akun yang ingin Anda onboard ke Trusted Remediator harus milik pelanggan AMS Advanced yang sama.
- Akun administrator yang didelegasikan: Akun yang digunakan untuk Trusted Advisor dan Compute Optimizer memeriksa konfigurasi untuk satu atau beberapa akun.
- Akun anggota: Ini adalah akun yang ditautkan ke akun administrator yang didelegasikan. Akun ini mewarisi konfigurasi dari akun administrator yang didelegasikan. Anda dapat memiliki satu akun anggota atau beberapa akun anggota.

Note

Akun anggota mewarisi konfigurasi dari akun administrator yang didelegasikan. Jika Anda memerlukan konfigurasi berbeda untuk akun tertentu, ikuti beberapa akun administrator yang didelegasikan dengan konfigurasi pilihan Anda. Rencanakan struktur akun dan konfigurasi dengan Cloud Architects sebelum Anda onboard.

- Wilayah AWS: Di Wilayah AWS mana sumber daya Anda berada. Untuk daftar Wilayah AWS, lihat [Layanan AWS berdasarkan Wilayah](#).
- Jadwal dan waktu remediasi: Jadwal remediasi pilihan Anda (harian atau mingguan). Trusted Remediator mengumpulkan Trusted Advisor cek dan memulai remediasi pada waktu yang dijadwalkan. Misalnya, Anda dapat mengatur jadwal remediasi untuk 1:00 pagi hari Minggu setiap minggu, Waktu Standar Timur Australia.

- Email pemberitahuan: Remediator Tepercaya menggunakan email notifikasi untuk memberi tahu Anda setiap hari jika ada perbaikan. Subjek email notifikasi adalah “Ringkasan remediasi Remediator Tepercaya” dan isinya memberikan informasi tentang remediasi Remediator Tepercaya yang dijalankan dalam 24 jam terakhir.

Note

Tinjau aplikasi dan sumber daya Anda setelah setiap perbaikan terjadwal. Untuk dukungan tambahan, hubungi AMS.

Setelah Anda mengirimkan permintaan onboard Anda dengan rincian yang diperlukan ke CA atau CSDM Anda, AMS akan memasukkan akun Anda ke Remediator Tepercaya. Trusted Remediator menggunakan AWS AppConfig AWS Systems Manager, kemampuan, untuk menentukan konfigurasi untuk Trusted Advisor pemeriksaan. Konfigurasi ini adalah seperangkat atribut yang disimpan di AWS AppConfig. Untuk mencegah tagihan yang tidak sah ke sumber daya Anda, semua Trusted Advisor pemeriksaan yang didukung disetel ke Tidak Aktif saat akun di-onboard ke Remediator Tepercaya. Konfigurasi ini membantu Anda memulihkan Trusted Advisor pemeriksaan tertentu secara otomatis, atau untuk menilai dan memulihkan pemeriksaan yang tersisa secara manual. Konfigurasi sangat dapat disesuaikan, memungkinkan Anda menerapkan konfigurasi untuk setiap pemeriksaan. Trusted Advisor Untuk informasi selengkapnya, lihat [Konfigurasi remediasi Trusted Advisor cek di Remediator Tepercaya](#).

Konfigurasi Remediator Tepercaya di Akun AWS

Saat orientasi selesai, CA atau CSDM Anda memberi tahu Anda dan konfigurasi default dibuat di administrator yang didelegasikan. Akun AWS Konfigurasi disimpan di AWS AppConfig bawah aplikasi Trusted Remediator. Anda dapat menggunakan [Manajemen RFC | Remediator Tepercaya | Konfigurasi remediasi | Pembaruan untuk meminta pembaruan](#) konfigurasi. Untuk informasi selengkapnya, lihat [Konfigurasi remediasi Trusted Advisor cek di Remediator Tepercaya](#).

Untuk melihat konfigurasi Remediator Tepercaya default, selesaikan langkah-langkah berikut:

1. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.

Note

Pastikan Anda berada di akun administrator yang didelegasikan.

2. Pilih Manajemen Aplikasi, AppConfig.
3. Pilih Trusted Remediator dari daftar aplikasi.

Berikut ini adalah contoh AWS AppConfig konsol yang menunjukkan konfigurasi Remediator Tepercaya:

Pilih cek dan rekomendasi untuk diperbaiki

Secara default, mode eksekusi remediasi tidak aktif untuk semua Trusted Advisor pemeriksaan dan rekomendasi Compute Optimizer dalam konfigurasi Anda. Ini mencegah remediasi yang tidak sah dan melindungi sumber daya. AMS menyediakan dokumen otomatisasi SSM yang dikuratori untuk perbaikan Trusted Advisor pemeriksaan.

Untuk memilih pemeriksaan yang ingin diperbaiki dengan Trusted Remediator, selesaikan langkah-langkah berikut:

1. Tinjau daftar [rekomendasi Compute Optimizer yang didukung Trusted Advisor dan dan nama dokumen otomatisasi SSM terkait](#) untuk memutuskan pemeriksaan dan rekomendasi mana yang ingin Anda perbaiki dengan Trusted Remediator.
2. Kirim [Manajemen | Remediator Tepercaya | Konfigurasi remediasi | Perbarui](#) permintaan untuk memperbarui konfigurasi untuk pemeriksaan yang Anda pilih Trusted Advisor . Untuk petunjuk tentang cara memilih cek, lihat [Konfigurasikan remediasi Trusted Advisor cek di Remediator Tepercaya](#).

Lacak remediasi Anda di Remediator Tepercaya

Setelah memperbarui konfigurasi tingkat akun, Trusted Remediator membuat OpsItems untuk setiap remediasi. Trusted Remediator menjalankan dokumen SSM untuk remediasi otomatis OpsItems sesuai dengan jadwal remediasi Anda. Untuk petunjuk tentang cara melihat semua remediasi OpsItems dari OpsCenter konsol Systems Manager, lihat [Lacak remediasi di Remediator Tepercaya](#).

Jalankan remediasi manual di Remediator Tepercaya

Anda dapat memulihkan Trusted Advisor pemeriksaan secara manual menggunakan RFC otomatis. Ketika Anda memilih remediasi manual, Trusted Remediator membuat eksekusi manual. OpsItem Lihat informasi yang lebih lengkap di [Jalankan remediasi manual di Remediator Tepercaya](#).

Rekomendasi Compute Optimizer didukung oleh Trusted Remediator

Tabel berikut mencantumkan rekomendasi Compute Optimizer yang didukung, dokumen otomatisasi SSM, parameter yang telah dikonfigurasi sebelumnya, dan hasil yang diharapkan dari dokumen otomatisasi. Tinjau hasil yang diharapkan untuk membantu Anda memahami kemungkinan risiko berdasarkan kebutuhan bisnis Anda sebelum Anda mengaktifkan dokumen otomatisasi SSM untuk perbaikan pemeriksaan.

Pastikan bahwa aturan konfigurasi yang sesuai untuk setiap pemeriksaan Compute Optimizer hadir untuk pemeriksaan yang didukung yang ingin Anda aktifkan remediasi. Untuk informasi selengkapnya, lihat [Memilih AWS Compute Optimizer untuk Trusted Advisor pemeriksaan](#).

Opsi pengoptim alan	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung

Pengukuran Hak

Rekomendasi EC2 instans Amazon	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation Jenis EC2 instans Amazon diperbarui sesuai rekomendasi Compute Optimizer. Opsi yang paling optimal dipilih sambil mempertahankan parameter platform yang sama (Arsitektur, Hypervisor, antarmuka Jaringan, jenis Virtualisasi, dan sebagainya) jika opsi ada.	- MinimumDaysSinceLastChange: Parameter untuk menentukan jumlah minimum hari sejak perubahan jenis contoh terakhir. Konfigurasi default adalah 7 hari. - Tidak ada kendala - Buat AMIBefore Ubah Ukuran: Untuk membuat instance AMI sebagai cadangan sebelum mengubah ukuran, setel ke 'Benar.' Untuk tidak membuat cadangan, atur ke 'False.' Defaultnya adalah 'True'. - Tidak ada kendala
Rekomendasi volume Amazon EBS	AWSManagedServices-ModifyEBSVolume	CreateSnapshot: Untuk membuat snapshot sebelum memodifikasi volume, atur ke 'Benar.' Untuk

Opsi pengoptim alan	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
	Volume Amazon EBS dimodifikasi sesuai dengan rekomendasi Compute Optimizer. Modifikasi dapat mencakup jenis volume, ukuran, IOPS, generasi volume (gp2, gp3 dll).	tidak membuat snapshot, atur ke 'False.' Defaultnya adalah 'True'. Tidak ada kendala • VolumeType: Jenis volume yang diinginkan. Jika tidak ada tipe yang ditentukan, tipe yang ada dipertahankan. Tidak ada kendala • VolumeSize: Ukuran volume yang diinginkan, dalam GiB. Ukuran volume target harus lebih besar dari atau sama dengan ukuran volume yang ada. Jika tidak ada ukuran yang ditentukan, ukuran yang ada dipertahankan. Tidak ada kendala • Iops: Jumlah I/O operasi per detik yang diminta (IOPS). Parameter ini hanya berlaku untuk volume io1, io2 dan gp3. Tidak ada kendala • Throughput: Throughput untuk penyediaan volume, dengan maksimum 1000 MiB/s. Parameter ini hanya berlaku untuk volume gp3. Tidak ada kendala

Opsi pengoptim alan	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
		RemediateStackDrift: Untuk memulai remediasi drift, jika ada penyimpangan yang disebabkan oleh modifikasi volume, atur ke 'Benar.' Untuk tidak mencoba remediasi drift, atur ke 'False.' Defaultnya adalah 'True'. Tidak ada kendala
Rekomendasi fungsi Lambda	AWSManagedServices-TrustedRemediatorOptimizeLambdaMemory AWS Lambda memori fungsi dioptimalkan sesuai dengan rekomendasi Compute Optimizer.	RecommendedMemorySize : Ukuran memori khusus, jika berbeda dari opsi yang direkomendasikan. Tidak ada kendala

Sumber daya mengganggu

Volume Amazon EBS yang mengganggu	AWSManagedServices-DeleteUnusedEBSVolume Volume Amazon EBS yang tidak terpasang akan dihapus.	- CreateSnapshot: Untuk membuat snapshot sebelum menghapus volume, atur ke 'Benar.' Untuk tidak membuat snapshot, atur ke 'False.' Defaultnya adalah 'True'. Tidak ada kendala - MinimumUnattachedDays: Hari minimum yang tidak terikat dari volume Amazon EBS untuk dihapus, hingga 62 hari. Defaultnya adalah 7. Tidak ada kendala

Opsi pengoptim alan	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Contoh Amazon EC2 yang menganggur	AWSManagedServices-StopEC2 Instance EC2 Instans Amazon yang menganggur akan dihentikan.	ForceStopWithInstanceStore: Untuk memaksa berhenti untuk instance menggunakan penyimpan an instance, setel ke 'True.' Untuk tidak memaksa berhenti, atur ke 'False.' Nilai default 'False' mencegah instance berhenti. Tidak ada kendala
Contoh RDS Amazon yang menganggur	AWSManagedServices-StopIdle RDSInstance Hentikan instans Amazon RDS yang menganggur. Mesin yang didukung adalah: MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQ L. Dokumen ini tidak berlaku untuk Aurora MySQL dan Aurora PostgreSQL. Instans akan dihentika n hingga 7 hari dan diluncurkan kembali secara otomatis.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Trusted Advisor cek yang didukung oleh Trusted Remediator

Tabel berikut mencantumkan Trusted Advisor pemeriksaan yang didukung, dokumen otomatisasi SSM, parameter yang telah dikonfigurasi sebelumnya, dan hasil yang diharapkan dari dokumen otomatisasi. Tinjau hasil yang diharapkan untuk membantu Anda memahami kemungkinan risiko berdasarkan kebutuhan bisnis Anda sebelum Anda mengaktifkan dokumen otomatisasi SSM untuk perbaikan pemeriksaan.

Pastikan bahwa aturan konfigurasi yang sesuai untuk setiap Trusted Advisor pemeriksaan ada untuk pemeriksaan yang didukung yang ingin Anda aktifkan remediasi. Untuk informasi selengkapnya, lihat

Lihat [AWS Trusted Advisor pemeriksaan yang didukung oleh AWS Config](#). Jika pemeriksaan memiliki AWS Security Hub kontrol yang sesuai, pastikan kontrol Security Hub diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan kontrol di Security Hub](#). Untuk informasi tentang mengelola parameter yang telah dikonfigurasi sebelumnya, lihat [Mengonfigurasi Trusted Advisor memeriksa remediasi](#) di Remediator Tepercaya.

Trusted Advisor pemeriksaan optimasi biaya yang didukung oleh Trusted Remediator

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Z4 AUBRNSmz Alamat IP Elastis yang Tidak Terkait	AWSManagedServices-TrustedRemediatorReleaseElasticIP Merilis alamat IP elastis yang tidak terkait dengan sumber daya apa pun.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c18d2gz150 - Instans Amazon dihentikan EC2	AWSManagedServices-TerminatedEC2 InstanceStoppedForPeriodOfTime - EC2 Instans Amazon dihentikan selama beberapa hari dihentikan.	• Buat AMIBefore Pengakhiran: Untuk membuat instance AMI sebagai cadangan sebelum menghentikan EC2 instans Amazon, pilih <code>true</code>. Untuk tidak membuat cadangan sebelum mengakhiri, pilih <code>false</code>. Nilai default-nya <code>true</code>. • AllowedDays: Jumlah hari instance dalam status berhenti sebelum dihentikan. Bawaannya adalah 30. Tidak ada kendala
c18d2gz128 Repositori Amazon ECR Tanpa Kebijakan	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy Membuat kebijakan siklus hidup untuk repositori yang ditentukan jika kebijakan siklus hidup belum ada.	ImageAgeLimit: Batas usia maksimum dalam beberapa hari (1-365) untuk gambar 'apa pun' di repositori Amazon ECR. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Siklus Hidup Dikonfigurasi		
DAvU99Dc4C Volume Amazon EBS yang Kurang Digunakan	<code>AWSManagedServices-DeleteUnusedEBSVolume</code> Menghapus volume Amazon EBS yang kurang dimanfaatkan jika volume tidak terhubung selama 7 hari terakhir. Snapshot Amazon EBS dibuat secara default.	• <code>CreateSnapshot</code>: Jika disetel ke <code>true</code>, maka otomatisasi akan membuat snapshot volume Amazon EBS sebelum dihapus. Pengaturan default-nya adalah <code>true</code>. Nilai yang valid adalah <code>true</code> dan <code>false</code> (peka huruf besar/kecil). • <code>MinimumUnattachedDays</code>: Minimum hari yang tidak terikat dari volume EBS untuk dihapus, hingga 62 hari. Jika disetel ke <code>0</code>, maka dokumen SSM tidak memeriksa periode yang tidak terpasang dan menghapus volume jika volume saat ini tidak terpasang. Defaultnya adalah nilai <code>7</code>. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
hj M8 LMh88u Penyeimbang Beban Idle	AWSManagedServices-DeleteIdleClassicLoadBalancer Menghapus Classic Load Balancer idle jika tidak digunakan dan tidak ada instance yang terdaftar.	IdleLoadBalancerDays: Jumlah hari Classic Load Balancer memiliki 0 koneksi yang diminta sebelum menganggapnya idle. Defaultnya adalah tujuh hari. Jika eksekusi otomatis diaktifkan, otomatisasi akan menghapus Classic Load Balancer yang tidak aktif jika tidak ada instance back-end yang aktif. Untuk semua Classic Load Balancer idle yang memiliki instans back-end aktif, tetapi tidak memiliki instans back-end yang sehat, remediasi otomatis tidak digunakan dan untuk remediasi manual dibuat. OpsItems
Ti39halfu8 Instans DB Idle Amazon RDS	AWSManagedServices-StopIdleRDSInstance Instans Amazon RDS DB yang telah dalam keadaan idle selama tujuh hari terakhir dihentikan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
COr6dfpM05 AWS Lambda fungsi yang disediakan secara berlebihan untuk ukuran memori	AWSManagedServices-ResizeLambdaMemory AWS Lambda ukuran memori fungsi diubah ukurannya ke ukuran memori yang direkomendasikan yang disediakan oleh Trusted Advisor.	RecommendedMemorySize: Alokasi memori yang direkomendasikan untuk fungsi Lambda. Rentang nilai antara 128 dan 10240. Jika ukuran fungsi Lambda dimodifikasi sebelum otomatisasi berjalan, maka pengaturan mungkin ditimpa oleh otomatisasi ini dengan nilai yang direkomendasikan oleh Trusted Advisor
QCH7DWOUX1 Instans Amazon EC2 Pemanfaatan Rendah	AWSManagedServices-StopEC2Instance (Dokumen SSM default untuk mode eksekusi auto dan manual.) EC2 Instans Amazon dengan pemanfaatan rendah dihentikan.	ForceStopWithInstanceStore: Setelah <code>true</code> untuk memaksa instance berhenti menggunakan penyimpanan instance. Jika tidak, atur ke <code>false</code> . Nilai default <code>false</code> mencegah instance berhenti. Nilai yang valid adalah <code>true</code> atau <code>false</code> (case-sensitive). Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
QCH7DWOUX1 Instans Amazon EC2 Pemanfaatan Rendah	AWSManagedServices-ResizeInstanceByOneLevel EC2 Instance Amazon diubah ukurannya dengan satu tipe instance ke bawah dalam tipe keluarga instance yang sama. Instance dihentikan dan dimulai selama operasi pengubahan ukuran dan dikembalikan ke keadaan awal setelah dokumen SSM berjalan selesai. Otomatisasi ini tidak mendukung pengubahan ukuran instans yang ada di Grup Auto Scaling.	• MinimumDaysSinceLastChange: Jumlah hari minimum sejak perubahan jenis instance terakhir. Jika jenis instance dimodifikasi dalam waktu tertentu, maka jenis instance tidak berubah. Gunakan 0 untuk melewati validasi ini. Nilai default-nya 7. • Buat AMIBefore Ubah Ukuran: Untuk membuat instance AMI sebagai cadangan sebelum mengubah ukuran, pilih <code>true</code>. Untuk tidak membuat cadangan, pilih <code>false</code>. Nilai default-nya <code>false</code>. Nilai yang valid adalah <code>true</code> dan <code>false</code> (peka huruf besar/kecil). • ResizeIfStopped: Untuk melanjutkan dengan perubahan ukuran instance, bahkan jika instance dalam keadaan berhenti, pilih <code>true</code>. Untuk tidak mengubah ukuran instance secara otomatis jika dalam keadaan berhenti, pilih <code>false</code>. Nilai yang valid adalah <code>true</code> dan <code>false</code> (peka huruf besar/kecil). Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
QCH7DWOUX1 Instans Amazon EC2 Pemanfaatan Rendah	AWSManagedServices-TerminateInstance EC2 Instans Amazon yang digunakan rendah dihentikan jika bukan bagian dari Grup Auto Scaling dan perlindungan penghentian tidak diaktifkan. AMI dibuat secara default.	Create AMIBefore Termination: Setel opsi ini <code>false</code> ke <code>true</code> atau untuk membuat instance AMI sebagai cadangan sebelum menghentikan EC2 instance. Nilai default-nya <code>true</code> . Nilai yang valid adalah <code>true</code> dan <code>false</code> (peka huruf besar/kecil). Tidak ada kendala
G31sq1e9u Cluster Pergeseran Merah Amazon yang Kurang Digunakan	AWSManagedServices-PauseRedshiftCluster Cluster Amazon Redshift dijeda.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c1cj39rr6v Konfigurasi Batalkan Unggahan Multipart Amazon S3 Tidak Lengkap	AWSManagedServices-TrustedRemediatorEnableS3 AbortIncompleteMultipartUpload Bucket Amazon S3 dikonfigurasi dengan aturan siklus hidup untuk membatalkan unggahan multibagian yang tetap tidak lengkap setelah hari-hari tertentu.	DaysAfterInitiation: Jumlah hari setelah Amazon S3 menghentikan unggahan multipart yang tidak lengkap. Default diatur ke 7 hari. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
c1z7kmr00n Rekomendasi pengoptimalan EC2 biaya Amazon untuk instans	Gunakan rekomendasi EC2 instans Amazon dan EC2 instans Amazon Idle dari Rekomendasi Compute Optimizer didukung oleh Trusted Remediator .	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c1z7kmr02n Rekomendasi pengoptimalan biaya Amazon EBS untuk volume	Gunakan rekomendasi volume Amazon EBS dan volume Idle Amazon EBS dari. Rekomendasi Compute Optimizer didukung oleh Trusted Remediator	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c1z7kmr03n Rekomendasi pengoptimalan biaya Amazon RDS untuk instans DB	Gunakan instans Idle Amazon RDS dari. Rekomendasi Compute Optimizer didukung oleh Trusted Remediator	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c1z7kmr05n AWS Lambda rekomendasi pengoptimalan biaya untuk fungsi	Gunakan rekomendasi fungsi Lambda dari. Rekomendasi Compute Optimizer didukung oleh Trusted Remediator	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Trusted Advisor pemeriksaan keamanan yang didukung oleh Trusted Remediator

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
12Fnkpl8Y5 Exposed Access Keys	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey Kunci akses IAM yang terbuka dinonaktifkan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Aplikasi yang dikonfigurasi dengan kunci akses IAM yang terbuka tidak dapat mengautentikasi.
Hs4Ma3G127 - API Gateway REST dan pencatatan eksekusi API harus WebSocket diaktifkan AWS Security Hub Cek yang sesuai: APIGateway.1	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging Pencatatan eksekusi diaktifkan pada tahap API.	LogLevel: Tingkat logging untuk mengaktifkan pencatatan eksekusi, ERROR - Logging diaktifkan hanya untuk kesalahan. INFO - Logging diaktifkan untuk semua acara. Anda harus memberikan izin API Gateway untuk membaca dan menulis log ke akun Anda CloudWatch untuk mengaktifkan log eksekusi, lihat Mengatur CloudWatch logging untuk REST APIs di API Gateway untuk detailnya.
Hs4Ma3G129 - Tahapan API Gateway REST API harus mengaktifkan penelusuran AWS X-Ray AWS Security Hub Cek	AWSManagedServices-EnableAPIGatewayXRayTracing Penelusuran X-Ray diaktifkan pada tahap API.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
yang sesuai: APIGateway.3		
Hs4Ma3G202 - Data cache API Gateway REST API harus dienkripsi saat istirahat AWS Security Hub Cek yang sesuai: APIGateway.5	AWSManagedServices-EnableAPIGatewayCacheEncryption Aktifkan enkripsi saat istirahat untuk data cache API Gateway REST API jika tahap API Gateway REST API telah mengaktifkan cache.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G177 - AWS Security Hub Pemeriksaan terkait - Grup penskalaan otomatis yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan penyeimbang beban .1 AutoScaling	AWSManagedServices-TrustedRoleEnableAutoScalingGroupELBHealthCheck Pemeriksaan kesehatan Elastic Load Balancing diaktifkan untuk Grup Auto Scaling.	HealthCheckGracePeriod: Jumlah waktu, dalam hitungan detik, Auto Scaling menunggu sebelum memeriksa status kesehatan instans Amazon Elastic Compute Cloud yang telah mulai digunakan. Mengaktifkan pemeriksaan kesehatan Elastic Load Balancing dapat mengakibatkan penggantian instance yang sedang berjalan jika salah satu penyeimbang beban Elastic Load Balancing yang terpasang pada grup Auto Scaling melaporkannya sebagai tidak sehat. Untuk informasi selengkapnya, lihat Melampirkan penyeimbang beban Elastic Load Balancing ke grup Auto Scaling

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G245 - tumpukan AWS CloudFormation harus diintegrasikan dengan Amazon Simple Notification Service AWS Security Hub Cek yang sesuai: CloudFormation.1	AWSManagedServices-EnableCFNStackNotification Kaitkan CloudFormation tumpukan dengan topik Amazon SNS untuk pemberitahuan.	PemberitahuanARNs: Topik Amazon SNS yang akan dikaitkan dengan tumpukan yang dipilih CloudFormation . ARNs Untuk mengaktifkan remediasi otomatis, Parameter yang NotificationARNs telah dikonfigurasi sebelumnya harus disediakan.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G210 - distribusi seharusnya mengaktifkan logging CloudFront AWS Security Hub Cek yang sesuai: CloudFront.2	AWSManagedServices-EnableCloudFrontDistributionLogging Logging diaktifkan untuk CloudFront distribusi Amazon.	• BucketName: Nama bucket Amazon S3 tempat Anda ingin menyimpan log akses. • S3KeyPrefix: Awalan untuk lokasi di bucket S3 untuk log distribusi Amazon. CloudFront • IncludeCookies: Menunjukkan apakah akan menyertakan cookie dalam log akses. Untuk mengaktifkan remediasi otomatis, parameter yang telah dikonfigurasi sebelumnya harus disediakan: • BucketName • S3 KeyPrefix • IncludeCookies Untuk kendala remediasi ini, lihat Bagaimana cara mengaktifkan logging untuk distribusi saya? CloudFront

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G109 - CloudTrail validasi file log harus diaktifkan AWS Security Hub Cek yang sesuai: CloudTrail.4	AWSManagedServices-TrustedRemediatorEnableCloudTrailLogValidation Mengaktifkan validasi log CloudTrail jejak.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G108 - CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch AWS Security Hub Cek yang sesuai: CloudTrail.5	AWSManagedServices-IntegrateCloudTrailWithCloudWatch AWS CloudTrail terintegrasi dengan CloudWatch Log.	- CloudWatchLogsLogGroupName: Nama grup CloudWatch log Log tempat CloudTrail log dikirimkan. Anda harus menggunakan grup log yang ada di akun Anda. - CloudWatchLogsRoleName: Nama peran IAM untuk titik akhir CloudWatch Log untuk diasumsikan menulis ke grup log pengguna. Anda harus menggunakan peran yang ada di akun Anda. Untuk mengaktifkan remediasi otomatis, parameter yang telah dikonfigurasi sebelumnya harus disediakan: - CloudWatchLogsLogGroupName - CloudWatchLogsRoleName

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G217 - CodeBuild lingkungan proyek harus memiliki konfigurasi logging AWS AWS Security Hub Cek yang sesuai: CodeBuild.4	AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig Mengaktifkan logging untuk CodeBuild proyek.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G306 - Cluster DB Neptune harus mengaktifkan perlindungan penghapusan AWS Security Hub Pemeriksaan yang sesuai: DocumentDB.3	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot Menghapus akses publik dari snapshot cluster manual Amazon DocumentDB.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G308 - Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan AWS Security Hub Pemeriksaan yang sesuai: DocumentDB.5	AWSManagedServices-TrustedRole mediatorEnableDocumentDBClusterDeletionProtection Mengaktifkan perlindungan penghapusan untuk klaster Amazon DocumentDB.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G323 - tabel DynamoDB harus memiliki perlindungan penghapusan diaktifkan AWS Security Hub Pemeriksaan yang sesuai: DynamoDB.6	AWSManagedServices-TrustedRole mediatorEnableDynamoDBTableDeletionProtection Mengaktifkan perlindungan penghapusan untuk tabel DynamoDB non-AMS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
EPS02jt06w - Cuplikan Publik Amazon EBS	AWSManagedServices-TrustedRole mediatorDisablePublicAccessOnEBSSnapshot Akses publik untuk snapshot Amazon EBS dinonaktifkan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G118 - Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar AWS Security Hub Cek yang sesuai: EC2.2	AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG Semua aturan masuk dan keluar dalam grup keamanan default akan dihapus.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G117 - Volume EBS yang terpasang harus dienkripsi saat istirahat AWS Security Hub Cek yang sesuai: EC2.3	AWSManagedServices-EncryptInstanceVolume Volume Amazon EBS terlampir pada instans dienkripsi.	• KMSKeyId: ID AWS KMS kunci atau ARN untuk mengenkripsi volume. • DeleteStaleNonEncryptedSnapshotBackups: Bendera yang memutuskan apakah cadangan snapshot dari volume lama yang tidak terenkripsi harus dihapus. Instance di-boot ulang sebagai bagian dari remediasi dan rollback DeleteStaleNonEncryptedSnapshotBackups dimungkinkan jika diatur yang membantu false pemulihan.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G120 - EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu AWS Security Hub Cek yang sesuai: EC2.4	AWSManagedServices-TerminateInstance(dokumen SSM default untuk mode eksekusi auto dan manual) EC2 Instans Amazon yang dihentikan selama 30 hari dihentikan.	Buat AMIBefore Pengakhiran: Untuk membuat instance AMI sebagai cadangan sebelum menghentikan EC2 instance, pilih <code>true</code>. Untuk tidak membuat cadangan sebelum mengakhiri, pilih <code>false</code>. Nilai default-nya <code>true</code>. Tidak ada kendala
Hs4Ma3G120 - EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu AWS Security Hub Cek yang sesuai: EC2.4	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime - EC2 Instans Amazon dihentikan untuk jumlah hari yang ditentukan di Security Hub (nilai default adalah 30) dihentikan.	Buat AMIBefore Terminasi: Untuk membuat instance AMI sebagai cadangan sebelum menghentikan EC2 instance, pilih <code>true</code>. Untuk tidak membuat cadangan sebelum mengakhiri, pilih <code>false</code>. Nilai default-nya <code>true</code>. Tidak ada kendala
Hs4Ma3G121 - Enkripsi default EBS harus diaktifkan AWS Security Hub Cek yang sesuai: EC2.7	AWSManagedServices-EncryptEBSDefault Enkripsi Amazon EBS secara default diaktifkan untuk yang spesifik Wilayah AWS	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Enkripsi secara default adalah pengaturan khusus Wilayah. Jika Anda mengaktifkannya untuk Wilayah, Anda tidak dapat menonaktifkannya untuk setiap volume atau snapshot di Wilayah tersebut.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G124 - Instans EC2 Amazon harus menggunakan Layanan Metadata Instance Versi 2 () IMDSv2 AWS Security Hub Cek yang sesuai: EC2.8	AWSManagedServices-TrustedRemediatorAktifkan EC2 Instance IMDSv2 EC2 Instans Amazon menggunakan Layanan Metadata Instans Versi 2 (). IMDSv2	- IMDSv1MetricCheckPeriod: Jumlah hari (42-455) untuk menganalisis metrik IMDSv1 penggunaan di CloudWatch. Jika EC2 instans Amazon dibuat dalam jangka waktu yang ditentukan, maka analisis dimulai dari tanggal pembuatan instans. - HttpPutResponseHopLimit: Jumlah maksimum hop jaringan yang diizinkan untuk token metadata instance. Nilai ini dapat dikonfigurasi antara 1 dan 2 hop. Batas hop membatasi akses token ke proses yang berjalan langsung pada instance, sementara batas hop 2 memungkinkan akses dari kontainer yang berjalan pada instance. 1 Tidak ada kendala
Hs4Ma3G207 - EC2 subnet seharusnya tidak secara otomatis menetapkan alamat IP publik AWS Security Hub Cek yang sesuai: EC2.15	AWSManagedServices-UpdateAutoAssignPublicIpv4Alamat Subnet VPC dikonfigurasi untuk tidak secara otomatis menetapkan alamat IP publik.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G209 - Daftar Kontrol Akses Jaringan yang Tidak Digunakan dihapus AWS Security Hub Cek yang sesuai: EC2.16	AWSManagedServices-DeleteUnusedNACL Hapus ACL jaringan yang tidak digunakan	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G215 - Grup keamanan Amazon yang tidak digunakan harus dihapus EC2 AWS Security Hub Cek yang sesuai: EC2.22	AWSManagedServices-DeleteSecurityGroups Hapus grup keamanan yang tidak digunakan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G247 - Amazon EC2 Transit Gateway seharusnya tidak secara otomatis menerima permintaan lampiran VPC AWS Security Hub Cek yang sesuai: EC2.23	AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach- Menonaktifkan penerimaan otomatis permintaan lampiran VPC untuk Gateway Transit EC2 Amazon non-AMS yang ditentukan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G235 - Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi AWS Security Hub Pemeriksaan yang sesuai: ECR.2	AWSManagedServices-TrustedRemediatorSetImageTagImmutability Menetapkan pengaturan mutabilitas tag gambar ke IMMUTABLE untuk repositori yang ditentukan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G216 - Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi AWS Security Hub Pemeriksaan yang sesuai: ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy Repositori ECR memiliki kebijakan siklus hidup yang dikonfigurasi.	LifecyclePolicyText: Teks kebijakan repositori JSON untuk diterapkan ke repositori. Untuk mengaktifkan remediasi otomatis, parameter yang telah dikonfigurasi sebelumnya harus disediakan: LifecyclePolicyText

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G325 - Kluster EKS harus mengaktifkan pencatatan audit AWS Security Hub Pemeriksaan yang sesuai: EKS.8	AWSManagedServices-TrustedRemediatorEnableEKSAuditLog Log audit diaktifkan untuk kluster EKS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G183 - Penyeimbang beban aplikasi harus dikonfigurasi untuk menjatuhkan header HTTP AWS Security Hub Pemeriksaan yang sesuai: ELB.4	AWSConfigRemediation-DropInvalidHeadersForALB Application Load Balancer dikonfigurasi ke bidang header yang tidak valid.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G184 - Load Balancer Aplikasi dan Load Balancer Klasik logging harus diaktifkan AWS Security Hub Pemeriksaan yang sesuai: ELB.5	AWSManagedServices-EnableELBLogging (dokumen SSM default untuk mode eksekusi auto dan manual) Application Load Balancer dan logging Classic Load Balancer diaktifkan.	• BucketName: Nama ember (bukan ARN). Pastikan kebijakan bucket dikonfigurasi dengan benar untuk pencatatan. • S3KeyPrefix: Awalan untuk lokasi di bucket Amazon S3 untuk log Elastic Load Balancing. Untuk mengaktifkan remediasi otomatis, parameter yang telah dikonfigurasi sebelumnya harus disediakan: • BucketName • S3 KeyPrefix Bucket Amazon S3 harus memiliki kebijakan bucket yang memberikan izin Elastic Load Balancing untuk menulis log akses ke bucket.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G184 - Load Balancer Aplikasi dan Load Balancer Klasik logging harus diaktifkan AWS Security Hub Pemeriksaan yang sesuai: ELB.5	AWSManagedServices-EnableELBLoggingV2 Application Load Balancer dan logging Classic Load Balancer diaktifkan.	• TargetBucketTagKey: Nama tag (peka huruf besar/kecil) yang digunakan untuk mengidentifikasi bucket Amazon S3 target. Gunakan ini bersama dengan TargetBucketTagValue untuk menandai bucket yang akan berfungsi sebagai bucket tujuan untuk pencatatan akses. • TargetBucketTagValue: Nilai tag (peka huruf besar/kecil) yang digunakan untuk mengidentifikasi bucket Amazon S3 target. Gunakan ini bersama dengan TargetBucketTagKey untuk menandai bucket yang akan berfungsi sebagai bucket tujuan untuk pencatatan akses. • S3BucketPrefix: Awalan (hierarki logis) untuk bucket Amazon S3. Awalan yang Anda tentukan tidak boleh menyertakan stringAWSLogs. Untuk informasi selengkapnya, lihat Mengatur objek menggunakan awalan. Untuk mengaktifkan remediasi otomatis, parameter yang telah dikonfigurasi sebelumnya harus disediakan: • TargetBucketTagKey • TargetBucketTagValue

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
		S3 BucketPrefix Bucket Amazon S3 harus memiliki kebijakan bucket yang memberikan izin Elastic Load Balancing untuk menulis log akses ke bucket.
Hs4Ma3G326 - Amazon EMR memblokir pengaturan akses publik harus diaktifkan AWS Security Hub Pemeriksaan yang sesuai: EMR.2	AWSManagedServices-TrustedRoleMediatorEnableEMRBlockPublicAccess Amazon EMR memblokir pengaturan akses publik diaktifkan untuk akun.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G135 - AWS KMS kunci tidak boleh dihapus secara tidak sengaja AWS Security Hub Pemeriksaan yang sesuai: KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS penghapusan kunci dibatalkan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G299 - Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik AWS Security Hub Pemeriksaan yang sesuai: Neptunuse.4	AWSManagedServices-TrustedRemediatorEnableNeptuneDBClusterDeletionProtection Mengaktifkan perlindungan penghapusan untuk klaster Amazon Neptune.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G319 - Firewall Jaringan harus mengaktifkan perlindungan penghapusan AWS Security Hub Cek yang sesuai: NetworkFirewall.9	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection- Mengaktifkan perlindungan penghapusan untuk AWS Network Firewall.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G223 - OpenSearch domain harus mengenkripsi data yang dikirim antar node AWS Security Hub Cek yang sesuai: OpenSearch.3	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption Enkripsi Node ke Node diaktifkan untuk domain.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Setelah node-to-node enkripsi diaktifkan, Anda tidak dapat menonaktifkan pengaturan. Sebagai gantinya, ambil snapshot manual dari domain terenkripsi, buat domain lain, migrasi data Anda, lalu hapus domain lama.
Hs4Ma3G222 - login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch AWS Security Hub Pemeriksaan yang sesuai: Opensearch.4	AWSManagedServices-EnableOpenSearchLogging Pencatatan kesalahan diaktifkan untuk OpenSearch domain.	CloudWatchLogGroupArn: ARN dari grup log log AnAmazon CloudWatch Logs. Untuk mengaktifkan remediasi otomatis, parameter yang telah dikonfigurasi sebelumnya harus disediakan: CloudWatchLogGroup Arn Kebijakan CloudWatch sumber daya Amazon harus dikonfigurasi dengan izin. Untuk informasi selengkapnya, lihat Mengaktifkan log audit di Panduan Pengguna OpenSearch Layanan Amazon

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G221 - domain harus mengaktifkan pencatatan audit OpenSearch AWS Security Hub Pemeriksaan yang sesuai: Opensearch.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch domain dikonfigurasi dengan pencatatan audit diaktifkan.	CloudWatchLogGroupArn: ARN dari grup CloudWatch Log untuk mempublikasikan log ke. Untuk mengaktifkan remediasi otomatis, parameter yang telah dikonfigurasi sebelumnya harus disediakan: CloudWatchLogGroup Arn Kebijakan CloudWatch sumber daya Amazon harus dikonfigurasi dengan izin. Untuk informasi selengkapnya, lihat Mengaktifkan log audit di Panduan Pengguna OpenSearch Layanan Amazon
Hs4Ma3G220 - Koneksi ke OpenSearch domain harus dienkripsi menggunakan TLS 1.2 AWS Security Hub Pemeriksaan yang sesuai: Opensearch.8	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 Kebijakan TLS disetel ke `Policy-Min-TLS-1-2-2019-07` dan hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Koneksi ke OpenSearch domain diperlukan untuk menggunakan TLS 1.2. Mengenkripsi data dalam perjalanan dapat memengaruhi kinerja. Uji aplikasi Anda dengan fitur ini untuk memahami profil kinerja dan dampak TLS.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G194 - Snapshot Amazon RDS harus pribadi AWS Security Hub Pemeriksaan yang sesuai: RDS.1	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Akses publik untuk snapshot Amazon RDS dinonaktifkan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G192 - Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh Konfigurasi PubliclyAccessible AWS AWS Security Hub Pemeriksaan yang sesuai: RDS.2	AWSManagedServices-TrustedResourceDisablingPublicAccessOnRDSInstance Nonaktifkan akses publik pada instans RDS DB.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G189 - Pemantauan yang ditingkatkan dikonfigurasi untuk instans Amazon RDS DB AWS Security Hub Pemeriksaan yang sesuai: RDS.6	AWSManagedServices-TrustedRemediatorEnableRDSEnhancedMonitoring Aktifkan pemantauan yang disempurnakan untuk instans Amazon RDS DB	- MonitoringInterval: Interval, dalam hitungan detik, antar titik saat metrik Pemantauan yang Ditingkatkan dikumpulkan untuk instans DB. Interval yang valid adalah 0, 1, 5, 10, 15, 30 dan 60. Untuk menonaktifkan pengumpulan metrik Pemantauan yang Ditingkatkan, tentukan 0. - MonitoringRoleName: Nama peran IAM yang memungkinkan Amazon RDS mengirim metrik pemantauan yang disempurnakan ke Amazon Logs. CloudWatch Jika peran tidak ditentukan, maka peran default <code>rds-monitoring-role</code> digunakan atau dibuat, jika tidak ada. Jika pemantauan yang ditingkatkan diaktifkan sebelum eksekusi otomatisasi, maka pengaturan mungkin ditimpa oleh otomatisasi ini dengan MonitoringRoleName nilai MonitoringInterval dan yang dikonfigurasi dalam parameter yang telah dikonfigurasi sebelumnya.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G190 - Cluster Amazon RDS harus mengaktifkan perlindungan penghapusan AWS Security Hub Pemeriksaan yang sesuai: RDS.7	AWSManagedServices-TrustedR emediatorEnableRDSDeletionP rotection Perlindungan penghapusan diaktifkan untuk klaster Amazon RDS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G198 - Instans Amazon RDS DB harus mengaktifkan perlindungan penghapusan AWS Security Hub Pemeriksaan yang sesuai: RDS.8	AWSManagedServices-TrustedR emediatorEnableRDSDeletionP rotection Perlindungan penghapusan diaktifkan untuk instans Amazon RDS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G199 - Instans RDS DB harus menerbitkan log ke Log CloudWatch AWS Security Hub Pemeriksaan yang sesuai: RDS.9	AWSManagedServices-TrustedR emediatorEnableRDSLogExports Ekspor log RDS diaktifkan untuk instans RDS DB atau cluster RDS DB.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. AWSServiceRoleForRDS peran terkait layanan diperlukan.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G160 - otentikasi IAM harus dikonfigurasi untuk instance RDS AWS Security Hub Pemeriksaan yang sesuai: RDS.10	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication AWS Identity and Access Management otentikasi diaktifkan untuk instance RDS.	ApplyImmediately: Menunjukkan jika modifikasi dalam permintaan ini dan modifikasi yang tertunda diterapkan secara asinkron sesegera mungkin, Untuk segera menerapkan perubahan, pilih. <code>true</code> Untuk menjadwalkan perubahan untuk jendela pemeliharaan berikutnya, pilih <code>false</code>. Tidak ada kendala
Hs4Ma3G161 - otentikasi IAM harus dikonfigurasi untuk cluster RDS AWS Security Hub Pemeriksaan yang sesuai: RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication Autentikasi IAM diaktifkan untuk cluster RDS.	ApplyImmediately: Menunjukkan jika modifikasi dalam permintaan ini dan modifikasi yang tertunda diterapkan secara asinkron sesegera mungkin, Untuk segera menerapkan perubahan, pilih. <code>true</code> Untuk menjadwalkan perubahan untuk jendela pemeliharaan berikutnya, pilih <code>false</code>. Tidak ada kendala
Hs4Ma3G162 - Peningkatan versi minor otomatis RDS harus diaktifkan AWS Security Hub Pemeriksaan yang sesuai: RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade Konfigurasi pemutakhiran versi minor otomatis untuk Amazon RDS diaktifkan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Instans Amazon RDS harus dalam <code>available</code> keadaan agar remediasi ini terjadi.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G16 3 - Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot AWS Security Hub Pemeriksaan yang sesuai: RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagtosnapshot pengaturan untuk kluster Amazon RDS diaktifkan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Instans Amazon RDS harus dalam keadaan tersedia agar remediasi ini terjadi.
Hs4Ma3G16 4 - Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot AWS Security Hub Pemeriksaan yang sesuai: RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagsToSnapshot pengaturan untuk Amazon RDS diaktifkan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Instans Amazon RDS harus dalam keadaan tersedia agar remediasi ini terjadi.
RSS93 HQwa1 Cuplikan Publik Amazon RDS	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Akses publik untuk snapshot Amazon RDS dinonaktifkan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G103 - Cluster Amazon Redshift harus melarang akses publik AWS Security Hub Pemeriksaan yang sesuai: Redshift.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster Akses publik di klaster Amazon Redshift dinonaktifkan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Menonaktifkan akses publik memblokir semua klien yang berasal dari internet. Dan cluster Amazon Redshift berada dalam kondisi modifikasi selama beberapa menit sementara remediasi menonaktifkan akses publik di cluster.
Hs4Ma3G106 - Cluster Amazon Redshift harus mengaktifkan pencatatan audit AWS Security Hub Pemeriksaan yang sesuai: Redshift.4	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterAuditLogging Pencatatan audit diaktifkan ke klaster Amazon Redshift Anda selama jendela pemeliharaan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Untuk mengaktifkan remediasi otomatis, parameter yang telah dikonfigurasi sebelumnya harus disediakan. BucketName: Ember harus sama Wilayah AWS. Cluster harus telah membaca bucket dan menempatkan izin objek. Jika pencatatan klaster Redshift diaktifkan sebelum eksekusi otomatisasi, maka pengaturan logging mungkin ditimpa oleh otomatisasi ini dengan S3KeyPrefix nilai BucketName dan yang dikonfigurasi dalam parameter yang telah dikonfigurasi sebelumnya.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G105 - Amazon Redshift harus memiliki upgrade otomatis ke versi utama diaktifkan AWS Security Hub Pemeriksaan yang sesuai: Redshift.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade-Upgrade versi utama diterapkan secara otomatis ke cluster selama jendela pemeliharaan. Tidak ada waktu henti langsung untuk cluster Amazon Redshift, tetapi cluster Amazon Redshift Anda mungkin mengalami downtime selama jendela pemeliharannya jika ditingkatkan ke versi utama.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G104 - Cluster Amazon Redshift harus menggunakan perutean VPC yang disempurnakan AWS Security Hub Pemeriksaan yang sesuai: Redshift.7	AWSManagedServices-TrustedRedshiftClusterEnhancedVPCRouting Perutean VPC yang disempurnakan diaktifkan untuk klaster Amazon Redshift.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G173 - Pengaturan Akses Publik Blok S3 harus diaktifkan pada tingkat ember AWS Security Hub Pemeriksaan yang sesuai: S3.8	AWSManagedServices-TrustedRemediatorBlockS3 BucketPublicAccess Blok akses publik tingkat ember diterapkan untuk bucket Amazon S3.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Remediasi ini dapat mempengaruhi ketersediaan objek S3. Untuk informasi tentang cara Amazon S3 mengevaluasi akses, lihat Memblokir akses publik ke penyimpanan Amazon S3 Anda.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G230 - Pencatatan akses server bucket S3 harus diaktifkan AWS Security Hub Pemeriksaan yang sesuai: S3.9	AWSManagedServices-EnableBucketAccessLogging(dokumen SSM default untuk mode eksekusi auto dan manual) Pencatatan akses server Amazon S3 diaktifkan.	• TargetBucket: Nama bucket S3 untuk menyimpan log akses server. • TargetObjectKeyFormat: Format kunci Amazon S3 untuk objek log (nilai peka huruf besar/kecil). Untuk menggunakan format sederhana untuk kunci S3 untuk objek log, pilih SimplePrefix . Untuk menggunakan kunci S3 yang dipartisi untuk objek log dan gunakan EventTime untuk awalan yang dipartisi, pilih. PartitionedPrefixEventTime Untuk menggunakan kunci S3 yang dipartisi untuk objek log dan gunakan DeliveryTime untuk awalan yang dipartisi, pilih. PartitionedPrefixDeliveryTime Nilai yang valid adalah SimplePrefix , PartitionedPrefixEventTime dan PartitionedPrefixDeliveryTime . Untuk mengaktifkan remediasi otomatis, parameter yang telah dikonfigurasi sebelumnya harus disediakan: TargetBucket Bucket tujuan harus sama Wilayah AWS dan Akun AWS sebagai

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
		bucket sumber, dengan izin yang benar untuk pengiriman log. Untuk informasi selengkapnya, lihat Mengaktifkan pencatatan akses server Amazon S3 .

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G230 - Pencatatan akses server bucket S3 harus diaktifkan AWS Security Hub Pemeriksaan yang sesuai: S3.9	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 - Pencatatan bucket Amazon S3 diaktifkan.	• TargetBucketTagKey: Nama tag (case-sensitive) untuk mengidentifikasi bucket target. Gunakan ini dan TargetBucketTagValue untuk menandai bucket yang akan digunakan sebagai bucket tujuan untuk pencatatan akses. • TargetBucketTagValue: Nilai tag (peka huruf besar/kecil) untuk mengidentifikasi bucket target, gunakan ini dan TargetBucketTagKey untuk menandai bucket yang akan digunakan sebagai bucket tujuan untuk pencatatan akses. • TargetObjectKeyFormat: Format kunci Amazon S3 untuk objek log (nilai peka huruf besar/kecil): Untuk menggunakan format sederhana untuk kunci S3 untuk objek log, pilih. SimplePrefix Untuk menggunakan kunci S3 yang dipartisi untuk objek log dan gunakan EventTime untuk awalan yang dipartisi, pilih. PartitionedPrefixEventTime Untuk menggunakan kunci S3 yang dipartisi untuk objek log dan gunakan DeliveryTime untuk awalan yang dipartisi, pilih. PartitionedPrefixDeliveryTime

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
		me Defaultnya adalah Partition edPrefixEventTime. Untuk mengaktifkan remediasi otomatis, parameter berikut harus disediakan: TargetBucketTagKeydan TargetBucketTagValue. Bucket tujuan harus sama Wilayah AWS dan Akun AWS sebagai bucket sumber, dengan izin yang benar untuk pengiriman log. Untuk informasi selengkapnya, lihat Mengaktifkan pencatatan akses server Amazon S3.
Pfx0 RwgBli Izin Bucket Amazon S3	AWSManagedServices-TrustedRemediatorBlockS3 BucketPublicAccess Akses publik blok	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Pemeriksaan ini terdiri dari beberapa kriteria peringatan. Otomatisasi ini memulihkan masalah akses publik. Remediasi untuk masalah konfigurasi lain yang ditandai oleh Trusted Advisor tidak didukung. Remediasi ini mendukung remediasi bucket S3 yang Layanan AWS dibuat (misalnya, cf-templates-0000000000).

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G27 2 - Pengguna seharusnya tidak memiliki akses root ke instance notebook SageMaker AWS Security Hub Cek yang sesuai: SageMaker.3	AWSManagedServices-TrustedRemediatorDisableSageMakerNotebookInstanceRootAccess Akses root untuk pengguna dinonaktifkan untuk contoh SageMaker notebook.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Remediasi ini menyebabkan pemadaman jika instance SageMaker notebook dalam keadaan. InService
Hs4Ma3G17 9 - Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS AWS Security Hub Pemeriksaan yang sesuai: SNS.1	AWSManagedServices-EnableSNSEncryptionAtRest Topik SNS dikonfigurasi dengan enkripsi sisi server.	KmsKeyId: ID kunci master pelanggan AWS terkelola (CMK) untuk Amazon SNS atau CMK kustom yang akan digunakan untuk enkripsi sisi server (SSE). Default diatur ke <code>alias/aws/sns</code>. Jika AWS KMS kunci khusus digunakan, itu harus dikonfigurasi dengan izin yang benar. Untuk informasi selengkapnya, lihat Mengaktifkan enkripsi sisi server (SSE) untuk topik Amazon SNS

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G158 - Dokumen SSM seharusnya tidak bersifat publik AWS Security Hub Pemeriksaan yang sesuai: SSM.4	AWSManagedServices-TrustedRemediatorDisableSSMDocPublicSharing- Menonaktifkan berbagi dokumen SSM secara publik.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Hs4Ma3G136 - Antrian Amazon SQS harus dienkripsi saat istirahat AWS Security Hub Pemeriksaan yang sesuai: SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest Pesan di Amazon SQS dienkripsi.	• <code>SqsManagedSseEnabled</code>: Setel <code>true</code> untuk mengaktifkan enkripsi antrian sisi server menggunakan kunci enkripsi milik Amazon SQS, setel <code>false</code> untuk mengaktifkan enkripsi antrian sisi server menggunakan kunci. AWS KMS • <code>KMSKeyId</code>: ID atau alias kunci master pelanggan AWS terkelola (CMK) untuk Amazon SQS atau CMK kustom yang akan digunakan untuk enkripsi sisi server untuk antrian. Jika tidak disediakan, <code>alias/aws/sqs</code> digunakan. • <code>KmsDataKeyReusePeriodSeconds</code>: Lamanya waktu, dalam hitungan detik, Amazon SQS dapat menggunakan kembali kunci data untuk mengenkripsi atau mendekripsi pesan sebelum menelepon lagi. AWS KMS Bilangan bulat yang mewakili detik, antara 60 detik (1 menit) dan 86.400 detik (24 jam). Pengaturan ini diabaikan jika <code>SqsManagedSseEnabled</code> disetel ke <code>true</code>. Anonim <code>SendMessage</code> dan <code>ReceiveMessage</code> permintaan ke antrian terenkripsi ditolak. Semua permintaan untuk antrian dengan

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
		SSE diaktifkan harus menggunakan HTTPS dan Signature Version 4.

Trusted Advisor pemeriksaan toleransi kesalahan yang didukung oleh Trusted Remediator

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
c18d2gz138 Pemulihan Amazon DynamoDB Point-in-time	AWSManagedServices-TrustedRemediatorEnableDDBPITR Mengaktifkan point-in-time pemulihan untuk tabel DynamoDB.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
R365s2qddf Versi Bucket Amazon S3	AWSManagedServices-TrustedRemediatorEnableBucketVersioning Versi bucket Amazon S3 diaktifkan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Remediasi ini tidak mendukung remediasi bucket S3 yang Layanan AWS dibuat (misalnya cf-templates-0000000000).
BueAdJ7nnp Pencatatan Bucket Amazon S3	AWSManagedServices-EnableBucketAccessLogging Pencatatan bucket Amazon S3 diaktifkan.	- TargetBucket: Nama bucket S3 untuk menyimpan log akses server. - TargetObjectKeyFormat: Format kunci Amazon S3 untuk objek log, untuk menggunakan format sederhana untuk tombol S3 untuk

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
		objek log, pilih. SimplePrefix Untuk menggunakan kunci S3 yang dipartisi untuk objek log dan gunakan EventTime untuk awalan yang dipartisi, pilih. PartitionedPrefixEventTime Untuk menggunakan kunci S3 yang dipartisi untuk objek log dan gunakan DeliveryTime untuk awalan yang dipartisi, pilih. PartitionedPrefixDeliveryTime Nilai default-nya PartitionedPrefixEventTime . Nilai yang valid adalah SimplePrefix , PartitionedPrefixEventTime dan PartitionedPrefixDeliveryTime (case-sensitive). Untuk mengaktifkan remediasi otomatis, parameter yang telah dikonfigurasi sebelumnya harus disediakan: • TargetBucket Bucket tujuan harus sama Wilayah AWS dan Akun AWS sebagai bucket sumber, dengan izin yang benar untuk pengiriman log. Untuk informasi selengkapnya, lihat

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
		Mengaktifkan pencatatan akses server Amazon S3.
F2ik5r6dep Amazon RDS Multi-AZ	AWSManagedServices-TrustedR emediatorEnableRDSMultiAZ Penyebaran Zona Multi-Ketersediaan diaktifkan.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Ada kemungkinan penurunan kinerja selama perubahan ini.
H7 IgTzj TYb Snapshot Amazon EBS	AWSManagedServices-TrustedR emediatorCreateEBSSnapshot Amazon EBSsnapshots dibuat.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
di QPADk ZVh Cadangan RDS	AWSManagedServices-EnableRDSBackupRetention Retensi cadangan Amazon RDS diaktifkan untuk DB.	- BackupRetentionPeriod: Jumlah hari (1-35) untuk mempertahankan backup otomatis. - ApplyImmediately: Menunjukkan jika retensi cadangan RDS berubah dan modifikasi yang tertunda diterapkan secara asinkron sesegera mungkin. Pilih <code>true</code> untuk segera menerapkan perubahan, atau <code>false</code> untuk menjadwalkan perubahan untuk jendela pemeliharaan berikutnya. Jika <code>ApplyImmediately</code> parameter disetel ke <code>true</code>, perubahan yang tertunda pada db diterapkan bersama dengan pengaturan RDSBackup retensi.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
c1qf5bt013 Instans Amazon RDS DB memiliki penyimpanan autoscaling dimatikan	AWSManagedServices-TrusteRemediatorEnableRDSInstanceStorageAutoScaling- Penskalaan otomatis penyimpanan diaktifkan untuk instans Amazon RDS DB.	MaxAllocatedStorageIncrease Percentage: Persentase kenaikan arus AllocatedStorage, untuk mengatur MaxAllocatedStorage. Default diatur ke 26. Anda harus mengatur ambang penyimpanan maksimum setidaknya 10% lebih banyak dari penyimpanan yang dialokasikan saat ini. Ini adalah praktik terbaik untuk mengatur ambang penyimpanan maksimum menjadi setidaknya 26% lebih banyak. Untuk detailnya, periksa Mengelola kapasitas secara otomatis dengan penskalaan otomatis penyimpanan Amazon Relational Database Service. Tidak ada kendala
7q GXs KIUw Connection Draining Classic Load Balancer	AWSManagedServices-TrusteRemediatorEnableCLBConnectionDraining Pengurusan koneksi diaktifkan untuk Classic Load Balancer.	ConnectionDrainingTimeout: Waktu maksimum, dalam hitungan detik, untuk menjaga koneksi yang ada tetap terbuka sebelum membatalkan pendaftaran instance. Default diatur ke 300 detik. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
c18d2gz106 Amazon EBS Tidak Termasuk dalam Paket AWS Backup	AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan Amazon EBS termasuk dalam AWS Backup Paket.	Remediasi menandai volume Amazon EBS dengan pasangan tag berikut. Pasangan tag harus cocok dengan kriteria pemilihan sumber daya berbasis tag untuk AWS Backup. • TagKey • TagValue Tidak ada kendala
c18d2gz107 Tabel Amazon DynamoDB Tidak Termasuk dalam Paket AWS Backup	AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlan Tabel Amazon DynamoDB disertakan dalam Paket. AWS Backup	Remediasi menandai Amazon DynamoDB dengan pasangan tag berikut. Pasangan tag harus cocok dengan kriteria pemilihan sumber daya berbasis tag untuk AWS Backup. • TagKey • TagValue Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
c18d2gz117 Amazon EFS Tidak Termasuk dalam AWS Backup Paket	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan Amazon EFS disertakan dalam AWS Backup Paket.	Remediasi menandai Amazon EFS dengan pasangan tag berikut. Pasangan tag harus cocok dengan kriteria pemilihan sumber daya berbasis tag untuk AWS Backup. • TagKey • TagValue Tidak ada kendala
c18d2gz105 Penyeimbang Beban Jaringan Cross Load Balancing	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing Penyeimbangan beban lintas zona diaktifkan pada Network Load Balancer.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c1qf5bt026 synchronous_commit Parameter Amazon RDS dimatikan	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Parameter synchronous_commit dihidupkan untuk Amazon RDS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
c1qf5bt030 innodb_flush_log_at_trx_commit Parameter Amazon RDS tidak 1	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Parameter innodb_flush_log_at_trx_commit diatur ke 1 untuk Amazon RDS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c1qf5bt031 sync_binlog Parameter Amazon RDS dimatikan	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Parameter sync_binlog dihidupkan untuk Amazon RDS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c1qf5bt036 Pengaturan innodb_default_row_format parameter Amazon RDS tidak aman	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Parameter innodb_default_row_format diatur ke DYNAMIC untuk Amazon RDS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c18d2gz144 Pemantauan EC2 Terperinci Amazon Tidak Diaktifkan	AWSManagedServices-TrustedRemediatorEnableEC2 InstanceDetailedMonitoring Pemantauan terperinci diaktifkan untuk Amazon EC2.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Trusted Advisor pemeriksaan kinerja yang didukung oleh Trusted Remediator

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
COr6dfpM06 AWS Lambda fungsi yang kurang disediakan untuk ukuran memori	AWSManagedServices-ResizeLambdaMemory Fungsi Lambda ukuran memori diubah ukurannya ke ukuran memori yang direkomendasikan yang disediakan oleh. Trusted Advisor	RecommendedMemorySize: Alokasi memori yang direkomendasikan untuk fungsi Lambda. Rentang nilai antara 128 dan 10240. Jika ukuran fungsi Lambda dimodifikasi sebelum eksekusi otomatisasi, maka otomatisasi ini mungkin menimpa pengaturan dengan nilai yang direkomendasikan oleh. Trusted Advisor
ZRxQIPsb6c Instans Amazon EC2 Pemanfaatan Tinggi	AWSManagedServices-ResizeInstanceByOneLevel EC2 Instans Amazon diubah ukurannya dengan satu jenis instans dalam tipe keluarga instance yang sama. Instance dihentikan dan dimulai selama operasi pengubahan ukuran dan dikembalikan ke keadaan awal setelah eksekusi selesai. Otomatisasi ini tidak mendukung pengubahan ukuran instans yang ada di Grup Auto Scaling.	- MinimumDaysSinceLastChange: Jumlah hari minimum sejak jenis instance terakhir berubah. Jika jenis instance dimodifikasi dalam waktu yang ditentukan, jenis instance tidak berubah. Gunakan 0 untuk melewati validasi ini. Nilai default-nya 7. - Buat AMIBefore Ubah Ukuran: Untuk membuat instance AMI sebagai cadangan sebelum mengubah ukuran, pilih. true Untuk tidak membuat cadangan, pilihfalse. Nilai default-nya false. Nilai yang valid adalah true dan false (peka huruf besar/kecil). - ResizelfStopped: Untuk melanjutkan dengan perubahan ukuran

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
		instance, bahkan jika instance dalam keadaan berhenti, pilih <code>true</code>. Untuk tidak mengubah ukuran instance secara otomatis jika dalam keadaan berhenti, pilih <code>false</code>. Nilai yang valid adalah <code>true</code> dan <code>false</code> (peka huruf besar/kecil). Tidak ada kendala
c1qf5bt021 innodb_change_buffering Parameter Amazon RDS menggunakan nilai kurang dari optimal	AWSManagedServices-TrustedRemediatorRemediateRDSParmeterGroupParameter Nilai innodb_change_buffering parameter diatur NONE untuk Amazon RDS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c1qf5bt025 autovacuum Parameter Amazon RDS dimatikan	AWSManagedServices-TrustedRemediatorRemediateRDSParmeterGroupParameter Parameter autovacuum dihidupkan untuk Amazon RDS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
c1qf5bt028 enable_indexonlyscan Parameter Amazon RDS dimatikan	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Parameter enable_indexonlyscan dihidupkan untuk Amazon RDS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c1qf5bt029 enable_indexscan Parameter Amazon RDS dimatikan	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Parameter enable_indexscan dihidupkan untuk Amazon RDS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c1qf5bt032 innodb_stats_persistent Parameter Amazon RDS dimatikan	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Parameter innodb_stats_persistent dihidupkan untuk Amazon RDS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c1qf5bt037 general_logging Parameter Amazon RDS dihidupkan	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Parameter general_logging dimatikan untuk Amazon RDS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala

Trusted Advisor pemeriksaan batas layanan yang didukung oleh Trusted Remediator

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Ln7rr0L7j9 EC2-Alamat IP Elastis VPC	AWSManagedServices-UpdateVpcElasticIPQuota Batas baru untuk alamat IP elastis EC2 -VPC diminta. Secara default, batas ditingkatkan sebesar 3.	Kenaikan: Jumlah untuk meningkatkan kuota saat ini. Nilai default-nya 3. Jika otomatisasi ini dijalankan beberapa kali sebelum Trusted Advisor pemeriksaan diperbarui dengan OK status, maka mungkin ada peningkatan batas yang lebih tinggi.
Km7QQ0L7j9 Gateway Internet VPC	AWSManagedServices-IncreaseServiceQuota- Batas baru untuk gateway internet VPC diminta. Secara default, batasnya meningkat tiga.	Kenaikan: Jumlah untuk meningkatkan kuota saat ini. Nilai default-nya 3. Jika otomatisasi ini dijalankan beberapa kali sebelum Trusted Advisor pemeriksaan diperbarui dengan OK status, maka mungkin ada peningkatan batas yang lebih tinggi.
JL7pp0L7j9 VPC	AWSManagedServices-IncreaseServiceQuota Batas baru untuk VPC diminta. Secara default, batasnya meningkat 3.	Kenaikan: Jumlah untuk meningkatkan kuota saat ini. Nilai default-nya 3. Jika otomatisasi ini dijalankan beberapa kali sebelum Trusted Advisor pemeriksaan diperbarui dengan OK status, maka mungkin ada peningkatan batas yang lebih tinggi.
FW7HH0L7j9	AWSManagedServices-IncreaseServiceQuota	Kenaikan: Jumlah untuk meningkatkan kuota saat ini. Nilai default-nya 3.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Grup Auto Scaling	Batas baru untuk Grup Auto Scaling diminta. Secara default, batasnya meningkat 3.	Jika otomatisasi ini dijalankan beberapa kali sebelum Trusted Advisor pemeriksaan diperbarui dengan OK status, maka mungkin ada peningkatan batas yang lebih tinggi.
3Njm0 DJQO9 Grup Opsi RDS	AWSManagedServices-Increase ServiceQuota Batas baru untuk grup opsi Amazon RDS diminta. Secara default, batasnya meningkat 3.	Kenaikan: Jumlah untuk meningkatkan kuota saat ini. Nilai default-nya 3. Jika otomatisasi ini dijalankan beberapa kali sebelum Trusted Advisor pemeriksaan diperbarui dengan OK status, maka mungkin ada peningkatan batas yang lebih tinggi.
EM8b3yLRTr Penyeimbang Beban Aplikasi ELB	AWSManagedServices-Increase ServiceQuota Batas baru untuk ELB Application Load Balancers diminta. Secara default, batasnya meningkat 3.	Kenaikan: Jumlah untuk meningkatkan kuota saat ini. Nilai default-nya 3. Jika otomatisasi ini dijalankan beberapa kali sebelum Trusted Advisor pemeriksaan diperbarui dengan OK status, maka mungkin ada peningkatan batas yang lebih tinggi.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
8WiQ YSt25 K Penyeimbang Beban Jaringan ELB	AWSManagedServices-Increase ServiceQuota Batas baru untuk ELB Network Load Balancers diminta. Secara default, batasnya meningkat 3.	Kenaikan: Jumlah untuk meningkatkan kuota saat ini. Nilai default-nya 3. Jika otomatisasi ini dijalankan beberapa kali sebelum Trusted Advisor pemeriksaan diperbarui dengan OK status, maka mungkin ada peningkatan batas yang lebih tinggi.

Trusted Advisor pemeriksaan keunggulan operasional didukung oleh Trusted Remediator

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
c18d2gz125 Amazon API Gateway Tidak Mencatat Log Eksekusi	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging Pencatatan eksekusi diaktifkan pada tahap API.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Anda harus memberikan izin API Gateway untuk membaca dan menulis log ke akun Anda CloudWatch untuk mengaktifkan log eksekusi, lihat Mengatur CloudWatch logging untuk REST APIs di API Gateway untuk detailnya.
c18d2gz168 Perlindungan Penghapusan	AWSManagedServices-TrustedRemediatorEnableELBDeletionProtection- Perlindungan penghapusan	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Elastic Load Balancing Tidak Diaktifkan untuk Load Balancer	an dihidupkan untuk Elastic Load Balancer.	Tidak ada kendala
c1qf5bt012 Amazon RDS Performance Insights dimatikan	AWSManagedServices-TrustedR emediatorEnableRDSPerformanceInsights Performance Insights diaktifkan untuk Amazon RDS.	• PerformanceInsightsRetentionPeriod: Jumlah hari untuk menyimpan data Performance Insights. Nilai Valid: 7 atau bulan* 31, di mana bulan adalah jumlah bulan dari 1-23. Contoh: 93 (3 bulan* 31), 341 (11 bulan* 31), 589 (19 bulan* 31) atau 731. • PerformanceInsightsKMSKeyId: Id AWS KMS kunci untuk enkripsi data Performance Insights. Jika Anda tidak menentukan nilai untuk PerformanceInsights KMSKeyId, Amazon RDS menggunakan AWS KMS kunci default Anda. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
c1fd6b96l4 Log Akses Amazon S3 Diaktifkan	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 Pencatatan akses bucket Amazon S3 diaktifkan.	- TargetBucketTagValue: Nilai tag (peka huruf besar/kecil) untuk mengidentifikasi bucket target, gunakan ini dan TargetBucketTagKey untuk menandai bucket yang akan digunakan sebagai bucket tujuan untuk pencatatan akses. - TargetObjectKeyFormat: Format kunci Amazon S3 untuk objek log (nilai peka huruf besar/kecil). Untuk menggunakan format sederhana untuk kunci S3 untuk objek log, pilihSimplePrefix . Untuk menggunakan kunci S3 yang dipartisi untuk objek log dan gunakan EventTime untuk awalan yang dipartisi, pilih. PartitionedPrefixEventTime Untuk menggunakan kunci S3 yang dipartisi untuk objek log dan gunakan DeliveryTime untuk awalan yang dipartisi, pilih. PartitionedPrefixDeliveryTime Nilai yang valid adalahSimplePrefix , PartitionedPrefixEventTime danPartitionedPrefixDeliveryTime . Untuk mengaktifkan remediasi otomatis, parameter yang telah

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
		dikonfigurasi sebelumnya harus disediakan: TargetBucketTagKeydan. TargetBucketTagValue Bucket tujuan harus sama Wilayah AWS dan Akun AWS sebagai bucket sumber, dengan izin yang benar untuk pengiriman log. Untuk informasi selengkapnya, lihat Mengaktifkan pencatatan akses server Amazon S3.

Konfigurasi remediasi Trusted Advisor cek di Remediator Terpercaya

Konfigurasi disimpan AWS AppConfig sebagai bagian dari aplikasi Remediator Terpercaya. Setiap kategori Trusted Advisor cek memiliki profil konfigurasi terpisah. Untuk informasi selengkapnya tentang Trusted Advisor kategori, lihat [Lihat kategori cek](#).

Anda dapat meminta untuk mengonfigurasi remediasi berdasarkan per sumber daya atau per Trusted Advisor pemeriksaan. Anda dapat menerapkan pengecualian menggunakan tag sumber daya.

Note

Remediasi Trusted Advisor temuan saat ini dikonfigurasi menggunakan AWS AppConfig, dan fitur ini sepenuhnya didukung hari ini. AMS mengantisipasi bahwa ini akan berubah di masa depan. Ini adalah praktik terbaik untuk menghindari membangun otomatisasi yang bergantung pada AWS AppConfig, karena metode ini dapat berubah. Ketahuilah bahwa Anda mungkin perlu memperbarui atau memodifikasi otomatisasi yang dibangun di sekitar AWS AppConfig implementasi saat ini di masa mendatang untuk kompatibilitas.

Compute Optimizer EC2 -> flag fitur instance memiliki parameter tambahan:

- allow-upscale Untuk mengizinkan instance kelas atas yang tidak dioptimalkan yang kurang disediakan. EC2 Nilai defaultnya adalah "false".

- `min-savings-opportunity-percentage` Peluang persentase penghematan minimum untuk remediasi otomatis. Nilai defaultnya adalah 10%

Konfigurasi remediasi default

Konfigurasi untuk Trusted Advisor pemeriksaan individual disimpan sebagai AWS AppConfig bendera. Nama bendera cocok dengan nama cek. Setiap konfigurasi cek berisi atribut berikut:

- **mode eksekusi:** Menentukan bagaimana Trusted Remediator melakukan remediasi default:
 - **Automated:** Trusted Remediator secara otomatis memulihkan sumber daya dengan membuat OpsItem, menjalankan dokumen SSM, dan kemudian menyelesaikan setelah eksekusi berhasil. OpsItem
 - **Petunjuk:** An OpsItem dibuat, tetapi dokumen SSM tidak dijalankan secara otomatis. Anda meninjau OpsItem dan menjalankan remediasi menggunakan RFC otomatis. Untuk informasi selengkapnya, lihat [Bekerja dengan remediasi di Remediator Tepercaya](#).
 - **Bersyarat:** Remediasi dinonaktifkan secara default. Anda dapat mengaktifkannya untuk sumber daya tertentu menggunakan tag. Untuk informasi selengkapnya, lihat bagian berikut [Sesuaikan remediasi dengan tag sumber daya](#) dan [Sesuaikan remediasi dengan tag penggantian sumber daya](#).
 - **Tidak aktif:** Remediasi tidak terjadi dan tidak ada OpsItem yang dibuat. Anda tidak dapat mengganti mode eksekusi untuk Trusted Advisor pemeriksaan yang disetel ke tidak aktif.
- **parameter yang telah dikonfigurasi sebelumnya:** Masukkan nilai untuk parameter dokumen SSM yang diperlukan untuk remediasi otomatis, dalam format, dipisahkan dengan koma (`Parameter=Value,`). Lihat parameter [Trusted Advisor cek yang didukung oleh Trusted Remediator](#) yang telah dikonfigurasi sebelumnya yang didukung untuk dokumen SSM terkait untuk setiap pemeriksaan.
- **alternative-automation-document:** Atribut ini membantu mengganti dokumen otomatisasi yang ada dengan dokumen lain yang didukung (jika tersedia untuk pemeriksaan tertentu). Secara default, atribut ini tidak dipilih.

Note

`alternative-automation-document` Atribut tidak mendukung dokumen otomatisasi kustom. Anda dapat menggunakan dokumen otomatisasi Remediator Tepercaya yang sudah ada yang tercantum di [Trusted Advisor cek yang didukung oleh Trusted Remediator](#).

Misalnya, untuk cekQch7DwouX1, ada tiga dokumen SSM terkait: AWSManagedServices-StopEC2Instance, AWSManagedServices-ResizeInstanceByOneLevel, dan. AWSManagedServices-TerminateInstance Nilai untuk alternative-automation-document dapat berupa AWSManagedServices-ResizeInstanceByOneLevel atau AWSManagedServices-TerminateInstance (AWSManagedServices-StopEC2Instance adalah dokumen SSM default untuk diperbaikiQch7DwouX1).

Nilai untuk setiap atribut harus sesuai dengan batasan atribut tersebut.

Tip

Sebelum Anda menerapkan konfigurasi default untuk Trusted Advisor pemeriksaan Anda, sebaiknya pertimbangkan untuk menggunakan fitur penandaan Sumber Daya dan penggantian sumber daya yang dijelaskan di bagian berikut. Konfigurasi default berlaku untuk semua sumber daya dalam akun, yang mungkin tidak diinginkan dalam semua kasus.

