AMS Mempercepat Konsep dan Prosedur

Panduan Pengguna AMS Accelerate

Versi October 3, 2025

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

Panduan Pengguna AMS Accelerate: AMS Mempercepat Konsep dan Prosedur

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 adalah properti dari pemiliknya masing-masing, yang mungkin atau mungkin tidak berafiliasi dengan, berhubungan dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu AMS Accelerate? 1
Rencana operasi 1
Mempercepat rencana operasi 2
Rencana operasi lanjutan 2
Cara kerjanya 2
Istilah kunci 3
Deskripsi layanan 10
AWS Managed Services (AMS) AMS Mempercepat fitur rencana operasi 10
Konfigurasi yang didukung 13
Layanan yang didukung 15
Peran dan tanggung jawab 18
Lingkup perubahan yang dilakukan oleh AMS Accelerate 34
Sistem operasi yang tidak didukung 35
Kontak dan eskalasi 36
Jam kontak 36
Jam kerja 37
Jalur eskalasi 37
Inventaris sumber daya 38
Memulai 39
Orientasi 39
Prasyarat orientasi 39
Langkah 1. Penemuan akun 42
Langkah 2. Sumber daya manajemen orientasi 44
Langkah 3. Fitur orientasi dengan kebijakan default 54
Langkah 4. Sesuaikan fitur 64
Menggunakan konsol AMS 66
Pola AMS 68
Cara kerja pola AMS 68
Pola AMS 69
Konfigurasi instans otomatis 72
Cara kerjanya 73
Instalasi otomatis Agen SSM 74
Perubahan konfigurasi instans otomatis 76
Offboard dari AMS Accelerate 80

Efek offboarding 80
Offboarding dengan dependensi 83
Mendapatkan bantuan offboarding 83
Pengaturan notifikasi 84
Penandaan 85
Tag 86
Apa itu tag? 87
Cara kerja penandaan 87
Tag yang dikelola pelanggan 87
Tag yang dikelola akselerasi 91
Tag yang disediakan pelanggan 92
Alat manajemen tag 93
Tagger Sumber Daya 93
CloudFormation 112
Terraform 116
Laporan insiden, permintaan layanan, dan pertanyaan penagihan 118
Manajemen insiden 118
Apa itu manajemen insiden? 119
Bagaimana respons dan resolusi insiden bekerja 120
Bekerja dengan insiden 121
Manajemen permintaan layanan 124
Kapan menggunakan permintaan layanan 125
Cara kerja manajemen permintaan layanan 126
Membuat permintaan layanan 126
Memantau dan memperbarui permintaan layanan 128
Mengelola permintaan layanan dengan API dukungan 129
Menanggapi permintaan layanan yang dihasilkan AMS Accelerate 129
Laporan insiden dan pengujian permintaan layanan 130
Pertanyaan penagihan 130
Manajemen acara yang direncanakan 132
Kriteria AMS PEM 132
Jenis PEM 132
Proses AMS PEM 133
PEM FAQs 133
Operasi Sesuai Permintaan 135
Meminta Operasi AMS Sesuai Permintaan 144

Membuat perubahan pada penawaran Operations on Demand 145
Laporan dan opsi 146
Laporan berdasarkan permintaan 146
Laporan manajemen host AMS 147
Laporan Cadangan AMS 147
AWS Config Laporan Kepatuhan Kontrol 150
Laporan Konfigurasi Respons Aturan Konfigurasi AMS Config 152
Insiden Mencegah dan Memantau Laporan Pembicara Teratas 154
Laporan Detail Biaya Penagihan 156
Laporan Remediator Tepercaya 157
Laporan layanan mandiri 160
Operasi API internal 161
Laporan patch (harian) 164
Laporan Backup (harian) 174
Laporan insiden (mingguan) 178
Laporan penagihan (bulanan) 181
Laporan agregat 184
Dasbor laporan layanan mandiri AMS 186
Kebijakan retensi data 193
Offboard dari SSR 194
Manajemen akses 195
Mengakses konsol tersebut 195
Izin untuk menggunakan fitur 195
Mengapa dan kapan kami mengakses akun Anda 210
Pemicu Akses 210
Akses peran IAM 211
Bagaimana kami mengakses akun Anda 213
Bagaimana dan kapan menggunakan root 214
Manajemen keamanan 215
Menggunakan Dokumen SSM Log4j untuk menemukan kejadian 216
Pemantauan keamanan infrastruktur 217
Menggunakan peran tertaut layanan 219
AWS kebijakan terkelola 232
Perlindungan data 241
Monitor dengan Amazon Macie 242
Monitor dengan GuardDuty 242

Monitor dengan Amazon Route 53 Resolver DNS Firewall ... 244
Enkripsi data ... 245
AWS Identity and Access Management ... 245
Mengautentikasi dengan identitas di AMS Accelerate ... 246
Mengelola akses menggunakan kebijakan ... 253
Respons Insiden Keamanan ... 254
Cara kerjanya ... 255
Persiapkan ... 255
Mendeteksi ... 256
Analisis ... 257
Mengandung ... 258
Membasmi ... 260
Memulihkan ... 261
Laporan Pasca Insiden ... 261
Runbook Respons Insiden Keamanan ... 262
Pencatatan dan pemantauan peristiwa keamanan ... 268
Kepatuhan konfigurasi ... 268
Pustaka Aturan Konfigurasi AMS ... 269
Tanggapan terhadap pelanggaran ... 294
Membuat pengecualian aturan ... 296
Mengurangi AWS Config biaya ... 297
Tanggapan temuan yang disesuaikan ... 297
Respons insiden ... 300
Respons insiden dan orientasi ... 300
Ketahanan ... 300
Kontrol keamanan untuk sistem end-of-support operasi ... 301
Praktik terbaik keamanan ... 301
Ubah ulasan keamanan permintaan ... 301
Proses Manajemen Risiko Keamanan Pelanggan ... 302
AMS Mempercepat standar teknis ... 303
Kontrol standar di AMS Accelerate ... 303
Perubahan yang menimbulkan risiko keamanan tinggi atau sangat tinggi di lingkungan Anda ... 317
FAQ Keamanan ... 319
Kapan insinyur operasi AMS mengakses lingkungan saya? ... 319

Peran apa yang diasumsikan oleh insinyur operasi AMS saat mereka mengakses akun saya? 319
Bagaimana cara insinyur operasi AMS mengakses akun saya? 320
Bagaimana cara melacak perubahan yang dibuat oleh AMS di AWS akun terkelola AMS saya? 320
Apa saja kontrol proses untuk akses insinyur operasi AMS ke akun saya? 321
Bagaimana akses istimewa dikelola? 321
Apakah insinyur operasi AMS menggunakan MFA? 322
Apa yang terjadi pada akses mereka ketika karyawan AMS meninggalkan organisasi atau mengubah peran pekerjaan? 322
Kontrol akses apa yang mengatur akses insinyur operasi AMS ke akun saya? 322
Bagaimana AMS memantau akses pengguna root? 323
Bagaimana AMS menanggapi insiden keamanan? 323
Sertifikasi dan kerangka kerja standar industri apa yang dipatuhi AMS? 323
Bagaimana saya bisa mendapatkan akses ke laporan terbaru tentang sertifikasi keamanan, kerangka kerja, dan kepatuhan? AWS 324
Apakah AMS berbagi diagram arsitektur referensi dari berbagai aspek fitur AMS? 324
Bagaimana AMS melacak siapa yang mengakses akun saya dan apa kebutuhan bisnis untuk akses? 324
Apakah teknisi AMS memiliki akses ke data saya yang disimpan dalam layanan penyimpanan AWS data, seperti Amazon S3, Amazon RDS, DynamoDB, dan Amazon Redshift? 325
Apakah insinyur AMS memiliki akses ke data pelanggan yang disimpan di Amazon EBS, Amazon EFS, dan Amazon? FSx 325
Bagaimana akses dibatasi atau dikontrol untuk peran otomatisasi yang memiliki hak istimewa tinggi untuk lingkungan saya? 325
Bagaimana AMS menerapkan prinsip hak istimewa paling sedikit seperti yang dianjurkan dalam Kerangka Kerja AWS Well-Architected untuk peran otomatisasi? 326
Sistem pencatatan dan pemantauan apa yang digunakan untuk mendeteksi upaya akses yang tidak sah atau aktivitas mencurigakan yang melibatkan peran otomatisasi? 326
Bagaimana insiden keamanan atau pelanggaran terkait infrastruktur otomatisasi ditangani, dan protokol apa yang membantu respons dan mitigasi yang cepat? 327
Apakah penilaian keamanan reguler, pemindaian kerentanan, dan tes penetrasi dilakukan pada infrastruktur otomatisasi? 327
Bagaimana akses ke infrastruktur otomasi dibatasi hanya untuk personel yang berwenang? 327

Langkah-langkah apa yang diterapkan untuk menegakkan standar keamanan dan mencegah akses yang tidak sah atau pelanggaran data dalam pipa otomatisasi? 327
Apakah deteksi atau pemantauan anomali diaktifkan untuk akses atau pencatatan audit guna mendeteksi eskalasi hak istimewa atau penyalahgunaan akses untuk secara proaktif memperingatkan tim AMS? 328
Jenis data pelanggan apa yang diambil dari akun terkelola AMS, dan bagaimana ini digunakan dan disimpan? 328
Pemantauan dan manajemen acara 329
Apa itu pemantauan? 329
Cara kerja pemantauan 330
EC2 pemberitahuan yang dikelompokkan misalnya 332
Pemberitahuan peringatan berbasis tag 333
Peringatan dari pemantauan dasar di AMS 334
Pemberitahuan insiden sadar aplikasi di AMS 357
Onboard ke AppRegistry dan membuat aplikasi 358
Buat tag untuk mengaktifkan pengayaan kasus 359
Sesuaikan tingkat keparahan kasus dukungan AMS untuk aplikasi Anda 359
Tinjau izin yang diperlukan 360
Manajer Alarm 361
Bagaimana Manajer Alarm bekerja 361
Memulai dengan Alarm Manager 362
Tag Alarm Manager 363
Profil konfigurasi Manajer Alarm 368
Membuat CloudWatch alarm tambahan 386
Melihat jumlah sumber daya yang dipantau oleh Manajer Alarm 387
Remediasi peringatan otomatis AMS 388
EC2 kegagalan pemeriksaan status: Catatan otomatisasi remediasi 393
EC2 otomatisasi remediasi penggunaan volume 394
Otomatisasi remediasi acara penyimpanan rendah Amazon RDS 395
Router Acara AMS 395
Aturan EventBridge Terkelola Amazon yang diterapkan oleh AMS 396
Membuat Aturan Terkelola untuk AMS 398
Mengedit Aturan Terkelola untuk AMS 399
Menghapus Aturan Terkelola untuk AMS 399
Remediator Tepercaya 399
Manfaat utama 399

Cara kerja Remediator Tepercaya ... 400
Istilah kunci ... 400
Memulai dengan Remediator Tepercaya ... 402
Rekomendasi Compute Optimizer yang Didukung ... 404
Trusted Advisor Cek yang didukung ... 408
Konfigurasikan remediasi cek ... 466
Alur kerja keputusan mode eksekusi ... 470
Konfigurasikan tutorial remediasi ... 470
Bekerja dengan remediasi ... 473
Log remediasi ... 477
Integrasi dengan QuickSight ... 481
Praktik terbaik ... 484
FAQs ... 484
Pemantauan dan manajemen insiden untuk EKS ... 488
Apa itu pemantauan dan manajemen insiden untuk Amazon EKS? ... 488
Cara kerja pemantauan dan manajemen insiden untuk Amazon EKS ... 489
Matriks tanggung jawab AMS (RACI) ... 490
Peringatan dasar ... 492
Peringatan dan tindakan ... 493
Persyaratan ... 500
Di atas kapal ... 502
Offboard ... 503
Manajemen kontinuitas ... 504
Bagaimana manajemen kontinuitas bekerja ... 504
Pilih paket cadangan AMS ... 505
Paket cadangan AMS default ... 506
Paket cadangan yang disempurnakan ... 506
Rencana pencadangan Data Sensitif ... 507
AMS Mempercepat rencana cadangan orientasi ... 507
Tandai sumber daya Anda untuk cadangan ... 508
Lihat cadangan di brankas AMS ... 510
Pemantauan dan pelaporan untuk cadangan ... 511
Manajemen tambalan ... 513
Rekomendasi penambalan ... 514
Rekomendasi tanggung jawab tambalan ... 515
Panduan untuk tim aplikasi ... 515

Panduan untuk tim operasi keamanan 516
Panduan untuk tim tata kelola dan kepatuhan 516
Contoh desain untuk aplikasi Windows ketersediaan tinggi 517
Rekomendasi tambalan FAQs 517
Buat jendela tambalan 518
Batas jendela pemeliharaan patch 518
Buat jendela patch Patch Tuesday: konsol AMS 520
Buat jendela tambalan: AWS CloudFormation 521
Buat jendela tambalan: Konsol Systems Manager 522
Buat jendela tambalan: Systems Manager CLI 524
Patch dengan kait 525
Kait tambalan AMS RACI 526
Buat dokumen SSM untuk kait patch 527
Konfigurasikan jendela pemeliharaan patch AMS untuk menggunakan dokumen Perintah SSM Anda sebagai kait patch AMS 527
AMS Mempercepat garis dasar tambalan 529
Garis dasar tambalan default 529
Garis dasar patch kustom 530
Izin penambalan sesuai permintaan 530
Memahami notifikasi tambalan dan kegagalan tambalan 531
Permintaan layanan patch dan pemberitahuan email 532
Pemberitahuan tambalan melalui CloudWatch Acara 532
Investigasi kegagalan tambalan 536
Optimalisasi biaya dengan Penjadwal Sumber Daya AMS 538
Menggunakan sumber daya dengan Resource Scheduler 539
Penjadwal Sumber Daya Orientasi 540
Menyesuaikan Penjadwal Sumber Daya 541
Menggunakan Resource Scheduler 542
Bekerja dengan periode dan jadwal 545
Memberi tag pada sumber daya 551
Estimator biaya 551
Penekan alarm 552
Manajemen log 554
Manajemen log - AWS CloudTrail 554
Mengakses dan mengaudit log CloudTrail 556
Melindungi dan mempertahankan kayu CloudTrail gelondongan 556

Mengakses log Amazon EC2 556
Mempertahankan log Amazon EC2 557
Manajemen log - Amazon EC2 557
Manajemen log - Log Aliran VPC Amazon 558
Melacak perubahan 560
Melihat catatan perubahan Anda 561
Kueri default 562
Memodifikasi filter datetime dalam kueri 570
Contoh kueri default 571
Ubah izin rekaman 582
AWS Systems Manager di Accelerate 584
Dokumen SSM Akselerasi AMS yang tersedia 584
AMS Mempercepat versi dokumen SSM 584
Harga Systems Manager 585
Riwayat dokumen 586
Pembaruan lebih awal 605
..... dcxxxiii

Apa itu AMS Accelerate?

Selamat datang di AMS Accelerate for Amazon Web Services (AWS). AMS Accelerate menyediakan berbagai layanan operasional untuk membantu Anda mencapai keunggulan operasional AWS. Baik Anda baru memulai di cloud, ingin menambah tim Anda saat ini, atau membutuhkan solusi operasional jangka panjang, Accelerate dapat membantu Anda memenuhi tujuan operasional Anda di cloud. Memanfaatkan Layanan AWS dan perpustakaan otomatisasi, konfigurasi, dan runbook, kami menyediakan solusi end-to-end operasional untuk lingkungan baru dan yang sudah ada. AWS

Layanan Accelerate memanfaatkan serangkaian fitur asli Layanan AWS dan untuk menyediakan serangkaian kemampuan manajemen infrastruktur yang komprehensif. Di dalamnya Layanan AWS, Accelerate membuat dan memelihara set kontrol pemantauan, pagar pembatas deteksi, otomatisasi, dan runbook yang dikuratori untuk mengoperasikan infrastruktur dengan cara yang sesuai dan aman.

Topik

- Rencana operasi AMS
- Menggunakan rencana operasi AMS Accelerate
- Istilah kunci AMS
- Deskripsi layanan
- Kemampuan untuk sistem operasi yang tidak didukung di Accelerate
- Kontak dan eskalasi
- Persediaan sumber daya untuk Accelerate

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.

Menggunakan rencana operasi AMS Accelerate

AMS Accelerate adalah rencana operasi AMS yang dapat mengoperasikan infrastruktur AWS yang mendukung beban kerja. Baik beban kerja Anda sudah ada di akun AWS atau Anda berencana untuk memigrasikan yang baru, Anda bisa mendapatkan keuntungan 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 dapat terus menggunakan mekanisme akses dan perubahan yang ada sementara AMS secara konsisten menerapkan praktik terbukti yang membantu meningkatkan skala tim Anda, mengoptimalkan biaya, meningkatkan keamanan dan efisiensi, dan meningkatkan ketahanan.

Meskipun AMS Accelerate dapat menyederhanakan operasi Anda, Anda tetap bertanggung jawab atas pengembangan aplikasi, penerapan, pengujian dan penyetelan, serta manajemen. AMS Accelerate hanya membuat perubahan di akun Anda sebagai akibat dari insiden, alarm, remediasi, dan beberapa permintaan layanan. AMS Accelerate tidak menyediakan sumber daya di akun atas nama Anda. AMS Accelerate menyediakan bantuan pemecahan masalah untuk masalah infrastruktur yang berdampak pada aplikasi, tetapi AMS Accelerate tidak mengakses atau memvalidasi konfigurasi aplikasi Anda tanpa sepengetahuan dan persetujuan Anda. Layanan dan perubahan AMS Accelerate disediakan langsung di AWS konsol dan APIs, sehingga Anda terus memanfaatkan akun yang ada dengan AWS dan solusi pasar AWS yang tersedia. AMS Accelerate tidak mengubah kode di infrastructure-as-code templat Anda (misalnya, AWS CloudFormation templat), tetapi dapat memandu tim Anda tentang perubahan mana yang diperlukan untuk mengikuti praktik operasional dan keamanan terbaik.

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 konfigurasikan.

- 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 diberitahukan 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 diberitahukan 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 Accelerate adalah rencana operasi layanan AWS Managed Services untuk mengelola operasi AWS infrastruktur Anda.

AWS Managed Services (AMS) AMS Mempercepat fitur rencana operasi

AMS Accelerate menawarkan fitur-fitur berikut:

- Manajemen insiden:

  Manajemen insiden adalah proses yang digunakan layanan AMS untuk menanggapi insiden yang Anda laporkan.

  AMS Accelerate secara proaktif mendeteksi dan menanggapi insiden dan membantu tim Anda dalam menyelesaikan masalah. Anda dapat menghubungi teknisi operasi AMS Accelerate 24x7 AWS menggunakan Support Center, dengan waktu respons SLAs tergantung pada tingkat respons yang Anda pilih untuk akun Anda.
- Monitoring (Pemantauan):

  Pemantauan adalah proses yang digunakan layanan AMS untuk melacak sumber daya Anda.

  Akun yang terdaftar di AMS Accelerate dikonfigurasi dengan penerapan dasar peristiwa CloudWatch Amazon dan alarm yang telah dioptimalkan untuk mengurangi kebisingan dan mengidentifikasi kemungkinan insiden yang akan datang. Setelah menerima peringatan, tim AMS menggunakan remediasi, orang, dan proses otomatis, untuk mengembalikan sumber daya ke keadaan sehat dan terlibat dengan tim Anda bila perlu untuk memberikan wawasan tentang pembelajaran tentang perilaku dan cara mencegahnya. Jika remediasi gagal, AMS memulai proses manajemen insiden. Anda dapat mengubah garis dasar dengan memperbarui file konfigurasi default.
- Keamanan:

  Manajemen keamanan adalah proses yang digunakan layanan AMS untuk melindungi sumber daya Anda. AWS Managed Services melindungi aset informasi Anda dan membantu menjaga infrastruktur AWS Anda tetap aman dengan menggunakan beberapa kontrol, termasuk AWS Config Aturan dan Amazon GuardDuty.

  AMS Accelerate mengelola pustaka Aturan AWS Config dan tindakan remediasi untuk memastikan bahwa semua akun Anda mematuhi standar industri untuk keamanan dan integritas operasional.

Aturan AWS Config terus melacak perubahan konfigurasi di antara sumber daya yang Anda rekam. Jika perubahan melanggar ketentuan aturan apa pun, AMS melaporkan temuannya, dan memungkinkan Anda untuk memulihkan pelanggaran secara otomatis atau berdasarkan permintaan, sesuai dengan tingkat keparahan pelanggaran. Aturan AWS Config memfasilitasi kepatuhan terhadap standar yang ditetapkan oleh: Center for Internet Security (CIS), National Institute of Standards and Technology (NIST) Cloud Security Framework (CSF), Health Insurance Portability and Accountability Act (HIPAA), dan Payment Card Industry (PCI) Standar Keamanan Data (DSS).

Selain itu, AMS Accelerate memanfaatkan Amazon GuardDuty untuk mengidentifikasi aktivitas yang berpotensi tidak sah atau berbahaya di lingkungan AWS Anda. GuardDuty Temuan dipantau 24x7 oleh AMS. AMS bekerja sama dengan Anda untuk memahami dampak dari temuan dan remediasi berdasarkan rekomendasi praktik terbaik. AMS juga mendukung Amazon Macie untuk melindungi data sensitif Anda seperti informasi kesehatan pribadi (PHI), informasi identitas pribadi (PII), dan data keuangan. Terakhir, AMS memantau dan melakukan triase semua peristiwa Amazon Route 53 Resolver ALERT dan BLOCK yang dihasilkan di akun terkelola untuk memeriksa lebih lanjut lalu lintas jaringan dan meningkatkan kemampuan detektifnya.

- Manajemen patch:

  Manajemen patch adalah proses yang digunakan layanan AMS untuk memperbarui sumber daya Anda.

  Untuk AWS akun dengan add-on tambalan, AWS Managed Services menerapkan dan menginstal pembaruan vendor ke EC2 instans Amazon untuk sistem operasi yang didukung selama jendela pemeliharaan yang Anda pilih. AMS membuat snapshot instance sebelum menambal, memantau instalasi patch, dan memberi tahu Anda tentang hasilnya. Jika tambalan gagal, AMS menyelidiki kegagalan dan merekomendasikan tindakan bagi Anda untuk memperbaiki masalah tersebut. Atau, AMS mengembalikan instance ke rollback, jika diminta. AMS menyediakan laporan cakupan kepatuhan patch dan memberi tahu Anda tentang tindakan yang disarankan untuk bisnis Anda.
- Manajemen Backup:

  AMS menggunakan manajemen cadangan untuk mengambil snapshot dari sumber daya Anda.

  AWS Managed Services membuat, memantau, dan menyimpan snapshot untuk AWS layanan yang didukung oleh AWS Backup. Anda menentukan jadwal pencadangan, frekuensi, dan periode retensi dengan membuat AWS Backup rencana saat melakukan orientasi akun dan aplikasi. Anda mengaitkan rencana dengan sumber daya. AMS melacak semua pekerjaan cadangan, dan, ketika pekerjaan cadangan gagal, memberi tahu tim kami untuk menjalankan remediasi. AMS

memanfaatkan snapshot Anda untuk melakukan tindakan restorasi selama insiden, jika diperlukan. AMS memberi Anda laporan cakupan cadangan dan laporan status cadangan.

- 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.

- Pakar yang ditunjuk:

  AMS Accelerate juga menunjuk Cloud Service Delivery Manager (CSDM) dan Cloud Architect (CA) untuk bermitra dengan organisasi Anda dan mendorong keunggulan operasional dan keamanan. CSDM dan CA Anda memberi Anda panduan selama dan setelah konfigurasi dan orientasi AMS Accelerate, menyampaikan laporan bulanan metrik operasional Anda, dan bekerja sama dengan Anda untuk mengidentifikasi potensi penghematan biaya menggunakan alat seperti AWS Cost Explorer, Laporan Biaya dan Penggunaan, dan. Trusted Advisor

- Alat operasi:

  AMS Accelerate dapat menyediakan operasi berkelanjutan untuk infrastruktur beban kerja Anda di AWS. Layanan tambalan, pencadangan, pemantauan, dan manajemen insiden kami bergantung pada tag sumber daya, serta AWS Systems Manager (SSM) serta CloudWatch agen yang diinstal dan dikonfigurasi pada instans Amazon Anda dengan profil EC2 instans IAM yang mengizinkan mereka untuk berinteraksi dengan layanan SSM dan Amazon. CloudWatch AMS Accelerate menyediakan alat seperti Resource Tagger untuk membantu Anda menandai sumber daya berdasarkan aturan, dan konfigurasi instans otomatis untuk menginstal agen yang diperlukan di EC2 instans Amazon Anda. Jika Anda mengikuti praktik infrastruktur yang tidak dapat diubah, Anda dapat menyelesaikan prasyarat langsung di konsol atau templat. infrastructure-as-code

- Optimalisasi biaya:

  Penjadwal Sumber Daya AMS mengotomatiskan memulai dan menghentikan instans Amazon Elastic Compute Cloud (Amazon EC2), instans Amazon Relational Database Service (Amazon RDS), dan grup Amazon Auto Scaling. EC2 Penjadwal Sumber Daya AMS membantu Anda mengurangi biaya operasional dengan menghentikan sumber daya yang tidak digunakan dan memulainya kembali saat kapasitasnya diperlukan.

- Pencatatan dan Pelaporan:

AWS Managed Services mengumpulkan dan menyimpan log yang dihasilkan sebagai hasil operasi di CloudWatch, CloudTrail, dan Amazon VPC Flow Logs. Logging dari AMS membantu dalam resolusi insiden dan audit sistem yang lebih cepat. AMS Accelerate juga 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 ditujukan untuk Anda.

- Manajemen permintaan layanan:

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

Semua pelanggan AMS Accelerate memulai dengan manajemen insiden, pemantauan, pemantauan keamanan, perekaman log, alat prasyarat, manajemen cadangan, dan kemampuan pelaporan. Anda dapat menambahkan add-on manajemen AMS Patch dengan harga tambahan.

> **Note**
>
> Untuk mengetahui daftar fitur yang tidak didukung AWS GovCloud (US), lihat Perbedaan AMS Accelerate AWS GovCloud (US)

Konfigurasi yang didukung

AMS Accelerate mendukung konfigurasi berikut:

- Bahasa: Inggris.
- Wilayah: Lihat AWS Wilayah yang didukung AWS Managed Services di halaman web Layanan AWS Regional.

  > **Note**
  >
  > Wilayah AWS yang diperkenalkan sebelum 20 Maret 2019 dianggap sebagai Wilayah “Asli” dan diaktifkan secara default. Wilayah yang diperkenalkan setelah tanggal ini adalah

Wilayah “Keikutsertaan” dan dinonaktifkan secara default. Jika akun Anda menggunakan beberapa Wilayah dan Anda mengaktifkan AMS Accelerate ke akun dengan Wilayah “Keikutsertaan” yang diaktifkan sebagai Wilayah default, fitur Pelaporan AMS hanya tersedia di Wilayah tersebut. Jika Anda tidak menetapkan Region default, Region terakhir yang Anda kunjungi adalah Region default Anda.
Untuk mengaktifkan Region, lihat Mengaktifkan Region. Untuk menyetel Wilayah default, lihat Memilih Wilayah. Untuk daftar status Keikutsertaan untuk setiap Wilayah, lihat Wilayah yang Tersedia di Panduan Pengguna Amazon Elastic Compute Cloud.

- Arsitektur sistem operasi (x86-64 atau ARM64): apa pun yang didukung oleh Systems Manager dan. CloudWatch
- Sistem operasi yang didukung:
  - AlmaLinux 8.3-8.9, 9.x (hanya didukung dengan AlmaLinux arsitektur x86)
  - 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 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 EOS OS mengikuti kontrol keamanan seperti yang ditentukan oleh AMS dalam Panduan Pengguna Akselerasi, atau
> 3. Anda mematuhi kontrol keamanan kompensasi lainnya yang diwajibkan oleh AMS.

Jika AMS tidak lagi dapat mendukung EOS OS, AMS mengeluarkan Rekomendasi Kritis untuk meningkatkan sistem operasi.
Agen 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

- Jika Anda menggunakannya AWS Control Tower untuk mengelola lingkungan multi-akun, pastikan Anda menjalankan versi terbaru AWS Control Tower untuk kompatibilitas dengan Accelerate. Lingkungan yang menggunakan AWS Control Tower versi lebih awal dari 2.7 (dirilis pada April 2021), tidak didukung. Untuk informasi tentang cara memperbarui AWS Control Tower, lihat Memperbarui Zona Pendaratan Anda.

Layanan yang didukung

AWS Managed Services menyediakan layanan dukungan manajemen operasional untuk AWS layanan berikut. Setiap AWS layanan berbeda dan sebagai hasilnya, tingkat dukungan manajemen operasional AMS bervariasi tergantung pada sifat dan karakteristik AWS layanan yang mendasarinya. Jika Anda meminta AWS Managed Services menyediakan layanan untuk perangkat lunak atau layanan apa pun yang tidak secara tegas diidentifikasi sebagai didukung dalam daftar berikut, AWS Managed Services yang disediakan untuk konfigurasi yang diminta pelanggan tersebut akan diperlakukan sebagai “Layanan Beta” berdasarkan Ketentuan Layanan.

- Insiden: Semua layanan AWS
- Permintaan layanan: Semua AWS layanan
- Penambalan: Amazon EC2

- Backup dan Restorasi: Semua Layanan AWS didukung oleh. AWS Backup Untuk daftar layanan yang didukung oleh AWS Backup, lihat sumber daya AWS Backup yang didukung.
- Penjadwal Sumber Daya: Instans Amazon Elastic Compute Cloud EC2 (Amazon), Amazon Relational Database Service (Amazon RDS), dan grup Amazon Auto Scaling EC2
- Layanan yang dipantau untuk acara operasional: Pemeriksaan yang didukung dan Trusted Advisor, Application Load Balancer, Aurora, Amazon, Elastic EC2 Load Balancing, Amazon FSx untuk NetApp ONTAP, FSx Amazon untuk Windows File Server, gateway NAT (layanan Terjemahan Alamat Jaringan (NAT)),,, AWS Health Dashboard Amazon Redshift OpenSearch, Amazon Relational Database Service (Amazon RDS), VPN. Site-to-Site Untuk mempelajari selengkapnya tentang pemantauan AMS Accelerate sebagai bagian dari layanan, lihat Peringatan dari pemantauan dasar di AMS.
- Layanan yang dipantau oleh Aturan Konfigurasi keamanan AWS : Akun GuardDuty,, Macie, Amazon API Gateway,,,,,, Amazon DynamoDB AWS Certificate Manager AWS Config CloudTrail, Amazon CloudWatch, AWS Database Migration Service Amazon AWS CodeBuild, Amazon, Amazon Elastic Block Store (EC2Amazon EBS), ElastiCache Amazon Elastic File System (Amazon EFS), Amazon Elastic File System (Amazon EFS), Amazon Elastic Kunetes Service (Amazon EKS), Elastic Load Balancing, Layanan Amazon, Amazon EMR, (IAM),,, OpenSearch Amazon Redshift, Layanan Database Relasional Amazon AWS Identity and Access Management , Amazon S3, AWS Lambda Amazon AWS Key Management Service AI,, SageMaker AWS Secrets Manager Layanan Pemberitahuan Sederhana Amazon AWS Systems Manager,, Amazon VPC (Grup keamanan, volume, alamat IP elastis, koneksi VPN, gateway Internet), Log Aliran VPC Amazon. Untuk lebih jelasnya, lihat Kepatuhan konfigurasi di Accelerate danPerlindungan data di Accelerate. Anda dapat menemukan informasi keamanan AMS tambahan di Panduan Keamanan pribadi kami yang dapat diakses melalui AWS Artifact, pada tab Laporan, untuk AWS Managed Services.

> **Note**
>
> AMS Accelerate for the Middle East (UEA) Region mendukung serangkaian fitur dalam lingkup seperti yang dijelaskan dalam tabel berikut. Akses ke konsol akun AMS dan instans di Wilayah ini didorong secara eksklusif oleh pemicu permintaan layanan masuk. Untuk informasi lebih lanjut tentang ketersediaan Accelerate in the Middle East (UEA) Region, konsultasikan dengan manajer akun Anda atau AWS Cloud Service Delivery Manager (CSDM).

AMS Mempercepat fitur dalam cakupan untuk Wilayah Timur Tengah (UEA)	Deskripsi fitur
Manajemen Insiden	AMS memberikan respons insiden dan bantuan untuk membantu tim Anda menyelesaikan masalah. Agar AMS dapat membantu Anda dalam manajemen insiden, Anda harus mengirimkan permintaan layanan. AMS tidak secara proaktif mendeteksi atau menanggapi insiden di Wilayah ini.
Pemantauan	Setelah menerima permintaan layanan dari Anda, AMS dapat membantu perbaikan sumber daya. AMS menggunakan remediasi otomatis, orang, dan proses untuk mengembalikan sumber daya Anda ke keadaan sehat. AMS tidak mengonfigurasi CloudWatch peristiwa dasar dan alarm di Wilayah ini. Jika Anda memiliki alat pemantauan yang ada, pelacakan proaktif sumber daya Anda mungkin tersedia berdasarkan penilaian Cloud Architect (CA) dan CSDM.
Keamanan	Setelah menerima permintaan layanan dari Anda, AMS dapat membantu perbaikan masalah keamanan. AMS tidak menerapka n kontrol keamanan seperti Aturan AWS Config dan GuardDuty atau memantau temuan keamanan di Wilayah ini. Jika Anda memiliki alat keamanan yang ada, pemantauan keamanan proaktif mungkin tersedia berdasark an penilaian CA dan CSDM.
Manajemen Patch	AMS dapat menerapkan pembaruan vendor ke EC2 instans Amazon untuk sistem operasi yang didukung selama jendela pemelihar aan yang dipilih, dan membuat snapshot pra-

AMS Mempercepat fitur dalam cakupan untuk Wilayah Timur Tengah (UEA)	Deskripsi fitur
	penambalan. Agar AMS dapat membantu Anda dengan manajemen tambalan, Anda harus mengirimkan permintaan layanan. Pemberita huan dan laporan tambalan AMS tidak tersedia di Wilayah ini.
Manajemen Backup	AMS dapat membuat dan menyimpan snapshot untuk Layanan AWS didukung oleh AWS Backup, dan membantu perbaikan cadangan. Agar AMS dapat membantu Anda dengan manajemen cadangan, Anda harus mengirimk an permintaan layanan. AMS tidak melacak pekerjaan cadangan di Wilayah ini.
Pakar yang Ditunjuk	AMS menunjuk Cloud Architect (CA) dan Cloud Service Delivery Manager (CSDM) untuk bermitra dengan organisasi pelanggan dan mendorong keunggulan operasional dan keamanan.
Manajemen Permintaan Layanan	Untuk meminta informasi tentang lingkungan terkelola, AMS, atau Layanan AWS penawaran Anda, kirimkan permintaan layanan melalui konsol AMS Accelerate. Anda dapat mengirimk an permintaan layanan untuk pertanyaan “Bagaimana” tentang Layanan AWS dan fitur, atau untuk meminta layanan AMS yang tersedia di Wilayah ini, seperti yang dijelaskan dalam tabel ini.

Peran dan tanggung jawab

Matriks AMS Accelerate yang bertanggung jawab, akuntabel, berkonsultasi, dan diinformasikan, atau RACI, memberikan tanggung jawab utama baik kepada pelanggan atau AMS untuk berbagai

kegiatan. Tabel menjelaskan tanggung jawab Anda (“Pelanggan”) versus tanggung jawab (“AMS Accelerate”) kami.

Lingkup perubahan yang dilakukan oleh AMS AccelerateBagian ini mencantumkan keadaan spesifik saat AMS diberi wewenang untuk membuat perubahan pada akun Anda; dan beberapa jenis perubahan yang tidak pernah dilakukan AMS.

AMS Mempercepat Matriks RACI

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

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

> **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.

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Pola AMS		
Buat pola baru	I	R
Menyebarkan dan menyesuaikan pola	R	C, I

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Uji dan hapus pola	R	I
Siklus hidup aplikasi		
Pengembangan aplikasi	R	I
Persyaratan, analisis, dan desain infrastruktur aplikasi	R	I
Deployment aplikasi	R	I
Penerapan sumber daya AWS	R	I
Pemantauan aplikasi	R	I
Pengujian/pengoptimalan aplikasi	R	I
Memecahkan masalah dan menyelesaikan masalah aplikasi	R	I
Memecahkan masalah dan menyelesaikan masalah	R	I
Pemantauan didukung untuk infrastruktur AWS	C	R
Respons insiden untuk masalah jaringan AWS	C	R
Respons insiden untuk masalah sumber daya AWS	C	R
Orientasi Akun Terkelola		
Berikan akses ke AWS Managed Account untuk tim dan alat AMS	R	C
Menerapkan perubahan dalam akun atau lingkungan untuk memungkin kan penyebaran alat di akun. Misalnya, perubahan Kebijakan Kontrol Layanan (SCPs)	R	C
Instal agen SSM dalam contoh EC2	R	C

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Instal dan konfigurasikan perkakas yang diperlukan untuk menyediakan layanan AMS. Misalnya, CloudWatch agen, skrip untuk patching, alarm, log, dan lainnya	I	R
Mengelola akses dan siklus hidup identitas untuk teknisi AMS	I	R
Kumpulkan semua input yang diperlukan untuk mengonfigurasi layanan AMS. Misalnya, durasi, jadwal, dan target jendela pemeliharaan patch	R	I
Minta konfigurasi layanan AMS dan berikan semua input yang diperlukan	R	I
Konfigurasikan layanan AMS seperti yang diminta oleh pelanggan. Misalnya, jendela pemeliharaan tambalan, tagger sumber daya, dan manajer alarm	C	R
Mengelola siklus hidup pengguna dan izin mereka, untuk layanan direktori lokal, yang digunakan untuk mengakses akun dan instans AWS	R	I
Merekomendasikan pengoptimalan instance cadangan	I	R
Akun onboard ke Remediator Tepercaya	C, I	R
Manajemen tambalan		
Kumpulkan semua input yang diperlukan untuk mengonfigurasi jendela pemeliharaan tambalan, garis dasar tambalan, dan target	R	I
Minta konfigurasi jendela pemeliharaan patch dan baseline, dan berikan semua input yang diperlukan	R	I
Konfigurasikan jendela pemeliharaan tambalan, garis dasar tambalan, dan target seperti yang diminta oleh pelanggan	C	R

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Pantau pembaruan yang berlaku untuk OS dan perangkat lunak yang didukung yang telah diinstal sebelumnya dengan OS yang didukung untuk EC2 instans	I	R
Laporkan pembaruan yang hilang ke OS yang didukung dan cakupan jendela pemeliharaan	I	R
Ambil snapshot dari instance sebelum menerapkan pembaruan	I	R
Terapkan pembaruan ke EC2 instance per konfigurasi pelanggan	I	R
Selidiki pembaruan yang gagal ke EC2 instance	C	R
Pembaruan AMIs dan tumpukan untuk grup Penskalaan Otomatis () ASGs	R	C
Patch sistem operasi Windows, dan paket Microsoft diinstal pada sistem operasi yang diatur oleh Windows Update	I	R
Patch aplikasi, perangkat lunak, atau dependensi aplikasi yang diinstal tidak dikelola oleh Pembaruan Windows	R	I
Patch sistem operasi Linux dan paket apa pun yang diaktifkan untuk manajemen oleh manajer paket asli sistem operasi (misalnya Yum, Apt, Zypper)	I	R
Patch aplikasi, perangkat lunak, atau dependensi aplikasi yang diinstal tidak dikelola oleh manajer paket asli sistem operasi Linux	R	I
Cadangan		
Kumpulkan semua input yang diperlukan untuk mengonfigurasi rencana cadangan dan sumber daya target	R	I
Minta konfigurasi paket Backup dan berikan semua input yang diperlukan	R	I

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Konfigurasikan rencana dan target cadangan seperti yang diminta oleh pelanggan	C	R
Tentukan jadwal cadangan dan sumber daya target	R	I
Lakukan backup per paket	I	R
Selidiki pekerjaan pencadangan yang gagal	I	R
Laporkan status pekerjaan cadangan dan cakupan cadangan	I	R
Validasi cadangan	R	I
Meminta pemulihan cadangan untuk sumber daya sumber daya layanan AWS yang didukung sebagai bagian dari manajemen insiden	R	I
Melakukan aktivitas restorasi cadangan untuk sumber daya layanan AWS yang didukung	I	R
Kembalikan aplikasi kustom atau pihak ketiga yang terpengaruh	R	I
Jaringan		
Penyediaan dan konfigurasi Akun Terkelola VPCs,, IGWs Koneksi langsung, dan Layanan jaringan AWS lainnya	R	I
Mengonfigurasi dan mengoperasikan AWS Security Groups/NAT/NACL di dalam akun Terkelola	R	I
Konfigurasi dan implementasi jaringan dalam jaringan pelanggan (misalnya DirectConnect)	R	I
Konfigurasi dan implementasi jaringan dalam jaringan AWS	R	I

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Monitor yang ditentukan oleh AMS untuk keamanan jaringan, termasuk grup keamanan	I	R
Konfigurasi dan manajemen logging tingkat jaringan (log aliran VPC dan lainnya)	I	R
Pencatatan		
Rekam semua log perubahan aplikasi	R	I
Rekam log perubahan infrastruktur AWS	I	R
Mengaktifkan dan menggabungkan jejak audit AWS	I	R
Log agregat dari sumber daya AWS	I	R
Pemantauan dan Remediasi		
Kumpulkan semua input yang diperlukan untuk mengonfigurasi manajer alarm, tagger sumber daya, dan ambang batas alarm	R	I
Minta konfigurasi manajer alarm dan berikan semua input yang diperlukan	R	I
Konfigurasikan manajer alarm, tagger sumber daya, dan ambang alarm seperti yang diminta oleh pelanggan.	C	R
Menerapkan metrik dan CloudWatch alarm dasar AMS per konfigurasi pelanggan	I	R
Pantau sumber daya AWS yang didukung menggunakan CloudWatch metrik dasar dan alarm	I	R
Selidiki peringatan dari sumber daya AWS	C	R

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Memulihkan peringatan berdasarkan konfigurasi yang ditentukan, atau buat insiden	I	R
Tentukan, pantau, dan selidiki monitor khusus pelanggan	R	I
Selidiki peringatan dari pemantauan aplikasi	R	C
Konfigurasikan Trusted Advisor cek untuk remediasi	R	C
Secara otomatis memulihkan pemeriksaan yang didukung Trusted Advisor	I	R
Memulihkan pemeriksaan yang didukung Trusted Advisor secara manual	R	C
Laporkan status remediasi	I	R
Memecahkan masalah kegagalan remediasi	R	C
Arsitektur Keamanan		
Tinjau sumber daya dan kode AMS untuk masalah keamanan dan potensi ancaman	I	R
Menerapkan kontrol keamanan dalam sumber daya dan kode AMS untuk mengurangi risiko keamanan	I	R
Aktifkan layanan AWS yang didukung untuk manajemen keamanan akun dan sumber daya AWS	I	R
Kelola kredensi istimewa untuk akses akun dan OS untuk teknisi AMS	I	R
Manajemen Risiko Keamanan		
Memantau layanan AWS yang didukung untuk manajemen keamanan, seperti GuardDuty dan Macie	I	R

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Tentukan dan buat Aturan Konfigurasi yang ditentukan AMS untuk mendeteksi apakah sumber daya AWS mematuhi praktik terbaik keamanan Center for Internet Security (CIS) dan NIST.	I	R
Pantau Aturan Konfigurasi yang Ditentukan AMS	I	R
Laporkan status kesesuaian Aturan Config	I	R
Tentukan daftar Aturan Config yang diperlukan dan perbaiki	I	R
Mengevaluasi dampak remediasi Aturan Config yang ditentukan AMS	R	I
Meminta perbaikan Aturan Konfigurasi yang ditentukan AMS di akun AWS	R	I
Lacak sumber daya yang dikecualikan dari Aturan Config yang ditentuka n AMS	R	I
Memulihkan Aturan Konfigurasi yang ditentukan AMS yang didukung di akun AWS	C	R
Memulihkan Aturan Konfigurasi yang ditentukan AMS yang tidak didukung di akun AWS	R	I
Tentukan, pantau, dan selidiki Aturan Konfigurasi khusus pelanggan	R	I
Manajemen Insiden		
Beri tahu tentang insiden yang terdeteksi oleh AMS di sumber daya AWS	I	R
Beri tahu tentang insiden di sumber daya AWS	R	I
Memberitahu tentang insiden untuk AWS sumber daya berdasarkan pemantauan	I	R

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Menangani masalah kinerja aplikasi dan pemadaman	R	I
Kategorikan prioritas insiden	I	R
Berikan respons insiden	I	R
Menyediakan resolusi insiden atau pemulihan infrastruktur untuk sumber daya dengan cadangan yang tersedia	C	R
Respon Insiden Keamanan - Mempersiapkan		
Komunikasi		
Menyediakan dan memperbarui 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	C	R
Pelatihan		
Memberikan dokumentasi kepada pelanggan untuk mendukung AMS selama proses respons insiden	I	R
Berlatih tanggung jawab bersama selama proses respons insiden melalui permainan keamanan	R	R
Manajemen sumber daya		
Konfigurasikan manajemen keamanan yang didukung Layanan AWS untuk peringatan, korelasi peringatan, pengurangan kebisingan, dan aturan tambahan	I	R

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Pertahankan inventaris sumber AWS daya yang komprehensif (Amazon EC2, Amazon S3, dll.), Termasuk detail tentang nilai dan kekritisan setiap aset untuk bisnis. Informasi ini akan berperan penting dalam menentukan strategi penahanan yang efektif	R	C
Gunakan AWS tag untuk mengidentifikasi sumber daya dan beban kerja	R	C
Menentukan dan mengkonfigurasi penyimpanan log dan arsip	I	R
Menetapkan garis dasar yang aman dengan mendefinisikan dan menegakkan kebijakan dan konfigurasi keamanan organisasi untuk AWS akun, layanan, dan manajemen akses	R	I
Respon Insiden Keamanan - Deteksi		
Pencatatan, indikator, dan pemantauan		
Konfigurasikan pencatatan dan pemantauan untuk mengaktifkan manajemen acara misalnya dan akun	I	R
Monitor didukung Layanan AWS untuk peringatan keamanan	I	R
Menyebarkan dan mengelola alat keamanan titik akhir	R	I
Memantau malware pada instance menggunakan keamanan endpoint	R	I
Beri tahu pelanggan tentang kejadian yang terdeteksi melalui pesan keluar	I	R
Mengkoordinasikan komunikasi pemangku kepentingan internal dan pembaruan kepemimpinan untuk meningkatkan waktu respons	R	I
Menentukan, menerapkan, dan memelihara layanan deteksi standar AMS (misalnya, Amazon GuardDuty dan AWS Config)	C	R

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Rekam log perubahan AWS infrastruktur	R	I
Aktifkan dan konfigurasikan 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	R	R
Pelaporan acara keamanan		
Beri tahu AMS tentang aktivitas mencurigakan atau investigasi keamanan aktif	R	I
Beri tahu kejadian dan insiden keamanan yang terdeteksi kepada pelanggan	I	R
Beri tahu peristiwa yang direncanakan yang dapat memicu proses Respons Insiden Keamanan	R	I
Respon Insiden Keamanan - Analisis		
Investigasi dan analisis		
Lakukan respons awal untuk peringatan keamanan yang didukung yang dihasilkan oleh sumber deteksi yang didukung	I	R
Menilai false/true positif menggunakan data yang tersedia	R	R
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	C

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Kumpulkan log aplikasi untuk membantu penyelidikan	R	I
Kumpulkan data dan log untuk membantu investigasi peringatan keamanan	R	R
Terlibat SMEs dalam Layanan AWS investigasi keamanan	C	R
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		
Menilai risiko dan memutuskan strategi penahanan, mengakui potensi dampak layanan	R	C
Buat cadangan sistem yang terpengaruh untuk analisis lebih lanjut	I	R
Berisi aplikasi dan beban kerja (melalui konfigurasi spesifik aplikasi atau aktivitas respons)	R	C
Tentukan strategi penahanan berdasarkan insiden keamanan dan sumber daya yang terpengaruh	I	R

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

Aktivitas	Pelanggan	AWS Managed Services (AMS)
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-l angkah 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 Masalah		
Korelasikan insiden untuk mengidentifikasi masalah	I	R
Lakukan analisis akar penyebab (RCA) untuk masalah	I	R
Memperbaiki masalah	I	R
Identifikasi dan atasi masalah aplikasi	R	I
Manajemen Layanan		
Meminta informasi menggunakan permintaan layanan	R	I
Balas permintaan layanan	I	R
Memberikan rekomendasi pengoptimalan biaya	I	R
Mempersiapkan dan menyampaikan laporan layanan bulanan	I	R

Aktivitas	Pelanggan	AWS Managed Services (AMS)
Manajemen Perubahan		
Mengubah proses manajemen dan perkakas untuk penyediaan dan pemutakhiran sumber daya di lingkungan terkelola	R	I
Pemeliharaan kalender perubahan aplikasi	R	I
Pemberitahuan Jendela pemeliharaan yang akan datang	R	I
Catat perubahan yang dibuat oleh Operasi AMS	I	R
Optimalisasi Biaya		
Kumpulkan semua input yang diperlukan untuk mengonfigurasi Resource Scheduler	R	I
Minta orientasi, konfigurasi Resource Scheduler dan berikan semua input yang diperlukan	R	I
Menerapkan Resource Scheduler per konfigurasi pelanggan	C, I	R
Nonaktifkan dan aktifkan Resource Scheduler di akun pelanggan	R	C
Membuat, menghapus, menjelaskan, dan memperbarui jadwal	C	R
Membuat, menghapus, menjelaskan, dan memperbarui periode	C	R
Selidiki dan pecahkan masalah dengan Resource Scheduler	I	R
Permintaan untuk offboarding Resource Scheduler	R	I
Offboard Resource Scheduler dari akun	C, I	R

Lingkup perubahan yang dilakukan oleh AMS Accelerate

AMS Accelerate hanya membuat perubahan untuk tujuan dan situasi tertentu yang dijelaskan selanjutnya. AMS membuat perubahan hanya pada tingkat infrastruktur, menggunakan konsol atau APIs. AMS tidak pernah mengubah lapisan aplikasi, kontrol, atau domain Anda. Anda dapat melihat perubahan apa pun yang dibuat oleh AMS (atau pengguna lain) menggunakan kumpulan kueri bawaan kami; untuk melakukannya, lihat. Melacak perubahan di akun AMS Accelerate

AWS sumber daya

AMS Accelerate menyebarkan atau memperbarui AWS sumber daya hanya dalam situasi berikut:

- Untuk menyebarkan dan memperbarui alat dan sumber daya yang dibutuhkan oleh AMS.
- Sebagai bagian dari pemantauan AMS, dalam menanggapi peristiwa dan alarm.
- Untuk memulihkan masalah keamanan sebagai bagian dari Tanggapan terhadap pelanggaran di Accelerate (membuat sumber daya yang tidak patuh sesuai dengan praktik terbaik keamanan).
- Selama remediasi dan restorasi sebagai bagian dari respons insiden.
- Saat menanggapi permintaan pelanggan untuk mengonfigurasi fitur AMS, seperti berikut ini:
  - Manajer alarm
  - Tagger sumber daya
  - Patch baseline dan jendela pemeliharaan
  - Penjadwal sumber daya
  - Rencana pencadangan

AMS Accelerate tidak menyebarkan atau memperbarui sumber daya di luar situasi ini. Jika Anda memerlukan bantuan dari AMS untuk membuat perubahan dalam situasi lain, pertimbangkan untuk menggunakan Operations on Demand.

Perangkat lunak sistem operasi

AMS Accelerate dapat membuat perubahan pada perangkat lunak sistem operasi Anda selama situasi tidak tersedianya melalui penyelesaian insiden sebagaimana didefinisikan dalam Perjanjian Tingkat Layanan kami. AMS juga dapat membuat perubahan pada sistem operasi Anda sebagai bagian dariKonfigurasi instans otomatis di AMS Accelerate.

Kode dan konfigurasi aplikasi

AMS Accelerate tidak pernah mengubah kode Anda (misalnya, CloudFormation templat AWS, infrastructure-as-code templat lain, atau fungsi Lambda), tetapi dapat memandu tim Anda tentang perubahan mana yang diperlukan untuk mengikuti praktik operasional dan keamanan terbaik. AMS Accelerate menyediakan bantuan pemecahan masalah untuk masalah infrastruktur yang berdampak pada aplikasi, tetapi AMS Accelerate tidak mengakses atau memvalidasi konfigurasi aplikasi Anda.

Kemampuan untuk sistem operasi yang tidak didukung di Accelerate

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.
Manajemen permintaan layanan	AMS menanggapi permintaan layanan.
Pemantauan	AMS memantau dan merespons pemeriksaan status EC2 sistem Amazon dan pemeriksaan status instans. Pemeriksaan status sistem meliputi: hilangnya konektivi tas 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 dan AWS Config aturan Amazon.

Kemampuan	Catatan
Manajemen Backup	AMS menyediakan manajemen Kontinuitas di Accelerate untuk EC2 menggunakan AWS Backup paket dan brankas yang disesuaikan AMS.

Kontak dan eskalasi

Anda memiliki manajer pengiriman layanan cloud (CSDM) yang ditunjuk yang memberikan bantuan konsultasi di seluruh AMS Accelerate, 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 Accelerate.
- Menanggapi dan menyelesaikan permintaan pelaporan penagihan dan layanan.
- Memberikan wawasan untuk rekomendasi optimalisasi keuangan dan kapasitas.

Jam kontak

Anda dapat menghubungi AMS Accelerate untuk alasan yang berbeda pada waktu yang berbeda.

Fitur	AMS Accelerate
	Tingkat Premium
Permintaan layanan	24/7
Manajemen insiden (P2-P3)	24/7
Pencadangan dan pemulihan	24/7

Fitur	AMS Accelerate
	Tingkat Premium
Manajemen tambalan	24/7
Pemantauan dan peringatan	24/7
Manajer pengiriman layanan cloud (CSDM)	Senin sampai Jumat: 08:00 — 17:00, jam kerja lokal

Jam kerja

Fitur	AMS Accelerate
	Tingkat Premium
Permintaan layanan	24/7
Manajemen insiden (P1)	24/7
Manajemen insiden (P2-P3)	24/7
Pencadangan dan pemulihan	24/7
Manajemen tambalan	24/7
Pemantauan dan peringatan	24/7
Manajer pengiriman layanan cloud (CSDM)	Senin sampai Jumat: 09:00 — 17:00, jam kerja lokal

Jalur eskalasi

AMS mendukung pelanggan dengan Manajemen Insiden dan Manajemen Permintaan Layanan, 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 kasus Insiden. Lihat perinciannya di Mengirimkan insiden untuk Accelerate. Untuk informasi umum tentang manajemen insiden AMS, lihatManajemen insiden di AMS Accelerate.

Untuk meminta informasi atau saran, atau meminta layanan tambahan dari AMS, gunakan konsol AMS dan kirimkan permintaan layanan. Lihat perinciannya di Membuat permintaan layanan di Accelerate. Untuk informasi umum tentang permintaan layanan AMS, lihatManajemen permintaan layanan di Accelerate.