Berikut ini adalah contoh tangkapan layar konsol dengan mode eksekusi diatur ke Manual dan atribut yang cocok dengan kendala mereka.

Sesuaikan remediasi dengan tag sumber daya

manual-for-tagged-onlyAtribut automated-for-tagged-onlydan dalam konfigurasi cek memungkinkan Anda untuk menentukan tag sumber daya untuk bagaimana Anda ingin memulihkan pemeriksaan individual. Ini adalah praktik terbaik untuk menggunakan metode ini ketika Anda perlu menerapkan perilaku remediasi yang konsisten ke sekelompok sumber daya yang berbagi tag atau tag yang sama. Berikut ini adalah deskripsi untuk tag ini:

- automated-for-tagged-only: Tentukan tag sumber daya (satu atau beberapa pasangan tag, dipisahkan koma) untuk pemeriksaan untuk memulihkan secara otomatis, terlepas dari mode eksekusi default.
- manual-for-tagged-only: Tentukan tag sumber daya (satu atau beberapa pasangan tag, dipisahkan koma) untuk remediasi yang harus dijalankan secara manual, terlepas dari mode eksekusi default.

Misalnya, jika Anda ingin mengaktifkan remediasi otomatis untuk semua sumber daya non-produksi dan menerapkan remediasi manual untuk sumber daya produksi, Anda dapat menetapkan konfigurasi sebagai berikut:

```
"execution-mode": "Conditional",  
"automated-for-tagged-only": "Environment=Non-Production",  
"manual-for-tagged-only": "Environment=Production",
```

Dengan konfigurasi sebelumnya yang ditetapkan pada sumber daya Anda, periksa perilaku remediasi adalah sebagai berikut:

- Sumber daya yang ditandai dengan 'Environment=Non-Production' diperbaiki secara otomatis.
- Sumber daya yang ditandai dengan 'Environment=Production' memerlukan intervensi manual untuk remediasi.
- Sumber daya tanpa tag 'Lingkungan' mengikuti mode eksekusi default ('Conditional', dalam hal ini. Jadi, tidak ada tindakan yang diambil pada sumber daya yang tersisa).

Untuk dukungan tambahan dengan konfigurasi Anda, hubungi Cloud Architect Anda.

Sesuaikan remediasi dengan tag penggantian sumber daya

Tag penggantian sumber daya memungkinkan Anda menyesuaikan perilaku remediasi untuk sumber daya individual, terlepas dari tag mereka. Dengan menambahkan tag tertentu ke sumber daya, Anda mengganti mode eksekusi default untuk sumber daya tersebut dan Trusted Advisor pemeriksaan. Tag penggantian sumber daya lebih diutamakan daripada konfigurasi default dan setelan penandaan sumber daya. Jadi, jika Anda menyetel mode eksekusi default ke Otomatis, Manual, atau Bersyarat untuk sumber daya yang menggunakan tag penggantian sumber daya, itu akan mengganti mode eksekusi default dan konfigurasi penandaan sumber daya apa pun.

Untuk mengganti mode eksekusi sumber daya, selesaikan langkah-langkah berikut:

1. Identifikasi sumber daya yang ingin Anda ganti konfigurasi remediasi.
2. Tentukan ID Trusted Advisor cek untuk cek yang ingin Anda ganti. Anda dapat menemukan cek IDs untuk Trusted Advisor cek yang didukung [Trusted Advisor cek yang didukung oleh Trusted Remediator](#).
3. Tambahkan tag ke sumber daya dengan kunci dan nilai berikut menggunakan [Tag | Update](#) atau [Tag | Jenis perubahan Pembaruan Massal](#):

- Kunci tag: TR-*Trusted Advisor check ID*-Execution-Mode (peka huruf besar/kecil)

Dalam contoh kunci tag sebelumnya, ganti Trusted Advisor check ID dengan tanda Trusted Advisor centang unik yang ingin Anda timpa.

- Nilai tag: Gunakan salah satu nilai berikut untuk nilai tag:
 - Otomatis: Remediator Tepercaya secara otomatis memulihkan sumber daya untuk pemeriksaan ini Trusted Advisor .
 - Petunjuk: An OpsItem dibuat untuk sumber daya, tetapi remediasi tidak dilakukan secara otomatis. Anda meninjau dan menjalankan remediasi menggunakan otomatis. Untuk informasi selengkapnya, lihat [Bekerja dengan remediasi di Remediator Tepercaya](#).
 - Tidak aktif: Remediasi dan OpsItem pembuatan tidak dilakukan untuk sumber daya ini dan pemeriksaan yang ditentukan Trusted Advisor .

Misalnya, untuk memulihkan volume Amazon EBS secara otomatis dengan ID Trusted Advisor cek, DAvU99Dc4C tambahkan tag ke volume EBS. Kunci tag adalah TR-DAvU99Dc4C-Execution-Mode dan nilai tag adalah Automated.

Berikut ini adalah contoh konsol yang menunjukkan bagian Tag:

Alur kerja keputusan mode eksekusi

Ada beberapa level untuk mengonfigurasi mode eksekusi untuk sumber daya Anda dan setiap Trusted Advisor pemeriksaan. Diagram berikut menunjukkan bagaimana Trusted Remediator memutuskan mode eksekusi mana yang akan digunakan berdasarkan konfigurasi Anda:

Konfigurasikan tutorial remediasi

Tutorial berikut memberikan contoh pembuatan remediasi umum di Trusted Remediator

Memulihkan semua sumber daya secara manual

Contoh ini mengonfigurasi remediasi manual untuk semua volume Amazon EBS dengan ID Trusted Advisor cek DAv U99Dc4C (Volume Amazon EBS yang Kurang Digunakan).

Konfigurasi remediasi manual untuk volume Amazon EBS dengan cek ID U99Dc4C DAV

1. Gunakan Remediation Configuration|Update, ubah jenis untuk meminta pembaruan konfigurasi.
2. Masukkan parameter berikut:
 - CheckIds: DAV U99Dc4C
 - ExecutionMode: Manual

Note

Beberapa pemeriksaan dapat dikonfigurasi dalam satu permintaan. Untuk pemeriksaan yang memerlukan konfigurasi yang sama, sertakan beberapa pemeriksaan IDs di CheckIdsparameter. Untuk pemeriksaan yang memerlukan konfigurasi berbeda, buat RemediationConfigurationobjek baru.

3. Kirim RFC.

Memulihkan semua sumber daya secara otomatis, kecuali untuk sumber daya yang dipilih

Contoh ini mengonfigurasi remediasi otomatis untuk semua volume Amazon EBS dengan ID Trusted Advisor cek DAV U99Dc4C (Volume Amazon EBS yang Kurang Digunakan), dengan pengecualian volume tertentu yang tidak akan diperbaiki (ditetapkan Tidak Aktif).

Konfigurasi remediasi otomatis untuk volume Amazon EBS dengan cek ID DAV U99Dc4C, dengan pengecualian sumber daya tidak aktif yang dipilih

1. Ganti remediasi otomatis untuk volume Amazon EBS yang dipilih:

Gunakan [Tag | Perbarui](#) atau [Tag | Jenis perubahan Pembaruan Massal](#) untuk menerapkan tag berikut untuk volume yang akan dikecualikan dari remediasi otomatis:

- Kunci: Mode Eksekusi TR- DAV U99Dc4C
 - Nilai: Tidak aktif
2. Gunakan jenis perubahan Remediation Configuration|Update untuk meminta pembaruan konfigurasi.
 3. Masukkan parameter berikut:

- CheckIds: DAv U99Dc4C
- ExecutionMode: Otomatis

4. Kirim RFC.

Memulihkan sumber daya yang ditandai secara otomatis

Contoh ini mengonfigurasi remediasi otomatis untuk semua volume Amazon EBS dengan tag `Stage=NonProd` dengan ID Trusted Advisor cek DAv U99Dc4C (Volume Amazon EBS yang Kurang Digunakan). Semua sumber daya lain tanpa tag ini tidak diperbaiki.

Konfigurasikan remediasi otomatis untuk volume Amazon EBS dengan tag **Stage=NonProd** untuk cek ID U99Dc4C DAv

1. Gunakan [Konfigurasi Remediasi | Perbarui](#), ubah jenis untuk meminta pembaruan konfigurasi.
2. Masukkan parameter berikut:
 - CheckIds: DAv U99Dc4C
 - ExecutionMode: Bersyarat
 - AutomatedForTaggedOnly: {"Tahap": "NonProd" }

Note

Nilai yang ditentukan untuk AutomatedForTaggedOnlyparameter mengesampingkan nilai yang dikonfigurasi sebelumnya. Untuk mempertahankan tag yang ada, sertakan dalam nilai baru.

3. Kirim RFC.

Setel ulang konfigurasi ke default

Contoh ini menghapus automated-for-tagged-onlykonfigurasi yang ada untuk cek Hs4Ma3G104. Untuk menghapus konfigurasi tag yang diterapkan sebelumnya, atur nilai AutomatedForTaggedOnlyparameter ke {}.

Setel ulang konfigurasi ke default untuk cek Hs4Ma3G104

1. Gunakan [Konfigurasi Remediasi | Perbarui](#) jenis perubahan untuk meminta pembaruan konfigurasi.
2. Masukkan parameter berikut:
 - CheckIds: Hs4Ma3G104
 - ExecutionMode: Masukkan nilai yang saat ini digunakan
 - AutomatedForTaggedOnly: {}
3. Kirim RFC.

Bekerja dengan remediasi di Remediator Terpercaya

Lacak remediasi di Remediator Terpercaya

Untuk melacak OpsItems remediasi, selesaikan langkah-langkah berikut:

1. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
2. Pilih Manajemen Operasi, OpsCenter.
3. (Opsional) Filter daftar berdasarkan Sumber = Remediator Terpercaya untuk menyertakan hanya Remediator Terpercaya dalam daftar. OpsItems

Berikut ini adalah contoh OpsCenter layar yang disaring oleh Source=Trusted Remediator:

Note

Selain melihat OpsItems dari OpsCenter, Anda dapat melihat log remediasi di bucket AMS S3. Untuk informasi selengkapnya, lihat [Log remediasi di Remediator Terpercaya](#).

Jalankan remediasi manual di Remediator Terpercaya

Trusted Remediator membuat OpsItems pemeriksaan yang dikonfigurasi untuk remediasi manual. Anda harus meninjau pemeriksaan ini dan memulai proses remediasi secara manual.

Untuk memulihkan secara manual OpsItem, selesaikan langkah-langkah berikut:

1. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
2. Pilih Manajemen Operasi, OpsCenter.
3. (Opsional) Filter daftar berdasarkan Sumber = Remediator Terpercaya untuk menyertakan hanya Remediator Terpercaya dalam daftar. OpsItems
4. Pilih OpsItem yang ingin Anda tinjau.
5. Tinjau data operasional OpsItem. Data operasional mencakup item-item berikut:
 - trustedAdvisorCheckKategori: Kategori ID Trusted Advisor cek. Misalnya, toleransi kesalahan
 - trustedAdvisorCheckId: ID Trusted Advisor cek unik.
 - trustedAdvisorCheckMetadata: Metadata sumber daya, termasuk ID sumber daya.
 - trustedAdvisorCheckNama: Nama Trusted Advisor cek.
 - trustedAdvisorCheckStatus: Status Trusted Advisor cek terdeteksi untuk sumber daya.
 - trustedAdvisorCheckManualRemediation: Data kustom yang memberikan rincian referensi untuk remediasi manual.
 - ManualExecutionInput: Objek yang mendefinisikan parameter yang dapat Anda ubah nilainya saat menjalankan remediasi manual.
 - DocumentName: Nama runbook (dokumen SSM).
 - CustomizableParameters: Nama parameter yang dapat Anda modifikasi.
 - DefaultInput: Objek yang mendefinisikan nama parameter dan nilai yang akan digunakan untuk remediasi manual. Nilai terisi berdasarkan parameter yang telah dikonfigurasi sebelumnya.
6. Untuk memulihkan secara manual OpsItem, selesaikan langkah-langkah berikut:
 - a. Gunakan [Remediator Terpercaya | Menemukan | Memperbaiki tipe perubahan ct-1c7ch8z5phrjp](#)
 - b. Masukkan nilai untuk parameter berikut:
 - DocumentName: HarusAWSManagedServices-RemediateTrustedRemediatorFinding.
 - Wilayah: The Wilayah AWS, dalam bentuk us-east-1.
 - Parameter: Masukkan parameter remediasi manual:
 - OpsItemId: ID Item Ops.

- RemediationDocumentName: Nama dokumen otomatisasi SSM yang akan digunakan. Dokumen harus dikaitkan dengan Item Ops. Jika beberapa dokumen dikaitkan dengan Item Ops, maka DocumentName harus ditentukan.
 - RemediationParameters: key/value Peta parameter untuk eksekusi otomatisasi, dalam bentuk: `{"ParameterName1\" : [\"ParameterValue1\"], \"ParameterName2\" : [\"ParameterValue2\"]}`. Anda hanya dapat menggunakan parameter yang ada di Item Ops trustedAdvisorCheckManualRemediation CustomizableParameters. Jika tidak ditentukan, parameter dan nilai diambil dari Item Ops.
- c. Pilih Jalankan. Jika tidak ada kesalahan, maka halaman RFC berhasil dibuat ditampilkan dengan detail RFC yang dikirimkan, dan output Run awal.
 - d. Pantau kemajuan eksekusi RFC.
 - e. Setelah eksekusi selesai, OpsItem diselesaikan. Jika RFC gagal, ikuti langkah-langkahnya. [Memecahkan masalah remediasi di Remediator Tepercaya](#) Untuk dukungan pemecahan masalah tambahan, hubungi AMS.

Memecahkan masalah remediasi di Remediator Tepercaya

Untuk bantuan dengan remediasi manual dan kegagalan remediasi, hubungi AMS.

Untuk melihat status dan hasil remediasi, selesaikan langkah-langkah berikut:

1. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
2. Pilih Manajemen Operasi, OpsCenter.
3. (Opsional) Filter daftar berdasarkan Sumber = Remediator Tepercaya untuk menyertakan hanya Remediator Tepercaya dalam daftar. OpsItems
4. Pilih OpsItem yang ingin Anda tinjau.
5. Di bagian Eksekusi Otomasi, tinjau Nama Dokumen dan Status serta hasil.
6. Tinjau kegagalan otomatisasi umum berikut. Jika masalah Anda tidak tercantum di sini, hubungi CSDM Anda untuk mendapatkan bantuan.

Kesalahan remediasi umum

Tidak ada eksekusi yang tercantum dalam Eksekusi Otomasi

Tidak ada eksekusi yang terkait dengan yang OpsItem mungkin menunjukkan bahwa eksekusi gagal dimulai karena nilai parameter yang salah.

Langkah pemecahan masalah

1. Dalam data Operasional, tinjau nilai `trustedAdvisorCheckAutoRemediation` properti.
2. Verifikasi bahwa nilai `DocumentName` dan Parameter sudah benar. Untuk nilai yang benar, tinjau [Konfigurasi remediasi Trusted Advisor cek di Remediator Terpercaya](#) detail tentang cara mengonfigurasi parameter SSM. Untuk meninjau parameter pemeriksaan yang didukung, lihat [Trusted Advisor cek yang didukung oleh Trusted Remediator](#)
3. Verifikasi bahwa nilai dalam dokumen SSM cocok dengan pola yang diizinkan. Untuk melihat detail parameter dalam konten dokumen, pilih nama dokumen di bagian Runbooks.
4. Setelah Anda meninjau dan memperbaiki parameter, perbaiki parameter secara manual. OpsItem Untuk langkah-langkah remediasi, lihat [Jalankan remediasi manual di Remediator Terpercaya](#).
5. Untuk mencegah kesalahan ini terulang, pastikan Anda mengonfigurasi remediasi dengan nilai parameter yang benar dalam konfigurasi Anda. Untuk informasi selengkapnya, lihat [Konfigurasi remediasi Trusted Advisor cek di Remediator Terpercaya](#)

Eksekusi gagal dalam Eksekusi Otomasi

Dokumen remediasi berisi beberapa langkah yang berinteraksi dengan Layanan AWS melakukan berbagai tindakan melalui APIs. Untuk mengidentifikasi penyebab spesifik kegagalan, selesaikan langkah-langkah berikut:

Langkah pemecahan masalah

1. Untuk melihat langkah-langkah eksekusi individual, pilih ID Eksekusi, tautan di bagian Eksekusi Otomasi. Berikut ini adalah contoh konsol Systems Manager yang menunjukkan langkah-langkah Execution untuk otomatisasi yang dipilih:
2. Pilih langkah dengan status Gagal. Berikut ini adalah contoh pesan kesalahan:
 - `NoSuchBucket` - An error occurred (`NoSuchBucket`) when calling the `GetPublicAccessBlock` operation: The specified bucket does not exist

Kesalahan ini menunjukkan bahwa nama bucket yang salah telah ditentukan dalam parameter konfigurasi remediasi yang telah dikonfigurasi sebelumnya.

Untuk mengatasi kesalahan ini, [jalankan otomatisasi secara manual](#) menggunakan nama bucket yang benar. Untuk mencegah masalah ini terulang, [perbarui konfigurasi remediasi dengan nama](#) bucket yang benar.

- DB instance my-db-instance-1 is not in available status for modification.

Kesalahan ini menunjukkan bahwa otomatisasi tidak dapat membuat perubahan yang diharapkan karena instans DB dalam keadaan tidak valid.

Untuk mengatasi kesalahan ini, [jalankan otomatisasi secara manual](#).

Log remediasi di Remediator Terpercaya

Trusted Remediator membuat log dalam format JSON dan mengunggahnya ke Amazon Simple Storage Service File log diunggah ke bucket S3 yang dibuat oleh AMS dan diberi nama. `ams-trusted-remediator-{your-account-id}-logs` AMS membuat bucket S3 di akun Administrator Delegasi. Anda dapat mengimpor file log ke dalam QuickSight untuk menghasilkan laporan remediasi yang disesuaikan.

Log item remediasi

Trusted Remediator menciptakan Remediation item log ketika remediasi OpsItem dibuat. Log ini berisi remediasi manual OpsItem dan remediasi otomatis. OpsItem Anda dapat menggunakan Remediation item log untuk melacak ikhtisar semua remediasi.

Lokasi log item remediasi untuk rekomendasi Compute Optimizer

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs/  
compute_optimizer_remediation_items/remediation creation time in yyyy-mm-  
dd format/10 digits epoch time or unix timestamp-Trustee Advisor check ID-  
Resource ID.json
```

Lokasi log item remediasi untuk pemeriksaan Trusted Advisor

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs/
remediation_items/*remediation creation time in yyyy-mm-dd format/10 digits
epoch time or unix timestamp-Trusted Advisor check ID- Resource ID*.json

URL file contoh log item remediasi

s3:///ams-trusted-remediator-*111122223333*-logs/
remediation_items/*2023-02-06/1675660464-DAvU99Dc4C-
vol-00bd8965660b4c16d*.json

Format log item Remediasi Compute Optimizer

```
{
  "AccountID": "Account_ID",
  "ComputeOptimizerCheckID": "Compute Optimizer check ID",
  "ComputeOptimizerCheckName": "Compute Optimizer check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

Trusted Advisor Format log item remediasi

```
{
  "TrustedAdvisorCheckID": Trusted Advisor check ID,
  "TrustedAdvisorCheckName": Trusted Advisor check name,
  "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
  "ResourceID": Resource ID,
  "RemediationTime": Remediation creation time,
  "ExecutionMode": Automated or Manual,
  "OpsItemID": OpsItem ID
}
```

Isi sampel format log item Remediasi Remediasi Compute Optimizer

```
{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
}
```

```
"RemediationTime": 1755044783,
"ExecutionMode": "Manual",
"OpsItemID": "oi-b8888b38fe78"
}
```

Trusted Advisor Format log item remediasi konten sampel

```
{
  "TrustedAdvisorCheckID": "DAvU99Dc4C",
  "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
  "TrustedAdvisorCheckResultTime": 1675614749,
  "ResourceID": "vol-00bd8965660b4c16d",
  "RemediationTime": 1675660464,
  "OpsItemID": "oi-cca5df7af718"
}
```

Log eksekusi remediasi otomatis, Compute Optimizer dan Trusted Advisor

Trusted Remediator membuat Automated remediation execution log ketika menjalankan dokumen SSM otomatis selesai. Log ini berisi rincian proses SSM untuk remediasi otomatis saja. OpsItem Anda dapat menggunakan file log ini untuk melacak remediasi otomatis.

Compute Optimizer Lokasi log remediasi otomatis

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs//
remediation_executions/*remediation creation time in yyyy-mm-dd format/10
digits epoch time or unix timestamp-Compute Optimizer recommendation
ID*.json

Trusted Advisor Lokasi log remediasi otomatis

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs//
remediation_executions/*remediation creation time in yyyy-mm-dd format/10
digits epoch time or unix timestamp-Trusted Advisor check ID-Resource
ID*.json

Compute Optimizer Contoh lokasi log remediasi otomatis

s3://ams-trusted-remediator-*111122223333*-logs/
remediation_executions/2025-06-26/1750908858-123456789012-compute-
optimizer-ec2-i-1235173471d2cd789.json

Trusted Advisor Contoh lokasi log remediasi otomatis

```
s3://ams-trusted-remediator-111122223333-logs/  
remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-  
vol-00bd8965660b4c16d.json
```

Konten sampel format log remediasi otomatis

```
{  
  "OpsItemID": "oi-767c77e05301",  
  "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",  
  "SSMExecutionStatus": "Success"}
```

Praktik terbaik dalam Remediator Tepercaya

Berikut ini adalah praktik terbaik untuk membantu Anda menggunakan Remediator Tepercaya:

- Jika Anda tidak yakin tentang hasil remedasi, mulailah dengan mode eksekusi manual. Terkadang, menerapkan eksekusi otomatis untuk remediasi sejak awal dapat menyebabkan hasil yang tidak terduga.
- Lakukan tinjauan mingguan terhadap remediasi dan OpsItems untuk mendapatkan wawasan dalam hasil Remediator Tepercaya.
- Akun anggota mewarisi konfigurasi dari akun administrator yang didelegasikan. Jadi, penting untuk menyusun akun dengan cara yang membantu Anda mengelola beberapa akun dengan konfigurasi yang sama. Anda dapat mengecualikan sumber daya dari konfigurasi default menggunakan tag.

Remediator Tepercaya FAQs

Berikut ini adalah pertanyaan yang sering diajukan tentang Remediator Tepercaya:

Apa itu Remediator Tepercaya dan bagaimana manfaatnya bagi saya?

Ketika ketidakpatuhan diidentifikasi oleh Trusted Advisor atau rekomendasi dikeluarkan oleh Compute Optimizer, Trusted Remediator merespons sesuai dengan preferensi yang Anda tentukan, baik dengan menerapkan remediasi, meminta persetujuan melalui remediasi manual, atau melaporkan remediasi selama Tinjauan Bisnis Bulanan (MBR) Anda yang akan datang. Remediasi terjadi pada waktu atau jadwal remediasi pilihan Anda. Trusted Remediator memberi Anda kemampuan untuk melayani diri sendiri dan bertindak berdasarkan Trusted Advisor pemeriksaan dengan fleksibilitas untuk mengonfigurasi dan memulihkan pemeriksaan secara individual atau

massal. Dengan pustaka dokumen remediasi yang telah diuji, AMS terus meningkatkan akun Anda dengan menerapkan pemeriksaan keamanan dan mengikuti praktik AWS terbaik. Anda hanya diberi tahu jika Anda menentukan untuk melakukannya dalam konfigurasi Anda. Pengguna AMS dapat ikut serta dalam Remediator Tepercaya tanpa biaya tambahan.

Bagaimana Trusted Remediator berhubungan dan bekerja dengan orang lain? Layanan AWS

Anda memiliki akses ke Trusted Advisor pemeriksaan dan rekomendasi Compute Optimizer sebagai bagian dari paket Enterprise Support yang ada. Trusted Remediator terintegrasi dengan Trusted Advisor dan Compute Optimizer untuk memanfaatkan kemampuan otomatisasi AMS yang ada. Secara khusus, AMS menggunakan dokumen AWS Systems Manager otomatisasi (runbook) untuk remediasi otomatis. AWS AppConfig digunakan untuk mengkonfigurasi alur kerja remediasi. Anda dapat melihat semua remediasi saat ini dan masa lalu melalui Systems Manager OpsCenter. Log remediasi disimpan dalam bucket Amazon S3. Anda dapat menggunakan log untuk mengimpor dan membuat dasbor pelaporan kustom. QuickSight

Siapa yang mengkonfigurasi remediasi?

Anda memiliki konfigurasi di akun Anda. Mengelola konfigurasi Anda adalah tanggung jawab Anda. Anda juga dapat menghubungi AMS untuk perubahan konfigurasi, dukungan, dan remediasi manual, serta pemecahan masalah kegagalan remediasi.

Bagaimana cara menginstal dokumen otomatisasi SSM?

Dokumen otomatisasi SSM secara otomatis dibagikan ke akun AMS onboard.

Apakah sumber daya yang dimiliki AMS juga akan diperbaiki?

Sumber daya yang dimiliki AMS tidak ditandai oleh Trusted Remediator. Remediator Tepercaya hanya berfokus pada sumber daya Anda.

Apa yang Wilayah AWS tersedia dalam Remediator Tepercaya dan siapa yang dapat menggunakannya?

Remediator Tepercaya tersedia untuk pelanggan AMS Advanced. Untuk daftar Wilayah dukungan saat ini, lihat [Layanan AWS menurut Wilayah](#).

Akankah Remediator Tepercaya menyebabkan penyimpangan sumber daya?

Karena dokumen otomatisasi SSM secara langsung memperbarui sumber daya melalui AWS API, penyimpangan sumber daya mungkin terjadi. Anda dapat menggunakan tag untuk memisahkan

sumber daya yang dibuat melalui paket yang ada CI/CD . Anda dapat mengonfigurasi Trusted Remediator untuk mengabaikan sumber daya yang ditandai sambil tetap memulihkan sumber daya Anda yang lain.

Bagaimana cara menjeda atau menghentikan Remediator Tepercaya?

Gunakan [Manajemen | Remediator Tepercaya | Status | Aktifkan atau nonaktifkan](#) jenis perubahan untuk menghentikan layanan Remediator Tepercaya. Gunakan jenis perubahan yang sama untuk mengaktifkan kembali Remediator Tepercaya.

Bagaimana cara memulihkan pemeriksaan yang tidak didukung oleh Trusted Remediator?

Anda dapat terus menghubungi AMS melalui Operations On Demand (OOD) untuk pemeriksaan yang tidak didukung. AMS membantu Anda memulihkan pemeriksaan ini. Untuk informasi selengkapnya, lihat [Operasi Sesuai Permintaan](#).

Sumber daya apa yang diterapkan oleh Trusted Remediator ke akun Anda?

Trusted Remediator menyebarkan sumber daya berikut di akun administrator delegasi Remediator Tepercaya:

- Ember Amazon S3 bernama. `ams-trusted-remediator-{your-account-id}-logs` Trusted Remediator membuat format Remediation item log dalam JSON saat remediasi OpsItem dibuat, dan mengunggah file log ke bucket ini.
- AWS AppConfig Aplikasi untuk menyimpan konfigurasi remediasi untuk Trusted Advisor pemeriksaan yang didukung dan rekomendasi Compute Optimizer.

Remediator Tepercaya tidak menyebarkan sumber daya di akun anggota Remediator Tepercaya.

Manajemen log

Topik

- [Apa itu manajemen log?](#)
- [Cara kerja pencatatan AMS](#)
- [Mengakses log Anda](#)
- [Menyesuaikan konfigurasi log Anda](#)

Manajemen log AMS mengumpulkan, mengumpulkan, dan mengontrol retensi log dari akun terkelola. AWS manajemen log mengumpulkan log dari EC2 instans Amazon dan AWS sumber daya yang digunakan dalam akun Anda ke dalam Log. CloudWatch Daftar lengkap layanan dari mana log saat ini digabungkan dapat ditemukan di [Log layanan agregat AMS](#).

Apa itu manajemen log?

Manajemen log adalah proses menangani peristiwa log yang dihasilkan oleh instans, aplikasi, dan layanan AWS. Fitur ini menentukan cara AMS memproses, menyimpan, dan memutar peristiwa log yang dihasilkan di akun AWS terkelola Anda. Log infrastruktur digunakan selama resolusi insiden dan untuk mendukung audit sistem.

Cara kerja pencatatan AMS

Manajemen log AMS single-account landing zone (SALZ) menggunakan berbagai agen dan alat pra-instal yang diimplementasikan saat instance dan aplikasi di-onboard atau disediakan.

Logging dikonfigurasi selama proses orientasi akun dan saat tumpukan diluncurkan.

Log landing zone multi-akun AMS (MALZ) yang dihasilkan oleh instans dan layanan AWS tersedia di Log CloudWatch atau Amazon Simple Storage Service (Amazon S3), di dalam setiap akun yang dikelola oleh AMS. AMS multi-account landing zone menyediakan Logging Account pusat yang bertindak sebagai lokasi agregasi pusat untuk beberapa log yang dihasilkan oleh akun aplikasi individual.

Tabel dalam [Mengakses log Anda](#) subbagian menjelaskan log mana yang tersedia di akun individual, dan mana yang tersedia di Akun Logging pusat.

Mengakses log Anda

Untuk mengakses log Anda, pastikan bahwa Anda memiliki salah satu peran IAM yang diperlukan dan berada di akun AMS Anda. Kemudian navigasikan ke direktori yang ditampilkan.

Multi-Account Landing Zone (MALZ)

Menyediakan lima peran IAM default, yang masing-masing memungkinkan akses ke semua log dalam akun Anda (semua diawali dengan `AWSManagedServices`):

- `AdminRole`
- `CaseRole`
- `ChangeManagementRole`
- `ReadOnlyRole`
- `SecurityOpsRole`

Akses ke peran ini dikonfigurasi melalui federasi, dengan setiap peran dipetakan ke grup dalam domain Direktori Aktif Anda.

Untuk mempelajari lebih lanjut tentang peran ini, lihat [Peran pengguna IAM di AMS](#).

Single-Account Landing Zone (SALZ)

Default `Customer_ReadOnly_Role` untuk landing zone akun tunggal AMS memungkinkan akses Anda ke semua log dalam akun Anda. Akses ke log dikontrol menggunakan peran AWS Identity and Access Management (IAM) yang dipetakan ke grup Active Directory.

Log layanan agregat AMS

Setiap AWS layanan log ke CloudWatch Log atau lokasi tertentu di bucket Amazon S3.

Note

Kecuali dinyatakan secara khusus, semua lokasi log bersifat lokal ke akun yang menghasilkan log, dan tidak digabungkan ke dalam akun Logging pusat.

Untuk menemukan nama CloudTrail jejak AMS default di akun SALZ dan MALZ, buka AWS Console untuk CloudTrail lalu ke halaman Trails dan cari AMS. Karena sumber daya AMS memiliki tag, Anda dapat menemukan jejak dengan cara ini. Contoh CloudTrail tag AMS:

Untuk mengakses log Anda, pastikan bahwa Anda memiliki salah satu peran IAM yang diperlukan dan berada di akun AMS Anda. Kemudian navigasikan ke direktori yang ditampilkan.

Multi-Account Landing Zone

Log Layanan Agregat zona pendaratan multi-akun AMS

	Nama layanan	Rincian log	Log lokasi
1	Amazon Aurora	Log umum, kueri lambat, dan kesalahan.	CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/{ <i>log_name</i> }
2	AWS CloudFormation (CFN)	Hanya pencatatan panggilan API.	AWS CloudFormation Panggilan API didokumentasikan melalui CloudTrail, yang mengirimkan lognya ke CloudWatch LogGroup dan kemudian menyinkronkan log ke dalam bucket S3. Log disimpan selama 14 hari secara default di CloudWatch LogGroup, dan disimpan tanpa batas waktu di bucket S3. CloudWatch LogGroup:/CloudTrail/Zona Pendaratan-Log Bucket S3 [di Akun Logging pusat]: aws-landing-zone-logs -ams-a {<i>account_ID</i> } -log-management- {<i>region</i> Jalur:/AWSLogs/{<i>account_ID</i> }/CloudTrail/

	Nama layanan	Rincian log	Log lokasi
3	Amazon CloudFront (CloudFront)	Pencatatan permintaan pengguna. CloudFront logging harus diaktifkan secara eksplisit. Untuk informasi, lihat Mengaktifkan pencatatan untuk layanan yang didukung .	Ember S3: ams-a { <i>account_ID</i> } -log-manajemen- { <i>region</i> Jalur: AWS/RedShift/{ <i>CloudFront distribution ID</i>
4	Amazon CloudWatch (CloudWatch)	Hanya pencatatan panggilan API.	CloudWatch LogGroup:/CloudTrail/Zona Pendaratan-Log Bucket S3 [di Akun Logging pusat]: aws-landing-zone-logs - { <i>account_ID</i> } - { <i>region</i> Jalur:/AWSLogs/{ <i>account_ID</i> }/CloudTrail/
5	Amazon Elastic Block Store (Amazon EBS)	Tidak ada log yang diproduksi oleh layanan EBS.	Tidak berlaku
6	Amazon Elastic Compute Cloud (Amazon EC2)	Log sistem dan aplikasi. Untuk informasi, lihat Amazon Elastic Compute Cloud (Amazon EC2) - log tingkat sistem .	CloudWatch Log:/{ <i>instance ID</i> }
7	Amazon Elastic File System (Amazon EFS)	Hanya pencatatan panggilan API.	CloudWatch LogGroup:/CloudTrail/Zona Pendaratan-Log Bucket S3 [di Akun Logging pusat]: aws-landing-zone-logs - { <i>account_ID</i> } - { <i>region</i> Jalur:/AWSLogs/{ <i>account_ID</i> }/CloudTrail/

	Nama layanan	Rincian log	Log lokasi
8	Elastic Load Balancing (ELB)	Akses dan entri log kesalahan. Penyeimbang beban elastis mencatat semua permintaan yang dikirim ke mereka, termasuk permintaan yang tidak dirutekan ke instance back-end. Misalnya, jika klien mengirim permintaan yang salah bentuk, atau tidak ada contoh yang sehat untuk merespons, permintaan tersebut masih dicatat. Untuk informasi selengkapnya tentang entri log Elastic Load Balancing, lihat • Classic Load Balancers: Akses entri log. • Application Load Balancers: Akses entri log. • Network Load Balancers: Akses entri log.	Log panggilan API: CloudWatch LogGroup:/CloudTrail/Zona Pendaratan-Log Bucket S3 [di Akun Logging pusat]: aws-landing-zone-logs - {account_ID} - {region} Jalur:/AWSLogs/{account_ID}/CloudTrail/ Akses log: Ember S3: mc-a {account_ID} - log {region} Jalur: aws/elbaccess
9	OpenSearch Layanan Amazon (OpenSearch Layanan)	Log kesalahan layanan. Anda harus secara eksplisit mengaktifkan OpenSearch logging. Untuk informasi, lihat Mengaktifkan pencatatan untuk layanan yang didukung	CloudWatch LogGroup:/CloudTrail/Zona Pendaratan-Log Bucket S3 [di Akun Logging pusat]: aws-landing-zone-logs - {account_ID} - {region} Jalur:/AWSLogs/{account_ID}/CloudTrail/

	Nama layanan	Rincian log	Log lokasi
10	Amazon ElastiCache	Hanya pencatatan panggilan API.	CloudWatch LogGroup:///Zona Pendaratan-Log CloudTrail
11	Amazon GuardDuty		Bucket S3 [di Akun Logging pusat]: aws-landing-zone-logs - <i>{account_ID}</i> - <i>{region}</i>
12	Amazon Inspector		Jalur:/AWSLogs/ <i>{account_ID}</i> / CloudTrail/
13	Amazon Macie		
14	Amazon Redshift	Koneksi, pengguna, dan log aktivitas. Logging diaktifkan secara default saat Anda membuat kluster Redshift Anda dengan menjalankan Create Redshift cluster CT (ct-1malj7snzxrkr). Untuk selengkapnya, lihat Pencatatan Audit Database.	Ember S3: ams-a <i>{account_ID}</i> -log-manajemen- <i>{region}</i> Jalur: /AWS//<i>{}</i> RedShift <i>CloudFront Distribution ID</i>
15	Amazon Relational Database Service (RDS)	Log khusus untuk tipe database. Anda harus secara eksplisit mengaktifkan logging RDS. Untuk informasi, lihat Mengaktifkan pencatatan untuk layanan yang didukung Anda hanya dapat mengakses log MSSQL melalui prosedur tersimpan; untuk informasi, lihat Mengarsipkan File Log.	CloudWatch LogGroup: /aws/rds/ <i>(instanceataucluster)/{}/{}</i> <i>database_name log_name</i>

	Nama layanan	Rincian log	Log lokasi
16	Amazon S3 (S3)	Log akses bucket. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal seperti pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan (jika ada). Informasi log akses dapat berguna dalam audit keamanan dan akses. Ini juga dapat membantu Anda untuk mempelajari basis pelanggan Anda, serta memahami tagihan Amazon S3. Untuk informasi selengkapnya tentang entri Log Akses S3, lihat Format Log Akses Server S3.	Ember S3: mc-a {<i>account_ID</i>} - log-manajemen- {<i>region</i>} Jalur: /aws/s3access/ {<i>bucket_name</i>} Bucket S3 [di Akun Logging pusat]: aws-landing-zone-s 3-access-logs- {<i>account_ID</i>} - {<i>region</i>} Jalur: /
17	Amazon Simple Email Service (SES)	Panggilan layanan API SES.	CloudWatch LogGroup: /CloudTrail/Zona Pendaratan-Log Bucket S3 [di Akun Logging pusat]: aws-landing-zone-logs - {<i>account_ID</i>} - {<i>region</i>} Jalur: /AWSLogs/{<i>account_ID</i>}/CloudTrail/
18	Amazon Virtual Private Cloud (Amazon VPC)	Data aliran VPC (informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan VPC Anda).	CloudWatch LogGroup: /aws/vpcflow/ {<i>VPC_ID</i>}

	Nama layanan	Rincian log	Log lokasi
19	Auto Scaling	Hanya pencatatan panggilan API.	CloudWatch LogGroup:/CloudTrail/Zona Pendaratan-Log
20	AWS Certificate Manager		Bucket S3 [di Akun Logging pusat]: aws-landing-zone-logs - {account_ID} - {region} Jalur:/AWSLogs/{account_ID }/CloudTrail/
21	AWS CodeDeploy	Log penerapan khusus instance.	Pada Instance
22	AWS Config	Panggilan layanan AWS Config API.	CloudWatch LogGroup:/CloudTrail/Zona Pendaratan-Log Bucket S3 [di Akun Logging pusat]: aws-landing-zone-logs - {account_ID} - {region} Jalur:/AWSLogs/{account_ID }/CloudTrail/
		Konfigurasi sumber daya berubah, seperti yang dilacak oleh AWS Config.	Bucket S3 [di Akun Logging pusat]: aws-landing-zone-logs - {account_ID} - {region} Jalur:/AWSLogs/{account_ID }/Config/
23	AWS Database Migration Service	Log migrasi basis data. Untuk selengkapnya, lihat Memperkenalkan manajemen log di AWS Database Migration Service.	Konsol migrasi basis data

	Nama layanan	Rincian log	Log lokasi
24	AWS Direct Connect (DX)	Hanya pencatatan panggilan API.	CloudWatch LogGroup:/CloudTrail/Zona Pendaratan-Log
25	AWS Glacier		Bucket S3 [di Akun Logging pusat]: aws-landing-zone-logs - {account_ID} - {region} Jalur:/AWSLogs/{ account_ID }/CloudTrail/
26	AWS IAM (SAYA)		
27	AWS Key Management Service		
28	AWS Management Console (konsol atau AWS Console)		
29	AWS Simple Notification Service (SNS)		
30	Layanan Antrian Sederhana AWS (SQS)		

Single-Account Landing Zone

Log Layanan Agregat zona pendaratan akun tunggal AMS

	Nama layanan	Rincian log	Log lokasi
1	Amazon Aurora	Log umum, kueri lambat, dan kesalahan.	CloudWatch LogGroup: /aws/rds/cluster/{ database_name }/ {log_name}

	Nama layanan	Rincian log	Log lokasi
2	Amazon CloudFormation (CloudFormation atau CFN)	Hanya pencatatan panggilan API.	CloudFormation Panggilan API didokumentasikan melalui CloudTrail, yang mengirimkan lognya ke CloudWatch LogGroup dan kemudian menyinkronkan log ke dalam bucket S3. CloudWatch LogGroup: /aws/ams/cloudtrail Ember S3: <code>ams-a {<i>account_ID</i> } -log-manajemen- {<i>region</i>}</code>
3	Amazon CloudFront (CloudFront)	Pencatatan permintaan pengguna. Anda harus secara eksplisit mengaktifkan CloudFront logging. Untuk informasi, lihat Mengaktifkan pencatatan untuk layanan yang didukung	Ember S3: <code>ams-a {<i>account_ID</i> } -log-manajemen- {<i>region</i>}</code> Jalur: <code>AWS/RedShift/{<i>CloudFront_distribution_ID</i>}</code>
4	Amazon CloudWatch (CloudWatch)	Hanya pencatatan panggilan API.	CloudWatch LogGroup: /aws/ams/cloudtrail
5	Amazon Elastic Block Store (EBS)	Tidak ada log yang diproduksi oleh layanan EBS.	Tidak berlaku
6	Amazon Elastic Compute Cloud (EC2)	Log sistem dan aplikasi. Untuk informasi, lihat Amazon Elastic Compute Cloud (Amazon EC2) - log tingkat sistem .	CloudWatch Log: <code>{<i>instance_ID</i>}</code>

	Nama layanan	Rincian log	Log lokasi
7	Amazon Elastic File System (Amazon EFS)	Hanya pencatatan panggilan API.	CloudWatch LogGroup: /aws/ams/cloudtrail
8	Elastic Load Balancing (ELB)	Akses dan entri log kesalahan. Penyeimbang beban elastis mencatat semua permintaan yang dikirim ke mereka, termasuk permintaan yang tidak dirutekan ke instance back-end. Misalnya, jika klien mengirim permintaan yang salah bentuk, atau tidak ada contoh yang sehat untuk merespons, permintaan tersebut masih dicatat. Untuk informasi selengkapnya tentang entri log penyeimbang beban elastis, lihat • Classic Load Balancers: Akses entri log. • Application Load Balancers: Akses entri log. • Network Load Balancers: Akses entri log.	CloudWatch LogGroup: /aws/ams/cloudtrail Ember S3: mc-a {<i>account_ID</i>} - log- {} <i>region</i> Jalur: aws/elbaccess
9	OpenSearch Layanan Amazon (OpenSearch Layanan)	Log kesalahan layanan. Anda harus secara eksplisit mengaktifkan OpenSearch logging. Untuk informasi, lihat Mengaktifkan pencatatan untuk layanan yang didukung	CloudWatch LogGroup: /aws/ams/cloudtrail

	Nama layanan	Rincian log	Log lokasi
10	Amazon ElastiCache	Hanya pencatatan panggilan API.	CloudWatch LogGroup: /aws/ams/cloudtrail
11	Amazon GuardDuty		
12	Amazon Inspector		
13	Amazon Macie		
14	Amazon Redshift	Koneksi, pengguna, dan log aktivitas. Logging diaktifkan secara default saat Anda membuat kluster Redshift Anda dengan menjalankan Create Redshift cluster CT (ct-1malj7snzxrkr). Untuk selengkapnya, lihat Pencatatan Audit Database.	Ember S3: ams-a {<i>account_ID</i>} -log-manajemen- {<i>region</i>} Jalur: /AWS//{<i>RedShift CloudFront_Distribution_ID</i>}
15	Amazon Relational Database Service (RDS)	Log khusus untuk tipe database. Pencatatan RDS harus diaktifkan secara eksplisit. Untuk informasi, lihat Mengaktifkan pencatatan untuk layanan yang didukung Anda hanya dapat mengakses log MSSQL melalui prosedur tersimpan; untuk informasi, lihat Mengarsipkan File Log.	CloudWatch LogGroup: /aws/rds/(instance cluster)/{nama database}/{nama log}

	Nama layanan	Rincian log	Log lokasi
16	Amazon S3 (S3)	Log akses bucket. Setiap catatan log akses memberikan detail tentang permintaan akses tunggal, seperti: pemohon, nama keranjang, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan (jika ada). Informasi log akses dapat berguna dalam audit keamanan dan akses; ini juga dapat membantu Anda mempelajari tentang basis pelanggan Anda dan memahami tagihan Amazon S3 Anda. Untuk informasi selengkapnya tentang entri Log Akses S3, lihat Format Log Akses Server S3.	Ember S3: mc-a {<i>account_ID</i>} - log-manajemen- {} <i>region</i> Jalur: /aws/s3access/ {} <i>bucket_name</i>
17	Amazon Simple Email Service (SES)	Panggilan layanan API SES.	CloudWatch LogGroup: /aws/ams/cloudtrail Ember S3: ams-a {<i>account_ID</i>} -log-manajemen- {} <i>region</i> Jalur: AWS/CloudTrail/AWSLogs/{<i>account_ID</i>}/CloudTrail/{<i>region</i>}
18	Amazon Virtual Private Cloud (Amazon VPC)	Data aliran VPC (informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan VPC Anda).	CloudWatch LogGroup: /aws/vpcflow/ {vpc_id}
19	Auto Scaling	Hanya pencatatan panggilan API.	CloudWatch LogGroup: /aws/ams/cloudtrail

	Nama layanan	Rincian log	Log lokasi
20	AWS Certificate Manager		
21	AWS CodeDeploy	Log penerapan khusus instance.	Pada contoh
22	AWS Config	Panggilan layanan AWS Config API.	CloudWatch LogGroup: /aws/ams/cloudtrail Ember S3: ams-a { <i>account_ID</i> } -log-manajemen- { <i>region</i> } Jalur:AWS/CloudTrail/AWSLogs/{ <i>account_ID</i> }/CloudTrail/{ <i>region</i> }
23	AWS Database Migration Service	Log migrasi basis data. Untuk selengkapnya, lihat Memperkenalkan manajemen log di AWS Database Migration Service .	Konsol migrasi basis data
24	AWS Direct Connect (DX)	Hanya pencatatan panggilan API.	CloudWatch LogGroup: /aws/ams/cloudtrail
25	AWS Glacier		
26	AWS IAM (SAYA)		
27	AWS Key Management Service		

	Nama layanan	Rincian log	Log lokasi
28	AWS Management Console (konsol atau AWS Console)		
29	AWS Simple Notification Service (SNS)		
30	Layanan Antrian Sederhana AWS (SQS)		

Log layanan bersama AMS

Tabel berikut menjelaskan log, dan lokasi log, untuk Layanan Bersama AMS di akun Anda.

Untuk mengakses log Anda, pastikan bahwa Anda memiliki salah satu peran IAM yang diperlukan dan berada di akun AMS Anda. Kemudian navigasikan ke direktori yang ditampilkan.

AMS single-account landing zone Layanan Bersama Logging

	Nama layanan bersama	Rincian log	Log lokasi
1	Tuan Rumah Bastion	Informasi mengenai pengguna yang mengakses host bastion.	Benteng Linux: CloudWatch Log: <code>{instance id}/var/log/secure</code> CloudWatch Log: <code>{instance id}/var/log/audit/audit.log</code> Benteng Windows:

	Nama layanan bersama	Rincian log	Log lokasi
			CloudWatch Log:/{instance id}/SecurityEventLog
2	Host Manajemen	Output skrip, yang membantu dalam tindakan manajemen akses otomatis dalam akun.	CloudWatch Log:/{instance id}/ApplicationEventLog
4	Host EPS (DSM)	Informasi mengenai pendaftaran instance ke platform Deep Security Management.	CloudWatch Log:/{instance id}/var/log/DSM.log
5	Directory Service	Informasi mengenai login akun, manajemen akun, pelacakan terperinci, akses objek, perubahan kebijakan, dan penggunaan hak istimewa dalam direktori akun. Anda harus secara eksplisit mengaktifkan pencatatan Layanan Direktori. Untuk informasi, lihat Mengaktifkan pencatatan untuk layanan yang didukung.	CloudWatch Log: /aws/directoryservice/ {direktori id} - {direktori nama dns}
6	Lambda	Output dari berbagai lambda, yang membantu dalam tindakan operasional otomatis dalam akun.	CloudWatch Log: /aws/lambda/{nama lambda}

AMS multi-account landing zone Layanan Bersama Logging

	Nama layanan bersama	Rincian log	Log lokasi
1	Benteng	Output dari login instans dan kegagalan otentikasi.	CloudWatch Log Benteng Linux: / <i>{instance_ID}</i> /var/log/secure.log CloudWatch Log Benteng Windows: / <i>{instance_ID}</i> /SecurityEventLog
2	Host Manajemen	Output dari scriptsy, yang membantu dalam tindakan manajemen akses otomatis dalam akun.	CloudWatch Log: / <i>{instance_ID}</i> / ApplicationEventLog
3	Host EPS (DSM)	Informasi mengenai pendaftaran instance ke platform Deep Security Management.	CloudWatch Log: / <i>{instance_ID}</i> / var/log/DSM.log
4	Directory Service	Informasi mengenai login akun, manajemen akun, pelacakan terperinci, akses objek, perubahan kebijakan, dan penggunaan hak istimewa dalam direktori akun. Anda harus secara eksplisit mengaktifkan pencatatan Layanan Direktori. Untuk informasi, lihat Mengaktifkan pencatatan untuk layanan yang didukung .	CloudWatch Log: /aws/directoryservice/ {} - {} <i>directory_ID</i> <i>directory_DNS_name</i>
5	Lambda	Output dari berbagai lambda, yang membantu dalam	CloudWatch Log: /aws/lambda/ {} <i>Lambda_name</i>

	Nama layanan bersama	Rincian log	Log lokasi
		tindakan operasional otomatis dalam akun.	

Amazon Elastic Compute Cloud (Amazon EC2) - log tingkat sistem

Log instance dikumpulkan oleh agen CloudWatch Log yang berjalan pada instance dan dapat diakses melalui grup CloudWatch Log dengan nama yang sama dengan instance. Misalnya, jika ID instance adalah i-0123456789abcdef0 dan nama file log adalah `/var/log/messages`, the Log Group would be i-0123456789abcdef0 and the Log Stream `/var/log/messages`

Lihat juga [Log layanan agregat AMS](#).

Untuk mengakses log Anda, pastikan bahwa Anda memiliki salah satu peran IAM yang diperlukan dan berada di akun AMS Anda. Kemudian navigasikan ke direktori yang ditampilkan.

Note

Log berikut dikumpulkan secara default.

Amazon Linux/Red Hat Linux/Centos Linux/Ubuntu/SUSE Linux

Berkas log/Aliran log

```

/var/log/amazon/ssm/amazon-ssm-agent.log
/var/log/amazon/ssm/errors.log
/var/log/audit/audit.log
/var/log/cloud-init-output.log
/var/log/cfn-init.log
/var/log/cfn-init-cmd.log
/var/log/cloud-init.log (Amazon Linux 1 / Amazon Linux 2 only)
/var/log/cron
/var/log/dnf.log
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler

```

```
/var/log/yum.log  
/var/log/aws/ams/bootstrap.log  
/var/log/aws/ams/build.log  
/var/log/syslog  
/var/log/dpkg.log  
/var/log/auth.log  
/var/log/zypper.log
```

Note

Untuk informasi tentang mengakses log untuk Amazon Linux 2023, lihat [Mengapa direktori /var/log kehilangan log di instans Amazon EC2 Linux 2023 saya?](#)

Windows

Berkas log/Aliran log

```
SecurityEventLog  
SystemEventLog  
AmazonSSMAgentLog  
MicrosoftWindowsAppLockerMSIAndScriptEventLog  
MicrosoftWindowsAppLockerEXEAndDLLEventLog  
AmazonCloudWatchAgentLog  
EC2ConfigServiceEventLog (Windows Server 2012 R2 Only)  
ApplicationEventLog  
AmazonCloudFormationLog  
MicrosoftWindowsGroupPolicyOperationalEventLog  
AmazonSSErrLog
```

Integrasi dengan Splunk

AMS mendukung layanan analisis log pelanggan berbasis AWS Lambda, seperti Splunk.

AMS memanfaatkan Add-on Splunk untuk layanan Web Amazon, yang memungkinkan data AWS dialirkan ke Splunk. Lihat [Persyaratan perangkat keras dan perangkat lunak](#).

Lihat posting blog Splunk ini [Cara melakukan streaming AWS CloudWatch Logs ke Splunk \(Petunjuk: lebih mudah dari yang Anda pikirkan\)](#). Karena streaming CloudWatch log diaktifkan secara default untuk pelanggan AMS, dan AMS mengonfigurasi fungsi AWS Lambda untuk Anda, meskipun Anda

perlu mengonfigurasi input Splunk HTTP Event Collector (HEC) dan mengirimkan permintaan ke AMS untuk fungsionalitas yang ditambahkan.

Berikut adalah bagaimana pengaturan input data mungkin terlihat:

Menyesuaikan konfigurasi log Anda

Anda dapat mengubah penyimpanan data log untuk CloudWatch log, dan Anda dapat mengaktifkan pencatatan untuk layanan AWS tambahan.

Mengubah retensi CloudWatch log

Anda dapat mengubah pengaturan penyimpanan data log untuk CloudWatch log. Secara default, log disimpan tanpa batas waktu dan tidak pernah kedaluwarsa. Anda dapat menyesuaikan kebijakan retensi untuk setiap grup log, menjaga retensi yang tak terbatas, atau memilih periode retensi antara 10 tahun dan satu hari. Untuk melihat periode retensi minimum yang diizinkan di AMS, lihat dokumen Standar Teknis AMS yang tersedia melalui AWS Artifact. Untuk mengakses AWS Artifact, hubungi CSDM Anda untuk mendapatkan petunjuk atau buka [Memulai dengan AWS](#) Artifact.

Fitur penyimpanan CloudWatch log log menghapus peristiwa log dalam aliran berdasarkan kebijakan penyimpanan. Itu tidak menghapus aliran log atau grup log. Untuk informasi umum, lihat Panduan Pengguna Amazon CloudWatch Logs [Apa itu Amazon CloudWatch Logs?](#) .

Untuk informasi tentang menyesuaikan periode penyimpanan log, dan untuk mempelajari lebih lanjut, lihat [Mengubah Penyimpanan Data Log di CloudWatch Log](#).

Mengaktifkan pencatatan untuk layanan yang didukung

Beberapa layanan tidak mengaktifkan logging secara default dan memerlukan pengaktifan eksplisit.

Untuk mengaktifkan pencatatan untuk CloudFront OpenSearch, Amazon RDS dan Route53, kirimkan RFC dengan Manajemen | Lainnya | Lainnya | Buat jenis perubahan (ct-1e1xtak34nx76) dengan nilai berikut, ganti yang sesuai: *variables*

Subject: Enable logging for *SERVICE_NAME*
Description: Service ARN: *SERVICE_ARN*

Manajemen keamanan

Manajemen keamanan AWS Managed Services (AMS) adalah proses dimana AMS mengidentifikasi aset organisasi dan menerapkan kebijakan dan prosedur untuk melindungi aset tersebut.

Note

AMS sekarang memiliki tipe perubahan (CT), Deployment | Komponen tumpukan lanjutan | Sertifikat ACM dengan tambahan SANs | Buat (ct-3l14e139i5p50), yang dapat Anda gunakan untuk mengirimkan permintaan sertifikat. AWS Certificate Manager Untuk informasi, lihat [AWS::CertificateManager::Certificate](#). CT ini menyediakan pembuatan nama alternatif subjek tambahan (SAN).

Untuk lebih memahami AWS keamanan umum, lihat [Praktik Terbaik untuk Keamanan, Identitas, & Kepatuhan](#).

AMS mengkategorikan risiko keamanan sebagai berikut:

- Risiko yang diketahui terdeteksi oleh anti-malware, yang ditangani oleh proses mitigasi malware.
- Peristiwa keamanan termasuk pelanggaran akses, yang ditangani oleh proses manajemen peristiwa keamanan.

Topik

- [Perlindungan data di AMS](#)
- [Manajemen identitas dan akses](#)
- [Respon Insiden Keamanan di AMS](#)
- [Ubah ulasan keamanan permintaan di AMS Advanced](#)

Perlindungan data di AMS

AMS terus memantau akun terkelola Anda dengan memanfaatkan AWS layanan asli seperti Amazon GuardDuty, Amazon Macie (opsional), serta alat dan proses kepemilikan internal lainnya. Setelah alarm dipicu, AMS bertanggung jawab atas triase awal dan respons terhadap alarm. Proses respons kami didasarkan pada standar NIST. AMS secara teratur menguji proses responsnya menggunakan

Simulasi Respons Insiden Keamanan dengan Anda untuk menyelaraskan alur kerja Anda dengan program respons keamanan pelanggan yang ada.

Ketika AMS mendeteksi pelanggaran apa pun, atau ancaman pelanggaran yang akan segera terjadi, AWS atau kebijakan keamanan Anda, kami mengumpulkan informasi, termasuk sumber daya yang terkena dampak dan perubahan terkait konfigurasi apa pun. AMS menyediakan follow-the-sun dukungan 24/7/365 dengan operator khusus yang secara aktif meninjau dan menyelidiki dasbor pemantauan, antrian insiden, dan permintaan layanan di semua akun terkelola Anda. AMS menyelidiki temuan ini dengan pakar keamanan kami untuk menganalisis aktivitas dan memberi tahu Anda melalui kontak eskalasi keamanan yang tercantum di akun Anda.

Berdasarkan temuan kami, AMS terlibat dengan Anda secara proaktif. Jika Anda yakin aktivitas tersebut tidak sah atau mencurigakan, AMS bekerja sama dengan Anda untuk menyelidiki dan memulihkan atau mengatasi masalah tersebut. Ada jenis temuan tertentu yang dihasilkan oleh GuardDuty yang mengharuskan Anda untuk mengkonfirmasi dampak sebelum AMS dapat mengambil tindakan apa pun. Misalnya, jenis GuardDuty temuan `UnauthorizedAccess:IAMUser/ConsoleLogin`, menunjukkan bahwa salah satu pengguna Anda telah masuk dari lokasi yang tidak biasa; AMS memberi tahu Anda dan meminta Anda meninjau temuan tersebut untuk mengonfirmasi apakah perilaku ini sah.

Amazon Macie

AWS Managed Services merekomendasikan agar Anda menggunakan Macie untuk mendeteksi daftar data sensitif yang besar dan komprehensif, seperti informasi kesehatan pribadi (PHI), informasi identitas pribadi (PII), dan data keuangan.

Macie dapat dikonfigurasi untuk berjalan secara berkala di bucket Amazon S3 apa pun, mengotomatiskan evaluasi objek baru atau yang dimodifikasi dalam ember dari waktu ke waktu. Saat temuan keamanan dihasilkan, AMS akan memberi tahu Anda dan bekerja sama dengan Anda untuk memulihkan sesuai kebutuhan.

Untuk informasi lebih lanjut, lihat [Menganalisis temuan Amazon Macie](#).

Keamanan Amazon Macie

Macie adalah layanan keamanan intelligence/AI bertenaga buatan yang membantu Anda mencegah kehilangan data dengan secara otomatis menemukan, mengklasifikasikan, dan melindungi data sensitif yang disimpan di AWS. Macie menggunakan pembelajaran mesin untuk mengenali data sensitif seperti informasi identitas pribadi (PII) atau kekayaan intelektual, memberikan nilai bisnis,

dan memberikan visibilitas ke tempat data ini disimpan dan bagaimana data tersebut digunakan dalam organisasi Anda. Macie terus memantau aktivitas akses data untuk anomali, dan memberikan peringatan ketika mendeteksi risiko akses tidak sah atau kebocoran data yang tidak disengaja. Layanan Macie mendukung Amazon S3 AWS CloudTrail dan sumber data.

AMS terus memantau peringatan dari Macie dan, jika diperingatkan, mengambil tindakan cepat untuk melindungi sumber daya dan akun Anda. Dengan penambahan Macie ke daftar layanan yang didukung AMS, kami juga sekarang bertanggung jawab untuk mengaktifkan dan mengonfigurasi Macie di semua akun Anda, sesuai instruksi Anda. Anda dapat melihat peringatan Macie dan tindakan kami saat terungkap di konsol AWS atau integrasi yang didukung. Selama onboarding akun, Anda dapat menunjukkan akun yang Anda gunakan untuk menyimpan PII. Untuk semua akun baru dengan PII, kami sarankan menggunakan Macie. Untuk akun yang ada dengan PII, hubungi kami dan kami akan menyalakannya di akun Anda. Akibatnya, Anda dapat memiliki lapisan perlindungan tambahan yang tersedia dan menikmati semua manfaat Macie di lingkungan AWS Anda yang dikelola oleh AMS.

AMS Macie FAQs

- Mengapa saya memerlukan Macie ketika semua akun AMS memiliki Trend Micro dan GuardDuty diaktifkan?

Macie membantu Anda melindungi data Anda di Amazon S3 dengan membantu Anda mengklasifikasikan data apa yang Anda miliki, nilai yang dimiliki data untuk bisnis, dan perilaku yang terkait dengan akses ke data tersebut. Amazon GuardDuty memberikan perlindungan luas atas akun AWS, beban kerja, dan data Anda dengan membantu mengidentifikasi ancaman seperti pengintaian aktor ancaman, masalah instans, dan aktivitas akun bermasalah. Kedua layanan tersebut menggabungkan analisis perilaku pengguna, pembelajaran mesin, dan deteksi anomali untuk mendeteksi ancaman dalam kategori masing-masing. Trend Micro tidak fokus pada identifikasi PII dan ancaman dari mereka.

- Bagaimana cara mengaktifkan Macie di akun AMS saya?

Jika Anda telah PII/PHI menyimpan di akun Anda atau berencana untuk menyimpannya, hubungi CSDM Anda atau ajukan permintaan layanan untuk mengaktifkan Macie untuk akun baru atau yang sudah ada yang dikelola oleh AMS.

- Apa implikasi biaya dari mengaktifkan Macie di akun AMS saya?

Harga Macie berfungsi untuk AMS mirip dengan layanan lain seperti Amazon Elastic Compute Cloud (Amazon EC2). Anda membayar Amazon Macie berdasarkan penggunaan dan peningkatan

AMS berdasarkan Anda. SLAs Biaya Macie didasarkan pada penggunaan, lihat Harga [Amazon Macie](#), diukur AWS CloudTrail berdasarkan peristiwa dan penyimpanan Amazon S3. Harap dicatat bahwa biaya Macie cenderung mendatar dari bulan kedua setelah diaktifkan karena dikenakan biaya berdasarkan data tambahan yang ditambahkan ke ember Amazon S3.

Untuk mempelajari lebih lanjut tentang Macie, lihat [Amazon Macie](#).

GuardDuty

GuardDuty adalah layanan pemantauan keamanan berkelanjutan yang menggunakan umpan intelijen ancaman, seperti daftar alamat IP dan domain berbahaya, dan pembelajaran mesin untuk mengidentifikasi aktivitas yang tidak terduga dan berpotensi tidak sah dan berbahaya dalam lingkungan AWS Anda. Ini dapat mencakup masalah seperti eskalasi hak istimewa, penggunaan kredensial yang terbuka, atau komunikasi dengan alamat IP berbahaya, atau domain. GuardDuty juga memantau perilaku akses akun Amazon Web Services untuk tanda-tanda kompromi, seperti penerapan infrastruktur yang tidak sah, seperti instance yang digunakan di Wilayah yang belum pernah digunakan, atau panggilan API yang tidak biasa, seperti perubahan kebijakan kata sandi untuk mengurangi kekuatan kata sandi. Untuk informasi lebih lanjut, lihat [Panduan GuardDuty Pengguna](#).

Untuk melihat dan menganalisis GuardDuty temuan Anda, gunakan prosedur berikut.

1. Buka [konsol GuardDuty](#).
2. Pilih Temuan, lalu pilih temuan tertentu untuk melihat detail. Detail untuk setiap temuan berbeda tergantung pada jenis temuan, sumber daya yang terlibat, dan sifat aktivitas.

Untuk informasi selengkapnya tentang bidang pencarian yang tersedia, lihat [detail GuardDuty pencarian](#).

GuardDuty keamanan

Amazon GuardDuty menawarkan deteksi ancaman yang memungkinkan Anda untuk terus memantau dan melindungi akun dan beban kerja AWS Anda. Amazon GuardDuty menganalisis aliran meta-data berkelanjutan yang dihasilkan dari akun Anda dan aktivitas jaringan yang ditemukan di Peristiwa, log aliran VPC AWS CloudTrail Amazon, dan log Sistem Nama Domain (DNS). Ini juga menggunakan intelijen ancaman terintegrasi seperti alamat IP berbahaya yang diketahui, deteksi anomali, dan pembelajaran mesin untuk mengidentifikasi ancaman secara lebih akurat. GuardDuty adalah layanan

AMS yang dipantau. Untuk mempelajari lebih lanjut tentang GuardDuty pemantauan Amazon, lihat [GuardDuty pemantauan](#). Untuk mempelajari selengkapnya GuardDuty, lihat [Amazon GuardDuty](#).

Semua akun AMS baru telah GuardDuty diaktifkan secara default. AMS mengonfigurasi GuardDuty selama onboarding akun. Anda dapat mengirimkan permintaan perubahan untuk mengubah pengaturan kapan saja. GuardDuty harga bekerja untuk AMS mirip dengan layanan lain seperti Amazon Elastic Compute Cloud (Amazon EC2). Anda membayar GuardDuty berdasarkan penggunaan dan peningkatan AMS berdasarkan Anda SLAs. GuardDuty biaya didasarkan pada penggunaan ([GuardDuty Harga Amazon](#)), diukur berdasarkan AWS CloudTrail peristiwa dan volume log Aliran VPC Amazon Anda.

Untuk GuardDuty di AMS, kategori deteksi utama berikut diaktifkan:

- Pengintaian - Aktivitas yang menyarankan pengintaian oleh aktor ancaman, seperti aktivitas API yang tidak biasa, pemindaian port intra-VPC, pola permintaan login gagal yang tidak biasa, atau pemeriksaan port yang tidak diblokir dari IP buruk yang diketahui.
- Masalah instans - Aktivitas instance yang bermasalah, seperti penambangan cryptocurrency, malware menggunakan algoritma pembuatan domain (DGA), aktivitas penolakan layanan keluar, volume lalu lintas jaringan yang luar biasa tinggi, protokol jaringan yang tidak biasa, komunikasi instance keluar dengan IP berbahaya yang diketahui, EC2 kredensi Amazon sementara yang digunakan oleh alamat IP eksternal, dan eksfiltrasi data menggunakan DNS.
- Aktivitas akun - Pola umum yang menunjukkan aktivitas akun termasuk panggilan API dari geolokasi yang tidak biasa atau proxy anonim, upaya untuk menonaktifkan AWS CloudTrail pencatatan, peluncuran instance atau infrastruktur yang tidak biasa, penerapan infrastruktur di Wilayah AWS yang tidak biasa, dan panggilan API dari alamat IP berbahaya yang diketahui.

AMS menggunakan GuardDuty akun terkelola Anda untuk terus memantau temuan dan peringatan dari GuardDuty dan, jika diperingatkan, operasi AMS mengambil tindakan proaktif untuk melindungi sumber daya dan akun Anda. Anda dapat melihat GuardDuty temuan dan tindakan kami saat terungkap di konsol AWS atau integrasi yang didukung.

GuardDuty bekerja dengan Trend Micro Deep Security Manager di akun Anda. Trend Micro Deep Security Manager menyediakan layanan Deteksi Intrusi/Pencegahan Intrusi berbasis host. Layanan Trend Micro Web Reputation memiliki beberapa tumpang tindih dengan GuardDuty kemampuan untuk mendeteksi ketika host mencoba berkomunikasi dengan host atau layanan web yang dikenal sebagai ancaman. Namun, GuardDuty menyediakan kategori deteksi ancaman tambahan dan menyelesaikannya dengan memantau lalu lintas jaringan, metode yang melengkapi deteksi berbasis

host Trend Micro. Deteksi ancaman berbasis jaringan memungkinkan peningkatan keamanan dengan tidak membiarkan kontrol gagal jika host telah menunjukkan perilaku bermasalah. AMS merekomendasikan penggunaan GuardDuty di semua akun AMS Anda.

Untuk mempelajari lebih lanjut tentang Trend Micro, lihat [Pusat Bantuan Trend Micro Deep Security](#); perhatikan bahwa tautan non-Amazon dapat berubah tanpa pemberitahuan kepada kami.

GuardDuty pemantauan

GuardDuty memberi tahu Anda tentang status lingkungan AWS Anda dengan menghasilkan [temuan keamanan](#) yang ditangkap dan dapat diwaspadai oleh AMS.

Amazon GuardDuty memantau keamanan lingkungan AWS Anda dengan menganalisis dan memproses log aliran VPC, log AWS CloudTrail peristiwa, dan log Sistem Nama Domain. Anda dapat memperluas cakupan pemantauan ini dengan mengonfigurasi GuardDuty untuk juga menggunakan daftar IP kustom, tepercaya, dan daftar ancaman Anda sendiri.

- Daftar IP tepercaya terdiri dari alamat IP yang Anda izinkan untuk komunikasi aman dengan infrastruktur dan aplikasi AWS Anda. GuardDuty tidak menghasilkan temuan untuk alamat IP pada daftar IP tepercaya. Pada waktu tertentu, Anda hanya dapat memiliki satu daftar IP tepercaya yang diunggah per akun AWS per wilayah.
- Daftar ancaman terdiri dari alamat IP berbahaya yang diketahui. GuardDuty menghasilkan temuan berdasarkan daftar ancaman. Pada waktu tertentu, Anda dapat memiliki hingga enam daftar ancaman yang diunggah per akun AWS per wilayah.

Untuk mengimplementasikan GuardDuty, gunakan AMS CT Deployment | Monitoring dan notifikasi | GuardDuty IP set | Create (ct-08avsj2e9mc7g) untuk membuat satu set alamat IP yang disetujui. Anda juga dapat menggunakan Penerapan AMS CT | Pemantauan dan pemberitahuan | GuardDuty ancaman intel set | Buat (ct-25v6r7t8gvkq5) untuk membuat satu set alamat IP yang ditolak.

Untuk daftar layanan yang dipantau AMS, lihat [Apa yang dipantau oleh sistem pemantauan AMS?](#).

Amazon Route 53 Resolver DNS Firewall

Amazon Route 53 Resolver merespons secara rekursif kueri DNS dari sumber daya AWS untuk catatan publik, nama DNS khusus Amazon VPC, dan zona host pribadi Amazon Route 53, dan tersedia secara default di semua VPCs. Dengan Route 53 Resolver DNS Firewall, Anda dapat memfilter dan mengatur lalu lintas DNS keluar untuk virtual private cloud (VPC) Anda. Untuk melakukannya, Anda membuat kumpulan aturan pemfilteran yang dapat digunakan kembali di grup

aturan DNS Firewall, mengasosiasikan grup aturan ke VPC Anda, lalu memantau aktivitas di log dan metrik DNS Firewall. Berdasarkan aktivitas, Anda dapat menyesuaikan perilaku DNS Firewall. Untuk informasi selengkapnya, lihat [Menggunakan DNS Firewall untuk memfilter lalu lintas DNS keluar](#).

Untuk melihat dan mengelola konfigurasi Route 53 Resolver DNS Firewall Anda, gunakan prosedur berikut:

1. Masuk ke AWS Management Console dan buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di bawah DNS Firewall, pilih Grup aturan.
3. Tinjau, edit, atau hapus konfigurasi yang ada, atau buat grup aturan baru. Untuk informasi selengkapnya, lihat [Cara kerja Route 53 Resolver DNS Firewall](#).

Amazon Route 53 Resolver DNS Firewall pemantauan dan keamanan

Amazon Route 53 DNS Firewall menggunakan konsep asosiasi aturan, tindakan aturan, dan prioritas evaluasi aturan. Daftar domain adalah seperangkat spesifikasi domain yang dapat digunakan kembali yang Anda gunakan dalam aturan DNS Firewall, di dalam grup aturan. Ketika Anda mengasosiasikan grup aturan dengan VPC, DNS Firewall membandingkan kueri DNS Anda terhadap daftar domain yang digunakan dalam aturan. Jika DNS Firewall menemukan kecocokan, maka ia menangani kueri DNS sesuai dengan tindakan aturan yang cocok. Untuk informasi selengkapnya tentang grup aturan dan aturan, lihat [Grup dan aturan DNS Firewall](#).

Daftar domain dibagi dalam dua kategori utama:

- Daftar domain terkelola, yang AWS membuat dan memelihara untuk Anda.
- Daftar domain Anda sendiri, yang Anda buat dan pelihara.

Kelompok aturan dievaluasi berdasarkan indeks prioritas asosiasi mereka.

Secara default, AMS menerapkan konfigurasi dasar yang terdiri dari aturan dan grup aturan berikut:

- Satu kelompok aturan bernama `DefaultSecurityMonitoringRule`. Grup aturan memiliki prioritas asosiasi tertinggi yang tersedia pada saat pembuatan untuk setiap VPC yang ada di setiap wilayah AWS
- Satu aturan bernama `DefaultSecurityMonitoringRule` dengan prioritas 1 dalam grup `DefaultSecurityMonitoringRule` aturan, menggunakan daftar Domain `AWSTManagedDomainsAggregateThreatList` Terkelola dengan tindakan ALERT.

Jika Anda memiliki konfigurasi yang ada, konfigurasi dasar diterapkan dengan prioritas lebih rendah daripada konfigurasi yang ada. Konfigurasi Anda yang ada adalah default. Anda menggunakan konfigurasi dasar AMS sebagai tangkapan semua jika konfigurasi yang ada tidak memberikan instruksi prioritas yang lebih tinggi tentang cara menangani resolusi kueri. Untuk mengubah atau menghapus konfigurasi dasar, lakukan salah satu hal berikut:

- Hubungi Cloud Service Delivery Manager (CSDM) atau Cloud Architect (CA) Anda.
- Buat Permintaan Perubahan (RFC) menggunakan [Manajemen | Lainnya | Lainnya | Buat CT \(ct-1e1xtak34nx76\)](#).
- Buat permintaan layanan.

Jika akun Anda dioperasikan dalam mode Pengembang atau mode Perubahan Langsung, Anda dapat melakukan perubahan sendiri.

AWS Certificate Manager Sertifikat (ACM)

AMS memiliki CT, Deployment | Komponen tumpukan lanjutan | Sertifikat ACM dengan tambahan SANs | Buat (ct-3l14e139i5p50), yang dapat Anda gunakan untuk mengirimkan permintaan sertifikat AWS Certificate Manager, dengan hingga lima nama alternatif Subjek tambahan (SAN) (seperti example.com, example.net, dan example.org). Untuk detailnya, lihat [Apa Itu AWS Certificate Manager?](#) dan [Karakteristik Sertifikat ACM](#).

Note

Pengaturan batas waktu ini bukan hanya tentang proses, tetapi juga validasi sertifikat ACM Anda melalui validasi email. Tanpa validasi Anda, RFC gagal.

Enkripsi data di AMS

AMS menggunakan beberapa AWS layanan untuk enkripsi data, terutama Amazon Simple Storage Service, AWS Key Management Service (AWS KMS), Amazon Elastic Block Store, Amazon Relational Database Service Amazon Redshift,,, Amazon ElastiCache AWS Lambda, dan Amazon OpenSearch Service.

Amazon S3

Amazon S3 menawarkan beberapa opsi enkripsi objek yang melindungi data bergerak dan data diam. Enkripsi di sisi server mengenkripsi objek Anda sebelum menyimpannya ke dalam disk di pusat datanya lalu mendekripsinya saat Anda mengunduh objek. Selama Anda mengautentikasi permintaan dan telah memiliki izin akses, tidak ada perbedaan dalam cara mengakses objek terenkripsi atau tidak terenkripsi. Untuk informasi selengkapnya, lihat [Perlindungan data di Amazon S3](#).

Amazon EBS

Dengan enkripsi Amazon EBS, Anda tidak perlu membangun, memelihara, dan mengamankan infrastruktur manajemen kunci Anda sendiri. Enkripsi Amazon EBS menggunakan AWS KMS kunci saat membuat volume dan snapshot terenkripsi. Operasi enkripsi terjadi pada server yang meng-host EC2 instans Amazon. Ini dilakukan untuk memastikan bahwa keduanya data-at-rest dan data-in-transit antara instance dan penyimpanan Amazon EBS terlampir aman. Anda dapat melampirkan volume terenkripsi maupun tak terenkripsi ke suatu instans secara bersamaan. Untuk informasi lebih lanjut, lihat [Enkripsi Amazon EBS](#).

Amazon RDS

Amazon RDS dapat mengenkripsi instans Amazon RDS DB Anda. Data yang dienkripsi saat istirahat mencakup penyimpanan yang mendasari untuk instans DB, pencadangan otomatisnya, replika baca, dan snapshot. Instans DB terenkripsi Amazon RDS menggunakan algoritme enkripsi AES-256 standar industri untuk mengenkripsi data Anda di server yang menghosting instans Amazon RDS DB Anda. Setelah data Anda dienkripsi, Amazon RDS menangani otentikasi akses dan dekripsi data Anda secara transparan dengan dampak minimal pada kinerja. Anda tidak perlu memodifikasi aplikasi klien basis data untuk menggunakan enkripsi. Untuk informasi selengkapnya, lihat [Mengekripsi sumber daya Amazon RDS](#).

Amazon Simple Queue Service

Selain opsi enkripsi sisi server (SSE) terkelola Amazon SQS default, Amazon SQS-managed SSE (SSE-SQS) memungkinkan Anda membuat enkripsi sisi server terkelola khusus yang menggunakan kunci enkripsi yang dikelola Amazon SQS untuk melindungi data sensitif yang dikirim melalui antrian pesan. Enkripsi sisi server (SSE) memungkinkan Anda mengirimkan data sensitif dalam antrian terenkripsi. SSE melindungi konten pesan dalam antrian menggunakan kunci enkripsi terkelola Amazon SQS (SSE-SQS) atau kunci yang dikelola di (SSE-KMS). AWS KMS Untuk informasi tentang mengelola SSE menggunakan AWS Management Console, lihat [Enkripsi saat istirahat](#).

Enkripsi data saat istirahat

OpenSearch Domain layanan menawarkan enkripsi data saat istirahat, fitur keamanan yang membantu mencegah akses tidak sah ke data Anda. Fitur ini menggunakan AWS Key Management Service (AWS KMS) untuk menyimpan dan mengelola kunci enkripsi Anda dan algoritma Advanced Encryption Standard dengan kunci 256-bit (AES-256) untuk melakukan enkripsi. Untuk informasi selengkapnya, lihat [Enkripsi Data saat Istirahat untuk OpenSearch Layanan Amazon](#).

Manajemen kunci

AWS KMS adalah layanan terkelola yang memudahkan Anda membuat dan mengontrol kunci master pelanggan (CMKs), kunci enkripsi yang digunakan untuk mengenkripsi data Anda. AWS KMS CMKs dilindungi oleh modul keamanan perangkat keras (HSMs) yang divalidasi oleh Program Validasi Modul Kriptografi FIPS 140-2 kecuali di Wilayah China (Beijing) dan China (Ningxia). Untuk informasi selengkapnya, lihat [Apa itu AWS Key Management Service?](#)

Manajemen identitas dan akses

AWS Identity and Access Management (IAM) adalah layanan web yang membantu Anda mengontrol akses ke AWS sumber daya dengan aman. Anda menggunakan IAM untuk mengontrol siapa yang diautentikasi (masuk) dan diotorisasi (memiliki izin) untuk menggunakan sumber daya. Selama onboarding AMS, Anda bertanggung jawab untuk membuat peran Admin IAM lintas akun dalam setiap akun terkelola Anda.

Pengamanan IAM Zona Pendaratan Multi-Akun (MALZ)

AMS multi-account landing zone (MALZ) memerlukan kepercayaan Active Directory (AD) sebagai tujuan desain utama manajemen akses AMS untuk memungkinkan setiap organisasi (baik AMS, dan pelanggan) mengelola siklus hidup identitas mereka sendiri. Ini menghindari kebutuhan untuk memiliki kredensial di direktori satu sama lain. Kepercayaan satu arah dikonfigurasi, sehingga Direktori Aktif Terkelola dalam Akun AWS mempercayai AD yang dimiliki atau dikelola pelanggan untuk mengautentikasi pengguna. Karena kepercayaan hanya satu arah, itu tidak berarti bahwa Managed AD dipercaya oleh Customer Active Directory.

Dalam konfigurasi ini, direktori pelanggan yang mengelola identitas pengguna dikenal sebagai Hutan Pengguna, dan AD Terkelola tempat EC2 instans Amazon dilampirkan dikenal sebagai Hutan Sumber Daya. Ini adalah pola desain Microsoft yang umum dimanfaatkan untuk otentikasi Windows; untuk informasi selengkapnya, [lihat](#) Model Desain Hutan.

Model ini memungkinkan kedua organisasi untuk mengotomatiskan siklus hidup masing-masing dan memungkinkan AMS dan Anda mencabut akses dengan cepat jika seorang karyawan meninggalkan

organisasi. Tanpa model ini, jika kedua organisasi menggunakan direktori umum (atau dibuat users/groups di direktori satu sama lain), maka kedua organisasi harus memasukkan alur kerja tambahan, dan sinkronisasi pengguna, untuk memperhitungkan karyawan yang memulai dan meninggalkan. Ini menimbulkan risiko karena proses itu memiliki latensi dan dapat rawan kesalahan.

Prasyarat akses MALZ

Integrasi Penyedia Identitas MALZ untuk akses ke konsol AWS/AMS, CLI, SDK.

Kepercayaan satu arah untuk EC2 instans Amazon di akun AMS Anda.

Mengautentikasi dengan identitas

AMS menggunakan peran IAM, yang merupakan jenis identitas IAM. Peran IAM sangat mirip dengan pengguna, karena itu adalah identitas dengan kebijakan izin yang menentukan apa yang dapat dan tidak dapat dilakukan identitas. AWS Namun, peran tidak memiliki kredensi yang terkait dengannya dan, alih-alih dikaitkan secara unik dengan satu orang, peran dimaksudkan untuk diasumsikan oleh siapa saja yang membutuhkannya. Seorang pengguna IAM dapat mengambil peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.

Peran akses dikendalikan oleh keanggotaan kelompok internal, yang dikelola dan ditinjau secara berkala oleh Manajemen Operasi.

Peran pengguna IAM di AMS

Peran IAM mirip dengan pengguna IAM, karena itu adalah AWS identitas dengan kebijakan izin yang menentukan apa yang dapat dan tidak dapat dilakukan identitas. AWS Namun, alih-alih secara unik terkait dengan satu orang, peran dimaksudkan untuk menjadi dapat diambil oleh siapa pun yang membutuhkannya.

Saat ini ada satu peran pengguna default `AMSCustomer_ReadOnly_Role`, untuk akun AMS standar dan peran tambahan, `customer_managed_ad_user_role` untuk akun AMS dengan Direktori Aktif Terkelola.

Kebijakan peran menetapkan izin untuk CloudWatch dan tindakan log Amazon S3, akses konsol AMS, pembatasan hanya-baca pada Layanan AWS sebagian besar, akses terbatas ke konsol S3 akun, dan akses tipe perubahan AMS.

Selain itu, `Customer_ReadOnly_Role` memiliki izin instans cadangan mutatif yang memungkinkan Anda untuk memesan instance. Ini memiliki beberapa nilai penghematan biaya, jadi, jika Anda tahu bahwa Anda akan memerlukan sejumlah EC2 instans Amazon untuk jangka waktu yang lama, Anda dapat memanggilnya. APIs Untuk mempelajari lebih lanjut, lihat [Instans EC2 Cadangan Amazon](#).

Note

Tujuan tingkat layanan AMS (SLO) untuk membuat kebijakan IAM khusus untuk pengguna IAM adalah empat hari kerja, kecuali kebijakan yang ada akan digunakan kembali. Jika Anda ingin mengubah peran pengguna IAM yang ada, atau menambahkan yang baru, kirimkan [IAM: Update Entity](#) atau [IAM: Create Entity](#) RFC, masing-masing.

Jika Anda tidak terbiasa dengan peran Amazon IAM, lihat Peran [IAM untuk informasi penting](#).

Zona Pendaratan Multi-Akun (MALZ): Untuk melihat kebijakan peran pengguna default, tanpa penyesuaian, zona pendaratan multi-akun AMS, lihat, selanjutnya. [MALZ: Peran Pengguna IAM Default](#)

MALZ: Peran Pengguna IAM Default

Pernyataan kebijakan JSON untuk peran pengguna landing zone multi-akun AMS multi-akun default.

Note

Peran pengguna dapat disesuaikan dan mungkin berbeda berdasarkan per akun. Petunjuk untuk menemukan peran Anda disediakan.

Ini adalah contoh peran pengguna MALZ default. Untuk memastikan bahwa Anda memiliki kebijakan yang ditetapkan yang Anda butuhkan, jalankan perintah AWS [get-role](#) atau masuk ke AWS Management -> [konsol IAM](#) dan pilih Peran di panel navigasi.

Peran akun inti OU

Akun inti adalah akun infrastruktur yang dikelola Malz. Akun inti zona pendaratan multi-akun AMS mencakup akun manajemen dan akun jaringan.

Akun Core OU: Peran dan kebijakan umum

Peran	Kebijakan atau kebijakan
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (Kebijakan Terkelola AWS Publik).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSsupportAkses (Kebijakan Terkelola AWS Publik).
AWSManagedServicesChangeManagementRole (Versi akun inti)	ReadOnlyAccess
	AWSsupportAkses
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

Akun Core OU: Peran dan kebijakan akun manajemen

Peran	Kebijakan atau kebijakan
AWSManagedServicesBillingRole	AMSBillingKebijakan (AMSBillingKebijakan).
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (Kebijakan Terkelola AWS Publik).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSsupportAkses (Kebijakan Terkelola AWS Publik).
AWSManagedServicesChangeManagementRole (Versi akun manajemen)	ReadOnlyAccess
	AWSsupportAkses
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

Peran	Kebijakan atau kebijakan
	<u>AMSMasterAccountSpecificChangeManagementInfrastructurePolicy</u>

Akun Core OU: Peran dan kebijakan akun jaringan

Peran	Kebijakan atau kebijakan
AWSManagedServicesReadOnlyRole	<u>ReadOnlyAccess</u> (Kebijakan Terkelola AWS Publik).
AWSManagedServicesCaseRole	<u>ReadOnlyAccess</u> <u>AWSSupportAkses</u> (Kebijakan Terkelola AWS Publik).
AWSManagedServicesChangeManagementRole (Versi akun jaringan)	<u>ReadOnlyAccess</u> <u>AWSSupportAkses</u> <u>AMSChangeManagementReadOnlyPolicy</u> <u>AMSChangeManagementInfrastructurePolicy</u> <u>AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy</u>

Peran Akun Aplikasi

Peran akun aplikasi diterapkan ke akun khusus aplikasi Anda.

Akun aplikasi: Peran dan kebijakan

Peran	Kebijakan atau kebijakan
AWSManagedServicesReadOnlyRole	<u>ReadOnlyAccess</u> (Kebijakan Terkelola AWS Publik).

Peran	Kebijakan atau kebijakan
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupportAkses (Kebijakan Terkelola AWS Publik). Kebijakan ini menyediakan akses ke semua operasi dan sumber daya pendukung. Untuk selengkapnya, lihat Memulai dengan AWS Support.
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess AWSSupportContoh Akses Kebijakan ini menyediakan akses ke semua operasi dan sumber daya pendukung. AWSCertificateManagerFullAccess informasi, (Kebijakan Terkelola AWS Publik) AWSWAFFullAccess informasi, (Kebijakan Terkelola AWS Publik). Kebijakan ini memberikan akses penuh ke sumber daya AWS WAF. AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole (Versi akun aplikasi)	ReadOnlyAccess AWSSupportAkses (Kebijakan Terkelola AWS Publik). Kebijakan ini menyediakan akses ke semua operasi dan sumber daya pendukung. Untuk selengkapnya, lihat Memulai dengan AWS Support.

Peran	Kebijakan atau kebijakan
AWSManagedServicesAdminRole	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AMSReservedInstancesPolicy
	AMSS3Kebijakan
	ReadOnlyAccess
	AWSSupportAkses
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFullAkses
	AMSS3Kebijakan
	AMSReservedInstancesPolicy

Contoh Kebijakan

Contoh disediakan untuk sebagian besar kebijakan yang digunakan. Untuk melihat [ReadOnlyAccess](#) kebijakan (yang merupakan halaman selama menyediakan akses hanya-baca ke semua AWS layanan), Anda dapat menggunakan tautan ini, jika Anda memiliki akun AWS aktif: [ReadOnlyAccess](#). Juga, versi kental disertakan di sini.

AMSBillingKebijakan

AMSBillingPolicy

Peran Penagihan baru dapat digunakan oleh departemen akuntansi Anda untuk melihat dan mengubah informasi penagihan atau pengaturan akun di akun Manajemen. Untuk mengakses informasi seperti Kontak Alternatif, melihat penggunaan sumber daya akun, atau menyimpan tab penagihan Anda atau bahkan mengubah metode pembayaran, Anda menggunakan peran ini. Peran baru ini terdiri dari semua izin yang tercantum di halaman web tindakan [AWS Billing IAM](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aws-portal:ViewBilling",
        "aws-portal:ModifyBilling"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToBilling"
    },
    {
      "Action": [
        "aws-portal:ViewAccount",
        "aws-portal:ModifyAccount"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToAccountSettings"
    },
    {
      "Action": [
        "budgets:ViewBudget",
        "budgets:ModifyBudget"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToAccountBudget"
    },
    {
      "Action": [
        "aws-portal:ViewPaymentMethods",
        "aws-portal:ModifyPaymentMethods"
      ]
    }
  ]
}
```

```
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToPaymentMethods"
  },
  {
    "Action": [
      "aws-portal:ViewUsage"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToUsage"
  },
  {
    "Action": [
      "cur:DescribeReportDefinitions",
      "cur:PutReportDefinition",
      "cur>DeleteReportDefinition",
      "cur:ModifyReportDefinition"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToCostAndUsageReport"
  },
  {
    "Action": [
      "pricing:DescribeServices",
      "pricing:GetAttributeValues",
      "pricing:GetProducts"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToPricing"
  },
  {
    "Action": [
      "ce:*",
      "compute-optimizer:*"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToCostExplorerComputeOptimizer"
  },
  {
```



```

        "Action": [
            "purchase-orders:ViewPurchaseOrders",
            "purchase-orders:ModifyPurchaseOrders"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "AllowAccessToPurchaseOrders"
    },
    {
        "Action": [
            "redshift:AcceptReservedNodeExchange",
            "redshift:PurchaseReservedNodeOffering"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "AllowAccessToRedshiftAction"
    },
    {
        "Action": "savingsplans:*",
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "AWSSavingsPlansFullAccess"
    }
]
}

```

AMSCChangeManagementReadOnlyPolicy

AMSCChangeManagementReadOnlyPolicy

Izin untuk melihat semua jenis perubahan AMS, dan riwayat jenis perubahan yang diminta.

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

Izin untuk meminta Deployment | Managed landing zone | Akun manajemen | Buat akun aplikasi (dengan VPC) mengubah jenis.

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

Izin untuk meminta Deployment | Managed landing zone | Akun jaringan | Buat jenis perubahan tabel rute aplikasi.

AMSSharedPolicy

AMSSharedPolicy(unter Management | Lainnya | Lainnya CTs)

Izin untuk meminta Management | Lainnya | Lainnya | Buat, dan Management | Lainnya | Lainnya | Perbarui jenis perubahan.

AMSSecretsManagerSharedPolicy

AMSSecretsManagerSharedPolicy

Izin untuk melihat rahasia yang passwords/hashe dibagikan oleh AMS melalui AWS Secrets Manager (misalnya kata sandi ke infrastruktur untuk audit).

Izin untuk membuat rahasia password/hashe untuk dibagikan dengan AMS. (misalnya, kunci lisensi untuk produk yang perlu digunakan).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowAccessToSharedNameSpaces",
    "Effect": "Allow",
    "Action": "secretsmanager:*",
    "Resource": [
      "arn:aws:secretsmanager::*:secret:ams-shared/*",
      "arn:aws:secretsmanager::*:secret:customer-shared/*"
    ]
  },
  {
    "Sid": "DenyGetSecretOnCustomerNamespace",
    "Effect": "Deny",
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "arn:aws:secretsmanager::*:secret:customer-shared/*"
  },
  {
    "Sid": "AllowReadAccessToAMSNameSpace",
    "Effect": "Deny",
```

```

    "NotAction": [
      "secretsmanager:Describe*",
      "secretsmanager:Get*",
      "secretsmanager:List*"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
]
}

```

AMSCChangeManagementPolicy

AMSCChangeManagementPolicy

Izin untuk meminta dan melihat semua jenis perubahan AMS, dan riwayat jenis perubahan yang diminta.

AMSReservedInstancesPolicy

AMSReservedInstancesPolicy

Izin untuk mengelola instans EC2 cadangan Amazon; untuk informasi harga, lihat Instans [EC2 Cadangan Amazon](#).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowReservedInstancesManagement",
    "Effect": "Allow",
    "Action": [
      "ec2:ModifyReservedInstances",
      "ec2:PurchaseReservedInstancesOffering"
    ],
    "Resource": [
      "*"
    ]
  }]
}

```

AMSS3Kebijakan

AMSS3Policy

Izin untuk membuat dan menghapus file dari bucket Amazon S3 yang ada.

Note

Izin ini tidak memberikan kemampuan untuk membuat bucket S3; yang harus dilakukan dengan Deployment | Komponen tumpukan lanjutan | Penyimpanan S3 | Buat jenis perubahan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

AWSSupportAkses

AWSSupportAccess

Akses penuh ke Dukungan. Untuk selengkapnya, lihat [Memulai dengan Dukungan](#). Untuk informasi Dukungan Premium, lihat [Dukungan](#).

JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [{
  "Effect": "Allow",
  "Action": [
    "support:*"
  ],
  "Resource": "*"
}]
}
```

AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions(Kebijakan yang AWS Dikelola Publik)

Izin untuk berlangganan, berhenti berlangganan, dan melihat AWS Marketplace langganan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "aws-marketplace:ViewSubscriptions",
      "aws-marketplace:Subscribe",
      "aws-marketplace:Unsubscribe"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }]
}
```

AWSCertificateManagerFullAccess

AWSCertificateManagerFullAccess

Akses penuh ke AWS Certificate Manager. Untuk informasi selengkapnya, lihat [AWS Certificate Manager](#).

[AWSCertificateManagerFullAccess](#)informasi, (Kebijakan Terkelola AWS Publik).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "acm:*"
    ],
    "Resource": "*"
  }]
}
```

AWSWAFFullAkses

AWSWAFFullAccess

Akses penuh ke AWS WAF. Untuk informasi selengkapnya, lihat [AWS WAF - Firewall Aplikasi Web](#).

[AWSWAFFullAccess](#) informasi, (Kebijakan yang AWS Dikelola Publik). Kebijakan ini memberikan akses penuh ke AWS WAF sumber daya.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "waf:*",
      "waf-regional:*",
      "elasticloadbalancing:SetWebACL"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }]
}
```

ReadOnlyAccess

ReadOnlyAccess

Akses hanya-baca ke semua AWS layanan dan sumber daya di konsol. AWS Saat AWS meluncurkan layanan baru, AMS memperbarui ReadOnlyAccess kebijakan untuk menambahkan izin hanya-baca untuk layanan baru. Izin yang diperbarui diterapkan pada semua entitas prinsipal yang kebijakannya dilampirkan.

Ini tidak memberikan kemampuan untuk masuk ke EC2 host atau host database.

Jika Anda aktif Akun AWS, maka Anda dapat menggunakan tautan ini [ReadOnlyAccess](#) untuk melihat seluruh ReadOnlyAccess kebijakan. Seluruh ReadOnlyAccess kebijakan sangat panjang karena menyediakan akses hanya-baca ke semua. Layanan AWS Berikut ini adalah kutipan sebagian dari kebijakan tersebut. ReadOnlyAccess

Zona Pendaratan Akun Tunggal (SALZ): Untuk melihat kebijakan peran pengguna default, tidak disesuaikan, zona pendaratan akun tunggal AMS, lihat, selanjutnya. [SALZ: Peran Pengguna IAM Default](#)

SALZ: Peran Pengguna IAM Default

Pernyataan kebijakan JSON untuk peran pengguna landing zone akun tunggal AMS default.

 Note

Peran pengguna default SALZ dapat disesuaikan dan mungkin berbeda berdasarkan per akun. Petunjuk untuk menemukan peran Anda disediakan.

Berikut ini adalah contoh peran pengguna SALZ default. Untuk memastikan bahwa Anda memiliki kebijakan yang ditetapkan untuk Anda, jalankan [get-role](#) perintah. Atau, masuk ke AWS Identity and Access Management konsol di <https://console.aws.amazon.com/iam/>, lalu pilih Peran.

Peran read-only pelanggan adalah kombinasi dari beberapa kebijakan. Rincian peran (JSON) mengikuti.

Kebijakan Audit Managed Services:

Kebijakan IAM ReadOnly Managed Services

Kebijakan Pengguna Managed Services

```
{  
  "Version": "2012-10-17",
```

```
"Statement": [
  {
    "Sid": "AllowCustomerToListTheLogBucketLogs",
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::mc-a*-logs-*"
    ],
    "Condition": {
      "StringLike": {
        "s3:prefix": [
          "aws/*",
          "app/*",
          "encrypted",
          "encrypted/",
          "encrypted/app/*"
        ]
      }
    }
  },
  {
    "Sid": "BasicAccessRequiredByS3Console",
    "Effect": "Allow",
    "Action": [
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation"
    ],
    "Resource": [
      "arn:aws:s3:::*"
    ]
  },
  {
    "Sid": "AllowCustomerToGetLogs",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject*"
    ],
    "Resource": [
      "arn:aws:s3:::mc-a*-logs-*/aws/*",
      "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
    ]
  }
],
```



```

{
  "Sid": "AllowAccessToOtherObjects",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteObject*",
    "s3:Get*",
    "s3:List*",
    "s3:PutObject*"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "AllowCustomerToListTheLogBucketRoot",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket"
  ],
  "Resource": [
    "arn:aws:s3:::mc-a*-logs-*"
  ],
  "Condition": {
    "StringEquals": {
      "s3:prefix": [
        "",
        "/"
      ]
    }
  }
},
{
  "Sid": "AllowCustomerCWLConsole",
  "Effect": "Allow",
  "Action": [
    "logs:DescribeLogStreams",
    "logs:DescribeLogGroups"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:*"
  ]
},
{
  "Sid": "AllowCustomerCWLAccessLogs",

```

```

    "Effect": "Allow",
    "Action": [
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:/infra/*",
        "arn:aws:logs:*:*:log-group:/app/*",
        "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
    ]
},
{
    "Sid": "AWSManagedServicesFullAccess",
    "Effect": "Allow",
    "Action": [
        "amscm:*",
        "amsskms:*"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "ModifyAWSBillingPortal",
    "Effect": "Allow",
    "Action": [
        "aws-portal:Modify*"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "DenyDeleteCWL",
    "Effect": "Deny",
    "Action": [
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:*"
    ]
},

```

```

{
  "Sid": "DenyMCCWL",
  "Effect": "Deny",
  "Action": [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:FilterLogEvents",
    "logs:GetLogEvents",
    "logs:PutLogEvents"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:/mc/*"
  ]
},
{
  "Sid": "DenyS3MCNamespace",
  "Effect": "Deny",
  "Action": [
    "s3:*"
  ],
  "Resource": [
    "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
    "arn:aws:s3:::mc-a*-logs-*/mc/*",
    "arn:aws:s3:::mc-a*-logs-*--audit/*",
    "arn:aws:s3:::mc-a*-internal-*/*",
    "arn:aws:s3:::mc-a*-internal-*"
  ]
},
{
  "Sid": "ExplicitDenyS3CfnBucket",
  "Effect": "Deny",
  "Action": [
    "s3:*"
  ],
  "Resource": [
    "arn:aws:s3:::cf-templates-*"
  ]
},
{
  "Sid": "DenyListBucketS3LogsMC",
  "Action": [
    "s3:ListBucket"
  ],

```

```

    "Effect": "Deny",
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
    ],
    "Condition": {
        "StringLike": {
            "s3:prefix": [
                "auditlog/*",
                "encrypted/mc/*",
                "mc/*"
            ]
        }
    }
},
{
    "Sid": "DenyS3LogsDelete",
    "Effect": "Deny",
    "Action": [
        "s3:Delete*",
        "s3:Put*"
    ],
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/*"
    ]
},
{
    "Sid": "DenyAccessToKmsKeysStartingWithMC",
    "Effect": "Deny",
    "Action": [
        "kms:*"
    ],
    "Resource": [
        "arn:aws:kms::*:key/mc-*",
        "arn:aws:kms::*:alias/mc-*"
    ]
},
{
    "Sid": "DenyListingOfStacksStartingWithMC",
    "Effect": "Deny",
    "Action": [
        "cloudformation:*"
    ],
    "Resource": [
        "arn:aws:cloudformation::*:stack/mc-*"
    ]
}

```

```

    ]
  },
  {
    "Sid": "AllowCreateCWMetricsAndManageDashboards",
    "Effect": "Allow",
    "Action": [
      "cloudwatch:PutMetricData"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "AllowCreateandDeleteCWDashboards",
    "Effect": "Allow",
    "Action": [
      "cloudwatch:DeleteDashboards",
      "cloudwatch:PutDashboard"
    ],
    "Resource": [
      "*"
    ]
  }
]
}

```

Kebijakan Bersama Manajer Rahasia Pelanggan

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*"
    }
  ]
}

```

```

    "Resource": [
      "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
      "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    ],
  },
  {
    "Sid": "DenyCustomerGetSecretCustomerNamespace",
    "Effect": "Deny",
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
    "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
    "Effect": "Deny",
    "NotAction": [
      "secretsmanager:Describe*",
      "secretsmanager:Get*",
      "secretsmanager:List*"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
]
}

```

Kebijakan Berlangganan Marketplace Pelanggan

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

```
]
}
```

Pencatatan dan pemantauan peristiwa keamanan

AMS terus memantau lingkungan yang dikelola untuk ancaman keamanan. Peristiwa keamanan mungkin terdeteksi oleh AMS atau oleh Anda. AMS secara teratur memperbarui proses otomatisasi berdasarkan Computer Security Incident Handling Guide oleh National Institute of Standards and Technology (NIST) —untuk mendeteksi ancaman keamanan dengan lebih baik.

Keamanan Titik Akhir (EPS)

Sumber daya yang Anda sediakan di lingkungan AMS Advanced secara otomatis menyertakan penginstalan klien pemantauan keamanan titik akhir (EPS). Proses ini memastikan bahwa sumber daya AMS Advanced-managed dipantau dan didukung 24x7. Selain itu, AMS Advanced memantau semua aktivitas agen, dan insiden dibuat jika ada peristiwa keamanan yang terdeteksi.

Note

[Insiden keamanan ditangani sebagai insiden; untuk informasi lebih lanjut, lihat Respons insiden.](#)

Keamanan endpoint memberikan perlindungan anti-malware, khususnya, tindakan berikut didukung:

- EC2 instans mendaftar dengan EPS
- EC2 instance deregister dari EPS
- EC2 contoh perlindungan anti-malware real-time
- Detak jantung yang diprakarsai agen EPS
- EPS mengembalikan file yang dikarantina
- Pemberitahuan acara EPS
- Pelaporan EPS

AMS Advanced menggunakan Trend Micro untuk keamanan endpoint (EPS). Ini adalah pengaturan EPS default. Untuk mempelajari lebih lanjut tentang Trend Micro, lihat [Pusat Bantuan Trend Micro](#)

[Deep Security](#); perhatikan bahwa tautan non-Amazon dapat berubah tanpa pemberitahuan kepada kami.

Pengaturan default AMS Advanced Multi-Account Landing Zone (MALZ) dijelaskan di bagian berikut; untuk pengaturan EPS landing zone multi-akun AMS non-default, [lihat pengaturan non-default AMS Advanced Multi-Account Landing Zone EPS](#).

Note

Anda dapat membawa EPS Anda sendiri, lihat [AMS membawa EPS Anda sendiri](#).

Pengaturan EPS umum

Pengaturan jaringan umum keamanan titik akhir.

Default EPS

Pengaturan	Default
Port Firewall (Grup Keamanan Instans)	Agen EPS Deep Security Manager (DSMs) harus memiliki port 4120 terbuka untuk komunikasi Agent/Relay to Manager, dan port 4119 untuk Konsol Manajer. Relay EPS harus memiliki port 4122 terbuka untuk komunikasi Manager/Agent to Relay. Tidak ada port khusus yang harus terbuka untuk komunikasi inbound instance pelanggan karena agen memulai semua permintaan.
Arah Komunikasi	Agen/Alat Dimulai
Interval Detak Jantung	Sepuluh menit
Jumlah detak jantung yang terlewat sebelum peringatan	Dua
Drift maksimum yang diizinkan (perbedaan) antara waktu server	Tidak terbatas.

Pengaturan	Default
Meningkatkan kesalahan offline untuk mesin virtual yang tidak aktif (terdaftar, tetapi tidak online)	Tidak
Kebijakan default	Kebijakan dasar (dijelaskan selanjutnya)
Aktivasi beberapa komputer dengan nama host yang sama	Dijijinkan
Peringatan untuk pembaruan yang tertunda dinaikkan	Setelah tujuh hari
Perbarui jadwal	AMS menargetkan siklus rilis bulanan untuk pembaruan perangkat lunak Trend Micro Deep Security Manager (DSM) /Deep Security Agent (DSA). Namun, AMS tidak mempertahankan SLA untuk pembaruan. Pembaruan dilakukan secara armada oleh tim pengembang AMS selama penerapan. Pembaruan DSA/DSA dicatat dalam peristiwa sistem Trend Micro DSM yang disimpan AMS secara lokal secara default selama 13 minggu. Untuk dokumentasi vendor, lihat Acara sistem di Pusat Bantuan Trend Micro Deep Security. Log juga diekspor ke grup log/aws/ams/eps/var/log/DSM.log di Amazon. CloudWatch
Perbarui sumber	Server Pembaruan Trend Micro (https://ipv6-iaus.trendmicro.com/iau_server.dll/)
Penghapusan data peristiwa atau log	Peristiwa dan log dihapus dari database DSM setelah tujuh hari.
Versi perangkat lunak agen diadakan	Hingga lima
Pembaruan aturan terbaru diadakan	Hingga sepuluh

Pengaturan	Default
Penyimpanan log	Secara default, file log disimpan dengan aman di Amazon S3, tetapi Anda juga dapat mengarsipkannya ke Amazon Glacier untuk membantu memenuhi persyaratan audit dan kepatuhan.

Kebijakan dasar

Pengaturan default kebijakan basis keamanan titik akhir.

Kebijakan dasar EPS

Pengaturan	Default
Modul yang Diaktifkan	Anti-Malware
Modul Dinonaktifkan	Reputasi Web
	Firewall
	Perlindungan Intrusi
	Pemantauan Integritas
	Inspeksi Log
	Kontrol Aplikasi

Anti-malware

Pengaturan anti-malware keamanan titik akhir.

Default anti-malware EPS

Pengaturan	Default	Catatan
Pemindaian Waktu Nyata	Pindai semuanya	Karantina semua virus yang dicurigai

Pengaturan	Default	Catatan
	Setiap Day/All hari (24 jam)	. Aktifkan IntelliTr ap dan spyware/g rayware perlindungan. Spyware dan Grayware memicu Anti-Malware dan mengakibatkan karantina item tersebut.
Pemindaian Manual	Pindai semuanya	Harus diminta, kemudian mengikuti konfigurasi pemindaia n real-time default.
Pemindaian Terjadwal	Pindai semuanya	Ditetapkan untuk hari Minggu terakhir setiap bulan, 6 pagi.
Perlindungan Cerdas	Nonaktif	N/A
File yang Dikarantina	Manajer Keamanan Trend Micro Deep (DSM)	Appx 1GB disk dicadangkan untuk karantina.
Batasan Pindai	Tren Mikro DSM	Pindai file dari semua ukuran.
Spyware atau Grayware yang Diizinkan	Tidak ada	N/A
Pemberitahuan Acara Lokal	Ya	N/A

Proses mitigasi malware

AMS menggunakan Deep Security Platform (sistem anti-malware) Trend Micro untuk mendeteksi dan merespons malware pada instans yang dikelola AMS Anda. Secara default, agen deteksi Trend Micro berjalan di semua EC2 instans Amazon, termasuk yang ada di layanan bersama dan subnet pribadi, untuk sistem operasi Windows dan Linux. Sistem anti-malware terhubung ke pemantauan AMS sehingga suatu peristiwa dihasilkan setiap kali malware terdeteksi. Jika ada dampak pelanggan, acara ditingkatkan ke proses manajemen insiden (untuk detailnya, lihat [Tanggapan insiden AMS](#)). Sementara AMS menilai dampaknya, Anda diberi tahu, dan upaya dilakukan untuk mengurangi dampaknya.

Definisi anti-malware Trend Micro diperbarui secara otomatis saat Trend Micro menerbitkan pembaruan.

Selama orientasi aplikasi, Anda menunjukkan tindakan yang ingin AMS lakukan saat malware ditemukan pada sebuah instance:

- Pastikan file yang dikarantina ada di daftar izinkan, hapus dari karantina dan lepaskan kembali ke sistem file.
- Hapus file yang dikarantina, menghapusnya dari instance.
- Tangguhkan instance dan ganti. Instans yang ditangguhkan kemudian tersedia untuk Anda pasang untuk penelitian forensik.

Setelah orientasi aplikasi:

- Ketika sistem anti-malware menemukan malware pada sebuah instance, AMS secara otomatis mengkarantina malware tersebut. Ini memicu peristiwa dan penyelidikan lanjutan.
- AMS memberi tahu Anda tentang peristiwa tersebut melalui pemberitahuan layanan dan mulai mengikuti tindakan mitigasi default yang Anda pilih.
- Jika Anda belum memilih tindakan default, AMS akan menanyakan tindakan mana yang harus diambil. Setelah menerima instruksi Anda, AMS menjalankan tindakan yang dipilih dan memberi tahu Anda. AMS memberi tahu Anda lagi setelah tindakan selesai, termasuk detail yang diperlukan untuk analisis forensik, jika berlaku.

Aktifkan IDS dan IPS di Trend Micro Deep Security

Anda dapat meminta agar AMS mengaktifkan Trend Micro Intrusion Detection System (IDS) dan Intrusion Protection Systems (IPS), fitur non-default, untuk akun Anda.

Untuk melakukan ini, kirimkan permintaan pembaruan (Manajemen | Lainnya | Lainnya | Pembaruan) dan sertakan daftar alamat email untuk menerima pemberitahuan ID dan IPS. Alamat ini ditambahkan ke topik SNS di akun Anda, yang dibuat AMS untuk Anda.

Note

AMS tidak dapat menambahkan layanan Trend Micro yang mungkin mengganggu kemampuan kami untuk menyediakan layanan AMS lainnya.

Pemindaian malware sistem lengkap

Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) memerlukan pemindaian malware sistem lengkap, yang diaktifkan pada VPC yang dikelola AMS secara default. Pemindaian sistem penuh diatur untuk terjadi pada 2AM (pada zona waktu yang ditetapkan pada server) karena mereka menggunakan banyak CPU. Pemindaian sistem penuh merupakan tambahan dari pemindaian malware biasa yang tidak menggunakan banyak CPU.

Ada tipe perubahan Manajemen (CT) baru, Nonaktifkan pemindaian malware, yang memungkinkan Anda menonaktifkan pemindaian malware sistem penuh. Anda dapat menemukan CT di Manajemen | Keamanan host | Pemindaian sistem lengkap | Nonaktifkan klasifikasi, ubah ID ct-1pybwg08h8qsz. Untuk mengaktifkan kembali pemindaian, gunakan Manajemen | Lainnya | Lainnya | Perbarui CT. Menonaktifkan pemindaian sistem penuh tidak menonaktifkan pemindaian malware biasa Anda.

Keamanan Amazon Inspector

Layanan Amazon Inspector memantau keamanan tumpukan yang dikelola AMS Anda. Amazon Inspector adalah layanan penilaian keamanan otomatis yang membantu mengidentifikasi kesenjangan dalam keamanan dan kepatuhan infrastruktur yang digunakan. AWS Penilaian keamanan Amazon Inspector memungkinkan Anda menilai tumpukan secara otomatis untuk eksposur, kerentanan, dan penyimpangan dari praktik terbaik dengan memeriksa aksesibilitas dan kerentanan jaringan yang tidak diinginkan di instans Amazon Anda. EC2 Setelah melakukan penilaian, Amazon Inspector menghasilkan daftar detail temuan keamanan yang diprioritaskan berdasarkan tingkat keparahan. Penilaian Amazon Inspector ditawarkan sebagai paket aturan yang

telah ditentukan sebelumnya yang dipetakan ke praktik dan definisi terbaik keamanan umum. Aturan-aturan ini diperbarui secara berkala oleh peneliti AWS keamanan. Untuk informasi lebih lanjut tentang Amazon Inspector, kunjungi Amazon [Inspector](#).

AMS Amazon Inspector FAQs

- Apakah Amazon Inspector diinstal ke akun AMS saya secara default?

Tidak. Amazon Inspector bukan bagian dari build AMI default atau konsumsi beban kerja.

- Bagaimana cara mengakses dan menginstal Amazon Inspector?

Kirim RFC (Manajemen | Lainnya | Lainnya | Buat) untuk meminta akses akun dan instalasi ke Inspector dan tim operasi AMS akan memodifikasi ReadOnly Customer_ _Role untuk menyediakan akses konsol Amazon Inspector (tanpa akses SSM).

- Apakah Amazon Inspector Agent harus diinstal pada semua EC2 instans Amazon yang ingin saya nilai?

Tidak, penilaian Amazon Inspector dengan paket aturan jangkauan jaringan dapat dijalankan tanpa agen untuk instans Amazon apa pun. EC2 Agen diperlukan untuk paket aturan penilaian tuan rumah. Untuk informasi selengkapnya tentang penginstalan agen, lihat [Menginstal Agen Amazon Inspector](#).

- Apakah ada biaya tambahan untuk layanan ini?

Ya. Harga Amazon Inspector dapat ditemukan di situs harga [Amazon Inspector](#).

- Apa temuan Amazon Inspector?

Temuan adalah masalah keamanan potensial yang ditemukan selama penilaian Amazon Inspector dari target penilaian yang dipilih. Temuan ditampilkan di konsol Amazon Inspector atau API, dan berisi deskripsi rinci tentang masalah keamanan dan rekomendasi untuk menyelesaikannya.

- Apakah laporan penilaian Amazon Inspector tersedia?

Ya. Laporan penilaian adalah dokumen yang merinci apa yang diuji dalam proses penilaian, dan hasil penilaian. Hasil penilaian Anda diformat menjadi laporan standar, yang dapat dihasilkan untuk berbagi hasil dalam tim Anda untuk tindakan remediasi, untuk memperkaya data audit kepatuhan, atau untuk menyimpan referensi di masa mendatang. Laporan penilaian Amazon Inspector dapat dibuat untuk penilaian yang dijalankan setelah berhasil diselesaikan.

- Dapatkah saya menggunakan tag untuk mengidentifikasi tumpukan yang ingin saya jalankan laporan Amazon Inspector?

Ya.

- Akankah tim Operasi AMS memiliki akses ke hasil penilaian Amazon Inspector?

Ya. Siapa pun yang memiliki akses ke konsol Amazon Inspector di AWS dapat melihat temuan dan laporan penilaian.

- Akankah tim Operasi AMS merekomendasikan atau mengambil tindakan berdasarkan temuan laporan Amazon Inspector?

Tidak. Jika Anda ingin perubahan dibuat berdasarkan temuan laporan Amazon Inspector, Anda harus meminta perubahan melalui RFC (Manajemen | Lainnya | Lainnya | Pembaruan).

- Apakah AMS akan diberi tahu ketika saya menjalankan laporan Amazon Inspector?

Saat Anda meminta akses Amazon Inspector, Operator AMS yang menjalankan RFC akan memberi tahu CSDM Anda tentang permintaan tersebut.

Untuk informasi selengkapnya, lihat [Amazon Inspector FAQs](#).

Tanggapan insiden AMS

AMS menggunakan praktik terbaik manajemen insiden TI (ITSM) tradisional untuk memulihkan layanan, bila diperlukan, secepat mungkin.

Kami menyediakan follow-the-sun dukungan 24/7/365 melalui beberapa pusat operasi di seluruh dunia dengan operator khusus yang secara aktif memantau dasbor dan antrian insiden.

Teknisi operasi kami menggunakan alat pelacak insiden internal untuk mengidentifikasi, mencatat, mengkategorikan, memprioritaskan, mendiagnosis, menyelesaikan, dan menutup insiden serta memberikan pembaruan tentang semua aktivitas ini kepada Anda melalui konsol AMS atau melalui API. Dukungan Operator kami, banyak di antaranya telah menghabiskan waktu di AWS Premium Support dalam berbagai profil dan peran teknologi, memanfaatkan berbagai Dukungan alat internal untuk membantu semua aktivitas tersebut. Operator ini sangat akrab dengan infrastruktur yang didukung AMS dan memiliki keterampilan teknis tingkat ahli untuk mengatasi semua masalah dukungan yang diidentifikasi. Dalam kasus yang jarang terjadi di mana operator kami membutuhkan bantuan, tim Dukungan dan AWS Layanan Premium tersedia untuk membantu sesuai kebutuhan.

Jika insiden prioritas tinggi memengaruhi beban kerja kritis Anda, AMS akan merekomendasikan pemulihan infrastruktur. Sering ada tradeoff antara pemecahan masalah atau memulihkan dari cadangan yang diketahui baik, dan risiko pelanggan dan dampak dari downtime layanan adalah

faktor penentu. Jika Anda memiliki waktu untuk mengabdikan diri untuk memecahkan masalah, AMS akan membantu Anda, tetapi jika urgensi untuk memulihkan tinggi, kami dapat segera memulai pemulihan.

Note

Data singkat yang bukan bagian dari template tumpukan atau pemulihan data hilang. AMS menggunakan upaya yang wajar untuk melakukan pemulihan infrastruktur sementara penawaran AWS layanan tidak tersedia. Pemulihan infrastruktur selesai setelah penawaran AWS layanan tersedia.

Jika Anda tidak mengizinkan pemulihan infrastruktur seperti yang direkomendasikan oleh AMS, Anda tidak akan memenuhi syarat untuk mendapatkan kredit layanan untuk komitmen layanan AMS untuk waktu penyelesaian insiden.

Validasi kepatuhan

AMS menyebarkan dan mengelola pustaka AWS Config aturan dan tindakan remediasi, untuk melindungi dari kesalahan konfigurasi yang dapat mengurangi keamanan dan integritas operasional akun Anda.

Sebagai contoh, ketika bucket Amazon S3 dibuat, AWS Config dapat mengevaluasi bucket Amazon S3 terhadap aturan yang mengharuskan bucket Amazon S3 untuk menolak akses baca publik. Jika kebijakan bucket Amazon S3 atau daftar kontrol akses bucket (ACL) mengizinkan akses baca publik, AWS Config menandai bucket dan aturan sebagai tidak sesuai. Ini Aturan AWS Config menandai sumber daya sebagai Compliant, Noncompliant, atau Not Applicable, berdasarkan hasil evaluasi mereka. Untuk informasi selengkapnya tentang AWS Config layanan, lihat [Panduan AWS Config Pengembang](#).

Anda dapat menggunakan AWS Config konsol, AWS CLI, atau AWS Config API untuk melihat aturan yang diterapkan di akun Anda dan status kepatuhan aturan dan sumber daya Anda. Untuk informasi selengkapnya, lihat AWS Config dokumentasi: [Melihat Kepatuhan Konfigurasi](#).

Note

Informasi tambahan tentang topik ini tersedia dengan mengakses laporan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#). Untuk mengakses Artifact AWS, Anda dapat menghubungi CSDM Anda untuk mendapatkan petunjuk atau

membuka [Memulai dengan Artifact AWS](#). Informasi ini tidak termasuk dalam panduan pengguna ini karena berisi konten keamanan sensitif.

Zona Pendaratan Multi-Akun yang melihat status kepatuhan Anda Aturan AWS Config

AMS multi-account landing zone menggunakan layanan AWS Config agregator untuk membuat tampilan kepatuhan terpusat di semua akun Anda. Ini berarti Anda dapat melihat status kepatuhan Aturan AWS Config di seluruh lingkungan landing zone multi-akun AMS di bawah AWS Config agregator di akun keamanan Anda.

Berikut ini adalah contoh AWS Config agregator yang menampilkan status kepatuhan pusat Aturan AWS Config di seluruh akun.

Untuk informasi selengkapnya, lihat dokumentasi AWS untuk [Config Aggregator](#).

- Bagaimana AMS menggunakan aturan AWS Config?

AMS membuat Aturan AWS Config untuk memberikan visibilitas ke dalam konfigurasi sumber AWS daya Anda terhadap kondisi yang ditentukan dalam aturan. Jika aturan tidak sesuai, Anda dapat meminta perubahan dan tim AMS Ops akan bekerja sama dengan Anda untuk mengambil tindakan korektif.

- Dalam hal ini, Anda melihat perubahan berikut muncul di akun AMS Anda:
 - Aturan AWS Config di bawah AWS Config > Aturan
 - Aturan Konfigurasi Kustom dengan fungsi Lambda mereka ada di akun Anda
 - Config Aggregator di akun Keamanan dan Otorisasi Config di semua akun (hanya Zona Pendaratan Multi-Akun)

Berikut ini adalah contoh Aturan AWS Config dan hasil evaluasi kepatuhan mereka ditunjukkan di bawah ini:

Untuk mempelajari AWS Config selengkapnya, lihat:

- AWS Config: [Apa Itu Config?](#)

- Aturan AWS Config: [Mengevaluasi Sumber Daya dengan](#) Aturan
- Aturan AWS Config: [Pemeriksaan Kepatuhan Dinamis: Aturan AWS Config — Pemeriksaan Kepatuhan Dinamis](#) untuk Sumber Daya Cloud
- AWS Config Aggregator: Agregasi Data [Multi-Wilayah Multi-Akun](#)

Pembatasan kebijakan kontrol layanan landing zone multi-akun AMS

Bagian ini telah disunting karena berisi informasi sensitif terkait keamanan AMS. Informasi ini tersedia melalui Dokumentasi konsol AMS. Untuk mengakses Artifact AWS, Anda dapat menghubungi CSDM Anda untuk mendapatkan petunjuk atau membuka [Memulai dengan Artifact AWS](#).

Ketahanan

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat [infrastruktur AWS global](#).

Keamanan infrastruktur

Note

Informasi tambahan tentang topik ini tersedia dengan mengakses laporan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#). Untuk mengakses Artifact AWS, Anda dapat menghubungi CSDM Anda untuk mendapatkan petunjuk atau membuka [Memulai dengan Artifact AWS](#). Informasi ini tidak termasuk dalam panduan pengguna ini karena berisi konten keamanan sensitif.

Kontrol keamanan untuk sistem end-of-support operasi

Sistem operasi yang berada di luar periode dukungan umum dari produsen sistem operasi "end-of-support" atau EOS, dan tidak menerima pembaruan keamanan, memiliki risiko keamanan yang meningkat.

AWS menawarkan beberapa layanan untuk membantu menangani sistem operasi end-of-support. Untuk informasi tentang Windows end-of-support, lihat [Program End-of-Support Migrasi untuk Windows Server](#).

Note

Informasi tambahan tentang topik ini tersedia dengan mengakses laporan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#). Untuk mengakses Artifact AWS, Anda dapat menghubungi CSDM Anda untuk mendapatkan petunjuk atau membuka [Memulai dengan Artifact AWS](#). Informasi ini tidak termasuk dalam panduan pengguna ini karena berisi konten keamanan sensitif.

Menggunakan grup keamanan

Grup keamanan bertindak sebagai firewall yang mengontrol lalu lintas untuk satu instans atau lebih. Grup keamanan AMS memungkinkan Anda menetapkan peraturan lalu lintas masuk dan aturan lalu lintas keluar berdasarkan tingkat instans. Anda dapat membuat grup keamanan dan menentukan sumber daya di akun AMS, instans Amazon, EC2 instans Amazon RDS DB, Load Balancer, instans replikasi Deep Security Manager (DSM), target pemasangan EFS, dan ElastiCache cluster, untuk dikaitkan dengan grup keamanan. Setelah dikaitkan, lalu lintas ke atau dari instance tersebut dibatasi oleh aturan yang ditetapkan dalam grup keamanan.

Untuk lebih memahami keamanan AWS umum, lihat [Praktik Terbaik untuk Keamanan, Identitas, & Kepatuhan](#) dan [Grup EC2 Keamanan Amazon untuk Instans Linux](#).

AMS sekarang memiliki serangkaian jenis perubahan untuk membuat dan mengelola grup keamanan:

- Penerapan | Komponen tumpukan tingkat lanjut | Grup keamanan | Buat (ct-10xx2g2d7hc90)
- Manajemen | Komponen tumpukan tingkat lanjut | Grup keamanan | Hapus (ct-3cp96z7r065e4)
- Manajemen | Komponen tumpukan tingkat lanjut | Grup keamanan | Pembaruan (ct-3memthlcmvc1b)

Sebagai contoh, lihat [Grup keamanan](#).

Grup keamanan

Di AWS VPCs, AWS Security Groups bertindak sebagai firewall virtual, mengontrol lalu lintas untuk satu atau beberapa tumpukan (instance atau satu set instance). Ketika tumpukan diluncurkan, itu terkait dengan satu atau beberapa grup keamanan, yang menentukan lalu lintas apa yang diizinkan untuk mencapainya:

- Untuk tumpukan di subnet publik Anda, grup keamanan default menerima lalu lintas dari HTTP (80) dan HTTPS (443) dari semua lokasi (internet). Tumpukan juga menerima lalu lintas SSH dan RDP internal dari jaringan perusahaan Anda, dan benteng AWS. Tumpukan tersebut kemudian dapat keluar melalui port apa pun ke Internet. Mereka juga dapat keluar ke subnet pribadi Anda dan tumpukan lain di subnet publik Anda.
- Tumpukan di subnet pribadi Anda dapat keluar ke tumpukan lain di subnet pribadi Anda, dan instance dalam tumpukan dapat sepenuhnya berkomunikasi melalui protokol apa pun satu sama lain.

Important

Grup keamanan default untuk tumpukan pada subnet pribadi memungkinkan semua tumpukan di subnet pribadi Anda untuk berkomunikasi dengan tumpukan lain di subnet pribadi tersebut. Jika Anda ingin membatasi komunikasi antar tumpukan dalam subnet pribadi, Anda harus membuat grup keamanan baru yang menjelaskan pembatasan tersebut. Misalnya, jika Anda ingin membatasi komunikasi ke server database sehingga tumpukan di subnet pribadi itu hanya dapat berkomunikasi dari server aplikasi tertentu melalui port tertentu, mintalah grup keamanan khusus. Cara melakukannya dijelaskan di bagian ini.

Grup Keamanan Default

MALZ

Tabel berikut menjelaskan pengaturan grup keamanan masuk (SG) default untuk tumpukan Anda. SG diberi nama "SentinelDefaultSecurityGroupPrivateOnly-VPC-ID" yang merupakan ID VPC di **ID** akun landing zone multi-akun AMS Anda. Semua lalu lintas diizinkan keluar ke "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly" melalui grup keamanan ini (semua lalu lintas lokal dalam subnet tumpukan diizinkan).

Semua lalu lintas diizinkan keluar ke 0.0.0.0/0 oleh grup keamanan kedua "".

SentinelDefaultSecurityGroupPrivateOnly

Tip

Jika Anda memilih grup keamanan untuk jenis perubahan AMS, seperti EC2 membuat, atau OpenSearch membuat domain, Anda akan menggunakan salah satu grup keamanan default yang dijelaskan di sini, atau grup keamanan yang Anda buat. Anda dapat menemukan daftar grup keamanan, per VPC, di EC2 konsol AWS atau konsol VPC.

Ada grup keamanan default tambahan yang digunakan untuk keperluan AMS internal.

Grup keamanan default AMS (lalu lintas masuk)

Jenis	Protokol	Rentang port	Sumber
Semua Lalu lintas	Semua	Semua	SentinelDefaultSecurityGroupPrivateOnly (membatasi lalu lintas keluar ke anggota grup keamanan yang sama)
Semua Lalu lintas	Semua	Semua	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (tidak membatasi lalu lintas keluar)
HTTP, HTTPS, SSH, RDP	TCP	80/443 (Sumber 0.0.0.0/0) Akses SSH dan RDP diizinkan dari benteng	SentinelDefaultSecurityGroupPublic (tidak membatasi lalu lintas keluar)
Benteng MALZ:			
SSH	TCP	22	SharedServices VPC CIDR dan DMZ VPC CIDR, ditambah pelanggan yang disediakan secara on- prem CIDRs
SSH	TCP	22	
RDP	TCP	3389	

Jenis	Protokol	Rentang port	Sumber
RDP	TCP	3389	
Benteng SALZ:			
SSH	TCP	22	mc-initial-garden- LinuxBastion SG
SSH	TCP	22	mc-initial-garden- LinuxBastion DMZSG
RDP	TCP	3389	mc-initial-garden- WindowsBastion SG
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMZSG

SALZ

Tabel berikut menjelaskan pengaturan grup keamanan masuk (SG) default untuk tumpukan Anda. SG diberi nama "mc-initial-garden- SentinelDefaultSecurityGroupPrivateOnly -**ID**" di mana **ID** adalah pengenalan unik. Semua lalu lintas diizinkan keluar ke "mc-initial-garden- SentinelDefaultSecurityGroupPrivateOnly" melalui grup keamanan ini (semua lalu lintas lokal dalam subnet tumpukan diizinkan).

Semua lalu lintas diizinkan keluar ke 0.0.0.0/0 oleh grup keamanan kedua "- -". mc-initial-garden SentinelDefaultSecurityGroupPrivateOnlyEgressAll **ID**

Tip

Jika Anda memilih grup keamanan untuk jenis perubahan AMS, seperti EC2 membuat, atau OpenSearch membuat domain, Anda akan menggunakan salah satu grup keamanan default yang dijelaskan di sini, atau grup keamanan yang Anda buat. Anda dapat menemukan daftar grup keamanan, per VPC, di EC2 konsol AWS atau konsol VPC.

Ada grup keamanan default tambahan yang digunakan untuk keperluan AMS internal.

Grup keamanan default AMS (lalu lintas masuk)

Jenis	Protokol	Rentang port	Sumber
Semua Lalu lintas	Semua	Semua	SentinelDefaultSecurityGroupPrivateOnly (membatasi lalu lintas keluar ke anggota grup keamanan yang sama)
Semua Lalu lintas	Semua	Semua	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (tidak membatasi lalu lintas keluar)
HTTP, HTTPS, SSH, RDP	TCP	80/443 (Sumber 0.0.0.0/0) Akses SSH dan RDP diizinkan dari benteng	SentinelDefaultSecurityGroupPublic (tidak membatasi lalu lintas keluar)
Benteng MALZ:			
SSH	TCP	22	SharedServices VPC CIDR dan DMZ VPC CIDR, ditambah pelanggan yang disediakan secara on-prem CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
Benteng SALZ:			
SSH	TCP	22	mc-initial-garden- LinuxBastion SG
SSH	TCP	22	mc-initial-garden- LinuxBastion DMZSG
RDP	TCP	3389	mc-initial-garden- WindowsBastion SG
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMZSG

Membuat, Mengubah, atau Menghapus Grup Keamanan

Anda dapat meminta grup keamanan khusus. Jika grup keamanan default tidak memenuhi kebutuhan aplikasi atau organisasi Anda, Anda dapat memodifikasi atau membuat grup keamanan baru. Permintaan semacam itu akan dianggap memerlukan persetujuan dan akan ditinjau oleh tim operasi AMS.

Untuk membuat grup keamanan di luar tumpukan dan VPCs, kirimkan RFC menggunakan jenis `Deployment | Advanced stack components | Security group | Create (review required)` perubahan (`ct-10xx2g2d7hc90`).

Untuk modifikasi grup keamanan Active Directory (AD), gunakan jenis perubahan berikut:

- Untuk menambahkan pengguna: Kirim RFC menggunakan Manajemen | Directory Service | Pengguna dan grup | Tambahkan pengguna ke grup [`ct-24pi85mjtza8k`]
- Untuk menghapus pengguna: Kirim RFC menggunakan Manajemen | Directory Service | Pengguna dan grup | Hapus pengguna dari grup [`ct-2019s9y3nfml4`]

Note

Saat menggunakan “review required” CTs, AMS merekomendasikan agar Anda menggunakan opsi Penjadwalan ASAP (pilih ASAP di konsol, biarkan waktu mulai dan berakhir kosong di API/CLI) karena ini CTs memerlukan operator AMS untuk memeriksa RFC, dan mungkin berkomunikasi dengan Anda sebelum dapat disetujui dan dijalankan. Jika Anda menjadwalkan ini RFCs, pastikan untuk mengizinkan setidaknya 24 jam. Jika persetujuan tidak terjadi sebelum waktu mulai yang dijadwalkan, RFC ditolak secara otomatis.

Temukan Grup Keamanan

Untuk menemukan grup keamanan yang dilampirkan ke tumpukan atau instance, gunakan EC2 konsol. Setelah menemukan tumpukan atau instance, Anda dapat melihat semua grup keamanan yang melekat padanya.

Untuk cara menemukan grup keamanan di baris perintah dan memfilter output, lihat [describe-security-groups](#).

Perpustakaan kontrol pencegahan dan detektif AMS

AWS Managed Services (AMS) memberi Anda kebijakan kontrol layanan ConfigRules yang telah terbukti (SCPs) dan dapat dimanfaatkan untuk meningkatkan postur keamanan Anda dan mengurangi kesenjangan kepatuhan di akun AMS Anda. [library/catalog](#)

Topik

- [Aturan yang Dikurasi SCPs dan Config](#)
- [Pemberitahuan khusus untuk aturan Config](#)

Aturan yang Dikurasi SCPs dan Config

Aturan Terkurasi SCPs dan Konfigurasi untuk AMS Advanced.

- Kebijakan kontrol layanan (SCPs): Yang disediakan SCPs adalah tambahan dari kebijakan AMS default.

Anda dapat menggunakan kontrol pustaka ini bersama-sama dengan kontrol default untuk memenuhi persyaratan keamanan tertentu.

- Aturan Konfigurasi: Sebagai ukuran dasar, AMS merekomendasikan penerapan Paket Kesesuaian (lihat Paket Kesesuaian dalam AWS Config panduan) selain aturan konfigurasi [AMS](#) default (lihat Artefak AMS untuk aturan default). Paket Kesesuaian mencakup sebagian besar persyaratan kepatuhan dan AWS memperbaruinya secara berkala.

Aturan yang tercantum di sini dapat digunakan untuk menutupi kesenjangan khusus kasus penggunaan yang tidak dicakup oleh Paket Kesesuaian

Note

Karena aturan default AMS dan paket kesesuaian diperbarui dari waktu ke waktu, Anda mungkin melihat duplikat aturan ini.

AMS merekomendasikan untuk melakukan pembersihan berkala dari Aturan Konfigurasi duplikat secara umum.

Untuk AMS Advanced, Aturan Konfigurasi tidak boleh menggunakan remediasi otomatis (lihat Memediasi [Sumber Daya AWS yang Tidak Sesuai dengan Aturan AWS Config](#)) untuk [menghindari](#) perubahan. out-of-band

SCP-AMS-001: Batasi pembuatan EBS

Cegah pembuatan volume EBS jika Anda tidak mengaktifkan enkripsi.

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:CreateVolume",
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-002: Batasi peluncuran EC2

Cegah peluncuran EC2 instance jika volume EBS tidak dienkripsi. Ini termasuk menolak EC2 peluncuran dari tidak terenkripsi AMIs karena SCP ini juga berlaku untuk volume root.

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:RunInstances",
  "Resource": "arn:aws:ec2:*:*:volume/*",
  "Effect": "Deny"
}
```

SCP-ADV-001: Batasi pengiriman RFC

Batasi peran AMS default agar tidak mengirimkan otomatis tertentu seperti RFCs Buat VPC atau Hapus VPC. Ini sangat membantu jika Anda ingin menerapkan izin yang lebih terperinci ke peran federasi Anda.

Misalnya, Anda mungkin `AWSServiceCatalogChangeManagement` Role ingin default dapat mengirimkan sebagian besar yang tersedia RFCs kecuali yang memungkinkan pembuatan dan penghapusan VPC, pembuatan subnet tambahan, offboarding akun aplikasi, memperbarui atau menghapus penyedia identitas SAMP:

SCP-AMS-003: Batasi atau pembuatan EC2 RDS di AMS

Cegah pembuatan instans Amazon EC2 dan RDS yang tidak memiliki tag tertentu, sambil mengizinkan AMS Backup IAM peran default AMS melakukannya. Ini diperlukan untuk pemulihan bencana atau DR.

```
{
  "Sid": "DenyRunInstanceWithNoOrganizationTag",
  "Effect": "Deny",
  "Action": [
    "ec2:RunInstances",
    "rds:CreateDBInstance"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:rds:*:*:db:*"
  ],
  "Condition": {
    "Null": {
      "aws:RequestTag/organization": "true"
    },
    "StringNotLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam:*:<Account_Number>:role/ams-backup-iam-role"
      ]
    }
  }
}
```

SCP-AMS-004: Batasi unggahan S3

Mencegah unggahan objek S3 yang tidak terenkripsi.

```
{
  "Sid": "DenyUnencryptedS3Uploads",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "StringNotLike": {
      "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"]
    }
  },
}
```

```

        "Null": {
            "s3:x-amz-server-side-encryption": "false"
        }
    }
}
]
}

```

SCP-AMS-005: Batasi akses API dan konsol

Cegah akses AWS Console dan API untuk permintaan yang berasal dari alamat IP buruk yang diketahui sebagai pelanggan yang ditentukan InfoSec.

SCP-AMS-006: Mencegah entitas IAM menghapus akun anggota dari organisasi

Mencegah AWS Identity and Access Management entitas menghapus akun anggota dari organisasi.

```

{
  "Effect": "Deny",
  "Action": ["organizations:LeaveOrganization"],
  "Resource": ["*"]
}

```

SCP-AMS-007: Mencegah berbagi sumber daya ke akun di luar organisasi Anda

Mencegah berbagi sumber daya dengan akun eksternal di luar AWS organisasi

```

{
  "Effect": "Deny",
  "Action": [
    "iam:*"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "Bool": {
      "iam:AllowsExternalPrincipals": "true"
    }
  }
},
{

```

```

"Effect": "Deny",
"Action": [
  "ram:CreateResourceShare",
  "ram:UpdateResourceShare"
],
"Resource": "*",
"Condition": {
  "Bool": {
    "ram:RequestedAllowsExternalPrincipals": "true"
  }
}
}

```

SCP-AMS-008: Mencegah berbagi dengan organisasi atau unit organisasi () OUs

Cegah berbagi sumber daya dengan akun and/or OU yang ada di organisasi.

```

{
  "Effect": "Deny",
  "Action": [
    "ram:CreateResourceShare",
    "ram:AssociateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringLike": {
      "ram:Principal": [
        "arn:aws:organizations::*:account/o-${OrganizationId}/${AccountId}",
        "arn:aws:organizations::*:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}"
      ]
    }
  }
}

```

SCP-AMS-009: Mencegah pengguna menerima undangan berbagi sumber daya

Cegah akun anggota menerima undangan untuk bergabung dengan pembagian sumber AWS RAM daya. API ini tidak mendukung kondisi apa pun dan mencegah pembagian hanya dari akun eksternal.

```

{
  "Effect": "Deny",
  "Action": ["ram:AcceptResourceShareInvitation"],
  "Resource": ["*"]
}

```

```
}
```

SCP-AMS-010: Mencegah Wilayah akun mengaktifkan dan menonaktifkan tindakan

Cegah mengaktifkan atau menonaktifkan AWS Wilayah baru untuk akun Anda. AWS

```
{
  "Effect": "Deny",
  "Action": [
    "account:EnableRegion",
    "account:DisableRegion"
  ],
  "Resource": "*"
}
```

SCP-AMS-011: Mencegah tindakan modifikasi penagihan

Mencegah modifikasi konfigurasi penagihan dan pembayaran.

```
{
  "Effect": "Deny",
  "Action": [
    "aws-portal:ModifyBilling",
    "aws-portal:ModifyAccount",
    "aws-portal:ModifyPaymentMethods"
  ],
  "Resource": "*"
}
```

SCP-AMS-012: Mencegah penghapusan atau modifikasi ke spesifik CloudTrails

Cegah modifikasi pada AWS CloudTrail jalur tertentu.

```
{
  "Effect": "Deny",
  "Action": [
    "cloudtrail:DeleteEventDataStore",
    "cloudtrail:DeleteTrail",
    "cloudtrail:PutEventSelectors",
    "cloudtrail:PutInsightSelectors",
    "cloudtrail:UpdateEventDataStore",
    "cloudtrail:UpdateTrail",
  ]
}
```

```
"cloudtrail:StopLogging"
],
"Resource": [
  "arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}"
]
}
```

SCP-AMS-013: Mencegah menonaktifkan enkripsi EBS default

Mencegah penonaktifan enkripsi Amazon EBS default.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

SCP-AMS-014: Mencegah pembuatan VPC dan subnet default

Cegah pembuatan VPC dan subnet Amazon default.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateDefaultSubnet",
    "ec2:CreateDefaultVpc"
  ],
  "Resource": "*"
}
```

SCP-AMS-015: Mencegah menonaktifkan dan memodifikasi GuardDuty

GuardDuty Cegah Amazon dimodifikasi atau dinonaktifkan.

```
{
  "Effect": "Deny",
  "Action": [
    "guardduty:AcceptInvitation",
    "guardduty:ArchiveFindings",
    "guardduty:CreateDetector",

```

```

    "guardduty:CreateFilter",
    "guardduty:CreateIPSet",
    "guardduty:CreateMembers",
    "guardduty:CreatePublishingDestination",
    "guardduty:CreateSampleFindings",
    "guardduty:CreateThreatIntelSet",
    "guardduty:DeclineInvitations",
    "guardduty>DeleteDetector",
    "guardduty>DeleteFilter",
    "guardduty>DeleteInvitations",
    "guardduty>DeleteIPSet",
    "guardduty>DeleteMembers",
    "guardduty>DeletePublishingDestination",
    "guardduty>DeleteThreatIntelSet",
    "guardduty:DisableOrganizationAdminAccount",
    "guardduty:DisassociateFromMasterAccount",
    "guardduty:DisassociateMembers",
    "guardduty:InviteMembers",
    "guardduty:StartMonitoringMembers",
    "guardduty:StopMonitoringMembers",
    "guardduty:TagResource",
    "guardduty:UnarchiveFindings",
    "guardduty:UntagResource",
    "guardduty:UpdateDetector",
    "guardduty:UpdateFilter",
    "guardduty:UpdateFindingsFeedback",
    "guardduty:UpdateIPSet",
    "guardduty:UpdateMalwareScanSettings",
    "guardduty:UpdateMemberDetectors",
    "guardduty:UpdateOrganizationConfiguration",
    "guardduty:UpdatePublishingDestination",
    "guardduty:UpdateThreatIntelSet"
  ],
  "Resource": "*"
}

```

SCP-AMS-016: Mencegah aktivitas pengguna root

Cegah pengguna root melakukan tindakan apa pun.

```

{
  "Action": "*",
  "Resource": "*",
  "Effect": "Deny",

```



```
"Condition": {
  "StringLike": {
    "aws:PrincipalArn": [
      "arn:aws:iam::*:root"
    ]
  }
}
```

SCP-AMS-017: Mencegah membuat kunci akses untuk pengguna root

Cegah pembuatan kunci akses untuk pengguna root.

```
{
  "Effect": "Deny",
  "Action": "iam:CreateAccessKey",
  "Resource": "arn:aws:iam::*:root"
}
```

SCP-AMS-018: Mencegah menonaktifkan blok akses publik akun S3

Cegah menonaktifkan blok akses publik akun Amazon S3. Ini mencegah ember apa pun di akun menjadi publik.

```
{
  "Effect": "Deny",
  "Action": "s3:PutAccountPublicAccessBlock",
  "Resource": "*"
}
```

SCP-AMS-019: Mencegah menonaktifkan AWS Config atau memodifikasi aturan Config

Mencegah menonaktifkan atau memodifikasi AWS Config aturan.

```
{
  "Effect": "Deny",
  "Action": [
    "config:DeleteConfigRule",
    "config:DeleteConfigurationRecorder",
    "config:DeleteDeliveryChannel",
    "config:DeleteEvaluationResults",
    "config:StopConfigurationRecorder"
  ]
}
```

```
],  
  "Resource": "*" }  
}
```

SCP-AMS-020: Cegah semua tindakan IAM

Cegah semua tindakan IAM.

```
{  
  "Effect": "Deny",  
  "Action": [  
    "iam:*"  
  ],  
  "Resource": "*" }  
}
```

SCP-AMS-021: Mencegah penghapusan grup dan aliran Log CloudWatch

Cegah penghapusan grup dan aliran Amazon CloudWatch Logs.

```
{  
  "Effect": "Deny",  
  "Action": [  
    "logs:DeleteLogGroup",  
    "logs:DeleteLogStream"  
  ],  
  "Resource": "*" }  
}
```

SCP-AMS-022: Mencegah penghapusan gletser

Cegah penghapusan Amazon Glacier.

```
{  
  "Effect": "Deny",  
  "Action": [  
    "glacier:DeleteArchive",  
    "glacier:DeleteVault"  
  ],  
  "Resource": "*" }  
}
```

SCP-AMS-023: Mencegah penghapusan IAM Access Analyzer

Mencegah penghapusan IAM Access Analyzer.

```
{
  "Action": [
    "access-analyzer:DeleteAnalyzer"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-024: Mencegah modifikasi pada Security Hub

Mencegah penghapusan. AWS Security Hub

```
{
  "Action": [
    "securityhub:DeleteInvitations",
    "securityhub:DisableSecurityHub",
    "securityhub:DisassociateFromMasterAccount",
    "securityhub:DeleteMembers",
    "securityhub:DisassociateMembers"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-025: Mencegah penghapusan di bawah Directory Service

Mencegah penghapusan sumber daya di bawah. AWS Directory Service

```
{
  "Action": [
    "ds:DeleteDirectory",
    "ds:DeleteLogSubscription",
    "ds:DeleteSnapshot",
    "ds:DeleteTrust",
    "ds:DeregisterCertificate",
    "ds:DeregisterEventTopic",
    "ds:DisableLDAPS",
    "ds:DisableRadius",

```

```
"ds:DisableSso",
"ds:UnshareDirectory"
],
"Resource": "*",
"Effect": "Deny"
}
```

SCP-AMS-026: Mencegah penggunaan layanan yang tidak terdaftar

Cegah penggunaan layanan yang tidak terdaftar.

Note

Ganti *service1* dan *service2* dengan nama layanan Anda. Contoh *access-analyzer* atau *IAM*.

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"]
}
```

SCP-AMS-027: Mencegah penggunaan layanan yang tidak terdaftar di Wilayah tertentu

Mencegah penggunaan layanan yang tidak terdaftar di AWS Wilayah tertentu.

Note

Ganti *service1* dan *service2* dengan nama layanan Anda. Contoh *access-analyzer* atau *IAM*.

Ganti *region1* dan *region2* dengan nama layanan Anda. Contoh *us-west-2* atau *use-east-1*.

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"],
  "Condition": {
```

```

    "StringEquals": {
      "aws:RequestedRegion": [
        "region1",
        "region2"
      ]
    }
  }
}

```

SCP-AMS-028: Mencegah tag diubah kecuali oleh kepala sekolah yang berwenang

Mencegah modifikasi tag oleh pengguna mana pun kecuali kepala sekolah yang berwenang.