Persediaan sumber daya untuk Accelerate

Semua sumber daya yang digunakan AMS Accelerate ke akun Akun AWS atau Anda tercantum dalam spreadsheet `resource_inventory.zip`file resource_inventory.xlsx (terkompresi).

> **Note**
>
> Di kolom Nama Sumber Daya, awalan CFN: menunjukkan ID CloudFormation logis, bukan nama sumber daya. Ini ditampilkan untuk sumber daya yang tidak disebutkan namanya, misalnya, untuk kebijakan bucket S3.

AMS menyebarkan serangkaian layanan seperti yang dijelaskan dalam. Deskripsi layanan Biaya untuk menerapkannya rendah ketika digunakan ke akun kosong, tetapi biaya meningkat seiring dengan meningkatnya pemanfaatan. Misalnya, log dibuat dan aturan konfigurasi dipanggil saat sumber daya berubah.

Ketika beberapa perubahan dilakukan pada aturan konfigurasi, beberapa pemanggilan kepatuhan konfigurasi dapat dipicu, yang mengarah ke biaya yang lebih tinggi. Kemungkinan yang sama berlaku untuk Amazon yang CloudWatch digunakan untuk memantau instans — semakin terperinci pemantauan Anda, semakin tinggi biaya layanan. AWS Backup adalah contoh lain. Jika Anda memiliki beberapa cadangan yang disimpan, atau jika Anda memiliki periode retensi yang lebih tinggi, Anda menggunakan lebih banyak penyimpanan dan biayanya lebih tinggi.

Angka-angka ini sulit diprediksi. Selama tinjauan bisnis bulanan Anda dengan manajer pengiriman layanan cloud (CSDM) Anda, lacak perubahan dan bekerja untuk mengidentifikasi area peluang untuk pengurangan biaya.

Memulai dengan AMS Accelerate

Jika AWS Managed Services (AMS) belum mengoperasikan akun, mulailah dengan menghubungi perwakilan penjualan Amazon Web Services (AWS) menggunakan halaman AWS Managed Services - Contact Sales kami.

Setelah Anda mendaftar untuk AMS, tim AMS Accelerate memandu Anda melalui proses orientasi berikut untuk masing-masing anggota Anda Akun AWS.

Tinjau set fitur di sini: Fitur AWS Managed Services

> **Note**
>
> AMS Accelerate mendukung GovCloud Wilayah. Jika layanan Anda akan berada di sebuah AWS GovCloud (US) Region, lihat juga Memulai dengan AWS GovCloud (US).

Proses orientasi akun untuk Accelerate

Memasukkan akun ke AMS Accelerate memiliki empat tahap.

1. Langkah 1. Penemuan akun di Acceleratemenilai status akun Anda saat ini dan mengidentifikasi pemblokir teknis untuk orientasi akun Anda.
2. Langkah 2. Sumber daya manajemen orientasi di Acceleratememinta Anda untuk menerima syarat dan ketentuan; dan membuat peran orientasi untuk arsitek cloud AMS Accelerate (CAs), yang akan membantu Anda menetapkan garis dasar keamanan, dan menyelesaikan masalah sesuai kebutuhan.
3. Langkah 3. Fitur AMS orientasi dengan kebijakan defaultuntuk Mempercepat fitur, seperti pemantauan, penambalan, dan pencadangan.
4. Langkah 4. Sesuaikan fitur di Acceleratememastikan bahwa sumber daya, termasuk EC2 instance, dikonfigurasi dengan benar untuk aplikasi Anda.

Mempercepat prasyarat orientasi

Sebelum Anda memulai proses orientasi, penting untuk memahami dependensi teknis yang diandalkan komponen Accelerate.

> **Note**
>
> Untuk menggunakan AMS Accelerate, Anda harus menggunakan salah satu dari dua Dukungan paket yang didukung: Enterprise On-Ramp atau Enterprise. Paket Pengembang dan Bisnis tidak memenuhi syarat untuk memenuhi syarat untuk AMS Accelerate. Untuk mempelajari lebih lanjut tentang berbagai paket, lihat Bandingkan Dukungan Paket.

AMS Mempercepat titik akhir VPC

Titik akhir VPC memungkinkan koneksi pribadi antara VPC Anda AWS dan layanan yang didukung serta layanan titik akhir VPC yang didukung oleh. AWS Jika Anda perlu memfilter konektivitas internet keluar, konfigurasikan titik akhir layanan VPC berikut untuk memastikan bahwa AMS Accelerate memiliki konektivitas dengan dependensi layanannya.

> **Note**
>
> Dalam daftar berikut, *region* mewakili pengenal untuk AWS Wilayah, misalnya `us-east-2` untuk Wilayah AS Timur (Ohio).

```
com.amazonaws.region.logs
com.amazonaws.region.monitoring
com.amazonaws.region.ec2
com.amazonaws.region.ec2messages
com.amazonaws.region.ssm
com.amazonaws.region.ssmmessages
com.amazonaws.region.s3
com.amazonaws.region.events
```

Untuk informasi tentang cara mengonfigurasi titik akhir AWS VPC, lihat titik akhir VPC.

> **Note**
>
> Jika Anda membuat titik akhir VPC di akun Anda untuk semua layanan yang disebutkan di atas, lihat contoh template ini. AWS CloudFormation Anda dapat memperbarui template ini dan menghapus atau menambahkan definisi titik akhir VPC sesuai kasus penggunaan Anda.

Konektivitas internet outbound di Accelerate

1. Unduh egressMgmt.zip.
2. Buka file **ams-egress.json**.
3. Temukan di URLs bawah properti JSON:
   - `WindowsPatching`
   - `RedHatPatching`
   - `AmazonLinuxPatching`
   - `EPELRepository`
4. Izinkan akses ke ini URLs.

Menguji konektivitas keluar di Accelerate

Uji konektivitas keluar menggunakan salah satu metode berikut.

> **Note**
>
> Sebelum menjalankan skrip/perintah, ganti merah *region* dengan pengenal Wilayah Anda, misalnya,. `us-east-1`

PowerShell Skrip Windows

```
$region = 'region'
@('logs','monitoring','ec2','ec2messages','ssm','ssmmessages','s3','events') | `
ForEach-Object { `
Test-NetConnection ("$_" + '.' + "$region" + '.amazonaws.com') -Port 443 } | `
Format-Table ComputerName,RemotePort,RemoteAddress,PingSucceeded,TcpTestSucceeded -
AutoSize
```

Perintah Linux

```
for endpoint in logs monitoring ec2 ec2messages ssm ssmmessages s3 events; do nc -zv
 $endpoint.region.amazonaws.com 443; done
```

Amazon EC2 Systems Manager di Accelerate

Anda harus menginstal AWS Systems Manager Agen (Agen SSM) pada semua EC2 instance yang Anda ingin AMS kelola. Anda juga perlu menambahkan izin bucket yang dibutuhkan Agen SSM. Untuk ikhtisar yang mencakup Amazon EC2, lihatLangkah 3. Fitur AMS orientasi dengan kebijakan default.

IAM dalam Mempercepat

Untuk memungkinkan pengguna membaca dan mengonfigurasi kemampuan AMS Accelerate, seperti mengakses konsol AMS atau mengonfigurasi cadangan, Anda harus memberikan izin eksplisit di AWS Identity and Access Management (IAM) untuk melakukan tindakan tersebut. Misalnya kebijakan IAM, lihat Izin untuk menggunakan fitur AMS.

Langkah 1. Penemuan akun di Accelerate

AMS bekerja dengan Anda selama penemuan akun untuk menilai status akun Anda saat ini, dan mengidentifikasi pemblokir teknis untuk orientasi akun Anda. AMS tidak menyediakan layanan operasional selama tahap penemuan akun. AMS menggunakan peran `AWSServiceRoleForSupport` terkait layanan untuk mengidentifikasi pemblokir teknis, dan kemudian bekerja sama dengan Anda untuk memulihkannya, sebelum pindah ke tahap orientasi Tingkat Akun.

Proses penemuan akun di Accelerate

Untuk membantu analisis dan penemuan akun Anda, AMS melakukan pemeriksaan operasional untuk mengidentifikasi pemblokir teknis melalui panggilan API hanya-baca. Setelah akun Anda terhubung ke AMS, pemeriksaan ini dilakukan berdasarkan permintaan untuk mempertahankan postur akun. AMS bekerja sama dengan Anda untuk memulihkan temuan apa pun yang terkait dengan pemeriksaan ini bila diperlukan. AMS menggunakan pemeriksaan operasional berikut dan tindakan API hanya-baca sebagai bagian dari Penemuan Akun:

Pemeriksaan Operasional	Tujuan	AWS Panggilan API Digunakan
AWS Control Tower Evaluasi Versi	Mengidentifikasi AWS Control Tower versi untuk memastikan bahwa itu adalah versi	• `ControlTower:GetLandingZone`

Pemeriksaan Operasional	Tujuan	AWS Panggilan API Digunakan
	minimum yang didukung untuk orientasi Anda. Akun AWS	• `ControlTower:ListEnabledControls` • `ControlTower:ListLandingZones`
AWS CloudTrail Evaluasi	Mengidentifikasi AWS CloudTrail jalur dan konfigurasinya untuk orientasi Anda Akun AWS untuk meminimalkan biaya jejak. CloudTrail	• `CloudTrail:GetTrail` • `CloudTrail:ListTrails` • `S3:GetBucketOwnershipControls` • `S3:GetBucketPolicy` • `KMS:GetKeyPolicy` • `CloudTrail:GetEventSelectors` • `S3:GetBucketLogging` • `S3: GetBucketLifecycleConfiguration` • `S3: GetBucketEncryption`
AWS CloudFormation Evaluasi Hook	Mengidentifikasi CloudFormation kait dalam orientasi Anda Akun AWS yang memblokir penerapan layanan AMS di situs Anda. Akun AWS	• `CloudFormation:ListTypes`

Pemeriksaan Operasional	Tujuan	AWS Panggilan API Digunakan
Evaluasi EC2 Instans Amazon	Mengidentifikasi EC2 instans di Agen Anda Akun AWS yang tidak menjalankan AWS Systems Manager Agen (Agen SSM) dan yang tidak didukung oleh AMS.	• `EC2:DescribeInstances` • `EC2:DescribeImages` • `SSM:DescribeInstanceInformation`

AMS Accelerate mengikuti praktik terbaik industri untuk memenuhi dan mempertahankan kelayakan kepatuhan. Akses AMS Accelerate Discovery ke akun Anda dicatat AWS CloudTrail melalui peran AWSServiceRoleForSupport terkait layanan. Ini membantu dengan persyaratan pemantauan dan audit. Untuk selengkapnya AWS CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Langkah 2. Sumber daya manajemen orientasi di Accelerate

Ini adalah ikhtisar dari proses sumber daya manajemen orientasi.

Anda menerima persyaratan

Manajer pengiriman layanan cloud (CSDM) memandu Anda melalui proses penerimaan. Anda harus menerima Syarat dan Ketentuan, pilih Wilayah AWS, add-on, dan Perjanjian Tingkat Layanan (SLA).

Anda memberikan izin untuk peran AMS

Anda perlu memberikan akses ke proses AMS dan ke Cloud Architect Anda. Anda melakukan ini dengan membuat AWS CloudFormation tumpukan untuk setiap peran. Lihat Template untuk membuat peran AMS dan kemudianBuat `aws_managedservices_onboarding_role` dengan AWS CloudFormation untuk Mempercepat. Untuk lebih jelasnya lihatManajemen akses di AMS Accelerate.

AMS meninjau konfigurasi Anda

Cloud Architect (CA) Anda juga mencari kemungkinan masalah konfigurasi di akun Anda, seperti Kebijakan Kontrol Layanan (SCPs), dan temuan keamanan yang mungkin mencegah AMS menerapkan alat dan sumber daya yang diperlukan oleh AMS. CA bekerja sama dengan Anda untuk membantu memulihkan temuan dan menghapus pemblokir apa pun untuk penerapan alat dan sumber daya AMS.

AMS meninjau konfigurasi AWS CloudTrail jejak Anda

Cloud Architect (CA) Anda akan meninjau konfigurasi CloudTrail jejak Anda, dan mengonfirmasi apakah Anda ingin AMS menerapkan CloudTrail jejak global, atau mengintegrasikan Accelerate dengan CloudTrail akun atau sumber daya jejak Organisasi Anda. Jika Anda memilih untuk mengintegrasikan Accelerate dengan CloudTrail jejak Anda, CA Anda akan memandu Anda melalui pembaruan yang diperlukan pada konfigurasi untuk sumber daya CloudTrail jejak Anda.

AMS menyebarkan sumber daya manajemen

Tim AMS menyebarkan alat dan AWS sumber daya untuk menyediakan berbagai layanan AMS Accelerate. Setelah selesai, AMS telah membuat akun AWS Managed Services dan AMS memberi tahu Anda bahwa akun Anda aktif.

Ini menyimpulkan tahap sumber daya manajemen Orientasi. Anda dapat melanjutkan langsung ke langkah selanjutnya dari proses orientasi:Langkah 3. Fitur AMS orientasi dengan kebijakan default.

> **Note**
>
> Sekarang akun Anda aktif, Anda memiliki opsi untuk melakukan salah satu tugas ini:
>
> - Buat insiden dan permintaan layanan untuk AWS infrastruktur menggunakan Support Center Console. Lihat Laporan insiden, permintaan layanan, dan pertanyaan penagihan di AMS Accelerate.
> - Lihat status kesesuaian di akun Anda tentang AWS Config Aturan yang digunakan oleh AMS,. Kepatuhan konfigurasi di Accelerate
> - Temukan dan analisis GuardDuty dan temuan Macie (opsional). Lihat Monitor dengan GuardDuty.
> - Akses dan audit CloudTrail log
> - Lacak perubahan di akun AMS Accelerate Anda. Lihat Melacak perubahan di akun AMS Accelerate.
> - Gunakan Resource Tagger untuk membuat tag. Lihat Mempercepat Tagger Sumber Daya.
> - Minta Patch, Backup, dan AWS Config Laporan. Lihat Laporan dan opsi.

Tinjau dan perbarui konfigurasi agar AMS Accelerate dapat menggunakan jejak Anda CloudTrail

AMS Accelerate bergantung pada AWS CloudTrail pencatatan untuk mengelola audit dan kepatuhan untuk semua sumber daya di akun Anda. Selama orientasi, Anda memilih apakah Accelerate menyebarkan CloudTrail jejak di AWS Wilayah utama atau menggunakan peristiwa yang dihasilkan oleh CloudTrail akun atau jejak Organisasi yang ada. Jika akun Anda tidak memiliki jejak yang dikonfigurasi, Accelerate akan menerapkan CloudTrail jejak terkelola selama orientasi.

> **Important**
>
> CloudTrail Konfigurasi manajemen log hanya diperlukan ketika Anda memilih untuk mengintegrasikan AMS Accelerate dengan CloudTrail akun atau jejak Organisasi Anda.

Tinjau konfigurasi CloudTrail jejak Anda, kebijakan bucket Amazon S3, AWS KMS dan kebijakan utama untuk tujuan pengiriman acara CloudTrail Anda dengan Cloud Architect (CA) Anda

Sebelum Accelerate dapat menggunakan CloudTrail jejak Anda, Anda harus bekerja dengan Cloud Architect (CA) Anda untuk meninjau dan memperbarui konfigurasi Anda untuk memenuhi persyaratan Accelerate. Jika Anda memilih untuk mengintegrasikan Accelerate dengan jejak CloudTrail Organisasi, CA akan bekerja sama dengan Anda untuk memperbarui bucket Amazon S3 tujuan pengiriman CloudTrail acara dan kebijakan AWS KMS utama untuk mengaktifkan kueri lintas akun dari akun Accelerate Anda. Bucket Amazon S3 Anda dapat berada di akun yang dikelola oleh Accelerate, atau akun yang Anda kelola. Selama orientasi, Accelerate memvalidasi bahwa kueri dapat dibuat ke tujuan pengiriman acara jejak CloudTrail Organisasi Anda, dan menjeda orientasi jika kueri gagal. Anda bekerja dengan CA Anda untuk memperbaiki konfigurasi ini sehingga orientasi dapat dilanjutkan.

Tinjau dan perbarui CloudTrail akun Anda atau konfigurasi jejak Organisasi

Konfigurasi berikut diperlukan untuk mengintegrasikan Mempercepat pengelolaan CloudTrail log CloudTrail akun atau sumber daya jejak Organisasi Anda:

- CloudTrail Jejak Anda dikonfigurasi untuk mencatat peristiwa dari semua Wilayah AWS.
- CloudTrail Jejak Anda mengaktifkan acara layanan global.
- CloudTrail Akun atau jejak Organisasi Anda mencatat semua peristiwa manajemen, termasuk peristiwa baca dan tulis, AWS KMS dan pencatatan peristiwa Amazon RDS Data API diaktifkan.

- CloudTrail Jejak Anda mengaktifkan validasi integritas file log.
- Bucket Amazon S3 CloudTrail jejak Anda mengirimkan peristiwa untuk mengenkripsi peristiwa menggunakan enkripsi SSE-S3 atau SSE-KMS.
- Bucket Amazon S3 yang dikirimkan oleh CloudTrail jejak Anda untuk mengaktifkan pencatatan akses server.
- Bucket Amazon S3 yang akan dikirimkan oleh CloudTrail jejak Anda memiliki konfigurasi siklus hidup yang menyimpan data CloudTrail jejak Anda setidaknya selama 18 bulan.
- Bucket Amazon S3 yang dikirimkan oleh CloudTrail jejak Anda agar Kepemilikan Objek disetel ke pemilik Bucket diberlakukan.
- Bucket Amazon S3 yang dikirimkan oleh CloudTrail jejak Anda dapat diakses oleh Accelerate.

Tinjau dan perbarui kebijakan bucket Amazon S3 untuk tujuan pengiriman CloudTrail acara Anda

Selama orientasi, Anda bekerja sama dengan Cloud Architect (CA) untuk menambahkan pernyataan kebijakan bucket Amazon S3 ke tujuan CloudTrail pengiriman acara. Untuk memungkinkan pengguna menanyakan perubahan di bucket Amazon S3 tujuan pengiriman CloudTrail acara dari akun Accelerate, Anda dapat menerapkan peran IAM bernama seragam di setiap akun di Organisasi yang dikelola Accelerate, dan menambahkannya ke daftar di `aws:PrincipalArn` semua pernyataan kebijakan bucket Amazon S3. Dengan konfigurasi ini, pengguna dapat melakukan kueri dan menganalisis peristiwa jejak CloudTrail Organisasi akun Anda di Accelerate menggunakan Athena. Untuk informasi selengkapnya tentang cara memperbarui kebijakan bucket Amazon S3, lihat Menambahkan kebijakan bucket menggunakan konsol Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

> **Important**
>
> Memperbarui kebijakan bucket Amazon S3 Anda hanya diperlukan jika Accelerate terintegrasi dengan CloudTrail jejak yang mengirimkan peristiwa ke bucket S3 terpusat. Accelerate tidak mendukung integrasi dengan CloudTrail jejak yang dikirim ke bucket terpusat tetapi tidak memiliki akun di bawah Organisasi. AWS

> **Note**
>
> Sebelum memperbarui kebijakan bucket Amazon S3, ganti *red* bidang dengan nilai yang berlaku:

- *amzn-s3-demo-bucket*dengan nama bucket Amazon S3 yang berisi jejak peristiwa dari akun Anda.
- *your-organization-id*dengan ID AWS Organisasi tempat akun Anda menjadi anggota.
- *your-optional-s3-log-delievery-prefix*dengan awalan pengiriman ember Amazon S3 CloudTrail jejak Anda. Misalnya,`my-bucket-prefix`, bahwa Anda mungkin telah menetapkan ketika Anda membuat CloudTrail jejak Anda.

  Jika Anda belum mengonfigurasi awalan pengiriman bucket Amazon S3 untuk jejak Anda, hapus "*your-optional-s3-log-delievery-prefix*" dan garis miring maju (/) dari pernyataan kebijakan bucket Amazon S3 berikut.

Tiga pernyataan kebijakan bucket Amazon S3 berikut memberikan akses Accelerate untuk mengambil konfigurasi dan menjalankan kueri AWS Athena untuk menganalisis peristiwa di bucket Amazon S3 tujuan pengiriman CloudTrail acara Anda dari akun Accelerate Anda.

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWBUCKETCONFIGAUDIT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
```

```
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWLISTBUCKET",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringLike": {
            "s3:prefix": "your-optional-s3-log-delievery-prefix/AWSLogs/*"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWGETOBJECT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/your-optional-s3-log-delievery-
prefix/AWSLogs/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
```

```
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

Tinjau dan perbarui kebijakan AWS KMS utama untuk tujuan pengiriman CloudTrail acara Anda

Selama orientasi, Anda bekerja dengan Cloud Architect (CA) untuk memperbarui kebijakan AWS KMS utama yang digunakan untuk mengenkripsi peristiwa CloudTrail jejak yang dikirimkan ke bucket Amazon S3 Anda. Pastikan Anda menambahkan pernyataan kebijakan AWS KMS kunci referensi ke AWS KMS kunci yang ada. Ini mengonfigurasi Accelerate untuk berintegrasi dengan bucket Amazon S3 tujuan pengiriman event CloudTrail trail yang ada dan mendekripsi peristiwa. Untuk memungkinkan pengguna melakukan kueri perubahan di bucket Amazon S3 tujuan pengiriman CloudTrail acara dari akun Accelerate, Anda dapat menerapkan Peran IAM bernama seragam di setiap akun di Organisasi yang dikelola Accelerate, dan menambahkannya ke daftar “aws:”. PrincipalArn Dengan konfigurasi ini, pengguna Anda dapat melakukan kueri peristiwa.

Ada berbagai skenario pembaruan kebijakan AWS KMS utama yang perlu dipertimbangkan. Anda mungkin hanya memiliki AWS KMS kunci yang dikonfigurasi ke CloudTrail jejak Anda untuk mengenkripsi semua peristiwa, dan tidak memiliki AWS KMS kunci yang mengenkripsi objek di bucket Amazon S3 Anda. Atau, Anda mungkin memiliki satu AWS KMS kunci yang mengenkripsi peristiwa yang dikirimkan oleh CloudTrail, dan AWS KMS kunci lain yang mengenkripsi semua objek yang disimpan di bucket Amazon S3 Anda. Bila Anda memiliki dua AWS KMS kunci, Anda memperbarui kebijakan AWS KMS kunci untuk setiap kunci untuk memberikan akses Accelerate ke CloudTrail acara Anda. Pastikan Anda mengubah pernyataan kebijakan AWS KMS kunci referensi ke kebijakan AWS KMS kunci yang ada sebelum memperbarui kebijakan. Untuk informasi selengkapnya tentang cara memperbarui kebijakan AWS KMS kunci, lihat Mengubah kebijakan kunci di Panduan AWS Key Management Service Pengguna.

> **Important**
>
> Anda harus memperbarui kebijakan AWS KMS kunci hanya jika Accelerate terintegrasi dengan CloudTrail jejak dengan enkripsi SSE-KMS file log diaktifkan.

> **Note**
>
> Sebelum Anda menerapkan pernyataan kebijakan AWS KMS kunci ini ke AWS KMS kunci yang digunakan untuk mengenkripsi AWS CloudTrail peristiwa yang dikirimkan ke bucket Amazon S3, ganti bidang *red* berikut dengan nilai yang berlaku:
>
> - *YOUR-ORGANIZATION-ID*dengan ID AWS Organisasi, akun Anda adalah anggota.

Pernyataan kebijakan AWS KMS utama ini memberikan Akselerasi akses untuk mendekripsi dan menanyakan peristiwa jejak yang dikirimkan ke bucket Amazon S3 dari setiap akun di Organisasi Anda dengan akses terbatas ke Athena, yang digunakan oleh Accelerate untuk menanyakan dan menganalisis peristiwa. CloudTrail .

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWTRAILOBJECTDECRYPTION",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "YOUR-ORGANIZATION-ID"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

Template untuk membuat peran AMS

Peran AMS berikut memberikan izin kepada arsitek cloud AMS (CA) Anda. File zip berikut berisi kode dan AWS CloudFormation templat Terraform yang menyederhanakan pembuatan peran IAM, kebijakan izin, dan kebijakan kepercayaan. Untuk informasi lebih lanjut, konsultasikan dengan CA Anda.

Nama Peran	Diperlukan oleh	Contoh Template
`aws_managedservices_onboarding_role`	Personel AMS selama orientasi saja	onboarding_role_minimal.zip

> **Note**
>
> Setelah Anda memilih dan mengunduh templat sampel (satu per peran), Anda akan mengunggahnya sebagai definisi AWS CloudFormation tumpukan. Buat `aws_managedservices_onboarding_role` dengan AWS CloudFormation untuk Mempercepat

Buat **`aws_managedservices_onboarding_role`** dengan AWS CloudFormation untuk Mempercepat

Anda dapat membuat AWS Identity and Access Management peran,`aws_managedservices_onboarding_role`, dengan AWS CloudFormation dari AWS Management Console. Atau, Anda dapat menggunakan perintah dari AWS CloudShell untuk menyebarkan peran.

Gunakan AWS Management Console

> **Note**
>
> Sebelum memulai, siapkan file JSON atau YAMG untuk setiap peran yang siap diunggah. Untuk informasi selengkapnya, lihat Template untuk membuat peran AMS.

Untuk membuat peran dari AWS Management Console, selesaikan langkah-langkah berikut:

1. Masuk ke AWS Management Console dan buka AWS CloudFormation konsol di https://console.aws.amazon.com/cloudformation.

2. Pilih Buat Tumpukan > Dengan sumber daya baru (standar). Anda melihat halaman berikut.

3. Pilih Unggah file templat, unggah file JSON atau YAMB dari peran IAM, lalu pilih Berikutnya. Anda melihat halaman berikut.

4. Masukkan nama tumpukan "**`ams-onboarding-role`**" di bidang Nama Tumpukan. Masukkan DateOfExpirymenggunakan format “YYYY-MM-DDT 00:00:00 Z” (disarankan 30 hari dari tanggal saat ini). Lanjutkan menggulir ke bawah dan memilih berikutnya sampai Anda mencapai halaman ini:

5. Pastikan kotak centang dipilih dan kemudian pilih Create Stack.
6. Pastikan tumpukan berhasil dibuat.

Gunakan perintah dari AWS CloudShell

Untuk menerapkan peran `aws_managedservices_onboarding_role` IAM, jalankan perintah berikut di: AWS CloudShell

AWS CLI

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/onboarding_role_minimal.zip" -o "onboarding_role_minimal.zip"
unzip -q -o onboarding_role_minimal.zip
aws cloudformation create-stack \
    --stack-name "aws-managedservices-onboarding-role" \
    --capabilities CAPABILITY_NAMED_IAM \
    --template-body file://onboarding_role_minimal.json \
    --parameters ParameterKey=DateOfExpiry,ParameterValue="`date -d '+30 days' -u '+
%Y-%m-%dT%H:%M:%SZ'`"
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/
latest/accelerate-guide/samples/onboarding_role_minimal.zip' -OutFile
 'onboarding_role_minimal.zip'
Expand-Archive -Path 'onboarding_role_minimal.zip' -DestinationPath . -Force
New-CFNStack `
    -StackName 'aws-managedservices-onboarding-role' `
    -Capability CAPABILITY_NAMED_IAM `
    -TemplateBody (Get-Content 'onboarding_role_minimal.json' -Raw) `
    -Parameter @{ParameterKey = "DateOfExpiry"; ParameterValue = (Get-
Date).AddDays(30).ToString('yyyy-MM-ddTHH:mm:ssZ')}
```

Setelah Anda membuat peran, bekerja dengan Cloud Architect (CA) Anda untuk menyelesaikan Langkah 2. Sumber daya manajemen orientasi di Accelerate prosesnya. Setelah AMS memberi tahu Anda bahwa akun Anda aktif, Anda siap untuk melakukan onboard instans Anda.

Langkah 3. Fitur AMS orientasi dengan kebijakan default

Pada tahap ini, Anda menggunakan fitur AMS dengan kebijakan default. Ini termasuk menambahkan EC2 instans Amazon dan mengonfigurasi pemantauan, pencadangan, AWS Config perbaikan, dan tambalan (jika ada, AMS Patch Orchestrator adalah add-on yang harus Anda minta secara khusus) sesuai dengan preferensi Anda. Anda dapat melakukannya sendiri, atau meminta fitur bawaan AMS berdasarkan input Anda. Untuk meminta bantuan dari AMS, buat permintaan layanan dan berikan semua input yang diperlukan untuk menyelesaikan tugas. Ingatlah bahwa permintaan layanan tidak segera diselesaikan.

> **Note**
>
> Meskipun akun mungkin menggunakan kebijakan default untuk pencadangan, tambalan, atau pemantauan, sumber daya perlu diberi tag agar kebijakan yang sesuai menjadi efektif.

Topik

- (Opsional) Template Mulai Cepat di Accelerate
- Orientasi Mempercepat pemantauan
- EC2 Instans orientasi untuk Mempercepat
- Orientasi AWS Backup di Accelerate

- Penambalan orientasi di Accelerate
- Tinjau laporan ketidaksesuaian di Accelerate

(Opsional) Template Mulai Cepat di Accelerate

Template Mulai Cepat mengotomatiskan penerapan dan konfigurasi AMS Resource Tagger di akun berkemampuan Accelerate. AWS Template ini menghemat waktu dan tenaga dibandingkan dengan pengaturan manual. Gunakan template ini apa adanya untuk menentukan dasar-dasar pemantauan, penambalan, dan pencadangan dalam satu akun. Atau, gunakan StackSet untuk menerapkan pengaturan di seluruh Organizations Units untuk menstandarisasi pengaturan untuk beberapa akun.

Anda juga dapat menggunakannya sebagai titik awal untuk membuat profil AMS Resource Tagger kustom Anda sendiri dan menggunakan cuplikan dari dokumentasi untuk membuat definisi yang lebih kompleks untuk penandaan.

Fungsionalitas template Mulai Cepat

Template Quick Start menyelesaikan tugas-tugas berikut:

- Membuat dan menerapkan versi konfigurasi untuk AMS Resource Tagger.
- Menerapkan tag ke EC2 instans Amazon yang memungkinkan pengelolaan AMS dan pembuatan sumber daya pemantauan.
- (Opsional) Menerapkan tag ke EC2 instance terkelola yang memungkinkannya ditambal pada jadwal yang diinginkan, dan membuat Jendela Pemeliharaan Patching untuk memfasilitasi penambalan.

  > ⚠ Warning
  >
  > Secara default, instance di-boot ulang dan instance yang dihentikan dimulai secara otomatis untuk instalasi patch.

- (Opsional) Menerapkan tag ke EC2 instance terkelola yang memungkinkannya dicadangkan seperti yang didefinisikan dalam Paket Cadangan AMS default.
- (Opsional) Menerapkan tag ke sumber daya Amazon Relational Database Service (Amazon RDS) terkelola yang memungkinkannya dicadangkan sesuai dengan paket cadangan yang Ditingkatkan. Paket cadangan juga memungkinkan Point in time recovery (PITR) untuk Amazon RDS. Jika pencadangan otomatis Amazon RDS tidak diaktifkan, maka database akan dimulai ulang mendekati waktu jendela pencadangan berikutnya.

Penggantian dan pengecualian template Mulai Cepat

Setelah Anda menggunakan template ini untuk membuat tumpukan Mulai Cepat, gunakan langkah-langkah berikut untuk mengecualikan instance tertentu dari Manajemen/Pemantauan, Penambalan, atau Pencadangan:

- Manajemen dan Pemantauan: Untuk mengecualikan EC2 instance agar tidak dikelola dan dipantau oleh AMS, tambahkan tag ini ke instance:`ExcludeFromAMSQuickStartMonitoring=true`.
- Patching: EC2 instance yang merupakan anggota grup Auto Scaling, Amazon Elastic Container Service, atau kluster Amazon Elastic Kubernetes Service dikecualikan dari Patching oleh template Mulai Cepat ini.

  Untuk menonaktifkan pembuatan Jendela Penambalan dan penandaan EC2 instance terkait tambalan, setel parameter tumpukan ke. CloudFormation `EnablePatching=false`

  Untuk mengecualikan EC2 instance agar tidak ditargetkan oleh jendela patching Quick Start kapan`EnablePatching=true`, tambahkan tag ini ke instance:`ExcludeFromAMSQuickStartPatching=true`.
- Backup: EC2 instance yang merupakan anggota grup Auto Scaling, ECS, atau kluster EKS dikecualikan dari Backup oleh template Mulai Cepat ini.

  Untuk mengecualikan EC2 instance agar tidak ditargetkan oleh Paket Cadangan AMS default, kapan`EnableBackup=true`, tambahkan tag ini ke instance tersebut:`ExcludeFromAMSQuickStartBackup=true`.

> **Tip**
>
> Anda dapat menandai EC2 instance secara massal. Gunakan Editor Tag untuk memilih secara massal dan menandai sumber daya dalam satu langkah di. AWS Management Console

Parameter template Mulai Cepat

Template Mulai Cepat ini mengonfigurasi Resource Tagger untuk menambahkan tag `ams:rt:ams-managed=true` ke semua EC2 instance di akun, tidak termasuk instance tempat Anda

menambahkan tag. `ExcludeFromAMSQuickStartMonitoring=true` Gunakan parameter berikut untuk mengontrol bagian opsional tumpukan ini sesuai dengan kebutuhan Anda:

CFN Parameter	Nilai	Efek
EnableBackup	'benar' (default)	Semua EC2 instans (`ams:rt:ams-managed=true`) yang dikelola AMS ditandai `ams:rt:backup-orchestrator=true` untuk pencadangan setiap hari pada pukul 04.00 UTC sesuai dengan Paket Cadangan AMS default. Untuk semua instans dan cluster RDS, template menerapkan `ams:rt:backup-orchestrator-enhanced=true` "pencadangan berkelanjutan" dengan retensi maksimum (31 hari) sesuai rencana pencadangan yang Ditingkatkan. Jika ini mengubah periode retensi PITR Anda, database mungkin dimulai ulang dalam beberapa kasus, misalnya jika ada pembaruan konfigurasi tertunda lainnya.
	'palsu'	Tidak ada instance yang ditargetkan untuk cadangan oleh template mulai cepat ini.
EnablePatching	'salah' (default)	Tidak ada instance yang ditargetkan untuk ditambal oleh template Mulai Cepat ini.
	'benar'	Semua instans (`ams:rt:ams-managed=true`) yang dikelola

CFN Parameter	Nilai	Efek
		AMS ditandai dengan `ams:rt:Patch Group=AMSQuickStartPatchWindow` dan sumber daya Jendela Pemeliharaan SSM dasar dibuat untuk memfasilitasi penambalan sesuai dengan jadwal yang ditentukan dalam. `CronExpression` Untuk menerapkan `ams:rt:Patch Group` tag ke EC2 instance, Anda harus menonaktifkan akses ke tag dalam metadata instance untuk instance tersebut.
CronExpression	-	Nilai default `cron(0 30 19 ? * SAT#2 *)` menetapkan Sabtu ke-2 setiap bulan pada pukul 19:30 sesuai dengan `Timezone` parameter. Gunakan sintaks cron.
Zona waktu	-	Contoh target ditambal sesuai dengan. `CronExpression` Gunakan format IANA.

Unduh template Mulai Cepat

Unduh file AMSQuick Start.zip.

Atau, jalankan perintah berikut AWS CloudShelluntuk menerapkan: `AMSQuickStart.yaml`

AWS Command Line Interface

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/AMSQuickStart.zip" -o "AMSQuickStart.zip"
unzip -q -o AMSQuickStart.zip
for region in region1 region2 ;
```

```
do
aws cloudformation create-stack \
    --region $region \
    --stack-name "AMSQuickStart" \
    --template-body file://AMSQuickStart.yaml \
    --parameters \
        ParameterKey=EnableBackup,ParameterValue="true" \
        ParameterKey=EnablePatching,ParameterValue="false" \
        ParameterKey=Timezone,ParameterValue="US/Eastern" \
        ParameterKey=CronExpression,ParameterValue="cron(0 30 19 ? * SAT#2 *)" \
;
done
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/latest/
accelerate-guide/samples/AMSQuickStart.zip' -OutFile 'AMSQuickStart.zip'
Expand-Archive -Path 'AMSQuickStart.zip' -DestinationPath . -Force
@('region1', 'region2') | `
ForEach-Object { `
New-CFNStack `
    -Region $_ `
    -StackName 'AMSQuickStart' `
    -TemplateBody (Get-Content 'AMSQuickStart.yaml' -Raw) `
    -Parameter @(
        @{ParameterKey = "EnableBackup"; ParameterValue = "true"},
        @{ParameterKey = "EnablePatching"; ParameterValue = "false"},
        @{ParameterKey = "Timezone"; ParameterValue = "US/Eastern"},
        @{ParameterKey = "CronExpression"; ParameterValue = "cron(0 30 19 ? * SAT#2
 *)"}
    )
}
```

Untuk deskripsi setiap parameter, lihat bagian sebelumnya,. Parameter template Mulai Cepat

Orientasi Mempercepat pemantauan

Pemantauan diaktifkan secara default untuk semua sumber daya baru kecuali EC2 instans Amazon. Anda dapat mulai memantau EC2 instans Amazon Anda dengan menandai instans Anda.

Untuk pemantauan onboard, pertama-tama pastikan konfigurasi Anda memantau sumber daya yang ingin AMS pantau, dan abaikan sumber daya yang ingin Anda abaikan.

Anda dapat menggunakan CloudWatch dasbor berikut untuk menjelajahi berapa banyak sumber daya yang ditargetkan oleh pemantauan dan penandaan AMS, dan berapa banyak yang tidak. Di akun Anda, navigasikan ke konsol CloudWatch dasbor, dan pilih salah satu dari berikut ini:

- Dasbor Pelaporan-Manajer-Alarm-AMS-Alarm
- Dasbor Pelaporan Tagger-Sumber Daya AMS

Untuk deskripsi lengkap tentang metrik dasbor, lihat:

- Melihat jumlah sumber daya yang dipantau oleh Manajer Alarm untuk Mempercepat
- Melihat jumlah sumber daya yang dikelola oleh Resource Tagger

Sumber daya orientasi untuk dipantau di Accelerate

Untuk mengganti perilaku default, misalnya, untuk menonaktifkan pemantauan default untuk EC2 non-sumber daya, Anda perlu menghapus tag sumber daya tersebut menggunakan profil konfigurasi khusus. Untuk informasi selengkapnya tentang penandaan untuk pemantauan, lihatPemantauan dalam Mempercepat.

Pemantauan dinonaktifkan untuk EC2 instance hingga Anda melakukan onboard instance, yang mencakup penandaan instance menggunakan profil konfigurasi khusus. Bagian selanjutnya menjelaskan orientasi EC2 instance.

Membuat profil konfigurasi pemantauan di Accelerate

- Untuk informasi tentang menggunakan konfigurasi default, lihatMempercepat Manajer Alarm.
- Untuk informasi tentang menggunakan konfigurasi kustom, lihatMemodifikasi konfigurasi default Accelerate alarm.

EC2 Instans orientasi untuk Mempercepat

EC2 Instance di-onboard ke AMS Accelerate melalui proses yang disebut Konfigurasi Instans Otomatis, yang memastikan bahwa setiap instance menulis log yang benar dan memancarkan metrik yang benar agar AMS dapat mengelola instance dengan benar. Anda harus memasukkan semua EC2 intances Anda, kecuali jika Anda secara khusus ingin AMS mengabaikannya. Konfigurasi Instans Otomatis mengharuskan kondisi tertentu terpenuhi yang memungkinkan AMS mengonfigurasi instance (untuk detail lihatPrasyarat untuk konfigurasi instans otomatis di Accelerate). Kondisi yang

paling penting adalah AWS Systems Manager agen (agen SSM) perlu diinstal pada setiap EC2 instans Amazon yang Anda ingin AMS kelola untuk Anda. Untuk informasi lebih lanjut tentang agen SSM, lihat Bekerja dengan agen SSM.

SSM pra-instal dalam standar AMIs untuk Accelerate

Agen SSM sudah diinstal pada AWS-disediakan AMIs untuk sistem operasi berikut.

- Amazon Linux dan Amazon Linux 2
- SUSE Linux Enterprise Server (SLES) 12 dan 15
- Microsoft Windows Server 2019, 2016, 2012 R2, 2012
- Ubuntu Linux 18.04 dan 20.04

Jika Anda menggunakan salah satu dari ini AWS-provided AMIs, lihatMenandai instance di Accelerate.

Instalasi SSM manual SSM di Accelerate

Untuk sistem operasi berikut, atau saat menggunakan AMI khusus, Anda dapat menginstal agen SSM secara manual. Atau, Anda dapat menggunakan fitur instalasi otomatis Agen SSM AMS. Untuk mempelajari lebih lanjut tentang instalasi auto SSM, lihatInstalasi otomatis Agen SSM. Untuk petunjuk tentang instalasi manual, pilih tautan untuk sistem operasi Anda:

- Instalasi CentOS SSM
- Instalasi Oracle SSM
- Instalasi Red Hat SSM
- Instalasi SUSE Linux Enterprise Server SSM
- Instalasi SSM Windows

Menandai instance di Accelerate

Setelah agen SSM diinstal, Anda harus menandai instance Anda. Lihat Menandai AMS Accelerate.

Konfigurasi instans otomatis di Accelerate

Setelah instans Anda diberi tag, AMS akan melakukan konfigurasi instans Otomatis, yang meliputi:

- Rekam log dan metrik sistem operasi

- Aktifkan akses jarak jauh untuk insinyur AMS
- Jalankan perintah jarak jauh pada instance

Tugas-tugas ini penting untuk layanan pemantauan, tambalan, dan log AMS; dan agar AMS menanggapi insiden. Untuk detail tentang pengaturan Konfigurasi Instans Otomatis, lihatKonfigurasi instans otomatis di AMS Accelerate.

Setelah konfigurasi instans Otomatis selesai, Anda dapat:

- Buat insiden dan permintaan layanan untuk EC2 instans Amazon dan sistem operasi menggunakan Support Center Console. Untuk informasi selengkapnya, lihat Laporan insiden, permintaan layanan, dan pertanyaan penagihan di AMS Accelerate.
- Akses dan audit EC2 log Amazon
- Dapatkan laporan tambalan

Orientasi AWS Backup di Accelerate

Untuk mengonfigurasi cadangan, Anda perlu membuat kebijakan cadangan yang disebut rencana cadangan. Rencana cadangan menentukan AWS sumber daya mana yang akan dicadangkan, seberapa sering mereka perlu dicadangkan, dan periode retensi cadangan. Sebaiknya evaluasi persyaratan kontinuitas, keamanan, dan kepatuhan organisasi Anda untuk menentukan rencana cadangan yang Anda butuhkan.

Keikutsertaan

- Pastikan bahwa AWS Backup diaktifkan untuk setiap akun, Wilayah, dan jenis sumber daya dengan mengikuti langkah-langkah di sini:

  Memulai 1: Layanan Opt-in.

  Secara opsional, Memulai 2: Buat cadangan sesuai permintaan.

Pilih paket cadangan

- Untuk memilih paket cadangan, lihatPilih paket cadangan AMS.

Tambahkan sumber daya

Sumber daya tidak terkait dengan rencana cadangan secara default. Mereka perlu ditambahkan ke rencana cadangan.

- Untuk menambahkan sumber daya ke rencana cadangan, lihatTandai sumber daya Anda untuk menerapkan paket cadangan AMS.
- Untuk mengaktifkan pencadangan pada semua sumber daya menggunakan tag, lihatMengelola tag untuk backup di Accelerate.

Penambalan orientasi di Accelerate

Anda perlu mengonfigurasi patching untuk memastikan bahwa perangkat lunak Anda memenuhi kebijakan kepatuhan Anda. up-to-date

AWS Backup Prasyarat: Untuk mengizinkan pembuatan snapshot volume root selama jendela pemeliharaan tambalan, pastikan itu AWS Backup diaktifkan untuk setiap akun dan wilayah untuk jenis sumber daya Amazon EBS dengan mengikuti langkah-langkah di sini: Memulai 1: Keikutsertaan Layanan. (Anda tidak perlu melanjutkan untuk Memulai 2: Buat cadangan sesuai permintaan.)

Kapan harus menambal: Penambalan terjadi selama jendela pemeliharaan. Anda dapat menjadwalkan jendela pemeliharaan sehingga tambalan hanya diterapkan selama waktu yang telah ditetapkan.

Apa yang harus ditambal: Anda harus mengaitkan EC2 instance Amazon yang ingin Anda tambal dengan jendela pemeliharaan. Untuk mengaitkan instance dengan jendela pemeliharaan, EC2 instans Amazon harus diberi tag, dan jendela pemeliharaan harus memiliki tag tersebut sebagai target.

Patch mana yang harus diinstal: Menggunakan patch baseline, Anda menetapkan aturan untuk secara otomatis menyetujui jenis patch tertentu, seperti sistem operasi atau patch tingkat keparahan tinggi. Anda juga dapat menentukan pengecualian pada aturan Anda, misalnya, daftar tambalan yang selalu disetujui atau ditolak.

Lihat Rekomendasi penambalan panduan tentang kebijakan EC2 tambalan Amazon.

- Untuk mulai mengonfigurasi manajemen tambalan, lihat Memahami manajemen tambalan di AMS Accelerate
- Untuk membuat konfigurasi patch kustom, lihatGaris dasar patch khusus dengan AMS Accelerate.

Tinjau laporan ketidaksesuaian di Accelerate

AMS menerapkan AWS Config aturan yang membantu Anda mengidentifikasi pelanggaran terhadap standar yang ditetapkan oleh Center for Internet Security (CIS), National Institute of Standards and Technology (NIST) Cloud Security Framework (CSF). Kami menyarankan Anda untuk meninjau laporan ketidaksesuaian dengan tim pengiriman Anda untuk memprioritaskan tindakan remediasi sehingga akun Anda didasari ke status kesesuaian.

Langkah 4. Sesuaikan fitur di Accelerate

Pada tahap ini, Anda telah melakukan onboard monitoring, patching, dan backup dengan kebijakan default. Sekarang Anda memiliki kesempatan untuk menyesuaikan kebijakan sesuai dengan kebutuhan Anda.

Anda dapat memilih untuk menggunakan kebijakan default untuk patch, backup atau monitoring, atau memilih kebijakan kustom berdasarkan kebutuhan Anda. AMS menggunakan tag untuk mengaitkan sumber daya dengan kebijakan operasional. AMS menyediakan Resource Tagger yang memungkinkan Anda menentukan aturan tentang cara tag diterapkan ke AWS sumber daya berdasarkan pengelompokan aplikasi atau logika pengelompokan lainnya Untuk informasi selengkapnya, lihat. Mempercepat Tagger Sumber Daya

Fitur tag yang disediakan pelanggan memungkinkan Anda menambahkan dan menghapus tag khusus ke sumber daya AMS. Lihat informasi yang lebih lengkap di Tag yang disediakan pelanggan di Accelerate.

Topik

- Sesuaikan pemantauan di Accelerate
- Sesuaikan cadangan di Accelerate
- Sesuaikan tambalan di Accelerate

Sesuaikan pemantauan di Accelerate

Untuk menyesuaikan pemantauan sumber daya cloud Anda berdasarkan kebutuhan aplikasi Anda:

1. Buat kebijakan pemantauan kustom. Lihat Memodifikasi konfigurasi default Accelerate alarm.
2. Menerapkan kebijakan khusus ke sumber daya menggunakan tag. Lihat Pemantauan dalam Mempercepat

3. Peringatan rute ke pemilik sumber daya. Lihat Pemberitahuan peringatan berbasis tag.

Anda dapat menggunakan CloudWatch dasbor berikut untuk mengeksplorasi berapa banyak sumber daya yang ditargetkan oleh pemantauan dan penandaan AMS, dan berapa banyak yang tidak. Di akun Anda, navigasikan ke konsol CloudWatch dasbor, dan pilih salah satu dari berikut ini:

- Dasbor Pelaporan-Manajer-Alarm-AMS-Alarm
- Dasbor Pelaporan Tagger-Sumber Daya AMS

Untuk deskripsi lengkap tentang metrik dasbor, lihat:

- Melihat jumlah sumber daya yang dipantau oleh Manajer Alarm untuk Mempercepat
- Melihat jumlah sumber daya yang dikelola oleh Resource Tagger

Sesuaikan cadangan di Accelerate

Anda tidak dapat menyesuaikan paket cadangan default AMS. Sebagai gantinya, buat rencana cadangan baru berdasarkan kebutuhan aplikasi Anda, lalu lampirkan sumber daya ke paket kustom Anda menggunakan tag. Terserah Anda untuk memilih sumber daya mana yang harus dicadangkan AMS, seberapa sering, dan untuk periode retensi apa. Sebaiknya evaluasi persyaratan kontinuitas, keamanan, dan kepatuhan organisasi Anda untuk menentukan rencana cadangan apa yang Anda butuhkan.

- Untuk membuat rencana cadangan, lihat Membuat rencana cadangan.
- Untuk menetapkan sumber daya ke rencana cadangan, lihat Menetapkan sumber daya ke rencana cadangan.

Sesuaikan tambalan di Accelerate

Patching memastikan bahwa perangkat lunak Anda memenuhi kebijakan kepatuhan Anda. up-to-date

Kapan harus menambal: Penambalan terjadi selama jendela pemeliharaan. Anda dapat menjadwalkan jendela pemeliharaan sehingga tambalan hanya diterapkan selama waktu yang telah ditetapkan.

Apa yang harus ditambal: Anda harus mengaitkan EC2 instance Amazon yang ingin Anda tambal dengan jendela pemeliharaan. Untuk mengaitkan instance dengan jendela pemeliharaan, EC2

instans Amazon harus diberi tag, dan jendela pemeliharaan harus memiliki tag tersebut sebagai target.

Patch mana yang harus diinstal: Menggunakan patch baseline, Anda menetapkan aturan untuk secara otomatis menyetujui jenis patch tertentu, seperti sistem operasi atau patch tingkat keparahan tinggi. Anda juga dapat menentukan pengecualian pada aturan Anda, misalnya, daftar tambalan yang selalu disetujui atau ditolak.

- Untuk rekomendasi penambalan umum, lihatRekomendasi penambalan.
- Untuk membuat jendela pemeliharaan khusus, lihatBuat jendela pemeliharaan tambalan di AMS.
- Untuk membuat baseline patch kustom, lihat. Garis dasar patch khusus dengan AMS Accelerate
- Untuk merutekan peringatan tambalan ke pemilik sumber daya, lihatMemahami notifikasi tambalan dan kegagalan tambalan di AMS Accelerate.

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 Accelerate memiliki fitur-fitur ini:

- Halaman pembuka: Halaman pembuka memiliki kotak informasi dan tautan untuk memfasilitasi akses Anda ke permintaan layanan, dan laporan Anda.
- Halaman fitur, tautan di panel navigasi sebelah kiri:
  - Dasbor: Memberikan ikhtisar status akun Anda saat ini termasuk:
    - Insiden pada sumber daya Anda: Tombol untuk membuka kasus insiden di AWS Support Center, ditambah berapa banyak kasus insiden yang Menunggu persetujuan dan memerlukan perhatian Anda dan berapa banyak yang Terbuka
    - Status kepatuhan: Tautan ke Aturan dan Sumber Daya yang tidak patuh atau sesuai
    - Permintaan layanan: Tombol untuk membuka kasus permintaan layanan di AWS Support Center, ditambah berapa banyak yang Menunggu persetujuan dan memerlukan perhatian Anda dan berapa banyak yang Terbuka
    - Keamanan tingkat akun: Tautan ke detail tentang GuardDuty temuan deteksi ancaman waktu nyata dan keamanan data dan temuan Macie
    - Tindakan cepat: Buka brankas Cadangan atau halaman konfigurasi instance Patch Anda
  - Laporan: Membuka halaman Laporan dan laporan default, Backup Harian dan Patch Harian dan Penagihan Bulanan
  - Konfigurasi: Pastikan sumber daya Anda dikelola dengan sukses dan sesuai dengan spesifikasi Anda.
    - Instal agen SSM: Agen SSM diperlukan
    - Konfigurasikan aturan penandaan: Membuka AMS Resource Tagger
    - Konfigurasikan alarm: Membuka konfigurasi CloudWatch alarm AMS
    - Konfigurasikan jadwal patch: Membuka konsol AWS Systems Manager
    - Konfigurasikan garis dasar patch: Membuka konsol AWS Patch Manager
    - Konfigurasikan paket cadangan: Membuka konsol AWS Backup
- Sorotan fitur: Informasi tentang pembaruan terbaru ke konsol
- Dokumentasi: Halaman landing dokumentasi AWS Managed Services

Pola AMS

Pola AWS Managed Services (AMS) adalah solusi umum yang memecahkan rangkaian kasus penggunaan di lingkungan yang dikelola AMS.

Saat Anda beroperasi di platform AMS, arsitek cloud AMS (CAs) bekerja sama dengan Anda untuk memenuhi persyaratan bisnis dan operasional Anda. Sementara pelanggan AMS beroperasi dengan cara yang unik, kami melihat bahwa pelanggan memiliki kasus penggunaan yang serupa. Dalam kasus seperti itu, CAs buat templat solusi umum, atau "pola", yang digunakan di beberapa lingkungan pelanggan dengan konfigurasi dan upaya penerapan minimal.

Pola AMS dibuat untuk membantu memberikan fitur kepada pelanggan AMS dan biasanya dibuat oleh akun CA pelanggan yang memintanya.

Cara kerja pola AMS

Untuk meminta detail selengkapnya tentang setiap pola termasuk templat cloudformation yang diperlukan agar Anda dapat menerapkan pola, kirimkan permintaan layanan AMS dengan Subjek "Permintaan detail tambahan tentang pola*`Pattern_Name`*" (ganti pola yang Anda inginkan) dan tambahkan arsitek cloud AMS (CA) ke opsi Kontak tambahan.

Pola AMS diklasifikasikan menjadi dua (2) kategori:

- Penggunaan Umum: Pola dianggap stabil karena telah digunakan dan digunakan oleh beberapa pelanggan AMS
- Mode Pratinjau: AMS merekomendasikan penerapan pola Mode Pratinjau di lingkungan non-produksi Anda untuk validasi, dan terlibat dengan Cloud Architect Anda untuk mendiskusikan kasus penggunaan sebelum penerapan.

> **Important**
>
> Pola AMS tidak mematuhi Perjanjian Tingkat Layanan AMS default Perjanjian Tingkat Layanan (SLAs) dan Tujuan Tingkat Layanan (SLOs). Support dan update untuk pola dilakukan atas dasar usaha terbaik.
> AWS Konten ini disediakan dengan tunduk pada ketentuan Perjanjian AWS Pelanggan atau perjanjian tertulis lainnya antara pelanggan dan Amazon Web Services, Inc. atau Amazon Web Services EMEA SARL ("AWS Eropa") atau keduanya.

Materi yang terkandung dalam perangkat lunak ini diberikan kepada Anda “apa adanya” dan tanpa jaminan dalam bentuk apa pun, tersurat, tersirat atau lainnya, termasuk tanpa batasan, jaminan kesesuaian apa pun untuk tujuan tertentu.

Pola AMS

Pola AMS.