Gunakan tag otorisasi untuk mengotorisasi prinsipal. Tag otorisasi harus dikaitkan dengan sumber daya dan dengan prinsipal. A hanya user/role dianggap sah jika tag pada sumber daya dan prinsipal cocok. Untuk informasi selengkapnya, lihat sumber daya berikut:

- [Mengamankan tag sumber daya yang digunakan untuk otorisasi menggunakan kebijakan kontrol layanan di AWS Organizations](#)
- [Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi](#)

```

{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-project}",
      "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
    },
    "Null": {
      "ec2:ResourceTag/access-project": false
    }
  }
},
{
  "Effect": "Deny",

```

```

"Action": [
  "ec2:CreateTags",
  "ec2:DeleteTags"
],
"Resource": [
  "*"
],
"Condition": {
  "StringNotEquals": {
    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-project}",
    "aws:PrincipalArn": "arn:aws:iam::${ACCOUNT_ID}:${RESOURCE_TYPE}/${RESOURCE_NAME}"
  },
  "ForAnyValue:StringEquals": {
    "aws:TagKeys": [
      "access-project"
    ]
  }
}
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalArn": "arn:aws:iam::${ACCOUNT_ID}:${RESOURCE_TYPE}/${RESOURCE_NAME}"
    },
    "Null": {
      "aws:PrincipalTag/access-project": true
    }
  }
}
}

```

SCP-AMS-029: Mencegah pengguna menghapus Amazon VPC Flow Logs

Mencegah penghapusan Amazon VPC Flow Logs.

```

{
  "Action": [

```

```

    "ec2:DeleteFlowLogs",
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream",
    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:PutLifecycleConfiguration",
    "firehose:DeleteDeliveryStream"
  ],
  "Resource": "*",
  "Effect": "Deny"
}

```

SCP-AMS-030: Mencegah berbagi subnet VPC dengan akun selain akun jaringan

Cegah berbagi subnet Amazon VPC dengan akun selain akun jaringan.

Note

Ganti **NETWORK_ACCOUNT_ID** dengan ID akun jaringan Anda.

```

{
  "Effect": "Deny",
  "Action": [
    "ram:AssociateResourceShare",
    "ram:CreateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "ram:Principal": "NETWORK_ACCOUNT_ID"
    },
    "StringEquals": {
      "ram:RequestedResourceType": "ec2:Subnet"
    }
  }
}

```

SCP-AMS-031: Mencegah peluncuran instance dengan tipe instans terlarang

Cegah pencucian jenis EC2 instans Amazon yang dilarang.

Note

Ganti *instance_type1* dan *instance_type2* dengan jenis instance yang ingin Anda batasi, seperti *t2.micro* atau string wildcard seperti **.nano*

```
{
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "ForAnyValue:StringLike": {
      "ec2:InstanceType": [
        "instance_type1",
        "instance_type2"
      ]
    }
  }
}
```

SCP-AMS-032: Mencegah peluncuran instance tanpa IMDSv2

Cegah EC2 instans Amazon tanpa IMDSv2.

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
```



```

    "NumericGreaterThan": {
      "ec2:MetadataHttpPutResponseHopLimit": "3"
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*"
  }
]

```

SCP-AMS-033: Mencegah modifikasi pada peran IAM tertentu

Mencegah modifikasi pada peran IAM tertentu.

```

{
  "Action": [
    "iam:AttachRolePolicy",
    "iam>DeleteRole",
    "iam>DeleteRolePermissionsBoundary",
    "iam>DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:PutRolePermissionsBoundary",
    "iam:PutRolePolicy",
    "iam:TagRole",
    "iam:UntagRole",
    "iam:UpdateAssumeRolePolicy",
    "iam:UpdateRole",
    "iam:UpdateRoleDescription"
  ],
  "Resource": [
    "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
}

```

```
"Effect": "Deny"
}
```

SCP-AMS-034: Mencegah AssumeRolePolicy modifikasi pada peran IAM tertentu

Mencegah modifikasi untuk peran IAM yang ditentukan. AssumeRolePolicy

```
{
  "Action": [
    "iam:UpdateAssumeRolePolicy"
  ],
  "Resource": [
    "arn:aws:iam::{{ACCOUNT_ID}}:role/{{RESOURCE_NAME}}"
  ],
  "Effect": "Deny"
}
```

ConfigRule: Tag yang dibutuhkan

Periksa apakah EC2 instance memiliki tag khusus yang Anda butuhkan. Selain itu InfoSec, ini juga berguna untuk Manajemen Biaya Anda

```
ConfigRuleName: required-tags
Description: >-
  A Config rule that checks whether EC2 instances have the required tags.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
InputParameters:
  tag1Key: COST_CENTER
  tag2Key: APP_ID
Source:
  Owner: AWS
  SourceIdentifier: REQUIRED_TAGS
```

ConfigRule: Kunci akses diputar

Periksa apakah kunci akses sedang diputar dalam periode waktu yang ditentukan. Ini biasanya diatur menjadi 90 hari per persyaratan kepatuhan tipikal.

```
ConfigRuleName: access-keys-rotated
```

Description: >-

A config rule that checks whether the active access keys are rotated within the number of days specified in `maxAccessKeyAge`. The rule is `NON_COMPLIANT` if the access keys have not been rotated for more than `maxAccessKeyAge` number of days.

InputParameters:

`maxAccessKeyAge`: '90'

Source:

`Owner`: AWS

`SourceIdentifier`: `ACCESS_KEYS_ROTATED`

`MaximumExecutionFrequency`: `TwentyFour_Hours`

ConfigRule: Kunci akses root IAM di AMS

Periksa apakah kunci akses root tidak ada di akun. Untuk akun AMS Advanced, ini diharapkan sesuai. out-of-the-box

`ConfigRuleName`: `iam-root-access-key-check`

Description: >-

A config rule that checks whether the root user access key is available. The rule is `COMPLIANT` if the user access key does not exist.

Source:

`Owner`: AWS

`SourceIdentifier`: `IAM_ROOT_ACCESS_KEY_CHECK`

`MaximumExecutionFrequency`: `TwentyFour_Hours`

ConfigRule: SSM dikelola EC2

Periksa apakah Anda EC2s dikelola oleh SSM Systems Manager.

`ConfigRuleName`: `ec2-instance-managed-by-systems-manager`

Description: >-

A Config rule that checks whether the EC2 instances in the account are managed by AWS Systems Manager.

Scope:

`ComplianceResourceTypes`:

- `'AWS::EC2::Instance'`
- `'AWS::SSM::ManagedInstanceInventory'`

Source:

`Owner`: AWS

`SourceIdentifier`: `EC2_INSTANCE_MANAGED_BY_SSM`

ConfigRule: Pengguna IAM yang tidak digunakan di AMS

Periksa kredensial pengguna IAM yang belum digunakan selama durasi tertentu. Seperti pemeriksaan rotasi kunci, ini biasanya default hingga 90 hari per persyaratan kepatuhan tipikal.

```
ConfigRuleName: iam-user-unused-credentials-check
Description: >-
  A config rule that checks whether IAM users have passwords
  or active access keys that have not been used within the
  specified number of days provided.
InputParameters:
  maxCredentialUsageAge: '90'
Source:
  Owner: AWS
SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: Pencatatan ember S3

Periksa apakah logging telah diaktifkan untuk bucket S3 di akun.

```
ConfigRuleName: s3-bucket-logging-enabled
Description: >-
  A Config rule that checks whether logging is enabled for S3 buckets.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::Bucket'
Source:
  Owner: AWS
SourceIdentifier: S3_BUCKET_LOGGING_ENABLED
```

ConfigRule: Versi ember S3

Periksa apakah pembuatan versi dan MFA-delete (opsional) diaktifkan di semua bucket S3

```
ConfigRuleName: s3-bucket-versioning-enabled
Description: >-
  A Config rule that checks whether versioning is enabled for S3
  buckets. Optionally, the rule checks if MFA delete is enabled for S3 buckets.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::Bucket'
```

Source:

Owner: AWS

SourceIdentifier: S3_BUCKET_VERSIONING_ENABLED

ConfigRule: Akses publik S3

Periksa apakah pengaturan akses publik (ACL Publik, Kebijakan Publik, Bucket Publik) dibatasi di seluruh akun

ConfigRuleName: s3-account-level-public-access-blocks

Description: >-

A Config rule that checks whether the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item.

Scope:

ComplianceResourceTypes:

- 'AWS::S3::AccountPublicAccessBlock'

InputParameters:

IgnorePublicAcls: 'True'

BlockPublicPolicy: 'True'

BlockPublicAcls: 'True'

RestrictPublicBuckets: 'True'

Source:

Owner: AWS

SourceIdentifier: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

ConfigRule: Temuan yang tidak diarsipkan GuardDuty

Periksa GuardDuty temuan yang tidak diarsipkan yang lebih tua dari durasi yang ditentukan. Durasi default adalah 30 hari untuk low-sev, 7 hari untuk medium-sev dan 1 hari untuk temuan high-sev.

ConfigRuleName: guardduty-non-archived-findings

Description: >-

A Config rule that checks whether the Amazon GuardDuty has findings that are non archived. The rule is NON_COMPLIANT if GuardDuty has non archived low/medium/high severity findings older than the specified number.

InputParameters:

daysLowSev: '30'

daysMediumSev: '7'

daysHighSev: '1'

Source:

```
Owner: AWS
SourceIdentifier: GUARDDUTY_NON_ARCHIVED_FINDINGS
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: Penghapusan CMK

Periksa kunci master AWS Key Management Service kustom (CMKs) yang dijadwalkan (alias tertunda) untuk dihapus. Ini penting karena ketidaksadaran seputar penghapusan CMK dapat menyebabkan data tidak dapat dipulihkan

```
ConfigRuleName: kms-cmk-not-scheduled-for-deletion
Description: >-
  A config rule that checks whether customer master keys (CMKs) are not
  scheduled for deletion in AWS Key Management Service (AWS KMS). The rule is
  NON_COMPLIANT if CMKs are scheduled for deletion.
Source:
  Owner: AWS
SourceIdentifier: KMS_CMK_NOT_SCHEDULED_FOR_DELETION
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: Rotasi CMK

Periksa apakah rotasi otomatis diaktifkan untuk setiap CMK di akun

```
ConfigRuleName: cmk-backing-key-rotation-enabled
Description: >-
  A config rule that checks that key rotation is enabled for each customer
  master key (CMK). The rule is COMPLIANT, if the key rotation is enabled
  for specific key object. The rule is not applicable to CMKs that have
  imported key material.
Source:
  Owner: AWS
SourceIdentifier: CMK_BACKING_KEY_ROTATION_ENABLED
MaximumExecutionFrequency: TwentyFour_Hours
```

Pemberitahuan khusus untuk aturan Config

Mungkin ada kemunculan Aturan Konfigurasi kritis yang tidak sesuai yang mengharuskan peningkatan kesadaran secara langsung dengan tim Anda dan Kepemimpinan. InfoSec Untuk skenario seperti itu, AMS menyarankan Anda mengonfigurasi notifikasi kustom berbasis peristiwa ketidakpatuhan.

Misalnya:

```

ConfigRuleName: required-tags
  Description: >-
    A Config rule that checks whether EC2 instances have the mandated tags.
  Scope:
    ComplianceResourceTypes:
      - 'AWS::EC2::Instance'
  InputParameters:
    tag1Key: COST_CENTER
    tag2Key: APP_ID
  Source:
    Owner: AWS
SourceIdentifier: REQUIRED_TAGS
NotificationEventRule:
  Type: 'AWS::Events::Rule'
  Properties:
    Name: CWEventForrequired-tags
    Description: >-
      SNS Notification for Non-Compliant Events of Config Rule:
      required-tags
    State: ENABLED
    EventPattern:
      detail-type:
        - Config Rules Compliance Change
      source:
        - aws.config
      detail:
        newEvaluationResult:
          complianceType:
            - NON_COMPLIANT
        configRuleARN:
          - 'Fn::GetAtt':
            - RequiredEC2Tags
            - Arn
    Targets:
      - Id: RemediationNotification
        Arn:
          Ref: SnsTopic
        InputTransformer:
          InputTemplate: >-
            "EC2 Instance <Instance_ID> is non-compliant. Please add required tags:
            COST_CENTER, APP_ID, Name, and Backup."
          InputPathsMap:

```

```
        instance_id: $.detail.resourceId
SnsTopic:
  Type: 'AWS::SNS::Topic'
  Properties:
    Subscription:
      - Endpoint: Cloud_Ops_Leaders@customer.com
        Protocol: email
    TopicName: noncompliant-instance-notification
SnsTopicPolicy:
  Type: 'AWS::SNS::TopicPolicy'
  Properties:
    PolicyDocument:
      Statement:
        - Sid: __default_statement_ID
          Effect: Allow
          Principal:
            AWS: '*'
          Action:
            - 'SNS:GetTopicAttributes'
            - 'SNS:SetTopicAttributes'
            - 'SNS:AddPermission'
            - 'SNS:RemovePermission'
            - 'SNS:DeleteTopic'
            - 'SNS:Subscribe'
            - 'SNS:ListSubscriptionsByTopic'
            - 'SNS:Publish'
            - 'SNS:Receive'
          Resource:
            Ref: SnsTopic
          Condition:
            StringEquals:
              'AWS:SourceOwner':
                Ref: 'AWS::AccountId'
        - Sid: TrustCWEToPublishEventsToMyTopic
          Effect: Allow
          Principal:
            Service: events.amazonaws.com
          Action: 'sns:Publish'
          Resource:
            Ref: SnsTopic
  Topics:
    - Ref: SnsTopic
```


Peran terkait layanan EventBridge aturan Amazon untuk AMS Advanced

AMS Advanced menggunakan peran terkait layanan (SLR) bernama `AWSServiceRoleForManagedServices_Events`— Peran ini mempercayai salah satu kepala layanan AWS Managed Services (`events.managedservices.amazonaws.com`) untuk mengambil peran tersebut untuk Anda. Layanan menggunakan peran untuk membuat aturan EventBridge terkelola. Aturan ini adalah infrastruktur yang diperlukan di AWS akun Anda untuk mengirimkan informasi perubahan status alarm dari akun Anda ke AWS Managed Services.

Izin untuk EventBridge SLR untuk AMS Advanced

Peran tertaut layanan `AWSServiceRoleForManagedServices_Events` memercayai layanan berikut untuk mengambil peran tersebut:

- `events.managedservices.amazonaws.com`

Terlampir pada peran ini adalah kebijakan `AWSManagedServices_EventsServiceRolePolicy` AWS terkelola (lihat [kebijakan terkelola AWS: `AWSManagedServices\_EventsServiceRolePolicy`](#)). Layanan menggunakan peran untuk mengirimkan informasi perubahan status alarm dari akun Anda ke AWS Managed Services. Anda harus mengonfigurasi izin agar entitas IAM (seperti pengguna, grup, atau peran) dapat membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat [Izin Peran Tertaut Layanan di Panduan Pengguna](#) AWS Identity and Access Management.

Anda dapat mengunduh JSON `AWSManagedServices_EventsServiceRolePolicy` di ZIP ini: [EventsServiceRolePolicy.zip](#).

Membuat EventBridge SLR untuk AMS Advanced

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda Onboard ke AMS di AWS Management Console, Management Console AWS CLI, atau AWS API, AMS Advanced akan membuat peran terkait layanan untuk Anda.

Important

Peran terkait layanan ini dapat muncul di akun Anda jika Anda menggunakan layanan AMS Advanced sebelum 7 Februari 2023, ketika mulai mendukung peran terkait layanan, maka AMS Accelerate membuat peran tersebut di `AWSServiceRoleForManagedServices_Events` akun Anda. Untuk mempelajari lebih lanjut, lihat [Peran baru muncul di akun IAM saya](#).

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda Onboard ke AMS, AMS Advanced membuat peran terkait layanan untuk Anda lagi.

Mengedit EventBridge SLR untuk AMS Advanced

AMS Advanced tidak mengizinkan Anda mengedit peran `AWSServiceRoleForManagedServices_Events` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) dalam Panduan Pengguna IAM.

Menghapus EventBridge SLR untuk AMS Advanced

Anda tidak perlu menghapus peran `AWSServiceRoleForManagedServices_Events` secara manual. Saat Anda Offboard dari AMS di AWS Management Console, AWS CLI atau AWS API, AMS Advanced membersihkan sumber daya dan menghapus peran terkait layanan untuk Anda.

Anda juga dapat menggunakan konsol IAM, AWS CLI atau AWS API untuk menghapus peran terkait layanan secara manual. Untuk melakukannya, Anda harus membersihkan sumber daya untuk peran terkait layanan terlebih dahulu, lalu Anda dapat menghapusnya secara manual.

Note

Jika layanan AMS Advanced menggunakan peran saat Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya AMS Advanced yang digunakan oleh `AWSServiceRoleForManagedServices_Events` peran terkait layanan

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran `AWSServiceRoleForManagedServices_Events` terkait layanan.

Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan](#) dalam Panduan Pengguna IAM.

Praktik terbaik keamanan

Bagian ini telah disunting karena berisi informasi sensitif terkait keamanan AMS. Informasi ini tersedia melalui Dokumentasi konsol AMS. Untuk mengakses Artifact AWS, Anda dapat menghubungi CSDM Anda untuk mendapatkan petunjuk atau membuka [Memulai dengan Artifact AWS](#).

Pengaturan non-default EPS landing zone multi-akun AMS

Bagian ini telah disunting karena berisi informasi sensitif terkait keamanan AMS. Informasi ini tersedia melalui Dokumentasi konsol AMS. Untuk mengakses Artifact AWS, Anda dapat menghubungi CSDM Anda untuk mendapatkan petunjuk atau membuka [Memulai dengan Artifact AWS](#).

Pagar Pembatas AMS

Pagar pembatas adalah aturan tingkat tinggi yang menyediakan tata kelola berkelanjutan untuk lingkungan AMS Anda secara keseluruhan.

Bagian ini telah disunting karena berisi informasi sensitif terkait keamanan AMS. Informasi ini tersedia melalui Dokumentasi konsol AMS. Untuk mengakses Artifact AWS, Anda dapat menghubungi CSDM Anda untuk mendapatkan petunjuk atau membuka [Memulai dengan Artifact AWS](#).

Kebijakan kontrol layanan MALZ

Bagian ini telah disunting karena berisi informasi sensitif terkait keamanan AMS. Informasi ini tersedia melalui Dokumentasi konsol AMS. Untuk mengakses Artifact AWS, Anda dapat menghubungi CSDM Anda untuk mendapatkan petunjuk atau membuka [Memulai dengan Artifact AWS](#).

Respon Insiden Keamanan di AMS

Keamanan adalah prioritas utama di AWS Managed Services (AMS). AMS menyebarkan sumber daya dan kontrol di akun Anda untuk mengelolanya. AWS memiliki model tanggung jawab bersama: AWS mengelola keamanan cloud, dan Anda bertanggung jawab atas keamanan di cloud. AMS melindungi data dan aset Anda serta membantu menjaga AWS infrastruktur Anda tetap aman dengan menggunakan kontrol keamanan dan pemantauan aktif untuk masalah keamanan. Kemampuan ini membantu Anda menetapkan garis dasar keamanan untuk aplikasi yang berjalan di Cloud. AWS AMS bekerja sama dengan Anda melalui Security Incident Response untuk menilai efeknya, dan kemudian melakukan penahanan dan remediasi berdasarkan rekomendasi praktik terbaik.

Ketika penyimpangan dari baseline terjadi, seperti oleh kesalahan konfigurasi atau perubahan faktor eksternal, Anda perlu merespons dan menyelidiki. Agar berhasil melakukannya, Anda perlu memahami konsep dasar Respons Insiden Keamanan dalam lingkungan AMS Anda. Anda juga harus memahami persyaratan untuk mempersiapkan, mendidik, dan melatih tim cloud sebelum masalah keamanan terjadi. Penting untuk mengetahui kontrol dan kemampuan yang dapat Anda gunakan, menyiapkan rencana respons untuk masalah keamanan umum seperti kompromi akun pengguna atau penyalahgunaan akun istimewa, dan mengidentifikasi metode remediasi yang menggunakan otomatisasi untuk meningkatkan kecepatan dan konsistensi respons. Selain itu, Anda perlu memahami kepatuhan dan persyaratan peraturan Anda karena terkait dengan membangun program Respons Insiden Keamanan untuk memenuhi persyaratan tersebut.

Security Incident Response dapat menjadi kompleks, tetapi dengan menerapkan pendekatan berulang Anda dapat menyederhanakan proses dan memungkinkan tim respons insiden untuk menjaga pemangku kepentingan aset puas dengan memberikan deteksi dan respons dini dan berkelanjutan. Dalam panduan ini, kami memberi Anda metodologi yang digunakan AMS untuk respons insiden, matriks tanggung jawab AMS (RACI), bagaimana Anda dapat dipersiapkan untuk acara keamanan, cara melibatkan AMS selama insiden keamanan, dan beberapa runbook respons insiden yang digunakan AMS.

Cara kerja AMS Security Incident Response

AWS Managed Services selaras dengan [Panduan Penanganan Insiden Keamanan Komputer NIST 800-61 untuk Respons Insiden Keamanan](#). Dengan menyelaraskan standar industri ini, kami menyediakan pendekatan yang konsisten untuk manajemen acara keamanan dan mematuhi praktik terbaik dalam mengamankan dan menanggapi insiden keamanan di cloud Anda.

Siklus hidup respons insiden

Saat deteksi mengidentifikasi dan menghasilkan peringatan keamanan, atau Anda meminta bantuan keamanan, tim AWS Managed Services Operations memastikan bahwa ada investigasi tepat waktu, menjalankan otomatisasi untuk melakukan pengumpulan data, triase dan analisis, memberi tahu Anda tentang analisis, melakukan investigasi dan aktivitas penahanan apa pun, lalu memposting analisis peristiwa.

Pengumpulan data, triase, analisis, dan kegiatan penahanan yang dilakukan selama respons insiden bervariasi tergantung pada jenis peristiwa keamanan yang diselidiki. Contoh alur kerja Respons Insiden Keamanan untuk skenario tertentu ada di akhir dokumen ini.

Selama insiden, AMS menentukan tindakan yang benar secara dinamis, yang dapat mengakibatkan langkah-langkah yang didokumentasikan diurutkan ulang atau dilewati sebagaimana mestinya untuk memastikan bahwa hasil yang tepat terjadi.

Persiapkan

Seiring berkembangnya lanskap ancaman, AMS terus memperluas kemampuan deteksi dan respons. Saat deteksi baru ditambahkan, AMS menggabungkan peringatan dari deteksi baru ini ke dalam platform deteksi dan respons. Responden keamanan AMS dilatih untuk menyelidiki dan bermitra dengan Anda selama siklus hidup Respons Insiden Keamanan.

Karena pendekatan kemitraan ini, penting bagi tim keamanan dan aplikasi Anda untuk terlibat dengan AMS untuk menangani peristiwa keamanan saat peristiwa ini terjadi. Dokumentasi ini menjelaskan apa yang diharapkan selama acara keamanan dan membantu Anda mempersiapkan respons cepat ketika insiden keamanan terjadi.

Dokumentasi ini menggunakan definisi NIST 800-61 tentang suatu peristiwa sebagai kejadian yang dapat diamati dalam sistem atau jaringan dan insiden sebagai pelanggaran atau ancaman pelanggaran kebijakan, kebijakan penggunaan yang dapat diterima, atau praktik keamanan standar.

Daftar periksa persiapan

Kerjakan daftar periksa berikut dengan manajer pengiriman solusi cloud AMS (CSDM) dan arsitek cloud AMS (CA) Anda:

- Pahami beban kerja apa yang berjalan di akun mana.
- Pahami tim internal apa yang bertanggung jawab atas berbagai beban kerja dan beri tag dengan tepat di beban kerja.
- Pertahankan detail kontak secara internal untuk tim lain yang mungkin diperlukan selama investigasi acara keamanan dan untuk keputusan penahanan.
- Konfirmasikan bahwa kontak keamanan telah diperbarui dan ditambahkan ke semua AWS akun yang dikelola. Kontak dikelola berdasarkan per akun.
- Ketahui cara meningkatkan insiden keamanan ke AMS, dan ketahui tingkat keparahan dan waktu respons yang diharapkan.
- Pastikan bahwa ketika pemberitahuan keamanan diterima, mereka diarahkan ke orang dan sistem yang sesuai seperti pager atau pusat operasi keamanan Anda.
- Pahami sumber log apa yang tersedia untuk Anda, di mana ini disimpan di akun Anda dan siapa yang memiliki akses ke sana.

- Memahami cara menggunakan CloudWatch Wawasan untuk Kueri Log selama investigasi.
- Pahami opsi penahanan yang tersedia untuk Anda berdasarkan sumber daya (EC2, IAM, S3, dan son on) dan konsekuensi pada ketersediaan beban kerja Anda saat dalam penahanan.

Mendeteksi

Selama pengelolaan AWS akun Anda, AMS memantau anomali dalam perilaku pengguna, aktivitas akun, dan potensi peristiwa keamanan menggunakan data yang dikumpulkan dari sumber deteksi dan kontrol termasuk namun tidak terbatas pada Amazon, Amazon, GuardDuty VPC Flow Logs, CloudWatch Amazon Macie, dan AWS Config Amazon internal Threat Intelligence feed.

AMS menggunakan AWS layanan asli dan teknologi deteksi lainnya untuk merespons peristiwa keamanan yang dibuat oleh:

- Jenis Penemuan Kesesuaian Config
- GuardDuty Menemukan Jenis
- Jenis Penemuan Macie
- Amazon Route 53 Resolver Acara Firewall DNS
- Acara Keamanan AMS (alarm jam tangan cloud)

Temuan tambahan ditambahkan saat layanan, produk, dan ekosistem ancaman berkembang.

Laporkan peristiwa keamanan ke AMS

Mengajukan insiden melalui Portal atau Dukungan Pusat Dukungan AMS untuk memberi tahu AMS tentang insiden keamanan atau untuk meminta penyelidikan.

Analisis

Setelah peristiwa keamanan diidentifikasi dan dilaporkan, langkah selanjutnya adalah menganalisis apakah peristiwa yang dilaporkan adalah positif palsu atau insiden nyata. AMS menggunakan otomatisasi dan teknik investigasi manual untuk menangani peristiwa keamanan. Analisis ini mencakup investigasi log dari sumber deteksi yang berbeda seperti log lalu lintas jaringan, log host, CloudTrail peristiwa, log AWS layanan, dan sebagainya. Analisis juga mencari pola yang menunjukkan perilaku anomali dengan korelasi.

Kemitraan Anda diperlukan untuk memahami konteks khusus untuk lingkungan akun dan untuk menetapkan apa yang normal untuk akun dan beban kerja Anda. Ini membantu AMS mengidentifikasi anomali lebih cepat dan respons insiden yang dipercepat.

Menangani komunikasi dari AMS tentang peristiwa keamanan

AMS memberi Anda informasi selama penyelidikan dengan melibatkan kontak keamanan Anda melalui tiket insiden. Manajer pengiriman layanan cloud AMS (CSDM) dan arsitek cloud AMS (CA) Anda adalah titik kontak yang harus dihubungi untuk komunikasi apa pun selama penyelidikan keamanan aktif.

Komunikasi mencakup pemberitahuan otomatis ketika peringatan keamanan dihasilkan, komunikasi setelah analisis peristiwa, membangun jembatan panggilan dan pengiriman artefak yang sedang berlangsung seperti file log, snapshot sumber daya yang terinfeksi, dan mendapatkan hasil investigasi kepada Anda selama acara keamanan.

Bidang standar yang disertakan dalam pemberitahuan peringatan keamanan AMS tercantum di bawah ini. Bidang ini memberi Anda informasi sehingga Anda dapat merutekan acara ke tim yang sesuai dalam organisasi Anda untuk perbaikan.

- Menemukan Jenis
- Menemukan Pengenal (Jika relevan)
- Menemukan Tingkat Keparahan
- Menemukan Deskripsi
- Menemukan Tanggal & Waktu yang dibuat
- AWS Id Akun
- Wilayah (Jika relevan)
- AWS Sumber Daya (IAMuser/role/policy,, S3 EC2, EKS)

Bidang tambahan disediakan tergantung pada Jenis Temuan, misalnya Temuan EKS mencakup detail Pod, Container, dan Cluster.

Mengandung

Pendekatan AMS terhadap penahanan adalah kemitraan dengan Anda. Anda memahami bisnis Anda dan dampak beban kerja yang mungkin terjadi dari aktivitas penahanan, seperti isolasi jaringan, pengguna IAM atau de-penyediaan peran, pembangunan ulang instans, dan sebagainya.

Bagian penting dari penahanan adalah pengambilan keputusan. Misalnya, mematikan sistem, mengisolasi sumber daya dari jaringan, atau mematikan akses atau mengakhiri sesi. Keputusan ini lebih mudah dibuat jika ada strategi dan prosedur yang telah ditentukan untuk menahan insiden tersebut. AMS menyediakan strategi penahanan dan kemudian menerapkan solusi setelah Anda mempertimbangkan risiko yang terlibat dengan penerapan tindakan penahanan.

Ada opsi penahanan yang berbeda tergantung pada sumber daya yang dianalisis. AMS mengharapkan beberapa jenis penahanan akan dikerahkan secara bersamaan selama penyelidikan insiden. Beberapa contoh ini meliputi:

- Menerapkan aturan perlindungan untuk memblokir lalu lintas yang tidak sah (Grup keamanan, NACL, Aturan WAF, aturan SCP, Tolak daftar, pengaturan tindakan tanda tangan ke karantina atau blokir)
- Isolasi Sumber Daya
- Isolasi Jaringan
- Menonaktifkan pengguna, peran, dan kebijakan IAM
- Memodifikasi/Mengurangi pengguna IAM, hak istimewa peran
- Mengakhirkan/menangguhkan/menghapus sumber daya komputasi
- Membatasi akses publik dari sumber daya yang terpengaruh
- Memutar kunci akses, kunci API, dan kata sandi
- Menggosok kredensi yang diungkapkan dan informasi sensitif

AMS mendorong Anda untuk mempertimbangkan jenis strategi penahanan untuk setiap jenis insiden besar yang berada dalam selera risiko mereka, dengan kriteria yang didokumentasikan dengan jelas untuk membantu pengambilan keputusan jika terjadi insiden. Kriteria untuk menentukan strategi yang tepat meliputi:

- Potensi kerusakan sumber daya
- Pelestarian bukti
- Ketidaktersediaan layanan (misalnya, konektivitas jaringan, layanan yang diberikan kepada pihak eksternal)
- Waktu dan sumber daya yang dibutuhkan untuk mengimplementasikan strategi
- Efektivitas strategi (Misalnya, penahanan sebagian, penahanan penuh)
- Permanen solusi (Misalnya, keputusan pintu satu arah vs pintu dua arah)

- Durasi solusi (Misalnya, solusi darurat yang akan dihapus dalam empat jam, solusi sementara yang akan dihapus dalam dua minggu, solusi permanen).
- Terapkan kontrol keamanan yang dapat Anda aktifkan untuk menurunkan risiko dan memberikan waktu untuk menentukan dan menerapkan penahanan yang lebih efektif.

Kecepatan penahanan sangat penting, AMS menyarankan pendekatan bertahap untuk mencapai penahanan yang efisien dan efektif dengan menyusun strategi pendekatan jangka pendek dan jangka panjang.

Gunakan panduan ini untuk mempertimbangkan strategi penahanan Anda yang melibatkan teknik berbeda berdasarkan jenis sumber daya.

- Strategi Penahanan

- Dapatkah AMS mengidentifikasi ruang lingkup insiden keamanan?
 - Jika ya, identifikasi semua sumber daya (pengguna, sistem, sumber daya).
 - Jika tidak, selidiki secara paralel dengan mengeksekusi langkah berikutnya pada sumber daya yang diidentifikasi.
- Bisakah sumber daya diisolasi?
 - Jika ya, maka lanjutkan untuk mengisolasi sumber daya yang terpengaruh.
 - Jika tidak, maka bekerja dengan pemilik dan manajer sistem untuk menentukan tindakan lebih lanjut yang diperlukan untuk mengatasi masalah.
- Apakah semua sumber daya yang terpengaruh terisolasi dari sumber daya yang tidak terpengaruh?
 - Jika ya, lanjutkan ke langkah berikutnya.
 - Jika tidak, maka teruslah mengisolasi sumber daya yang terkena dampak sampai penahanan jangka pendek dicapai untuk mencegah insiden meningkat lebih lanjut.
- Sistem Backup
 - Apakah salinan cadangan dari sistem yang terpengaruh dibuat untuk analisis lebih lanjut?
 - Apakah salinan forensik dienkripsi dan disimpan di lokasi yang aman?
 - Jika ya, lanjutkan ke langkah berikutnya.
 - Jika tidak, enkripsi gambar forensik, lalu simpan di lokasi yang aman untuk mencegah penggunaan, kerusakan, dan gangguan yang tidak disengaja.

Membasmi

Setelah insiden diatasi, pemberantasan mungkin diperlukan untuk menghilangkan sumber ancaman sama sekali untuk mengamankan sistem sebelum Anda melanjutkan ke tahap pemulihan berikutnya. Langkah-langkah pemberantasan mungkin termasuk menghapus malware dan menghapus akun pengguna yang disusupi, serta mengidentifikasi dan mengurangi semua kerentanan yang dieksploitasi. Selama pemberantasan, penting untuk mengidentifikasi semua akun, sumber daya, dan contoh yang terpengaruh dalam lingkungan sehingga dapat diperbaiki.

Ini adalah praktik terbaik bahwa pemberantasan dan pemulihan dilakukan secara bertahap sehingga langkah-langkah remediasi diprioritaskan. Untuk insiden skala besar, pemulihan mungkin memakan waktu berbulan-bulan. Maksud dari fase awal harus meningkatkan keamanan secara keseluruhan dengan perubahan nilai tinggi yang relatif cepat (hari ke minggu) untuk mencegah insiden di masa depan. Fase selanjutnya harus fokus pada perubahan jangka panjang (misalnya, perubahan infrastruktur) dan pekerjaan yang sedang berlangsung untuk menjaga perusahaan seaman mungkin.

Untuk beberapa insiden, pemberantasan tidak diperlukan atau dilakukan selama pemulihan.

Pertimbangkan hal berikut:

- Dapatkah sistem dicitrakan ulang dan kemudian dikeraskan dengan tambalan atau tindakan pencegahan lainnya untuk mencegah atau mengurangi risiko serangan?
- Apakah semua malware dan artefak lainnya yang ditinggalkan oleh penyerang dihapus dan sistem yang terpengaruh mengeras terhadap serangan lebih lanjut?

Memulihkan

AMS bermitra dengan Anda untuk memulihkan sistem ke operasi normal, mengonfirmasi bahwa sistem berfungsi normal, dan (sebagaimana berlaku) memulihkan kerentanan untuk mencegah insiden serupa.

Pertimbangkan hal berikut:

- Apakah sistem yang terpengaruh ditambah dan dikeraskan terhadap serangan baru-baru ini dan kemungkinan serangan future?
- Hari dan waktu apa yang layak untuk mengembalikan sistem yang terkena dampak kembali ke produksi?

- Alat apa yang akan Anda gunakan untuk menguji, memantau, dan memverifikasi bahwa sistem yang Anda kembalikan ke produksi tidak rentan terhadap teknik serangan awal?

Laporan Pasca Insiden

Setelah acara, AMS menjalankan proses peninjauan investigasi untuk semua insiden keamanan. Dan, AMS memulai proses koreksi kesalahan (COE) untuk mengatasi insiden keamanan yang disebabkan oleh sistem atau kesalahan prosedural yang masuk akal memiliki ruang untuk perbaikan. AMS bermitra dengan Anda untuk terus meningkatkan pengalaman investigasi keamanan. Proses COE membantu AMS mengidentifikasi faktor-faktor yang berkontribusi dari peristiwa yang berdampak pada pelanggan dan menghubungkan penyebab tersebut ke item tindakan berikutnya yang dapat mencegah kejadian serupa berulang, atau membantu mengurangi durasi atau tingkat dampak.

Proses peninjauan investigasi untuk insiden keamanan membahas hal-hal berikut untuk mengidentifikasi peluang perbaikan:

- Berapa waktu yang telah berlalu dari awal insiden hingga penemuan insiden, hingga penilaian dampak awal, dan untuk setiap tahap proses penanganan insiden (misalnya, penahanan, pemulihan)?
- Berapa lama waktu yang dibutuhkan tim respons insiden untuk menanggapi laporan awal insiden tersebut?
- Berapa lama waktu yang dibutuhkan untuk melakukan analisis dampak awal?
- Apakah ini bisa dicegah dan bagaimana caranya? Apakah ada alat atau proses yang bisa mencegah hal ini?
- Bisakah kita mendeteksi ini lebih cepat dan bagaimana?
- Apa yang bisa membuat penyelidikan berjalan lebih cepat?
- Apakah Prosedur Respons Insiden yang terdokumentasi diikuti? Apakah mereka memadai?
- Apakah berbagi informasi dengan pemangku kepentingan lain dilakukan tepat waktu Bagaimana itu bisa diperbaiki?
- Apakah kolaborasi dengan tim lain (AWS Keamanan, tim akun, tim AWS Pengembangan, dan tim keamanan pelanggan) efektif? Jika tidak, apa yang bisa diperbaiki?
- Langkah persiapan apa yang hilang yang mungkin membantu, matriks eskalasi, RACI, model tanggung jawab bersama, dan sebagainya? Apakah ada kebutuhan untuk memperbarui Runbook?
- Apa perbedaan antara penilaian dampak awal dan penilaian dampak akhir? Apa yang dapat kita lakukan untuk meningkatkan akurasi penilaian sebelumnya dalam respons insiden?

- Apa Item Tindakan dari Pelajaran yang Dipetik?

Runbook Respons Insiden Keamanan di AMS

Bagian ini berisi dua runbook:

- [Respon terhadap aktivitas pengguna root](#)
- [Respon terhadap peristiwa malware](#)

Respon terhadap aktivitas pengguna root

[Pengguna root](#) adalah superuser di dalam AWS akun Anda. Perhatikan bahwa AMS memantau penggunaan root. Ini adalah praktik terbaik untuk menggunakan pengguna root hanya untuk beberapa tugas yang memerlukannya, seperti mengubah pengaturan akun Anda, mengaktifkan akses AWS Identity and Access Management (IAM) ke penagihan dan manajemen biaya, mengubah kata sandi root Anda, dan mengaktifkan otentikasi multi-faktor (MFA). Untuk informasi selengkapnya, lihat [Tugas yang memerlukan kredensi pengguna root](#).

Untuk informasi selengkapnya tentang cara menginformasikan AMS tentang penggunaan root yang direncanakan, lihat [Kapan dan cara menggunakan akun root di AMS](#).

Ketika aktivitas pengguna root terdeteksi, upaya gagal untuk masuk yang mungkin menunjukkan serangan brute force atau aktivitas di akun setelah login berhasil, peristiwa yang dihasilkan, dan insiden yang dikirim ke kontak keamanan yang Anda tentukan.

AWS Managed Services Operations menyelidiki aktivitas pengguna root yang tidak direncanakan, melakukan pengumpulan data, triase, dan analisis, serta melakukan aktivitas penahanan sesuai arahan Anda, diikuti dengan analisis pasca peristiwa.

Jika Anda memiliki model operasi AMS Advanced, Anda menerima komunikasi tambahan dari insinyur AMS CSDM dan AMS Ops yang mengonfirmasi aktivitas pengguna root yang tidak direncanakan karena tanggung jawab AMS untuk mengamankan kredensial pengguna root. AMS menyelidiki aktivitas pengguna root hingga Anda mengonfirmasi jalur ke depan.

Persiapkan

Beri tahu AMS tentang penggunaan pengguna root yang direncanakan dengan mengirimkan permintaan layanan AMS dengan data dan waktu acara yang direncanakan untuk mencegah aktivitas respons insiden yang tidak perlu.

Lakukan secara berkala GameDays dengan AMS untuk memvalidasi proses respons insiden pelanggan AMS, orang dan sistem terkini, dan membangun memori otot dengan individu yang bertanggung jawab untuk mencapai respons insiden yang lebih cepat.

Fase A: Mendeteksi

AMS memantau aktivitas root di akun melalui sumber deteksi termasuk GuardDuty dan pemantauan AMS.

Jika Anda memiliki AMS Accelerate, model operasi merespons insiden yang meminta penyelidikan untuk aktivitas pengguna root yang tidak terduga. Ketika ini terjadi, Operasi AMS memulai runbook Akun Terkompromi.

Jika Anda memiliki AMS Advanced, model operasi merespons insiden tersebut, atau memberi tahu CSDM tentang aktivitas pengguna root yang direncanakan untuk menghentikan investigasi Kompromi Akun yang aktif.

Fase B: Analisis

AMS melakukan penyelidikan menyeluruh terhadap peristiwa pengguna root ketika ditentukan bahwa aktivitas tersebut tidak diotorisasi. Menggunakan otomatisasi dan tim respons keamanan AMS, log dan peristiwa dianalisis untuk anomali dan perilaku tak terduga bagi pengguna root. Log diberikan kepada Anda untuk membantu menentukan apakah aktivitas tersebut tidak diketahui, atau apakah itu adalah peristiwa pengguna root resmi, atau jika memerlukan penyelidikan lebih lanjut.

Beberapa contoh informasi yang diberikan selama penyelidikan untuk mendukung pemeriksaan internal meliputi:

- Informasi akun: Akun apa yang digunakan akun root?
- Alamat e-mail untuk pengguna root: Setiap pengguna root dikaitkan dengan alamat e-mail dari organisasi Anda
- Detail otentikasi: Dari mana dan kapan pengguna root mengakses lingkungan Anda?
- Catatan aktivitas: Apa yang dilakukan pengguna saat masuk sebagai root? Catatan-catatan ini dalam bentuk CloudWatch peristiwa. Memahami cara membaca log ini membantu dalam penyelidikan.

Ini adalah praktik terbaik bahwa Anda siap menerima informasi analisis dan memiliki rencana bagaimana mencapai titik kontak resmi untuk akun dalam organisasi Anda. Karena pengguna root tidak disebut sebagai individu, menentukan siapa yang memiliki akses ke alamat email root yang

digunakan untuk akun dalam organisasi Anda membantu merutekan pertanyaan secara internal dengan cepat.

Fase C: Mengandung dan Membasmi

AMS bermitra dengan tim keamanan Anda untuk melakukan penahanan sesuai arahan kontak Keamanan Pelanggan resmi Anda. Opsi penahanan meliputi:

- Memutar kredensi dan kunci yang sesuai.
- Mengakhiri sesi aktif ke akun dan sumber daya.
- Memberantas sumber daya yang dibuat.

Selama aktivitas penahanan, AMS bekerja sama dengan tim keamanan Anda untuk memastikan setiap gangguan pada beban kerja Anda diminimalkan dan kredensial root diamankan dengan tepat.

Setelah rencana penahanan selesai, Anda bekerja dengan tim Operasi AMS untuk tindakan pemulihan apa pun yang diperlukan.

Laporan Pasca Insiden

Sebagaimana diperlukan, AMS memulai proses peninjauan investigasi untuk mengidentifikasi pelajaran apa pun yang dipetik. Sebagai bagian dari penyelesaian COE, AMS mengkomunikasikan temuan yang relevan kepada pelanggan yang terkena dampak untuk membantu mereka meningkatkan proses respons insiden mereka.

AMS mendokumentasikan semua detail akhir investigasi, mengumpulkan metrik yang sesuai, dan kemudian melaporkan insiden tersebut ke tim internal AMS mana pun yang memerlukan informasi, termasuk CSDM dan CA yang Anda tetapkan.

Respon terhadap peristiwa malware

EC2 Instans Amazon digunakan untuk menampung berbagai beban kerja termasuk perangkat lunak pihak ketiga dan perangkat lunak yang dikembangkan khusus yang digunakan oleh tim aplikasi dalam organisasi. AMS menyediakan dan mendorong Anda untuk menerapkan beban kerja Anda pada gambar yang ditambah dan dipelihara secara berkelanjutan oleh AMS.

Selama pengoperasian instance, AMS memantau anomali perilaku atau aktivitas melalui berbagai kontrol deteksi keamanan, termasuk Amazon, Endpoint Protection, Network GuardDuty Traffic, dan Amazon internal Threat Intelligence feed.

Pelanggan AMS dengan model operasi AMS Advanced secara otomatis menginstal klien pemantauan keamanan titik akhir (EPS) pada sumber daya yang disediakan. Ini memastikan bahwa sumber daya dipantau dan didukung 24x7, termasuk pembuatan insiden keamanan ketika suatu peristiwa terdeteksi.

AMS juga memantau Temuan GuardDuty Malware. Ini tersedia di AMS Advanced dan AMS Accelerate, jika diaktifkan. Lihat [Perlindungan Malware di Amazon GuardDuty](#) untuk informasi selengkapnya.

Note

Jika Anda memilih [Bring Your Own EPS](#), maka proses untuk respons insiden berbeda dari apa yang diuraikan di halaman ini. Untuk informasi lebih lanjut, lihat dokumentasi yang direferensikan.

Ketika malware terdeteksi, insiden dibuat dan Anda diberitahu tentang peristiwa tersebut. Pemberitahuan ini diikuti oleh aktivitas remediasi apa pun yang terjadi. Operasi AMS menyelidiki, melakukan pengumpulan data, triase dan analisis, dan kemudian melakukan aktivitas penahanan sesuai arahan Anda, diikuti dengan analisis pasca peristiwa.

Fase A: Mendeteksi

AMS memantau peristiwa pada instans dengan GuardDuty dan pemantauan solusi keamanan titik akhir. AMS menentukan aktivitas pengayaan dan triase yang sesuai untuk membantu Anda membuat keputusan penahanan atau penerimaan risiko berdasarkan temuan atau jenis peringatan.

Pengumpulan data dilakukan berdasarkan jenis temuan. Pengumpulan data melibatkan kueri beberapa sumber data baik di dalam maupun di luar akun yang terpengaruh untuk membangun gambaran aktivitas yang diamati atau konfigurasi yang menjadi perhatian.

AMS melakukan korelasi temuan dengan alarm dan peringatan atau telemetri lain dari akun yang terkena dampak atau platform intelijen ancaman AMS.

Fase B: Analisis

Setelah data dikumpulkan, data dianalisis untuk mengidentifikasi aktivitas atau indikator yang menjadi perhatian. Selama fase penyelidikan ini, AMS bermitra dengan Anda untuk mengintegrasikan pengetahuan bisnis dan domain tentang instans dan beban kerja untuk membantu memahami apa yang diharapkan dan apa yang tidak biasa.

Beberapa contoh informasi yang diberikan selama penyelidikan untuk mendukung pemeriksaan internal meliputi:

- Informasi Akun: Di akun apa aktivitas malware diamati?
- Detail Instance: Instance apa yang terlibat dengan peristiwa malware?
- Stempel waktu acara: Kapan peringatan dipicu?
- Informasi Beban Kerja: Apa yang berjalan pada instance?
- Detail malware, jika relevan: Keluarga malware dan informasi Open Source tentang malware.
- Pengguna atau Rincian Peran: Pengguna atau peran apa yang dipengaruhi oleh dan terlibat dalam aktivitas?
- Catatan Aktivitas: Aktivitas apa yang direkam pada instance? Ini dalam bentuk CloudWatch peristiwa, dan peristiwa sistem dari instance. Memahami cara membaca log ini akan membantu Anda dalam penyelidikan
- Aktivitas Jaringan: Titik akhir apa yang terhubung ke instance, apa yang terhubung dengan instance, dan apa analisis lalu lintas?

Merupakan praktik terbaik untuk bersiap menerima informasi investigasi, dan memiliki rencana tentang cara menghubungi titik kontak yang sesuai untuk akun, contoh, dan beban kerja dalam organisasi Anda. Memahami topologi jaringan Anda dan koneksi yang diharapkan dapat membantu mempercepat analisis dampak. Pengetahuan tentang pengujian penetrasi yang direncanakan di lingkungan dan penerapan terbaru yang dilakukan oleh pemilik aplikasi juga dapat mempercepat penyelidikan.

Jika Anda menentukan bahwa kegiatan tersebut direncanakan dan diotorisasi, maka insiden tersebut diperbarui dan penyelidikan berakhir. Jika kompromi dikonfirmasi, maka Anda dan AMS menentukan rencana penahanan yang sesuai.

Phace C: Mengandung dan Membasmi

AMS bermitra dengan Anda untuk menentukan aktivitas penahanan yang sesuai berdasarkan data yang dikumpulkan dan informasi yang diketahui. Opsi penahanan termasuk tetapi tidak terbatas pada:

- Melestarikan data melalui snapshot
- Memodifikasi aturan jaringan untuk membatasi lalu lintas masuk atau keluar dari instance
- Memodifikasi kebijakan pengguna dan peran SCP, IAM untuk membatasi akses

- Mengakhiri, Menangguhkan, atau Mematikan Instans
- Mengakhiri koneksi persisten
- Memutar kredensial/kunci yang sesuai

Jika Anda memilih untuk melakukan aktivitas pemberantasan terhadap instans, AMS mendukung Anda dalam mencapai hal ini. Opsi termasuk, tetapi tidak terbatas pada:

- Menghapus perangkat lunak yang tidak diinginkan
- Membangun kembali instance dari gambar yang sepenuhnya ditambal dan menerapkan ulang aplikasi dan konfigurasi
- Memulihkan instance dari cadangan sebelumnya
- Menyebarkan aplikasi dan layanan ke instance lain dalam akun Anda yang mungkin cocok untuk meng-host beban kerja.

Penting untuk menentukan bagaimana malware dikirimkan dan dijalankan pada instance sebelum pemulihan layanan untuk memastikan bahwa setiap kontrol tambahan diterapkan untuk mencegah terulangnya malware pada instance. AMS memberikan wawasan atau informasi tambahan kepada mitra atau tim forensik Anda yang diperlukan untuk mendukung forensik.

Pada titik ini, Anda bekerja dengan Operasi AMS untuk kegiatan pemulihan. AMS bekerja sama dengan Anda untuk meminimalkan gangguan pada beban kerja dan mengamankan instans.

Laporan Pasca Insiden

Sesuai kebutuhan, AMS memulai proses peninjauan investigasi untuk mengidentifikasi pelajaran yang dipetik. Sebagai bagian dari menyelesaikan COE, AMS mengkomunikasikan temuan yang relevan kepada Anda untuk membantu Anda meningkatkan proses respons insiden Anda.

AMS mendokumentasikan rincian akhir investigasi, mengumpulkan metrik yang sesuai, dan melaporkan insiden tersebut ke tim internal AMS yang memerlukan informasi, termasuk CSDM dan CA yang Anda tetapkan.

Ubah ulasan keamanan permintaan di AMS Advanced

Proses peninjauan permintaan perubahan AWS Managed Services memastikan bahwa AMS melakukan tinjauan keamanan terhadap perubahan yang diminta saat diterapkan atas nama Anda di akun Anda.

[AMS Standar teknis lanjutan](#) tentukan kriteria keamanan minimum, konfigurasi, dan proses untuk menetapkan keamanan dasar akun Anda. Saat AMS menerapkan perubahan yang diminta, kami mengikuti standar ini.

AMS mengevaluasi semua permintaan perubahan terhadap standar teknis AMS. Setiap perubahan yang dapat menurunkan postur keamanan akun Anda dengan menyimpang dari standar teknis akan melalui proses peninjauan keamanan. Selama proses ini, risiko yang relevan disorot oleh AMS dan ditinjau serta disetujui oleh pemberi persetujuan risiko resmi Anda untuk menyeimbangkan keamanan dan kebutuhan bisnis.

Proses Manajemen Risiko Keamanan Pelanggan

Proses AMS Advanced Customer Security Risk Management (CSRM) membantu mengidentifikasi dan mengkomunikasikan risiko dengan jelas kepada pemilik yang tepat. Proses ini meminimalkan risiko keamanan di lingkungan Anda dan mengurangi overhead operasional yang sedang berlangsung untuk risiko yang teridentifikasi.

Secara default, ketika seseorang dari organisasi Anda meminta agar AMS menerapkan perubahan pada lingkungan terkelola Anda, AMS meninjau perubahan tersebut untuk menentukan apakah permintaan tersebut berada di luar standar teknis, yang dapat mengubah postur keamanan akun Anda. Jika ada risiko keamanan yang tinggi atau sangat tinggi, maka tinjauan perubahan diterima atau ditolak oleh petugas keamanan resmi Anda. Perubahan yang diminta juga dievaluasi untuk efek buruk pada kemampuan AMS untuk mengoperasikan akun. Jika tinjauan menemukan kemungkinan dampak buruk, maka ulasan dan persetujuan tambahan diperlukan dalam AMS.

Anda dapat memilih keluar dari alur kerja berbasis persetujuan dalam proses CSRM untuk risiko tinggi atau sangat tinggi. Untuk mengubah opsi CSRM untuk akun tertentu dari CSRM Standar ke Hanya Pemberitahuan, bekerjalah dengan Manajer Pengiriman Layanan Cloud Anda untuk membuat penerimaan risiko satu kali. Jika Anda memilih untuk melanjutkan dengan opsi Notifikasi Saja, AMS menerapkan perubahan yang diminta terlepas dari kategori risiko. Dan, AMS mengirimkan pemberitahuan risiko kepada pemberi persetujuan risiko resmi Anda alih-alih meminta persetujuan sebelum implementasi perubahan. Bicaralah dengan Cloud Architects atau Cloud Service Delivery Manager untuk informasi selengkapnya tentang proses CSRM AMS, cara mengubah opsi CSRM default saat melakukan onboarding akun AMS baru, atau cara memperbarui akun yang ada.

 Note

AMS sangat menyarankan agar Anda menggunakan opsi default CSRM Standar di semua akun Anda.

AMS Standar teknis lanjutan

Berikut ini adalah kategori standar teknis AMS Advanced:

ID	Kategori
AMS-STD-001	Konfigurasi Penandaan
AMS-STD-002	AWS Identity and Access Management
AMS-STD-003	Keamanan Jaringan
AMS-STD-004	Pengujian Penetrasi
AMS-STD-005	Amazon GuardDuty
AMS-STD-006	Keamanan Host
AMS-STD-007	Pencatatan
AMS-STD-008	AMS-MARAH
AMS-STD-009	Lain-lain

Kontrol standar di AMS Advanced

Berikut ini adalah kontrol standar di AMS:

AMS-STD-001 - Konfigurasi Penandaan

Berikut ini adalah kontrol standar untuk 001 - Tagging Configuration.

1. Semua AWS sumber daya yang dibutuhkan oleh tim AMS untuk tujuan operasional dan manajemen harus memiliki pasangan nilai kunci berikut.

- AppId= AMSInfrastructure
 - Lingkungan= AMSInfrastructure
 - AppName = AMSInfrastructure
 - AMSResource=Benar
2. Semua tag yang diperlukan oleh tim AMS selain yang tercantum sebelumnya harus memiliki awalan seperti yang disebutkan dalam daftar awalan AMS (lihat Catatan).
 3. Nilai tag yang diperlukan oleh tim AMS (AppId, Lingkungan, dan AppName) dapat diubah pada salah satu sumber daya yang dibuat oleh Anda berdasarkan permintaan perubahan Anda.
 4. Tag apa pun pada tumpukan yang diperlukan oleh AMS tidak boleh dihapus berdasarkan permintaan perubahan Anda.
 5. Anda tidak dapat menggunakan konvensi penamaan tag AMS untuk infrastruktur Anda, seperti yang disebutkan di poin 2.
 6. Anda dapat membuat tag kustom di sumber daya yang diperlukan oleh AMS (biasanya untuk kasus penggunaan penagihan dan pelaporan biaya). Tag kustom dipertahankan jika sumber daya diperbarui oleh pembaruan tumpukan dan bukan dengan memperbarui template.

Note

Daftar Awalan AMS

1. ams-*
2. AWSManagedLayanan*
3. /ams/ *
4. am*
5. AM*
6. Ams*
7. mc*
8. MC*
9. Mc*
- 10.sentinel*
- 11.Sentinel*
- 12.Managed_Services*

13NEWAMS*
 14AWS_*
 15aw*
 16VPC_*
 17.CloudTrail*
 18.Cloudtrail*
 19/aws_reserved/
 20MENELAN*
 21EPSDB*
 22MMS*
 23.TemplateId*
 24.StackSet-am*
 25.StackSet-AWS-Zona Pendaratan
 26.IAMPolicy*
 27.pelanggan-mc-*
 28.Akar*
 29.LandingZone*
 30.StateMachine*
 31.codedeploy_service_role
 32.managementhost
 33.sentinel.int.
 34.eps
 35.UnhealthyInServiceBastion
 36.ms-

AMS-STD-002 - (IAM) AWS Identity and Access Management

ID	Standar teknis

ID	Standar teknis
1.1	Sesi batas waktu default pengguna federasi adalah satu jam dan dapat ditingkatkan hingga empat jam.
1.2	Waktu Akses Stack Default adalah 12 jam.
2.0	AWS Penggunaan Akun Root
2.1	Jika ada penggunaan akun root karena alasan apa pun, Amazon GuardDuty harus dikonfigurasi untuk menghasilkan temuan yang relevan.
2.2	Untuk akun single-account landing zone (SALZ) dan akun manajemen multi-account landing zone (MALZ) (sebelumnya dikenal sebagai Master/Billing akun), akun pengguna Root harus mengaktifkan MFA virtual dan token lunak MFA dibuang selama akun on-boarding, sehingga AMS maupun pelanggan tidak dapat masuk sebagai root. Proses kehilangan kata sandi AWS root standar harus diikuti bersama dengan AMS Cloud Service Delivery Manager (CSDM) Anda. Konfigurasi ini harus tetap ada selama siklus hidup akun terkelola AMS.
2.3	Anda tidak boleh membuat kunci akses untuk akun root.
3.0	Pembuatan dan Modifikasi Pengguna
3.1	IAM users/roles dengan akses terprogram dan dengan izin baca saja dapat dibuat tanpa kebijakan terbatas waktu. Namun, izin untuk mengizinkan pembacaan objek (misalnya, S3:GetObject) di semua bucket Amazon Simple Storage Service di akun tidak diizinkan.

ID	Standar teknis
3.1.1	Pengguna manusia IAM untuk akses konsol dan dengan izin baca saja dapat dibuat dengan kebijakan terikat waktu (hingga 180 hari) sedangkan kebijakan terikat waktu akan menghasilkan pemberitahuan risiko. removal/renewal/extension Namun, izin untuk mengizinkan pembacaan objek (misalnya, S3:GetObject) di semua ember S3 di akun tidak diizinkan.
3.2	Pengguna IAM dan peran untuk konsol dan akses terprogram dengan izin mutasi infrastruktur apa pun (manajemen tulis dan izin) di akun pelanggan tidak boleh dibuat tanpa penerimaan risiko. Ada pengecualian untuk izin tulis tingkat objek S3 yang diizinkan tanpa penerimaan risiko selama bucket tertentu berada dalam cakupan dan operasi penandaan pada tag terkait non-AMS.
3.3	Pengguna IAM dengan akses terprogram, diberi nama <code>customer_servicenow_user</code> dan <code>customer_servicenow_logging_user</code> diperlukan untuk ServiceNow integrasi dalam akun aplikasi SALZ atau MALZ dan *akun inti* dapat dibuat tanpa kebijakan terbatas waktu.

ID	Standar teknis
3.4	Pengguna IAM dengan akses terprogram, menggunakan <code>customer_cloud_endure_policy</code> dan <code>customer_cloud_endure_deny_policy</code> (dengan akses hanya-baca) yang diperlukan untuk CloudEndure integrasi dalam akun SALZ dan MALZ dapat dibuat tetapi memerlukan kebijakan terbatas waktu untuk periode migrasi yang direncanakan. Batas waktu bisa untuk jangka waktu maksimum 180 hari tanpa RA. SCP juga berwenang untuk perubahan akun MALZ agar kebijakan ini berfungsi selama periode yang diperlukan. Anda menentukan jendela migrasi yang sesuai untuk kebutuhan Anda dan menyesuaikan sesuai kebutuhan.
4.0	Kebijakan, Tindakan, dan APIs
4.1	Semua pengguna dan peran IAM Anda di akun SALZ harus memiliki Kebijakan Penolakan Pelanggan (CDP) default yang dilampirkan untuk melindungi infrastruktur AMS dari kerusakan yang tidak disengaja atau disengaja.
4.2	AMS SCPs harus diaktifkan di semua akun terkelola AMS di MALZ.
4.3	Identitas yang mampu melakukan tindakan administratif pada kunci KMS, seperti, dan <code>PutKeyPolicy</code> <code>ScheduleKeyDeletion</code> , harus dibatasi hanya untuk operator AMS dan prinsip otomatisasi.

ID	Standar teknis
4.4	Kebijakan tidak boleh memberikan akses administrator dengan pernyataan yang setara dengan “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*” tanpa penerimaan risiko.
4,5	Kebijakan IAM tidak boleh menyertakan tindakan apa pun yang mencakup tindakan Izinkan S3: *** pada bucket apa pun tanpa penerimaan risiko.
4.6	Panggilan API terhadap kebijakan kunci KMS untuk kunci infrastruktur AMS dalam kebijakan IAM pelanggan tidak boleh diizinkan.
4.7	Tindakan yang melewati proses manajemen perubahan (RFC) tidak boleh diizinkan, seperti memulai atau menghentikan instance, pembuatan bucket S3 atau instance RDS, dan sebagainya.
4.8	Tindakan yang membuat perubahan pada catatan DNS infrastruktur AMS di Amazon Route 53 tidak boleh diizinkan.
4.9	Pengguna manusia IAM dengan akses konsol yang dibuat setelah mengikuti proses hukum, tidak boleh memiliki kebijakan apa pun yang dilampirkan secara langsung kecuali kebijakan kepercayaan, peran, dan kebijakan terbatas waktu.
4.10	Profil EC2 instans Amazon dengan akses baca ke rahasia atau namespace tertentu di AWS Secrets Manager dalam akun yang sama dapat dibuat.

ID	Standar teknis
4.11	Izin AWS Managed Services Change Management (AMSCM) atau AWS Managed Services Service Knowledge Management System (AMSSKMS) dapat ditambahkan ke peran apa pun (kemampuan untuk membuka). SR/Incident/RFC
4.12	Kebijakan IAM tidak boleh menyertakan tindakan apa pun yang mencakup tindakan Izinkan log: DeleteLogGroup dan log: DeleteLogStream pada grup CloudWatch log AMS Amazon mana pun.
4.13	Izin untuk membuat kunci Multi-wilayah tidak boleh diizinkan.
4.14	Untuk menyediakan akses ke bucket S3 ARNs yang belum dibuat di akun Anda, gunakan kunci kondisi S3 khusus layanan s3:ResourceAccount untuk menentukan nomor akun.
4.15	Anda dapat melihat, membuat, membuat daftar, dan menghapus akses ke dasbor khusus Anda, tetapi hanya melihat dan mencantumkan akses di CloudWatch dasbor Amazon.
4.15.1	Anda dapat melihat, membuat, membuat daftar, dan menghapus akses ke dasbor kustom lensa penyimpanan S3 Anda.
4.16	Izin penuh terkait SQL Workbench dapat diberikan roles/users untuk bekerja di database Amazon Redshift.
4.17	AWS CloudShell Izin apa pun dapat diberikan kepada peran pelanggan sebagai alternatif CLI.

ID	Standar teknis
4.18	Peran IAM dengan Layanan AWS sebagai prinsipal tepercaya juga harus sesuai dengan standar teknis IAM.
4.19	Peran Tertaut Layanan (SLRs) tidak tunduk pada standar teknis AMS IAM, karena dibuat dan dikelola oleh Tim Layanan IAM.
4.20	Kebijakan IAM tidak boleh mengizinkan akses baca tak terbatas ke objek bucket Amazon S3 (misalnya, Amazon S3GetObject:) di semua bucket dalam akun: • Di akun mode Pengembang: Pelanggaran menghasilkan Pemberitahuan Risiko • Di akun mode non-pengembang: Pelanggaran memerlukan Penerimaan Risiko
4.21	Semua izin IAM untuk jenis sumber daya “savingsplan” dapat diberikan kepada pelanggan.
4.22	Insinyur AMS tidak diizinkan untuk menyalin atau memindahkan data pelanggan (file, objek S3, database) secara manual di salah satu layanan penyimpanan data, seperti Amazon S3, Amazon Relational Database Service, Amazon DynamoDB, dan sebagainya, atau dalam sistem file OS.
4.23	Kebijakan SCP tidak boleh dimodifikasi untuk mengizinkan akses tambahan apa pun di salah satu akun yang dikelola AMS.

ID	Standar teknis
4.24	Setiap perubahan dalam kebijakan SCP yang mungkin merusak infrastruktur AMS atau kemampuan manajemen tidak boleh diizinkan. (Catatan: Sumber daya AMS memiliki tag AppId= AMSInfrastructure dan mengikuti AMS Protected Namespace).
4.25	Fitur Penyediaan IAM Otomatis AMS harus diaktifkan di akun Anda sebagai fitur keikutsertaan.
4.26	Peran atau pengguna yang diasumsikan manusia AMS tidak boleh memiliki akses ke konten pelanggan di S3, RDS, DynamoDB, Redshift, ElastiCache, EFS, dan FSx Selain itu, akses apa pun ke yang diketahui dan baru APIs dirilis oleh pihak lain Layanan AWS yang memberikan akses ke konten pelanggan harus ditolak secara eksplisit dalam peran operator.
5.0	Federasi
5.1	Otentikasi harus dikonfigurasi menggunakan federasi di akun terkelola AMS.
5.2	Harus ada kepercayaan keluar satu arah dari AMS AD ke direktori aktif Anda (AMS AD mempercayai AD di prem).
5.3	Penyimpanan identitas Anda yang digunakan untuk mengautentikasi ke AMS tidak boleh ada di akun aplikasi terkelola AMS.
6.0	Kebijakan Lintas Akun

ID	Standar teknis
6.1	Kebijakan kepercayaan peran IAM antara akun AMS yang dimiliki oleh pelanggan yang sama sesuai catatan pelanggan, dapat dikonfigurasi.
6.2	Kebijakan kepercayaan peran IAM antara akun AMS dan non-AMS harus dikonfigurasi hanya jika akun non-AMS dimiliki oleh pelanggan AMS yang sama (dengan mengonfirmasi bahwa akun tersebut berada di bawah AWS Organizations akun yang sama atau dengan mencocokkan domain email dengan nama perusahaan pelanggan).
6.3	Kebijakan kepercayaan peran IAM antara akun AMS dan akun pihak ketiga tidak boleh dikonfigurasi tanpa penerimaan risiko.
6.4	Kebijakan lintas akun untuk mengakses semua yang dikelola pelanggan CMKs antara akun AMS dari pelanggan yang sama dapat dikonfigurasi.
6.5	Kebijakan lintas akun untuk mengakses kunci KMS apa pun dalam akun non-AMS oleh akun AMS dapat dikonfigurasi.
6.6	Kebijakan lintas akun untuk mengakses kunci KMS apa pun dalam akun AMS oleh akun pihak ketiga tidak boleh diizinkan tanpa penerimaan risiko.
6.6.1	Kebijakan lintas akun untuk mengakses kunci KMS apa pun dalam akun AMS oleh akun non-AMS hanya dapat dikonfigurasi jika akun non-AMS dimiliki oleh pelanggan AMS yang sama.

ID	Standar teknis
6.7	Kebijakan lintas akun untuk mengakses data bucket S3 atau sumber daya tempat data dapat disimpan (seperti Amazon RDS, Amazon DynamoDB, atau Amazon Redshift) antara akun AMS dari pelanggan yang sama dapat dikonfigurasi.
6.8	Kebijakan lintas akun untuk mengakses data bucket S3 atau sumber daya tempat data dapat disimpan (seperti Amazon RDS, Amazon DynamoDB, atau Amazon Redshift) di akun non-AMS dari akun AMS dengan akses hanya-baca dapat dikonfigurasi.
6.9	Kebijakan lintas akun untuk mengakses data bucket S3 atau sumber daya di mana data dapat disimpan (seperti Amazon RDS, Amazon DynamoDB, atau Amazon Redshift) dengan izin menulis dari AMS ke akun non-AMS (atau akun non-AMS ke AMS) harus dikonfigurasi hanya jika akun non-AMS dimiliki oleh pelanggan AMS yang sama (dengan mengonfirmasi bahwa mereka berada di bawah AWS Organizations akun yang sama atau dengan mencocokkan email domain dengan nama perusahaan pelanggan).
6.10	Kebijakan lintas akun untuk mengakses data bucket S3 atau sumber daya tempat data dapat disimpan (seperti Amazon RDS, Amazon DynamoDB, atau Amazon Redshift) di akun pihak ketiga dari akun AMS dengan akses hanya baca dapat dikonfigurasi.

ID	Standar teknis
6.11	Kebijakan lintas akun untuk mengakses data bucket S3 atau sumber daya tempat data dapat disimpan (seperti Amazon RDS, Amazon DynamoDB, atau Amazon Redshift) di akun pihak ketiga dari akun AMS dengan akses tulis tidak boleh dikonfigurasi.
6.12	Kebijakan lintas akun dari akun pihak ketiga untuk mengakses bucket S3 pelanggan AMS atau sumber daya tempat data dapat disimpan (seperti Amazon RDS, Amazon DynamoDB, atau Amazon Redshift) tidak boleh dikonfigurasi tanpa penerimaan risiko.
7.0	Grup Pengguna
7.1	Grup IAM dengan izin readonly dan non mutatif diizinkan.
8.0	Kebijakan berbasis sumber daya
8.1	Sumber daya infrastruktur AMS harus dilindungi dari manajemen oleh identitas yang tidak sah dengan lampiran kebijakan berbasis sumber daya.
8.2	Sumber daya Anda harus dikonfigurasi dengan kebijakan berbasis sumber daya dengan hak istimewa terkecil, kecuali Anda secara eksplisit menentukan kebijakan yang berbeda.
9.0	Layanan penyediaan layanan mandiri (SSPS)

ID	Standar teknis
9.1	Peran atau kebijakan IAM default AMS (termasuk profil instans, SSPS, pola) tidak boleh dimodifikasi dengan atau tanpa penerimaan risiko apa pun. Pengecualian diperbolehkan (tanpa penerimaan risiko) untuk kebijakan kepercayaan. Penandaan peran, kebijakan, atau perubahan pengguna, juga diizinkan dalam peran SSP default.
9.3	Kebijakan SSPS untuk peran konsol Systems Manager Automation tidak dapat dilampirkan ke peran kustom apa pun selain dari peran default. Kebijakan SSPS lainnya hanya boleh dilampirkan ke peran IAM kustom setelah memastikan lampiran kebijakan ke peran kustom tidak memberikan izin tambahan di luar desain yang dimaksudkan untuk layanan SSPS default.

AMS-STD-003 - Keamanan Jaringan

Berikut ini adalah kontrol standar untuk 003 - Keamanan Jaringan:

ID	Standar teknis
	Jaringan
1.0	Semua EC2 instance harus diakses melalui SSH atau RDP hanya melalui host Bastion, rentang VPC CIDR host bastion atau dari rentang VPC CIDR instance yang sama.
2.0	IP elastis pada EC2 instans diizinkan
3.0	Bidang kontrol AMS dan dengan ekstensi di bidang data TLS 1.2+ harus digunakan.

ID	Standar teknis
4.0	Semua lalu lintas keluar harus lewat menggunakan akun IGW atau TGW.
5.0	Grup keamanan tidak boleh memiliki sumber sebagai 0.0.0.0/0 dalam aturan masuk jika tidak dilampirkan ke penyeimbang beban sesuai 9.0
6.0	Bucket atau objek S3 tidak boleh dipublikasikan tanpa penerimaan risiko.
7.0	Akses manajemen server pada port SSH/22 atau SSH/2222 (Bukan SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/5900-5901 TS/CITRIX/1494 atau 1604, LDAP/389 atau 636 dan RPC/135, NETBIOS/137-139 tidak boleh diizinkan dari luar VPC melalui kelompok keamanan.
8.0	Akses manajemen basis data pada port (MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433) atau pada port khusus tidak boleh diizinkan dari publik yang tidak dirutekan ke VPC melalui DX, VPC-peer, atau VPN melalui grup keamanan. IPs
8.1	Sumber daya apa pun di mana data pelanggan dapat disimpan tidak boleh diekspos ke internet publik secara langsung.
9.0	Akses aplikasi langsung melalui port HTTP/80, HTTPS/8443 dan HTTPS/443 dari Internet hanya diizinkan untuk memuat penyeimbang, tetapi tidak untuk sumber daya komputasi apa pun secara langsung, misalnya, instance, kontainer, dll. EC2 ECS/EKS/Fargate

ID	Standar teknis
10.0	Akses aplikasi melalui port HTTP/80 dan HTTPS/443 dari rentang IP pribadi pelanggan dapat diizinkan.
11.0	Setiap perubahan pada grup keamanan yang mengontrol akses ke infrastruktur AMS tidak boleh diizinkan tanpa penerimaan risiko.
12.0	AMS Security mengacu pada standar setiap kali grup keamanan diminta untuk dilampirkan ke sebuah instans.
13.0	Akses benteng pelanggan pada port 3389 dan 22 harus diizinkan hanya dari rentang IP Pribadi yang dialihkan ke VPC melalui DX, VPC-peer, atau VPN.
14.0	Asosiasi lintas akun zona yang dihosting pribadi dengan VPCs dari AMS ke akun non-AMS (atau akun non-AMS ke AMS) harus dikonfigurasi hanya jika akun non-AMS dimiliki oleh pelanggan AMS yang sama (dengan mengonfirmasi bahwa akun tersebut berada di bawah akun AWS Organization yang sama atau dengan mencocokkan domain email dengan nama perusahaan pelanggan) menggunakan alat internal.
15.0	Koneksi peering VPC antar akun milik pelanggan yang sama dapat diizinkan.