Pola AMS

Nama	Gambaran umum	Manfaat	Kategori
Sesuaikan Pemberitahuan CloudWatch Alarm	Sesuaikan pemberitahuan CloudWatch alarm untuk menyertakan informasi dari tag instance seperti nama instance, ID aplikasi, dan sebagainya.	Menambahkan informasi kontekstual ke notifikasi alarm akan membuatnya lebih bermakna dan memberikan informasi yang dapat ditindaklanjuti.	Pemantauan
Pelaporan Penggunaan Disk	Pola Pelaporan Penggunaan Disk mengumpulkan ruang konsumsi volume di beberapa akun aplikasi dan menyajikan hasilnya sebagai laporan terpusat di Amazon S3 dengan kemampuan kueri tabel Athena.	Memberikan wawasan tentang penggunaan aktual volume akun untuk menentukan peluang penghematan biaya.	Optimalisasi biaya
Tumpukan Prowler	Menjalankan pemeriksaan Prowler pada akun yang	Bantu membuka blokir Accelerate onboarding (Prowler)	Keamanan

Nama	Gambaran umum	Manfaat	Kategori
	menggunakan Amazon EC2 di mana tidak CloudShell dapat digunakan.	jika tidak CloudShell dapat digunakan baik karena masalah izin atau batas waktu tanpa memengaruhi postur keamanannya saat ini.	
Replikasi AMS Amazon S3 dengan Tombol Objek Kustom	Buat salinan objek Amazon S3 dan simpan semua metadata dan kunci objek (folder). Menghapus bagian dari kunci objek sumber, atau membuat kunci objek tujuan khusus selama replikasi.	Sesuaikan kunci objek (folder) selama replikasi Amazon S3 tanpa memerlukan skrip tambahan untuk memindahkan objek ke folder yang diperlukan.	Keandalan
Penghapusan Snapshot Amazon EBS	Otomatisasi berdasarkan Lambda dan CloudWatch Acara untuk mengotomatiskan penghapusan snapshot Amazon EBS yang diambil di luar, berdasarkan retensi. AWS Backup	Membantu membersihkan foto individu yang diambil di luar AWS Backup orkestrator, menghemat biaya tambahan dari waktu ke waktu.	Optimalisasi biaya

Nama	Gambaran umum	Manfaat	Kategori
Rotasi Rahasia AMS Amazon RDS	Menggunakan CloudFormation template, secara otomatis menyebarkan semua sumber daya yang diperlukan (fungsi Lambda, grup Keamanan, antarmuka jaringan elastis ENIs atau) yang diperlukan untuk memutar rahasia untuk database Amazon RDS yang didukung, Redshift, dan DocumentDB.	Otomatiskan rotasi rahasia database, dan berikan mekanisme notifikasi saat terjadi kegagalan rotasi.	Keamanan
Rotasi Kunci Otomatis	Secara otomatis memutar akses dan kunci rahasia untuk pengguna IAM berdasarkan, pada CloudWatch Acara dan Lambda.	Rotasi akses dan kunci rahasia yang lebih mudah untuk pengguna IAM.	Keamanan

Nama	Gambaran umum	Manfaat	Kategori
Tagger Snapshot Volume Amazon EBS	Tandai semua volume dan snapshot Amazon EBS menggunakan tag di instans Amazon EC2 .	Membantu mengkategorikan dan melacak biaya dengan informasi bisnis yang bermakna dan relevan sehingga memudahkan untuk memvalidasi di mana uang dibelanjakan, dan memungkinkan penggunaan otomatisasi untuk volume dan snapshot yang ditandai. Praktik terbaik yang sangat direkomendasikan oleh pilar Optimasi AWS Biaya.	Penandaan (pengoptimalan biaya, Keamanan, manajemen insiden, dan otomatisasi)

Konfigurasi instans otomatis di AMS Accelerate

AMS Accelerate menyediakan layanan konfigurasi instans otomatis. Layanan ini memastikan bahwa sebuah instance memancarkan log dan metrik yang benar agar AMS dapat mengelola instance dengan benar. Konfigurasi instans otomatis memiliki prasyarat dan langkah-langkahnya sendiri untuk orientasi, yang dijelaskan nanti di bagian ini.

Topik

- Cara kerja konfigurasi instans otomatis di Accelerate
- Instalasi otomatis Agen SSM
- Perubahan konfigurasi instans otomatis

Cara kerja konfigurasi instans otomatis di Accelerate

Konfigurasi instans otomatis memungkinkan AMS Accelerate untuk melakukan konfigurasi tertentu setiap hari pada instance yang Anda tunjukkan dengan menambahkan agen dan tag tertentu.

Prasyarat untuk konfigurasi instans otomatis di Accelerate

Ketentuan ini harus dipenuhi agar AMS Accelerate dapat melakukan tindakan otomatis yang dijelaskan sebelumnya pada instans terkelola.

Agen SSM diinstal

AMS Mempercepat konfigurasi instans otomatis mengharuskan Agen AWS Systems Manager SSM diinstal.

Untuk informasi tentang penggunaan fitur instalasi otomatis Agen SSM AMS, lihatInstalasi otomatis Agen SSM.

Untuk informasi tentang cara menginstal Agen SSM secara manual, lihat berikut ini:

- Linux: Instal Agen SSM secara manual di EC2 instans Amazon untuk Linux - AWS Systems Manager
- Windows: Instal Agen SSM secara manual di EC2 instans Amazon untuk Windows Server - AWS Systems Manager

Agen SSM berada dalam keadaan terkelola

Konfigurasi instans otomatis AMS Accelerate memerlukan Agen SSM operasional. Agen SSM harus diinstal, dan EC2 instans Amazon harus dalam status terkelola. Untuk informasi selengkapnya, lihat AWS dokumentasi, Bekerja dengan Agen SSM.

Pengaturan konfigurasi instans otomatis

Dengan asumsi prasyarat telah terpenuhi, menambahkan tag EC2 instans Amazon tertentu secara otomatis memulai konfigurasi instans otomatis AMS Accelerate. Gunakan salah satu metode berikut untuk menambahkan tag ini:

1. (Sangat disarankan) Gunakan AMS Accelerate Resource Tagger

   Untuk mengonfigurasi logika penandaan untuk akun Anda, lihatCara kerja penandaan. Setelah penandaan selesai, tag dan konfigurasi instans otomatis ditangani secara otomatis.

2. Tambahkan tag secara manual

   Tambahkan tag berikut secara manual ke EC2 instance Amazon:

   Kunci: ams:rt:ams-managed, Nilai: true.

> **Note**
>
> Layanan konfigurasi instans mencoba menerapkan konfigurasi AMS yang diperlukan setelah tag ams:rt:ams-managed diterapkan ke instance. Layanan ini menegaskan konfigurasi yang diperlukan AMS setiap kali instance dimulai, dan saat pemeriksaan konfigurasi harian AMS terjadi.

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**
>
> - Jika akun Anda di-onboard ke AMS Accelerate setelah 6/03/2024, maka fitur ini diaktifkan secara default. Untuk menonaktifkan fitur ini, hubungi CA atau CSDM Anda.
> - Untuk mengaktifkan fitur ini di akun yang terhubung sebelum 6/03/2024, hubungi CA atau CSDM Anda.
> - Fitur ini hanya tersedia untuk EC2 instance yang tidak ada dalam grup Auto Scaling dan yang menjalankan sistem operasi Linux yang didukung oleh AMS.

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 SSMManaged EC2 InstanceDefaultPolicy
  - Amazon SSMManaged 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 konfigurasikan 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 konfigurasi instans otomatis

Otomatisasi konfigurasi instans AMS Accelerate membuat perubahan berikut di akun Anda:

1. Izin IAM

   Menambahkan Kebijakan yang dikelola IAM yang diperlukan untuk memberikan izin instans untuk menggunakan agen yang diinstal oleh AMS Accelerate.

2. Agen
   a. CloudWatch Agen Amazon bertanggung jawab untuk memancarkan log dan metrik OS. Otomatisasi konfigurasi instans memastikan bahwa CloudWatch agen diinstal dan menjalankan versi minimum AMS Accelerate.
   b. Agen AWS Systems Manager SSM bertanggung jawab untuk menjalankan perintah jarak jauh pada instance. Otomatisasi konfigurasi instans memastikan bahwa Agen SSM menjalankan versi minimum AMS Accelerate.
3. CloudWatch Konfigurasi

a. Untuk memastikan bahwa metrik dan log yang diperlukan dipancarkan, AMS Accelerate menyesuaikan konfigurasi. CloudWatch Untuk informasi lebih lanjut, lihat bagian berikut,CloudWatch detail perubahan konfigurasi.

Konfigurasi instans otomatis membuat perubahan atau penambahan pada profil dan CloudWatch konfigurasi instans IAM Anda.

Izin IAM mengubah detail

Setiap instans terkelola harus memiliki AWS Identity and Access Management peran yang mencakup kebijakan terkelola berikut:

- arn:aws:iam: :AWS:Kebijakan/Amazon SSMManaged InstanceCore
- arn:aws:iam: :aws:policy/ CloudWatchAgentServerPolicy
- arn:aws:iam: :aws:policy/ AMSInstance ProfileBasePolicy

Dua yang pertama adalah kebijakan AWS yang dikelola. Kebijakan yang dikelola AMS adalah:

AMSInstanceProfileBasePolicy

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "secretsmanager:CreateSecret",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:/ams/byoa/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:Encrypt"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Jika instans Anda sudah memiliki peran IAM terlampir, tetapi tidak ada kebijakan ini, AMS menambahkan kebijakan yang hilang ke peran IAM Anda. Jika instans Anda tidak memiliki peran IAM, AMS melampirkan peran AMSOSConfigurationCustomerInstanceProfileIAM. Peran AMSOSConfigurationCustomerInstanceProfileIAM memiliki semua kebijakan yang diwajibkan oleh AMS Accelerate.

> **Note**
>
> Jika batas profil instans default 10 tercapai, maka AMS meningkatkan batas menjadi 20, sehingga profil instance yang diperlukan dapat dilampirkan.

CloudWatch detail perubahan konfigurasi

Detail tambahan pada CloudWatch konfigurasi.

- CloudWatch lokasi file konfigurasi pada instance:
  - Windows:%ProgramData%\ Amazon\AmazonCloudWatchAgent\ amazon-cloudwatch-agent .json
  - Linux:/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/ams-percepate-config.json
- CloudWatch lokasi file konfigurasi 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
- Metrik yang dikumpulkan:
  - Windows:
    - AWS Systems Manager Agen SSM (CPU_usage)
    - CloudWatch Agen (CPU_usage)

    - Pemanfaatan ruang disk untuk semua disk (% ruang kosong)
    - Memori (% byte yang berkomitmen digunakan)
  - Linux:
    - AWS Systems Manager Agen SSM (CPU_usage)
    - CloudWatch Agen (CPU_usage)
    - CPU (cpu_usage_idle, cpu_usage_iowait, cpu_usage_user, cpu_usage_system)
    - Disk (used_percent, inodes_used, inodes_total)
    - Diskio (io_time, write_bytes, read_bytes, menulis, membaca)
    - Mem (mem_used_percent)
    - Swap (swap_used_percent)
- Log dikumpulkan:
  - 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

Offboard dari AMS Accelerate

AMS Accelerate menyediakan cara mudah untuk mengoperasikan lingkungan operasi kelas enterprise. Dan, AMS Accelerate menyediakan model operasi infrastruktur pendukung untuk AWS migrasi dan penggunaan. Namun, setelah menggunakan AMS Accelerate, Anda dapat memutuskan untuk di-source, atau menetapkan kembali tanggung jawab operasi AWS infrastruktur ke tim lain. Untuk melakukan ini, Anda harus melepaskan akun Anda dari layanan AMS.

Saat Anda melepaskan akun dari AMS Accelerate, AMS mentransfer semua tanggung jawab yang ditentukan dalam deskripsi layanan kami kembali kepada Anda. Misalnya, Anda tidak akan memiliki kemampuan untuk memotong insiden atau permintaan layanan ke AMS. Demikian pula, teknisi operasi dan otomatisasi kami tidak akan lagi memiliki akses ke akun Accelerate Anda, mencegah kami memulihkan kesehatan, ketersediaan, dan temuan keamanan dan kepatuhan. AWS Beban kerja Anda dapat terus berjalan di akun yang sama dengan AMS yang beroperasi.

Tim yang akan melakukan layanan operasi infrastruktur Anda ke depan harus disertakan untuk menentukan orang, alat, dan proses apa yang akan Anda gunakan setelah Accelerate offboarding Anda. AMS meninggalkan beberapa perkakas AMS seperti pagar pembatas dan log untuk memungkinkan pengembangan lingkungan dan model operasi “menjadi”. Tinjau dokumentasi berikut dengan seksama untuk memahami alat yang dapat terus Anda gunakan dan cara meminta untuk keluar dari akun.

AMS Mempercepat efek offboarding

Sambil bersiap untuk turun dari Accelerate, ingatlah pertimbangan berikut.

- Access: `ams-access-management` AWS CloudFormation Tumpukan yang mendefinisikan `ams-access-management` AWS Identity and Access Management peran tidak dihapus. Setelah offboarding, sumber daya ini tetap ada, tetapi tidak digunakan oleh komponen lain yang tertinggal. Anda dapat menghapus tumpukan dan peran sesuai keinginan Anda.
- Retensi sumber daya AMS: Setelah offboarding, beberapa sumber daya AMS tetap ada di akun Anda. Untuk melihat sumber daya mana yang dipertahankan dan apa yang dapat Anda lakukan dengannya, lihat `resource_inventory.zip`spreadsheet (terkompresi).
- Otomatisasi: Setelah offboarding, runbook otomatisasi AWS SSM yang dikuratori AMS, dan fungsi AWS Lambda, tidak lagi tersedia.
- Manajemen cadangan: AMS menggunakan manajemen cadangan untuk mengambil snapshot sumber daya Anda. Setelah offboarding, Anda dapat terus menggunakan jadwal pencadangan, frekuensi, dan periode retensi yang ditentukan AWS Backup kecuali untuk paket cadangan AMS; lihat. Pilih paket cadangan AMS AWS Identity and Access Management Sumber daya yang dibuat oleh AMS Backup Orchestrator dihapus, tetapi bukan brankas cadangan yang ditulis AMS dan kunci yang sesuai. AWS KMS Accelerate tidak lagi memantau pekerjaan cadangan atau melakukan tindakan restorasi selama insiden.
- Optimalisasi biaya: Setelah offboarding, Penjadwal Sumber Daya AMS dihapus. Penjadwal Sumber Daya AMS membantu Anda mengurangi biaya operasional dengan menghentikan sumber daya yang tidak digunakan dan memulainya kembali saat kapasitasnya diperlukan. AMS tidak terus memberikan rekomendasi pengoptimalan biaya. Untuk detail tentang Resource Scheduler, lihat Optimalisasi biaya dengan Penjadwal Sumber Daya AMS.
- Pakar yang ditunjuk: Setelah offboarding, Cloud Service Delivery Manager (CSDM) yang ditunjuk dan Cloud Architect (CA) tidak lagi memberikan panduan, melaporkan, atau mendorong keunggulan operasional dan keamanan untuk akun Accelerate off-board Anda.
- Manajemen insiden: Manajemen insiden adalah proses yang digunakan layanan AMS untuk menanggapi insiden yang Anda laporkan. Setelah offboarding, Accelerate tidak lagi mendeteksi dan menanggapi insiden, atau membantu tim Anda dalam menyelesaikan masalah. Anda tidak akan dapat bertukar insiden dan komunikasi permintaan layanan dengan Akselerasi dan Percepat akses konsol untuk akun Accelerate Anda dinonaktifkan.
- Pencatatan dan Pelaporan: Setelah offboarding, Anda menyimpan log yang disimpan sebagai hasil dari CloudWatch, CloudTrail, dan Log Aliran VPC. Anda dapat membiarkan konfigurasi layanan tersebut apa adanya untuk terus menghasilkan log; Namun, AMS tidak lagi memantau konfigurasi tersebut. Accelerate tidak lagi menyediakan laporan layanan bulanan yang merangkum metrik kinerja utama AMS. Anda menyimpan data yang dihasilkan dari Pelaporan Layanan Mandiri (SSR) (lihatLaporan layanan mandiri), tetapi Accelerate tidak menghasilkan yang baru.

- Pemantauan: Pemantauan adalah proses yang digunakan layanan AMS untuk melacak sumber daya Anda. Selama offboarding, AMS menghapus alat khusus AMS, seperti Manajer Alarm dan Tagger Sumber Daya, serta aturan EventBridge acara dan alarm apa pun yang digunakan AMS sebagai bagian dari garis dasar pemantauan AMS. CloudWatch Accelerate tidak akan lagi merespons alarm atau mengkonfigurasi yang baru setelah offboarding. Untuk detail tentang Manajer Alarm dan Tagger Sumber Daya, lihat Manajer Alarm dan Tagger Sumber Daya Berbasis Tag.
- Alat operasi: AMS Accelerate dapat menyediakan operasi berkelanjutan untuk infrastruktur beban kerja Anda di AWS. Setelah melakukan offboarding akun Accelerate, Anda tidak lagi memiliki akses ke alat seperti Resource Tagger untuk membantu Anda menandai sumber daya berdasarkan aturan, atau konfigurasi instans otomatis untuk menginstal agen yang diperlukan dalam instans Anda EC2 . CloudWatch dan Agen SSM pada instance dibiarkan di tempatnya dengan konfigurasi yang ada. Profil `AMSOSConfigurationCustomerInstanceRole` lAM dan `AMSInstanceProfileBasePolicy` yang terpisah dari instans Anda dan dihapus dari akun Accelerate Anda.
- Manajemen patch: Manajemen patch adalah proses yang digunakan layanan AMS untuk memperbarui EC2 instans Anda. Setelah offboarding, AMS tidak lagi membuat snapshot instance sebelum menambal, tidak lagi menginstal dan memantau instalasi patch, dan tidak lagi memberi tahu Anda tentang hasilnya. Anda mempertahankan garis dasar Patch dan snapshot yang dibuat di masa lalu. Selain itu, konfigurasi jendela pemeliharaan tambalan Anda tetap ada tetapi tambalan tidak lagi diinstal oleh Accelerate.
- Manajemen masalah: Setelah offboarding, Accelerate tidak lagi melakukan analisis untuk mengidentifikasi dan menyelidiki masalah dan untuk mengidentifikasi akar penyebabnya.
- Keamanan: Manajemen keamanan adalah proses yang digunakan layanan AMS untuk melindungi sumber daya Anda. Setelah offboarding, Anda menyimpan GuardDuty detektor dan temuan Amazon Anda, dan AWS Config aturan apa pun yang Anda buat. AWS Config aturan yang diterapkan oleh Accelerate dihapus. Mempercepat tidak lagi memantau, memperbaiki, atau melaporkan temuan dari alat ini.
- 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.

Offboarding dari AMS Accelerate dengan dependensi pada Alarm Manager dan Resource Tagger

AWS CloudFormation Tumpukan khusus yang menerapkan konfigurasi yang terkait dengan Manajer Alarm atau Tagger Sumber Daya, bersama dengan tumpukan konfigurasi Manajer Alarm dan Tagger Sumber Daya yang disediakan AMS, tetap ada di akun Anda saat Anda keluar dari AWS Managed Services.

Untuk menghapus tumpukan konfigurasi AMS selama proses offboarding, Anda harus menghapus dependensi dan referensi apa pun di Manajer Alarm atau Tagger Sumber Daya dari CloudFormation templat khusus sebelum memulai proses offboarding. Menghapus referensi membantu memastikan bahwa tumpukan dihapus dengan benar dari akun Anda saat Anda keluar dari AMS.

> **Important**
>
> Tinjau CloudFormation template Anda dengan cermat dan hapus referensi apa pun ke Manajer Alarm dan Tagger Sumber Daya sebelum Anda memulai proses offboarding. Kegagalan untuk melakukannya dapat mengakibatkan retensi tumpukan ini di akun Anda, bahkan setelah Anda keluar dari AMS. Perhatikan bahwa meskipun tumpukan ini berisi informasi konfigurasi khusus untuk Manajer Alarm dan Tagger Sumber Daya, keberadaannya tidak menimbulkan biaya atau biaya yang berkelanjutan.

Mendapatkan bantuan offboarding untuk akun Accelerate

AMS menutup akun Anda setelah menerima pemberitahuan setidaknya 30 hari melalui Permintaan Penghentian Layanan Akun AMS. Tanggal Pengakhiran Layanan adalah hari terakhir dari bulan kalender setelah berakhirnya periode pemberitahuan penghentian yang diperlukan 30 hari; asalkan, jika akhir periode pemberitahuan penghentian yang diperlukan jatuh setelah hari ke-20 bulan kalender, Tanggal Penghentian Layanan akan menjadi hari terakhir dari bulan kalender berikutnya.

Untuk meminta off-boarding akun, Anda harus:

1. Kirim permintaan resmi ke offboard akun menggunakan permintaan layanan. Satu permintaan layanan (SR) yang mendokumentasikan semua akun yang ingin Anda offboard, atau satu SR per akun.

   Dalam permintaan, berikan daftar akun IDs ke offboard, alasan offboarding, dan pertimbangan tambahan apa pun.
2. Beri tahu CSDM Anda tentang akun yang ingin Anda offboard dan minta bantuan mereka untuk menjalankan proses offboarding.

Pengaturan notifikasi di Accelerate

Komunikasi antara Anda dan AMS terjadi karena berbagai alasan:

- Acara yang dibuat oleh monitoring alerts
- Menambal notifikasi layanan, jika Anda telah memilih untuk menambahkan Patch
- Permintaan layanan dan laporan insiden
- AWS Pengumuman penting sesekali (CSDM Anda menghubungi Anda jika ada tindakan di pihak Anda diperlukan)

Semua notifikasi dikirim menggunakan email yang Anda berikan untuk notifikasi tambalan saat Anda berada di onboard. Jika tidak, notifikasi akan dikirim ke email default yang Anda berikan ke AMS saat Anda onboard. 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.

Anda dapat menggunakan daftar kontak bernama untuk notifikasi berbasis non-sumber daya, seperti peringatan berdasarkan atau GuardDuty Config AWS . Misalnya, Anda mungkin memiliki daftar bernama `SecurityContacts` dan nama lain`0perationsContacts`. AMS mengirimkan alarm dan pemberitahuan ke daftar ini.

Lihat AWS Config Laporan Kepatuhan Kontrol untuk detail selengkapnya.

Menandai AMS Accelerate

Sebagian besar fitur Accelerate (menambal, mencadangkan, memantau) menggunakan tag dan profil konfigurasi untuk memutuskan sumber daya mana yang akan dikelola, tindakan apa yang akan diterapkan, dan kapan menerapkannya. Tag adalah label yang Anda terapkan pada sumber daya. Profil konfigurasi berisi aturan berdasarkan tag tersebut.

Setiap fitur Accelerate memiliki persyaratan penandaan sendiri. Beberapa fitur mengharuskan Anda untuk menggunakan tag tertentu, sementara yang lain memungkinkan Anda untuk menggunakan salah satu dari Anda sendiri.

Untuk informasi tentang tag yang diperlukan, lihatTag yang dikelola pelanggan di Accelerate.

Untuk informasi tentang tag yang dapat ditentukan pelanggan, lihat Tag yang disediakan pelanggan di Accelerate

Daftar Isi

- Tag di AMS Accelerate
  - Apa itu tag?
  - Cara kerja penandaan
  - Tag yang dikelola pelanggan di Accelerate
    - Pemantauan dalam Mempercepat
    - Mengkonfigurasi tag untuk EC2 instance di Accelerate
    - Mengelola tag untuk backup di Accelerate
  - Tag yang dikelola akselerasi
  - Tag yang disediakan pelanggan di Accelerate
- Alat manajemen tag untuk Mempercepat
  - Mempercepat Tagger Sumber Daya
    - Apa itu Resource Tagger?
    - Bagaimana Resource Tagger bekerja
    - Profil Konfigurasi Resource Tagger di AMS Accelerate
      - Sintaks dan struktur
    - Kasus penggunaan Resource Tagger di AMS Accelerate
      - Melihat tag yang diterapkan oleh Resource Tagger

        - Menggunakan Resource Tagger untuk membuat tag
        - Mencegah Resource Tagger dari memodifikasi sumber daya
        - Contoh profil konfigurasi
        - Menggabungkan konfigurasi default
        - Menonaktifkan konfigurasi default
        - Menghapus tag yang diterapkan oleh Resource Tagger
        - Melihat atau membuat perubahan pada konfigurasi Resource Tagger
        - Menerapkan perubahan konfigurasi
        - Mengonfigurasi Terraform untuk mengabaikan tag Resource Tagger
        - Melihat jumlah sumber daya yang dikelola oleh Resource Tagger
    - Menggunakan CloudFormation untuk membuat tag untuk AMS Accelerate
        - AWS CloudFormation Kasus penggunaan untuk AMS Accelerate
            - Menandai EC2 instance dengan AWS CloudFormation Accelerate
            - Menandai AutoScaling Grup (ASG) dengan AWS CloudFormation for Accelerate
            - Menerapkan profil konfigurasi dengan AWS CloudFormation untuk Accelerate
    - Menggunakan Terraform untuk membuat tag untuk AMS Accelerate

Tag di AMS Accelerate

Daftar Isi

- Apa itu tag?
- Cara kerja penandaan
- Tag yang dikelola pelanggan di Accelerate
    - Pemantauan dalam Mempercepat
    - Mengkonfigurasi tag untuk EC2 instance di Accelerate
    - Mengelola tag untuk backup di Accelerate
- Tag yang dikelola akselerasi
- Tag yang disediakan pelanggan di Accelerate

Apa itu tag?

Tag adalah label yang Anda tetapkan ke AWS sumber daya. Setiap tag terdiri dari kunci dan nilai opsional, yang keduanya Anda tetapkan.

Anda menggunakan tag untuk mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Misalnya, Anda dapat menentukan satu set tag untuk EC2 instans Amazon akun Anda, yang membantu Anda melacak setiap pemilik instans dan tingkat tumpukan.

Tag tidak memiliki arti semantik ke Amazon EC2 dan ditafsirkan secara ketat sebagai serangkaian karakter.

Untuk mempelajari lebih lanjut, lihat Menandai AWS sumber daya.

Cara kerja penandaan

Ada beberapa cara untuk menerapkan tag ke sumber daya Anda. Anda dapat menandai sumber daya secara langsung di konsol setiap AWS layanan saat membuat sumber daya; menggunakan Editor AWS Tag untuk menambah, menghapus, atau mengedit tag untuk beberapa sumber daya; atau menggunakan alat penyediaan seperti tag AWS CloudFormation Sumber Daya. AMS Accelerate juga menyediakan AMS Accelerate Resource Tagger yang Anda gunakan untuk menentukan aturan bagi pengelola siklus hidup tag otomatis. Untuk informasi tentang penggunaan Resource Tagger di AMS Accelerate, lihatMempercepat Tagger Sumber Daya. AMS Accelerate juga menyediakan tag yang disediakan pelanggan untuk menambah dan menghapus tag khusus ke sumber daya AMS Anda. Untuk informasi selengkapnya tentang tag yang disediakan pelanggan, lihat. Tag yang disediakan pelanggan di Accelerate

Tag yang dikelola pelanggan di Accelerate

Tag tertentu diperlukan untuk memicu berbagai tindakan Akselerasi AMS.

Daftar Isi

- Pemantauan dalam Mempercepat
- Mengkonfigurasi tag untuk EC2 instance di Accelerate
- Mengelola tag untuk backup di Accelerate

Pemantauan dalam Mempercepat

AMS Accelerate memantau sumber daya yang didukung untuk kesehatan, ketersediaan, dan keandalan. Untuk informasi selengkapnya tentang penawaran layanan ini, lihatPemantauan dan manajemen acara di AMS Accelerate.