ID	Standar teknis
16.0	Basis AMS AMIs dapat dibagikan dengan akun non-AMS selama kedua akun dimiliki oleh pelanggan yang sama (dengan mengonfirmasi bahwa mereka berada di bawah AWS Organizations akun yang sama atau dengan mencocokkan domain email dengan nama perusahaan pelanggan) menggunakan alat internal.
17.0	Port FTP 21 tidak boleh dikonfigurasi di salah satu grup keamanan tanpa penerimaan risiko.
18.0	Konektivitas jaringan lintas akun melalui gateway transit diizinkan selama semua akun dimiliki oleh pelanggan.
19.0	Membuat subnet pribadi ke publik tidak diizinkan
20.0	Koneksi peering VPC dengan akun pihak ketiga (tidak dimiliki oleh pelanggan) tidak boleh diizinkan.
21.0	Lampiran Transit Gateway dengan akun pihak ketiga (tidak dimiliki oleh pelanggan) tidak boleh diizinkan.
22.0	Setiap lalu lintas jaringan yang diperlukan untuk AMS untuk menyediakan layanan kepada pelanggan tidak boleh diblokir di titik keluar jaringan pelanggan.
23.0	Berbagi aturan resolver dengan Akun AWS dimiliki oleh pelanggan yang sama diperbolehkan dengan pemberitahuan risiko
19.0	ICMP

ID	Standar teknis
19.1	Permintaan ICMP masuk ke Amazon EC2 dari infra pelanggan akan memerlukan pemberitahuan risiko.
19.2	Permintaan masuk dari publik yang IPs dialihkan ke Amazon VPC melalui DX, VPC-peer, atau VPN melalui grup keamanan diperbolehkan.
19.3	Permintaan masuk dari publik yang IPs tidak diarahkan ke Amazon VPC melalui DX, VPC-peer, atau VPN melalui grup keamanan akan memerlukan penerimaan risiko.
19.4	Permintaan ICMP keluar dari Amazon EC2 ke tujuan mana pun diizinkan.
20.0	Berbagi kelompok keamanan
20.1	Jika grup keamanan memenuhi standar keamanan ini, maka grup tersebut dapat dibagi antara VPCs di akun yang sama dan antar akun di organisasi yang sama.
20.2	Jika grup keamanan tidak memenuhi standar ini dan penerimaan risiko sebelumnya diperlukan untuk grup keamanan ini, maka penggunaan fitur berbagi grup keamanan antara VPCs di akun yang sama, atau antar akun di organisasi yang sama, tidak diizinkan tanpa penerimaan risiko untuk VPC atau akun baru itu.

AMS-STD-004 - Pengujian Penetrasi

Berikut ini adalah kontrol standar untuk 004 - Pengujian Penetrasi

1. AMS tidak mendukung infrastruktur pentest. Ini adalah tanggung jawab pelanggan. Misalnya, Kali bukan distribusi Linux yang didukung AMS.
2. Pelanggan harus mematuhi [Pengujian Penetrasi](#).
3. AMS harus diberitahu sebelumnya 24 jam sebelumnya dalam kasus ketika pelanggan ingin melakukan pengujian penetrasi infrastruktur dalam akun.
4. AMS akan menyediakan infrastruktur pentesting pelanggan sesuai kebutuhan pelanggan yang secara eksplisit dinyatakan dalam permintaan perubahan atau permintaan layanan oleh pelanggan.
5. Manajemen identitas untuk infrastruktur pentesting pelanggan adalah tanggung jawab pelanggan.

AMS-STD-005 - GuardDuty

Berikut ini adalah kontrol standar untuk 005 - GuardDuty

1. GuardDuty harus diaktifkan di semua akun pelanggan setiap saat.
2. GuardDuty Temuan dari Akun Aplikasi Terkelola Pelanggan (CMA) di MALZ tidak akan menghasilkan alarm untuk tim operasi.
3. GuardDuty peringatan harus disimpan dalam akun yang sama atau akun terkelola lainnya di bawah organisasi yang sama.
4. Fitur daftar IP tepercaya tidak GuardDuty boleh digunakan. Sebaliknya pengarsipan otomatis dapat digunakan sebagai alternatif, yang berguna untuk tujuan audit.
5. GuardDuty delegasi administrator tidak boleh diaktifkan di MALZ karena administrator yang didelegasikan akan dapat melakukan tindakan hak istimewa tinggi seperti menonaktifkan akun lain tanpa penerimaan GuardDuty risiko.
6. GuardDuty Filter Arsip Otomatis harus menggunakan cakupan minimal untuk pengembalian maksimum. Misalnya, jika AMS akan melihat beberapa yang tidak dapat diprediksi IPs di blok CIDR yang berbeda, dan ada ASN perusahaan yang sesuai untuk digunakan, gunakan ASN. Namun, jika Anda dapat menjangkau rentang tertentu atau alamat /32, maka cakupannya.

AMS-STD-006 - Keamanan Host

Berikut ini adalah kontrol standar untuk 006 - Host Security

- Agen anti-virus harus berjalan pada semua EC2 kasus setiap saat. (misalnya, Trend Micro DSM).
- Modul anti-malware harus diaktifkan.

- Agen EPS harus menyertakan semua direktori dan file untuk pemindaian.
- File yang dikarantina oleh solusi anti-virus dapat dibagikan dengan Anda sesuai permintaan.
- Solusi keamanan endpoint pihak ketiga tidak boleh diinstal.
- Frekuensi pembaruan tanda tangan anti-virus harus diatur setidaknya sekali dalam sehari.
- Frekuensi pemindaian terjadwal harus diatur setidaknya sekali dalam sebulan.
- Pemindaian real-time (on-access) harus diaktifkan dan dijalankan setiap saat.
- AMS tidak boleh menjalankan skrip kustom apa pun yang tidak dimiliki atau ditulis oleh AMS pada instans Anda. (Catatan: Anda dapat melakukannya dengan menggunakan akses Admin tumpukan melalui CT akses Stack Admin atau dengan menggunakan [AWS Systems Manager Automation \(AMS SSPS\)](#)).
- Network Level Authentication (NLA) tidak boleh dinonaktifkan pada host windows.
- Sistem operasi host harus up to date dengan patch keamanan terbaru sesuai siklus patch yang dikonfigurasi.
- Akun terkelola AMS tidak boleh memiliki instans yang tidak dikelola di akun.
- Pembuatan akun administrator lokal pada instans Anda oleh AMS tidak boleh diizinkan.
- Pasangan kunci pada tidak EC2 boleh dibuat.
- Anda tidak boleh menggunakan sistem operasi yang dinyatakan sebagai End of Life (EOL) dan tidak ada dukungan keamanan lebih lanjut yang diberikan oleh vendor atau pihak ketiga.

AMS-STD-007 - Penebangan

Berikut ini adalah kontrol standar untuk 007 - Logging

ID	Standar teknis
1.0	Jenis log
1.1	Log OS: Semua host harus log pada acara otentikasi host minimum, mengakses peristiwa untuk semua penggunaan hak istimewa yang ditinggikan dan peristiwa akses untuk semua perubahan pada konfigurasi akses dan hak istimewa termasuk keberhasilan dan kegagalan keduanya.

ID	Standar teknis
1.2	AWS CloudTrail: pencatatan peristiwa CloudTrail manajemen harus diaktifkan dan dikonfigurasi untuk mengirimkan log ke bucket S3.
1.3	VPC Flow Logs: Semua log lalu lintas jaringan harus dicatat melalui VPC Flow Logs.
1.4	Pencatatan Akses Server Amazon S3: Ember S3 yang diamanatkan AMS yang menyimpan log harus mengaktifkan pencatatan akses server.
1.5	AWS Config Snapshots: AWS Config harus merekam perubahan konfigurasi untuk semua sumber daya yang didukung di semua wilayah dan mengirimkan file snapshot konfigurasi ke bucket S3 setidaknya sekali per hari.
1.6	Log Sistem Perlindungan Titik Akhir (EPS): Pencatatan solusi EPS harus diaktifkan dan dikonfigurasi untuk mengirimkan log ke grup CloudWatch log Log.
1.7	Log Aplikasi: Pelanggan diberdayakan untuk mengaktifkan pencatatan di aplikasi mereka dan menyimpannya di grup CloudWatch log Log atau bucket S3.
1.8	Pencatatan level objek S3: Pelanggan diberdayakan untuk mengaktifkan pencatatan level objek di bucket S3 mereka.
1.9	Service Logging: Pelanggan diberdayakan untuk mengaktifkan dan meneruskan log untuk layanan SSPS seperti layanan inti lainnya.

ID	Standar teknis
1.10	Log Elastic Load Balancing (Classic/Applicati on Load Balancer/NetworkLoad Balancer): Entri akses dan log kesalahan harus disimpan di bucket S3 yang dikelola AMS 2.0.
2.0	Kontrol akses
2.1	Anda tidak boleh memiliki akses tulis atau hapus di bucket S3 yang diperlukan oleh AMS yang menyimpan log dan log; CloudWatch grup log.
2.2	Anda harus memiliki akses read-only ke semua log di akun Anda.
2.3	Bucket S3 yang diamankan AMS yang menyimpan log tidak boleh mengizinkan pengguna akun pihak ketiga sebagai prinsip dalam kebijakan bucket.
2.4	Log dari grup CloudWatch log Log tidak boleh dihapus tanpa persetujuan eksplisit dari kontak keamanan resmi Anda.
3.0	Retensi log
3.1	Grup CloudWatch log log yang diamankan AMS harus memiliki periode retensi minimum 90 hari pada log.
3.2	Ember S3 yang diamankan AMS yang menyimpan log harus memiliki periode retensi minimum 18 bulan pada log.
3.3	AWS Backup snapshot harus tersedia dengan retensi minimum 31 hari pada sumber daya yang didukung.

ID	Standar teknis
4.0	Enkripsi
4.1	Enkripsi harus diaktifkan di semua bucket S3 yang diperlukan oleh Tim AMS yang menyimpan log.
4.2	Setiap penerusan log dari akun pelanggan ke akun lain harus dienkripsi.
5.0	Integritas
5.1	Mekanisme integritas file log harus diaktifkan. "Validasi file log" harus dikonfigurasi di AWS CloudTrail jalur yang diperlukan oleh tim AMS.
6.0	Penerusan log
6.1	Setiap log dapat diteruskan dari satu akun AMS ke akun AMS lain dari pelanggan yang sama.
6.2	Setiap log dapat diteruskan dari AMS ke akun non-AMS hanya jika akun non-AMS dimiliki oleh pelanggan AMS yang sama.
6.3	Setiap log dari akun pelanggan tidak boleh diteruskan ke akun pihak ketiga (yang tidak dimiliki oleh pelanggan).

AMS-STD-008 - AMS-MAD

Berikut ini adalah kontrol standar untuk 008 - AMS-MAD

ID	Standar teknis
1.0	Manajemen Akses

ID	Standar teknis
1.1	Hanya pengguna istimewa AMS dengan login interaktif dan tugas otomatisasi yang harus diizinkan masuk ke host manajemen untuk administrasi AD terkelola di akun pelanggan.
1.2	Admin AD hanya boleh memiliki hak administrator yang didelegasikan (Grup Administrator Delegasi AMS).
1.3	Insinyur yang masuk ke lingkungan AD pelanggan (host manajemen atau instans) harus memiliki akses terikat waktu.
1.4	Pelanggan hanya membaca akses ke objek AD menggunakan Alat Administrator Server Jarak Jauh dalam sebuah EC2 instance.
1.5	Hak administratif untuk pengguna atau grup direktori aktif tidak boleh diizinkan.
1.6	AWS Berbagi direktori dengan yang Akun AWS dimiliki oleh pelanggan yang sama diperbolehkan dengan pemberitahuan risiko.
2.0	Akun layanan
2.1	Akun Layanan Terkelola Grup (GMSA) harus digunakan di mana pun didukung oleh aplikasi, bukan akun layanan standar.
2.2	Semua akun layanan lainnya harus dibuat setelah proses penerimaan risiko.

ID	Standar teknis
2.3	Grup Keamanan AD tidak boleh digunakan kembali kecuali diminta secara eksplisit oleh pelanggan. Grup AD baru harus dibuat. Objek komputer yang meminta akses ke akun layanan harus ditambahkan ke grup keamanan baru.
2.4	Setiap akun layanan GMSA harus ditambahkan di bawah Unit Organisasi (OU) “Akun Layanan Terkelola”.
2.5	Setiap akun layanan non-GMSA harus ditambahkan di bawah OU “Pengguna → Akun Layanan”.
3.0	Objek Kebijakan Grup (GPO)
3.1	Pengaturan apa pun di bawah GPO “Pengaturan Windows> Pengaturan Keamanan” tidak boleh dimodifikasi jika mengurangi postur keamanan akun dengan cara apa pun dari keadaan saat ini.
3.2	Di MALZ, RFCs dikirimkan dari akun aplikasi yang meminta pembuatan GPO, GPO harus ditautkan ke OU yang sesuai dengan akun Aplikasi. Semua GPOs yang memengaruhi semua akun harus berasal dari akun Layanan Bersama.
3.3	Waktu habis Sesi Idle RDP default harus diatur ke 15 menit untuk semua server di bawah domain direktori aktif.
4.0	Kepercayaan Direktori Aktif

ID	Standar teknis
4.1	Kepercayaan keluar satu arah (Direktori yang di-host AMS ke Direktori Pelanggan) diizinkan jika forwarder bersyarat dialihkan ke VPC melalui DX, VPC-peer, atau VPN. IPs
5.0	Lainnya
5.1	Mekanisme integritas file log harus diaktifkan. "Validasi file log" harus dikonfigurasi di AWS CloudTrail jalur yang diperlukan oleh tim AMS.
6.0	Penerusan log
6.1	Pengguna pelanggan, grup, objek komputer, OU atau entitas lain tidak boleh menggunakan konvensi penamaan AMS sesuai konvensi penamaan AMS.
6.2	Semua OUs harus dikelola oleh AMS.

AMS-STD-009 - Miscellaneous

Berikut ini adalah kontrol standar untuk 009 - Miscellaneous

- Jika enkripsi diaktifkan dalam sumber daya, objek, database, atau sistem file, itu tidak boleh dinonaktifkan.

Perubahan yang menimbulkan risiko keamanan tinggi atau sangat tinggi di lingkungan Anda

Perubahan berikut menimbulkan risiko keamanan yang tinggi atau sangat tinggi di lingkungan Anda:

AWS Identity and Access Management

- High_risk-iam-001: Buat kunci akses untuk akun root
- High_risk-IAM-002: Modifikasi kebijakan SCP untuk memungkinkan akses tambahan

- High_risk-IAM-003: Modifikasi kebijakan SCP yang dapat merusak infrastruktur AMS
- High_risk-IAM-004: Pembuatan a role/user dengan izin mutasi infrastruktur (tuliskan, manajemen izin atau penandaan) di akun pelanggan
- High_risk-IAM-005: Kebijakan kepercayaan peran IAM antara akun AMS dan akun pihak ketiga (tidak dimiliki oleh pelanggan)
- High_risk-IAM-006: Kebijakan lintas akun untuk mengakses kunci KMS apa pun dari akun AMS oleh akun pihak ketiga)
- High_risk-IAM-007: Kebijakan lintas akun dari akun pihak ketiga untuk mengakses bucket S3 pelanggan AMS atau sumber daya tempat data dapat disimpan (seperti Amazon RDS, Amazon DynamoDB, atau Amazon Redshift)
- High_risk-IAM-008: Tetapkan izin IAM dengan izin mutasi infrastruktur apa pun di akun pelanggan
- High_risk-IAM-009: Izinkan daftar dan membaca di semua bucket S3 di akun
- High_risk-IAM-010: Penyediaan IAM Otomatis dengan izin read/write

Keamanan jaringan

- High_risk-net-001: Buka port manajemen OS SSH/22 atau SSH/2222 (Bukan SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/5900-5901 TS/CITRIX/1494 atau 1604, LDAP/389 atau 636 dan NETBIOS/137-139 dari internet
- High_risk-net-002: Buka port manajemen database MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433 atau port pelanggan manajemen apa pun dari internet
- High_risk-net-003: Buka port aplikasi HTTP/80, HTTPS/8443 dan HTTPS/443 pada sumber daya komputasi apa pun secara langsung. Misalnya, EC2 instance, ECS/EKS/Fargate kontainer, dan sebagainya dari internet
- High_risk-net-004: Setiap perubahan pada grup keamanan yang mengontrol akses ke infrastruktur AMS
- High_risk-net-006: VPC mengintip dengan akun pihak ketiga (tidak dimiliki oleh pelanggan)
- High_risk-net-007: Menambahkan firewall pelanggan sebagai titik keluar untuk semua lalu lintas AMS
- High_risk-net-008: Lampiran Transit Gateway dengan akun pihak ketiga tidak diperbolehkan
- High_Risk-S3-001: Menyediakan atau mengaktifkan akses publik di bucket S3

Pencatatan

- High_risk-log-001: Nonaktifkan. CloudTrail (Diperlukan Persetujuan Manajer Situs Operasi)
- High_risk-log-002: Nonaktifkan Log Aliran VPC. (Diperlukan Persetujuan Manajer Situs Operasi)
- High_risk-log-003: Penerusan log melalui metode apa pun (pemberitahuan acara S3, penarikan agen SIEM, push agen SIEM dll) dari akun yang dikelola AMS ke akun pihak ketiga (tidak dimiliki oleh pelanggan)
- High_risk-log-004: Gunakan jejak non-AMS untuk CloudTrail

Keamanan Host

- High_risk-host-001: Nonaktifkan Keamanan Titik Akhir di akun untuk alasan apa pun. (Diperlukan Persetujuan Manajer Situs Operasi)
- High_risk-host-002: Nonaktifkan patching di sumber daya atau di tingkat akun.
- High_risk-host-003: Menerapkan instance yang tidak dikelola di akun. EC2
- High_risk-host-004: Menjalankan skrip khusus yang disediakan oleh pelanggan.
- High_risk-host-005: Pembuatan akun Administrator Lokal pada instance.
- High_risk-host-006: Jenis file Trend Micro EPS/pengecualian pemindaian ekstensi atau menonaktifkan perlindungan malware pada titik akhir.

Note

Penerimaan risiko tidak diperlukan untuk pengecualian anti-malware EPS atau aturan GuardDuty Suppression yang terkait dengan tes penetrasi atau pemindaian kerentanan atau layanan yang memengaruhi events/known masalah kinerja yang menjamin tindakan proaktif. Pemberitahuan risiko sudah cukup dalam situasi ini.

- High_risk-host-007: Buat untuk KeyPair EC2
- High_risk-host-008: Nonaktifkan Keamanan Titik Akhir di EC2
- High_risk-host-009: Akun yang menggunakan OS End of Life (EOL)

Lain-lain

- High_risk-enc-001: Nonaktifkan enkripsi di sumber daya apa pun jika diaktifkan

Direktori Aktif Terkelola

- High_risk-AD-001: Memberikan hak admin kepada pengguna atau grup direktur aktif
- High_risk-AD-002: Kebijakan GPO yang mampu mengurangi postur keamanan akun

Manajemen kontinuitas di AMS Advanced

Sebagai bagian dari manajemen kontinuitas, AWS Managed Services (AMS) menyediakan akses otomatis ke AWS Backup, layanan asli dengan AWS. Ini memfasilitasi akses ke layanan yang mendukung Amazon EBS, Amazon, Amazon RDS EC2, Amazon EFS, dan banyak lagi.

Untuk mempelajari lebih lanjut, lihat [AWS Backup: Cara Kerjanya](#).

Topik

- [Apa itu manajemen kontinuitas?](#)
- [Bagaimana manajemen kontinuitas bekerja](#)
- [Respon pemulihan bencana](#)
- [Perencanaan pemulihan bencana](#)

Apa itu manajemen kontinuitas?

Manajemen kontinuitas adalah proses yang digunakan AMS untuk menyediakan cadangan dan snapshot untuk akun Anda.

AMS menyediakan akses ke AWS Backup melalui jenis perubahan yang Anda gunakan untuk membuat dan mengelola pekerjaan dan rencana cadangan.

Bagaimana manajemen kontinuitas bekerja

AMS digunakan [AWS Backup](#) untuk manajemen kontinuitas.

Saat mulai bekerja dengan AWS Backup di AMS:

1. Jalankan cadangan sesuai permintaan
2. Buat paket cadangan (opsional, AMS menyediakan paket cadangan default)
3. Gunakan AMS default dan brankas cadangan (opsional)
4. Kelola (jalankan, perbaiki, hapus, dan sebagainya) rencana cadangan dan titik pemulihan Anda

Paket cadangan AMS

Rencana cadangan adalah ekspresi kebijakan yang menentukan kapan dan bagaimana Anda ingin mencadangkan sumber daya AWS yang didukung, seperti database RDS, volume EBS, tabel DynamoDB, dan sistem file EFS. Kebijakan penjadwalan dan penyimpanan dikelola melalui paket pencadangan khusus, yang dapat Anda buat menggunakan jenis perubahan (CT) dengan AMS Advanced atau gunakan AWS Backup dengan AMS Accelerate. Tetapkan sumber daya ke paket cadangan Anda menggunakan tag dan AWS Backup secara otomatis mencadangkan dan mempertahankan cadangan untuk sumber daya yang ditetapkan sesuai dengan rencana cadangan yang ditentukan. Anda dapat membuat beberapa rencana pencadangan jika Anda memiliki beban kerja dengan berbagai persyaratan cadangan.

Rencana cadangan dapat memiliki hingga enam aturan cadangan yang menentukan jadwal dan periode retensi, di antara detail lainnya. Jadwal pencadangan menentukan kapan AWS Backup memulai pekerjaan cadangan dan seberapa sering cadangan dibuat. Anda dapat memilih frekuensi per jam, harian, mingguan, atau bulanan. Pengaturan hari penghapusan menentukan berapa hari snapshot disimpan sebelum dihapus secara otomatis.

Note

AMS Advanced: Jika Anda bermigrasi dari sistem cadangan AMS lama, AMS akan membuat paket cadangan default untuk kompatibilitas mundur. Pasangan kunci:value dalam skenario ini adalah Backup:True. Untuk mendukung kompatibilitas mundur, nilai di sini tidak peka huruf besar/kecil, jadi Backup:True atau Backup:True adalah semua tag yang valid. Semua pasangan kunci:value lainnya peka huruf besar/kecil.

AWS Backup dapat beroperasi pada tingkat volume EBS atau di tingkat EC2 instans Amazon, tetapi tidak melakukan keduanya pada saat yang sama, karena ini dapat menyebabkan kondisi balapan di mana cadangan dapat berbenturan.

Paket cadangan default, landing zone multi-akun

Selama RFC pembuatan Akun baru, AMS memastikan bahwa ada paket cadangan default menyeluruh di tingkat akun untuk melindungi beban kerja Anda. Nilai untuk bidang wajib ditetapkan secara default, seperti yang ditunjukkan pada bagian berikut:

Paket cadangan AMS default

default-backup-plan

Kunci TAG: Backup

Nilai TAG: True

```
RuleForDailyBackups schedule expression: cron(30 23 ? * *) (a daily backup for 23:30
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(30 23 ? * 7 *) (a weekly backup for
23:30 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(30 23 * ? *) (a monthly backup for
23:30 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(30 23 1 1 ? *) (a yearly backup for
23:30 UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Paket cadangan AMS default	Waktu Mulai	Penyimpanan
cadangan per jam	N/A	N/A
cadangan harian	setiap hari 11:30 WIB UTC	7 hari
cadangan mingguan	mingguan 23:30 UTC, hanya pada hari Sabtu	4 minggu
cadangan bulanan	bulanan 11:30 UTC, pada hari 1 setiap bulan	26 minggu
cadangan tahunan	11:30 UTC, pada hari pertama setiap bulan	2 tahun

Paket cadangan AMS default yang disempurnakan

Rencana ini adalah cetak biru untuk praktik AWS Backup terbaik untuk melindungi terhadap serangan ransomware. Ini menerapkan strategi pencadangan harian, mingguan, bulanan, dan tahunan. AWS Backup [pencadangan berkelanjutan](#) diaktifkan dengan retensi maksimum (31 hari) pada [sumber daya yang didukung](#).

ams-enhanced-default-backup-rencana

Kunci TAG: backup-orchestrator-enhanced

Nilai TAG: true

```
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
  UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForDailyBackups continuous backup: true
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
  UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
  02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
  UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Paket cadangan AMS yang disempurnakan	Waktu Mulai	Penyimpanan
cadangan per jam	N/A	N/A
cadangan harian	setiap hari 4:00 UTC	31 hari
cadangan mingguan	Sabtu, 2:00 UTC	6 minggu
cadangan bulanan	1 bulan ini, 2:00 UTC	26 minggu
cadangan tahunan	1 Januari, 2:00 UTC	2 tahun

Rencana cadangan AMS sensitif data

Paket ini adalah cetak biru untuk praktik terbaik AWS Backup untuk melindungi terhadap serangan ransomware untuk aplikasi yang sensitif terhadap data. Ini menerapkan strategi cadangan per jam, harian, mingguan, bulanan, dan tahunan. Pencadangan [berkelanjutan AWS Backup](#) diaktifkan dengan retensi maksimum (31 hari) pada [sumber daya yang didukung](#).

ams-data-sensitive-backup-rencana

Kunci TAG: backup-orchestrator-data-sensitive

Nilai TAG: true

```
RuleForHourlyBackups schedule expression: cron(0 * ? * * *) (an hourly backup at the
hour mark)
RuleForHourlyBackups delete after days: 7 days
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Paket cadangan AMS Sensitif Data	Waktu Mulai	Penyimpanan
cadangan per jam	pada tanda jam	7 hari
cadangan harian	setiap hari 4:00 UTC	31 hari
cadangan mingguan	Sabtu, 2:00 UTC	6 minggu
cadangan bulanan	1 bulan ini, 2:00 UTC	26 minggu
cadangan tahunan	1 Januari, 2:00 UTC	2 tahun

Brankas cadangan AMS

AWS Backup mengatur snapshot ke dalam unit penyimpanan logis yang disebut vaults.

Anda dapat mengontrol pemberitahuan brankas cadangan di tingkat brankas individual menggunakan tag. Anda dapat memilih keluar dari notifikasi untuk brankas tertentu dengan menambahkan tag `AMSNotificationOptOut` dan menyetel nilainya `True` pada brankas tertentu. Untuk melanjutkan mendapatkan notifikasi dari brankas, hapus tag.

[Untuk melihat daftar cadangan AMS Anda, buka konsol.AWS Backup](#) Di panel navigasi, pilih Backup vaults dan pilih salah satu brankas cadangan AMS dari tabel berikut. Di bagian Cadangan, lihat daftar semua cadangan di brankas cadangan. Pilih cadangan untuk mengedit, menghapus, atau memulihkan.

Vault untuk paket cadangan AMS

Nama AMS Vault	Deskripsi
ams-automated-backups	Vault ini menerima semua titik pemulihan yang diambil oleh AWS Backup paket default-backup-plandefault AMS Advanced.
ams-automated-enhanced-backups	Vault ini menerima semua titik pemulihan yang diambil oleh AWS Backup paket default yang ditingkatkan AMS Advanced ams-enhanced-default-backup-plan.
ams-automated-data-sensitive-cadangan	Vault ini menerima semua titik pemulihan yang diambil oleh rencana AMS Advanced AWS Backup planams-data-sensitive-backup.
ams-manual-backups	Ini adalah lokasi default untuk semua cadangan dari paket cadangan Start Backup Job RFC (ct-2hhud2lx01tq7), jika tidak ada nama vault yang ditentukan.
ams-custom-backups	Ini adalah lokasi default untuk snapshot yang diambil AMS sebelum menambal instance menggunakan Patch Orchestrator atau aktivitas patch bulanan. Ini secara otomatis dihapus sesuai dengan kebijakan default siklus hidup patch AMS selama 60 hari.

Jenis perubahan cadangan AMS

AMS menyediakan beberapa CTs bagi Anda untuk membuat dan menggunakan paket cadangan.

⚠ Important

Jangan mengedit paket cadangan default AMS Anda karena perubahan Anda mungkin hilang. Sebagai gantinya, buat paket baru untuk konfigurasi kustom Anda.

- [Paket Backup: Buat](#)
- [Backup Job: Mulai](#)
- [Backup Job: Berhenti](#)
- [Titik Pemulihan: Hapus](#)
- [DynamoDB | Buat dari Backup](#)
- [Volume EBS: Buat Dari Cadangan](#)
- [Amazon Elastic File System \(EFS\): Buat Dari Backup](#)

Pemantauan dan pelaporan cadangan AMS

⚠ Important

Pemantauan dan pelaporan cadangan AMS hanya tersedia di wilayah yang didukung AMS. Itu adalah AS Timur (Virginia), AS Barat (California N.), AS Barat (Oregon), AS Timur (Ohio), Kanada (Tengah), Amerika Selatan (Sao Paulo), UE (Irlandia), UE (Frankfurt), UE (London), UE (Paris), Asia Pasifik (Mumbai), Asia Pasifik (Seoul), Asia Pasifik (Singapura), Asia Pasifik (Sydney)), Asia Pasifik (Tokyo).

AMS menghasilkan laporan swalayan harian serta laporan bulanan tentang cakupan sumber daya dan status pekerjaan cadangan. Laporan bulanan dibagikan dalam Ulasan Bisnis Bulanan (MBRs). Untuk mempelajari lebih lanjut tentang laporan pencadangan harian, lihat [pencadangan harian](#).

Pakar AMS memantau semua tugas pencadangan Anda yang dikonfigurasi menggunakan AWS Backup. Jika terjadi kegagalan pencadangan, AMS menyelidiki kegagalan tersebut dan memberi tahu Anda tentang akar penyebab dan opsi perbaikan, jika tersedia. Untuk menghindari kebisingan peringatan, selama peristiwa yang menyebabkan banyak kegagalan pencadangan di akun Anda, AMS membuat rekomendasi kolektif, melalui CSDM Anda, alih-alih memberi tahu Anda untuk setiap kegagalan individu.

Perhatikan bahwa AMS tidak memantau pencadangan apa pun yang dikonfigurasi menggunakan fitur pencadangan mandiri AWS layanan.

Respon pemulihan bencana

Selain opsi yang dijelaskan di bagian berikut, ada baiknya Anda mengetahui langkah apa yang harus diambil untuk memulai pemulihan bencana (DR) dengan AMS.

Jika Anda mengalami bencana dan perlu memulai pemulihan, ikuti panduan umum ini:

1. Buka insiden prioritas tinggi dengan kategori Ketersediaan. AMS akan membuka jembatan konferensi dan mengundang tim Anda untuk bergabung.
2. Ketahui daftar sumber daya yang perlu Anda pulihkan.
3. Ketahui target landing zone (LZ) yang perlu Anda pulihkan (misalnya, akun yang sama, AZ yang berbeda atau akun yang berbeda dan wilayah yang berbeda).
4. Kirim permintaan pemulihan untuk setiap sumber daya di landing zone target. Ikuti rencana DR Anda yang ada atau lihat opsi di bagian berikut (misalnya, [Perlindungan bencana untuk EC2 snapshot EBS di AMS](#), atau [Perlindungan bencana EC2 dengan Elastic Disaster Recovery di AMS](#)).
5. Kembalikan fungsionalitas aplikasi dan gunakan bantuan AMS untuk memecahkan masalah terkait infrastruktur.

AMS dapat membantu Anda mempersiapkan acara ini dan dengan membuat rencana DR untuk organisasi Anda untuk membahas pertanyaan-pertanyaan ini. Untuk detail selengkapnya, hubungi manajer pengiriman layanan cloud (CSDM) atau arsitek cloud (CA) Anda.

Perencanaan pemulihan bencana

Disaster Recovery (DR) adalah layanan penting untuk kelangsungan dan kepatuhan bisnis perusahaan. AMS bermitra dengan Anda untuk membantu Anda merencanakan, menerapkan, dan mempertahankan strategi DR Anda di AMS.

AMS landing zone (LZ), multi-akun dan akun tunggal, menyediakan asli, Multi-AZ, ketersediaan tinggi untuk komponen infrastruktur AMS yang memenuhi sebagian besar skenario perlindungan bencana. Namun, tergantung pada cakupan geografis bisnis Anda, Anda mungkin memerlukan perlindungan regional. Untuk ketersediaan lintas wilayah dan DR, akun AMS lain diperlukan di wilayah yang berbeda (ini berlaku untuk landing zone multi-akun dan landing zone akun tunggal).

AMS sejalan dengan panduan AWS DR seperti yang dijelaskan di blog ini, [Memulihkan sistem kritis misi dengan cepat dalam bencana](#), dan mendukung empat opsi berikut:

- Multi Situs (atau Sangat Tersedia)
- Siaga Hangat
- Lampu Pilot
- Pencadangan dan Pemulihan

Opsi ini dan dukungan AMS untuk mereka dijelaskan di bagian berikut.

Multi-situs atau sangat tersedia (HA)

Solusi HA biasanya disediakan oleh fungsionalitas bawaan aplikasi, seperti pengelompokan atau replikasi sinkron. Pengguna diarahkan ke Prod dan HA/DR node. DNS menunjuk ke node secara langsung atau melalui penyeimbang beban elastis (ELB).

Arsitek cloud AMS (CA) Anda akan bekerja dengan Anda sebagai bagian dari perencanaan Anda Well-Architected-Review dan DR.

HA DR menggunakan layanan dan fitur aplikasi dan AWS-native, seperti yang diilustrasikan dalam grafik berikut:

Situs DR bisa sama atau berbeda Wilayah AWS.

Note

Wilayah yang berbeda (Cross-Region) akan memiliki lingkungan Active Directory yang berbeda.

Langkah DR (failover): Failover otomatis, tidak diperlukan langkah manual. Jika terjadi kegagalan pada LZ primer, pengguna akan secara otomatis diarahkan kembali ke node. DR/HA Ini dicapai dengan konfigurasi DNS dan aplikasi.

Metrik HA DR:

- Tujuan Titik Pemulihan (RPO): <5 menit
- Tujuan Waktu Pemulihan dan (RTO): <5 menit

- Pemeliharaan: Tinggi (Perubahan sinkron diperlukan di kedua lingkungan, seperti konfigurasi Aplikasi, tambalan, SG atau ALB, sertifikat, dan sebagainya).
- Biaya: Tinggi

Warm standby

Istilah “warm standby” digunakan untuk menggambarkan skenario pemulihan bencana (DR) di mana versi lingkungan yang diperkecil berjalan di cloud.

Replikasi data ditangani oleh lapisan aplikasi, biasanya secara asinkron, ke instance online, sedangkan instance lainnya (misalnya, Application dan Web tier) mungkin dimatikan untuk menghemat biaya. Pengguna diarahkan hanya ke situs Produksi. AWS Sumber daya lain seperti penyeimbang beban elastis (ELB) dapat disediakan sebelumnya di situs DR juga.

AMS Cloud Architect (CA) Anda akan bekerja dengan Anda sebagai bagian dari perencanaan Anda Well-Architected-Review dan DR.

Warm Standby DR menggunakan layanan dan fitur aplikasi dan AWS-native, seperti yang diilustrasikan dalam grafik berikut:

Situs DR bisa sama atau berbeda Wilayah AWS.

Note

Wilayah yang berbeda (Cross-Region) akan memiliki lingkungan Active Directory yang berbeda.

Langkah DR (failover):

1. Rem replikasi data dan jadikan instance data di situs DR sebagai master
2. Perbarui konfigurasi aplikasi sesuai kebutuhan (IP baru, nama server, dan sebagainya)
3. Alihkan DNS ke situs DR (ELB)
4. Dependensi AD jika diperlukan (Akun layanan,, SPNs GPOs, dan sebagainya)

Metrik HA DR:

- Tujuan Titik Pemulihan (RPO): <1 jam
- Tujuan Waktu Pemulihan dan (RTO): <1 jam (tergantung pada jumlah instance dan orkestrasi)
- Pemeliharaan: Tinggi (Perubahan sinkron diperlukan di kedua lingkungan, seperti konfigurasi Aplikasi, penambalan, grup keamanan (SG) atau penyeimbang beban aplikasi (ALB), sertifikat, dan sebagainya).
- Biaya: Sedang

Pilot light

Dalam pendekatan pemulihan bencana (DR) ini, Anda mereplikasi bagian dari lingkungan Prod Anda untuk serangkaian layanan inti terbatas. Sebagian kecil infrastruktur Anda selalu berjalan, secara bersamaan menyinkronkan data yang dapat berubah (seperti database atau dokumen), sementara bagian lain dari infrastruktur Anda dimatikan dan hanya digunakan selama pengujian. Tidak seperti pendekatan pencadangan dan pemulihan, Anda harus memastikan bahwa elemen inti Anda yang paling penting sudah dikonfigurasi dan berjalan di landing zone DR (lampu pilot).

AMS Cloud Architect Anda akan bekerja dengan Anda sebagai bagian dari perencanaan Anda Well-Architected-Review dan DR.

Pilot Light DR menggunakan aplikasi dan layanan dan fitur AWS asli, seperti yang diilustrasikan dalam grafik berikut:

Situs DR bisa sama atau berbeda Wilayah AWS.

Note

Wilayah yang berbeda (Cross-Region) akan memiliki lingkungan Active Directory yang berbeda.

Langkah DR (failover):

1. Rem replikasi data dan jadikan instance data di situs DR sebagai master
2. Mulai instans dan infrastruktur yang dimatikan
3. Perbarui konfigurasi aplikasi sesuai kebutuhan (IP baru, nama server, dan sebagainya)
4. Tambahkan instance ke ELB sesuai kebutuhan

5. Alihkan DNS ke situs DR (ELB)

6. Dependensi AD, jika diperlukan (Akun layanan,, SPNs GPOs, dan sebagainya)

Metrik DR Pilot Light:

- Tujuan Titik Pemulihan (RPO): <1 jam
- Tujuan Waktu Pemulihan dan (RTO): ~ 1 jam (tergantung pada jumlah instance dan orkestrasi)
- Pemeliharaan: Medium
- Biaya: Sedang

Pencadangan dan pemulihan

Pendekatan pemulihan bencana (DR) yang sederhana dan berbiaya rendah ini mencadangkan data dan aplikasi Anda dari mana saja ke landing zone DR untuk digunakan selama pemulihan dari bencana.

Arsitek AMS Cloud Anda bekerja dengan Anda sebagai bagian dari perencanaan Backup dan DR Anda.

Backup and Restore DR menggunakan perkakas dan proses otomatis AMS, seperti yang diilustrasikan dalam grafik berikut:

Dua metode pencadangan dan replikasi dapat digunakan:

- Snapshot EBS (Recovery Point Objective (RPO) > 1 jam), dikenal sebagai “EBS”
- AWS Elastic Disaster Recovery (Recovery Point Objective (RPO) ~ 0,25 jam), yang dikenal sebagai “DRS”

Situs DR bisa sama atau berbeda Wilayah AWS.

Note

Wilayah yang berbeda (Cross-Region) memiliki lingkungan Active Directory yang berbeda.

Langkah DR (failover):

1. Kembalikan instance dari snapshot (proses dua langkah dengan instance placeholder terlebih dahulu)
2. Perbarui konfigurasi aplikasi (IP baru, nama server, dan sebagainya)
3. Siapkan infrastruktur lain sesuai kebutuhan (SG, ELB, dan sebagainya)
4. Alihkan DNS ke situs DR (ELB)
5. Perbarui atau pulihkan dependensi AD jika diperlukan (akun layanan, nama utama layanan (SPNs), objek kebijakan grup (GPOs), dan sebagainya)

Backup dan Restore metrik DR:

- Tujuan Titik Pemulihan (RPO): > 1 jam atau ~ 0,25 jam (tergantung pada solusi yang dipilih - EBS atau DRE)
- Tujuan Waktu Pemulihan dan (RTO): ~ 1 jam (tergantung pada jumlah instance dan orkestrasi)
- Pemeliharaan: Tinggi (Perubahan sinkron diperlukan di kedua lingkungan, seperti konfigurasi aplikasi, tambalan, grup keamanan atau penyeimbang beban aplikasi, sertifikat, dan sebagainya).
- Biaya: Sedang

Perlindungan bencana untuk EC2 snapshot EBS di AMS

Prasyarat:

- Zona Pendaratan AMS Prod (sumber)
- Zona Pendaratan AMS DR (target DR)
- Snapshot EBS diaktifkan untuk EC2 instance (AWS Backup)

Solusi replikasi snapshot:

- Cross AZ: Tidak berlaku - Snapshot EBS sangat tersedia di Wilayah berdasarkan desain
- Lintas Wilayah: AWS Backup

Diagram berikut mewakili proses EC2 pemulihan dari snapshot EBS di AMS:

EC2 Langkah DR pada AMS:

1. Naikkan RFC untuk membagikan snapshot EBS dengan akun target (diperlukan untuk Cross-Region DR).

: Manajemen, Komponen Stack Tingkat Lanjut, Snapshot EBS, Bagikan

2. Buat tumpukan EC2 AMS placeholder di subnet tujuan (subnet situs DR). Rekomendasinya adalah menggunakan konsumsi CFN untuk membuat tumpukan karena pelanggan dapat menggabungkan langkah-langkah penetapan grup keamanan dan lainnya (seperti menambahkan instance ke ELB) di tumpukan yang sama.

Ubah jenis: Deployment, Ingestion, Stack from Template, Create CloudFormation

3. Naikkan RFC untuk melakukan pemulihan volume EC2 tumpukan.

Ubah jenis: Manajemen, Komponen Stack Lanjutan, tumpukan EC2 instance, Kembalikan volume.

CT mengembalikan volume dari snapshot yang dibagikan di langkah 1 dan menempel pada instance placeholder yang dibuat pada langkah 2.

Fungsi Volume Restore CT:

- Matikan instance placeholder
- Kembalikan volume dari snapshot
- Tukar volume
- Mulai instance
- Tinggalkan domain lama
- Mengubah nama host
- Nyalakan ulang. Skrip bootstrap AMS bergabung dengan instance ke domain target (DR) saat memulai

Volume mengembalikan input CT:

- InstanceId (ID contoh placeholder)
- RootDeviceSnapshotId, snapshot EBS untuk volume root yang dipulihkan
- KMSKeyId, pengenal kunci KMS, atau ARN, untuk mengenkripsi semua volume yang dipulihkan pada instance EC2
- DeviceNames, hingga 25 (opsional)

- SnapshotIds, hingga 25 (opsional). Daftar snapshot dari volume yang akan dipulihkan

Perlindungan bencana EC2 dengan Elastic Disaster Recovery di AMS

Prasyarat:

- Zona Pendaratan AMS Prod (sumber)
- Zona Pendaratan AMS DR (target DR)
- Anda harus terlebih dahulu menginisialisasi layanan Elastic Disaster Recovery untuk semua Wilayah AWS yang Anda rencanakan untuk menggunakannya.

Buat peran IAM di DR landing zone (LZ) Anda untuk akses konsol Elastic Disaster Recovery.

- Penting: Dokumen SSM dibuat sebagai Post Launch Action dalam DRS. Tindakan ini harus diaktifkan di semua server Anda pada PostLaunch pengaturan.
- instance tujuan (placeholder) harus memiliki kunci tag: "AWSDRS", value:""AllowLaunchingIntoThisInstance. Instans placeholder harus dalam keadaan berhenti. Jika tidak, AMS tidak dapat memilih instance placeholder di bawah pengaturan peluncuran dan Elastic Disaster Recovery tidak dapat memulihkan di atas instance placeholder.

Untuk diagram proses penyiapan dan pemulihan Elastic Disaster Recovery EC2 di AMS, lihat [arsitektur umum AWS Elastic Disaster Recovery \(AWS DRS\)](#).

EC2 Langkah DR dengan Pemulihan Bencana Elastis di AMS:

1. Buat tumpukan EC2 AMS placeholder di subnet tujuan (subnet situs DR) dengan tag yang tepat, untuk informasi lebih lanjut, lihat bagian sebelumnya. Sebaiknya gunakan konsumsi CFN untuk membuat tumpukan karena Anda dapat menggabungkan langkah-langkah penetapan grup keamanan dan menandai instance, volume EBS, dan lainnya (seperti menambahkan instance ke ELB) di tumpukan yang sama.

Ubah jenis: Deployment, Ingestion, Stack from Template, Create CloudFormation

2. Hentikan instance placeholder.

Ubah jenis: Manajemen, Komponen tumpukan lanjutan, EC2 contoh, Berhenti

3. Jika tidak dilakukan pada langkah 1, beri tag instance placeholder dan volume EBS-nya dengan kunci: "AWSDRS", value:"". AllowLaunchingIntoThisInstance

Ubah jenis: Manajemen, Komponen tumpukan lanjutan, Tag, Perbarui.

- Gunakan instance placeholder dari langkah 1 sebagai target di bawah Launch into instance ID, DRS Launch Settings untuk server sumber. Memulai latihan pemulihan instans dari konsol Elastic Disaster Recovery untuk Source Server.

 Note

Volume instance placeholder disimpan di akun. Untuk menghapus volume ini, kirimkan Manajemen | Komponen tumpukan lanjutan | Volume EBS | Hapus jenis perubahan (ct-3e3h8u0sp5z80) di akhir operasi pemulihan bencana.

Elastic Disaster Recovery memulihkan alur kerja:

- Instance target (placeholder) harus dalam status berhenti
- Tukar volume dan hapus volume root sumber (placeholder)
- Mulai instance
- Jalankan Tindakan Peluncuran Pos untuk menyelesaikan item berikut:
 - Aktifkan Agen SSM.
 - Tukar volume dan hapus volume root sumber (placeholder).
 - Mulai instance
- Jalankan Dokumen PostLaunchScript SSM. Dokumen ini melakukan berikut:
 1. Meninggalkan domain lama.
 2. Mengubah nama host.
 3. Nyalakan ulang. Skrip bootstrap AMS bergabung dengan instance ke domain target (DR) selama startup.

Manajemen patch di AMS

Topik

- [AMS Patch Orchestrator: model patching berbasis tag](#)
- [Menggunakan Patch Orchestrator](#)
- [Penambalan sesuai permintaan](#)
- [Penambalan standar AMS](#)
- [Menambal komitmen layanan](#)

Di AMS, manajemen tambalan adalah layanan yang membantu Anda mempertahankan pembaruan vendor OS di instans Amazon Elastic Compute Cloud (Amazon EC2) Anda. Anda memiliki kebebasan untuk menyesuaikan frekuensi dan proses menambal EC2 instans Amazon Anda.

Anda mengonfigurasi manajemen tambalan selama orientasi, dan Anda dapat memperbaruinya dengan menggunakan proses RFC. Tumpukan yang dibuat menggunakan sistem manajemen perubahan dan templat yang kompatibel dengan tambalan (untuk Amazon, grup Auto EC2 Scaling, HA one-tier atau two-tier stack) berlangganan manajemen patch secara otomatis.

AMS menyediakan fitur, Patch Orchestrator — patching berbasis tag, untuk mengonfigurasi patching.

Untuk definisi istilah tambalan, lihat [Istilah kunci AMS](#).

Important

- Tidak mungkin tumpukan atau instance konstituen tumpukan untuk memilih keluar dari manajemen tambalan, jika template AMS tempat tumpukan dibuat kompatibel dengan manajemen tambalan. Saat ini, patching kompatibel dengan template stack berikut:
 - EC2 Tumpukan Amazon | Buat, dan EC2 tumpukan Amazon | Buat (dengan volume tambahan)
 - EC2 Instans Amazon diluncurkan dengan AWS CloudFormation menelan
 - Grup Auto Scaling | Buat (EC2 instance Amazon dalam grup ditambah)
 - Tumpukan Satu Tingkat Ketersediaan Tinggi | Buat, dan Ketersediaan Tinggi Tumpukan Dua Tingkat | Buat
- Jika ada insiden berkelanjutan yang memengaruhi tumpukan, operator AMS dapat menjadwalkan ulang atau membatalkan patching terjadwal.

- Secara default, semua instance dalam tumpukan yang kompatibel dengan tambalan tertentu ditambah di tempat. Untuk menambal grup Auto Scaling dengan pengganti Amazon Machine Image (AMI) menggunakan AMS latest/patched AMI, kirimkan permintaan layanan. Pembaruan AMIs dibagikan ke akun setiap bulan.

Important

Anda dapat menentukan repositori patch alternatif untuk node terkelola. Sementara AMS mengimplementasikan konfigurasi patch yang Anda minta, Anda bertanggung jawab untuk memilih dan memvalidasi keamanan repositori yang Anda pilih. Anda juga harus menerima risiko apa pun dari penggunaan repositori ini, seperti risiko rantai pasokan.

Berikut ini adalah praktik terbaik untuk keamanan proses manajemen tambalan Anda:

- Gunakan hanya sumber repositori yang tepercaya dan terverifikasi
- Default ke repositori vendor OS standar jika memungkinkan
- Secara teratur mengaudit konfigurasi repositori kustom

Tip

AMS menyarankan agar Anda mengaktifkan cadangan untuk instans yang memiliki aplikasi atau layanan berharga. Untuk informasi tentang mengaktifkan backup, lihat [Manajemen kontinuitas di AMS Advanced](#)

AMS Patch Orchestrator: model patching berbasis tag

Jika Anda telah onboard ke model patching berbasis tag AMS Patch Orchestrator yang baru, Anda dapat menggunakan tag untuk menerapkan konfigurasi tambalan Anda ke kumpulan sumber daya yang tepat, yang disebut grup patch, mulai dari satu instance hingga semua instance Anda. Untuk informasi tentang tag AMS, lihat [Menggunakan tag](#). Petunjuk tentang pengaturan tag Patch Orchestrator disediakan di bagian berikut.

Patch diinstal selama jendela patch yang Anda tentukan dengan [SSM Patch Window](#) | Create. Setiap jendela patch adalah jendela pemeliharaan AWS Systems Manager yang berjalan sesuai jadwal pilihan Anda, memiliki durasi yang dikonfigurasi, dan berlaku untuk satu grup patch. Instance yang

bukan bagian dari jendela patch eksplisit ditambal selama jendela pemeliharaan default yang Anda tentukan saat Anda onboard ke Patch Orchestrator.

 Important

Jika beberapa jendela pemeliharaan patch dijadwalkan untuk berjalan pada waktu yang sama, mereka harus memiliki kurang dari 1001 instance yang diproses pada waktu tertentu. Ini adalah batasan AWS Systems Manager. AMS merekomendasikan setidaknya satu jam per setiap lima puluh kali.

Secara default, semua patch yang disediakan vendor sistem operasi (OS) diinstal selama jendela pemeliharaan atau patch sesuai permintaan. Ini disebut default patch baseline. [Jika Anda ingin membatasi patch mana yang diinstal, Anda dapat menentukan baseline patch kustom dengan salah satu patch baseline create CTs \(per OSES\), lihat Patching subkategori.](#) Misalnya, Anda dapat menggunakan baseline patch khusus sehingga hanya pembaruan keamanan penting dan penting yang diinstal untuk satu atau beberapa grup patch.

Setelah tambalan diinstal pada sebuah instance, instance di-reboot. Pemberitahuan tambalan dikirim sebelum dan sesudah penambalan, dan pengingat tambahan dikirim dalam waktu 96 jam sebelum jadwal dimulai. Selain itu, AMS menerapkan pembaruan pada alat manajemen infrastruktur (seperti agen AWS SSM) selama jendela pemeliharaan yang dipilih.

 Important

AMS tidak menggunakan pelaporan kepatuhan patch bulanan untuk instans dengan tambalan yang hilang, dan tidak akan mengirimkan laporan bulanan. Perubahan ini telah dilakukan mengingat laporan operasional swalayan yang baru-baru ini dirilis yang menyegarkan setiap 24 jam dan tersedia untuk Anda sesuai permintaan dan memberikan data terbaru dan terperinci. Untuk mempelajari lebih lanjut tentang laporan, lihat Pelaporan layanan mandiri. Untuk mempelajari lebih lanjut tentang laporan, lihat [Laporan layanan mandiri](#).

Untuk informasi selengkapnya tentang notifikasi, lihat [Pemberitahuan tambalan](#).

Menggunakan Patch Orchestrator

Aktifkan AMS Patch Orchestrator untuk akun Anda dengan mengirimkan permintaan layanan yang mencakup detail berikut:

- Kategori: Lain-lain
- Subjek: Onboard ke Patch Orchestrator
- Email CC: Alamat email CC menerima pemberitahuan saat status RFC orientasi ini berubah
- Detail: Tempelkan informasi berikut ke dalam email dan berikan nilai Anda. Perhatikan bahwa ini ThirdTagKey adalah opsional. Untuk rekomendasi dan contoh, lihat tabel berikut.

```
Default maintenance window Schedule:
Default Maintenance Window Schedule TimeZone:
Default Maintenance Window Duration:
Default Maintenance Window Cutoff:
Default Patch Backup Retention In Days:
Default Maintenance Window Notification Emails:
First Tag Key:
Second Tag Key:
Third Tag Key:
```

Tabel berikut menjelaskan format dan rekomendasi untuk nilai yang Anda berikan.

Konfigurasi patching berbasis tag orkestrator patch

Nama parameter	Informasi	Rekomendasi atau contoh
Jadwal Jendela Pemeliharaan Default	Jadwal jendela pemeliharaan default dalam bentuk ekspresi cron atau rate. Misalnya: • <code>cron(0 3 ? * 6L *)</code>: 03:00 pagi pada hari Jumat terakhir setiap bulan • <code>rate(7 days)</code>: Setiap tujuh hari	Kami merekomendasikan agar jendela berjalan setidaknya a sekali per bulan pada hari kerja yang konsisten.

Nama parameter	Informasi	Rekomendasi atau contoh
	Untuk informasi selengkapnya tentang membuat ekspresi cron, dan tautan ke cron dan sumber daya ekspresi tingkat, lihat Cron dan ekspresi tingkat untuk jendela pemeliharaan.	
Jendela Pemeliharaan Default Jadwal Zona Waktu	Zona waktu yang dijalankan jendela pemeliharaan default didasarkan pada, dalam format Internet Assigned Numbers Authority (IANA).	Misalnya: - Amerika/Los_Angeles - DII/UTC
Durasi Jendela Pemeliharaan Default	Durasi jendela pemeliharaan default dalam jam.	Setidaknya 1 jam per setiap 50 instance, ditambah 2 jam untuk cutoff.
Pemotongan Jendela Pemeliharaan Default	Jumlah jam sebelum akhir Jendela Pemeliharaan Default di mana tidak ada perintah patching baru yang dimulai. Interval ini ada untuk memberikan waktu yang cukup untuk penambalan selesai sebelum jendela berakhir.	Setidaknya 2 jam.
Retensi Cadangan Patch Default Dalam Hari (opsional)	Waktu default dalam beberapa hari untuk menjaga titik pemulihan EBS dibuat sebelum menambal instance.	Kami merekomendasikan untuk menjaga default, yaitu 60.

Nama parameter	Informasi	Rekomendasi atau contoh
Email Pemberitahuan Jendela Pemeliharaan Default	Satu hingga lima alamat email atau daftar distribusi untuk menerima pemberitahuan tentang status patching jendela pemeliharaan default.	Sebaiknya gunakan daftar distribusi grup alih-alih email individual.
Kunci Tag Pertama	Tombol tag pertama yang digunakan untuk membuat nilai tag Grup Patch Anda.	Sebagai contoh, AppId. Tentukan null jika Anda sudah mendefinisikan grup tambalan Anda sendiri dengan tag Grup Patch.
Kunci Tag Kedua	Tombol tag kedua yang digunakan untuk membuat nilai tag Grup Patch Anda.	Misalnya, Lingkungan. Tentukan null jika Anda telah mendefinisikan grup tambalan Anda sendiri dengan tag Grup Patch.
Kunci Tag Ketiga (opsional)	Tombol tag ketiga opsional yang digunakan untuk membuat nilai tag Grup Patch Anda.	Misalnya, Grup.

Setelah Anda masuk ke model layanan patching Patch Orchestrator yang baru, semua instance yang ditandai dengan tepat di akun Anda milik grup patch dengan tag Grup Patch. Patch Orchestrator menggunakan tag Patch Group yang ada, atau tag buatan AMS yang terdiri dari dua atau tiga nilai tag gabungan yang Anda tentukan selama onboarding Patch Orchestrator. Misalnya, **{Tag Value 1} - {Tag Value 2} - {Tag Value 3}**. AMS memperbarui tag Grup Patch yang diterapkan AMS ini setiap 12 jam. Jika diperlukan, Anda dapat memperbarui nilai tag Grup Patch Anda dengan jenis perubahan [Tag | Update \(Review Required\)](#) atau [Tag | Update \(Review Required\)](#).

Misalnya, jika EC2 instans Amazon Anda memiliki pasangan kunci tag berikut: nilai:

- AppId:MyApplication
- Environment:Production

- Group:1

Selama onboarding Anda menentukan kunci tag berikut:

- First Tag Key = AppId
- Second Tag Key = Environment
- Third Tag Key = Group

AMS membuat tag Grup Patch berikut dan menerapkannya ke instance Anda:Patch
Group:MyApplication-Production-1.

 Note

Peringatan kegagalan patch tidak dibuat untuk instance yang memiliki sistem operasi yang tidak didukung, atau yang dihentikan selama jendela pemeliharaan.

Prasyarat Patch Orchestrator

Alur kerja Patch Orchestrator menargetkan instans EC2 Amazon yang ditambah oleh versi terbaru Dokumen Otomasi Manajer Sistem:. AWSManagedServices-PatchInstanceFromMaintenanceWindow

Sebagai bagian dari alur kerja dokumen, dokumen perintah run “AWS-RunPatchBaseline” dijalankan terhadap setiap EC2 instance Amazon dari anggota grup patch. Untuk mempelajari lebih lanjut, lihat [Tentang dokumen SSM AWS- RunPatchBaseline](#).

Persyaratan:

- EC2 Instans Amazon diterapkan dari Amazon Machine Image (AMI) yang disediakan AMS, atau pada AMI melalui CT “Stack from migration partner migrated instance” (ct-257p9zjk14ija).
- Koneksi internet jalan keluar diaktifkan. Untuk firewall/proxy solusi, persyaratannya adalah mengizinkan titik akhir pembaruan Windows titik akhir cermin repositori and/or Linux, pengaturan proxy manajer sistem AWS, dan konfigurasi proxy metadata. Untuk informasi selengkapnya, lihat [Mengonfigurasi Agen SSM untuk menggunakan proxy](#) dan [Menggunakan proxy HTTP](#)
- Peran IAM yang cocok dengan akses permisif minimum untuk layanan SSM peran IAM.
customer-mc-ec2-instance-profile

- Kami merekomendasikan 10 GB ruang partisi root yang tersedia. Untuk OS Linux, setidaknya 2 GB tersedia di `/var` partisi.
- Otoritas Sertifikat yang berfungsi dan valid untuk unduhan pembaruan.
- Layanan Pembaruan Server Windows (WSUS) - Registri termasuk namun tidak terbatas pada: `DisableWindowsUpdateAccess`, `NoWindowsUpdate`; Pembaruan Otomatis tidak boleh mengganggu pengoperasian proses Pembaruan Windows.

Validasi:

- Untuk instance OS Linux menggunakan pengelola paket yum, Anda dapat memvalidasi ketersediaan pembaruan dengan menjalankan `#yum check-update`
- Untuk Linux OS RedHat 5.7 dan yang lebih baru, 6.1 dan yang lebih baru, dan 7.0 dan yang lebih baru; EC2 Instans Amazon dimigrasi ke akun AMS Anda melalui CT "Stack from migration partner migrated instance" (ct-257p9zjk14ija), Anda perlu memvalidasi status manajer langganan untuk kinerja pembaruan.
- Pada OS Windows, aktifkan Layanan Pembaruan Server Windows (WSUS). Tidak ada kebijakan lokal yang harus memblokir kemampuan WSUS untuk memindai atau menginstal pembaruan. Setelah masuk sebagai administrator, Anda dapat memvalidasinya dengan melakukan pemindaian untuk pembaruan yang tersedia dari konsol Layanan Pembaruan Windows. Rilis OS Windows Server termasuk 2012R2, 2016 dan 2019 memiliki pengaturan Pembaruan Windows default untuk diunduh dan diinstal. Anda dapat mengonfigurasi pengaturan yang diinginkan sebelum memindai. Pada rilis OS selanjutnya, operasi ini dapat memicu instalasi; konfigurasi perilaku yang diinginkan sebelumnya.
- Minta validasi dari tim Operasi AMS dengan mengirimkan permintaan layanan: "Dokumen AWSManagedServices-CheckPatchingPrerequisites otomatisasi untuk dijalankan terhadap EC2 instans Amazon untuk penilaian kesiapan tambalan."

Note

Peringatan kegagalan patch tidak dibuat untuk instance yang memiliki sistem operasi yang tidak didukung, atau yang dihentikan selama jendela pemeliharaan.

Jendela tambalan

Contoh dalam grup patch tertentu ditambah selama satu atau lebih jendela patch. Jendela tambalan berjalan pada jadwal yang didefinisikan sebagai ekspresi cron atau rate, dan memiliki durasi yang dapat dikonfigurasi yang dimaksudkan untuk menjaga gangguan terkait tambalan dalam interval waktu yang dipilih. AMS merekomendasikan untuk membuat beberapa jendela tambalan yang secara kolektif mencakup semua instance Anda, agar sesuai dengan rutinitas penambalan spesifik organisasi Anda, dan untuk menggunakan jendela pemeliharaan default sebagai fallback. Jendela tambalan dibuat dengan jenis perubahan RFC Deployment | Patching | Jendela patch SSM | Buat (ct-0el2j07llrxs7). Semua instance yang bukan bagian dari jendela tambalan ditambah selama jendela pemeliharaan default yang dibuat selama orientasi.

Biasanya, jendela patch tidak perlu diperbarui untuk menyertakan instance baru. Biasanya, ini dilakukan dengan memodifikasi tag instance. Misalnya, pertimbangkan urutan peristiwa berikut:

1. Dua contoh ditandai dengan `AppId:MyApplication,,Environment:Production. Group:1`

Ini menghasilkan tag pada instance ini, dengan asumsi First Tag Key = `AppId`, Second Tag Key = `Environment`, Third Tag Key = `Group` dan jendela patch untuk grup patch `MyApplication - Production-1` dibuat.

2. Tiga contoh lagi dibuat dan ditandai dengan `AppId:MyApplication,,Environment:Production. Group:1`

Ini menghasilkan tag untuk Grup Patch: `MyApplication -Production-1`.

Tidak diperlukan perubahan pada jendela tambalan karena ia mengambil kelima instance pada saat proses terjadwal berikutnya.

Untuk diskusi lebih rinci dan panduan tentang penggunaan jenis perubahan ini, lihat [SSM Patch Window](#) | Create.

Pemberitahuan tambalan

Important

Mulai 1 Februari 2025, pelanggan AMS tidak akan lagi menerima pemberitahuan untuk Windows Pemeliharaan Patch kosong di akun terkelola mereka.

Alamat email berlangganan (hingga lima) menerima email yang mirip dengan yang berikut ini sebelum jendela pemeliharaan patch dimulai:

Dear Customer,

The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* was started at:
2020-02-21T12:02:18.196Z.

Details:

- Maintenance Window AccountId: *YOUR_ACCOUNT_ID*
- Maintenance Window Region: *YOUR_ACCOUNT_REGION*
- Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*
- Maintenance Window Name: *THE_MAINTENANCE_WINDOW_NAME*
- Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH_GROUP_NAME*

- Maintenance Window Patch Group: *PATCH_GROUP_NAME*
- Maintenance Window ExecutionId: *THE_EXECUTION_ID*

Targets:

InstanceId	InstanceName	StackId
-----	-----	-----
<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>

A follow-up message with a detailed report is sent as soon as the maintenance window is over.

Please raise a service request if you have any inquires about AMS Patch Orchestrator by following this URL:
<https://console.aws.amazon.com/managedservices/servicerequest/new>

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

Di akhir aktivitas tambalan, alamat email berlangganan menerima email yang mirip dengan yang berikut ini:

Dear Customer,

The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* ended at:
2020-02-21T12:03:20.058Z, with status: SUCCESS.

Details:

- Maintenance Window AccountId: *YOUR_ACCOUNT_ID*
- Maintenance Window Region: *YOUR_ACCOUNT_REGION*
- Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*

```

Maintenance Window Name:      THE_MAINTENANCE_WINDOW_NAME
Maintenance Window Description: MaintenanceWindow for patching patch
Group PATCH_GROUP_NAME
Maintenance Window Patch Group: PATCH_GROUP_NAME
Maintenance Window ExecutionId: THE_EXECUTION_ID

Targets:
  RfcId              InstanceId      InstanceName      StackId
  Status
  -----
  THE_RFC_ID        THE_INSTANCE_ID  THE_INSTANCE_NAME THE_STACK_NAME
STATUS

```

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

Please raise an Incident if an issue is impacting one of your production applications by following this URL:

<https://console.aws.amazon.com/managedservices/incident/new>

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

Setiap 96 jam sistem penambalan AMS mengidentifikasi semua jendela pemeliharaan terkelola tambalan yang akan datang dalam 96 jam itu dan mengirimkan pemberitahuan pengingat ke semua alamat email berlangganan yang termasuk dalam jendela 96 jam itu. Ini bisa sesedikit satu jam sebelum jendela, atau 96 jam penuh. Misalnya:

```

Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME will start at:
2020-05-06T16:35:36.523Z.
Details:
  Maintenance Window AccountId: YOUR_ACCOUNT_ID
  Maintenance Window Region:    YOUR_ACCOUNT_REGION
  Maintenance Window Id:        THE_MAINTENANCE_WINDOW_ID
  Maintenance Window Name:      THE_MAINTENANCE_WINDOW_NAME
  Maintenance Window Description: MaintenanceWindow for patching patch
  Group PATCH_GROUP_NAME
  Maintenance Window Patch Group: PATCH_GROUP_NAME

```

Maintenance Window Next Start Time: 2020-05-06T16:35:36.523Z

Maintenance Window Schedule: rate(24 hours)

Maintenance Window Timezone: *THE_TIMEZONE*

At this time, these are the instances in the "*PATCH_GROUP_NAME*" Patch Group:

InstanceId	InstanceName	StackId	InstanceState

<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped

<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped

<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped

A notification message is sent as soon as the maintenance window starts.

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

If you would like to disable this maintenance window or you have inquires about the AMS Patch Orchestrator click on the following URL:

<https://console.aws.amazon.com/managedservices/servicerequest/new>

If you would like to delete this maintenance window, you can run the CT with id "ct-0q0bic0ywqk6c" against the stack id "stack-rctyznutkyj4tkkzq".

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

Garis dasar patch

Secara default, semua patch yang disediakan vendor sistem operasi (OS) diinstal menggunakan baseline patch default AMS. Jika Anda ingin membatasi patch mana yang diinstal, Anda dapat secara opsional membuat baseline patch menggunakan tipe perubahan RFC Deployment | Patching | SSM patch baseline | Create (CT ID bervariasi per sistem operasi). *OS*

Untuk informasi tentang penggunaan jenis perubahan ini, lihat [Menambal subkategori](#).

Tag yang dicadangkan Patch Orchestrator

Patch Orchestrator juga menghasilkan tag berikut yang tidak dapat diubah:

- **AMSPatchGrup** - Tag ini digunakan untuk pembuatan nilai tag Grup Patch. Anda tidak harus memodifikasi AMSPatch Grup. Anda dapat memodifikasi tag “Grup Patch” jika Anda ingin menggunakan nilai “Grup Patch” khusus. Patch Orchestrator terus menghasilkan nilai untuk AMSPatch Grup berdasarkan kunci tag yang disediakan selama orientasi, tetapi tidak akan mengubah nilai tag “Grup Patch” jika telah disetel ke nilai khusus oleh Anda. Untuk berhenti menggunakan nilai “Grup Patch” khusus, Anda dapat mengatur nilai “Grup Patch” agar sesuai dengan nilai tag AMSPatch Grup.
- **AMSDefaultPatchGroup**— Tag ini menunjukkan apakah sebuah instance merupakan bagian dari jendela pemeliharaan default, dengan nilai True atau False. Jika Grup Patch instance tidak ditetapkan ke jendela pemeliharaan, nilai ini disetel ke True.

Penambalan sesuai permintaan

AMS memiliki tipe perubahan yang berfungsi dengan baseline patch Anda, untuk memungkinkan Anda menjalankan tambalan pada instance sesuai permintaan. Ini bisa berupa baseline default yang Anda tetapkan saat naik pesawat, atau baseline patch Patch Orchestrator Systems Manager yang Anda tetapkan dengan jenis perubahan Patch Baseline (ID CT bervariasi per sistem operasi).

Anda dapat menggunakan jenis perubahan patching sesuai permintaan dengan atau tanpa Patch Orchestrator.

Untuk informasi tentang menggunakan jenis perubahan ini, lihat [On Demand Patching | Run](#).

Note

Anda tidak dapat menggunakan instance yang merupakan bagian dari grup Auto Scaling dalam jenis perubahan patching sesuai permintaan.

Penambalan standar AMS

AMS mendukung pelanggan yang sudah ada menggunakan model patching standar AMS, tetapi model ini tidak tersedia untuk pelanggan baru dan sedang pensiun demi AMS Patch Orchestrator.

Konten tambalan umum untuk patching standar AMS termasuk pembaruan vendor untuk sistem operasi yang didukung dan perangkat lunak yang sudah diinstal sebelumnya dengan sistem operasi yang didukung (misalnya, IIS dan Apache Server).

Selama onboarding AMS, Anda menentukan persyaratan penambalan, kebijakan, frekuensi, dan jendela tambalan pilihan. Konfigurasi ini berarti Anda dapat menghindari aplikasi offline sekaligus untuk penambalan infrastruktur, sehingga Anda dapat mengontrol infrastruktur apa yang ditambal kapan.

 Note

Proses penambalan yang dijelaskan dalam topik ini hanya berlaku untuk tumpukan Anda. Infrastruktur AMS ditambal selama proses terpisah. AWS Managed Services Maintenance Window (atau Maintenance Window) melakukan aktivitas pemeliharaan untuk AWS Managed Services (AMS) dan berulang pada hari Kamis kedua setiap bulan mulai pukul 15:00 hingga 16:00 Waktu Pasifik. AMS dapat mengubah jendela pemeliharaan dengan pemberitahuan 48 jam. Anda mengonfigurasi jendela patch AMS saat onboarding, atau Anda menyetujui atau menolak pemberitahuan layanan patch bulanan.

AMS secara teratur memindai EC2 instans Amazon yang dikelola untuk pembaruan yang tersedia melalui fungsionalitas pembaruan sistem operasi. Kami juga menyediakan pembaruan rutin ke Amazon Machine Images (AMIs) berbasis AMS yang didukung di lingkungan kami.

Setelah divalidasi, rilis AMS AMI dibagikan dengan semua akun AMS. Anda dapat melihat rilis AWS AMI yang tersedia dengan menggunakan panggilan [DescribeImages](#) Amazon EC2 API atau menggunakan EC2 konsol Amazon. Untuk menemukan AMS yang tersedia AMIs, lihat [Cari AMI IDs, AMS](#).

AMS melakukan jadwal patching ad hoc hanya jika diminta oleh Anda. Sebelumnya AMS akan mengirim pemberitahuan; saat ini, pemberitahuan tidak dikirim.

 Note

Secara default, AMS menggunakan Systems Manager untuk menerapkan patch dengan meminta manajer paket (Linux) atau layanan Pembaruan Sistem (Windows) menanyakan repositori defaultnya untuk melihat paket baru mana yang tersedia. Jika, selama day-to-day operasi Anda, Anda telah menginstal paket pada host Linux menggunakan manajer paket default, manajer paket itu juga mengambil paket baru untuk perangkat lunak itu ketika mereka tersedia. Dalam kasus seperti itu, Anda mungkin ingin mengambil tindakan penambalan (dijelaskan di bagian ini) untuk memilih keluar untuk contoh itu.

Sistem operasi yang didukung

Sistem operasi yang didukung (x86-64)

- Amazon Linux 2023
- Amazon Linux 2 (diharapkan tanggal akhir dukungan AMS 30 Juni 2026)
- Oracle Linux 9.x, 8.x
- Red Hat Enterprise Linux (RHEL) 9.x, 8.x
- SUSE Linux Server Perusahaan 15 SP6
- SUSE Linux Enterprise Server untuk SAP 15 SP3 dan yang lebih baru
- Microsoft Windows Server 2022, 2019, 2016
- Ubuntu 20.04, 22.04, 24.04

Sistem operasi yang didukung (ARM64)

- Amazon Linux 2023
- Amazon Linux 2 (diharapkan tanggal akhir dukungan AMS 30 Juni 2026)

Patch yang didukung

AWS Managed Services mendukung patching terutama pada tingkat sistem operasi. Patch yang diinstal mungkin berbeda menurut sistem operasi.

Important

Semua pembaruan diunduh dari repositori jarak jauh layanan dasar patch Systems Manager yang dikonfigurasi pada instance, dan dijelaskan nanti dalam topik ini. Instance harus dapat terhubung ke repositori sehingga patch dapat dilakukan.

Untuk memilih keluar dari layanan baseline patch untuk repositori yang mengirimkan paket yang ingin Anda pertahankan sendiri, jalankan perintah berikut untuk menonaktifkan repositori:

```
yum-config-manager DASHDASHdisable REPOSITORY_NAME
```

Ambil daftar repositori yang saat ini dikonfigurasi dengan perintah berikut:

```
yum repolist
```

- Repositori Amazon Linux yang telah dikonfigurasi sebelumnya (biasanya empat):

ID Repositori	Nama repositori
amzn-utama/terbaru	Basis Utama AMZN
amzn-update/terbaru	AMZN-pembaruan-basis
epel/x86_64	Paket Ekstra untuk Enterprise Linux 6 - x86_64
pbis	Pembaruan Paket PBIS

- Repositori Red Hat Enterprise Linux yang telah dikonfigurasi sebelumnya (lima untuk Red Hat Enterprise Linux 7 dan lima untuk Red Hat Enterprise Linux 6):

ID Repositori	Nama repositori
Wilayah Rhui- -7/x86_64 client-config-server	Red Hat Update Infrastruktur 2.0 Konfigurasi Klien Ser
Wilayah Rhui- /7Server/X86_64 rhel-server-releases	Server Linux Perusahaan Red Hat 7
Wilayah Rhui- /7Server/X86_64 rhel-server-releases	Red Hat Enterprise Linux Server 7 RH Umum () RPMs
epel/x86_64	Paket Ekstra untuk Enterprise Linux 7 - x86_64
pbis	Pembaruan Paket PBIS

ID Repositori	Nama repositori
Wilayah Rhui- -6 client-config-server	Infrastruktur Pembaruan Red Hat 2.0
Wilayah Rhui- rhel-server-releases	Server Linux Perusahaan Red Hat 6 (RPMs)
Wilayah Rhui- rhel-server-rh-common	Red Hat Enterprise Linux Server 6 RH Umum () RPMs
epel	Paket Ekstra untuk Enterprise Linux 6 - x86_64
pbis	Pembaruan Paket PBIS

- CentOS 7 repositori yang telah dikonfigurasi sebelumnya (biasanya lima):

ID Repositori	Nama Repositori
dasar/7/x86_64	CentOS-7 - Dasar
pembaruan/7/x86_64	CentOS-7 - Pembaruan
tambahan/7/x86_64	CentOS-7 - Ekstra
epel/x86_64	Paket Ekstra untuk Enterprise Linux 7 - x86_64
pbis	Pembaruan Paket PBIS

- Untuk Microsoft Windows Server, semua pembaruan terdeteksi dan diinstal menggunakan Agen Pembaruan Windows, yang dikonfigurasi untuk menggunakan katalog Pembaruan Windows (ini tidak termasuk pembaruan dari Pembaruan Microsoft).

Pada sistem operasi Microsoft Windows, Patch Manager menggunakan file taksi Microsoft wsusscn2.cab sebagai sumber pembaruan keamanan sistem operasi yang tersedia. File ini berisi informasi tentang pembaruan terkait keamanan yang diterbitkan Microsoft. Patch Manager mengunduh file ini secara teratur dari Microsoft dan menggunakannya untuk memperbarui kumpulan tambalan yang tersedia untuk instance Windows. File hanya berisi pembaruan yang

diidentifikasi Microsoft sebagai terkait dengan keamanan. Saat informasi dalam file diproses, Patch Manager juga menghapus pembaruan yang telah diganti dengan pembaruan selanjutnya. Oleh karena itu, hanya pembaruan terbaru yang ditampilkan dan tersedia untuk instalasi. Misalnya, jika KB4 012214 menggantikan KB3135456, hanya KB4 012214 yang tersedia sebagai pembaruan di Patch Manager.

Untuk membaca selengkapnya tentang file wsusscn2.cab, lihat artikel Microsoft [Menggunakan WUA untuk Memindai Pembaruan Offline](#).

Patching dan desain infrastruktur

AMS menggunakan metode penambalan yang berbeda tergantung pada desain infrastruktur Anda: dapat berubah atau tidak dapat diubah (untuk definisi terperinci, lihat). [Istilah kunci AMS](#)

Dengan infrastruktur yang dapat berubah, penambalan dilakukan dengan menggunakan metodologi tradisional di tempat untuk menginstal pembaruan langsung ke EC2 instans Amazon, secara individual, oleh insinyur operasi AMS. Metode penambalan ini digunakan untuk tumpukan yang bukan grup Auto Scaling, dan berisi satu instans EC2 Amazon atau beberapa instance. Dalam skenario ini, mengganti AMI yang menjadi dasar instance atau tumpukan akan menghancurkan semua perubahan yang dibuat pada sistem itu sejak pertama kali diterapkan, sehingga tidak dilakukan. Pembaruan diterapkan ke sistem yang sedang berjalan, dan Anda mungkin mengalami downtime sistem (tergantung pada konfigurasi tumpukan) karena aplikasi atau sistem restart. Ini dapat dikurangi dengan strategi Blue/Green pembaruan. Untuk informasi selengkapnya, lihat [AWS CodeDeploy Memperkenalkan Blue/Green Penerapan](#).

Dengan infrastruktur yang tidak dapat diubah, metode penambalan adalah penggantian AMI. Instance yang tidak dapat diubah diperbarui secara seragam menggunakan AMI yang diperbarui yang menggantikan AMI yang ditentukan dalam konfigurasi grup Auto Scaling. Rilis AMS diperbarui (yaitu, ditambah) AMIs setiap bulan, biasanya minggu Patch Tuesday. Bagian berikut menjelaskan cara kerjanya.

Cara kerja patching standar AMS

AMS menggunakan layanan Systems Manager Run Command untuk patching kritis bulanan yang dijadwalkan secara rutin dan sesuai kebutuhan, dengan dua metode penambalan utama, penggantian di tempat dan AMI, tergantung pada strategi penerapan infrastruktur Anda (bisa berubah vs tidak dapat diubah). Bagian ini menjelaskan layanan, jenis, metode, dan proses penambalan AMS.

AMS mendefinisikan dua jenis patch, yang dijadwalkan berbeda:

- Penambalan kritis: Pembaruan diterapkan secepat mungkin, setelah menerima pemberitahuan.
- Penambalan standar: Pembaruan vendor OS reguler dan diterapkan setiap bulan.

Patch diterapkan baik melalui penambalan di tempat atau penggantian AMI (atas permintaan).

Perbarui pemindaian

AMS menggunakan [Amazon EC2 Run Command Service](#) untuk menghubungi EC2 tumpukan Amazon Anda dan menerapkan skrip pemindaian dan penambalan yang diperlukan. AMS menggunakan komponen manajemen paket asli yang sudah diinstal pada sistem operasi yang didukung untuk melakukan semua perilaku pemindaian dan penambalan yang diperlukan di EC2 tumpukan Amazon. Untuk Red Hat dan Amazon Linux, layanan ini menggunakan yum. Untuk Windows, layanan ini menggunakan Agen Pembaruan Windows.

Pemindaian dilakukan setiap hari menggunakan [SSM Maintenance Windows](#) dan dokumen AWS default AMS. RunPatchBaseline Setiap EC2 tumpukan Amazon yang dapat dijangkau dipindai, menggunakan repositori pembaruan untuk Linux dan Windows. Proses penambalan AMS mendeteksi semua tumpukan EC2 Amazon yang dapat dijangkau dan kemudian melakukan pemindaian dalam proses batch sehingga tumpukan selalu tetap dalam keadaan sehat, bahkan jika terjadi kegagalan saat menjalankan pemindaian. Hasil pemindaian kemudian disimpan untuk setiap EC2 tumpukan Amazon.

Untuk melihat hasil pemindaian tumpukan atau instance, kirimkan permintaan layanan dengan ID tumpukan atau ID instance.

Proses penambalan AMS default adalah menginstal semua tambalan yang tersedia terlepas dari klasifikasi atau tingkat keparahan tambalan (misalnya, kritis versus standar). Pengecualian untuk ini adalah tambalan yang telah Anda kecualikan secara eksplisit untuk tumpukan (tambalan yang didefinisikan sebagai wajib oleh AMS tidak boleh dikecualikan).

Anda dikirim pemberitahuan layanan patching 14 hari sebelum jendela pemeliharaan yang diusulkan. Ini memberi Anda waktu untuk menguji tambalan yang diusulkan dan menerima atau menolaknya. Jika Anda tidak membalas notifikasi layanan patching, instance Anda tidak ditambal. Ketika saatnya tiba untuk menginstal patch, AMS membuat Request for Change (RFC) untuk setiap tumpukan, dan RFC itu muncul di daftar RFC akun Anda.

Jendela pemeliharaan dan pemberitahuan yang dikonfigurasi AMS

Dengan penambalan yang dikonfigurasi AMS, setiap akun memiliki jendela pemeliharaan bulanan, yang Anda tentukan saat Anda melakukan onboard akun. AWS Managed Services Maintenance Window (atau Maintenance Window) melakukan aktivitas pemeliharaan untuk AWS Managed Services (AMS) dan berulang pada hari Kamis kedua setiap bulan mulai pukul 15:00 hingga 16:00 Waktu Pasifik. AMS dapat mengubah jendela pemeliharaan dengan pemberitahuan 48 jam.

Jendela tambalan berbeda. Permintaan layanan keluar patching (juga dikenal sebagai pemberitahuan layanan) mencakup jendela patch yang disarankan.

Note

Untuk informasi tentang membalas notifikasi layanan patching, lihat [Tindakan yang dapat Anda lakukan dalam penambalan standar AMS](#)

Pemberitahuan layanan patching dikirim melalui email ke alamat email kontak pada file untuk akun Anda. Pemberitahuan tersebut menyertakan tautan ke konsol AWS Support tempat Anda dapat menanggapi. Anda juga dapat menanggapi pemberitahuan menggunakan halaman Permintaan Layanan AMS. Pemberitahuan layanan meliputi:

- Daftar pembaruan IDs (CSUs, IUs, dan OUs) yang berlaku untuk tumpukan, dan pembaruan yang Anda minta dikecualikan dari penambalan (jika ada).
- IDs contoh yang akan terpengaruh.
- Jendela tambalan yang diusulkan saat pembaruan akan diterapkan. Anda dapat meminta jendela tambalan yang berbeda.
- Permintaan agar Anda menerima penambalan yang diusulkan, atau meminta informasi tambahan. AMS memberi Anda waktu untuk menguji dampak pembaruan dan menyetujui atau menolak penambalan, atau meminta agar pembaruan tertentu dikecualikan. Jika Anda memerlukan lebih banyak waktu untuk menguji, dan ingin pembaruan diterapkan setelah pengujian Anda, tanggapilah pemberitahuan layanan dan jelaskan apa yang Anda inginkan, atau kirimkan permintaan layanan untuk RFC patch baru berdasarkan detail RFC sebelumnya. Jika Anda tidak membalas pemberitahuan layanan sama sekali, tidak ada tindakan penambalan yang diambil dan RFC dibatalkan.

Jika Anda menyetujui pemberitahuan layanan, AMS menjalankan patch RFC dan menerapkan pembaruan dalam jendela patch yang disepakati, sesuai komitmen layanan.

Ketika patching selesai, AMS mengirimkan korespondensi dalam Permintaan Layanan, dengan ringkasan hasil dari aktivitas patching (yaitu, berhasil atau gagal).

Penambalan di tempat

Penambalan di tempat mengacu pada metode di mana AMS masuk ke setiap instance tumpukan dan menerapkan tambalan.

Penambalan di tempat terjadi pada infrastruktur yang dapat berubah menggunakan instans EC2 Amazon yang menjalankan sistem operasi yang didukung. Patching menerapkan semua pembaruan yang tidak dikecualikan yang tersedia hingga saat itu. Ketika tambalan kritis dilepaskan, ada proses penambalan penting tambahan.

Penambalan standar: di tempat

Penambalan standar terjadi pada jadwal patch yang disepakati yang disarankan dalam pemberitahuan layanan tambalan, dan mencakup pembaruan tambalan reguler yang tidak dianggap penting.

Sebelum jendela patching yang diusulkan, dan dengan tanggapan afirmatif Anda terhadap notifikasi, patch RFC dibuat dan muncul di dasbor RFC Anda.

Penambalan kritis: di tempat

Saat vendor OS merilis pembaruan keamanan penting, AMS memberi tahu Anda tentang patch RFC dengan mengirimkan pemberitahuan layanan (ke email kontak untuk akun Anda) untuk setiap tumpukan, sesuai dengan komitmen layanan AMS. Pemberitahuan layanan mencakup hal-hal berikut untuk setiap pembaruan:

- Perbarui tanggal rilis
- Perbarui kekritisannya
- Perbarui detail (referensi KB, dll.)
- IDs tumpukan yang terpengaruh

Anda dapat menguji pembaruan yang tercantum dalam notifikasi, dan menyetujui atau menolak tambalan dengan membalas pemberitahuan layanan. Jika Anda menyetujui pemberitahuan, Anda perlu menyediakan jendela patch tertentu per tumpukan untuk menginstal pembaruan.

Note

Jendela tambalan yang berada dalam waktu 24 jam setelah membalas pemberitahuan layanan dapat dijadwal ulang berdasarkan kapasitas yang tersedia.

Jika Anda tidak membalas dalam waktu 10 hari atau jika Anda menolak tambalan yang diusulkan, tambalan dibatalkan.

Jika Anda ingin menerapkan pembaruan setelah periode yang diizinkan (disediakan dalam pemberitahuan), kirimkan permintaan layanan untuk jadwal tambalan baru berdasarkan detail pemberitahuan sebelumnya.

Jika Anda menyetujui pemberitahuan layanan, AMS menerapkan pembaruan dalam jendela tambalan yang Anda tentukan, sesuai dengan komitmen layanan.

Dalam kasus beberapa pembaruan, Anda dapat mengecualikan pembaruan tertentu dari penambalan dengan menentukan pembaruan yang akan dikecualikan dalam tanggapan Anda terhadap pemberitahuan layanan.

AMS mengirimkan pemberitahuan layanan untuk setiap tumpukan, dari hasil setiap pembaruan (yaitu, berhasil atau gagal).

AMI memperbarui patching (menggunakan patch AMIs untuk grup Auto Scaling)

Penambalan penggantian AMI dilakukan pada infrastruktur yang tidak dapat diubah dengan memperbarui ID AMI yang dikonfigurasi untuk menerapkan instans EC2 Amazon baru dalam grup Auto Scaling.

Amazon Machine Images (AMIs) dirilis secara teratur untuk sistem operasi yang didukung. Vendor sistem operasi merilis tambalan baru secara berkala. AMS mengambil AMI yang disediakan Amazon, memperbaruinya dengan tambalan terbaru, dan kemudian menambahkan komponen yang sesuai untuk memungkinkannya beroperasi di lingkungan AMS. Kemudian, AMS AMI baru tersedia untuk semua pelanggan AMS dengan membagikan AMI ke akun. Tumpukan grup Auto Scaling Anda dapat disegarkan setiap bulan dengan AMS yang baru dirilis ini. AMIs Grafik berikut mengilustrasikan bagaimana AMIs digunakan di AMS lingkungan Anda.

Grup Auto Scaling membuat instance-nya berdasarkan AMI yang dikonfigurasi untuk grup Auto Scaling. Saat pembagian AMS diperbarui AMIs, Anda memiliki opsi berikut tergantung pada cara Anda mengelola pembaruan AMI:

- Jika Anda menggunakan alat penyebaran aplikasi (misalnya, UserData CodeDeploy, dan sebagainya) yang menyesuaikan instance Anda secara otomatis setelah dibuat, Anda dapat melakukan hal berikut:
 - Balas pemberitahuan layanan patching, atau kirimkan permintaan layanan, untuk AMS AMI terbaru untuk menggantikan AMI konfigurasi grup Auto Scaling Anda saat ini. Setelah ID AMI dalam konfigurasi grup Auto Scaling diganti, AMS memulai pembaruan bergulir instans Anda dan konfigurasi instans grup Auto Scaling Anda (misalnya, menginstal aplikasi, skrip boot, dll.) diterapkan ke instans baru yang dibuat dengan AMS AMI baru secara otomatis.
- Jika Anda menggunakan custom/golden AMI dalam konfigurasi grup Auto Scaling, Anda dapat:
 - Buat instance dengan AMS AMI baru, sesuaikan instance, dan buat AMI emas baru. Bagikan AMI emas baru dengan AMS menggunakan EC2 konsol Amazon, dan kirimkan permintaan layanan ke AMS untuk memperbarui konfigurasi grup Auto Scaling Anda untuk menggunakan AMI kustom baru Anda.
 - Bagikan AMI emas Anda yang ada dengan AMS dengan menggunakan EC2 konsol Amazon, dan kirimkan permintaan layanan AMS untuk memperbarui AMI emas Anda. Untuk melakukan ini, AMS membuat instance dari AMI emas Anda, menerapkan tambalan ke instance itu, membuat AMI emas baru untuk Anda, dan kemudian memperbarui konfigurasi grup Auto Scaling Anda untuk menggunakan AMI baru. Kekurangannya di sini adalah AMS tidak dapat menguji apakah AMI kustom baru Anda bekerja seperti yang Anda inginkan. Sebagai gantinya, Anda harus menguji instance yang dibuat dengan AMI baru dan memverifikasi bahwa semuanya berfungsi dengan benar sebelum membuat AMI emas baru, membagikannya, dan meminta AMS memperbarui grup Auto Scaling Anda. AMS tidak merekomendasikan opsi ini.

Penambalan standar: Pembaruan AMI

Setiap bulan AMS merilis Amazon Machine Images (AMIs) baru dengan peningkatan layanan dan tambalan baru yang berlaku untuk AMIs

Note

AMS baru AMIs dihasilkan setelah Patch Tuesday dari AWS yang diperbarui AMIs. Kemudian, AMS mengujinya sebelum membuatnya tersedia. Setelah pengujian AMIs lulus baru, saham AMS diperbarui AMIs ke akun terkelola.

Penambalan kritis: Pembaruan AMI

Bila diperlukan, AMS menyediakan AMIs update dengan patch keamanan penting yang dirilis sejak rilis AMI bulanan terakhir.

Proses untuk pembaruan keamanan penting untuk infrastruktur yang tidak dapat diubah identik dengan proses AMI bulanan untuk infrastruktur yang tidak dapat diubah, kecuali bahwa AMS AMI baru dibuat di luar jadwal normal (Patch Tuesday), berdasarkan rilis pembaruan penting baru. AMS menyediakan AMI baru dengan patch keamanan penting sesuai dengan perjanjian tingkat layanan (SLAs) yang ditentukan untuk akun Anda. Pembaruan AMS grup Auto Scaling hanya berdasarkan permintaan. Gunakan permintaan layanan untuk mengirimkan permintaan penggantian AMI.

Kegagalan penambalan standar AMS

Jika terjadi pembaruan yang gagal, AMS melakukan analisis untuk memahami penyebab kegagalan dan mengkomunikasikan hasil analisis kepada Anda. Jika kegagalan disebabkan oleh AMS, kami mencoba lagi pembaruan jika berada dalam jendela pemeliharaan. Jika tidak, AMS akan membuat notifikasi layanan untuk pembaruan instans yang gagal dan menunggu instruksi Anda.

Untuk kegagalan yang disebabkan oleh sistem Anda, Anda dapat mengirimkan permintaan layanan dengan RFC patch baru untuk memperbarui instance.

Tindakan yang dapat Anda lakukan dalam penambalan standar AMS

Selain menguji yang baru AMIs, ada beberapa tindakan yang dapat Anda ambil untuk mengelola penambalan infrastruktur Anda:

- Jika membutuhkan waktu lebih lama untuk menguji pembaruan daripada jendela tambalan yang diizinkan, Anda dapat meminta AMS menerapkan pembaruan yang dibatalkan saat Anda siap dengan mengirimkan permintaan layanan (gunakan detail dalam pemberitahuan layanan asli sebagai dasarnya).

- Anda dapat meminta pembaruan penting (IU) atau pembaruan lainnya (OU) diterapkan sebelum jendela pembaruan otomatis berikutnya dengan mengirimkan permintaan layanan yang menyediakan daftar pembaruan, contoh yang berlaku, dan detail lainnya yang sesuai. Karena CT ini tidak otomatis, dibutuhkan waktu lebih lama untuk menjadwalkan dan menjalankan. Periksa tujuan tingkat layanan (SLOs) untuk waktu yang tepat. Untuk informasi selengkapnya, lihat [Tujuan tingkat layanan AMS \(SLOs\)](#).

Selain itu, Anda dapat menggunakan AMS yang sudah ada, ditambah, AMIs untuk membuat kustom AMIs. Untuk selengkapnya, lihat [AMI | Buat](#).

 Note

Anda tidak dapat meminta AMS AMI baru berdasarkan pembaruan penting atau pembaruan lain sebelum jendela pemeliharaan berikutnya karena proses rilis AMS AMI mengikuti irama seragam untuk kepentingan semua pelanggan AMS.

Mengubah apa yang patched/opting keluar

Dengan penambahan yang dikonfigurasi AMS, dalam respons Anda terhadap pemberitahuan layanan penambahan atau dalam Permintaan Layanan, Anda dapat mengubah sumber daya apa yang ditambah. Anda dapat melakukan tindakan berikut:

- Tentukan daftar tambalan yang harus dikecualikan dari remediasi, per tumpukan dan per sistem operasi.
- Tentukan daftar sumber daya yang harus dikecualikan dari tambalan tertentu atau semua tambalan.
- Tentukan daftar sumber daya yang harus selalu dikecualikan dari semua tambalan.
- Tentukan daftar sumber daya yang harus ditambah pada hari dan waktu tertentu (baik jika Anda belum menentukan jendela pemeliharaan).

Untuk mengecualikan satu atau beberapa tambalan, kirimkan permintaan layanan, atau tanggapilah pemberitahuan layanan penambahan menggunakan templat yang disediakan berikutnya. Jangan mengirimkan RFC. Sertakan dalam permintaan nama tambalan atau nama yang ingin Anda kecualikan dan alasannya. Sertakan informasi ini dalam Permintaan Layanan sebagai berikut:

- Nama: Nama tambalan. Untuk patch Windows, ini adalah nama KB, seperti KB3145384. Untuk patch Linux, ini adalah nama paket, seperti `openssh-6.6.1p1-25.61.amzn1.x86_64`.
- Alasan: Komentar yang menunjukkan mengapa tambalan dikecualikan.
- Waktu Kedaluwarsa: date/time Saat pengecualian berakhir.

Jika patch yang dikecualikan sudah diinstal, itu dihapus.

Permintaan ditinjau oleh operator yang akan mendiskusikannya dengan Anda jika mengecualikan tambalan tersebut menimbulkan risiko keamanan yang signifikan. Tanggal kedaluwarsa untuk patch yang dikecualikan juga dinegosiasikan. Setelah tanggal kedaluwarsa yang disepakati, pengecualian berakhir, dan tambalan diinstal pada tambalan berikutnya.

Tambalan pada daftar pengecualian masih dikembalikan dalam hasil pemindaian, jika berlaku.

Note

Tidak seperti Windows, patch Linux adalah versi khusus. Perbedaan ini penting karena versi baru dari patch yang dikecualikan tidak dikecualikan secara otomatis. Adalah tanggung jawab Anda untuk memberi tahu AMS untuk mengecualikan versi baru dari patch Linux jika itu yang ingin Anda lakukan.

Templat balasan pemberitahuan layanan tambalan

Anda harus membalas pemberitahuan layanan penambalan, menggunakan format yang ditentukan, agar penambalan dapat dilakukan pada instance Anda. Anda harus melakukan ini jika Anda belum mengatur jendela pemeliharaan dengan AMS.

Saat Anda membalas pemberitahuan layanan, gunakan format yang diberikan.

Jika tidak ada jendela pemeliharaan yang disetel, beri tahu kami kapan harus menambal apa yang ditunjukkan berikut:

UTC	StartTime	StackId	InstanceId (Optional)
2019-04-01	15:00	stack-123456789012	i-1234566789
2019-04-01	15:00	stack-123456789013	i-1234566784
2019-04-01	15:00	stack-123456789014	i-1234566783
2019-04-01	15:00	stack-123456789015	i-1234566782

Jika Anda memiliki jendela pemeliharaan yang ditetapkan dan ingin sumber daya tertentu dikecualikan dari tambalan tertentu, gunakan format berikut:

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	<i>PATCH</i>
stack-123456789013	i-1234566784	<i>PATCH</i>
stack-123456789014	i-1234566783	<i>PATCH</i>
stack-123456789015	i-1234566782	<i>PATCH</i>

Jika Anda memiliki jendela pemeliharaan yang ditetapkan dan ingin sumber daya tertentu selalu dikecualikan dari semua tambalan, gunakan format berikut:

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	ALL
stack-123456789015	i-1234566782	ALL

Mempersiapkan penambalan

Untuk mempersiapkan lingkungan Anda untuk penambalan otomatis, kami merekomendasikan hal berikut:

- Pastikan Anda memiliki inventaris lengkap dari semua instance yang akan ditambah.
- Pastikan sumber daya Anda didukung secara teratur sebagai bagian dari strategi Continuity of Business Anda. Cadangan tambahan dibuat sebagai bagian dari urutan tambalan, dan ini secara otomatis dihapus sesuai dengan kebijakan retensi Patch Orchestrator Anda yang dikonfigurasi (defaultnya adalah 60 hari).
- Pastikan bahwa semua lisensi yang relevan mutakhir.
- Ubah jendela pemeliharaan tumpukan Anda menjadi tambalan terhuyung-huyung sehingga tumpukan pengujian ditambah sebelum tumpukan produksi. Dengan begitu, kesalahan apa pun dengan penambalan ditemukan di tumpukan pengujian dan dapat diidentifikasi sebelum tumpukan produksi ditambah.

Melihat pengaturan tambalan

Untuk mengetahui konfigurasi patching Anda saat ini, Anda dapat melakukan hal berikut:

- Kirim permintaan layanan ke AMS dengan kueri.

- Tunggu pemberitahuan layanan tambalan. Pemberitahuan penambalan menyarankan Anda tentang semua tambalan yang akan diterapkan dan contoh yang akan ditambal, dan juga menyarankan jendela tambalan.

Anda dapat mengirimkan permintaan layanan untuk memodifikasi hal-hal berikut:

- Interval Pemindaian: Jumlah waktu, dalam hitungan menit, antara pemindaian kepatuhan yang dilakukan pada contoh tumpukan ini.

Default adalah 240 (4 jam).

- NotificationWindow: Seberapa jauh sebelumnya (dalam hitungan menit) dari perubahan terjadwal (tambalan) pemberitahuan harus dikirimkan kepada Anda. Default adalah 10080 (7 hari).

Penambalan standar AMS FAQs

Bagian ini memberikan jawaban atas beberapa pertanyaan yang sering diajukan.

- T: Bagaimana cara memilih keluar dari patching secara global?

J: Untuk memilih keluar dari penambalan secara global, ajukan permintaan layanan. Perhatikan bahwa Anda tidak dapat memilih keluar dari patch wajib AMS. Semua tumpukan akan terus dipindai sehingga kami dapat melaporkan kerentanan.

- T: Bagaimana cara mengecualikan tumpukan tertentu dari penambalan?

J: Untuk secara permanen mengecualikan tumpukan tertentu dari penambalan, kirimkan permintaan layanan. Untuk mengecualikan tumpukan tertentu dari siklus tambalan tertentu, tanggapilah pemberitahuan penambalan yang akan datang dengan daftar tumpukan yang akan dikecualikan. Untuk informasi, lihat [Mengubah apa yang patched/patching keluar](#). Perhatikan bahwa Anda tidak dapat memilih keluar dari patch wajib.

- T: Apa yang terjadi jika saya tidak menyetujui pemberitahuan layanan patching?

J: Anda memiliki 14 hari untuk menyetujui permintaan layanan patching standar dan 10 hari untuk menyetujui pemberitahuan patch kritis. Jika Anda tidak menyetujui permintaan layanan dalam jangka waktu tersebut, komitmen layanan dibatalkan dan tidak ada penambalan yang terjadi.

Dalam hal penambalan wajib, tambalan diterapkan terlepas dari respons terhadap permintaan layanan.

- T: Bagaimana cara mengecualikan patch dan paket tertentu agar tidak diinstal?

J: Untuk mengecualikan patch atau paket tertentu secara permanen, kirimkan permintaan layanan. Untuk mengecualikan tambalan atau paket tertentu dari siklus tambalan tertentu, tanggapilah pemberitahuan tambalan yang akan datang dengan daftar tambalan atau paket yang akan dikecualikan. Lihat perinciannya di [Mengubah apa yang patched/opting keluar](#). Perhatikan bahwa Anda tidak dapat memilih keluar dari patch wajib.

- T: Apa yang terjadi jika sistem gagal sebagai akibat dari patching?

A: AMS memonitor setiap sistem. AMS mengirimkan pemberitahuan layanan kepada Anda tentang hasil setiap pembaruan (yaitu, berhasil atau gagal) per tumpukan dan instance. Jika kegagalan terdeteksi, AMS menyelidiki, bekerja untuk memulihkan instance, dan kemudian insinyur operasi AMS mencoba menambal secara manual. Untuk informasi, lihat [Kegagalan penambalan standar AMS](#).

- T: Pembaruan apa yang dikelola oleh AMS?

J: AMS mengelola pembaruan tingkat sistem operasi yang diberitahukan AMS oleh vendor. Untuk informasi selengkapnya, lihat [Patch yang didukung](#).

- T: Pembaruan apa yang tidak dikelola oleh AMS?

J: Pembaruan tingkat aplikasi tidak dikelola oleh AMS.

- T: Bagaimana grup Auto Scaling diperbarui?

J: Grup Auto Scaling diperbarui dengan penggantian AMI dalam konfigurasi grup Auto Scaling dan membentuk pembaruan bergulir. Pembaruan bergulir mengamati HealthyHostThreshold pengaturan konfigurasi tambalan Anda, yang menentukan berapa banyak EC2 instans Amazon dalam tumpukan yang harus dipertahankan aktif selama penambalan. Untuk informasi

selengkapnya, lihat [AMI memperbarui patching \(menggunakan patch AMIs untuk grup Auto Scaling\)](#).

- T: Bagaimana cara menginstal pembaruan di luar siklus normal?

J: Untuk pembaruan tingkat OS yang ingin Anda instal di luar jadwal penambalan normal, kirimkan permintaan layanan dengan menggunakan notifikasi tambalan yang Anda terima. Ini mungkin terjadi jika pengujian patch yang diusulkan Anda memakan waktu lebih dari 21 hari (untuk tambalan standar) atau 14 hari (untuk tambalan kritis). Out-of-band penambalan dapat dilakukan di tempat untuk instance Amazon EC2 mandiri.

- T: Bagaimana tumpukan atau instance yang baru diterapkan ditambah?

J: Saat membuat instans EC2 tumpukan Amazon baru atau grup Auto Scaling, Anda harus selalu menentukan AMS AMI terbaru, yang sudah memiliki tambalan terbaru. Untuk infrastruktur yang dapat berubah, penambalan sebaris harus dilakukan segera setelah tumpukan diterapkan.

Menambal komitmen layanan

Berdasarkan jenis penyebaran infrastruktur Anda, dan kekritisannya pembaruan, kami menyediakan komitmen layanan untuk pembaruan keamanan penting untuk infrastruktur yang dapat berubah dan tidak dapat diubah, dan pembaruan penting untuk infrastruktur yang dapat berubah dan tidak dapat diubah.

Penambalan standar

Ini adalah komitmen layanan AMS untuk patching standar.

Penambalan standar, infrastruktur yang dapat berubah (penambalan di tempat)

Acara/Aksi	Pengukuran komitmen layanan
Pembaruan Penting dirilis dalam sebulan.	Jam dimulai

Acara/Aksi	Pengukuran komitmen layanan
Empat belas hari sejak pemberitahuan patch standar dibuat, AMS memberi tahu Anda tentang penambalan yang direncanakan yang akan datang melalui pemberitahuan layanan dan melalui email untuk setiap tumpukan. Pemberitahuan layanan meliputi: • Daftar pembaruan IDs (CSUs dan IUs) yang berlaku (diperlukan dan tidak diterapkan) untuk tumpukan, dan pembaruan tersebut dikecualikan dari penambalan • IDs tumpukan yang terpengaruh • Jendela pemeliharaan saat pembaruan akan diterapkan	Jam berhenti setelah pemberitahuan layanan dikirim.
Anda menguji dampak pembaruan dan menyetujui atau menolak RFC. Jika Anda tidak membalas dalam 14 hari atau Anda menolak penambalan dalam tanggapan Anda terhadap pemberitahuan layanan, tidak ada tindakan yang diambil. Jika Anda membutuhkan waktu lebih dari 14 hari untuk menguji, dan ingin pembaruan diterapkan setelah periode 14 hari, kirimkan permintaan layanan untuk RFC patch baru berdasarkan rincian RFC sebelumnya.	Jika Anda tidak menyetujui atau membalas dalam 14 hari, perubahan yang tertunda dibatalkan dan komitmen layanan untuk pembaruan tidak berlaku.

Acara/Aksi	Pengukuran komitmen layanan
Jika Anda menyetujui pemberitahuan layanan dalam waktu 14 hari, AMS menerapkan pembaruan. Anda dapat memilih untuk mengecualikan pembaruan tertentu dari RFC dengan menentukan pembaruan yang akan dikecualikan dalam tanggapan Anda terhadap pemberitahuan layanan.	Jam dimulai jika Anda menyetujui pemberitahuan layanan dalam waktu 14 hari sejak diterimanya. Jam berhenti setelah instalasi pembaruan telah dicoba.
AMS mengirimkan pemberitahuan layanan kepada Anda tentang hasil dari setiap pembaruan yang dicoba. Pemberitahuan layanan mencakup rincian berikut: • ID EC2 contoh Amazon • Pembaruan 1 Sukses/Gagal: ARN a1, ARN a2... • Pembaruan 2 Sukses/Gagal: ARN b1, ARN b2... • Pembaruan N Sukses/Gagal: ARN c1, ARN c2...	Tidak berlaku.
Jika terjadi pembaruan yang gagal, AMS melakukan analisis untuk memahami penyebab kegagalan dan mengkomunikasikan hasil analisis kepada Anda. Jika kegagalan disebabkan oleh AMS, AMS akan mencoba ulang pembaruan jika dalam jendela pemeliharaan, jika tidak, AMS akan membuat pemberitahuan layanan untuk kombinasi pembaruan instans yang gagal dan menunggu instruksi Anda di jendela pemeliharaan.	Tidak berlaku.

Acara/Aksi	Pengukuran komitmen layanan
Untuk kegagalan yang disebabkan oleh Anda, kirimkan permintaan layanan untuk RFC patch baru untuk memperbarui instance.	Tidak berlaku.

Penambalan kritis

Ini adalah komitmen layanan AMS untuk pembaruan keamanan penting.

Pembaruan keamanan kritis, infrastruktur yang dapat berubah

Acara/Aksi	Pengukuran komitmen layanan
CSU dirilis.	Jam dimulai
AMS memberi tahu Anda tentang patch RFC melalui pemberitahuan layanan (yang juga mengirim email) untuk setiap tumpukan. Pemberitahuan layanan meliputi: • Pembaruan tanggal rilis • Perbarui kekritisannya • Perbarui detail: referensi KB, dan sebagainya • IDs tumpukan yang terpengaruh	Jam berhenti setelah pemberitahuan layanan dikirim.
Anda menguji pembaruan yang tercantum dalam RFC, dan menyetujui atau menolak RFC dalam waktu 10 hari dengan membalas pemberitahuan layanan. Anda menyediakan jendela pemeliharaan khusus (per tumpukan) untuk menginstal pembaruan. Jendela pemeliharaan yang ditentukan dalam waktu 24 jam setelah membalas pemberitahuan layanan dapat dijadwal ulang berdasarkan kapasitas yang tersedia.	Jika Anda tidak menyetujui atau membalas dalam 14 hari, perubahan yang tertunda dibatalkan dan komitmen layanan untuk pembaruan tidak berlaku.

Acara/Aksi	Pengukuran komitmen layanan
Jika Anda tidak membalas dalam 10 hari, atau jika Anda menolak patch RFC, tindakan yang tertunda dibatalkan. Jika Anda ingin menerapkan pembaruan setelah periode 14 hari, kirimkan permintaan layanan untuk RFC patch baru berdasarkan rincian RFC sebelumnya.	
Jika Anda menyetujui pemberitahuan layanan, AMS menerapkan pembaruan. Untuk beberapa pembaruan, Anda dapat memilih untuk mengecualikan pembaruan tertentu dari perubahan dengan menentukan pembaruan yang akan dikecualikan dalam tanggapan Anda terhadap pemberitahuan layanan.	Jika jendela pemeliharaan yang diinginkan tidak berada dalam jangka waktu komitmen layanan, komitmen layanan untuk pembaruan terlewatkan hanya jika RFC tidak dijalankan dalam jendela pemeliharaan yang diinginkan.
AMS mengirimkan pemberitahuan layanan kepada Anda tentang hasil dari setiap pembaruan yang diterapkan. Pemberitahuan layanan mencakup rincian berikut: • ID EC2 contoh Amazon • Update Sukses: ARN a1, ARN a2... • Pembaruan Gagal: ARN c1, ARN c2...	Tidak berlaku.

Acara/Aksi	Pengukuran komitmen layanan
Jika terjadi pembaruan yang gagal, AMS melakukan analisis untuk memahami penyebab kegagalan dan mengkomunikasikan hasil analisis kepada Anda. Jika kegagalan disebabkan oleh AMS, AMS akan mencoba ulang pembaruan jika dalam jendela pemeliharaan, jika tidak, AMS akan membuat pemberitahuan layanan untuk kombinasi pembaruan instans yang gagal dan menunggu instruksi Anda di jendela pemeliharaan baru.	Tidak berlaku.
Untuk kegagalan yang disebabkan oleh Anda, kirimkan permintaan layanan untuk RFC patch baru untuk memperbarui instance.	Tidak berlaku.

Pembaruan keamanan kritis, infrastruktur yang tidak dapat diubah

Acara/Aksi	Pengukuran komitmen layanan
CSU dirilis.	Jam dimulai
AMS memberi tahu Anda tentang hal berikut melalui pemberitahuan layanan: • Perbarui tanggal rilis • Perbarui kekritisannya • Perbarui detail (referensi KB, dan sebagainya) • Gambar Mesin Amazon AMS (AMI) terpengaruh • Tanggal dan waktu rilis yang diantisipasi untuk pembaruan baru AMIs	Jam terus berjalan.
Rilis AMS diperbarui AMIs di akun terkelola.	Jam berhenti.

Acara/Aksi	Pengukuran komitmen layanan
Jika Anda menyetujui pemberitahuan layanan, AMS menerapkan pembaruan. AMS memberi tahu Anda tentang yang AMIs dibagikan di akun Anda, melalui pemberitahuan layanan, dan melalui email.	Tidak berlaku.
Jika pengujian yang baru AMIs membutuhkan waktu lebih lama dari waktu yang ditentukan (satu minggu), Anda dapat mengirimkan permintaan layanan ke AMS untuk memperbarui grup Auto Scaling Anda dengan AMS AMI baru (sebagaimana adanya). Jika Anda ingin memodifikasi AMS AMI baru dengan konfigurasi Anda, gunakan RFC dengan Manajemen Lainnya Lainnya Perbarui CT (ct-0xdawir96cy7k) untuk meminta kami memperbarui grup Auto Scaling Anda.	Tidak berlaku.

Laporan dan opsi

AWS Managed Services (AMS) mengumpulkan data dari berbagai layanan AWS asli untuk memberikan laporan bernilai tambah tentang penawaran AMS utama.

AMS menawarkan dua jenis pelaporan terperinci:

- Berdasarkan laporan permintaan: Anda dapat meminta laporan tertentu secara ad hoc melalui Cloud Service Delivery Manager (CSDM). Laporan ini tidak memiliki batasan karena Anda mungkin perlu memintanya beberapa kali selama acara orientasi atau kritis. Namun, ketahuilah bahwa laporan ini tidak dirancang untuk disediakan sesuai jadwal seperti laporan mingguan. Untuk lebih memahami kebutuhan Anda atau untuk informasi lebih lanjut tentang penggunaan pelaporan swalayan, hubungi CSDM Anda.
- Laporan layanan mandiri: Laporan layanan mandiri AMS memungkinkan Anda untuk secara langsung menanyakan dan menganalisis data sesering yang Anda butuhkan. Gunakan laporan layanan mandiri untuk mengakses laporan dari konsol AMS dan melaporkan kumpulan data melalui bucket S3 (satu bucket per akun). Ini memungkinkan Anda untuk mengintegrasikan data ke alat Business Intelligence (BI) favorit Anda sehingga Anda dapat menyesuaikan laporan untuk kebutuhan Anda.

Topik

- [Laporan berdasarkan permintaan](#)
- [Laporan layanan mandiri](#)

Laporan berdasarkan permintaan

Topik

- [Laporan AMS Patch](#)
- [Laporan Cadangan AMS](#)
- [Insiden Mencegah dan Memantau Laporan Pembicara Teratas](#)
- [Laporan Detail Biaya Penagihan](#)
- [Laporan Remediator Terpercaya](#)

AMS mengumpulkan data dari berbagai layanan AWS asli untuk memberikan laporan nilai tambah pada penawaran AMS utama. Untuk salinan laporan ini, buat permintaan ke Cloud Service Delivery Manager (CSDM) Anda.

Laporan AMS Patch

Laporan yang tersedia

- [Laporan Ringkasan Detail Instans Patch](#)
- [Laporan Detail Patch](#)
- [Contoh yang Melewatkan Laporan Patch](#)
- [Menambal laporan Cakupan SSM](#)

Laporan Ringkasan Detail Instans Patch

Laporan Ringkasan Detail Instance Patch menyediakan detail instans yang dikumpulkan untuk instance yang onboard ke pelaporan. Ini adalah laporan informasi yang membantu mengidentifikasi semua instance onboard, status akun, detail instans, cakupan jendela pemeliharaan, waktu eksekusi jendela pemeliharaan, detail tumpukan, dan jenis platform. Laporan ini memberikan yang berikut:

1. Data tentang contoh produksi dan non-produksi akun. Catatan: Tahap produksi dan non-produksi berasal dari Nama Akun dan bukan dari Tag Instance.
2. Data tentang distribusi instance menurut jenis platform. Catatan: Jenis platform 'N/A' adalah ketika tidak AWS Systems Manager dapat mengambil informasi platform.
3. Data tentang distribusi status instans, dan jumlah instance yang berjalan, dihentikan, atau dihentikan.

Nama Bidang	Definisi
Laporkan Datetime	Tanggal dan waktu laporan dibuat.
ID akun	AWS Account ID yang memiliki ID instans
Nama Akun	Nama akun AWS
Akun Produksi	Pengidentifikasi prod AMS, akun non-prod, tergantung pada apakah nama akun menyertak

Nama Bidang	Definisi
	an nilai 'PROD', 'NONPROD'. Contoh: PROD, NONPROD, Tidak Tersedia
Status Akun	Status akun AMS. Misalnya: AKTIF, TIDAK AKTIF
Komitmen layanan akun AMS	PREMIUM, PLUS
Zona Pendaratan	Tandai untuk jenis landing zone akun. Misalnya: MALZ, NON-MALZ
Pembatasan Akses	Wilayah yang aksesnya dibatasi. Misalnya: TANAH AS
Id Instance	ID EC2 contoh
Nama Instance	Nama EC2 contoh
Jenis Platform Instance	Jenis Sistem Operasi (OS). Misalnya: Windows, Linux, dan sebagainya
Nama Platform Instance	Nama Sistem Operasi (OS). Misalnya: MicrosoftWindowsServer 2012R2Standard, RedHatEnterpriseLinuxServer
Nama Stack	Nama tumpukan yang berisi instance
Jenis Tumpukan	AMS stack (infrastruktur AMS dalam akun pelanggan) atau Customer stack (infrastruktur terkelola AMS yang mendukung aplikasi pelanggan). Contoh: AMS, PELANGGAN
Nama Grup Auto Scaling	Nama Grup Auto Scaling (ASG) yang berisi instance

Nama Bidang	Definisi
Grup Patch Instance	Nama grup tambalan digunakan untuk mengelompokkan instance bersama-sama dan menerapkan jendela pemeliharaan yang sama. Jika grup tambalan tidak ditetapkan, nilainya akan menjadi “Tidak Ditugaskan”
Jenis Grup Patch Instance	Jenis grup tambalan. DEFAULT: grup patch default dengan jendela pemeliharaan default, ditentukan oleh <code>AMSDefaultPatchGroup:True</code> tag pada instance. PELANGGAN: grup tambalan yang dibuat pelanggan. NOT_ASSIGNED: tidak ada grup tambalan yang ditetapkan
Negara Instance	Status dalam siklus hidup EC2 instance. Contoh: TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING. Untuk informasi selengkapnya, lihat Siklus hidup instans.
Cakupan Jendela Pemeliharaan	Jika ada future Maintenance Window pada contoh ini. Contoh: COVERED atau NOT_COVERED
Tanggal Eksekusi Jendela Pemeliharaan	Lain kali jendela pemeliharaan diharapkan untuk dijalankan. Jika NULL, eksekusi jendela tunggal, yaitu tidak berulang

Laporan Detail Patch

Laporan Detail Patch AWS Managed Services (AMS) menyediakan detail tambalan dan cakupan jendela pemeliharaan berbagai instans, termasuk:

1. Data pada grup Patch dan jenisnya.
2. Data tentang Pemeliharaan Windows, durasi, cutoff, future dates eksekusi jendela pemeliharaan (jadwal) dan instance yang terpengaruh di setiap jendela.
3. Data pada semua sistem operasi di bawah akun dan jumlah contoh yang sistem operasi diinstal.

Nama Bidang	Definisi
Laporkan Datetime	Tanggal dan waktu laporan dibuat.
account-id	AWS Account ID yang memiliki ID instans
Nama Akun	Nama akun AWS
Id Instance	ID EC2 contoh
Akun Produksi	Pengidentifikasi prod AMS, akun non-prod, tergantung pada apakah nama akun menyertakan nilai 'PROD', 'NONPROD'. Jika data tidak tersedia nilainya akan “Tidak Tersedia”
Status Akun	Status akun AMS. Misalnya: AKTIF, TIDAK AKTIF
Jenis Platform Instance	Jenis Sistem Operasi (OS). Misalnya: Windows, Linux
Nama Platform Instance	Nama Sistem Operasi (OS). Misalnya: MicrosoftWindowsServer 2012R2Standard, RedHatEnterpriseLinuxServer
Jenis Tumpukan	AMS stack (infrastruktur AMS dalam akun pelanggan) atau tumpukan Pelanggan (infrastr

Nama Bidang	Definisi
	struktur terkelola AMS yang mendukung aplikasi (misalnya, pelanggan). Misalnya: AMS, PELANGGAN
Grup Patch Instance	Nama grup tambalan digunakan untuk mengelompokkan instance bersama-sama dan menerapkan jendela pemeliharaan yang sama. Jika grup tambalan tidak ditetapkan, nilainya akan menjadi "Tidak Ditugaskan"
Jenis Grup Patch Instance	Jenis grup tambalan. DEFAULT: grup patch default dengan jendela pemeliharaan default, ditentukan oleh <code>AMSDefaultPatchGroup:True</code> tag pada instance PELANGGAN: grup tambalan yang dibuat pelanggan UNASSED: tidak ada grup tambalan yang ditetapkan
Negara Instance	Status dalam siklus hidup EC2 instance. Misalnya: TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING Untuk informasi selengkapnya, lihat Siklus hidup instans.
Id Jendela Pemeliharaan	Pengidentifikasi jendela pemeliharaan
Status Jendela Pemeliharaan	Nilai yang mungkin diaktifkan atau DINONAKTIKAN.
Jenis Jendela Pemeliharaan	Jenis jendela pemeliharaan

Nama Bidang	Definisi
Jendela Pemeliharaan Tanggal Eksekusi Berikutnya	Lain kali jendela pemeliharaan diharapkan untuk dijalankan. Jika NULL, eksekusi jendela tunggal, yaitu tidak berulang
Jendela Pemeliharaan Eksekusi Terakhir	Terakhir kali jendela pemeliharaan dijalankan
Durasi Jendela Pemeliharaan (jam)	Durasi jendela pemeliharaan dalam beberapa jam
Cakupan Jendela Pemeliharaan	Cakupan jendela pemeliharaan
Id Dasar Patch	Patch baseline saat ini dilampirkan ke instance
Status Patch	Status kepatuhan patch secara keseluruhan. Misalnya: COMPLIANT, NON_COMPLIANT. Jika setidaknya ada satu tambalan yang hilang, instance dianggap tidak sesuai, jika tidak sesuai.
Sesuai - Total	Hitungan tambalan yang sesuai (semua tingkat keparahan)
Noncompliant - Total	Hitungan tambalan yang tidak sesuai (semua tingkat keparahan)
Sesuai - Kritis	Hitungan tambalan yang sesuai dengan tingkat keparahan “kritis”
Compliant - Tinggi	Hitungan tambalan yang sesuai dengan tingkat keparahan “tinggi”
Sesuai - Medium	Hitungan tambalan yang sesuai dengan tingkat keparahan “sedang”
Sesuai - Rendah	Hitungan tambalan yang sesuai dengan tingkat keparahan “rendah”

Nama Bidang	Definisi
Sesuai - Informasi	Hitungan tambalan yang sesuai dengan tingkat keparahan “informasional”
Sesuai - Tidak ditentukan	Hitungan tambalan yang sesuai dengan tingkat keparahan “tidak ditentukan”
Tidak patuh - Kritis	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “kritis”
Tidak patuh - Tinggi	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “tinggi”
Tidak Sesuai - Sedang	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “sedang”
Tidak patuh - Rendah	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “rendah”
Noncompliant - Informasi	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “informasional”
Tidak sesuai - Tidak ditentukan	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “tidak ditentukan”

Contoh yang Melewatkan Laporan Patch

Laporan AWS Managed Services (AMS) Instance That Missed Patches memberikan detail tentang instans yang melewati patch selama eksekusi jendela pemeliharaan terakhir, termasuk:

1. Data pada patch yang hilang di tingkat ID patch.
2. Data pada semua instance yang memiliki setidaknya satu tambalan hilang bersama dengan atribut seperti keparahan patch, hari yang belum ditambah, rentang, dan tanggal rilis tambalan.

Nama Bidang	Definisi
Laporkan Datetime	Tanggal dan waktu laporan dibuat.
account-id	AWS Account ID yang memiliki ID instans
Nama Akun	Nama akun AWS
Akun Produksi	Pengidentifikasi prod AMS, akun non-prod, tergantung pada apakah nama akun menyertakan nilai 'PROD', 'NONPROD'.
Status Akun	Status akun AMS. Misalnya: AKTIF atau TIDAK AKTIF
Tingkat layanan akun AMS	PREMIUM atau PLUS
ID Instans	ID EC2 contoh
Jenis Platform Instance	Jenis Sistem Operasi (OS). Misalnya: Windows
Negara Instance	Status siklus hidup EC2 instance. Misalnya: TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING Untuk informasi selengkapnya, lihat Siklus hidup instance.
ID Patch	ID patch yang dirilis. Sebagai contoh: KB3172729
Keparahan Patch	Tingkat keparahan patch per penerbit. Misalnya: KRITIS, PENTING, SEDANG, RENDAH, TIDAK DITENTUKAN
Klasifikasi Patch	Klasifikasi patch per penerbit. Misalnya: CRITICALUPDATES, SECURITYUPDATES, UPDATEROLLUPS, UPDATES, FEATUREPACKS

Nama Bidang	Definisi
Tanggal Rilis Patch (UTC)	Tanggal rilis patch per penerbit
Status Instal Patch	Instal status patch pada instance per SSM. Misalnya: TERPASANG, HILANG, TIDAK BERLAKU
Hari Belum Ditambal	Jumlah hari instance belum ditambal sejak pemindaian SSM terakhir
Hari Rentang Belum Ditambal	Bucketing hari belum ditambal. Misalnya: <30 HARI, 30-60 HARI, 60-90 HARI, 90+ HARI

Menambal laporan Cakupan SSM

Laporan AMS Patching SSM Coverage memberi tahu Anda apakah EC2 instans di akun telah menginstal Agen SSM atau tidak.

Nama Bidang	Definisi
Nama Pelanggan	Nama pelanggan untuk situasi di mana ada beberapa sub-pelanggan
Wilayah Sumber Daya	AWS Wilayah tempat sumber daya berada
Nama akun	Nama akun
AWS ID Akun	ID AWS akun
Id Sumber Daya	ID EC2 contoh
Nama Sumber Daya	Nama EC2 contoh
Bendera yang sesuai	Menunjukkan apakah sumber daya telah menginstal Agen SSM ("Compliant") atau tidak ("NON_COMPLIANT")

Laporan Cadangan AMS

Laporan yang tersedia

- [Backup Job Sukses/Laporan Kegagalan](#)
- [Laporan Ringkasan Cadangan](#)
- [Summary/Coverage Laporan Backup](#)

Backup Job Sukses/Laporan Kegagalan

Success/Failure Laporan Backup Job memberikan informasi tentang backup yang dijalankan dalam beberapa minggu terakhir. Untuk menyesuaikan laporan, tentukan jumlah minggu yang Anda inginkan untuk mengambil data. Jumlah default minggu adalah 12. Tabel berikut mencantumkan data yang disertakan dalam laporan:

Nama Bidang	Definisi
ID Akun AWS	ID Akun AWS tempat sumber daya tersebut berada
Nama Akun	Nama akun AWS
ID Pekerjaan Backup	ID pekerjaan Backup
ID Sumber Daya	ID sumber daya yang dicadangkan
Jenis Sumber Daya	Jenis sumber daya yang sedang dicadangkan
Wilayah Sumber Daya	AWS Wilayah sumber daya yang didukung
Status Cadangan	Keadaan cadangan. Untuk informasi selengkapnya, lihat Status pekerjaan Backup
ID Titik Pemulihan	Pengidentifikasi unik dari titik pemulihan
Pesan status	Deskripsi kesalahan atau peringatan yang terjadi selama pekerjaan pencadangan
Ukuran Backup	Ukuran cadangan dalam GB

Nama Bidang	Definisi
Titik Pemulihan ARN	ARN dari cadangan yang dibuat
Usia titik pemulihan dalam beberapa hari	Jumlah hari yang telah berlalu sejak titik pemulihan dibuat
Kurang dari 30 hari	Indikator backup yang berumur kurang dari 30 hari

Laporan Ringkasan Cadangan

Nama Bidang	Definisi
Nama Pelanggan	Nama pelanggan untuk situasi di mana beberapa sub-pelanggan berada
Bulan Backup	Bulan cadangan
Tahun Backup	Tahun cadangan
Jenis Sumber Daya	Jenis sumber daya yang sedang dicadangkan
# Sumber Daya	Jumlah sumber daya yang didukung
# poin Pemulihan	Jumlah snapshot yang berbeda
Backup kurang dari 30 hari	Jumlah backup yang berumur kurang dari 30 hari
Usia titik Pemulihan Maks	Usia titik pemulihan tertua dalam beberapa hari
Usia titik Pemulihan Min	Usia titik pemulihan terbaru dalam beberapa hari

Summary/Coverage Laporan Backup

Summary/Coverage Laporan Backup mencantumkan berapa banyak sumber daya yang saat ini tidak dilindungi oleh AWS Backup paket apa pun. Diskusikan dengan CDSM Anda rencana yang tepat untuk meningkatkan cakupan, jika memungkinkan, dan untuk mengurangi risiko kehilangan data.

Nama Bidang	Definisi
Nama Pelanggan	Nama pelanggan untuk situasi di mana beberapa sub-pelanggan berada
Wilayah	AWS wilayah tempat sumber daya berada
Nama akun	Nama akun
AWS ID Akun	ID AWS akun
Jenis Sumber Daya	Jenis sumber daya. Sumber daya didukung oleh AWS Backup (Aurora, DocumentDB, DynamoDB, EBS,, EFS,,, RDS, dan S3) EC2 FSx
ARN Sumber Daya	ARN sumber daya
ID Sumber Daya	ID sumber daya
Cakupan	Menunjukkan apakah sumber daya tercakup atau tidak (“COVERED” atau “NOT_COVERED”)
# sumber daya	Jumlah sumber daya yang didukung di akun
perc_cakupan	Persentase sumber daya yang didukung dengan cadangan yang dijalankan dalam 30 hari terakhir.

Insiden Mencegah dan Memantau Laporan Pembicara Teratas

Laporan yang tersedia

- [Insiden mencegah laporan](#)
- [Memantau laporan Pembicara Teratas](#)

Insiden mencegah laporan

Laporan Insiden Mencegah mencantumkan CloudWatch alarm Amazon yang secara otomatis diperbaiki, mencegah kemungkinan insiden. Untuk mempelajari lebih lanjut, lihat [Remediasi otomatis](#). Tabel berikut mencantumkan informasi yang disertakan dalam laporan ini:

Nama Bidang	Definisi
eksekusi_start_time_utc	Tanggal di mana otomatisasi dijalankan
nama_pelanggan	Nama pelanggan akun
account_name	Nama akun
AwsAccountId	ID akun AWS
document_name	Nama dokumen SSM atau otomatisasi yang dijalankan
duration_in_minutes	Panjang otomatisasi dalam hitungan menit
Wilayah	AWS Wilayah tempat sumber daya berada
automation_execution_id	ID eksekusi
automation_execution_status	Status eksekusi

Memantau laporan Pembicara Teratas

Laporan Monitoring Top Talkers menyajikan jumlah CloudWatch peringatan Amazon yang dihasilkan selama periode waktu tertentu dan memberikan visualisasi sumber daya yang menghasilkan jumlah peringatan tertinggi. Laporan ini membantu Anda mengidentifikasi sumber daya yang menghasilkan jumlah peringatan tertinggi. Sumber daya ini mungkin kandidat untuk melakukan Analisis Akar Penyebab untuk memperbaiki masalah atau untuk memodifikasi ambang alarm untuk mencegah

pemicu yang tidak perlu ketika tidak ada masalah yang sebenarnya. Tabel berikut mencantumkan informasi yang disertakan dalam laporan ini:

Nama Bidang	Definisi
Nama pelanggan	Nama pelanggan
AccountId	ID AWS akun
Kategori peringatan	Jenis peringatan yang dipicu
Deskripsi	Deskripsi peringatan
ID Sumber Daya	ID sumber daya yang memicu peringatan
Nama Sumber Daya	Nama sumber daya yang memicu peringatan
Wilayah	AWS Wilayah tempat sumber daya berada
Status insiden	Status terbaru dari insiden yang dihasilkan oleh alarm
Kejadian pertama	Pertama kali peringatan itu dipicu
Kejadian baru-baru ini	Waktu terakhir peringatan itu dipicu
Hitungan Peringatan	Jumlah peringatan yang dihasilkan antara kejadian pertama dan terakhir

Laporan Detail Biaya Penagihan

Laporan Detail Biaya Penagihan AWS Managed Services (AMS) memberikan detail tentang biaya penagihan AMS dengan akun tertaut dan layanan AWS masing-masing, termasuk:

- Biaya tingkat layanan AMS, persentase peningkatan, tingkatan layanan AMS tingkat akun, dan biaya AMS.
- Akun tertaut dan biaya AWS penggunaan

Nama Bidang	Definisi
Bulan Penagihan	Bulan dan tahun layanan ditagih
ID Akun Pembayar	ID 12 digit yang mengidentifikasi akun yang akan bertanggung jawab untuk membayar biaya AMS
ID Akun Tertaut	ID 12 digit yang mengidentifikasi akun AMS yang mengkonsumsi layanan yang menghasilkan biaya
AWS Nama Layanan	AWS Layanan yang digunakan
AWS Biaya	AWS Biaya untuk nama AWS layanan yang tercantum dalam Nama AWS Layanan
Rencana Harga	Nama paket harga yang terkait dengan akun yang ditautkan
Proporsi Peningkatan	Persentase peningkatan (sebagai desimal V.WXYZ) berdasarkan pricing_plan, SLA, dan layanan AWS
AWS Biaya yang Disesuaikan	AWS penggunaan disesuaikan untuk AMS
Biaya AWS yang Ditingkatkan	Persentase biaya AWS yang akan dikenakan biaya untuk AMS; $\text{adjusted\_aws\_charges} * \text{uplift\_percent}$
Instans Pengeluaran EC2 RDS	Belanjaan EC2 dan instans RDS
Biaya AMS	Total biaya AMS untuk produk; $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$
Biaya Minimum Prorata	Jumlah yang kami kenakan untuk memenuhi minimum kontrak

Nama Bidang	Definisi
Biaya Minimum	Biaya Minimum AMS (jika berlaku)
Akun Tertaut Total Biaya AMS	Jumlah semua biaya untuk linked_account
Total Biaya AMS Akun Pembayar	Jumlah semua biaya untuk akun pembayar

Laporan Remediator Tepercaya

Laporan yang tersedia

- [Laporan Ringkasan Remediator Remediator Tepercaya](#)
- [Laporan Ringkasan Konfigurasi Remediator Tepercaya](#)
- [Trusted Advisor Periksa laporan Ringkasan](#)

Laporan Ringkasan Remediator Remediator Tepercaya

Laporan Status Remediator Tepercaya memberikan informasi tentang remediasi yang terjadi selama siklus remediasi sebelumnya. Jumlah default minggu adalah 1. Untuk menyesuaikan laporan, tentukan jumlah minggu berdasarkan jadwal remediasi Anda.

Nama Bidang	Definisi
Tanggal	Tanggal pengumpulan data.
account-id	ID AWS akun yang dimiliki sumber daya
Nama Akun	Nama AWS akun
Periksa Kategori	Kategori AWS Trusted Advisor cek
Periksa Nama	Nama cek yang diperbaiki Trusted Advisor
ID pemeriksaan	ID cek yang diperbaiki Trusted Advisor
Mode Eksekusi	Mode eksekusi yang dikonfigurasi untuk Trusted Advisor pemeriksaan tertentu

Nama Bidang	Definisi
OpsItem ID	ID yang OpsItem dibuat oleh Trusted Advisor untuk remediasi
OpsItem Status	Status yang OpsItem dibuat oleh Trusted Advisor pada saat pelaporan
ID Sumber Daya	ARN sumber daya yang dibuat untuk remediasi

Laporan Ringkasan Konfigurasi Remediator Tepercaya

Laporan Ringkasan Konfigurasi Remediator Tepercaya memberikan informasi tentang konfigurasi Remediator Remediator Tepercaya saat ini untuk setiap pemeriksaan. Trusted Advisor

Nama Bidang	Definisi
Tanggal	Tanggal pengumpulan data.
account-id	ID AWS akun tempat konfigurasi berlaku
Nama Akun	Nama AWS akun
Periksa Kategori	Kategori AWS Trusted Advisor cek
Periksa Nama	Nama Trusted Advisor pemeriksaan perbaikan yang berlaku untuk konfigurasi
ID pemeriksaan	ID dari Trusted Advisor pemeriksaan yang diperbaiki bahwa konfigurasi berlaku untuk
Mode Eksekusi	Mode eksekusi yang dikonfigurasi untuk Trusted Advisor pemeriksaan tertentu
Ganti ke Otomatis	Pola tag, jika dikonfigurasi, untuk mengganti mode eksekusi ke Otomatis
Ganti ke Manual	Pola tag, jika dikonfigurasi, untuk mengganti mode eksekusi ke Manual

Trusted Advisor Periksa laporan Ringkasan

Laporan Ringkasan Trusted Advisor Periksa memberikan informasi tentang Trusted Advisor pemeriksaan saat ini. Laporan ini mengumpulkan data setelah setiap jadwal remediasi mingguan. Jumlah default minggu adalah 1. Untuk menyesuaikan laporan, tentukan jumlah minggu berdasarkan siklus remediasi Anda.

Nama Bidang	Definisi
Tanggal	Tanggal pengumpulan data.
account-id	ID AWS akun tempat konfigurasi berlaku
Nama Pelanggan	Nama AWS akun
Periksa Kategori	Kategori AWS Trusted Advisor cek
Periksa Nama	Nama Trusted Advisor pemeriksaan perbaikan yang berlaku untuk konfigurasi
ID pemeriksaan	ID dari Trusted Advisor pemeriksaan yang diperbaiki bahwa konfigurasi berlaku untuk
Status	Status peringatan cek. Status yang mungkin ok (hijau), peringatan (kuning), kesalahan (merah), atau not_available
Sumber Daya Ditandai	Jumlah sumber AWS daya yang ditandai (terdaftar) oleh Trusted Advisor cek.
Sumber Daya Diabaikan	Jumlah sumber AWS daya yang diabaikan oleh Trusted Advisor karena Anda menandainya sebagai ditekan.
Sumber daya dalam keadaan kritis	Jumlah sumber daya dalam keadaan kritis
Sumber daya dalam status peringatan	Jumlah sumber daya dalam keadaan peringatan

Laporan layanan mandiri

AWS Managed Services (AMS) self-service reports (SSR) adalah fitur yang mengumpulkan data dari berbagai AWS layanan asli dan menyediakan akses ke laporan tentang penawaran AMS utama. SSR menyediakan informasi yang dapat Anda gunakan untuk mendukung operasi, manajemen konfigurasi, manajemen aset, manajemen keamanan, dan kepatuhan.

Gunakan SSR untuk mengakses laporan dari konsol AMS dan melaporkan kumpulan data melalui bucket Amazon S3 (satu ember per akun). Anda dapat memasukkan data ke alat intelijen bisnis (BI) favorit Anda untuk menyesuaikan laporan berdasarkan kebutuhan unik Anda. AMS membuat bucket S3 ini (nama bucket S3: (ams-reporting-data-a<Account_ID>)) di AWS Wilayah utama Anda, dan data dibagikan dari bidang kontrol AMS yang dihosting di Wilayah us-east-1.

Important

Untuk mengakses fitur ini, Anda harus memiliki salah satu peran berikut:

- Zona Pendaratan Multi-Akun: `AWSServiceCatalogReadOnlyRole`
- Zona Pendaratan Akun Tunggal: `ReadOnlyPelanggan_ _Peran`

Important

Menggunakan tombol kustom dengan AWS Glue

Untuk mengenkripsi AWS Glue metadata Anda dengan kunci KMS yang dikelola pelanggan, Anda harus melakukan langkah-langkah tambahan berikut untuk memungkinkan AMS mengumpulkan data dari akun:

1. Buka AWS Key Management Service konsol di <https://console.aws.amazon.com/kms>, lalu pilih Customer Managed Keys.
2. Pilih ID kunci yang Anda rencanakan untuk digunakan untuk mengenkripsi AWS Glue metadata.
3. Pilih tab Alias, lalu pilih Buat alias.
4. Di kotak teks, masukkan `AmsReportingFlywheelCustomKey`, lalu pilih Buat alias.

Topik

- [Operasi API internal](#)
- [Laporan patch \(harian\)](#)
- [Laporan Backup \(harian\)](#)
- [Laporan insiden \(mingguan\)](#)
- [Laporan penagihan \(bulanan\)](#)
- [Laporan agregat](#)
- [Dasbor laporan layanan mandiri AMS](#)
- [Kebijakan retensi data](#)
- [Offboard dari SSR](#)

Operasi API internal

Jika Anda memantau operasi API, Anda mungkin melihat panggilan ke operasi khusus internal berikut:

- `GetDashboardUrl`
- `ListReportsV2`

Operasi API internal: `GetDashboardUrl`

Operasi ini muncul di log sistem saat dipanggil oleh konsol AMS. Ini tidak memiliki kasus penggunaan lain. Ini tidak tersedia untuk penggunaan langsung Anda.

Mengembalikan URL dasbor tertanam untuk laporan terkait. Operasi ini menerima `dashboardName` pengembalian oleh `ListReports`.

Permintaan sintaks

```
HTTP/1.1 200
Content-type: application/json
{
  "dashboardName": "string"
}
```

Permintaan elemen

dashboardName: Nama QuickSight dasbor tempat URL diminta. Nama dasbor dikembalikan dalam ListReports V2.

Tipe: String

Sintaks respons

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

Elemen respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200. Layanan mengembalikan data berikut dalam format JSON.

url: Mengembalikan QuickSight URL untuk dimintadashboardName.

Tipe: String

Kesalahan

Untuk informasi tentang kesalahan yang umum terjadi pada semua tindakan, lihat [Kesalahan umum](#).

BadRequestException:

Permintaan yang diajukan tidak valid. Misalnya, jika input tidak lengkap atau salah. Lihat pesan kesalahan yang menyertainya untuk detailnya.

Kode Status HTTP: 400

NotFoundException:

Sumber daya yang diminta tidak ditemukan. Pastikan URI permintaan sudah benar.

Kode Status HTTP: 404

TooManyRequestsException:

Permintaan telah mencapai batas pelambatan. Coba lagi setelah periode waktu yang ditentukan.

Kode Status HTTP: 429

UnauthorizedException:

Permintaan ditolak karena penelepon tidak memiliki izin yang memadai.

Kode Status HTTP: 401

Operasi API internal: ListReports V2

API ini muncul di log sistem saat dipanggil oleh konsol AMS. Ini tidak memiliki kasus penggunaan lain. Ini tidak tersedia untuk penggunaan langsung Anda.

Mengembalikan daftar laporan operasional yang tersedia untuk akun tertentu.

Permintaan sintaks

Permintaan tidak memiliki badan permintaan.

Sintaks respons

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
      "dashboard": "string",
      "lastUpdatedTime": "string",
    }
  ],
  "reportsType": "string"
}
```

Elemen respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200. Layanan mengembalikan data berikut dalam format JSON.

reportsList: Daftar laporan operasional yang tersedia.

Jenis: Array objek Dashboard

reportsType: Menunjukkan apakah laporan dikumpulkan di beberapa akun atau tidak.

Tipe: String

Kesalahan

Untuk informasi tentang kesalahan yang umum terjadi pada semua tindakan, lihat [Kesalahan umum](#).

BadRequestException:

Permintaan yang diajukan tidak valid. Misalnya, input tidak lengkap atau salah. Lihat pesan kesalahan yang menyertainya untuk detailnya.

Kode Status HTTP: 400

NotFoundException:

Sumber daya yang diminta tidak ditemukan. Pastikan URI permintaan sudah benar.

Kode Status HTTP: 404

TooManyRequestsException:

Permintaan telah mencapai batas pelambatan. Coba lagi setelah periode waktu yang ditentukan.

Kode Status HTTP: 429

UnauthorizedException:

Permintaan ditolak karena penelepon tidak memiliki izin yang memadai.

Kode Status HTTP: 401

Laporan patch (harian)

Laporan yang tersedia

-
- [Detail tambalan](#)
- [Contoh yang melewati tambalan](#)

Ini adalah laporan informasi yang membantu mengidentifikasi semua instance yang terhubung ke Patch Orchestrator (PO), status akun, detail instance, cakupan jendela pemeliharaan, waktu eksekusi jendela pemeliharaan, detail tumpukan, dan jenis platform.

Dataset ini menyediakan:

- Data tentang contoh Produksi dan Non-Produksi dari suatu akun. Tahap Produksi dan Non-Produksi berasal dari nama akun dan bukan dari tag instance.
- Data tentang distribusi instance menurut jenis platform. Jenis platform 'N/A' terjadi ketika AWS Systems Manager (SSM) tidak bisa mendapatkan informasi platform.
- Data tentang distribusi status instans, jumlah instans yang berjalan, berhenti, atau penghentian.

Nama Bidang Konsol	Nama Bidang Dataset	Definisi
Pembatasan Akses	access_restrictions	Wilayah yang aksesnya dibatasi
ID akun	aws_account_id	AWS ID akun tempat ID instans berada
Id Akun Admin	aws_admin_account_id	AWS Organizations Akun tepercaya diaktifkan oleh Anda.
Nama Akun	account_name	AWS nama akun
Status Akun	account_status	Status akun AMS
	account_sla	Komitmen layanan akun AMS
Tipe Akun	malz_role	Peran MALZ
Nama Grup Auto Scaling	instance_asg_name	Nama Grup Auto Scaling (ASG) yang berisi instance
Id Instance	instance_id	ID EC2 contoh
Nama Instance	instance_name	Nama EC2 contoh
Grup Patch Instance	instance_patch_group	Nama grup tambalan digunakan untuk mengelompokkan instance bersama dan menerapkan jendela pemeliharaan yang sama

Nama Bidang Konsol	Nama Bidang Dataset	Definisi
Jenis Grup Patch Instance	instance_patch_group_type	Jenis grup tambalan
Jenis Platform Instance	instance_platform_type	Jenis Sistem Operasi (OS)
Nama Platform Instance	instance_platform_name	Nama Sistem Operasi (OS)
Negara Instance	instance_state	Status dalam siklus hidup EC2 instance
Tag Instance	ec2_tag	Tag yang terkait dengan ID EC2 instans Amazon
Zona Pendaratan	malz_bendera	Bendera untuk akun terkait Malz
Cakupan Jendela Pemeliharaan	mw_covered_flag	Jika sebuah instance memiliki setidaknya satu jendela pemeliharaan yang diaktifkan dengan tanggal eksekusi future, maka itu dianggap tertutup, jika tidak tidak tercakup
Tanggal Eksekusi Jendela Pemeliharaan	earliest_window_execution_time	Lain kali jendela pemeliharaan diharapkan untuk dijalankan
Tanggal Eksekusi Jendela Pemeliharaan	earliest_window_execution_time	Lain kali jendela pemeliharaan diharapkan untuk dijalankan
Akun Produksi	prod_account	Pengidentifikasi prod AMS, akun non-prod, tergantung pada apakah nama akun menyertakan nilai 'PROD', 'NONPROD'.
Laporkan Datetime	dataset_datetime	Tanggal dan waktu laporan dibuat.

Nama Bidang Konsol	Nama Bidang Dataset	Definisi
Nama Stack	instance_stack_name	Nama tumpukan yang berisi instance
Jenis Tumpukan	instance_stack_type	Tumpukan AMS (infrastruktur AMS dalam akun pelanggan) atau Tumpukan pelanggan (infrastruktur terkelola AMS yang mendukung aplikasi pelanggan)

Detail tambalan

Laporan ini memberikan detail tambalan dan cakupan jendela pemeliharaan berbagai instance.

Laporan ini menyediakan:

- Data pada grup Patch dan jenisnya.
- Data tentang Pemeliharaan Windows, durasi, cutoff, future dates eksekusi jendela pemeliharaan (jadwal) dan instance yang terpengaruh di setiap jendela.
- Data pada semua sistem operasi di bawah akun dan jumlah contoh bahwa sistem operasi diinstal.