AMS Mempercepat secara berkala onboard tambahan Layanan AWS untuk pemantauan dasar. Jika Anda menggunakan konfigurasi default Resource Tagger, pembaruan ini akan diterapkan secara otomatis ke akun Anda, dan perubahan akan ditampilkan ke sumber daya yang didukung.

Untuk ikut serta agar EC2 instans Amazon dikelola oleh AMS Accelerate, Anda harus menerapkan tag berikut melalui profil Kustomisasi di AppConfig; untuk informasi selengkapnya, lihat Langkah 3: Membuat konfigurasi dan profil konfigurasi.

Terapkan tag berikut ke sumber daya Anda:

Kunci	Nilai
ams:rt:ams-dikelola	true

Misalnya, Anda dapat membuat dokumen konfigurasi yang disesuaikan seperti ini untuk menerapkan tag ke semua sumber daya yang didukung AMS EC2 :

```
{
    "AWS::EC2::Instance": {
        "AllEC2": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Important**
>
> Ingatlah untuk menerapkan perubahan konfigurasi Anda setelah Anda membuatnya. Di SSM AppConfig, Anda harus menerapkan versi konfigurasi baru setelah membuatnya.

Layanan selain Amazon EC2 akan memiliki pemantauan dasar default. Untuk memilih keluar sumber daya Anda untuk dipantau oleh AMS Accelerate, Anda dapat menggunakan profil konfigurasi kustomisasi untuk mengecualikan sumber daya tertentu atau Layanan AWS. Ini memungkinkan Anda untuk mengontrol sumber daya mana yang harus memiliki tag pemantauan untuk menerapkan definisi alarm dasar. Lihat Kasus penggunaan Resource Tagger di AMS Accelerate.

Menggunakan Resource Tagger

Konfigurasi AMS Accelerate Resource Tagger di akun Anda membantu memastikan bahwa tag berikut diterapkan secara otomatis, jika Anda menerapkan tag yang satu ini (ams:rt:ams-managed).

Anda akan melihat tag berikut diterapkan ke sumber daya yang didukung untuk pemantauan dasar.

Kunci	Nilai	Aturan
am: rt: ams-monitoring-policy	ams-dipantau	Berlaku untuk semua EC2 sumber daya yang didukung oleh AMS
am: rt: ams-monitoring-policy-platform	ams-monitored-linux	Berlaku untuk semua EC2 instans Amazon yang menjalankan OS Linux
am: rt: ams-monitoring-policy-platform	ams-monitored-windows	Berlaku untuk semua EC2 instans Amazon yang menjalankan OS Windows

Untuk layanan lain yang didukung

Terapkan tag berikut ke sumber daya Anda, sesuai dengan aturan yang diberikan:

Kunci	Nilai	Aturan
am: rt: ams-monitoring-policy	ams-dipantau	Berlaku untuk semua sumber daya yang didukung oleh pemantauan AMS Accelerate.
am: rt: ams-monitoring-with-kms	ams-monitored-with-kms	OpenSearch Domain dengan KMS
am: rt: ams-monitoring-with-master	ams-monitored-with-master	OpenSearch Domain dengan Dedicated Master Node

Jika Anda tidak menggunakan Resource Tagger

Lihat bantuan Mempercepat tag tanpa Resource Tagger untuk menerapkan tag pemantauan yang benar menggunakan metode selain menggunakan AMS Resource Tagger.

Mengkonfigurasi tag untuk EC2 instance di Accelerate

AMS Accelerate mengelola agen di EC2 instans Amazon Anda, seperti agen SSM dan agen. CloudWatch Untuk informasi selengkapnya tentang penawaran layanan ini, lihat Konfigurasi instans otomatis di AMS Accelerate

Untuk ikut serta agar EC2 instans Amazon dikelola oleh AMS Accelerate, Anda harus menerapkan tag berikut ke instans Amazon EC2 Anda:

Kunci	Nilai
ams:rt:ams-dikelola	true

Mengelola tag untuk backup di Accelerate

AMS Accelerate mengelola cadangan sumber daya yang didukung. Untuk informasi selengkapnya tentang penawaran layanan ini, lihatManajemen kontinuitas di AMS Accelerate.

Manajemen cadangan AMS Accelerate menggunakan tag untuk mengidentifikasi sumber daya mana yang harus dicadangkan secara otomatis (dan juga menyediakan kemampuan pencadangan

manual). Anda dapat menggunakan kombinasi kunci tag: nilai apa pun untuk mengaitkan sumber daya Anda dengan paket cadangan. Untuk ikut serta dalam pencadangan otomatis menggunakan ams-default-backup-plan AWS Backup paket, Anda harus menerapkan tag berikut ke sumber daya yang didukung:

Kunci	Nilai
ams:rt:backup-orkestrator	true

> **Note**
>
> Selama orientasi, AMS Accelerate menandai semua sumber daya dengan ams:rt: backup-orchestrator-onboarding dengan nilai true untuk interval pendek, snapshot retensi pendek. Ini dikelola oleh rencana ams-onboarding-backup-plancadangan. Untuk informasi selengkapnya tentang AWS Backup paket yang dikelola AMS Accelerate, lihat. Pilih paket cadangan AMS

Tag yang dikelola akselerasi

Selama orientasi ke AMS Accelerate, beberapa AWS sumber daya diterapkan ke akun Anda. Jadi Anda dapat mengidentifikasi mereka, sumber daya ini ditandai dengan yang berikut:

Kunci	Nilai
AMS: Pemilik Sumber Daya	AMS
ams: resourceOwnerService	Deskripsi layanan AMS Accelerate mana yang menawarkan sumber daya ini berasal, misalnya, Penerapan AMS, Pencadangan, Kontrol, Pemantauan, Patch, dan sebagainya.
AppId	AMSInfrastructure
AppName	
Lingkungan	

> **Note**
>
> Tag ini diterapkan menggunakan tag AWS CloudFormation tingkat tumpukan, dan mengandalkan AWS CloudFormation penyebaran tag ke sumber daya yang dibuat. Untuk informasi selengkapnya, lihat Tag sumber daya.

Tag yang disediakan pelanggan di Accelerate

Apa itu tag yang disediakan pelanggan?

Tag yang disediakan pelanggan adalah fitur layanan AMS Accelerate yang digunakan untuk menentukan aturan yang mengatur cara sumber daya AMS ditandai di akun Anda. Dengan tag yang disediakan pelanggan, Anda dapat menambahkan tag kustom yang ditentukan pengguna ke sumber daya AMS yang diterapkan ke akun Anda. Fitur tag yang disediakan pelanggan secara otomatis ditambahkan ke akun yang diminta saat Anda meminta ke Cloud Service Delivery Manager (CSDM) menggunakan layanan otomatis. Perhatikan bahwa Anda tidak dapat mengganti tag AMS. Tag AMS dimulai dengan 'ams: '.

Anda dapat menentukan tag (label) Anda sendiri dan menentukan fungsionalitas tag ini untuk semua sumber daya AMS Accelerate Anda. Anda dapat memberikan tag ini sebelum Anda onboard ke AMS sehingga tag AMS dan tag kustom Anda diterapkan selama proses onbaording. Atau, Anda dapat memberikan tag setelah orientasi.

Bagaimana cara menambahkan tag yang disediakan pelanggan?

Untuk meminta penambahan tag ini ke sumber daya Anda, hubungi CSDM Anda. Tag ini akan diterapkan ke sumber daya AMS di akun Anda.

Apa ruang lingkup tag?

Fitur ini saat ini hanya tersedia untuk pelanggan Accelerate dan di Wilayah AWS komersial. Anda dapat menambahkan tag ke semua akun yang Anda miliki atau ke daftar akun tertentu.

> **Note**
>
> Tag ini hanya berlaku untuk sumber daya AMS dan tidak memengaruhi sumber daya Anda sendiri.

Alat manajemen tag untuk Mempercepat

Daftar Isi

- Mempercepat Tagger Sumber Daya
- Menggunakan CloudFormation untuk membuat tag untuk AMS Accelerate
- Menggunakan Terraform untuk membuat tag untuk AMS Accelerate

Mempercepat Tagger Sumber Daya

Dengan Resource Tagger, Anda dapat menentukan aturan untuk mengatur cara AWS sumber daya ditandai di akun Anda. Saat melakukan onboarding akun, AMS Accelerate menerapkan kebijakan penandaan Anda untuk memastikan sumber daya dalam akun terkelola Anda diberi tag.

Daftar Isi

- Apa itu Resource Tagger?
- Bagaimana Resource Tagger bekerja
- Profil Konfigurasi Resource Tagger di AMS Accelerate
  - Sintaks dan struktur
- Kasus penggunaan Resource Tagger di AMS Accelerate
  - Melihat tag yang diterapkan oleh Resource Tagger
  - Menggunakan Resource Tagger untuk membuat tag
  - Mencegah Resource Tagger dari memodifikasi sumber daya
  - Contoh profil konfigurasi
  - Menggabungkan konfigurasi default
  - Menonaktifkan konfigurasi default
  - Menghapus tag yang diterapkan oleh Resource Tagger
  - Melihat atau membuat perubahan pada konfigurasi Resource Tagger
  - Menerapkan perubahan konfigurasi
  - Mengonfigurasi Terraform untuk mengabaikan tag Resource Tagger
  - Melihat jumlah sumber daya yang dikelola oleh Resource Tagger

Apa itu Resource Tagger?

Resource Tagger adalah layanan AMS Accelerate yang menawarkan Anda gunakan untuk menentukan aturan untuk mengatur cara AWS sumber daya ditandai di akun Anda. Ini bertujuan untuk memberi Anda visibilitas lengkap tentang bagaimana tag Anda diterapkan ke AWS sumber daya Anda.

Resource Tagger secara otomatis membuat, memperbarui, dan menghapus tag pada AWS sumber daya yang didukung, berdasarkan aturan penandaan yang Anda tentukan di profil konfigurasi Anda. Misalnya, Anda dapat menentukan aturan yang menerapkan tag ke kumpulan EC2 instans Amazon, yang menunjukkan bahwa mereka harus dikelola oleh AMS Accelerate, yang mengakibatkan instans dipantau atau dicadangkan. Anda dapat menggunakan tag seperti ini untuk mengidentifikasi status kepatuhan AWS sumber daya berdasarkan kebijakan yang ditentukan di profil AWS AppConfig konfigurasi Anda. Untuk informasi selengkapnya, lihat AWS AppConfig.

AMS Accelerate menyediakan konfigurasi penandaan terkelola default sehingga sumber daya Anda dapat dipantau oleh AMS Accelerate. Anda menentukan sumber daya mana yang harus dikelola oleh AMS Accelerate, dan aturan penandaan terkelola memastikan bahwa sumber daya yang memiliki tag yang sesuai dipantau oleh AMS Accelerate.

Dengan Resource Tagger, jika Anda memilih, Anda dapat mengganti atau menonaktifkan tag terkelola AMS Accelerate default, memberikan aturan penandaan Anda sendiri untuk memenuhi kebijakan Anda, dan menggunakan mekanisme lain, seperti Terraform, untuk menghindari penyimpangan. Anda dapat menentukan pengecualian untuk skala, berdasarkan operasi Anda. Misalnya, Anda dapat menentukan kebijakan untuk menerapkan tag untuk semua EC2 instans Amazon dengan platform yang didukung (seperti Windows dan Linux), dan mengecualikan dari menandai instance tertentu. IDs

> **Important**
>
> Resource Tagger mengontrol semua tag di akun Anda yang memiliki awalan ams:rt:. Tag apa pun yang dimulai dengan awalan ini akan dihapus kecuali ada dalam aturan konfigurasi Resource Tagger. Untuk meringkas, tag apa pun pada sumber daya yang didukung yang dimulai dengan ams:rt: dianggap dimiliki oleh Resource Tagger. Jika Anda menandai sesuatu secara manual dengan, misalnya, ams:rt:, tag itu akan dihapus secara otomatis jika tidak ditentukan di salah satu profil konfigurasi Resource Tagger.

Bagaimana Resource Tagger bekerja

Saat akun Anda di-onboard ke AMS Accelerate, dua dokumen konfigurasi JSON akan di-deploy ke akun Anda. AWS AppConfig Dua dokumen, yang disebut profil Konfigurasi, adalah AMSManagedTag, disebut sebagai profil konfigurasi default, dan CustomerManagedTags, disebut sebagai profil konfigurasi kustomisasi. Anda menggunakan profil konfigurasi kustomisasi untuk menentukan kebijakan dan aturan Anda sendiri untuk akun Anda, dan itu tidak ditimpa oleh AMS Accelerate.

Kedua profil berada di aplikasi AMSResourceTagger, dan di lingkungan. AMSInfrastructure Semua tag yang diterapkan oleh tagger sumber daya memiliki key prefix ams:rt:.

Profil konfigurasi kustomisasi:

Profil konfigurasi kustomisasi awalnya kosong pada saat orientasi akun; Namun, aturan apa pun yang ditempatkan dalam dokumen profil diberlakukan, selain aturan di profil konfigurasi default. Setiap konfigurasi dalam profil konfigurasi kustomisasi sepenuhnya dikelola oleh Anda, dan tidak ditimpa oleh AMS Accelerate, kecuali oleh permintaan Anda.

Anda dapat menentukan aturan penandaan kustom yang Anda inginkan di profil konfigurasi kustom untuk AWS sumber daya yang didukung, dan Anda juga dapat menentukan modifikasi pada konfigurasi default AMS Accelerate-managed di sini, lihat. Kasus penggunaan Resource Tagger di AMS Accelerate

> **Important**
>
> Jika Anda memperbarui profil ini, Resource Tagger secara otomatis memberlakukan perubahan di semua sumber daya yang relevan di situs Anda. Akun AWS Perubahan diberlakukan secara otomatis, tetapi mungkin membutuhkan waktu hingga 60 menit untuk diterapkan.

Anda dapat memperbarui profil ini dengan menggunakan AWS Management Console, atau melalui alat AWS CLI/SDK. Untuk informasi tentang memperbarui profil konfigurasi kustomisasi, lihat panduan AWS AppConfig pengguna: Apa itu AWS AppConfig?

Profil konfigurasi default:

Dokumen profil konfigurasi default adalah internal AMS Accelerate dan berisi aturan default yang disediakan AMS Accelerate yang tidak dapat Anda ubah atau hapus secara permanen. Profil ini

dapat diperbarui kapan saja oleh AMS Accelerate dan tersedia bagi Anda untuk ditinjau; setiap perubahan yang Anda buat terhadapnya akan dihapus secara otomatis. Jika Anda ingin mengubah atau menonaktifkan salah satu aturan konfigurasi default yang Anda gunakan profil konfigurasi kustomisasi, lihatKasus penggunaan Resource Tagger di AMS Accelerate.

Profil Konfigurasi Resource Tagger di AMS Accelerate

Profil konfigurasi membantu memastikan bahwa tag diterapkan secara seragam ke sumber daya sepanjang masa sumber daya.

Sintaks dan struktur

Profil konfigurasi adalah objek JSON dengan struktur berikut:

```
{
   "Options": {
      "ReadOnly": false
   },
   "ResourceType": {
      "ConfigurationID": {
      "Enabled": true,
      "Filter": { ... },
      "Tags": [  ...  ]
      },
      "ConfigurationID": {
      ...
      }
   },
   "ResourceType": {
     ...
   }
}
```

Opsi: (opsional) Tentukan opsi untuk bagaimana Anda ResourceTagger ingin berperilaku. Menghilangkan blok sama dengan mengatur semua opsi ke nilai defaultnya. Lihat di bawah untuk pengaturan Opsi yang tersedia:

- ReadOnly: (opsional, default ke false): Menentukan ReadOnly mode untuk Resource Tagger. Setel ReadOnly ke true untuk menonaktifkan Resource Tagger yang membuat atau menghapus tag pada sumber daya AWS. Untuk informasi selengkapnya, lihat Mencegah Resource Tagger dari memodifikasi sumber daya.

ResourceType: Kunci ini harus berupa salah satu string yang didukung berikut, dan mewakili semua konfigurasi yang terkait dengan jenis sumber daya yang ditunjukkan:

- AWS::AutoScaling::AutoScalingKelompok
- AWS::DynamoDB::Table
- AWS::EC2::Instance
- AWS::EC2::NatGateway
- AWS::EC2:: VPNConnection
- AWS::EFS::FileSystem
- AWS::EKS::Cluster
- AWS::ElasticLoadBalancing::LoadBalancer
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::Elasticsearch::Domain
- AWS::FSx::FileSystem
- AWS::OpenSearch::Domain
- AWS: :RDS:: DBCluster
- AWS: :RDS:: DBInstance
- AWS::Redshift::Cluster
- AWS::S3::Bucket
- AWS::Synthetics::Canary

ConfigurationId: Kunci ini harus unik dalam dokumen profil, dan secara unik menamai blok konfigurasi berikut. Jika dua blok konfigurasi di blok yang sama memiliki ConfigurationId yang sama, ResourceTypeblok yang muncul terakhir di profil akan berlaku. Jika Anda menentukan ConfigurationId di profil penyesuaian Anda yang sama dengan yang ditentukan dalam dokumen default, blok konfigurasi yang ditentukan dalam profil penyesuaian akan berlaku.

> **Important**
>
> ConfigurationId harus ***not***tumpang tindih dengan profil AMS Accelerate; misalnya, itu tidak boleh AMSMonitoringLinux atau AMSMonitoringWindows, jika tidak maka akan menonaktifkan konfigurasi masing-masing profil konfigurasi Tags. AMSManaged

Diaktifkan (opsional, default ke true): Menentukan apakah blok konfigurasi berlaku. Setel ini ke false untuk menonaktifkan blok konfigurasi. Blok konfigurasi yang dinonaktifkan tidak berpengaruh.

Filter: Menentukan sumber daya yang konfigurasi berlaku. Setiap objek filter dapat memiliki salah satu (tetapi hanya satu) dari bidang berikut:

- AWS::AutoScaling::AutoScalingKelompok:
  - AutoScalingGroupName: Nama Grup Autoscaling. Bidang ini mendukung pencocokan wildcard.
- AWS::DynamoDB::Table:
  - TableName: Nama tabel DynamoDB. Bidang ini mendukung pencocokan wildcard.
- AWS::EC2::Instance:
  - AvailabilityZone: Filter cocok dengan EC2 instance di zona ketersediaan yang ditentukan. Bidang ini mendukung pencocokan wildcard, jadi *a cocok dengan us-east-1a, ap-northeast-1a, dan sebagainya.
  - InstanceId: Filter cocok dengan EC2 instance ID yang ditentukan. Bidang ini mendukung pencocokan wildcard, jadi i-00000* akan cocok dengan instance apa pun yang memiliki ID instance dimulai dengan i-00000.
  - Platform: Filter mencocokkan EC2 instance dengan platform yang ditentukan. Nilai yang valid adalah windows, linux atau wildcard* (untuk mencocokkan platform apa pun).
- AWS::EC2::NatGateway:
  - NatGatewayId: ID dari NAT Gateway. Bidang ini mendukung pencocokan wildcard.
  - Status: Status gateway NAT (tertunda | gagal | tersedia | menghapus | dihapus atau wildcard “*”)
  - VpcId: ID VPC tempat NAT Gateway berada. Bidang ini mendukung pencocokan wildcard.
  - SubnetId: ID Subnet di mana NAT Gateway berada. Bidang ini mendukung pencocokan wildcard
- AWS::EC2:: VPNConnection:
  - VpnConnectionId: ID koneksi. Bidang ini mendukung pencocokan wildcard.
- AWS::EFS::FileSystem:
  - FileSystemId: ID dari sistem file EFS. Bidang ini mendukung pencocokan wildcard.
- AWS::EKS::Cluster:
  - ClusterName: Nama cluster. Bidang ini mendukung pencocokan wildcard.
- AWS::ElasticLoadBalancing::LoadBalancer (Classic Load Balancer):
  - LoadBalancerName: LoadBalancer Nama. Bidang ini mendukung pencocokan wildcard.
  - Skema: Dapat berupa “menghadap internet”, “internal” atau wildcard “*”.

  - VPCId: VPCId Di mana loadbalancer digunakan, bisa menjadi wildcard “*”.
- AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer (ALB)):
  - LoadBalancerArn: Nama Sumber Daya LoadBalancer Amazon (ARN).
  - DNSName: DNSName Dari LoadBalancer. Bidang ini mendukung pencocokan wildcard.
  - LoadBalancerName: LoadBalancer Nama. Bidang ini mendukung pencocokan wildcard.
- AWS::Elasticsearch::Domain:
  - DomainId: DomainId ElasticSearch Sumber daya. Bidang ini mendukung pencocokan wildcard.
  - DomainName: DomainName ElasticSearch Sumber daya. Bidang ini mendukung pencocokan wildcard.
  - HasMasterNode: Nilai Boolean benar atau salah. Cocokkan jika Domain memiliki node master khusus.
  - HasKmsKeyNilai boolean benar atau salah. Cocokkan jika Domain memiliki kunci KMS untuk enkripsi saat istirahat.
- AWS::FSx::FileSystem:
  - FileSystemId: ID dari sistem FSx file. Bidang ini mendukung pencocokan wildcard.
- AWS::OpenSearch::Domain:
  - DomainId: DomainId OpenSearch Sumber daya. Bidang ini mendukung pencocokan wildcard.
  - DomainName: DomainName OpenSearch Sumber daya. Bidang ini mendukung pencocokan wildcard.
  - HasMasterNode: Boolean; Jika Domain memiliki node master khusus, ini dapat diatur ke true.
  - HasKmsKey: Jika Domain memiliki kunci KMS untuk enkripsi saat istirahat, ini dapat diatur ke true.
- AWS: :RDS::: DBCluster
  - DBClusterIdentifier: Filter mencocokkan pengidentifikasi cluster RDS dengan pengenal yang ditentukan. Bidang ini tidak mendukung pencocokan wildcard, jadi pengidentifikasi cluster harus ditentukan.
  - Mesin: Mesin yang digunakan oleh Instans RDS. Bidang ini mendukung pencocokan wildcard.
  - EngineVersion: Versi mesin. Bidang ini mendukung pencocokan wildcard.
- AWS: :RDS::: DBInstance
  - DBInstanceIdentifier: Filter cocok dengan instance RDS dengan ID instance yang ditentukan. Bidang ini tidak mendukung pencocokan wildcard, jadi pengidentifikasi instance harus ditentukan.

  - Mesin: Mesin yang digunakan oleh Instans RDS. Bidang ini mendukung pencocokan wildcard.
  - EngineVersion: Versi mesin. Bidang ini mendukung pencocokan wildcard.
- AWS::Redshift::Cluster:
  - ClusterIdentifier: Pengidentifikasi Cluster. Bidang ini mendukung pencocokan wildcard.
- AWS::S3::Bucket:
  - BucketName: Nama ember S3. Bidang ini mendukung pencocokan wildcard.
- AWS::Synthetics::Canary:
  - CanaryName: Nama kenari Synthetics.

Properti Filter lainnya:

- Tag: Filter berlaku untuk sumber daya apa pun yang sudah memiliki tag yang diberikan diterapkan. Nilai untuk properti ini harus berupa objek JSON dengan bidang berikut:
  - Key: Harus berupa string yang tepat, dan menentukan bahwa sumber daya harus memiliki tag dengan kunci yang tepat.
  - Nilai: Menentukan nilai yang cocok untuk tag. Mendukung wildcard, sehingga nilai Sample cocok dengan nilai apa pun yang diakhiri dengan string Sample.
- Fn: :AND: Sebuah array JSON dari objek JSON. Setiap objek mengikuti aturan yang sama dengan blok konfigurasi Filter. Ini menentukan bahwa filter cocok dengan sumber daya apa pun yang cocok dengan semua sub-filter.
- Fn: :OR: Sebuah array JSON dari objek JSON. Setiap objek mengikuti aturan yang sama dengan blok konfigurasi Filter. Ini menentukan bahwa filter cocok dengan sumber daya apa pun yang cocok dengan salah satu sub-filter.
- Fn: :NOT: Objek JSON yang mengikuti aturan yang sama dengan blok konfigurasi Filter. Ini menentukan bahwa filter secara eksplisit tidak cocok dengan sumber daya apa pun yang cocok dengan sub-filter. Gunakan ini untuk menentukan pengecualian pada aturan penandaan Anda.

Tag: Tag yang akan diterapkan ke sumber daya yang cocok. (Lihat Konvensi penamaan dan penggunaan tag.) Bidang ini adalah array pasangan kunci-nilai:

- Kunci: Kunci tag yang akan diterapkan.
- Nilai: Nilai tag yang akan diterapkan.

> **Note**
>
> Tag yang diterapkan oleh Resource Tagger selalu memiliki kunci yang dimulai dengan ams:rt:. Jika Anda tidak menentukan awalan ini di profil Anda, Resource Tagger menyisipkannya untuk Anda. Ini adalah bagaimana Resource Tagger membedakan tag yang dimilikinya dan dikelola dari tag yang digunakan oleh alat lain untuk tujuan lain.

Kasus penggunaan Resource Tagger di AMS Accelerate

Bagian ini mencantumkan tindakan yang umum dilakukan dengan Resource Tagger.

Melihat tag yang diterapkan oleh Resource Tagger

Semua tag yang diterapkan oleh Resource Tagger memiliki key prefix ams:rt:. Misalnya, definisi tag berikut menghasilkan tag dengan kunci AMS: rt:sampleKey dan nilai sampleValue. Semua tag dengan awalan ini diperlakukan sebagai bagian dari Resource Tagger.

```
{
 "Key": "sampleKey",
 "Value": "sampleValue"
}
```

> **Important**
>
> Jika Anda secara manual membuat tag Anda sendiri dengan awalan ams:rt:, itu dianggap dikelola oleh Resource Tagger. Ini berarti bahwa jika sumber daya dikelola oleh Resource Tagger, tetapi profil konfigurasi tidak menunjukkan bahwa tag harus diterapkan, maka Resource Tagger menghapus tag yang ditambahkan secara manual. Jika Anda secara manual menandai sumber daya yang dikelola oleh Resource Tagger, jangan gunakan awalan ams:rt: untuk kunci tag.

Menggunakan Resource Tagger untuk membuat tag

AMS Accelerate Resource Tagger adalah komponen yang digunakan di akun Anda selama orientasi AMS Accelerate. Resource Tagger memiliki seperangkat aturan yang dapat dikonfigurasi yang menentukan bagaimana sumber daya Anda harus ditandai, kemudian memberlakukan aturan

tersebut, secara otomatis menambahkan dan menghapus tag pada sumber daya untuk memastikan mereka mematuhi aturan Anda.

Jika Anda ingin menggunakan Resource Tagger untuk menandai sumber daya Anda, lihatMempercepat Tagger Sumber Daya.

Berikut ini adalah contoh cuplikan konfigurasi Resource Tagger yang menambahkan tag ams:rt:ams-managed dengan nilai true ke semua instance Amazon. EC2 Tag ams:rt:ams-managed memilih Anda agar sumber daya Anda dipantau oleh AMS Accelerate.

```
{
    "AWS::EC2::Instance": {
        "SampleConfigurationBlock": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> Berhati-hatilah saat menentukan nama untuk konfigurasi baru Anda (`SampleConfigurationBlock`dalam contoh yang diberikan) karena Anda mungkin secara tidak sengaja mengganti konfigurasi yang dikelola AMS dengan nama yang sama.

Mencegah Resource Tagger dari memodifikasi sumber daya

Resource Tagger dapat diatur ke mode read-only yang mencegahnya menambahkan atau menghapus tag apa pun pada sumber daya Anda. Ini berguna jika Anda ingin menyediakan mekanisme penandaan Anda sendiri.

Saat dalam mode hanya-baca, Resource Tagger masih memeriksa aturan penandaan yang ditentukan dalam profil konfigurasi terkelola dan pelanggan, dan memindai sumber daya yang tidak memenuhi aturan penandaan ini. Setiap sumber daya yang tidak sesuai akan muncul dengan. AWS Config Aturan AWS Config Yang bisa Anda cari memiliki `AMSResourceTagger-` awalan. Misalnya `AMSResourceTagger-EC2Instance` AWS Config aturan mengevaluasi jika tag yang sesuai dibuat untuk `AWS::EC2::Instance` sumber daya berdasarkan profil konfigurasi.

Resource Tagger berhenti pada titik ini, dan tidak membuat perubahan apa pun pada sumber daya Anda (tidak menambah atau menghapus tag).

Anda dapat mengaktifkan mode hanya-baca dengan memodifikasi profil konfigurasi pelanggan untuk menyertakan ReadOnlykunci di blok Opsi. Misalnya, cuplikan profil konfigurasi berikut menunjukkan tampilannya:

```
{
    "Options": {
        "ReadOnly": true
    },
    "AWS::EC2::Instance": {
        [... the rest of your configuration ...]
    }
}
```

Resource Tagger akan bereaksi terhadap konfigurasi baru ini segera setelah selesai digunakan, dan berhenti menambahkan dan menghapus tag pada sumber daya.

> **Note**
>
> Untuk mengaktifkan kembali modifikasi tag, ubah ReadOnlynilainya menjadi false, atau hapus kunci sama sekali, karena nilai defaultnya adalah false.

Untuk selengkapnya tentang pengaturan Opsi, lihatSintaks dan struktur, selanjutnya.

Contoh profil konfigurasi

Contoh dokumen profil berikut menetapkan bahwa semua EC2 instance Windows yang merupakan bagian dari CloudFormation tumpukan stack-* dikelola oleh AMS Accelerate; namun, secara eksplisit mengecualikan instance tertentu dengan ID i-000000000000001. EC2

```
{
```

```
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "Windows"
                    },
                    {
                        "Tag": {
                            "Key": "aws:cloudformation:stack-name",
                            "Value": "stack-*"
                        }
                    },
                    {
                        "Fn::NOT": {
                            "InstanceId": "i-00000000000000001"
                        }
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> Berhati-hatilah saat menentukan nama untuk konfigurasi baru Anda (`SampleConfigurationBlock`dalam contoh yang diberikan) karena Anda mungkin secara tidak sengaja mengganti konfigurasi yang dikelola AMS dengan nama yang sama.

Menggabungkan konfigurasi default

Profil konfigurasi default disediakan oleh AMS Accelerate pada saat orientasi akun. Profil ini menyediakan aturan default yang diterapkan di akun Anda.

Meskipun Anda tidak dapat mengubah profil konfigurasi default, Anda dapat memberikan penggantian ke default dengan menentukan blok konfigurasi di profil konfigurasi kustomisasi Anda dengan ConfigurationId yang sama dengan blok konfigurasi default. Jika Anda melakukan ini, blok konfigurasi Anda akan menimpa blok konfigurasi default.

Misalnya, pertimbangkan dokumen konfigurasi default berikut:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

Untuk mengubah nilai tag yang diterapkan di sini dari `SampleValueA` ke`SampleValueB`, dan menerapkan tag ke semua instance, bukan hanya instance Windows, Anda akan memberikan profil konfigurasi penyesuaian berikut:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "*"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueB"
   }]
  }
 }
}
```

> **Important**
>
> Ingatlah untuk menerapkan perubahan konfigurasi Anda setelah Anda membuatnya. Untuk informasi selengkapnya, lihat Menerapkan perubahan konfigurasi. Di SSM AppConfig, Anda harus menerapkan versi konfigurasi baru setelah membuatnya.

Menonaktifkan konfigurasi default

Anda dapat menonaktifkan aturan konfigurasi default dengan menambahkan blok konfigurasi dengan ConfigurationId yang sama ke profil konfigurasi kustomisasi Anda dan memberikan bidang Enabled untuk nilai false.

Misalnya, jika konfigurasi berikut ada di profil konfigurasi default:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

Anda dapat menonaktifkan aturan penandaan ini dengan memasukkan yang berikut dalam profil konfigurasi kustomisasi Anda:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": false
  }
 }
}
```

> **Important**
>
> Ingatlah untuk menerapkan perubahan konfigurasi setelah Anda membuatnya; untuk informasi, lihatMenerapkan perubahan konfigurasi. Di SSM AppConfig, Anda harus menerapkan versi konfigurasi baru setelah membuatnya.

Menghapus tag yang diterapkan oleh Resource Tagger

Tag apa pun yang diawali dengan ams:rt akan dihapus oleh Resource Tagger jika tag tidak ada di profil konfigurasi, atau, jika ada, di mana filter tidak cocok. Ini berarti Anda dapat menghapus tag yang diterapkan oleh Resource Tagger dengan melakukan salah satu hal berikut:

- Memodifikasi bagian konfigurasi kustomisasi yang mendefinisikan tag.
- Menambahkan pengecualian untuk sumber daya tertentu sehingga tidak lagi cocok dengan filter.

Misalnya: jika instance Linux memiliki tag berikut:

```
"Tags": [{
    "Key": "ams:rt:MyOwnTag",
    "Value": true
},{
    "Key": "myTag",
    "Value": true
}]
```

Dan Anda menerapkan profil konfigurasi Resource Tagger berikut:

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Platform": "Windows"
            },
            "Tags": [{
                "Key": "ams:rt:ams-managed",
                "Value": "true"
            }]
        }
```

```
    }
}
```

Resource Tagger bereaksi terhadap perubahan konfigurasi baru, dan satu-satunya tag pada instance menjadi:

```
"Tags": [{
    "Key": "myTag",
    "Value": true
}]
```

> **Warning**
>
> Berhati-hatilah saat menentukan nama untuk konfigurasi baru Anda (`SampleConfigurationBlock`dalam contoh yang diberikan) karena Anda mungkin secara tidak sengaja mengganti konfigurasi yang dikelola AMS dengan nama yang sama.

> **Important**
>
> Ingatlah untuk menerapkan perubahan konfigurasi setelah Anda membuatnya; untuk informasi, lihatMenerapkan perubahan konfigurasi. Di SSM AppConfig, Anda harus menerapkan versi konfigurasi baru setelah membuatnya.

Melihat atau membuat perubahan pada konfigurasi Resource Tagger

Dua profil konfigurasi JSON, AMSManagedTag dan CustomerManagedTags, yang diterapkan ke akun Anda AppConfig di AWS saat orientasi dan berada di aplikasi AMSResource Tagger, dan di AMSInfrastructurelingkungan, dapat ditinjau melalui API. AppConfig GetConfiguration

Berikut ini adalah contoh dari GetConfiguration panggilan ini:

```
aws appconfig get-configuration
 --application AMSResourceTagger
 --environment AMSInfrastructure
 --configuration AMSManagedTags
 --client-id ANY_STRING
 outfile.json
```

Aplikasi: unit AppConfig logis untuk menyediakan kemampuan, untuk Resource Tagger, ini adalah AMSResource Tagger.

- Lingkungan: AMSInfrastructure.
- Konfigurasi: Untuk melihat definisi tag default AMS Accelerate, nilainya adalah AMSManaged Tag, sedangkan untuk melihat definisi tag pelanggan, nilainya adalah CustomerManagedTags.
- ID Klien: Pengidentifikasi contoh aplikasi unik, ini bisa berupa string apa pun.
- Definisi tag kemudian dapat dilihat dalam file output yang ditentukan, dalam hal ini, outfile.json.

Definisi alarm kemudian dapat dilihat dalam file output yang ditentukan, dalam hal ini, outfile.json.

Anda dapat melihat versi konfigurasi mana yang digunakan ke akun Anda dengan melihat penerapan sebelumnya di lingkungan. AMSInfrastructure

Untuk mengganti aturan tag:

Salah satu aturan tag yang ada dapat diganti dengan memperbarui profil penyesuaian baik dengan AWS CloudFormation oleh Menerapkan profil konfigurasi dengan AWS CloudFormation untuk Accelerate atau, atau langsung menggunakan API using AppConfig. CreateHostedConfigurationVersion Menggunakan ConfigurationId yang sama sebagai aturan tag konfigurasi default mengesampingkan aturan default, dan menerapkan aturan kustom sebagai gantinya.

Untuk menyebarkan perubahan yang dibuat pada CustomerManagedTagsdokumen:

Setelah Anda membuat perubahan pada profil konfigurasi penyesuaian, Anda harus menerapkan perubahan untuk mereka. Untuk menerapkan perubahan baru, AppConfig StartDeploymentAPI harus dijalankan menggunakan AWS AppConfig Konsol atau CLI.

Menerapkan perubahan konfigurasi

Setelah kustomisasi selesai, perubahan ini harus diterapkan melalui AWS AppConfig StartDeploymentAPI. Petunjuk berikut menunjukkan cara menerapkan menggunakan. AWS CLI Selain itu, Anda dapat menggunakan AWS Management Console untuk membuat perubahan ini. Untuk selengkapnya, lihat Langkah 5: Menerapkan konfigurasi.

```
aws appconfig start-deployment
--application-id <application_id>
--environment-id <environment_id>
--deployment-strategy-id <deployment_strategy_id>
```

```
--configuration-profile-id <configuration_profile_id>
--configuration-version 1
```

- ID Aplikasi: ID aplikasi AMSResource Tagger aplikasi. Dapatkan ini dengan panggilan ListApplicationsAPI.
- ID Lingkungan: ID lingkungan; dapatkan ini dengan panggilan ListEnvironmentsAPI.
- ID Strategi Penerapan: ID strategi penerapan; dapatkan ini dengan panggilan ListDeploymentStrategiesAPI.
- ID Profil Konfigurasi: ID profil konfigurasi dari CustomerManagedTags; dapatkan ini dengan panggilan ListConfigurationProfilesAPI.
- Versi Konfigurasi: Versi profil konfigurasi yang ingin Anda gunakan.

> **Important**
>
> Resource Tagger menerapkan tag seperti yang ditentukan dalam profil konfigurasi. Setiap modifikasi manual yang Anda buat (dengan AWS Management Console, atau CloudWatch CLI/SDK) ke tag sumber daya secara otomatis dikembalikan kembali, jadi pastikan perubahan Anda ditentukan melalui Resource Tagger. Untuk mengetahui tag mana yang dibuat oleh Resource Tagger, cari kunci tag yang diawali dengan. `ams:rt:`

Batasi akses ke penerapan dengan tindakan StopDeploymentAPI StartDeploymentdan pengguna tepercaya yang memahami tanggung jawab dan konsekuensi penerapan konfigurasi baru ke target Anda.

Untuk mempelajari lebih lanjut tentang cara menggunakan AWS AppConfig fitur untuk membuat dan menerapkan konfigurasi, lihat dokumentasi di Bekerja dengan AWS AppConfig.

Mengonfigurasi Terraform untuk mengabaikan tag Resource Tagger

Jika Anda menggunakan Terraform untuk menyediakan sumber daya Anda, dan Anda ingin menggunakan Resource Tagger untuk menandai sumber daya Anda, tag Resource Tagger dapat diidentifikasi sebagai drift oleh Terraform.

Anda dapat mengonfigurasi Terraform untuk mengabaikan semua tag Resource Tagger menggunakan blok konfigurasi siklus hidup, atau blok konfigurasi global ignore_tags. Untuk informasi selengkapnya, lihat dokumentasi Terraform tentang Penandaan Sumber Daya di Penandaan Sumber Daya.

Contoh berikut menunjukkan cara membuat konfigurasi global untuk mengabaikan semua tag yang dimulai dengan awalan `ams:rt:` tag Resource Tagger:

```
provider "aws" {
  # ... potentially other configuration ...

  ignore_tags {
    key_prefixes = ["ams:rt:"]
  }
}
```

Melihat jumlah sumber daya yang dikelola oleh Resource Tagger

Resource Tagger mengirimkan metrik setiap jam ke Amazon CloudWatch, di namespace. `AMS/ResourceTagger` Metrik dipancarkan hanya untuk jenis sumber daya yang didukung oleh Resource Tagger.

Nama Metrik	Dimensi	Deskripsi
ResourceCount	Komponen, ResourceType	Jumlah sumber daya (dari jenis sumber daya yang ditentukan) yang digunakan di wilayah ini. Unit: Hitungan
ResourcesMissingManagedTags	Komponen, ResourceType	Jumlah sumber daya (dari jenis sumber daya tertentu) yang memerlukan tag terkelola, sesuai dengan profil konfigurasi, tetapi belum diberi tag oleh Resource Tagger. Unit: Hitungan
UnmanagedResources	Komponen, ResourceType	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. Unit: Hitungan

Nama Metrik	Dimensi	Deskripsi
MatchingResourceCount	Komponen, ResourceType, ConfigClauseName	Jumlah sumber daya (dari jenis sumber daya tertentu) yang cocok dengan blok konfigurasi Resource Tagger. Agar sumber daya cocok dengan blok konfigurasi, blok harus diaktifkan dan sumber daya harus cocok dengan filter blok. Unit: Hitungan

Metrik ini juga dapat dilihat sebagai grafik, di dasbor AMS-Resource-Tagger-Reporting-. Untuk melihat dasbor, dari konsol CloudWatch manajemen Amazon, pilih AMS-Resource-Tagger-Reporting-Dashboard. Secara default, grafik di dasbor ini menampilkan data untuk periode 12 jam sebelumnya.

AMS Accelerate menyebarkan CloudWatch alarm ke akun Anda untuk mendeteksi peningkatan signifikan dalam jumlah sumber daya yang tidak dikelola, misalnya, sumber daya yang dikecualikan dari manajemen oleh AMS Resource Tagger. Operasi AMS akan menyelidiki peningkatan sumber daya yang tidak dikelola yang melebihi: baik tiga sumber daya dari jenis yang sama, atau peningkatan 50% atas semua sumber daya dari jenis yang sama. Jika perubahan tampaknya tidak disengaja, Operasi AMS dapat menghubungi Anda untuk meninjau perubahan tersebut.

Menggunakan CloudFormation untuk membuat tag untuk AMS Accelerate

Anda dapat menggunakan AWS CloudFormation untuk menerapkan tag di tingkat tumpukan (lihat AWS CloudFormation dokumentasi, tag sumber daya) atau di tingkat sumber daya individual (misalnya, lihat Menandai EC2 sumber daya Amazon Anda).

> **Important**
>
> Beberapa komponen layanan AMS Accelerate memerlukan tag dengan awalan ams:rt:. Resource Tagger percaya bahwa ia memiliki tag ini, dan akan menghapusnya jika tidak ada aturan konfigurasi Resource Tagger yang mengizinkannya. Anda selalu perlu menerapkan profil konfigurasi Resource Tagger untuk tag ini, bahkan jika Anda menggunakan AWS CloudFormation atau Terraform.

AWS CloudFormation Kasus penggunaan untuk AMS Accelerate

Bagian ini mencantumkan tindakan yang umum dilakukan dengan AWS CloudFormation.

Topik

- Menandai EC2 instance dengan AWS CloudFormation Accelerate
- Menandai AutoScaling Grup (ASG) dengan AWS CloudFormation for Accelerate
- Menerapkan profil konfigurasi dengan AWS CloudFormation untuk Accelerate

Menandai EC2 instance dengan AWS CloudFormation Accelerate

Berikut ini adalah contoh bagaimana Anda dapat menerapkan tag ams:rt:ams-managed dengan nilai true ke instance Amazon yang dikelola oleh. EC2 AWS CloudFormation Tag ams:rt:ams-managed memilih Anda agar sumber daya Anda dipantau oleh AMS Accelerate.

```
 Type: AWS::EC2::Instance

Properties:
  InstanceType: "t3.micro"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

Menandai AutoScaling Grup (ASG) dengan AWS CloudFormation for Accelerate

Berikut ini adalah contoh bagaimana Anda dapat menerapkan tag ams:rt:ams-managed dengan nilai true ke grup Auto Scaling yang dikelola oleh. AWS CloudFormation Perhatikan bahwa grup Auto Scaling akan menyebarkan tag ke EC2 instans Amazon yang dibuat olehnya. Tag ams:rt:ams-managed memilih Anda agar sumber daya Anda dipantau oleh AMS Accelerate.

```
  Type: AWS::AutoScaling::AutoScalingGroup
Properties:
  AutoScalingGroupName: "SampleASG"

  # ...other properties...
```

```
  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

Menerapkan profil konfigurasi dengan AWS CloudFormation untuk Accelerate

Jika Anda ingin menerapkan profil `CustomerManagedTags` konfigurasi Anda menggunakan AWS CloudFormation, Anda dapat menggunakan CloudFormation template berikut. Letakkan konfigurasi JSON yang Anda inginkan di `AMSResourceTaggerConfigurationVersion.Content` lapangan.

Saat Anda menerapkan template dalam CloudFormation Stack atau Stack Set, penyebaran `AMSResourceTaggerDeployment` sumber daya akan gagal jika Anda belum mengikuti format JSON yang diperlukan untuk konfigurasi. Lihat Sintaks dan struktur untuk detail tentang format yang diharapkan.

Untuk bantuan dalam menerapkan template ini sebagai kumpulan CloudFormation tumpukan atau tumpukan, lihat AWS CloudFormation dokumentasi yang relevan di bawah ini:

- Membuat tumpukan di AWS CloudFormation konsol
- Membuat tumpukan dengan AWS CLI
- Membuat set tumpukan

> **Note**
>
> Jika Anda menerapkan versi konfigurasi menggunakan salah satu templat ini, dan kemudian menghapus kumpulan CloudFormation tumpukan/tumpukan, versi konfigurasi templat akan tetap sebagai versi yang diterapkan saat ini, dan tidak ada penerapan tambahan yang akan dilakukan. Jika Anda ingin kembali ke konfigurasi default, Anda perlu menerapkan konfigurasi kosong secara manual (yaitu, hanya`{}`), atau memperbarui tumpukan Anda ke konfigurasi kosong, daripada menghapus tumpukan.

JSON

```
{
  "Description": "Custom configuration for the AMS Resource Tagger.",
  "Resources": {
    "AMSResourceTaggerConfigurationVersion": {
```

```
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "Content": "{\"Options\": {\"ReadOnly\": false}}",
        "ContentType": "application/json"
      }
    },
    "AMSResourceTaggerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSResourceTaggerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Resource Tagger.
Resources:
  AMSResourceTaggerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
```

```
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      Content: |
        {
          "Options": {
            "ReadOnly": false
          }
        }
      ContentType: application/json
  AMSResourceTaggerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      ConfigurationVersion:
        !Ref AMSResourceTaggerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-ResourceTagger-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-ResourceTagger-Configuration-EnvironmentId
```

Menggunakan Terraform untuk membuat tag untuk AMS Accelerate

Jika Anda tidak ingin menggunakan AMS Accelerate Resource Tagger, Anda dapat menerapkan tag Anda sendiri menggunakan Terraform. Namun, jika Anda tidak ingin menggunakan Resource Tagger karena penyimpangan dari definisi Terraform Anda, ada cara bagi Anda untuk menggunakan Resource Tagger dan mengabaikan penyimpangan yang ditimbulkannya; lihat. Mengonfigurasi Terraform untuk mengabaikan tag Resource Tagger

> **Important**
>
> Beberapa komponen layanan AMS Accelerate memerlukan tag dengan awalan ams:rt:. Resource Tagger percaya bahwa ia memiliki tag ini, dan menghapusnya jika tidak ada aturan konfigurasi Resource Tagger yang mengizinkannya. Anda harus menerapkan profil konfigurasi Resource Tagger untuk tag ini, bahkan jika Anda menggunakan AWS CloudFormation atau Terraform.

Berikut ini adalah contoh bagaimana Anda dapat menerapkan tag ams:rt:ams-managed dengan nilai true ke instance Amazon yang dikelola oleh Terraform. EC2 Tag ams:rt:ams-managed memilih Anda agar sumber daya Anda dipantau oleh AMS Accelerate.

```
  resource "aws_instance" "sample_linux_instance" {
    # ...ami and other properties...

    instance_type = "t3.micro"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

Berikut ini adalah contoh bagaimana Anda dapat menerapkan tag ams:rt:ams-managed dengan nilai true ke grup Auto Scaling yang dikelola oleh Terraform. Perhatikan bahwa grup Auto Scaling menyebarkan tag ke EC2 instans Amazon yang dibuat olehnya. Tag ams:rt:ams-managed memilih Anda agar sumber daya Anda dipantau oleh AMS Accelerate.

```
  resource "aws_autoscaling_group" "sample_asg" {
    # ...other properties...

    name = "terraform-sample"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

Untuk deskripsi tentang cara mengelola tag sumber daya yang dibuat Terraform, lihat. Mengonfigurasi Terraform untuk mengabaikan tag Resource Tagger

Laporan insiden, permintaan layanan, dan pertanyaan penagihan di AMS Accelerate

Dengan AMS Accelerate, Anda dapat meminta bantuan terkait masalah operasional dan permintaan kapan saja melalui AWS Support Center di AWS Management Console. Insinyur operasi AMS Accelerate tersedia untuk menanggapi insiden dan permintaan layanan Anda round-the-clock, dengan waktu respons Perjanjian Tingkat Layanan (SLAs) untuk layanan. AMS Accelerate operations engineer secara proaktif memberi tahu Anda tentang peringatan dan pertanyaan penting menggunakan mekanisme yang sama.

AMS Accelerate menyediakan berbagai layanan operasional untuk membantu Anda mencapai keunggulan operasional AWS. Untuk mendapatkan pemahaman cepat tentang bagaimana AMS membantu tim Anda mencapai keunggulan operasional secara keseluruhan AWS Cloud dengan beberapa kemampuan operasional utama kami termasuk round-the-clock helpdesk, pemantauan proaktif, keamanan, penambalan, pencatatan, dan pencadangan, lihat Diagram Arsitektur Referensi AMS.

Topik

- Manajemen insiden di AMS Accelerate
- Manajemen permintaan layanan di Accelerate
- Laporan insiden dan pengujian permintaan layanan di Accelerate
- Pertanyaan penagihan untuk AMS Accelerate

Manajemen insiden di AMS Accelerate

Di AMS Accelerate, Anda menggunakan file AWS Support Center Consoleuntuk mengajukan laporan insiden. Insiden adalah masalah Layanan AWS kinerja yang memengaruhi lingkungan terkelola Anda, sebagaimana ditentukan oleh AMS Accelerate atau Anda. Insiden yang diidentifikasi oleh tim AMS Accelerate 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 Akselerasi AMS menentukan apakah peristiwa tersebut tidak berdampak, atau insiden (gangguan atau degradasi layanan), atau masalah (akar penyebab yang mendasari satu atau lebih insiden).

> **Note**
>
> Tim AMS Accelerate juga menerima insiden yang dibuat oleh Anda secara terprogram menggunakan AWS Support API dengan kode layanan. `service-ams-operations-report-incident`

Untuk informasi tentang menggunakan Dukungan, lihat Memulai dengan Dukungan.

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.

Bagaimana respons dan resolusi insiden bekerja

AMS Accelerate menggunakan praktik terbaik manajemen insiden IT Service Management (ITSM) untuk memulihkan layanan, bila diperlukan, secepat mungkin.

Kami menyediakan follow-the-sun dukungan 24/7/365 melalui pusat operasi di seluruh dunia dengan operator khusus yang secara aktif mengawasi dasbor pemantauan dan antrian insiden.

Insinyur operasi kami menggunakan alat pelacak insiden internal untuk mengidentifikasi, mencatat, mengkategorikan, memprioritaskan, mendiagnosis, menyelesaikan, dan menutup insiden; kami memberi Anda pembaruan tentang semua aktivitas ini melalui Support Center dan melalui AWS Support API. AWS Operator kami memanfaatkan berbagai alat AWS pendukung internal untuk membantu semua aktivitas tersebut. Operator ini sangat akrab dengan infrastruktur yang didukung AMS Accelerate dan memiliki keterampilan teknis tingkat ahli untuk mengatasi masalah dukungan yang teridentifikasi. Jika operator kami membutuhkan bantuan, Dukungan Premium dan tim AWS layanan tersedia.

Setelah insiden Anda diterima oleh tim operasi AMS Accelerate, kami memvalidasi prioritas dan klasifikasi yang bekerja dengan Anda jika ada klarifikasi yang diperlukan. Misalnya, jika laporan insiden diklasifikasikan lebih baik sebagai permintaan layanan, laporan tersebut direklasifikasi dan tim permintaan layanan AMS Accelerate mengambil alih dan Anda diberi tahu. Jika insiden dapat diselesaikan oleh operator penerima, langkah-langkah diambil untuk menyelesaikan insiden dengan cepat. Operator AMS Accelerate berkonsultasi dengan dokumentasi internal untuk resolusi dan, jika diperlukan, meningkatkan insiden ke sumber daya pendukung lainnya sampai insiden tersebut diselesaikan. Setelah diselesaikan, tim operasi AMS Accelerate mendokumentasikan insiden dan resolusi untuk penggunaan di masa mendatang.

Dalam kasus di mana insiden tingkat keparahan kritis memengaruhi beban kerja kritis Anda, AMS Accelerate dapat merekomendasikan pemulihan infrastruktur. Seringkali ada trade-off antara pemecahan masalah dan hanya memulihkan dari cadangan fungsional yang diketahui, dan risiko serta dampak Anda dari downtime layanan adalah faktor penentu. Jika Anda memiliki waktu untuk menyelesaikan masalah, AMS Accelerate akan membantu Anda, dan manajer pengiriman layanan

cloud (CSDM) Anda mungkin terlibat, tetapi jika urgensi untuk memulihkan tinggi, AMS Accelerate dapat segera memulai pemulihan.

Bekerja dengan insiden di AMS Accelerate

Dari AWS Support Center, Anda dapat melakukan tugas-tugas berikut:

- Laporkan dan perbarui insiden. Untuk melaporkan insiden Akselerasi AMS, pilih Operasi AMS -- Laporkan Insiden dari menu Layanan.
- Dapatkan daftar, dan informasi terperinci tentang, semua insiden yang Anda kirimkan.
- Persempit pencarian Anda untuk insiden berdasarkan status dan filter lainnya.
- Tambahkan komunikasi dan lampiran file ke insiden Anda, dan tambahkan penerima email untuk korespondensi kasus.
- Memulai obrolan langsung atau meminta panggilan kembali pada insiden Anda.

> **Note**
>
> Fitur obrolan langsung bukan untuk acara keamanan; untuk masalah keamanan, buat kasus dukungan prioritas tinggi (P1 atau P2).

- Selesaikan insiden.
- Nilai komunikasi insiden.

Contoh berikut menjelaskan penggunaan Support Center untuk mengirimkan insiden. Setelah dikirimkan, tim AMS Accelerate bekerja dengan Anda untuk menyelesaikan insiden sesuai standar AMS Accelerate SLA.

Mengirimkan insiden untuk Accelerate

Untuk melaporkan insiden menggunakan Support Center, lihat dokumentasi dukungan: Membuat kasus dukungan

Untuk melaporkan insiden menggunakan Dukungan pusat:

1. Klik Buat kasus. Halaman buat kasus insiden terbuka.
2. Buka menu Jenis masalah dukungan teknis dan pilih Operasi AMS -- Laporkan Insiden. Berikan informasi tentang insiden Anda dan pilih Buat.

3. Agar tetap mendapat informasi melalui email pada setiap langkah proses penyelesaian insiden, pastikan untuk mengisi opsi Email CC; jika Anda terhubung dengan federasi, masuk sebelum mengikuti tautan di email yang dikirimkan AMS Accelerate kepada Anda tentang insiden tersebut.

> **Note**
>
> Buat deskripsi Anda sedetail mungkin. Sertakan informasi sumber daya yang relevan, serta hal lain yang dapat membantu kami memahami masalah Anda. Misalnya, untuk memecahkan masalah kinerja, termasuk stempel waktu dan log. Untuk permintaan fitur atau pertanyaan panduan umum, sertakan deskripsi lingkungan dan tujuan Anda. Dalam semua kasus, ikuti Description Guidance (Panduan Deskripsi) yang muncul di formulir pengajuan kasus Anda. Ketika Anda memberikan detail sebanyak mungkin, Anda meningkatkan kemungkinan kasus Anda dapat diselesaikan dengan cepat.