Nama Bidang	Nama Bidang Dataset	Definisi
Laporkan Datetime	dataset_datetime	Tanggal dan waktu laporan dibuat.
ID akun	aws_account_id	AWS ID akun tempat ID instans berada
Nama Akun	account_name	AWS nama akun
Status Akun	account_status	Status akun AMS

Nama Bidang	Nama Bidang Dataset	Definisi
Sesuai - Kritis	compliant_critical	Hitungan tambalan yang sesuai dengan tingkat keparahan “kritis”
Compliant - Tinggi	compliant_high	Hitungan tambalan yang sesuai dengan tingkat keparahan “tinggi”
Sesuai - Sedang	compliant_medium	Hitungan tambalan yang sesuai dengan tingkat keparahan “sedang”
Sesuai - Rendah	compliant_low	Hitungan tambalan yang sesuai dengan tingkat keparahan “rendah”
Compliant - Informasi	compliant_informational	Hitungan tambalan yang sesuai dengan tingkat keparahan “informasional”
Sesuai - Tidak ditentukan	compliant_unspecified	Hitungan tambalan yang sesuai dengan tingkat keparahan “tidak ditentukan”
Sesuai - Total	compliant_total	Hitungan tambalan yang sesuai (semua tingkat keparahan)
Id Instance	instance_id	ID EC2 contoh
Nama Instance	instance_name	Nama EC2 contoh
	account_sla	Tingkat layanan akun AMS
Jenis Platform Instance	instance_platform_type	Jenis Sistem Operasi (OS)
Nama Platform Instance	instance_platform_name	Nama Sistem Operasi (OS)

Nama Bidang	Nama Bidang Dataset	Definisi
Jenis Grup Patch Instance	instance_patch_group_type	DEFAULT: grup patch default dengan jendela pemeliharaan default, ditentukan oleh AMSDefault PatchGroup tag: True pada instance PELANGGAN: grup tambalan yang dibuat pelanggan NOT_ASSIGNED: tidak ada grup tambalan yang ditetapkan
Grup Patch Instance	instance_patch_group	Nama grup tambalan digunakan untuk mengelompokkan instance bersama dan menerapkan jendela pemeliharaan yang sama
Negara Instance	instance_state	Nyatakan dalam siklus hidup EC2 instance
Tag Instance	ec2_tag	Tag yang terkait dengan ID EC2 instans Amazon
Jendela Pemeliharaan Eksekusi Terakhir	last_execution_window	Terakhir kali jendela pemeliharaan dijalankan
Id Jendela Pemeliharaan	window_id	ID jendela pemeliharaan
Status Jendela Pemeliharaan	window_state	Status jendela pemeliharaan
Jenis Jendela Pemeliharaan	jendela_type	Jenis jendela pemeliharaan
Jendela Pemeliharaan Tanggal Eksekusi Berikutnya	window_next eksekusi_waktu	Lain kali jendela pemeliharaan diharapkan untuk dijalankan

Nama Bidang	Nama Bidang Dataset	Definisi
Durasi Jendela Pemeliharaan (jam)	window_duration	Durasi jendela pemeliharaan dalam beberapa jam
Cakupan Jendela Pemeliharaan	mw_covered_flag	Jika sebuah instance memiliki setidaknya satu jendela pemeliharaan yang diaktifkan dengan tanggal eksekusi future, maka itu dianggap tertutup, jika tidak tidak tercakup
Tidak patuh - Kritis	noncompliant_critical	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “kritis”
Tidak patuh - Tinggi	tidak patuh_high	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “tinggi”
Tidak Sesuai - Sedang	noncompliant_medium	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “sedang”
Tidak patuh - Rendah	tidak patuh_low	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “rendah”
Noncompliant - Informasi	tidak patuh_informasional	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “informasional”
Tidak sesuai - Tidak ditentukan	tidak patuh_tidak ditentukan	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “tidak ditentukan”

Nama Bidang	Nama Bidang Dataset	Definisi
Noncompliant - Total	tidak patuh_total	Hitungan tambalan yang tidak sesuai (semua tingkat keparahan)
Id Dasar Patch	patch_baseline_id	Patch baseline saat ini dilampirkan ke instance
Status Patch	patch_status	Status kepatuhan patch secara keseluruhan. Jika setidaknya ada satu tambalan yang hilang, instance dianggap tidak sesuai, jika tidak sesuai.
Akun Produksi	prod_account	Pengidentifikasi prod AMS, akun non-prod, tergantung pada apakah nama akun menyertakan nilai 'PROD', 'NONPROD'.
Jenis Tumpukan	instance_stack_type	Tumpukan AMS (infrastruktur AMS dalam akun pelanggan) atau Tumpukan pelanggan (infrastruktur terkelola AMS yang mendukung aplikasi pelanggan)
	window_next_exec_yyyy	Bagian tahun dari window_next_execution_time
	window_next_exec_mm	Bulan bagian dari window_next_execution_time
	Window_next_exec_d	Bagian hari dari window_next_execution_time

Nama Bidang	Nama Bidang Dataset	Definisi
	window_next _Exec_HHMI	Jam:Menit bagian dari window_next_execution_time

Contoh yang melewati tambalan

Laporan ini memberikan detail tentang instance yang melewati tambalan selama eksekusi jendela pemeliharaan terakhir.

Laporan ini menyediakan:

- Data pada patch yang hilang di tingkat ID patch.
- Data pada semua instance yang memiliki setidaknya satu patch dan atribut yang hilang seperti tingkat keparahan patch, hari yang belum ditambah, rentang, dan tanggal rilis patch.

Nama Bidang	Nama Bidang Dataset	Definisi
Laporkan Datetime	dataset_datetime	Tanggal dan waktu laporan dibuat
ID akun	aws_account_id	AWS ID akun yang dimiliki oleh ID instans
Nama Akun	account_name	AWS nama akun
Nama Pelanggan Orang Tua	customer_name_parent	
Nama Pelanggan	nama_pelanggan	
Akun Produksi	prod_account	Pengidentifikasi akun AMS prod atau non-prod, tergantung pada apakah nama akun menyertakan nilai 'PROD' atau 'NONPROD'.
Status Akun	account_status	Status akun AMS

Nama Bidang	Nama Bidang Dataset	Definisi
Tipe Akun	account_type	
	account_sla	Tingkat layanan akun AMS
Id Instance	instance_id	ID dari EC2 instans Anda
Nama Instance	instance_name	Nama EC2 instans Anda
Jenis Platform Instance	instance_platform_type	Jenis Sistem Operasi (OS)
Negara Instance	instance_state	Nyatakan dalam siklus hidup EC2 instance
Tag Instance	ec2_tag	Tag yang terkait dengan ID EC2 instans Amazon
Id Patch	patch_id	ID patch yang dirilis
Keparahan Patch	patch_sev	Tingkat keparahan patch per penerbit
Klasifikasi Patch	patch_class	Klasifikasi patch per penerbit patch
Tanggal Rilis Patch (UTC)	release_dt_utc	Tanggal rilis patch per penerbit
Status Instal Patch	install_state	Instal status patch pada instance per SSM
Hari Belum Ditambal	days_belum ditambal	Jumlah hari instance belum ditambal sejak pemindaian SSM terakhir
Hari Rentang Belum Ditambal	days_unpatched_bucket	Bucketing hari yang belum ditambal

Laporan Backup (harian)

Laporan cadangan mencakup wilayah primer dan sekunder (bila berlaku). Ini mencakup status cadangan (sukses/kegagalan), dan data pada snapshot yang diambil.

Laporan ini menyediakan:

- Status Backup
- Jumlah snapshot yang diambil
- Titik pemulihan
- Rencana cadangan dan informasi brankas

Nama Bidang	Nama Bidang Dataset	Definisi
Laporkan Datetime	dataset_datetime	Tanggal dan waktu laporan dibuat.
ID akun	aws_account_id	AWS Account ID yang memiliki ID instans
Id Akun Admin	aws_admin_account_id	AWS Organizations Akun tepercaya diaktifkan oleh Anda.
Nama Akun	account_name	Nama akun AWS
Akun SLA	account_sla	Komitmen layanan akun AMS
	malz_bendera	Bendera untuk akun terkait Malz
	malz_role	Peran MALZ
	access_restrictions	Wilayah yang aksesnya dibatasi
Cuplikan cadangan dijadwalkan datetime mulai	start_by_dt_utc	Timestamp saat snapshot dijadwalkan untuk dimulai

Nama Bidang	Nama Bidang Dataset	Definisi
Cadangan snapshot tanggal mulai aktual	kreasi_dt_utc	Stempel waktu saat snapshot benar-benar dimulai
Backup snapshot penyelesaian datetime	completion_dt_utc	Stempel waktu saat snapshot selesai
Datetime kedaluwarsa snapshot cadangan	kedaluwarsa_dt_utc	Stempel waktu saat snapshot kedaluwarsa
Status Backup Job	backup_job_status	Keadaan snapshot
Jenis Backup	backup_type	Jenis cadangan
Id Pekerjaan Backup	backup_job_id	Pengidentifikasi unik dari pekerjaan cadangan
Ukuran Cadangan Dalam Bytes	backup_size_in_bytes	Ukuran cadangan dalam byte
Rencana Cadangan ARN	backup_plan_arn	Rencana cadangan ARN
Id Paket Backup	backup_plan_id	Paket cadangan pengenalan unik
Nama Paket Backup	backup_plan_name	Nama Backup Plan
Versi Rencana Cadangan	backup_plan_version	Versi paket cadangan
Id Aturan Cadangan	backup_rule_id	Id aturan cadangan
Brankas Cadangan ARN	backup_vault_arn	Brankas cadangan ARN
Nama Brankas Cadangan	backup_vault_name	Nama brankas cadangan
Peran IAM ARN	iam_role_arn	ARN IAM role
Id Instance	instance_id	Id contoh unik
Negara Instance	instance_state	Status instans

Nama Bidang	Nama Bidang Dataset	Definisi
Tag Instance	ec2_tag	Tag yang terkait dengan ID EC2 Instance
ARN Sumber Daya	resource_arn	Nama sumber daya Amazon
Id Sumber Daya	resource_id	Pengidentifikasi sumber daya unik
Wilayah Sumber Daya	resource_region	Wilayah primer (dan sekunder, bila berlaku) sumber daya.
Jenis Sumber Daya	resource_type	Jenis sumber daya
Titik Pemulihan ARN	recovery_point_arn	ARN dari titik pemulihan
Id Titik Pemulihan	recovery_point_id	Pengidentifikasi unik dari titik pemulihan
Status Titik Pemulihan	pemulihan_point_status	Status titik pemulihan
Titik Pemulihan Hapus Setelah Hari	recovery_point_delete_after_days	Hapus titik pemulihan setelah sehari-hari
Titik pemulihan pindah ke penyimpanan dingin setelah sehari-hari	recovery_point_move_to_cold_storage_after_days	Jumlah hari setelah tanggal penyelesaian ketika snapshot cadangan dipindahkan ke cold storage
Status Enkripsi Titik Pemulihan	recovery_point_is_encrypted	Status enkripsi titik pemulihan
ARN Kunci Enkripsi Titik Pemulihan	recovery_point_encryption_key_arn	Kunci enkripsi titik pemulihan ARN
Id Tumpukan	stack_id	Pengidentifikasi unik tumpukan cloudformation
Nama Stack	stack_name	Nama Stack

Nama Bidang	Nama Bidang Dataset	Definisi
Tag: Grup Patch Default AMS	tag_ams_default_patch_group	Nilai Tag: Grup Patch Default AMS
Tag: Id Aplikasi	tag_app_id	Nilai Tag: ID Aplikasi
Tag: Nama Aplikasi	tag_app_name	Nilai Tag: Nama Aplikasi
Tag: Backup	tag_backup	Nilai Tag: Cadangan
Tag: Kerangka Kepatuhan	tag_compliance_framework	Nilai Tag: Kerangka Kepatuhan
Tag: Pusat Biaya	tag_cost_center	Nilai Tag: Pusat Biaya
Tag: Pelanggan	tag_pelanggan	Nilai Tag: Pelanggan
Tag: Klasifikasi Data	tag_data_klasifikasi	Nilai Tag: Klasifikasi Data
Tag: Jenis Lingkungan	tag_environment_type	Nilai Tag: Jenis Lingkungan
Tag: Jam Operasi	tag_hours_of_operation	Nilai Tag: Jam Operasi
Tag: Tim Pemilik	tag_owner_team	Nilai Tag: Tim Pemilik
Tag: Email Tim Pemilik	tag_owner_team_email	Nilai Tag: Email Tim Pemilik
Tag: Grup Patch	tag_patch_group	Nilai Tag: Grup Patch
Tag: Prioritas Dukungan	tag_support_priority	Nilai Tag: Prioritas Dukungan
Status Volume	volume_state	Status Volume

Laporan insiden (mingguan)

Laporan ini memberikan daftar agregat insiden beserta prioritas, tingkat keparahan, dan status terbarunya, termasuk:

- Data kasus dukungan dikategorikan sebagai insiden pada akun yang dikelola

- Informasi insiden diperlukan untuk memvisualisasikan metrik insiden untuk akun terkelola
- Data kategori insiden dan status remediasi setiap insiden

Baik visualisasi dan data tersedia untuk laporan insiden Mingguan.

- Visualisasi dapat diakses melalui konsol AMS di akun melalui halaman Laporan.
- Dataset dengan skema berikut, dapat diakses melalui bucket S3 di akun terkelola.
- Gunakan kolom tanggal yang disediakan untuk memfilter insiden berdasarkan bulan, kuartal, minggu, and/or hari kejadian dibuat atau diselesaikan.

Nama Bidang	Nama Bidang Dataset	Definisi
Laporkan Datetime	dataset_datetime	Tanggal dan waktu laporan dibuat.
ID akun	aws_account_id	AWS ID akun tempat insiden tersebut berada.
Id Akun Admin	aws_admin_account_id	AWS Organizations Akun terpercaya diaktifkan oleh Anda.
Nama Akun	account_name	AWS nama akun.
Id Kasus	kasus_id	ID insiden tersebut.
Bulan Dibuat	dibuat_bulan	Bulan ketika insiden itu dibuat.
Prioritas	Prioritas	Prioritas insiden tersebut.
Kepelikan	kepelikan	Tingkat keparahan insiden tersebut.
Status	status	Status insiden tersebut.
Kategori	yuma_kategori	Kategori insiden tersebut.

Nama Bidang	Nama Bidang Dataset	Definisi
Hari yang Dibuat	created_day	Hari ketika insiden itu dibuat dalam YYYY-MM-DD format.
Minggu yang Dibuat	dibuat_wk	Minggu ketika insiden itu dibuat dalam format YYYY-WW. Minggu hingga Sabtu dihitung sebagai awal dan akhir minggu. Minggu adalah dari 01 hingga 52. Minggu 01 selalu merupakan minggu yang berisi hari pertama dalam setahun. Misalnya, 2023-12-31 dan 2024-01-01 berada di minggu 2024-01.
Kuartal yang Dibuat	dibuat_qtr	Kuartal ketika insiden dibuat dalam format YYYY-Q. 01/01 hingga 03/31 didefinisikan sebagai Q1, dan seterusnya.
Hari terselesaikan	terselesaikan_hari	Hari ketika insiden itu diselesaikan dalam YYYY-MM-DD format.

Nama Bidang	Nama Bidang Dataset	Definisi
Minggu terselesaikan	terselesaikan_wk	Minggu ketika insiden itu diselesaikan dalam format YYYY-WW. Minggu hingga Sabtu dihitung sebagai awal dan akhir minggu. Minggu adalah dari 01 hingga 52. Minggu 01 selalu merupakan minggu yang berisi hari pertama dalam setahun. Misalnya, 2023-12-31 dan 2024-01-01 berada di minggu 2024-01.
Bulan terselesaikan	terselesaikan_bulan	Bulan ketika insiden diselesaikan dalam format YYYY-MM.
Kuartal terselesaikan	terselesaikan_qtr	Kuartal ketika insiden diselesaikan dalam format YYYY-Q. 01/01 hingga 03/31 didefinisikan sebagai Q1, dan seterusnya.
Aturan Pengelompokan yang Dibuat	pengelompokan_rule	Aturan pengelompokan yang berlaku untuk insiden tersebut. Baik “no_grouping” atau “instance_grouping”.
Contoh IDs	instance_ids	Contoh yang terkait dengan insiden tersebut.

Nama Bidang	Nama Bidang Dataset	Definisi
Jumlah peringatan	number_of_alerts	Jumlah peringatan yang terkait dengan insiden itu. Jika Anda mengaktifkan pengelompokan, maka angka ini bisa lebih besar dari 1. Jika Anda tidak mengaktifkan pengelompokan, maka itu akan selalu menjadi 1.
Dibuat pada saat	dibuat_at	Stempel waktu saat insiden itu dibuat.
Alarm ARNs	alarm_arns	Nama Sumber Daya Amazon ("arn") dari alarm yang terkait dengan insiden Anda.
Alarm terkait	related_alarm	Nama-nama yang dapat dibaca manusia dari semua alarm yang terkait dengan insiden tersebut.

Laporan penagihan (bulanan)

Detail biaya penagihan

Laporan ini memberikan detail tentang biaya penagihan AMS dengan akun tertaut dan layanan AWS masing-masing.

Laporan ini menyediakan:

- Data tentang biaya tingkat layanan AMS, persentase peningkatan, tingkatan layanan AMS tingkat akun, dan biaya AMS.
- Data tentang akun tertaut dan biaya penggunaan AWS.

⚠ Important

Laporan Penagihan Bulanan hanya tersedia di Akun Pembayar Manajemen (MPA) atau Akun Tagihan yang ditentukan. Ini adalah akun tempat tagihan bulanan AMS Anda dikirim. Jika Anda tidak dapat menemukan akun ini, hubungi Cloud Service Delivery Manager (CSDM) untuk mendapatkan bantuan.

Nama Bidang	Nama Bidang Dataset	Definisi
Tanggal Penagihan	date	Bulan dan tahun layanan ditagih
Id Akun Pembayar	payer_account_id	ID 12 digit yang mengidentifikasi akun yang bertanggung jawab untuk membayar biaya AMS
ID Akun Tertaut	linked_account_id	ID 12 digit yang mengidentifikasi akun AMS yang menggunakan layanan yang menghasilkan ekspansi
AWS Nama Layanan	product_name	AWS Layanan yang digunakan
AWS Biaya	aws_charges	AWS Biaya untuk nama AWS layanan di Nama AWS Layanan
Rencana Harga	pricing_plan	Paket harga yang terkait dengan akun tertaut
Grup Layanan AMS	tier_uplifting_groups	Kode grup layanan AMS yang menentukan persentase peningkatan

Nama Bidang	Nama Bidang Dataset	Definisi
Proporsi Peningkatan	uplift_percent	Persentase peningkatan (sebagai desimal V.WXYZ) berdasarkan pricing_plan, SLA, dan layanan AWS
AWS Biaya yang Disesuaikan	adjusted_aws_usage	AWS penggunaan disesuaikan untuk AMS
Biaya Terangkat AWS	uplifted_aws_charges	Persentase AWS biaya yang akan dikenakan untuk AMS; $\text{adjusted\_aws\_charges} * \text{uplift\_percent}$
Contoh Pengeluaran EC2 RDS	instances_ec2_rds_spend	Belanjaan EC2 dan instans RDS
Biaya Instans Cadangan	ris_charges	Biaya instans cadangan
Biaya Instans Cadangan yang Ditingkatkan	terangkat_ris	Persentase biaya instans cadangan untuk becharged untuk AMS; $\text{ris\_charges} * \text{uplift\_percent}$
Biaya Savings Plan	sp_charge	SavingsPlan biaya penggunaa n
Biaya Savings Plan yang Ditingkatkan	terangkat_sp	Persentase biaya paket tabungan yang akan dikenakan biaya untuk AMS; $\text{sp\_charges} * \text{uplift\_percent}$
Biaya AMS	ams_charges	Total biaya ams untuk produk; $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$

Nama Bidang	Nama Bidang Dataset	Definisi
Biaya Minimum Prorata	prorated_minimum	Jumlah yang kami kenakan untuk memenuhi minimum kontrak
Akun Tertaut Total Biaya AMS	linked_account_total ams_charges	Jumlah semua biaya untuk linked_account
Total Biaya AMS Akun Pembayar	payer_account_total ams_charges	Jumlah semua biaya untuk akun pembayar
Biaya Minimum	minimum_fee	Biaya Minimum AMS (jika berlaku)
Diskon Instans Cadangan dan Savings Plan	adj_ri_sp_charges	RI/SP discount to be applied against RI/SPbiaya (berlaku dalam keadaan tertentu)

Laporan agregat

Pelaporan layanan mandiri agregat (SSR) memberi Anda tampilan laporan layanan mandiri yang ada yang dikumpulkan di tingkat organisasi, lintas akun. Ini memberi Anda visibilitas ke metrik operasional utama, seperti kepatuhan patch, cakupan cadangan, dan insiden, di semua akun di bawah manajemen AMS di dalam Anda. AWS Organizations

SSR agregat tersedia di semua komersial di Wilayah AWS mana AWS Managed Services tersedia. Untuk daftar lengkap Wilayah yang tersedia, lihat [tabel Wilayah](#).

Aktifkan laporan agregat

Anda harus mengelola SSR agregat dari akun AWS Organizations [manajemen](#). Akun manajemen adalah AWS akun yang Anda gunakan untuk membuat organisasi Anda.

Untuk mengaktifkan SSR Agregat untuk akun AWS Organizations manajemen yang terhubung ke AMS, akses konsol AMS Anda dan navigasikan ke Laporan. Pilih Akses Organisasi di top-right-hand

sudut untuk membuka panel [AWS Managed Services Console: Organization View](#). Dari panel ini, Anda dapat mengelola fungsionalitas SSR Agregat.

AWS Organizations Akun manajemen yang tidak terhubung ke AMS tidak memiliki akses ke konsol AMS. Untuk mengaktifkan SSR Agregat untuk akun AWS Organizations manajemen yang tidak terhubung ke AMS, pertama-tama autentikasi ke akun Anda Akun AWS, lalu navigasikan ke [AWS konsol](#) dan cari Managed Services. Ini membuka halaman Pemasaran AMS. Di halaman ini, pilih tautan Akses Organisasi di bilah navigasi untuk membuka AWS Managed Services console: Organization View, tempat Anda dapat mengelola fungsionalitas SSR Agregat.

Saat pertama kali Anda mengakses [AWS Managed Services Console: Tampilan Organisasi](#), selesaikan langkah-langkah berikut:

1. Jika Anda belum menyiapkan AWS Organizations, pilih Aktifkan AWS Organizations dari konsol Anda. Untuk informasi tambahan tentang pengaturan AWS Organizations, lihat [Panduan AWS Organizations Pengguna](#). Anda dapat melewati langkah ini jika Anda sudah menggunakannya AWS Organizations.
2. Untuk mengaktifkan layanan Pelaporan Layanan Mandiri Gabungan. pilih Aktifkan akses tepercaya di konsol.
3. (Opsional) Daftarkan Administrator Delegasi untuk memiliki akses baca untuk tampilan organisasi.

Melihat laporan agregat sebagai administrator yang didelegasikan

Administrator yang didelegasikan adalah akun yang Anda pilih untuk memiliki akses baca ke laporan gabungan. Administrator yang didelegasikan harus merupakan akun yang terhubung ke AMS dan menjadi satu-satunya akun yang memiliki akses baca ke laporan agregat.

Untuk memilih administrator yang didelegasikan, masukkan ID akun di Langkah 3 di AWS Managed Services Console: Tampilan Organisasi. Anda hanya dapat memiliki satu akun administrator yang didelegasikan terdaftar pada satu waktu. Perhatikan bahwa akun administrator yang didelegasikan harus berupa akun yang dikelola AMS.

Untuk memperbarui akun administrator yang didelegasikan, navigasikan ke [AWS Managed Services Console: Tampilan Organisasi](#), lalu pilih Hapus Administrator yang Delegasi. Konsol meminta Anda untuk memasukkan ID akun baru untuk mendaftar sebagai administrator yang didelegasikan.

Baca laporan agregat

Jika Anda tidak mendaftarkan administrator yang didelegasikan, dan akun AWS Organizations manajemen Anda di-onboard ke AMS, maka akun AWS Organizations manajemen akan mendapatkan akses baca ke laporan gabungan secara default. Jika akun AWS Organizations manajemen tidak dikelola oleh AMS, maka Anda harus memilih akun administrator yang didelegasikan untuk memiliki akses baca ke laporan agregat.

Setiap saat, hanya satu akun yang terhubung ke AMS yang memiliki akses baca ke laporan agregat, baik akun AWS Organizations manajemen atau administrator yang didelegasikan terdaftar. Semua akun anggota lain dalam organisasi Anda (dan terhubung ke AMS) masih memiliki akses hanya ke laporan akun tunggal untuk setiap akun individu.

[Setelah Anda mengaktifkan SSR Agregat, navigasikan ke Laporan Anda.](#) Semua laporan layanan mandiri Anda yang ada tercantum di bagian ini, dan tag biru menunjukkan bahwa laporan tersebut telah digabungkan. Perhatikan bahwa Anda harus mengakses konsol AMS dari akun yang Anda pilih untuk memiliki akses baca ke laporan gabungan. Ini adalah akun AWS Organizations manajemen atau akun administrator yang didelegasikan.

Setelah Anda mengaktifkan SSR Agregat, laporan agregat tersedia dari siklus pelaporan berikutnya dan seterusnya.

Nonaktifkan laporan agregat

Untuk menonaktifkan SSR Agregat, buka [AWS Managed Services Console: Organization View](#). Pilih Nonaktifkan akses tepercaya. Setelah Anda menonaktifkan akses tepercaya untuk SSR Agregat, laporan layanan mandiri AMS Anda berhenti digabungkan di tingkat organisasi, di seluruh akun. Perhatikan juga bahwa penonaktifan mulai berlaku dari siklus pelaporan berikutnya dan seterusnya.

Setelah menonaktifkan SSR Agregat, ada penantian sebelum laporan di konsol AMS Anda muncul sebagai laporan akun tunggal. Penundaan ini terjadi karena penonaktifan fitur mulai berlaku dari siklus pelaporan berikutnya dan seterusnya.

Dasbor laporan layanan mandiri AMS

Laporan swalayan AMS menawarkan dua dasbor: [Dasbor Tagger Sumber Daya](#) dan [Dasbor Aturan Konfigurasi Keamanan](#)

Dasbor Tagger Sumber Daya

Dasbor Tagger Sumber Daya AMS menyediakan informasi terperinci tentang sumber daya yang didukung oleh Resource Tagger, serta status tag saat ini yang dikonfigurasi Resource Tagger untuk diterapkan pada sumber daya tersebut.

Cakupan Resource Tagger berdasarkan jenis sumber daya

Dataset ini terdiri dari daftar sumber daya yang memiliki tag yang dikelola oleh Resource Tagger.

Cakupan sumber daya menurut jenis sumber daya divisualisasikan sebagai empat bagan garis yang menggambarkan metrik berikut:

- Jumlah Sumber Daya: Jumlah total sumber daya di Wilayah, menurut jenis sumber daya.
- Tag Terkelola Sumber Daya yang Hilang: Jumlah total sumber daya di Wilayah, menurut jenis sumber daya, yang memerlukan tag terkelola tetapi tidak ditandai oleh Resource Tagger.
- Sumber Daya Tidak Terkelola: Jumlah total sumber daya di Wilayah, menurut jenis sumber daya, yang tidak memiliki tag terkelola yang diterapkan padanya oleh Resource Tagger. Ini biasanya berarti bahwa sumber daya ini tidak cocok dengan konfigurasi Tagger Sumber Daya apa pun, atau secara eksplisit dikecualikan dari konfigurasi.
- Sumber Daya Terkelola: Mitra dengan metrik Sumber Daya Tidak Dikelola (Jumlah Sumber Daya - Sumber Daya Tidak Dikelola).

Tabel berikut mencantumkan data yang disediakan oleh laporan ini.

Nama bidang	Nama bidang dataset	Definisi
Laporkan Datetime	dataset_datetime	Tanggal dan waktu laporan dibuat (waktu UTC)
Akun AWS ID	aws_account_id	Akun AWS ID
Id Akun Admin	aws_admin_account_id	AWS Organizations Akun terpercaya diaktifkan oleh Anda.
Wilayah	region	Wilayah AWS

Nama bidang	Nama bidang dataset	Definisi
Jenis Sumber Daya	resource_type	Bidang ini mengidentifikasi jenis sumber daya. Hanya jenis sumber daya yang didukung oleh Resource Tagger yang disertakan.
Hitungan Sumber Daya	resource_count	Jumlah sumber daya (dari jenis sumber daya yang ditentukan) yang digunakan di Wilayah ini.
ResourcesMissingManagedTags	resource_missing_managed_tags_count	Jumlah sumber daya (dari jenis sumber daya tertentu) yang memerlukan tag terkelola, sesuai dengan profil konfigurasi, tetapi belum diberi tag oleh Resource Tagger.
UnmanagedResources	unmanaged_resource_count	Jumlah sumber daya (dari jenis sumber daya yang ditentukan) tanpa tag terkelola yang diterapkan oleh Resource Tagger. Biasanya, sumber daya ini tidak cocok dengan blok konfigurasi Resource Tagger, atau secara eksplisit dikecualikan dari blok konfigurasi.

Kepatuhan aturan konfigurasi Resource Tagger

Dataset ini terdiri dari daftar sumber daya dalam Wilayah AWS, berdasarkan jenis sumber daya, yang memiliki profil konfigurasi tertentu yang diterapkan padanya. Ini divisualisasikan sebagai grafik garis.

Tabel berikut mencantumkan data yang disediakan oleh laporan ini.

Nama bidang	Nama bidang dataset	Definisi
Laporkan Datetime	dataset_datetime	Tanggal dan waktu laporan dibuat (waktu UTC)
Akun AWS ID	aws_account_id	Akun AWS ID
Id Akun Admin	aws_admin_account_id	AWS Organizations Akun terpercaya diaktifkan oleh Anda.
Wilayah	region	Wilayah AWS
Jenis Sumber Daya	resource_type	Bidang ini mengidentifikasi jenis sumber daya. Hanya jenis sumber daya yang didukung oleh Resource Tagger yang disertakan.
ID Profil Konfigurasi	configuration_profile_id	ID profil konfigurasi Resource Tagger. Profil konfigurasi digunakan untuk menentukan kebijakan dan aturan yang digunakan untuk menandai sumber daya Anda.
MatchingResourceCount	resource_count	Jumlah sumber daya (dari jenis sumber daya tertentu) yang cocok dengan ID profil konfigurasi Resource Tagger. Agar sumber daya cocok dengan profil konfigurasi, profil harus diaktifkan dan sumber daya harus sesuai dengan aturan profil.

Resource Tagger sumber daya yang tidak sesuai

Dataset ini terdiri dari daftar sumber daya yang tidak sesuai untuk konfigurasi Resource Tagger tunggal. Data ini adalah snapshot harian kepatuhan sumber daya, yang menunjukkan status sumber daya pelanggan pada saat laporan ini dikirim ke akun pelanggan (tidak ada tampilan historis). Ini divisualisasikan sebagai tabel pivot yang terdiri dari sumber daya yang bukan keluhan untuk konfigurasi tertentu.

Tabel berikut mencantumkan data yang disediakan oleh laporan ini.

Nama bidang	Nama bidang dataset	Definisi
Laporkan Datetime	dataset_datetime	Tanggal dan waktu laporan dibuat (waktu UTC)
Akun AWS ID	aws_account_id	Akun AWS ID
Id Akun Admin	aws_admin_account_id	AWS Organizations Akun terpercaya diaktifkan oleh Anda.
Wilayah	region	Wilayah AWS
Jenis Sumber Daya	resource_type	Bidang ini mengidentifikasi jenis sumber daya. Hanya jenis sumber daya yang didukung oleh Resource Tagger yang disertakan.
ID Sumber Daya	resource_id	Pengidentifikasi unik untuk sumber daya yang didukung oleh Resource Tagger.
Cakupan Negara	coverage_state	Bidang ini menunjukkan apakah sumber daya ditandai sebagai dikonfigurasi oleh ID konfigurasi Resource Tagger.
ID Profil Konfigurasi	configuration_profile_id	ID profil konfigurasi Resource Tagger. Profil konfigurasi

Nama bidang	Nama bidang dataset	Definisi
		digunakan untuk menentukan kebijakan dan aturan yang digunakan untuk menandai sumber daya Anda.

Dasbor Aturan Konfigurasi Keamanan

Dasbor Aturan Konfigurasi Keamanan memberikan pandangan mendalam tentang kepatuhan sumber daya dan AWS Config aturan akun AMS. Anda dapat memfilter laporan berdasarkan tingkat keparahan aturan untuk memprioritaskan temuan yang paling penting. Tabel berikut mencantumkan data yang disediakan oleh laporan ini.

Nama bidang	Nama bidang dataset	Definisi
Akun AWS ID	Akun AWS ID	ID akun terkait dengan sumber daya terkait.
Id Akun Admin	aws_admin_account_id	AWS Organizations Akun tepercaya diaktifkan oleh Anda.
laporkan datetime	Tanggal Laporan	Tanggal dan waktu laporan dibuat.
nama_pelanggan	Nama Pelanggan	Nama pelanggan.
account_name	Nama Akun	Nama yang terkait dengan ID akun
resource_id	ID Sumber Daya	Pengenal untuk sumber daya.
resource_region	Wilayah Sumber Daya	Di Wilayah AWS mana sumber daya berada.
resource_type	Jenis Sumber Daya	Jenis Layanan AWS atau sumber daya.

Nama bidang	Nama bidang dataset	Definisi
resource_name	Nama Sumber Daya	Nama untuk sumber daya.
resource_ams_flag	Sumber Daya Bendera AMS	Jika sumber daya dimiliki AMS, maka flag ini disetel ke TRUE. Jika sumber daya milik pelanggan, maka tanda ini disetel ke FALSE. Jika kepemilikan tidak diketahui, maka bendera ini disetel ke UNKNOWN.
config_rule	Aturan Config	Nama yang tidak dapat disesuaikan untuk aturan konfigurasi.
config_rule_description	Deskripsi Aturan Config	Deskripsi aturan konfigurasi.
source_identifier	Pengenal Sumber	Pengidentifikasi unik untuk aturan konfigurasi terkelola dan tidak ada pengidentifikasi untuk aturan konfigurasi khusus.
compliance_flag	Bendera Kepatuhan	Menunjukkan apakah sumber daya sesuai atau tidak sesuai dengan aturan konfigurasi.
rule_type	Jenis Aturan	Menunjukkan apakah aturan tersebut telah ditentukan sebelumnya atau dibuat khusus.

Nama bidang	Nama bidang dataset	Definisi
exception_flag	Bendera Pengecualian	Bendera pengecualian sumber daya menunjukkan penerimaan risiko terhadap sumber daya yang tidak sesuai. Jika flag pengecualian sumber daya TRUE untuk sumber daya, maka sumber daya dikecualikan. Jika flag pengecualian adalah NULL, maka sumber daya tidak dikecualikan.
cal_dt	Tanggal	Tanggal evaluasi aturan.
remediation_description	Deskripsi Remediasi	Deskripsi tentang cara memulihkan kepatuhan aturan.
kepelikan	Kepelikan	Tingkat keparahan aturan Config menunjukkan dampak ketidakpatuhan.
customer_action	Tindakan Pelanggan	Tindakan yang dibutuhkan oleh Anda untuk memulihkan aturan tersebut.
usulan	Rekomendasi	Deskripsi tentang apa yang diperiksa aturan konfigurasi.
remediation_category	Kategori Remediasi	Tindakan default yang dilakukan AMS saat aturan ini menjadi tidak patuh.

Kebijakan retensi data

AMS SSR memiliki kebijakan penyimpanan data per laporan setelah periode yang dilaporkan, data dihapus dan tidak lagi tersedia.

Nama laporan	Konsol SSR Retensi Data	Bucket SSR S3 Retensi Data
Ringkasan Detail Instance (Patch Orchestrator)	2 Bulan	2 Tahun
Detail Patch	2 Bulan	2 Tahun
Contoh yang melewati tambalan selama eksekusi jendela pemeliharaan	2 Bulan	2 Tahun
Detail Biaya Penagihan AMS	2 Tahun	2 Tahun
Laporan Backup Harian	1 Bulan	2 Tahun
Laporan Insiden Mingguan	2 Bulan	2 Tahun
Dasbor Aturan Konfigurasi Keamanan	3 Bulan	2 Tahun
Dasbor Tagger Sumber Daya	1 tahun	2 tahun

Offboard dari SSR

Untuk keluar dari layanan SSR, buat permintaan layanan (SR) melalui konsol AMS. Setelah Anda mengirimkan SR, insinyur operasi AMS membantu Anda lepas dari SSR. Di SR, berikan alasan untuk itu Anda ingin offboard.

Untuk melepaskan akun dan melakukan pembersihan sumber daya, buat SR melalui konsol AMS. Setelah Anda mengirimkan SR, insinyur operasi AMS membantu Anda menghapus bucket SSR Amazon S3.

Jika Anda keluar dari AMS, Anda secara otomatis di-offboard dari konsol SSR AMS. AMS secara otomatis berhenti mengirim data ke akun Anda. AMS menghapus bucket SSR S3 Anda sebagai bagian dari proses offboarding.

Laporan insiden, permintaan layanan, dan pertanyaan penagihan di AMS

Topik

- [Manajemen insiden](#)
- [Manajemen permintaan layanan](#)
- [Pertanyaan penagihan](#)

Dengan AWS Managed Services (AMS), Anda dapat meminta bantuan terkait masalah operasional dan permintaan kapan saja melalui konsol AMS. Insinyur operasi AMS tersedia untuk menanggapi insiden dan permintaan layanan Anda 24x7, dengan waktu respons Perjanjian Tingkat Layanan (SLAs) dan Tujuan Tingkat Layanan (SLOs), tergantung pada Tingkat Layanan akun yang Anda pilih (Plus, Premium). Insinyur operasi AMS secara proaktif memberi tahu Anda tentang peringatan dan pertanyaan penting menggunakan mekanisme yang sama.

Manajemen insiden

Topik

- [Apa itu manajemen insiden?](#)
- [Komitmen layanan manajemen insiden](#)
- [Contoh manajemen insiden](#)

Insiden adalah masalah Layanan AWS kinerja yang memengaruhi lingkungan terkelola Anda, sebagaimana ditentukan oleh AWS Managed Services (AMS) atau Anda. Insiden yang diidentifikasi oleh tim AMS pertama kali diterima sebagai “peristiwa”: perubahan status sistem yang ditangkap oleh pemantauan. Jika ambang batas yang dikonfigurasi dilanggar, peristiwa tersebut memicu alarm, juga disebut peringatan. Tim operasi AMS menentukan apakah peristiwa tersebut tidak berdampak, insiden (gangguan layanan atau degradasi), atau masalah (akar penyebab yang mendasari dari satu atau lebih insiden yang diselesaikan).

Tim AMS juga menerima insiden yang diidentifikasi oleh Anda melalui Dukungan pusat atau secara terprogram menggunakan AWS [Support API dengan kode](#) layanan. `sentinel-report-incident`

Setelah insiden Anda diterima oleh tim operasi AMS, insiden tersebut ditinjau untuk memastikan bahwa insiden tersebut tidak diklasifikasikan dengan lebih baik sebagai permintaan layanan. Jika harus diklasifikasikan sebagai permintaan layanan, itu segera direklasifikasi dan tim permintaan layanan AMS mengambil alih dan Anda diberi tahu. Jika insiden dapat diselesaikan oleh operator penerima, langkah-langkah diambil untuk segera menyelesaikan insiden tersebut. Operator AMS berkonsultasi dengan dokumentasi internal untuk resolusi dan, jika diperlukan, meningkatkan insiden ke sumber daya pendukung lainnya sampai insiden diselesaikan. Agar tetap mendapat informasi pada setiap langkah proses penyelesaian insiden, pastikan untuk mengisi opsi Email CC, dan, jika Anda akan terhubung dengan federasi, masuk sebelum mengikuti tautan di email yang dikirimkan AMS. Setelah diselesaikan, tim operasi AMS mendokumentasikan insiden dan resolusi untuk penggunaan di masa mendatang.

Jika resolusi insiden memerlukan perubahan infrastruktur, tinjauan keamanan mungkin diperlukan. Perubahan infrastruktur yang mungkin memerlukan tinjauan keamanan termasuk yang terkait dengan IAM, atau kebijakan berbasis sumber daya, atau persetujuan risiko. Jenis insiden tersebut memerlukan insinyur Operasi AMS untuk membuat RFC sebelum melakukan perubahan, dan persetujuan Anda terhadap RFC tersebut diperlukan. Misalnya, jika resolusi insiden memerlukan pembaruan kebijakan IAM, akan ada tinjauan keamanan AMS dan kemudian insinyur Operasi AMS akan membuat RFC dengan Manajemen | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Perbarui entitas atau jenis perubahan kebijakan (ct-27tuth19k52b4) dan tunggu Anda menyetujui RFC sebelum melanjutkan.

Note

AMS sekarang memungkinkan resolusi insiden yang mengharuskan perubahan infrastruktur dibuat tanpa langkah tambahan persetujuan RFC. Jika perubahan yang diperlukan untuk menyelesaikan insiden TIDAK memerlukan tinjauan keamanan (perubahan tidak terkait dengan IAM, atau kebijakan berbasis sumber daya, atau persetujuan risiko), AMS dapat membuat perubahan berdasarkan persetujuan Anda yang diterima dalam insiden tersebut, tanpa memerlukan persetujuan terpisah dalam RFC.

Untuk definisi istilah manajemen insiden, lihat [Ketentuan Utama AMS](#).

Untuk memahami jalur eskalasi insiden, lihat [Mendapatkan](#) bantuan.

Untuk deskripsi respons AMS terhadap insiden, lihat [respons insiden AMS](#).

Apa itu manajemen insiden?

Manajemen insiden adalah proses yang digunakan AMS untuk merekam, menindaklanjuti, mengkomunikasikan kemajuan, dan memberikan pemberitahuan tentang, insiden aktif.

Tujuan dari proses manajemen insiden adalah untuk memastikan bahwa operasi normal layanan terkelola Anda dipulihkan secepat mungkin, dampak bisnis diminimalkan, dan semua pihak terkait terus mendapat informasi.

Contoh insiden termasuk (tetapi tidak terbatas pada) hilangnya atau degradasi konektivitas jaringan, proses atau API yang tidak responsif, atau tugas terjadwal yang tidak dilakukan (misalnya, cadangan yang gagal).

Grafik berikut menggambarkan alur kerja insiden yang dilaporkan oleh Anda ke AMS.

Grafik ini menggambarkan alur kerja insiden yang dilaporkan oleh AMS kepada Anda.

Prioritas insiden

Insiden yang dibuat di AWS Support center, console atau Support API (SAPI), memiliki klasifikasi yang berbeda dari insiden yang dibuat di konsol AMS.

- Rendah: Fungsi non-kritis dari layanan bisnis Anda, atau aplikasi, yang terkait dengan sumber daya AWS atau AMS terpengaruh.
- Medium: Layanan bisnis atau aplikasi yang terkait dengan sumber daya AWS and/or AMS terkena dampak sedang dan berfungsi dalam keadaan terdegradasi.
- Tinggi: Bisnis Anda terpengaruh secara signifikan. Fungsi penting aplikasi Anda yang terkait dengan sumber daya AWS and/or AMS tidak tersedia. Dicadangkan untuk pemadaman paling kritis yang mempengaruhi sistem produksi.

Note

AWS Support Console menawarkan lima tingkat prioritas insiden yang kami terjemahkan ke tiga level AMS.

Masalah vs insiden

Ketika AMS percaya bahwa sebuah insiden mengungkapkan cacat atau kesalahan konfigurasi yang lebih besar dan dapat berulang, itu dianggap sebagai masalah daripada hanya insiden. Dalam kasus seperti itu, AMS melakukan analisis masalah dan menawarkan saran untuk menyelesaikan masalah.

Komitmen layanan manajemen insiden

Komitmen layanan manajemen insiden

Acara atau tindakan	Pengukuran komitmen layanan
Kasus 1: Sebuah peristiwa dengan dampak yang diketahui dihasilkan. AMS membuka insiden dan memberi tahu Anda. Kasus 2: AMS menghubungi Anda untuk mengonfirmasi dampak acara. Anda mengonfirmasi bahwa peristiwa tersebut adalah insiden. Kasus 3: Anda melihat masalah dan mengirimkan laporan insiden.	Jam untuk respons insiden dan resolusi insiden dimulai ketika: Kasus 1: AMS menciptakan insiden. Kasus 2: Anda mengonfirmasi bahwa peringatan tersebut adalah insiden. Kasus 3: Anda mengirimkan insiden. Komitmen layanan tergantung pada prioritas insiden yang dibuat.
Jika Anda mengirimkan insiden tersebut, AMS mengirimkan tanggapan untuk mengakuinya. Jika AMS membuat insiden atas nama Anda, respons insiden terpisah tidak akan dikirim.	Jam untuk resolusi insiden terus berdetak. Jam untuk waktu respons insiden berhenti ketika AMS mengirimkan pengakuan insiden.  Note Waktu yang dihabiskan menunggu input dari Anda dikecualikan dari perhitungan waktu resolusi insiden. Untuk insiden yang dibuat AMS, waktu respons awal adalah waktu pembuatan pemberitahuan insiden awal kepada Anda.

Acara atau tindakan	Pengukuran komitmen layanan
Untuk sumber daya/layanan yang dimaksud, AMS memeriksa kesehatan untuk memverifikasi apakah: - Kejadian yang terdeteksi AMS atau insiden yang dikirimkan pelanggan memenuhi syarat sebagai insiden, dan - insiden tersebut diprioritaskan dengan benar, dan Jika insiden yang Anda kirimkan tidak diprioritaskan dengan benar, AMS akan memprioritaskannya kembali. Jika AMS mengubah prioritas insiden, pemberitahuan akan dikirimkan kepada Anda bersama dengan alasan di balik perubahan prioritas. Dalam kasus tertentu, masalah yang Anda kirimkan mungkin tidak memenuhi syarat sebagai insiden, tergantung pada penyebabnya. Dalam kasus tersebut, AMS menutup insiden dan mengirim Anda pemberitahuan yang menjelaskan alasannya. Terlepas dari kategorisasi acara, AMS bekerja dengan Anda untuk membantu sesuai kebutuhan. Untuk memahami aturan kategorisasi insiden, lihat. Prioritas insiden	Jika prioritas insiden berubah, komitmen layanan untuk prioritas baru berlaku; jam terus berdetak. Dalam kasus ketika insiden ditutup karena tidak memenuhi definisi insiden, komitmen layanan tidak berlaku; jam berhenti.

Acara atau tindakan	Pengukuran komitmen layanan
AMS bekerja pada insiden tersebut untuk menyelesaikannya dalam komitmen layanan. Dalam kasus tertentu, jika AMS menentukan bahwa tumpukan atau sumber daya yang tidak tersedia tidak dapat diselesaikan tepat waktu, AMS akan menawarkan Pemulihan Infrastruktur sebagai opsi untuk resolusi. Pemulihan Infrastruktur melibatkan penerapan ulang tumpukan yang ada, berdasarkan templat tumpukan yang terkena dampak, dan memulai pemulihan data berdasarkan titik pemulihan terakhir yang diketahui (snapshot EBS/RDS), kecuali ditentukan lain oleh Anda. Data pada EC2 instance individu akan hilang. Jika Anda tidak mengizinkan Pemulihan Infrastruktur seperti yang direkomendasikan oleh AWS, Anda tidak akan memenuhi syarat untuk mendapatkan kredit layanan untuk Komitmen Layanan Waktu Resolusi Insiden terkait.	Jam berhenti ketika: - AMS telah memulihkan semua layanan atau sumber daya yang tidak tersedia yang berkaitan dengan Insiden tersebut ke keadaan yang tersedia, atau - pemulihan infrastruktur dimulai.
Kadang-kadang, AMS memerlukan klarifikasi dari, atau aktivitas oleh, Anda untuk menjaga upaya penyelesaian insiden terus maju, kecuali Anda memiliki tindakan yang telah ditentukan sebelumnya dan disetujui. Akibatnya, ada komunikasi antara AMS dan Anda untuk menyelesaikan insiden	Jam berhenti ketika: AMS sedang menunggu respons atau tindakan dari Anda. Jam dimulai ulang saat: AMS menerima respons dari Anda atau tindakan yang diperlukan AMS dari Anda selesai.

 Note

Untuk daftar lengkap komitmen layanan, unduh [Perjanjian Tingkat Layanan AMS](#).

Contoh manajemen insiden

Contoh manajemen insiden.

Topik

- [Pengujian insiden](#)
- [Melaporkan insiden](#)
- [Memantau dan memperbarui insiden](#)
- [Mengelola insiden dengan AWS Support API](#)
- [Menanggapi insiden yang dihasilkan AMS](#)

Contoh berikut menjelaskan penggunaan konsol AMS untuk mengirimkan insiden. Setelah dikirimkan, tim AMS bekerja dengan Anda untuk menyelesaikan insiden sesuai Perjanjian Tingkat Layanan (SLA) Anda.

Pengujian insiden

Saat menguji kiriman insiden AMS, kami meminta Anda memasukkan dalam teks subjek tanda ini: AMSTestNoOpsActionRequired. Bendera ini memberi tahu AMS bahwa pengiriman insiden hanya untuk pengujian. Ketika insinyur operasi AMS melihat bendera itu, mereka tidak akan menanggapi pengajuan insiden dengan cara apa pun.

Melaporkan insiden

Gunakan konsol AMS untuk melaporkan insiden. Penting untuk membuat insiden baru untuk setiap masalah atau pertanyaan baru. Saat membuka kasus yang terkait dengan pertanyaan lama, akan sangat membantu untuk memasukkan nomor kasus terkait sehingga kami dapat merujuk ke korespondensi sebelumnya.

Note

Jika korespondensi kasus menyimpang dari masalah asli, operator AMS mungkin meminta Anda untuk melaporkan insiden baru.

Untuk melaporkan insiden menggunakan konsol AMS:

1. Dari navigasi kiri, pilih Insiden

Daftar Insiden terbuka:

Jika daftar insiden Anda kosong, opsi Hapus filter akan mengatur ulang filter ke Status apa pun.

Jika Anda tahu ingin menggunakan telepon atau obrolan, klik Buat insiden di Support Center untuk membuka halaman Create insiden di Support Center Console, yang diisi otomatis dengan jenis layanan AMS.

Important

- Panggilan telepon yang dimulai dengan Dukungan direkam, untuk meningkatkan respons dengan lebih baik. Jika panggilan turun, Anda harus menelepon kembali melalui kasus Support Center, tidak AWS memiliki mekanisme untuk menelepon Anda kembali.
- Dukungan telepon dan obrolan dirancang untuk membantu kasus dukungan, insiden, dan permintaan layanan, bukan RFC atau masalah keamanan.
- Untuk masalah RFC, gunakan opsi korespondensi pada halaman detail RFC yang relevan, untuk menghubungi insinyur AMS.
- Untuk masalah keamanan, buat kasus dukungan prioritas tinggi (P1 atau P2). Fitur obrolan langsung bukan untuk acara keamanan.

2. Jika Anda ingin menemukan insiden yang ada, pilih filter status insiden di daftar drop-down.

- Semua insiden yang belum terselesaikan.
- Insiden baru yang belum ditetapkan.
- Insiden yang telah ditetapkan.
- Insiden yang Anda buka kembali.
- Insiden yang ditugaskan dan rumit.
- Insiden yang membutuhkan umpan balik Anda sebelum langkah berikutnya.

- Insiden yang baru-baru ini Anda kirimkan informasi.
- Sebuah insiden yang telah berakhir.
- Semua insiden di akun.

3. Pilih Buat.

Halaman Buat insiden terbuka:

4. Pilih Prioritas:

- Rendah: Fungsi non-kritis dari layanan bisnis Anda atau aplikasi yang terkait dengan sumber AWS daya/AMS terpengaruh.
- Medium: Layanan bisnis atau aplikasi yang terkait dengan sumber AWS daya/AMS cukup terpengaruh dan berfungsi dalam keadaan terdegradasi.
- Tinggi: Bisnis Anda terpengaruh secara signifikan. Fungsi penting aplikasi Anda yang terkait dengan sumber daya AWS/AMS tidak tersedia. Dicadangkan untuk pemadaman paling kritis yang mempengaruhi sistem produksi.

5. Pilih Kategori.

Note

Jika Anda akan menguji fungsionalitas insiden, tambahkan flag no-action (AMSTestNoOpsActionRequired) ke judul insiden Anda.

6. Masukkan informasi untuk:

- Subjek: Judul deskriptif untuk laporan insiden.
- Email CC: Daftar alamat email untuk orang yang ingin Anda informasikan tentang laporan dan resolusi insiden.
- Detail: Deskripsi komprehensif tentang insiden tersebut, sistem yang terkena dampak, dan hasil yang diharapkan dari resolusi tersebut. Jawab pertanyaan yang telah ditetapkan sebelumnya, atau hapus dan masukkan informasi yang relevan.

Untuk menambahkan lampiran, pilih Tambahkan Lampiran, telusuri lampiran yang Anda inginkan, dan klik Buka. Untuk menghapus lampiran, klik ikon Hapus:

7. Pilih Kirim.

Halaman detail terbuka dengan informasi tentang insiden—seperti Jenis, Subjek, Dibuat, ID, dan Status—dan area Korespondensi yang menyertakan deskripsi permintaan yang Anda buat.

Klik Balas untuk membuka area korespondensi dan memberikan rincian tambahan atau pembaruan status.

Klik Tutup Kasus ketika insiden telah diselesaikan.

Klik Muat Lebih banyak jika ada lebih banyak korespondensi daripada yang akan muat pada satu halaman.

Jangan lupa untuk menilai komunikasi!

Insiden Anda ditampilkan di halaman daftar Insiden.

YouTube Video: [Bagaimana cara meningkatkan insiden dari konsol AWS Managed Services?](#)

Memantau dan memperbarui insiden

Anda dapat memperbarui, memantau, dan meninjau laporan insiden dan permintaan layanan, keduanya disebut kasus, dengan menggunakan konsol AMS, atau menggunakan API secara terprogram. Dukungan Untuk informasi tentang penggunaan Dukungan API, lihat [DescribeCases](#) operasi.

Untuk memantau kasus, insiden, atau permintaan layanan, menggunakan konsol AMS, ikuti langkah-langkah berikut.

1. Di konsol AMS Laporan insiden atau dasbor permintaan Layanan, telusuri kasus dan pilih Subjek untuk membuka halaman detail dengan status dan korespondensi saat ini.

Jika kasus insiden atau permintaan layanan yang dilaporkan diperbarui oleh tim operasi AMS, Anda menerima email dan tautan ke insiden tersebut di konsol AMS sehingga Anda dapat merespons. Anda tidak dapat menanggapi korespondensi insiden dengan membalas email.

 Important

Anda harus telah memasukkan alamat email untuk menerima pemberitahuan perubahan status untuk permintaan layanan atau kasus insiden. Pemberitahuan hanya masuk ke alamat email yang ditambahkan ke kasing saat dibuat.

Tautan dalam email notifikasi tidak akan berfungsi kecuali Anda menggunakan server email di jaringan federasi AMS Anda. Namun, Anda dapat menanggapi korespondensi dengan membuka konsol AMS Anda dan menggunakan halaman detail kasus.

2. Jika ada banyak kasus dalam daftar, Anda dapat menggunakan opsi Filter:

- Semua terbuka (default): Gunakan filter ini untuk melihat semua kasus yang belum diselesaikan.
- Tidak ditugaskan: Gunakan jika Anda baru saja mengirimkan kasus dan belum menerima pemberitahuan bahwa status kasus telah berubah. Catatan, insiden dan kasus permintaan layanan ditangani dengan ketepatan waktu yang berbeda tergantung pada prioritas yang diajukan (insiden) atau perjanjian tingkat layanan Anda (permintaan layanan).
- Buka: Gunakan jika Anda telah menerima pemberitahuan bahwa kasusnya adalah tindakan “Amazon Tertunda”; ini berarti bahwa kasus telah ditetapkan tetapi pekerjaan belum dimulai.
- Dibuka kembali: Gunakan jika Anda telah menerima pemberitahuan bahwa kasus dibuka kembali setelah diselesaikan.
- Bekerja dalam proses: Gunakan jika Anda telah menerima pemberitahuan bahwa operator telah mulai mengerjakan kasus ini.
- Tindakan pelanggan yang tertunda: Gunakan jika Anda telah menerima permintaan operator untuk tindakan di pihak Anda.
- Tindakan pelanggan selesai: Gunakan jika Anda telah menerima pemberitahuan bahwa tindakan Anda pada kasus tersebut telah diproses.
- terselesaikan: Gunakan untuk melihat kasus yang Anda tahu telah diselesaikan. Kasus yang diselesaikan dipertahankan dalam sejarah selama dua belas bulan.
- Status apa pun: Gunakan filter ini untuk melihat semua kasus, apa pun statusnya.

3. Untuk memeriksa status terbaru, segarkan halaman.

4. Jika ada begitu banyak korespondensi sehingga tidak semuanya muncul di halaman, pilih Load More.
5. Untuk memberikan pembaruan status kasus, pilih Balas, masukkan korespondensi baru, lalu pilih Kirim.
6. Untuk menutup kasus setelah diselesaikan untuk kepuasan Anda, pilih Tutup kasus.

Pastikan untuk menilai layanan melalui peringkat bintang 1-5 untuk memberi tahu AMS bagaimana keadaan kami!

Mengelola insiden dengan AWS Support API

[AWS Support API](#) memungkinkan Anda membuat insiden dan menambahkan korespondensi ke dalamnya selama penyelidikan masalah dan interaksi Anda dengan staf AWS Support. AWS Support API memodelkan sebagian besar perilaku [AWS Support Center](#). Untuk detail selengkapnya tentang cara menggunakan layanan dukungan AWS ini, lihat [Memprogram Kasus Dukungan AWS](#).

Note

Saat menggunakan AWS Support API, atau SAPI, untuk insiden AMS Advanced, gunakan kode layanan ini: `sentinel-report-incident`.

Menanggapi insiden yang dihasilkan AMS

AMS secara proaktif memantau sumber daya Anda; untuk informasi selengkapnya, lihat [Pemantauan dan manajemen acara](#). Terkadang AMS mengidentifikasi dan membuat kasus insiden, paling sering untuk memberi tahu Anda tentang suatu insiden. Jika tindakan diperlukan dari pihak Anda untuk menyelesaikan suatu insiden, AMS mengirimkan pemberitahuan ke informasi kontak yang telah Anda berikan untuk akun tersebut. Anda menanggapi insiden ini dengan cara yang sama seperti yang Anda lakukan pada insiden lainnya. Anda biasanya akan menanggapi insiden melalui konsol AMS; dalam beberapa kasus, kontak melalui email atau telepon diperlukan.

Note

AMS mengirimkan komunikasi ke alamat email utama Anda di akun AWS Anda; sebaiknya tambahkan alias email kontak Operations alternatif untuk memfasilitasi proses manajemen insiden. Ini tercakup selama proses orientasi AMS dan dokumentasi orientasi terkait.

Jika Anda telah memberikan AMS dengan kontak berbasis non-sumber daya (yang Anda informasikan kepada CSDM Anda) selama orientasi, kontak tersebut akan digunakan. Misalnya, Anda dapat memberikan daftar kontak bernama "SecurityContacts" untuk Anda gunakan CSDMs/CAs untuk insiden atau pemberitahuan terkait keamanan. Tag kontak pada Anda instances/resources digunakan untuk insiden yang dihasilkan AMS, jika Anda telah memberikan persetujuan Anda kepada CSDM untuk menggunakan informasi tag. Untuk mempelajari lebih lanjut tentang layanan notifikasi ini, lihat [Pemberitahuan](#).

Manajemen permintaan layanan

Topik

- [Kapan menggunakan permintaan layanan](#)
- [Cara kerja manajemen permintaan layanan](#)
- [Menguji permintaan layanan di AMS](#)
- [Membuat permintaan layanan di AMS](#)
- [Memantau dan memperbarui permintaan layanan di AMS](#)
- [Menanggapi permintaan layanan yang dihasilkan AMS](#)

Permintaan layanan adalah komunikasi kepada AMS yang dibuat oleh Anda untuk meminta informasi atau saran. Contoh yang baik dari permintaan layanan standar adalah untuk panduan atau bantuan dalam mengonfigurasi layanan AMS, seperti Alarm Manager, Patch Orchestrator, dan sebagainya. Anda juga dapat menerima permintaan layanan dari AMS; ini disebut permintaan layanan keluar atau pemberitahuan layanan. Untuk melihat daftar permintaan layanan Anda, dan permintaan layanan keluar, (pemberitahuan layanan), yang dikirimkan kepada Anda oleh AMS, lihat halaman Permintaan layanan konsol AMS.

Untuk mempelajari lebih lanjut tentang permintaan layanan keluar, lihat [Menanggapi permintaan layanan yang dihasilkan AMS](#).

Anda membuat permintaan layanan AWS Managed Services (AMS) dengan menggunakan konsol AMS atau, secara terprogram, menggunakan API. Dukungan Untuk detail tentang penggunaan API, lihat [Dukungan API](#). Untuk AMS pilih kode sentinel-service-request layanan.

Setelah permintaan layanan Anda diterima oleh tim operasi AMS, itu diprioritaskan sesuai dengan perjanjian tingkat layanan Anda. Untuk terus mendapat informasi pada setiap langkah proses

penyelesaian permintaan layanan, pastikan untuk mengisi opsi Email CC, dan, jika Anda akan terhubung dengan federasi, masuk sebelum mengikuti tautan di email yang dikirim AMS.

Gunakan halaman AMS console Create Service Request untuk melakukan tugas-tugas berikut:

- Membuat dan memperbarui permintaan layanan
- Dapatkan daftar, dan informasi terperinci tentang, semua permintaan layanan Anda saat ini
- Persempit pencarian Anda untuk permintaan layanan berdasarkan tanggal dan pengenalan insiden, termasuk permintaan yang telah diselesaikan
- Tambahkan komunikasi dan lampiran file ke permintaan Anda, dan tambahkan penerima email untuk korespondensi kasus
- Selesaikan permintaan layanan
- Nilai komunikasi permintaan layanan

Kapan menggunakan permintaan layanan

Contoh berikut menjelaskan permintaan layanan:

- AMS atau panduan AWS umum
- Pertanyaan terkait Patch MW
- Pertanyaan terkait jadwal Backup
- Pertanyaan tentang fungsionalitas AWS layanan

Berikut ini adalah contoh dari apa yang tidak boleh diajukan dalam permintaan layanan:

- Masalah akses
- Kegagalan tambalan
- Kegagalan Backup
- Kegagalan RFC atau RFC yang menyebabkan gangguan bisnis (Insiden Penggunaan untuk gangguan bisnis)
- Pertanyaan RFC atau masukan tambahan atau perubahan ruang lingkup RFC (Gunakan korespondensi dua arah RFC)

Cara kerja manajemen permintaan layanan

Permintaan layanan ditangani oleh tim operasi AMS on-call.

Setelah permintaan layanan Anda diterima oleh tim operasi AMS, permintaan tersebut akan ditinjau untuk memastikan bahwa permintaan tersebut tidak diklasifikasikan dengan lebih tepat sebagai insiden. Jika harus diklasifikasikan sebagai insiden, itu segera direklasifikasi, tim manajemen insiden AMS mengambil alih, dan Anda diberi tahu.

Jika permintaan layanan dapat diselesaikan dengan pengajuan RFC, operator peninjau mengirimi Anda email yang meminta Anda mengirimkan RFC yang sesuai (rincian disediakan).

Jika operator AMS dapat menyelesaikan permintaan layanan, langkah-langkah untuk melakukannya segera diambil. Misalnya, jika permintaan layanan adalah untuk saran arsitektur atau informasi lainnya, maka operator merujuk Anda ke sumber daya yang sesuai atau menjawab pertanyaan secara langsung.

Jika analisis permintaan layanan Anda mengidentifikasi bug atau permintaan fitur, AMS mengirimkan pemberitahuan melalui permintaan layanan. Karena tidak ada ETA untuk permintaan fitur atau perbaikan bug, permintaan layanan asli ditutup. Hubungi CSDM Anda untuk menindaklanjuti pertanyaan terkait dengan permintaan layanan asli.

Jika permintaan layanan berada di luar cakupan untuk operasi AMS, operator mengirimkan permintaan ke manajer pengiriman layanan cloud Anda sehingga mereka dapat berkomunikasi dengan Anda, atau ke tim AWS operasi yang sesuai, bersama dengan email kepada Anda, mengenai langkah-langkah apa yang sedang diambil.

Permintaan layanan tidak diselesaikan sampai Anda telah menunjukkan bahwa Anda puas dengan hasilnya.

Note

Kami merekomendasikan untuk memberikan email kontak, nama, dan nomor telepon dalam semua kasus untuk memfasilitasi komunikasi.

Menguji permintaan layanan di AMS

Saat menguji permintaan layanan AMS, kami meminta Anda menyertakan tanda ini dalam teks subjek: `AMSTestNoOpsActionRequired` untuk memberi tahu AMS bahwa permintaan layanan

hanya untuk pengujian. Ketika insinyur operasi AMS melihat bendera itu, mereka tidak menanggapi permintaan layanan.

Membuat permintaan layanan di AMS

Untuk membuat permintaan layanan menggunakan konsol AWS Managed Services (AMS):

1. Dari navigasi kiri, pilih **Permintaan layanan**.

Daftar permintaan Layanan terbuka.

Jika daftar permintaan layanan Anda kosong, opsi **Hapus filter** akan mengatur ulang filter ke Status apa pun.

Jika Anda tahu ingin menggunakan telepon atau obrolan, klik **Buat permintaan layanan** di **Support Center** untuk membuka halaman **Buat permintaan layanan** di **Konsol Pusat Dukungan**, yang diisi otomatis dengan jenis layanan AMS.

Note

Panggilan telepon yang dimulai dengan Dukungan pusat direkam, untuk meningkatkan respons dengan lebih baik. Jika panggilan turun, Anda harus menelepon kembali melalui kasus **Support Center**, tidak AWS memiliki mekanisme untuk menelepon Anda kembali.

Important

Dukungan telepon dan obrolan dirancang untuk membantu kasus dukungan, insiden, dan permintaan layanan. Untuk masalah RFC, gunakan opsi korespondensi pada halaman detail RFC yang relevan, untuk menghubungi insinyur AMS.

2. Jika Anda ingin menemukan permintaan layanan yang ada, pilih filter status permintaan layanan di daftar drop-down.

- Semua permintaan layanan yang belum diselesaikan.

- Permintaan layanan baru yang belum ditetapkan.
- Permintaan layanan yang telah ditetapkan.
- Permintaan layanan yang Anda buka kembali.
- Permintaan layanan yang ditugaskan, rumit,.
- Permintaan layanan yang memerlukan umpan balik Anda sebelum langkah berikutnya.
- Permintaan layanan yang baru-baru ini Anda kirimkan informasinya.
- Permintaan layanan yang telah disimpulkan.
- Semua permintaan layanan di akun.

3. Pilih Buat.

Halaman Create a service request terbuka.

4. Pilih Kategori.

Note

Jika Anda akan menguji fungsionalitas permintaan layanan, tambahkan flag `no-action,AMSTestNoOpsActionRequired`. ke judul permintaan layanan Anda.

5. Masukkan informasi untuk:

- Subjek: Ini membuat tautan ke detail permintaan layanan di halaman daftar.
- Email CC: Email ini menerima korespondensi selain kontak email default Anda.
- Detail: Berikan informasi sebanyak mungkin di sini.

Untuk menambahkan lampiran, pilih Tambahkan Lampiran, telusuri lampiran yang Anda inginkan, dan klik Buka. Untuk menghapus lampiran, klik ikon Hapus:

6. Pilih Kirim.

Halaman detail terbuka dengan informasi tentang permintaan layanan - seperti Jenis, Subjek, Dibuat, ID, dan Status - dan area Korespondensi yang menyertakan deskripsi permintaan yang Anda buat.

Selain itu, permintaan layanan Anda ditampilkan pada halaman daftar Permintaan Layanan. Gunakan ini ketika Anda memiliki peringatan tetapi belum mendengar dari AMS.

Klik Balas untuk membuka area korespondensi dan memberikan detail tambahan atau pembaruan status.

Klik Selesaikan Kasus ketika permintaan layanan telah diselesaikan.

Klik Muat Lainnya untuk melihat korespondensi tambahan yang tidak sesuai di halaman awal.

Jangan lupa untuk menilai komunikasi!

Untuk kueri terkait penagihan, buat kasus permintaan layanan dari Support Center Console.

YouTube Video: [Bagaimana dan kapan harus mengajukan permintaan layanan dari AWS Console dan apa itu Tujuan Tingkat Layanannya?](#)

Memantau dan memperbarui permintaan layanan di AMS

Anda dapat memperbarui, memantau, dan meninjau laporan insiden dan permintaan layanan, keduanya disebut kasus, dengan menggunakan konsol AMS, atau menggunakan API secara terprogram. Dukungan Untuk informasi tentang penggunaan Dukungan API, lihat [DescribeCases](#) operasi.

Untuk memantau kasus, insiden, atau permintaan layanan, menggunakan konsol AMS, ikuti langkah-langkah berikut.

1. Di konsol AMS Laporan insiden atau dasbor permintaan Layanan, telusuri kasus dan pilih Subjek untuk membuka halaman detail dengan status dan korespondensi saat ini.

Jika kasus insiden atau permintaan layanan yang dilaporkan diperbarui oleh tim operasi AMS, Anda menerima email dan tautan ke insiden tersebut di konsol AMS sehingga Anda dapat merespons. Anda tidak dapat menanggapi korespondensi insiden dengan membalas email.

 Important

Anda harus telah memasukkan alamat email untuk menerima pemberitahuan perubahan status untuk permintaan layanan atau kasus insiden. Pemberitahuan hanya masuk ke alamat email yang ditambahkan ke kasing saat dibuat.

Tautan dalam email notifikasi tidak akan berfungsi kecuali Anda menggunakan server email di jaringan federasi AMS Anda. Namun, Anda dapat menanggapi korespondensi dengan membuka konsol AMS Anda dan menggunakan halaman detail kasus.

2. Jika ada banyak kasus dalam daftar, Anda dapat menggunakan opsi Filter:

- Semua terbuka (default): Gunakan filter ini untuk melihat semua kasus yang belum diselesaikan.
- Tidak ditugaskan: Gunakan jika Anda baru saja mengirimkan kasus dan belum menerima pemberitahuan bahwa status kasus telah berubah. Catatan, insiden dan kasus permintaan layanan ditangani dengan ketepatan waktu yang berbeda tergantung pada prioritas yang diajukan (insiden) atau perjanjian tingkat layanan Anda (permintaan layanan).
- Buka: Gunakan jika Anda telah menerima pemberitahuan bahwa kasusnya adalah tindakan “Amazon Tertunda”; ini berarti bahwa kasus telah ditetapkan tetapi pekerjaan belum dimulai.
- Dibuka kembali: Gunakan jika Anda telah menerima pemberitahuan bahwa kasus dibuka kembali setelah diselesaikan.
- Bekerja dalam proses: Gunakan jika Anda telah menerima pemberitahuan bahwa operator telah mulai mengerjakan kasus ini.
- Tindakan pelanggan yang tertunda: Gunakan jika Anda telah menerima permintaan operator untuk tindakan di pihak Anda.
- Tindakan pelanggan selesai: Gunakan jika Anda telah menerima pemberitahuan bahwa tindakan Anda pada kasus tersebut telah diproses.
- terselesaikan: Gunakan untuk melihat kasus yang Anda tahu telah diselesaikan. Kasus yang diselesaikan dipertahankan dalam sejarah selama dua belas bulan.
- Status apa pun: Gunakan filter ini untuk melihat semua kasus, apa pun statusnya.

3. Untuk memeriksa status terbaru, segarkan halaman.

4. Jika ada begitu banyak korespondensi sehingga tidak semuanya muncul di halaman, pilih Load More.
5. Untuk memberikan pembaruan status kasus, pilih Balas, masukkan korespondensi baru, lalu pilih Kirim.
6. Untuk menutup kasus setelah diselesaikan untuk kepuasan Anda, pilih Tutup kasus.

Pastikan untuk menilai layanan melalui peringkat bintang 1-5 untuk memberi tahu AMS bagaimana keadaan kami!

Menanggapi permintaan layanan yang dihasilkan AMS

Manajemen tambalan AMS mengirimkan permintaan layanan (alias pemberitahuan layanan) kepada Anda sebelum waktu jendela pemeliharaan yang ditetapkan; untuk informasi selengkapnya, lihat [jendela pemeliharaan AMS](#). AMS juga mengirimkan pemberitahuan layanan kepada Anda ketika ada kemungkinan infrastruktur Anda akan terpengaruh oleh AWS layanan atau ketika EC2 instance di akun Anda mungkin perlu di-boot ulang; untuk informasi selengkapnya, lihat [Pemberitahuan layanan](#).

Note

AMS mengirimkan komunikasi ke alamat email utama pada AWS akun Anda yang telah Anda berikan; kami sarankan untuk menambahkan alias email kontak Operations alternatif untuk memfasilitasi permintaan layanan atau proses manajemen pemberitahuan layanan. Menambahkan email ini tercakup selama proses orientasi AMS dan dokumentasi orientasi terkait.

Pertanyaan penagihan

Untuk mengajukan pertanyaan terkait tagihan, lengkapi langkah-langkah berikut:

1. Buka [AWS Dukungan Pusat](#) di <https://console.aws.amazon.com/support/> rumah #/.
2. Pilih Akun & penagihan.
3. Pilih Buat kasus.
4. Pilih Akun dan penagihan, lalu ikuti petunjuk untuk mengirimkan kasus Anda.

Operasi Sesuai Permintaan

Operations on Demand (OOD) adalah fitur AWS Managed Services (AMS) yang memperluas cakupan standar rencana operasi AMS Anda dengan menyediakan layanan operasional yang saat ini tidak ditawarkan secara native oleh [rencana operasi AMS](#) atau AWS. Setelah dipilih, penawaran katalog disampaikan dengan kombinasi otomatisasi dan sumber daya AMS yang sangat terampil. Tidak ada komitmen jangka panjang atau kontrak tambahan, memungkinkan Anda untuk memperluas AMS dan AWS operasi dan kemampuan yang ada sesuai kebutuhan. Anda setuju untuk membeli blok jam (blok OOD), 20 jam per blok, setiap bulan.

Anda dapat memilih dari katalog penawaran standar dan memulai keterlibatan OOD baru melalui permintaan layanan. Contoh penawaran OOD termasuk membantu pemeliharaan Amazon EKS, operasi AWS Control Tower, dan pengelolaan cluster SAP. Penawaran katalog baru ditambahkan secara teratur berdasarkan permintaan dan kasus penggunaan operasional yang paling sering kita lihat.

OOD tersedia untuk rencana operasi AMS Advanced dan AMS Accelerate dan tersedia di semua [Wilayah AWS](#) tempat AMS tersedia.

AMS melakukan Customer Security Risk Management (CSRM) saat menerapkan perubahan yang Anda minta. Untuk mempelajari lebih lanjut tentang proses CSRM, lihat [Mengubah ulasan keamanan permintaan](#).

Operations on Demand katalog penawaran

Operations on Demand (OOD) menawarkan layanan yang dijelaskan dalam tabel berikut.

Note

Untuk definisi istilah utama, lihat [Ketentuan Utama](#) dokumentasi AWS Managed Services.

Rencana Operasi	Judul	Deskripsi	Hasil yang Diharapkan
AMS Accelerate	Pemeliharaan kluster Amazon EKS	AMS membebaskan pengembang kontainer Anda dengan menangani pemeliharaan berkelanjutan	Tim pelanggan membantu pekerjaan operasi

		dari penerapan Amazon Elastic Kubernetes Service (Amazon EKS) Anda. AMS melakukan end-to-end prosedur yang diperlukan untuk memperbarui kluster yang menangani komponen bidang kontrol, add-on, dan node. AMS melakukan pembaruan ke tipe node terkelola serta kumpulan add-on Amazon EKS dan Kubernetes yang dikurasi.	yang mendasari memperbarui kluster Amazon EKS.
AMS Accelerate	Gedung dan Penjual AMI	AMS menyediakan manajemen berkelanjutan dari AMI building dan vending untuk pelanggan. Teknisi kami melakukan rilis bulanan langganan AMIs, rilis sesuai permintaan AMIs untuk aktivitas penambalan yang muncul, mengelola perubahan menggunakan runbook, dan memantau build AMI menggunakan Pemantauan. CloudWatch Kami juga menyediakan bantuan pemecahan masalah dan pelaporan terperinci untuk semua yang AMIs digunakan dalam akun yang ditunjuk. Penawaran ini mengharuskan AMI build Pipelines untuk diterapkan melalui pembuat EC2 Gambar. AMS tidak mendukung otomatisasi atau layanan lain yang berinteraksi dengan pembuat EC2 Gambar.	Postur keamanan pelanggan meningkat dan waktu pelanggan yang dihabiskan untuk membangun dan menjual AMIs berkurang.

AMS Accelerate	Eksekusi perubahan yang dikuratori	Bekerja dengan teknisi operasi terampil kami untuk menerjemahkan persyaratan bisnis Anda ke dalam permintaan perubahan yang divalidasi yang dapat dijalankan dengan aman di AWS lingkungan Anda. Manfaatkan pendekatan unik kami untuk otomatisasi dan pengetahuan tentang praktik terbaik operasional (misalnya, penilaian dampak, kemunduran, aturan dua orang), apakah itu perubahan sederhana dalam skala atau tindakan kompleks dengan dampak hilir.	Pelanggan dibantu dengan mendefinisikan, membuat, dan mengeksekusi permintaan perubahan kustom. Perubahan dapat dilakukan secara manual atau otomatis (CloudFormationSSM). Termasuk konsultasi dengan Dukungan panduan konfigurasi bila diperlukan. Tidak dimaksudkan untuk perubahan kode aplikasi, instalasi/penyebaran aplikasi, migrasi data, atau perubahan konfigurasi OS.

AMS Accelerate	AWS Network Firewall Operasi	AMS berkolaborasi dengan Anda untuk melakukan onboard firewall dan menerapkan serta mengelola kebijakan dan aturan untuk operasi firewall yang sedang berlangsung. Teknisi kami melakukan ini dengan memanfaatkan praktik terbaik operasional dan otomatisasi kami untuk mengonfigurasi kebijakan dan aturan standar, dan dengan memungkinkan pemantauan untuk mendeteksi perubahan yang dilakukan di luar proses otomatisasi. AMS dengan cepat memberi tahu Anda tentang perubahan yang tidak diinginkan dan memberikan opsi untuk memasukkannya, jika diminta, atau mengembalikan akun ke konfigurasi sebelumnya untuk memastikan stabilitas keseluruhan sistem Anda.	Tim pelanggan membantu mengurangi overhead manajemen dengan mendeteksi perubahan firewall jaringan yang tidak disengaja dengan cepat, menghasilkan resolusi insiden yang lebih baik dan mengurangi waktu analisis akar penyebab untuk masalah yang diharapkan dan tidak terduga.
AMS Accelerate	AWS Control Tower operasi	Operasi dan pengelolaan AWS Control Tower landing zone Anda yang sedang berlangsung, termasuk AWS Transit Gateway dan AWS Organizations - menyediakan solusi landing zone yang komprehensif. Kami menangani penjual akun, manajemen SCP dan OU, remediasi drift, manajemen pengguna SSO, dan AWS Control Tower peningkatan dengan perpustakaan kontrol kustom dan pagar pembatas kami.	Tim pelanggan membantu dengan beberapa pekerjaan operasi yang mendasari pengelolaan AWS Control Tower, AWS Transit Gateway, dan AWS Organizations.

AMS Accelerate	AWS landing zone Mempercepat operasi	AMS menyediakan operasi berkelanjutan dari zona AWS pendaratan yang dikerahkan melalui AWS Landing Zone Accelerator (LZA). Teknisi kami menangani perubahan file konfigurasi, manajemen lingkungan AWS Control Tower (CT) (penjual akun, pembuatan OU, pagar pembatas CT), manajemen kebijakan kontrol layanan (SCP), deteksi dan remediasi drift CT, manajemen konfigurasi jaringan, dan pembaruan CT dan kerangka kerja LZA. AWS LZA menyediakan sarana untuk mengatur dan mengatur AWS lingkungan multi-akun yang aman menggunakan praktik dan layanan terbaik operasional seperti. AWS Control Tower	Tim pelanggan membantu operasi dan manajemen solusi Akselerator Zona AWS Pendaratan yang sedang berlangsung.

AMS Accelerate	Bantuan Cluster SAP	Khusus mengkhawatirkan, pemantauan, penambalan cluster, cadangan, dan remediasi insiden untuk cluster SAP Anda. Item katalog ini memungkinkan Anda untuk menurunkan beberapa pekerjaan operasional yang sedang berlangsung dari tim operasi SAP Anda sehingga mereka dapat fokus pada manajemen kapasitas dan penyetelan kinerja.	Tim SAP pelanggan atau mitra membantu beberapa pekerjaan operasi yang mendasarinya. Masih mengharuskan pelanggan untuk menyediakan kemampuan SAP lainnya seperti manajemen kapasitas, tuning kinerja, DBA, dan administrasi dasar SAP.

AMS Accelerate	SQL Server pada Operasi EC2	AMS berkolaborasi dengan Anda untuk melakukan onboard, mengimplementasikan, dan mengelola operasi berkelanjutan dari database SQL Server Anda yang diterapkan pada instance. EC2 Teknisi kami memanfaatkan praktik terbaik operasional dan otomatisasi kami untuk membebaskan tim database Anda dengan melakukan tugas-tugas seperti pencadangan dan penambalan, memperluas dukungan operasional AMS ke penambalan SQL Server untuk menyertakan pembaruan bergulir yang sadar cluster, layanan pencadangan dan pemulihan yang selaras dengan strategi pertahanan ransomware kami, dan memantau kepatuhan terhadap kontrol pencadangan dan penambalan yang disediakan pelanggan.	Pelanggan SQL Server membantu pembongkaran patching dan operasi database cadangan untuk meningkatkan ketahanan, dan postur keamanan beban kerja mereka, selain mengoptimalkan biaya lisensi dengan membawa lisensi mereka sendiri (BYOL) ke. EC2

AMS Lanjutan	Pemeliharaan Kluster Amazon EKS	AMS membebaskan pengembang kontainer Anda dengan menangani pemeliharaan dan kesehatan berkelanjutan dari penerapan Amazon Elastic Kubernetes Service (Amazon EKS) Anda. AMS melakukan end-to-end prosedur yang diperlukan untuk memperbarui kluster yang menangani komponen bidang kontrol, add-on, dan node. AMS melakukan pembaruan ke tipe node terkelola serta kumpulan add-on Amazon EKS dan Kubernetes yang dikurasi.	Tim pelanggan membantu pekerjaan operasi yang mendasari memperbarui kluster Amazon EKS.
AMS Lanjutan	Eksekusi RFC Prioritas	Kapasitas insinyur operasi AMS yang ditunjuk untuk memprioritaskan pelaksanaan permintaan perubahan (RFC) Anda. Semua kiriman menerima tingkat respons yang lebih tinggi dan urutan prioritas dapat disesuaikan dengan berinteraksi langsung dengan para insinyur melalui ruang pertemuan Amazon Chime.	Pelanggan menerima respons SLO 8 jam untuk RFCs.

AMS Advanced dan AMS Mempercepat	Peningkatan OS Lama	Hindari migrasi instans dengan memutakhirkan instance ke versi sistem operasi yang didukung. Kami dapat melakukan upgrade di tempat pada instans pilihan Anda memanfaatkan otomatisasi dan kemampuan upgrade vendor perangkat lunak (misalnya, Microsoft Windows 2008 R2 ke Microsoft Windows 2012 R2). Pendekatan ini sangat ideal untuk aplikasi lama yang tidak dapat dengan mudah diinstal ulang pada instance baru dan memberikan perlindungan tambahan dari ancaman keamanan yang diketahui dan tidak tanggung-tanggung pada versi OS yang lebih lama. Sistem operasi berikut didukung untuk peningkatan di tempat: • Microsoft Windows 2012 R2 ke Microsoft Windows 2016 dan di atasnya • Microsoft Windows 2016 ke Microsoft Windows 2022 dan di atasnya • Red Hat Enterprise Linux 7 ke Red Hat Enterprise Linux 8 • Red Hat Enterprise Linux 8 ke Red Hat Enterprise Linux 9 • Oracle Linux 7 ke Oracle Linux 8	Solusi ini disediakan untuk aplikasi yang tidak dapat lagi diinstal ulang pada instance baru (misalnya, kode sumber yang hilang, ISV keluar dari bisnis, dan sebagainya). Anda dapat memutar pemutakhiran yang gagal kembali ke keadaan semula. Dari perspektif operasional, rolling back lebih disukai karena menempatkan instance dalam keadaan yang lebih didukung dengan patch keamanan terbaru.

- [Meminta Operasi AMS Sesuai Permintaan](#)
- [Membuat perubahan pada penawaran Operations on Demand](#)

Meminta Operasi AMS Sesuai Permintaan

AWS Managed Services (AMS) Operations on Demand (OOD) tersedia untuk semua Akun AWS yang telah onboard ke AMS. Untuk memanfaatkan Operations on Demand, mintalah informasi tambahan dari manajer pengiriman layanan cloud (CSDM), Solutions Architect (SA), manajer akun, atau Cloud Architect (CA). Penawaran OOD yang tersedia tercantum dalam [katalog tabel penawaran Operations on Demand](#) sebelumnya. Setelah pelingkupan keterlibatan selesai, kirimkan permintaan layanan ke Operasi AMS untuk memulai keterlibatan untuk OOD.

Setiap permintaan layanan OOD harus berisi informasi rinci berikut yang berkaitan dengan keterlibatan:

- Penawaran OOD spesifik diminta, dan untuk setiap penawaran OOD tertentu:
 - Jumlah blok (satu blok sama dengan 20 jam waktu sumber daya operasional dalam satu bulan kalender tertentu, yang akan dibebankan pada tarif standar saat AWS itu untuk penawaran Operations on Demand yang berlaku) untuk dialokasikan ke penawaran OOD tertentu.
 - ID akun untuk setiap akun AWS Managed Services yang meminta penawaran OOD spesifik.

Permintaan layanan OOD harus dikirimkan oleh Anda melalui:

- Akun AWS Managed Services yang menerima penawaran Operations on Demand yang berlaku, atau
- Akun AWS Managed Services yang merupakan akun AWS Organizations Manajemen dalam semua mode fitur, atas nama akun anggotanya yang merupakan akun AWS Managed Services.

Setelah permintaan layanan OOD diterima, Operasi AMS meninjau dan memperbarui akun dengan persetujuan, persetujuan sebagian, atau penolakan mereka.

Setelah permintaan layanan penawaran OOD disetujui, AMS dan Anda berkoordinasi untuk memulai keterlibatan. Tidak ada penawaran OOD yang dimulai sampai permintaan layanan disetujui dan tanggal mulai keterlibatan disepakati.

AMS menggunakan alokasi langganan bulanan blok OOD. Kami mengalokasikan jumlah blok yang disetujui setiap bulan, mulai dari tanggal mulai keterlibatan, hingga Anda meminta untuk memilih

keluar melalui permintaan layanan baru. Blok OOD berlaku untuk satu bulan kalender. Blok yang tidak digunakan, atau bagian blok, tidak digulung atau dibawa ke bulan-bulan mendatang.

Anda ditagih minimal satu blok OOD setiap bulan, terlepas dari jumlah jam yang sebenarnya digunakan. Setiap blok OOD tambahan, dialokasikan, di mana tidak ada jam yang digunakan, tidak ditagih.

Membuat perubahan pada penawaran Operations on Demand

Untuk meminta perubahan pada keterlibatan yang sedang berlangsung untuk penawaran Operations on Demand (OOD), kirimkan permintaan layanan yang berisi informasi berikut:

- Modifikasi yang diminta, dan
- Tanggal yang diminta untuk modifikasi menjadi efektif.

Setelah menerima permintaan layanan OOD, Operasi AMS meninjau permintaan tersebut dan memperbarui dengan persetujuan mereka atau meminta agar CSDM yang ditetapkan bekerja dengan Anda untuk menentukan ruang lingkup dan implikasi dari modifikasi tersebut. Jika modifikasi ditentukan untuk memerlukan upaya pelingkupan dengan CSDM, Anda diminta untuk mengirimkan permintaan layanan OOD kedua untuk memulai keterlibatan yang dimodifikasi setelah selesainya latihan pelingkupan.

Setelah disetujui, alokasi blok yang paling baru dimodifikasi menjadi dan terus aktif, menggantikan alokasi blok sebelumnya, kecuali disetujui lain oleh dan Anda. AWS

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting dalam setiap rilis AMS Advanced User Guide. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

- Versi API: 2019-05-21
- Baru atau Diperbarui CTs dan Penelusuran: Riwayat Dokumen [Referensi Jenis Perubahan Tingkat Lanjut AMS](#).
- AMS Baru AMIs: [Gambar Mesin AMS Amazon \(AMIs\)](#).

Perubahan	Deskripsi	Tanggal
Tabel yang diperbarui untuk AWS Identity and Access Management (IAM) dalam kontrol Standar di bagian AMS Advanced	Informasi terbaru dalam tabel mengenai kebijakan IAM dan akses ke bucket Amazon S3.	September 25, 2025
Langkah yang diperbarui untuk kueri terkait penagihan	Langkah terbaru untuk membuat permintaan layanan untuk kueri terkait penagihan di bagian Membuat permintaan layanan di AMS.	September 25, 2025
Informasi terbaru untuk pemberitahuan email untuk jenis perubahan	Informasi dan contoh yang diperbarui untuk menambahkan pemberitahuan email untuk jenis perubahan di bagian Konfigurasi pemberitahuan email RFC (konsol).	September 25, 2025
Jenis perubahan yang diperbarui	Bagian penandaan otomatis infrastruktur AMS yang diperbarui dengan jenis perubahan untuk menandai sumber daya buatan AMS.	September 25, 2025

[FAQ VM yang diperbarui
i Import/Export di AWS
Managed Services](#)

Memperbarui RFC yang digunakan untuk meminta profil instance agar alat dapat melakukan perintah dari instance.

September 24, 2025

[Update Request for change
\(RFC\) untuk meluncurkan
SUSE Linux Enterprise Server
untuk SAP Applications 15
instance SP6](#)

Langkah 2 yang diperbarui di bawah cara meluncurkan SUSE Linux Enterprise Server baru untuk aplikasi SAP 15 SP6 instance dengan RFC yang benar.

September 22, 2025

[Permintaan Perubahan yang
Diperbarui \(RFC\)](#)

Diperbarui AWS Elastic Disaster Recovery di bagian FAQ AWS Managed Services dengan RFC yang benar untuk membuat peran IAM yang diperlukan dalam akun Anda.

September 22, 2025

[Menambahkan 4 pemeriksa
an optimasi Trusted Advisor
biaya baru yang didukung oleh
Trusted Remediator](#)

Menambahkan pemeriksaan pengoptimalan biaya berikut:

September 22, 2025

- c1z7kmr00n - Rekomendasi pengoptimalan biaya Amazon untuk instans EC2
- c1z7kmr02n - Rekomendasi optimasi biaya Amazon EBS untuk volume
- c1z7kmr03n - Rekomendasi pengoptimalan biaya Amazon RDS untuk instans DB
- c1z7kmr05n - rekomendasi optimasi biaya untuk fungsi AWS Lambda

<u>Catatan yang diperbarui untuk Availability Zones (AZs)</u>	Informasi terbaru mengenai grup keamanan di AMS.	September 5, 2025
<u>Jenis perubahan yang diperbarui</u>	Memperbarui Amazon FSx di bagian FAQ AWS Managed Services dengan jenis perubahan untuk membagikan iklan Terkelola ke akun aplikasi.	September 5, 2025
<u>Jenis perubahan yang diperbarui</u>	Memperbarui Amazon DocumentDB di bagian FAQ AWS Managed Services dengan jenis perubahan untuk menggunakan penghapusan APIs	September 5, 2025
<u>Jenis perubahan yang diperbarui</u>	Memperbarui bagian FAQ Alexa for Business di AWS Managed Services dengan jenis perubahan menjadi dua pengguna IAM akses terbatas untuk menginstal dan mengoperasikan gateway Alexa for Business Anda.	September 5, 2025
<u>Jenis perubahan yang diperbarui</u>	Diperbarui AppStream 2.0 di bagian FAQ AWS Managed Services dengan jenis perubahan untuk membuat dan memilih peran IAM yang akan tersedia di semua instance streaming armada	September 5, 2025

<u>Jenis perubahan yang diperbarui</u>	Diperbarui EventBridge di bagian FAQ AWS Managed Services dengan jenis perubahan untuk meminta peran EventBridge layanan sebelum digunakan EventBridge untuk memicu AWS sumber daya lain.	September 5, 2025
<u>Dukungan pemeriksaan Trusted Advisor keamanan yang diperbarui oleh Trusted Remediator</u>	Memperbarui parameter dan kendala yang telah dikonfigurasi sebelumnya yang Didukung untuk memeriksa Hs4Ma3G108 - jejak harus diintegrasikan dengan Amazon Logs CloudTrail CloudWatch	September 5, 2025
<u>Dukungan pemeriksaan Trusted Advisor keamanan yang diperbarui oleh Trusted Remediator</u>	Pemeriksaan Trusted Advisor keamanan yang diperbarui untuk menambahkan versi 2 dari Hs4Ma3G184 - Application Load Balancers dan Classic Load Balancers logging harus diaktifkan	September 5, 2025
<u>Pemeriksaan keunggulan Trusted Advisor operasional yang diperbarui didukung oleh bagian Remediator Terpercaya</u>	Pemeriksaan keunggulan Trusted Advisor operasional yang diperbarui didukung oleh bagian Remediator Terpercaya untuk menambahkan centang baru yang didukung c1fd6b9614 Amazon S3 Access Logs Diaktifkan.	Agustus 28, 2025
<u>Jenis perubahan yang diperbarui</u>	Ubah jenis untuk peran IAM kustom.	Agustus 25, 2025

Diperbarui Menggunakan Wawasan CloudWatch Aplikasi untuk server .Net dan SQL di bagian AMS	Jenis perubahan yang direvisi untuk menggunakan CloudWatch Application Insights.	Agustus 25, 2025
Permintaan Perubahan yang Diperbarui (RFC)	Minta perubahan (RFC) untuk menambahkan lebih banyak tag ke bucket Amazon S3.	Agustus 25, 2025
Permintaan Perubahan yang Diperbarui (RFC)	Request for change (RFC) untuk menandai semua sumber daya yang dibuat oleh AMS untuk tujuan manajemen.	Agustus 25, 2025
Lambda yang diperbarui di bagian FAQ AWS Managed Services	Jenis perubahan yang direvisi untuk akses ke AWS layanan lain untuk membuat sumber acara.	Agustus 25, 2025
Lambda yang diperbarui di bagian FAQ AWS Managed Services	Jenis perubahan yang direvisi untuk menyediakan fungsi Lambda.	Agustus 25, 2025
Bagian Buat, Ubah, atau Hapus Grup Keamanan yang Diperbarui	Jenis perubahan yang direvisi untuk membuat grup keamanan di luar tumpukan dan. VPCs	Agustus 25, 2025
Bagian Remediator Terpercaya yang diperbarui untuk menyertakan konten baru untuk Compute Optimizer	Bagian Remediator Terpercaya yang diperbarui untuk menyertakan konten baru untuk AWS Compute Optimizer rekomendasi yang didukung.	Agustus 18, 2025
Tautan Glosarium TOC dihapus	AWS Glosarium.	Agustus 8, 2025

[Rekomendasi jenis perubahan yang tepat](#)

Untuk mengintegrasikan metrik pelanggan Anda ke sistem pemantauan aplikasi Anda, minta AMS membuat topik Amazon SNS untuk metrik dengan mengirimkan RFC dengan Deployment | Monitoring dan notifikasi | SNS | Buat CT (ct-3dfnglm4ombbs).

Agustus 8, 2025

[Rekomendasi jenis perubahan yang tepat](#)

Untuk menghapus volume instance placeholder, kirimkan Manajemen | Komponen tumpukan lanjutan | Volume EBS | Hapus jenis perubahan (ct-3e3h8u0sp5z80).

Agustus 8, 2025

[Peringatan pemantauan baru: SecureChannelFailure dan Saluran Aman Rusak](#)

[Peringatan dari pemantauan dasar di AMS AMS perbaikan otomatis](#) peringatan.

Agustus 8, 2025

[Pemeriksaan Remediator Tepercaya Baru](#)

[Trusted Advisor pemeriksaan pengoptimalan biaya didukung oleh pemeriksaan Trusted Advisor keamanan Remediator Tepercaya yang didukung oleh Trusted Remediator](#)
Hs4Ma3G120— AWSManagedServices-TerminateEC 2, Hs4Ma3G230— 2InstanceStoppedForPeriodOfTime, dan c18d2gz150— 2. AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV AWSManagedServices-TerminateEC InstanceStoppedForPeriodOfTime

Agustus 8, 2025

Memperbarui standar IAM di poin 3.2	Bahasa yang diklarifikasi dan menghapus penyebutan penandaan.	Juli 25, 2025
Pembaruan opsi opt-out peringatan	Penambahan tag memungkinkan Anda untuk memilih keluar dari dua peringatan tambahan.	Juli 25, 2025
penghentian layanan penyediaan layanan mandiri	CloudEndure Layanan penyediaan layanan mandiri tidak digunakan lagi demi. AWS Application Migration Service	Juli 25, 2025
Fitur baru untuk backup	Sesuaikan notifikasi pada brankas cadangan dengan tag baru.	Juli 25, 2025
Tabel kontrol yang diperbarui	Menghapus beberapa kontrol duplikat di bagian tabel AMS-STD-002 - AWS Identity and Access Management (IAM).	Juni 26, 2025
Prasyarat layanan AWS Transfer Family SSP yang diperbarui	Menambahkan informasi ke bagian prasyarat.	Juni 26, 2025
Contoh kebijakan IAM yang diperbarui	Contoh kebijakan IAM yang diperbarui dengan lebih banyak batasan, seperti yang direkomendasikan.	Juni 26, 2025
AMI yang diperbarui didukung OSes	Menambahkan Ubuntu Linux 24.04 di bawah Ubuntu Linux 22.04 dan mengubah semua referensi ke SP5 . SP6	Juni 26, 2025

Layanan penyediaan layanan mandiri, tidak digunakan lagi MediaStore	Menambahkan catatan penghentian untuk AWS Elemental MediaStore	Juni 26, 2025
Layanan penyediaan layanan mandiri, Amazon Inspector Classic tidak digunakan lagi	Menambahkan catatan penghentian untuk Amazon Inspector Classic.	Juni 26, 2025
Layanan penyediaan layanan mandiri, Amazon Connect tidak digunakan lagi	Menambahkan catatan penghentian untuk Amazon Connect.	Juni 26, 2025
Bagian yang diperbarui untuk konfigurasi yang Didukung di AMS	Memperbarui konfigurasi yang didukung untuk sistem operasi yang didukung dan sistem operasi End of Support (EOS) yang Didukung di AMS.	Juni 25, 2025
Layanan penyediaan layanan mandiri, tidak digunakan lagi WorkDocs	Halaman yang dihapus dan referensi ke usang WorkDocs.	Juni 19, 2025
Catatan keamanan penting manajemen patch untuk repositori patch alternatif	Catatan keamanan penting dan praktik terbaik untuk menggunakan repositori patch alternatif di AMS.	10 Juni 2025
Pembaruan sistem operasi yang didukung	Sistem operasi yang didukung AMS Advanced diperbarui, beberapa ditambahkan, beberapa dihapus.	22 Mei 2025
Hanya internal APIs	Hanya internal APIs yang muncul di beberapa CloudWatch log.	22 Mei 2025

Pembaruan Remediator Tepercaya AMS	Cara menggunakan parameter baru,preconfigured-parameters , untuk menyesuaikan Trusted Advisor cek di Trusted Remediator.	22 Mei 2025
Pembaruan Registri Kontainer Elastis SSP Amazon	Lebih banyak peran secara otomatis disediakan saat Anda menggunakan layanan Amazon ECR.	8 Mei 2025
FAQ dan pembaruan Remediator Tepercaya AMS Advanced.	Beberapa pembaruan untuk Trusted Advisor pemeriksaan yang didukung, FAQ Remediator Tepercaya (menambahkan “Sumber daya apa yang diterapkan Remediator Tepercaya ke akun Anda?”) , dan banyak lagi. Lihat juga Trusted Advisor cek yang didukung oleh Trusted Remediator .	8 Mei 2025
Pembaruan kontrol keamanan AMS Advanced Standard.	Menambahkan kontrol “Berbagi grup keamanan”.	8 Mei 2025
Ruang nama AMS yang dilindungi lanjutan.	AMS melindungi ruang nama EPSMarketplaceSubscriptionRole dan EPS ditambahkan.	April 24, 2025
Lokasi log lanjutan AMS.	Lokasi log tambahan ditambahkan.	April 24, 2025

<u>Mode Penyediaan Layanan Mandiri Tingkat Lanjut AMS untuk pembaruan prasyarat AppStream 2.0.</u>	Prasyarat untuk AppStream 2.0 telah ditambahkan: Anda harus menyertakan nama bucket Amazon S3 saat mengirimkan RFC penyediaan untuk layanan.	April 24, 2025
<u>Peringatan remediasi otomatis Amazon RDS AMS Advanced Baru.</u>	ID Peringatan: - 0224, terpicu ketika penyimpanan yang dialokasikan yang diminta mencapai atau melebihi ambang penyimpanan maksimum yang dikonfigurasi.	Maret 27, 2025
<u>AMS Advanced AWS telah menutup akses pelanggan baru ke Amazon CloudSearch, efektif 25 Juli 2024.</u>	Pelanggan yang sudah ada masih dapat menggunakan layanan ini tetapi tidak akan ada fitur baru.	Maret 27, 2025
<u>AMS Advanced AWS telah menutup akses pelanggan baru AWS CodeCommit, efektif 25 Juli 2024.</u>	Pelanggan yang sudah ada masih dapat menggunakan layanan ini tetapi tidak akan ada fitur baru.	Maret 27, 2025
<u>Remediator Tepercaya sekarang tersedia.</u>	Trusted Remediator, solusi AWS Managed Services yang mengotomatiskan remediasi AWS Trusted Advisor pemeriksaan, kini tersedia.	Maret 19, 2025
<u>AMS Advanced Peringatan RDS perbaikan otomatis baru.</u>	RDS-EVENT-0224 ditambahkan.	Maret 17, 2025

[AMS Advanced Fitur baru: Pemberitahuan insiden.](#)

Anda dapat menggunakan AppRegistry untuk membuat aplikasi dan menyesuaikan pemberitahuan insiden untuk aplikasi tersebut.

13 Maret 2025

[Pembaruan AMS ke ambang pemantauan alarm RDS.](#)

Ambang alarm Pemanfaatan CPU Rata-rata RDS telah diubah dari 75% menjadi 90%.

Februari 20, 2025

[Laporan layanan mandiri yang diperbarui dengan opsi data baru untuk tampilan laporan agregat](#)

Opsi data yang ditambahkan untuk menyertakan Nama Bidang baru:Admin Account ID, Nama Bidang Set Data:aws_admin_account_id , dan Definisi: Trusted AWS Organization account enabled by the customer untuk laporan layanan mandiri berikut:

Januari 28, 2025

- Laporan patch (harian)
- Laporan Backup (harian)
- Laporan insiden (mingguan)

[Perbarui ke AWS Batch SSP](#)

Anda dapat menggunakan RFC berikut untuk menyediakan AWS Batch di akun AMS Anda: Manajemen | Layanan AWS | Layanan yang disediakan sendiri | Tambah (ct-1w8z66n899dct).

Januari 28, 2025

Fitur AMS baru: Laporan Layanan Mandiri Agregat	Pelaporan layanan mandiri agregat (SSR) memberi Anda tampilan laporan layanan mandiri yang ada yang dikumpulkan di tingkat organisasi, lintas akun.	Januari 21, 2025
Perbarui ke bagian Forecast SSP	Catatan tambahan: AWS telah menutup akses pelanggan baru ke Amazon Forecast, efektif 29 Juli 2024. Amazon Forecast pelanggan lama dapat terus menggunakan layanan seperti biasa.	Januari 10, 2025
Perbarui ke bagian ruang nama yang dilindungi AMS	Menambahkan namespace dilindungi yang hilang (*mc, *MC, dan *Mc) ke daftar namespace yang dilindungi AMS.	Januari 9, 2025
Perbarui ke bagian Cara kerja pemantauan	Menambahkan informasi tentang fitur baru, mengonfigurasi pemberitahuan peringatan berdasarkan sumber daya, atau ID instans, bukan berdasarkan insiden.	Januari 8, 2025
Diperbarui: konten pembaruan berbasis tag	Memperbaiki kesalahan ketik di keyname dan memperbaiki jalur file konfigurasi yang buruk.	Januari 6, 2025
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	November 21, 2024

Tabel penawaran Operasi On Demand yang Diperbarui

Sistem operasi berikut didukung untuk peningkatan di tempat:

November 11, 2024

- Microsoft Windows 2016 ke Microsoft Windows 2022 dan di atasnya

Tabel penawaran Operasi On Demand yang Diperbarui

Sistem operasi berikut didukung untuk peningkatan di tempat:

November 1, 2024

- Microsoft Windows 2012 R2 ke Microsoft Windows 2016 dan di atasnya
- Red Hat Enterprise Linux 7 ke Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 8 ke Red Hat Enterprise Linux 9
- Oracle Linux 7 ke Oracle Linux 8

Diperbarui konfigurasi yang didukung

Diperbarui didukung sistem operasi Oracle Linux untuk 9.0-9.3, 8.0-8.9, 7.5-7.9.

Oktober 24, 2024

[Gambar Mesin Amazon AMS yang Diperbarui \(AMIs\)](#)

Diperbarui berbasis Windows AMIs untuk menghapus Windows 2012 dan 2012 R2. Diperbarui berbasis Linux AMIs untuk menghapus beberapa AMIS yang tidak lagi mendukung dan menambahkan yang berikut:

Oktober 24, 2024

- Amazon Linux 2 (ARM64)
- RHEL 9
- SUSE Linux Server Perusahaan 15 SP5

[Anda sekarang dapat menyertakan beberapa alamat email dalam peringatan berbasis tag.](#)

Beberapa alamat email sekarang didukung dalam peringatan berbasis tag.

September 20, 2024

[Ubah bagian ulasan keamanan permintaan ditambahkan.](#)

Bagian baru telah ditambahkan yang memberikan rincian tentang proses peninjauan keamanan permintaan perubahan.

September 17, 2024

[Bagian baru ditambahkan.](#)

Bagian baru yang menjelaskan bagaimana tinjauan keamanan permintaan perubahan terjadi di AMS Advanced sekarang tersedia.

September 12, 2024

[Layanan baru yang didukung oleh AMS Advanced.](#)

AWS Resilience Hub sekarang didukung oleh AMS Advanced.

Agustus 30, 2024

[Layanan baru yang didukung oleh AMS Advanced.](#)

Lima layanan baru sekarang didukung oleh AMS Advanced:

Agustus 21, 2024

- Amazon Bedrock
- Amazon Kendra
- Amazon Quantum Ledger Database (Amazon QLDB)
- AWS Service Catalog AppRegistry
- Layanan Terkelola Amazon untuk Prometheus

[Pengaturan default jaringan keamanan endpoint baru sekarang tersedia.](#)

Sumber pembaruan sekarang termasuk dalam pengaturan jaringan default EPS.

Agustus 21, 2024

[Diperbarui: Catatan AMS AMI](#)

File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.

Juli 30, 2024

[AMS sekarang mendukung Amazon Route 53 Resolver DNS Firewall.](#)

AMS sekarang mendukung Amazon Route 53 Resolver DNS Firewall

Juli 30, 2024

[AWS DataSync Pembaruan SSPS](#)

AWS DataSync tidak lagi memerlukan awalan “datasync-” pada nama bucket Amazon S3.

Juli 30, 2024

[Dasbor Aturan Konfigurasi Keamanan](#)

Dasbor Aturan Konfigurasi Keamanan sekarang tersedia dalam pelaporan Layanan Mandiri.

Juli 24, 2024

AMS sekarang mendukung Oracle Linux 8.9, RHEL 8.10, dan RHEL 9.4.	AMS sekarang mendukung Oracle Linux 8.9, RHEL 8.10, dan RHEL 9.4.	Juli 5, 2024
Amazon Bedrock sekarang tersedia dalam mode penyediaan layanan mandiri	Anda sekarang dapat meminta Amazon Bedrock dalam mode AMS SSP.	27 Juni 2024
Amazon Route 53 Resolver Peristiwa firewall DNS dalam Respons Insiden Keamanan	AMS sekarang memantau peristiwa firewall DNS Amazon Route 53 Resolver di Respons Insiden Keamanan	Juni 21, 2024
Menambahkan informasi tambahan tentang cara mengaktifkan AMS membawa fitur EPS (BYOEPS) Anda sendiri.	Menambahkan informasi tambahan tentang cara mengaktifkan AMS membawa fitur EPS (BYOEPS) Anda sendiri.	Juni 5, 2024
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	23 Mei 2024
Informasi ditambahkan tentang penggunaan peran khusus dengan AWS Amplify dalam mode penyediaan layanan mandiri (hanya lingkungan MALZ).	Petunjuk ditambahkan tentang bagaimana lingkungan MALZ dapat menggunakan peran khusus AWS Amplify dalam mode penyediaan layanan mandiri.	23 Mei 2024
Amazon Kendra sekarang tersedia dalam mode Penyediaan Layanan Mandiri.	Amazon Kendra sekarang tersedia dalam mode Penyediaan Layanan Mandiri.	23 Mei 2024

AMS Advanced mendukung sistem operasi tambahan.	AMS Advanced mendukung Red Hat Enterprise Linux (RHEL) 9.x dan Ubuntu 20.04 dan 22.04.	April 25, 2024
AMS Advanced mendukung ARM64 arsitektur untuk Amazon Linux 2.	AMS Advanced mendukung ARM64 arsitektur untuk Amazon Linux 2.	April 25, 2024
Diperbarui Offboard dari bagian akun landing zone multi-akun landing zone (MALZ).	Menambahkan informasi terperinci tentang cara melepaskan akun Aplikasi dan Inti dari landing zone multi-akun.	April 11, 2024
Diperbarui: Deskripsi manajemen permintaan layanan.	Deskripsi manajemen permintaan Layanan yang diperbarui dalam topik deskripsi Layanan.	Maret 21, 2024
Diperbarui: Bagian komitmen layanan manajemen insiden.	Menambahkan tautan ke Perjanjian Tingkat Layanan AMS.	Maret 21, 2024
Diperbarui: Bagaimana bagian kerja manajemen permintaan layanan.	Menambahkan klarifikasi tentang cara AMS menangani permintaan layanan yang berisi permintaan fitur atau bug.	Maret 21, 2024
Diperbarui: Dapatkan bagian dukungan.	Diperbarui Dapatkan bagian dukungan untuk menyertakan bagian pertanyaan Penagihan baru.	Maret 21, 2024

Diperbarui: Penyediaan IAM Otomatis AMS	Penyediaan IAM Otomatis AMS yang diperbarui dengan informasi daftar penolakan kustom	Maret 21, 2024

Pembaruan lebih awal

Tabel berikut menjelaskan perubahan penting pada dokumentasi panduan AMS Advanced sebelum Maret 2024.

Ubah	Deskripsi	Tautan
Februari 2024		
Sistem Operasi yang Didukung Diperbarui	Memperbarui Sistem Operasi yang Didukung untuk menyertakan SUSE Linux Enterprise Server 15 SP5.	Lihat Konfigurasi yang didukung
Menambahkan catatan ke Peringatan dari pemantauan dasar di AMS.	Catatan tambahan yang menunjukkan bahwa alarm untuk Penggunaan Volume EC2 non-Root dinonaktifkan secara default.	Lihat Peringatan dari pemantauan dasar di AMS
Menambahkan bagian baru AMS Event Router ke Monitoring dan manajemen acara.	Menambahkan bagian baru yang membahas AMS Advanced Event Router.	Lihat Menggunakan Aturan EventBridge Terkelola Amazon di AMS
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	Lihat AMIs. csv-and-notes.02.2024
Februari 2024		

Ubah	Deskripsi	Tautan
Menambahkan bagian baru untuk peran terkait layanan EventBridge aturan Amazon untuk AMS Advanced	Menambahkan bagian baru untuk peran terkait layanan EventBridge aturan Amazon untuk AMS Advanced di bagian Keamanan Infrastruktural.	Lihat Peran terkait layanan EventBridge aturan Amazon untuk AMS Advanced
Bagian Mode Penyediaan Layanan Mandiri yang Diperbarui	Menambahkan bagian baru untuk Amazon Inspector baru dalam Mode Penyediaan Layanan Mandiri.	Lihat Amazon Inspector Classic (AMS SSPS)
Januari 2024		
Bagian manajemen acara Terencana (PEM) yang diperbarui	Menambahkan detail tambahan dan FAW ke manajemen acara yang direncanakan (PEM).	Lihat Manajemen acara yang direncanakan di AWS Managed Services
Menambahkan bagian baru untuk instalasi auto SSM Agent	Menambahkan bagian baru untuk instalasi otomatis Agen SSM dalam konfigurasi EC2 instans Otomatis.	Lihat Instalasi otomatis Agen SSM
Ditambahkan AWS Resilience Hub (AMS SSPS)	Menambahkan layanan SSPS baru.	Lihat Gunakan SSP AMS untuk menyediakan AWS Resilience Hub di akun AMS Anda
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	Lihat AMIs. csv-and-notes.01.2024
Desember 2023		

Ubah	Deskripsi	Tautan
Mode Perubahan Langsung yang Diperbarui di AMS	Menambahkan subbagian baru, kasus penggunaan Mode Perubahan Langsung, ke mode Perubahan Langsung di AMS.	Lihat Mode Perubahan Langsung di AMS
Diperbarui AWS Amplify (AMS SSPS)	FAQ yang diperbarui untuk mengklarifikasi bahwa Penerimaan Risiko diperlukan untuk meminta Amplify.	Lihat Gunakan SSP AMS untuk menyediakan AWS Amplify di akun AMS Anda
Baru AWS Elastic Disaster Recovery (AMS SSPS)	Menambahkan layanan SSPS baru	Lihat Gunakan SSP AMS untuk menyediakan AWS Elastic Disaster Recovery di akun AMS Anda
Layanan Dikelola Amazon Baru untuk Prometheus (AMS SSPS)	Menambahkan layanan SSPS baru	Lihat Gunakan SSP AMS untuk menyediakan Layanan Terkelola Amazon untuk Prometheus di akun AMS Anda
Diperbarui Bagian Bagaimana manajemen kontinuitas bekerja.	Menambahkan subbagian baru, pemantauan dan pelaporan cadangan AMS.	Lihat Bagaimana manajemen kontinuitas bekerja
DevOpsGuru Amazon Baru (AMS SSPS)	Menambahkan layanan SSPS baru	Lihat Gunakan AMS SSP untuk menyediakan Amazon DocumentDB (dengan kompatibilitas MongoDB) di akun AMS Anda
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	Lihat AMIs. csv-and-notes.12.2023

Ubah	Deskripsi	Tautan
November, 2023		
Diperbarui Amazon CloudWatch Synthetics (AMS SSPS)	Diperbarui FAQs untuk menggunakan nama peran yang benar.	Lihat Menggunakan AMS SSP untuk menyediakan Amazon CloudWatch Synthetics di akun AMS Anda
Mode Penyediaan Layanan Mandiri Amazon API Gateway yang diperbarui	Menambahkan peran tambahan, <code>customer_apigateway_cloudwatch_role</code> , ke bagian API Gateway.	Lihat Gunakan AMS SSP untuk menyediakan Amazon API Gateway di akun AMS Anda
Menambahkan layanan baru ke mode Penyediaan Layanan Mandiri	Ditambahkan AWS Service Catalog AppRegistry ke bagian mode Penyediaan Layanan Mandiri	Lihat Gunakan SSP AMS untuk menyediakan AWS Service Catalog AppRegistry di akun AMS Anda
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	Lihat AMIs. csv-and-notes.11.2023
September, 2023		
Menambahkan catatan untuk Menggunakan Patch Orchestrator	Menambahkan catatan berikut ke bagian Menggunakan Patch Orchestrator: “Peringatan kegagalan patch tidak dibuat untuk instance yang memiliki sistem operasi yang tidak didukung, atau yang dihentikan selama jendela pemeliharaan”	Lihat Manajemen patch di AMS

Ubah	Deskripsi	Tautan
Enkripsi data yang diperbarui dengan layanan tambahan	Menambahkan layanan ke enkripsi Data di AMS.	Lihat Perlindungan data di AMS
Menambahkan paragraf baru ke pesan kesalahan RFC.	Menambahkan paragraf baru untuk menambahkan Buat tautan permintaan layanan.	Lihat Memecahkan masalah kesalahan RFC di AMS
Nama peran IAM yang dikoreksi.	Mengoreksi rolename IAM customer_emr_cluster_autosc aling_role.	Lihat Mode Penyediaan Layanan Mandiri di AMS
Informasi pemantauan dasar yang diperbarui	Referensi dihapus ke dua alarm usang dan. RDSRead LatencyAlarm RDSWrite LatencyAlarm	Lihat Peringatan dari pemantauan dasar di AMS
Agustus, 2023		
Ditambahkan: Respon Insiden Keamanan AMS	Menambahkan dokumenta si untuk menggunakan AMS Security Incident Response.	Lihat Respon Insiden Keamanan di AMS
Juli, 2023		
Ditambahkan: Penyediaan IAM Otomatis	Menambahkan dokumenta si untuk menggunakan Penyediaan IAM Otomatis.	Lihat AMS Penyediaan IAM Otomatis
Diperbarui: Akses tabel peran	Menambahkan peran yang hilang untuk AMS Access.	Lihat Akun pelanggan AMS mengakses peran IAM
Juni, 2023		

Ubah	Deskripsi	Tautan
Diperbarui: Daftar peringatan RDS yang dipantau.	Memperbarui daftar peringatan RDS untuk pemantauan dasar AMS. 9 jenis peringatan RDS baru ditambahkan dan 3 jenis peringatan RDS yang ada telah dihapus.	Lihat Peringatan dari pemantauan dasar di AMS .
Diperbarui: Akses tabel peran	Peran baru untuk AMS Security.	Lihat Akun pelanggan AMS mengakses peran IAM
Mei, 2023		
Diperbarui: Kebijakan Tanggal Mulai Penagihan Layanan.	Definisi Tanggal Mulai Penagihan yang diperbarui.	Lihat Istilah kunci AMS .
April, 2023		
Diperbarui: Laporan Layanan Mandiri Penagihan Bulanan.	Catatan tambahan: Laporan Penagihan Bulanan hanya tersedia di akun Managemen t Payer (AMS Advanced multi-account landing zone), tetapi tersedia untuk semua akun terkelola AMS Accelerate yang ditautkan.	Lihat Laporan penagihan (bulanan) .
Diperbarui: Dihapus “Standard Patching” konten	AMS menggunakan Patch Orchestrator.	Manajemen patch di AMS
Diperbarui: Apa itu AMS?	Memindahkan beberapa topik sebelumnya di bawah Apa itu AMS? untuk menjadi bagian dari Deskripsi Layanan AMS.	Deskripsi layanan
Diperbarui: Offboarding multi-account landing zone	Membuat berbagai klarifikasi.	Offboard dari akun landing zone multi-akun AMS

Ubah	Deskripsi	Tautan
Diperbarui: AWS Transfer Family (AMS SSPS)	Menambahkan tautan ke tutorial pengaturan transfer.	Gunakan SSP AMS untuk menyediakan AWS Transfer Family di akun AMS Anda
Konten yang Diperbarui: Penyediaan layanan mandiri	Mengganti "CodeSuite" dengan "Layanan kode" sesuai hukum AWS.	Gunakan SSP AMS untuk menyediakan layanan Kode AMS di akun AMS Anda
Konten yang Diperbarui: CloudWatch metrik dan alarm	Menambahkan tautan ke Contoh: Hitung kemunculan istilah.	Membuat CloudWatch metrik dan alarm khusus di AMS
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	AMIs. csv-and-notes.04.2023
Maret, 2023		
Konten yang Diperbarui: Offboarding dari AMS	Mengklarifikasi sumber daya apa yang dihapus saat offboard akun landing zone multi-akun	Offboard dari akun landing zone multi-akun AMS
Diperbarui: AMS AMIs	Menambahkan tautan ke file AMI ZIP untuk setiap bulan di bagian Riwayat Dokumen.	Riwayat dokumen
Diperbarui: Remediasi otomatis	Dihapus dukungan LVM untuk otomatisasi EC2 volume.	Remediasi peringatan otomatis AMS
Diperbarui: Patch RACI	Beberapa pembaruan dan klarifikasi pada RACI untuk ditambah.	Matriks tanggung jawab AMS (RACI)

Ubah	Deskripsi	Tautan
Konten yang Diperbarui: Penyediaan layanan mandiri	Menambahkan bullet FAQ. Untuk meluncurkan agen AWS Datasync baru, konsumsi WIGS tidak diperlukan.	Mode Penyediaan Layanan Mandiri di AMS
Konten yang Diperbarui: Penyediaan layanan mandiri	Menambahkan bullet FAQ. Untuk meluncurkan agen AWS Datasync baru, konsumsi WIGS tidak diperlukan.	Mode Penyediaan Layanan Mandiri di AMS
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	AMIs. csv-and-notes.03.2023
Februari, 2023		
Konten yang Diperbarui: Offboarding dari AMS	Mengklarifikasi cara melepaskan lingkungan landing zone multi-akun, VPCs, dan akun Aplikasi	Akun AMS offboard
Konten yang Diperbarui: Menemukan ARNs	Ditambahkan describe- table DynamoDB CLI untuk menemukan tabel DynamoDB ARN	Temukan Nama Sumber Daya Amazon (ARNs) di AMS

Ubah	Deskripsi	Tautan
Konten yang Diperbarui: Penyediaan Layanan Mandiri	Menghapus opsi AMS CodeSuite "" karena ini bukan SSPS yang sebenarnya. Anda masih dapat menggunakan Management AWS service Self-provisioned service Add (review required) (ct-3qe6io8t6jtny) ubah jenis dan minta tiga layanan:, dan. CodeBuild CodeDeploy CodePipeline AMS kemudian akan menyediakan peran IAM berikut ke akun Anda:customer_codebuild_service_role ,customer_codedeploy_service_role , danaws_codepipeline_service_role . Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.	Mode Penyediaan Layanan Mandiri di AMS
Konten yang Diperbarui: Pembaruan Secrets Manager	Peran yang dikoreksi diperlukan untuk landing zone multi-akun (MALZ) vs single-account landing zone (SALZ).	Berbagi Kunci menggunakan Secrets Manager FAQ
Konten yang Diperbarui: Remediasi peringatan otomatis AMS	Menambahkan dukungan untuk volume Logical Volume Manager (LVM).	EC2 otomatisasi remediasi penggunaan volume

Ubah	Deskripsi	Tautan
Konten yang Diperbarui: AMS Amazon Machine Images (AMIs)	Menambahkan bagian Offboarding AMS AMIs dengan kode sampel untuk dihapus AMIs dari akun Anda.	Gambar Mesin AMS Amazon (AMIs)
Konten yang Diperbarui: Peran Pengguna IAM	Memperbarui kebijakan IAM: AMSBilling Kebijakan.	Peran pengguna IAM di AMS
Konten Baru: Tidak Didukung OSes	Menambahkan informasi tentang layanan apa yang disediakan AMS untuk sistem operasi yang tidak didukung (OSes).	Kemampuan untuk sistem operasi yang tidak didukung di AMS
Konten yang Diperbarui: Laporan sesuai permintaan	Laporan sesuai permintaan tertentu tidak tersedia di AMS Advanced dan salah ditampilkan sebagai tersedia.	Laporan berdasarkan permintaan
Konten yang Diperbarui: Offboarding Akun AMS	Instruksi yang diklarifikasi untuk offboarding akun aplikasi MALZ.	Akun Aplikasi AMS Offboard
Konten yang Diperbarui: Secrets Manager	Memperbaiki nama peran IAM yang diperlukan untuk menggunakan Secrets Manager.	FAQ Secrets Manager di AWS Managed Services
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	AMIs. csv-and-notes.02.2023
Januari, 2023		

Ubah	Deskripsi	Tautan
Konten Baru: AWS Device Farm (AMS SSPS)	Menambahkan layanan SSPS baru: AWS Device Farm.	Gunakan SSP AMS untuk menyediakan AWS Device Farm di akun AMS Anda
Diperbarui: didukung versi Windows	Menambahkan dukungan untuk Windows Server 2022.	Gambar Mesin AMS Amazon (AMIs), Konfigurasi yang didukung, dan Pemberitahuan AMS AMI dengan SNS
Diperbarui: Manajemen kontinuitas	Memperbarui aturan dalam paket cadangan AMS default.	Paket cadangan default, landing zone multi-akun
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	AMIs. csv-and-notes.01.2023
Desember, 2022		
Diperbarui: Menggunakan benteng	Memperbaiki tautan buruk.	Mengakses instance menggunakan benteng
Diperbarui: Resource Scheduler	Membuat beberapa perbaikan dan menambahkan tautan ke Penjadwal AWS Instance untuk konteks lebih lanjut.	AWS Managed Services Resource Scheduler

Ubah	Deskripsi	Tautan
Diperbarui: Windows AMIs dan Konfigurasi yang Didukung (untuk Windows AMIs baru)	Konten AMS AMI yang diperbarui ditambahkan dari EC2 Peluncuran (Windows Server 2016 dan yang lebih baru) ke EC2 Peluncuran (Windows Server 2016 dan Windows Server 2019) dan menambahkan EC2 LaunchV2 (Windows Server 2022 dan yang lebih baru). Diperbarui berbasis Windows dari AMIs Microsoft Windows Server (2012, 2012 R2, 2016, dan 2019) ke Microsoft Windows Server (2012, 2012 R2, 2016, 2019 dan 2022).	Gambar Mesin AMS Amazon (AMIs) dan Deskripsi layanan
Diperbarui: Bagian Penjadwal Sumber Daya	Metode yang disempurnakan untuk menerapkan dan menyesuaikan Penjadwal Sumber Daya AMS.	AWS Managed Services Resource Scheduler
Diperbarui: Mengatur AMS: DNS pribadi dan publik	Memperbarui diagram arsitektur DNS.	Menyiapkan DNS pribadi dan publik
Diperbarui: MALZ arsitektur jaringan	Memperbarui diagram dan menambahkan panduan untuk Accelerate akun aplikasi.	Arsitektur jaringan MALZ
Diperbarui: Menyiapkan: Menggunakan tag	Catatan baru: penandaan khusus hanya didukung untuk akun aplikasi MALZ, bukan akun inti.	Penandaan otomatis infrastruktur AMS

Ubah	Deskripsi	Tautan
Diperbarui: Manajemen akses: menggunakan benteng	Pengantar yang diperbarui untuk menyertakan benteng RDP.	Menghemat biaya pada benteng single-account landing zone (SALZ)
Diperbarui: Pengaturan default AMS: peringatan	EC2 Contoh yang ditambahkan: Penggunaan Volume Non-Root ke tabel peringatan.	Peringatan dari pemantauan dasar di AMS
Diperbarui: Manajemen Kontinuitas	Menambahkan panduan tentang pencadangan berkelanjutan.	Bagaimana manajemen kontinuitas bekerja
Diperbarui: Konfigurasi EC2 instans otomatis	Menambahkan dukungan untuk PowerBroker Identity Service (PBIS) dan On Instance Code (OIC).	Secara otomatis memperbarui PBIS pada instance Linux dan Secara otomatis memperbarui kode pada instance Linux
Diperbarui: Penyediaan Layanan Mandiri untuk Secrets Manager	Memperbarui CT untuk menambahkan Secrets Manager ke akun Anda (di bawah FAQs).	Gunakan SSP AMS untuk menyediakan AWS Secrets Manager di akun AMS Anda
Diperbarui: Manajemen log	Memperbarui daftar log EC2 tingkat sistem.	Amazon Elastic Compute Cloud (Amazon EC2) - log tingkat sistem
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	AMIs. csv-and-notes.12.2022
November, 2022		
Diperbarui: Gambar Mesin AMS Amazon (AMIs)	Diperbarui versi SUSE Linux yang didukung.	Gambar Mesin AMS Amazon (AMIs)

Ubah	Deskripsi	Tautan
Diperbarui: akun MALZ	Menambahkan panduan untuk menghapus akun aplikasi yang Dikelola Pelanggan.	Akun aplikasi yang Dikelola Pelanggan
Diperbarui: Menyiapkan AMS	Ditambahkan customer-ams-amazon2-security-enhanced .	Pemberitahuan AMS AMI dengan SNS
Diperbarui: Cara kerja pemantauan	Penjelasan terbaru tentang pemberitahuan layanan dan laporan insiden.	Cara kerja pemantauan
Diperbarui: Jenis akun Aplikasi MALZ	Memperbaiki penjelasan jenis akun.	Jenis akun aplikasi
Diperbarui: Mode pengembangan	Menambahkan peringatan tentang mode Pengembang.	Sebelum Anda memulai dengan mode AMS Developer
Diperbarui: Manajemen acara yang direncanakan	Ditambahkan bagian: Jenis PEM	Manajemen acara yang direncanakan di AWS Managed Services
Diperbarui: Gambar Mesin Amazon (AMIs)	Diperbarui versi SUSE Linux yang didukung	Gambar Mesin AMS Amazon (AMIs)
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	AMIs. csv-and-notes.11.2022
Oktober, 2022		
Baru: Konfigurasi Instans Otomatis	Bagian baru menjelaskan proses Konfigurasi Instans Otomatis.	Konfigurasi instans otomatis di AMS Advanced

Ubah	Deskripsi	Tautan
Baru: Hanya CT manual yang dapat diterima untuk beberapa SSPS	Memperbarui lebih dari 50 layanan penyediaan swalayan FAQs untuk menggunakan CT manual dan bukan CT otomatis untuk menambahkan SSPS.	Mode Penyediaan Layanan Mandiri di AMS
Pembaruan: Menyiapkan AMS	Menambahkan dua kebijakan ke profil instans Amazon EC2 IAM untuk MALZ.	EC2 Profil instans IAM
Baru: Perpustakaan detektif kustom dan aturan pencegahan.	Menambahkan serangkaian contoh kebijakan kontrol layanan (SCPs) dan kontrol aturan Config preventif berdasarkan pembelajaran kami dari beberapa pelanggan.	Aturan yang Dikurasi SCPs dan Config
Pembaruan: AWS Backup peringatan	Menambahkan peringatan: "Jangan mengedit paket cadangan AMS karena perubahan Anda mungkin hilang. Sebagai gantinya, buat paket cadangan baru menggunakan ct-2hyozb pa0sx0m untuk konfigurasi kustom Anda."	Bagaimana manajemen kontinuitas bekerja
Pembaruan: AWS Backup hati-hati	Menambahkan catatan tentang menambahkan peran IAM baru ke federasi Anda.	Menerapkan sumber daya IAM di AMS Advanced
Pembaruan: Manajemen pemantauan	Peringatan menghasilkan laporan insiden, bukan permintaan layanan.	Cara kerja pemantauan

Ubah	Deskripsi	Tautan
Pembaruan: Bawa EPS Anda sendiri	Berlaku untuk SALZ serta MALZ.	AMS membawa EPS Anda sendiri
Pembaruan: Mempercepat akun Aplikasi	Mengklarifikasi bahwa akun Accelerate Anda adalah akun Aplikasi.	Jenis akun aplikasi
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	AMIs. csv-and-notes.10.2022
September, 2022		
Diperbarui: Contoh perintah CLI untuk menemukan sumber daya	Menambahkan contoh baru dan bahwa --region opsi mungkin diperlukan.	Menemukan data yang Anda butuhkan (SKMS), AMS
Diperbarui: Menyediakan peran IAM	Peran IAM sekarang dapat dibuat dan dikelola dengan. <code>AWSManagedServices CloudFormationAdminRole</code>	Membuat tumpukan menggunakan mode Perubahan Langsung
Diperbarui: Standar Teknis AMS	AMS-STD-007 Logging: (#20) Persyaratan penerusan yang diklarifikasi.	Keamanan dan kepatuhan
Diperbarui: Bagaimana manajemen kontinuitas bekerja	Merevisi kata-kata Start Backup Job menjadi “sesuai permintaan” daripada “sudah ada”.	Bagaimana manajemen kontinuitas bekerja

Ubah	Deskripsi	Tautan
Diperbarui: Keamanan dan kepatuhan	Deskripsi dan panduan yang diperbarui untuk standar AMS-STD-007 nomor 20: meneruskan log antar akun.	Keamanan dan kepatuhan
Diperbarui: Ubah kasus penggunaan manajemen	Menghapus tautan rusak ke Panduan Pengguna Manajemen Perubahan lama.	Ubah kasus penggunaan manajemen
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	AMIs. csv-and-notes.09.2022
Agustus 11, 2022		

Ubah	Deskripsi	Tautan
Diperbarui: Judul Bab untuk konsistensi dan pembacaan, memindahkan beberapa sub-bagian topik ke bagian yang lebih tepat	“Arsitektur jaringan MALZ” dan “arsitektur jaringan SALZ” sekarang, keduanya, subbagian dari bagian “Arsitektur jaringan” tingkat atas, sebelumnya bagian “arsitektur jaringan AMS” “Mode untuk manajemen perubahan” adalah judul baru untuk “Manajemen perubahan” “Pengaturan default” sekarang menjadi subbagian dari “Menyiapkan AMS” “Aturan klaim AD FS dan pengaturan SAMP” (sebelumnya “Aturan klaim Layanan ActiveDirectory Federasi (ADFS) dan pengaturan SAMP) sekarang menjadi subbagian dari “Menyiapkan AMS” “Manajemen akses” adalah judul baru untuk “Akses di AMS” dan dipindahkan ke atas di TOC “Menemukan data yang Anda butuhkan” adalah judul baru untuk “Manajemen pengetahuan layanan”	Apa itu AWS Managed Services?

Ubah	Deskripsi	Tautan
	“Laporan dan opsi” adalah judul baru untuk “Pelaporan AMS” dan lebih rendah di TOC “Operations on Demand” sekarang menjadi topik terakhir di TOC	
Diperbarui: Menemukan dan ARN, Baru: Menemukan sumber daya dengan ARN	Kedua prosedur sepenuhnya ditulis ulang untuk kegunaan.	Temukan Nama Sumber Daya Amazon (ARNs) di AMS dan Temukan sumber daya oleh ARN di AMS.
Diperbarui: Menghubungkan CMA Anda dengan Transit Gateway	Otomatisasi tidak mendukung penambahan rute ke domain rute inti, dan prosedur perlu diperbarui.	Menghubungkan CMA Anda dengan Transit Gateway
Diperbarui: Harga komponen dasar MALZ	Semua harga dalam Dolar AS, diformat dengan tanda dolar.	Komponen dasar lingkungan AMS
Diperbarui: Catatan AMS AMI	File zip menyertakan catatan tentang gambar mesin AMS Amazon terbaru (AMIs) dan file CSV terbaru AMIs.	AMIs. csv-and-notes.08.2022
Juli 14, 2022		
Diperbarui: Pelaporan Layanan Mandiri	Menambahkan instruksi untuk mengenkripsi AWS Glue metadata dengan kunci KMS.	Laporan layanan mandiri
Diperbarui: Pemantauan dasar AMS	Menambahkan peringatan DeleteRecoveryPoint cadangan.	Peringatan dari pemantauan dasar di AMS

Ubah	Deskripsi	Tautan
Diperbarui: Sistem operasi yang didukung	Ditambahkan Tanggal Akhir Dukungan untuk Amazon Linux 2.	Konfigurasi yang didukung
Diperbarui: Penyediaan Layanan Mandiri	Menambahkan prasyarat untuk Transfer SSPS. AWS	Gunakan SSP AMS untuk menyediakan AWS Transfer Family di akun AMS Anda
Diperbarui: Pelaporan AMS	Menambahkan catatan tentang Opt-in Regions.	Laporan dan opsi
Diperbarui: korespondensi RFC dan lampiran	Jenis file teks yang diizinkan yang diklarifikasi; khususnya , file YAMG harus diakhiri dengan .yaml (bukan .yml.tl).	Tambahkan korespondensi dan lampiran RFC (konsol)
Juni 21, 2022		
Konten diperbarui	Mode AMS yang sebelumnya dikenal sebagai “Mode Manajemen Ubah” atau “Mode CM Standar” sekarang dikenal sebagai “mode RFC.” Bagian mode telah diperluas.	Ikhtisar mode.
Alarm baru	Menambahkan AWS Backup alarm.	Peringatan dari pemantauan dasar di AMS
Juni 16, 2022		

Ubah	Deskripsi	Tautan
Konten baru	Manajemen insiden. Insiden yang bukan merupakan risiko keamanan sekarang dapat diselesaikan oleh AMS dengan persetujuan Anda dalam laporan insiden dan tidak memerlukan RFC dan persetujuan terpisah.	Manajemen insiden
Konten diperbarui	MALZ: Diagram arsitektur jaringan yang diperbarui. Pembaruan: VPC Peering untuk akun master VPC ke layanan bersama vpc harus dihapus karena tidak ada.	Arsitektur akun jaringan
	Layanan penyediaan layanan mandiri Sagemaker (SSPS). Diperbarui dengan peran IAM baru yang ditambahkan saat orientasi untuk penggunaan Sagemaker.	Gunakan AMS SSP untuk menyediakan Amazon SageMaker AI di akun AMS Anda

Ubah	Deskripsi	Tautan
	Untuk daftar pemberitahuan SNS yang AMIs didukung: Menambahkan customer-ams-sles 12, customer-ams-sles 15, customer-ams-amazon 1-security enhanced, customer-ams-rhel 8, customer-ams-rhel 8-security enhanced, 18, 2012, 2019, dan 2019-security-enhanced. customer-ams-ubuntu customer-ams-windows customer-ams-windows customer-ams-windows Dihapus customer-ams-rhel 6 dan customer-ams-rhel 6-keamanan ditingkatkan AMIs.	Pemberitahuan AMS AMI dengan SNS
	Email eskalasi yang dihapus.	Mendapatkan bantuan di AWS Managed Services
	Memindahkan daftar topik ke paragraf pembuka di bawah.	Apa itu AWS Managed Services?
	Log layanan yang diperbarui dengan tautan yang lebih baik untuk log penyeimbangan beban, juga diformat ulang.	Log layanan agregat AMS
Layanan penyediaan layanan mandiri EKS (SSPS). Menambahkan informasi tentang mengaktifkan enkripsi rahasia amplop di cluster Anda.	Gunakan AMS SSP untuk menyediakan Amazon EKS AWS Fargate di akun AMS Anda	

Juni 09, 2022

Ubah	Deskripsi	Tautan
Konten yang diperbarui, Mendapatkan bantuan	Email jalur eskalasi yang dihapus. AMS menyediakan metode komunikasi melalui laporan insiden, permintaan layanan, dan RFCs.	Mendapatkan bantuan di AWS Managed Services

Mei 12, 2022

Konten baru, model berlangganan Operations on Demand (OOD)	AMS telah mengubah orientasi Operations on Demand dari model pendaftaran dan perpanjangan saat ini, menjadi alokasi langganan dan model keikutsertaan default. Saat Anda menggunakan akun AMS, Anda secara otomatis terdaftar di Operations on Demand sekarang.	Operasi Sesuai Permintaan

April 14, 2022

Konten baru, Optimalisasi Biaya	AMS memberikan rekomendasi untuk optimasi biaya.	Optimalisasi biaya di AWS Managed Services
Konten yang diperbarui, Percepat akun di MALZ	Nama peran yang salah (CustomerDefaultAdminRole) telah diperbarui ke nama peran yang benar (AccelerateDefaultAdminRole).	AMS Mempercepat akun Bagian “Mengakses akun Akselerasi Anda”.
Konten yang diperbarui, AMS mengakses peran IAM	Menambahkan peran AMS IAM lainnya yang digunakan untuk mengakses akun Anda.	Mengapa dan kapan AMS mengakses akun Anda Bagian “akses akun pelanggan AMS peran IAM”.

Ubah	Deskripsi	Tautan
Konten yang diperbarui, paket cadangan AMS	Menambahkan paket cadangan yang dikelola AMS.	Paket cadangan AMS dan Brankas cadangan AMS
Konten yang diperbarui, AWS Secrets Manager	Memperbarui FAQ.	Gunakan SSP AMS untuk menyediakan AWS Secrets Manager di akun AMS Anda
Konten yang diperbarui, orientasi Direct Change Mode (DCM)	AMS tidak mendukung pelanggan Service Catalog orientasi ke DCM.	Memulai dengan mode Perubahan Langsung
Konten yang diperbarui, Deskripsi Layanan	Mengklarifikasi bagian Layanan yang Didukung: • Amazon EKS di AWS Fargate -> Amazon Elastic Kubernetes Service di Fargate • Amazon ECS untuk Fargate -> Layanan Kontainer Elastis Amazon di Fargate AWS • Amazon Kinesis -> Aliran Data Amazon Kinesis	AWS Layanan yang didukung
Konten yang diperbarui, Offboarding akun MALZ	Diperbarui untuk referensi jenis perubahan baru untuk akun aplikasi offboarding.	Akun Aplikasi AMS Offboard

Ubah	Deskripsi	Tautan
Konten yang diperbarui, manajemen insiden mode Pengembang	Deskripsi SLA insiden yang diperbarui ke: AMS SLA tidak berlaku untuk sumber daya yang dibuat atau diperbarui di luar Manajemen Perubahan AMS (Termasuk Mode Pengembang) oleh karena itu, sumber daya yang diperbarui atau dibuat dalam mode Pengembang secara otomatis terdegradasi ke P3 dan dukungan adalah upaya terbaik.	Manajemen insiden dalam mode Pengembang AMS
Konten yang diperbarui, orientasi DCM	Template RFC untuk DCM baru sekarang menyertakan bidang untuk ARN Penyedia SAFL Anda.	Memulai dengan mode Perubahan Langsung
Konten yang diperbarui, DCM untuk AWS CloudFormation	Petunjuk untuk membuat dan memperbarui AWS CloudFormation tumpukan sekarang menyertakan contoh YANG.	Transformasi AMS
Konten yang diperbarui, akun MALZ Tools	Ada peran IAM baru untuk migrasi: AWSManagedServicesMigrationRole	AWS Layanan Migrasi Aplikasi (AWS MGN) dan Aktifkan akses ke akun AMS Tools baru
Konten baru, akun landing zone multi-akun	Anda dapat membuat akun Accelerate di akun Manajemen AMS landing zone multi-akun.	AMS Mempercepat akun

Ubah	Deskripsi	Tautan
Konten yang diperbarui, API/ CLI instalasi SDK	Petunjuk penginstalan mencantumkan nama file yang salah untuk Mac/Linux penginstalan, dan perintah yang salah. Ini telah diperbaiki.	Menggunakan AMS API dan CLI
Konten yang diperbarui, Percepat akun di MALZ	Ada nama aturan (Customer DefaultAdminRole) yang salah, itu telah diperbarui ke yang benar (AccelerateDefault AdminRole).	AMS Mempercepat akun, Bagian “Mengakses akun Akselerasi Anda”
Konten yang diperbarui, pemantauan	Pemantauan penggunaan root direvisi dari 85% menjadi 95%.	Peringatan dari pemantauan dasar di AMS
Konten yang diperbarui, pemberitahuan AMI	Anda dapat membuat banyak jenis notifikasi SNS untuk AMS baru AMIs, kami telah menambahkan informasi tentang membuat berbagai jenis.	Pemberitahuan AMS AMI dengan SNS
Konten yang diperbarui, pengaturan default AMS	Referensi yang dihapus ke Macie Classic, digantikan oleh Macie.	Peringatan dari pemantauan dasar di AMS
Konten yang diperbarui, awalan cadangan AMS	Mengalfabetisasi daftar awalan yang dicadangkan.	Awalan cadangan AMS
Konten yang diperbarui, Deskripsi Layanan	Bagian fitur tentang manajemen perubahan dan penyediaan layanan mandiri diperbarui dengan informasi lebih lanjut tentang mode AMS.	AWS Managed Services (AMS) AMS Fitur rencana operasi lanjutan

Ubah	Deskripsi	Tautan
Konten yang diperbarui, AWS Secrets Manager	Berbagi Kunci menggunakan Secrets Manager.	Februari 10, 2022
Konten baru, Penyediaan layanan mandiri, Amazon Connect	Menambahkan FAQ tentang cara meminta untuk menambahkan daftar negara untuk panggilan keluar atau masuk.	Februari 10, 2022
Konten baru, Penyediaan layanan mandiri, Amazon EKS di Fargate	Menambahkan batasan FAQ yang menerapkan kluster EKS melalui kit pengembangan AWS cloud (CDK) atau CloudFormation Ingest tidak didukung di AMS.	Februari 10, 2022
Konten diubah, mode Pengembang	Koreksi, Anda tidak menggunakan RFC atau permintaan layanan untuk menetapkan pengguna ke solusi federasi Anda, Anda melakukannya sendiri tergantung pada solusi Anda.	Februari 10, 2022
	Perhatikan bahwa IAM tidak didukung di DCM.	Februari 10, 2022
Konten yang diubah, mode Perubahan Langsung (DCM)	DCM, perhatikan validasi yang kami lakukan.	Februari 10, 2022
	DCM, klarifikasi pembatasan peran yang berbeda.	Februari 10, 2022
Konten yang diubah, Memantau peringatan dasar	Peringatan sumber daya kluster Redshift berubah.	Februari 10, 2022

Ubah	Deskripsi	Tautan
Konten yang diubah, pelaporan layanan mandiri	Menambahkan nama bucket s3 yang tepat, (ams-reporting-data-a<Account_ID>) untuk digunakan pelanggan untuk mengambil laporan.	Februari 10, 2022
Konten yang diubah, konten yang diperbarui untuk referensi jenis perubahan otomatis, bukan Manajemen manual Lainnya Lainnya (MOO)	Konten akun aplikasi multi-account landing zone (MALZ) yang diperbarui untuk mereferensikan jenis perubahan otomatis (tiga, “Mengaitkan lampiran TGW ke tabel rute”, “Buat rute di tabel rute TGW untuk terhubung ke VPC ini”, dan “Mengonfigurasi tabel Rute VPC Anda untuk menunjuk ke gateway transit Zona Pendaratan Multi-Akun AMS”). Menerima peringatan yang dihasilkan oleh AMS Pemberitahuan peringatan berbasis tag	Februari 10, 2022
Konten yang diubah: AMS AMIs.	Menambahkan informasi baru tentang peningkatan keamanan AMIs. lihat Konfigurasi yang didukung, Gambar Mesin AMS Amazon (AMIs) dan Keamanan ditingkatkan AMIs	27 Januari 2022

Ubah	Deskripsi	Tautan
Konten baru: Penyediaan layanan mandiri.	Ditambahkan Amazon Fsx untuk OpenZFS. Lihat Gunakan AMS SSP untuk menyediakan Amazon FSx untuk OpenZFS di akun AMS Anda .	27 Januari 2022
Konten yang diubah: CodeDeploy layanan penyediaan layanan mandiri (SSPS).	Nama peran tambahan, dan catatan pembatasan tambahan. lihat. Gunakan SSP AMS untuk menyediakan AWS CodeDeploy di akun AMS Anda	27 Januari 2022
Konten yang diubah: Tautan yang diperbarui.	Memperbaiki tautan rusak: AMS-AMIs, Menemukan pengaturan Anda, Menemukan ID Tumpukan, Menemukan ID VPC,, ListVpcSummaries ListStack Summaries, dan. GetStack APIs Sebagai contoh, lihat Temukan tumpukan IDs di AMS .	Januari 13, 2022
Konten yang diubah: EKS Support untuk Fargate	Menambahkan batasan ke FAQs: Membuat atau mengelola EC2 nodegroup dengan EKS tidak didukung. Lihat Gunakan AMS SSP untuk menyediakan Amazon EKS AWS Fargate di akun AMS Anda .	Januari 13, 2022

Ubah	Deskripsi	Tautan
Konten yang diubah: CloudFormation, Mode Perubahan Langsung (DCM)	Menambahkan instruksi untuk membuat atau memperbarui tumpukan CF menggunakan AmsStackTransform. Lihat Membuat tumpukan menggunakan mode Perubahan Langsung .	Januari 13, 2022
Konten yang diubah: Keseseragaman dalam Nama Layanan AWS	Referensi AMS untuk Layanan AWS sama persis dengan AWS judul atau metadata resmi. Sebelumnya, ada variasi kecil yang rumit pencocokan pola. Sebagai contoh, lihat Gunakan AMS SSP untuk menyediakan Alexa for Business di akun AMS Anda .	Januari 13, 2022
Konten yang diubah: Penyediaan layanan mandiri Elastic Container Registry (ECR)	Menambahkan item FAQ untuk menggunakan ECR untuk mengelola izin pengguna. Lihat Gunakan AMS SSP untuk menyediakan Amazon Elastic Container Registry di akun AMS Anda .	Januari 13, 2022

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.