Anda juga dapat menggunakan AWS Support API dengan kode layanan `service-ams-operations-report-incident` untuk melaporkan insiden.

Memantau dan memperbarui insiden Accelerate

Anda dapat memperbarui, memantau, dan meninjau laporan insiden dan permintaan layanan, baik yang disebut kasus, dengan menggunakan Support Center, atau secara terprogram menggunakan Dukungan API, `DescribeCases`operasi.

Untuk memantau kasus, insiden, atau permintaan layanan, menggunakan Dukungan Center, ikuti langkah-langkah berikut.

1. Di konsol AWS Manajemen, telusuri ke Support.
2. Dari navigasi kiri, pilih Kasus dukungan Anda, telusuri kasus dan pilih tautan Subjek untuk membuka halaman detail dengan status dan korespondensi saat ini.

   Jika Anda ingin menggunakan telepon atau obrolan pada saat ini, klik Buka kasus di Pusat Dukungan untuk membuka halaman Buat kasus di Dukungan Tengah, diisi otomatis dengan jenis layanan AMS.

   Ketika kasus insiden atau permintaan layanan yang dilaporkan diperbarui oleh tim Percepat operasi, Anda menerima email dan tautan ke insiden di Pusat Dukungan sehingga Anda dapat merespons.

> **Note**
>
> Anda tidak dapat menanggapi korespondensi kasus dengan membalas email.

Jika ada banyak kasus di dasbor, Anda dapat menggunakan opsi Filter:

- Subjek: Gunakan filter ini untuk mencari kata kunci dalam subjek kasus.
- Keparahan: Gunakan ini untuk memfilter kasus berdasarkan tingkat keparahan dengan memilih tingkat keparahan dari daftar.
- Jenis kasus: Gunakan ini untuk melihat semua kasus dari jenis kasus tertentu. Percepatan insiden dan permintaan layanan muncul di bawah Jenis Kasus Dukungan Teknis bersama dengan kasus khusus layanan apa pun.
- Status: Gunakan ini untuk memfilter kasus berdasarkan status dengan memilih status tertentu dari daftar.

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 Accelerate dengan API dukungan

Anda dapat menggunakan Dukungan API untuk membuat insiden dan menambahkan korespondensi dengan Dukungan staf selama penyelidikan atas masalah Anda. Dukungan API memodelkan sebagian besar perilaku AWS Support Center.

Untuk informasi tentang Anda dapat menggunakan layanan AWS dukungan ini, lihat Memprogram Kehidupan Kasus AWS Dukungan.

> **Note**
>
> Tim AMS Accelerate menerima insiden yang dibuat oleh Anda secara terprogram menggunakan kode layanan with. `service-ams-operations-report-incident`

Menanggapi insiden yang dihasilkan AMS Accelerate

AMS Accelerate secara proaktif memonitor sumber daya Anda. Untuk informasi selengkapnya, lihat Pemantauan dan manajemen acara di AMS Accelerate. Terkadang AMS Accelerate mengidentifikasi dan menciptakan insiden, paling sering untuk memberi tahu Anda tentang suatu peristiwa. Jika tindakan dari pihak Anda diperlukan untuk menyelesaikan suatu insiden, pemberitahuan akan dikirim oleh tim AMS Accelerate ke informasi kontak yang Anda berikan untuk akun tersebut. Anda menanggapi pemberitahuan ini dengan cara yang sama seperti insiden lainnya—biasanya melalui Support Center, meskipun dalam beberapa kasus kontak melalui email atau telepon diperlukan.

> **Important**
>
> Untuk menerima pemberitahuan perubahan status untuk kasus insiden atau permintaan layanan, masukkan alamat email di bidang alamat.

Tonton video Akshay untuk mempelajari lebih lanjut (4:15)

Manajemen permintaan layanan di Accelerate

Topik

- Kapan menggunakan permintaan layanan untuk Accelerate
- Cara kerja manajemen permintaan layanan di Accelerate
- Membuat permintaan layanan di Accelerate
- Memantau dan memperbarui permintaan layanan untuk Accelerate
- Mengelola permintaan layanan dengan API dukungan untuk Accelerate
- Menanggapi permintaan layanan yang dihasilkan AMS Accelerate

AMS Accelerate menggunakan manajemen permintaan layanan untuk merekam, menindaklanjuti, mengkomunikasikan kemajuan, dan memberikan pemberitahuan permintaan layanan aktif.

Tujuan dari proses manajemen permintaan layanan adalah untuk memastikan bahwa layanan terkelola Anda memberikan apa yang Anda butuhkan.

Untuk kueri terkait penagihan, buat permintaan layanan.

> **Note**
>
> Tim AMS Accelerate menerima permintaan layanan yang dibuat oleh Anda secara terprogram menggunakan AWS Support API dengan kode layanan. `service-ams-operations-service-request`

Menggunakan AWS Support Center, Anda dapat melakukan tugas-tugas berikut:

- Laporkan dan perbarui permintaan layanan. Untuk permintaan layanan AMS Accelerate, pilih Operasi AMS -- Permintaan Layanan dari menu Layanan.
- Dapatkan daftar, dan informasi terperinci tentang, semua permintaan layanan yang Anda kirimkan.
- Persempit pencarian Anda untuk permintaan layanan berdasarkan status dan filter lainnya.
- 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 untuk Accelerate

Contoh berikut menjelaskan permintaan layanan. Setelah Anda mengirimkan permintaan layanan, tim AMS Accelerate bekerja sama dengan Anda untuk menyelesaikan permintaan per AMS SLA Anda.

- 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

Cara kerja manajemen permintaan layanan di Accelerate

Permintaan layanan ditangani oleh tim operasi Accelerate AMS on-call.

Setelah permintaan layanan Anda diterima oleh tim operasi Akselerasi AMS, permintaan tersebut akan ditinjau untuk memastikan bahwa permintaan layanan tersebut diklasifikasikan dengan benar sebagai permintaan layanan atau insiden. Jika direklasifikasi sebagai insiden, proses manajemen insiden AMS Accelerate dimulai dan Anda akan dikirimi pemberitahuan.

Jika operator AMS Accelerate 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 Accelerate, operator mengirimkan permintaan ke manajer pengiriman layanan cloud Anda, sehingga mereka dapat berkomunikasi dengan Anda, atau ke tim AWS dukungan yang sesuai, bersama dengan email kepada Anda tentang langkah-langkah apa yang sedang diambil.

Permintaan layanan tidak diselesaikan sampai Anda telah menunjukkan bahwa Anda puas dengan hasilnya.

> **Note**
>
> Kami menyarankan Anda memberikan email kontak, nama, dan nomor telepon dalam semua kasus untuk memfasilitasi komunikasi.

Membuat permintaan layanan di Accelerate

Untuk membuat permintaan layanan, ikuti langkah-langkah berikut:

1. Dari konsol AMS Accelerate, telusuri ke Dasbor.
2. Pilih Buka permintaan layanan, AMS — Permintaan Layanan telah dipilih sebelumnya.
3. Pilih Kategori.
4. Pilih Keparahan (Hanya tingkatan Plus atau Premium).
5. Masukkan informasi untuk:

   - Subjek: Judul deskriptif untuk permintaan layanan.
   - Deskripsi: Deskripsi komprehensif tentang permintaan layanan, sistem yang terkena dampak, dan hasil resolusi yang diharapkan.
6. Untuk menambahkan lampiran, pilih Lampirkan file, telusuri lampiran yang Anda inginkan, dan pilih Buka. Untuk menghapus lampiran, pilih ikon hapus
7. Hubungi kami: Kontak default AMS melalui web. Untuk memilih opsi lain:

   - Bahasa kontak pilihan: Bahasa Inggris adalah bahasa yang didukung untuk permintaan layanan AMS Accelerate.
   - Web: Permintaan layanan Anda dikirimkan melalui web dan ditangani oleh tim operasi AMS.
   - Obrolan: Mengobrol online dengan perwakilan operasi AMS Accelerate. Opsi ini menambahkan Anda ke antrian obrolan.
   - Telepon: Perwakilan operasi AMS menelepon Anda kembali. Masukkan Wilayah AWS, nomor telepon, dan ekstensi Anda jika berlaku.
   - Kontak tambahan: Masukkan alamat email tambahan yang ingin disalin pada permintaan layanan Anda.
8. Pilih Kirim.

   Halaman detail kasus terbuka dengan informasi tentang permintaan layanan, seperti Jenis, Subjek, Dibuat, ID, dan Status. Plus, area Korespondensi yang mencakup deskripsi permintaan yang Anda buat.

   Untuk membuka area korespondensi dan memberikan rincian tambahan atau pembaruan status, pilih Balas.

   Setelah permintaan layanan diselesaikan, pilih Selesaikan Kasus.

   Jika ada begitu banyak korespondensi sehingga tidak semuanya muncul di halaman, pilih Muat Lainnya.

Pastikan untuk menilai layanan melalui peringkat bintang 1-5 untuk memberi tahu AMS bagaimana keadaan kami.

> **Note**
>
> Jika Anda akan menguji fungsionalitas permintaan layanan, kami sarankan Anda menambahkan tanda tanpa tindakan ke subjek permintaan layanan Anda, seperti`AMSTestNoOpsActionRequired`. Kemudian Anda dapat menguji tanpa memulai proses resolusi permintaan layanan.
> Tim AMS Accelerate menerima permintaan layanan yang dibuat oleh Anda secara terprogram menggunakan AWS Support API dengan kode layanan. `service-ams-operations-service-request`

Memantau dan memperbarui permintaan layanan untuk Accelerate

Untuk memantau kasus, insiden, atau permintaan layanan, menggunakan Dukungan Center, ikuti langkah-langkah berikut.

1. Di konsol AWS Manajemen, telusuri ke Support.
2. Dari navigasi kiri, pilih Kasus dukungan Anda, telusuri kasus dan pilih tautan Subjek untuk membuka halaman detail dengan status dan korespondensi saat ini.

   Jika Anda ingin menggunakan telepon atau obrolan pada titik ini, klik Buka kasus di Pusat Dukungan untuk membuka halaman Buat kasus di Dukungan Tengah, diisi otomatis dengan jenis layanan AMS.

   Ketika kasus insiden atau permintaan layanan yang dilaporkan diperbarui oleh tim Percepat operasi, Anda menerima email dan tautan ke insiden di Pusat Dukungan sehingga Anda dapat merespons.

   > **Note**
   >
   > Anda tidak dapat menanggapi korespondensi kasus dengan membalas email.

   Jika ada banyak kasus di dasbor, Anda dapat menggunakan opsi Filter:

- Subjek: Gunakan filter ini untuk mencari kata kunci dalam subjek kasus.
- Keparahan: Gunakan ini untuk memfilter kasus berdasarkan tingkat keparahan dengan memilih tingkat keparahan dari daftar.
- Jenis kasus: Gunakan ini untuk melihat semua kasus dari jenis kasus tertentu. Percepatan insiden dan permintaan layanan muncul di bawah Jenis Kasus Dukungan Teknis bersama dengan kasus khusus layanan apa pun.
- Status: Gunakan ini untuk memfilter kasus berdasarkan status dengan memilih status tertentu dari daftar.

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 permintaan layanan dengan API dukungan untuk Accelerate

Anda dapat menggunakan AWS Support API untuk membuat permintaan layanan dan menambahkan korespondensi kepada mereka selama penyelidikan masalah dan interaksi Anda dengan staf AWS pendukung. API AWS dukungan memodelkan sebagian besar perilaku AWS Support Center.

Tim AMS juga menerima permintaan layanan yang dibuat oleh Anda secara terprogram menggunakan AWS Support API dengan kode service-ams-operations-service layanan -request.

Untuk informasi selengkapnya tentang cara menggunakan layanan AWS dukungan ini, lihat Memprogram Masa Pakai Kasus AWS Dukungan.

Menanggapi permintaan layanan yang dihasilkan AMS Accelerate

AMS Accelerate secara proaktif memantau sumber daya Anda; untuk informasi selengkapnya, lihatPemantauan dan manajemen acara di AMS Accelerate. Terkadang AMS Accelerate membuat permintaan layanan, atau pemberitahuan layanan untuk Anda, biasanya jika tindakan dari pihak Anda diperlukan untuk menyelesaikan permintaan layanan. Dalam hal ini, tim AMS Accelerate

mengirimkan pemberitahuan ke kontak yang telah Anda berikan untuk akun tersebut. Anda menanggapi permintaan layanan ini dengan cara yang sama seperti kasus lainnya—biasanya melalui Support Center, meskipun dalam beberapa kasus, korespondensi email atau telepon diperlukan.

> **Important**
>
> Untuk menerima pemberitahuan perubahan status untuk permintaan layanan atau kasus insiden, Anda harus telah memasukkan alamat email di bidang alamat. Pemberitahuan hanya masuk ke alamat email yang ditambahkan ke kasing saat dibuat.

Tautan dalam email notifikasi hanya berfungsi jika Anda menggunakan server email di jaringan federasi AMS Accelerate. Jika tidak, Anda dapat menanggapi korespondensi dengan membuka konsol AMS Accelerate Anda dan menggunakan halaman detail kasus.

> **Note**
>
> AMS Accelerate mengirimkan komunikasi ke alamat email utama Anda di AWS akun Anda; sebaiknya tambahkan alias email kontak operasi alternatif untuk memfasilitasi proses request/notification manajemen layanan. Ini tercakup selama proses orientasi AMS Accelerate dan dalam dokumentasi orientasi terkait.

Laporan insiden dan pengujian permintaan layanan di Accelerate

Saat menguji laporan insiden atau permintaan layanan, kami meminta Anda menyertakan AMSTestNoOpsActionRequireddalam teks subjek. Hal ini memungkinkan AMS tahu bahwa insiden atau permintaan hanya untuk pengujian. Ketika insinyur operasi AMS melihatnya, mereka tidak akan merespons dengan cara apa pun.

Pertanyaan penagihan untuk AMS Accelerate

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.

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 kegiatan terkait 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.
- Acara Keamanan Pelanggan: Acara keamanan yang direncanakan. Misalnya, 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 bantuan dengan kebutuhan spesifik Anda, hubungi CSDM Anda.

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 melalui Kasus: Permintaan Layanan (SRs) /Insiden selama acara PEM?

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

  Jika berlaku, Anda dapat menggunakan opsi kontak Langsung.
- 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 Kasus terkait PEM diajukan?

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

- Tautan ke detail PEM disediakan secara internal untuk insinyur AMS.

Apakah ada SLAs atau SLOs untuk permintaan PEM?

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

  Untuk informasi selengkapnya, lihat Laporan insiden, permintaan layanan, dan pertanyaan penagihan di AMS Accelerate.

Bisakah kita membuat PEM melalui Permintaan Layanan (SR)?

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

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 AWStempat 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 klaster 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 contol 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 mengharus kan pelanggan untuk menyediak an 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-en d prosedur yang diperlukan untuk memperbarui klaster 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 mempriori taskan 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.

Topik

- 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 dionboard 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

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 manajemen host AMS
- Laporan Cadangan AMS
- AWS Config Laporan Kepatuhan Kontrol
- Laporan Konfigurasi Respons Aturan Konfigurasi AMS Config
- Insiden Mencegah dan Memantau Laporan Pembicara Teratas
- Laporan Detail Biaya Penagihan

- Laporan Remediator Tepercaya

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 manajemen host AMS

Laporan yang tersedia

- Laporan Cakupan Agen SSM

Laporan Cakupan Agen SSM

Laporan Cakupan Agen SSM AMS 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 selengkap nya, 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
Titik Pemulihan ARN	ARN dari cadangan yang dibuat

Nama Bidang	Definisi
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_COVE RED”)
# sumber daya	Jumlah sumber daya yang didukung di akun
perc_cakupan	Persentase sumber daya yang didukung dengan cadangan yang dijalankan dalam 30 hari terakhir.

AWS Config Laporan Kepatuhan Kontrol

Laporan Kepatuhan AWS Config Kontrol memberikan pandangan mendalam tentang kepatuhan sumber daya dan AWS Config aturan akun AMS, Anda memfilter laporan berdasarkan Keparahan Aturan Konfigurasi untuk memprioritaskan temuan yang paling penting. Tabel berikut mencantumkan data yang disediakan oleh laporan ini:

Bidang	Deskripsi
Tanggal	Tanggal laporan
Nama pelanggan	Nama pelanggan
AWS ID akun	ID AWS akun terkait untuk pelanggan
Pengidentifikasi sumber	AWS Config aturan pengidentifikasi sumber unik
Deskripsi Aturan	AWS Config deskripsi aturan
Jenis Aturan	AWS Config jenis aturan
Bendera Kepatuhan	AWS Config negara kepatuhan aturan
Jenis Sumber Daya	AWS jenis sumber daya
Nama Sumber Daya	AWS nama sumber daya
Kepelikan	Tingkat keparahan default yang direkomen dasikan yang ditentukan oleh AMS untuk AWS Config aturan
Kategori Remediasi	Kategori respons remediasi terkait untuk suatu aturan AWS Config
Deskripsi Remediasi	Tindakan remediasi dijelaskan untuk membuat AWS Config aturan menjadi patuh
Tindakan pelanggan	Tindakan pelanggan diperlukan untuk membuat AWS Config aturan agar sesuai
Laporan metrik Delta	Perubahan kepatuhan aturan antara 2 tanggal yang diberikan

Laporan Konfigurasi Respons Aturan Konfigurasi AMS Config

Laporan Konfigurasi Respons Aturan Konfigurasi AMS memberikan pandangan mendalam tentang cara Anda mengonfigurasi Accelerate saat ini untuk merespons aturan konfigurasi AMS yang tidak sesuai. Untuk informasi selengkapnya tentang cara mengubah respons untuk aturan konfigurasi AMS, lihat AMS Mempercepat respons temuan yang disesuaikan.

Laporan ini hanya menampilkan konfigurasi yang telah Anda ubah, dan mengecualikan konfigurasi default AMS yang tercantum di Perpustakaan Aturan Konfigurasi AMS. Laporan ini menyediakan data tentang konfigurasi respons aturan konfigurasi sumber daya dan AMS akun AMS, termasuk yang berikut ini:

- Daftar AWS akun yang Anda ubah respons default untuk aturan konfigurasi AMS.
- Daftar tag yang Anda kaitkan respons untuk aturan konfigurasi AMS.
- Daftar konfigurasi respons untuk setiap aturan, akun, dan tag.
- Daftar sumber daya yang telah Anda ubah respons default untuk aturan konfigurasi AMS.

Laporan Konfigurasi Respons Terbaru

Bidang	Deskripsi
Tanggal	Tanggal di mana laporan dibuat
Nama pelanggan	Nama pelanggan
AWS ID akun	ID AWS akun yang terkait dengan konfigurasi
Nama Akun	AWS nama akun grup sumber daya tingkat akun
Menemukan Jenis	Jenis temuan yang diidentifikasi. Dalam hal ini, AWS Config
Pengidentifikasi Sumber	AWS Config Aturan Pengidentifikasi Sumber Unik
ID Grup Sumber Daya	ID Grup Sumber Daya yang terkait dengan konfigurasi respons

Bidang	Deskripsi
Tindakan Respons Dikonfigurasi	Jenis tindakan yang dipicu oleh AMS
SSM Runbook Terkait	Runbook Remediasi yang akan dijalankan, jika ada
Jenis Grup Sumber Daya	Ini bisa berupa Akun atau Tag

Sumber daya dengan Respons Default Kustom dari Aturan Config

Nama Bidang	Definisi
Nama Pelanggan	Nama pelanggan
Tanggal	Tanggal di mana laporan dibuat
AWS Nama Akun	AWS nama akun
account-id	ID AWS akun terkait
Aturan Konfigurasi AMS	Aturan konfigurasi AMS yang menargetkan sumber daya dan menerapkannya dengan konfigurasi
ID Sumber Daya	ID sumber daya di akun pelanggan yang ditargetkan oleh aturan konfigurasi AMS
Wilayah Sumber Daya	AWS Wilayah tempat konfigurasi diterapkan
Jenis Sumber Daya	AWS jenis sumber daya
ID Grup Sumber Daya	ID grup Sumber daya yang terkait dengan konfigurasi respons
Sumber Daya Bendera AMS	Jika AWS sumber daya digunakan oleh AMS, maka bidang ini disetel ke `True`

Nama Bidang	Definisi
Jenis Pemicu	Jenis respons yang dikonfigurasi untuk sumber daya
Bendera Kepatuhan	Status kepatuhan aturan konfigurasi AMS

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

Nama Bidang	Definisi
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 menghasil kan 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; adjusted_aws_charges * uplift_percent

Nama Bidang	Definisi
Instans Pengeluaran EC2 RDS	Belanjakan EC2 dan instans RDS
Biaya AMS	Total biaya AMS untuk produk; uplifted_ aws_charges + instance_ec2_rds_spend + uplifted_ris+uplifted_sp
Biaya Minimum Prorata	Jumlah yang kami kenakan untuk memenuhi minimum kontrak
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

Nama Bidang	Definisi
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
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

Nama Bidang	Definisi
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

Nama Bidang	Definisi
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.

Agar pengguna dapat melihat laporan Akselerasi AMS di konsol AMS, Anda harus memberikan izin eksplisit di AWS Identity and Access Management (IAM) untuk melakukan tindakan tersebut. Misalnya kebijakan IAM, lihat Izin untuk menggunakan fitur AMS.

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

- Ringkasan detail instance untuk penambalan AMS
- Detail tambalan

- Contoh yang melewatkan tambalan

Ringkasan detail instance untuk penambalan AMS

Ini adalah laporan informasi yang membantu mengidentifikasi semua instance yang terhubung ke AMS Patching, status akun, detail instans, 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

Nama Bidang Konsol	Nama Bidang Dataset	Definisi
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
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

Nama Bidang Konsol	Nama Bidang Dataset	Definisi
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 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
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)

Nama Bidang	Nama Bidang Dataset	Definisi
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)
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

Nama Bidang	Nama Bidang Dataset	Definisi
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
Durasi Jendela Pemeliharaan (jam)	window_duration	Durasi jendela pemeliharaan dalam beberapa jam
Cakupan Jendela Pemelihar aan	mw_covered_flag	Jika sebuah instance memiliki setidaknya satu jendela pemeliharaan yang diaktifka n 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”

Nama Bidang	Nama Bidang Dataset	Definisi
Noncompliant - Informasi	tidak patuh _informasional	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “informasional”
Tidak sesuai - Tidak ditentuka n	tidak patuh _tidak ditentukan	Hitungan tambalan yang tidak sesuai dengan tingkat keparahan “tidak ditentukan”
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, tergantun g 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)

Nama Bidang	Nama Bidang Dataset	Definisi
	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
	window_next _Exec_HHMI	Jam:Menit bagian dari window_next_execution_time

Contoh yang melewatkan tambalan

Laporan ini memberikan detail tentang instance yang melewatkan 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 ditambal, 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 Bidang	Nama Bidang Dataset	Definisi
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
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

Nama Bidang	Nama Bidang Dataset	Definisi
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

Nama Bidang	Nama Bidang Dataset	Definisi
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
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 pengenal unik
Nama Paket Backup	backup_plan_name	Nama Backup Plan

Nama Bidang	Nama Bidang Dataset	Definisi
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
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 berhari-hari

Nama Bidang	Nama Bidang Dataset	Definisi
Titik pemulihan pindah ke penyimpanan dingin setelah berhari-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
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

Nama Bidang	Nama Bidang Dataset	Definisi
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.

Nama Bidang	Nama Bidang Dataset	Definisi
Id Akun Admin	aws_admin_account_id	AWS Organizations Akun tepercaya 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.
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.

Nama Bidang	Nama Bidang Dataset	Definisi
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.
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”.

Nama Bidang	Nama Bidang Dataset	Definisi
Contoh IDs	instance_ids	Contoh yang terkait dengan insiden tersebut.
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 mengident ifikasi akun yang bertanggung jawab untuk membayar biaya AMS
ID Akun Tertaut	linked_account_id	ID 12 digit yang mengident ifikasi 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; adjusted_aws_charges * uplift_percent
Contoh Pengeluaran EC2 RDS	instances_ec2_rds_spend	Belanjakan 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; ris_charges * 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; sp_charges * uplift_percent
Biaya AMS	ams_charges	Total biaya ams untuk produk; uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris+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 tepercaya 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 tepercaya 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 menentuka n 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 tepercaya 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 menentuka n 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 pengident ifikasi 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 untuk AMS Patching	2 Bulan	2 Tahun
Detail Patch	2 Bulan	2 Tahun
Contoh yang melewatkan 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.

Manajemen akses di AMS Accelerate

Manajemen akses adalah bagaimana sumber daya Anda dilindungi dengan hanya mengizinkan akses yang diotorisasi dan diautentikasi. Dengan AMS Accelerate, Anda bertanggung jawab untuk mengelola akses ke sumber daya Anda Akun AWS dan sumber daya dasarnya, seperti solusi manajemen akses, kebijakan akses, dan proses terkait. Untuk membantu Anda mengelola solusi akses, AMS Accelerate menerapkan AWS Config aturan yang mendeteksi kesalahan konfigurasi IAM yang umum, lalu mengirimkan pemberitahuan remediasi. Kesalahan konfigurasi IAM yang umum adalah bahwa pengguna root memiliki kunci akses. Aturan `iam-root-access-key-check` konfigurasi memeriksa apakah kunci akses pengguna root tersedia dan sesuai atau jika kunci akses tidak ada. Untuk daftar aturan konfigurasi yang diterapkan oleh AMS, lihat library AWS Config Aturan AMS.

Topik

- Dapatkan akses ke konsol Accelerate
- Izin untuk menggunakan fitur AMS
- Mengapa dan kapan AMS mengakses akun Anda
- Bagaimana AMS mengakses akun Anda
- Bagaimana dan kapan menggunakan akun pengguna root di AMS

Dapatkan akses ke konsol Accelerate

Saat Anda melakukan onboard dengan Accelerate, Anda secara otomatis memiliki akses ke konsol Accelerate. Anda dapat mengakses konsol dengan mencari Managed Services di konsol manajemen AWS Anda. Konsol Accelerate memberi Anda tampilan ringkasan ke dalam fitur yang Anda miliki dengan Accelerate. Tampilan ini mencakup komponen individual yang disajikan di dasbor dan halaman konfigurasi.

Izin untuk menggunakan fitur AMS

Untuk memungkinkan pengguna membaca dan mengonfigurasi kemampuan AMS Accelerate, seperti mengakses Konsol AMS atau mengonfigurasi cadangan, Anda harus memberikan izin eksplisit ke peran IAM mereka untuk melakukan tindakan tersebut. AWS CloudFormation Templat berikut berisi kebijakan yang diperlukan untuk membaca dan mengonfigurasi layanan yang terkait dengan

AMS sehingga Anda dapat menetapkannya ke peran IAM Anda. Mereka dirancang agar selaras dengan tanggung jawab pekerjaan umum di industri TI, di mana izin Administrator atau Hanya Baca diperlukan; namun, jika Anda perlu memberikan izin yang berbeda kepada pengguna, Anda dapat mengedit kebijakan untuk menyertakan atau mengecualikan izin tertentu. Anda juga dapat membuat kebijakan khusus Anda sendiri.

Template menyediakan dua kebijakan. `AMSAccelerateAdminAccess`Kebijakan ini dimaksudkan untuk digunakan untuk menyiapkan dan mengoperasikan komponen AMS Accelerate. Kebijakan ini biasanya diasumsikan oleh admin TI dan memberikan izin untuk mengonfigurasi fitur AMS seperti patching dan backup. `AMSAccelerateReadOnly`Memberikan izin minimum yang diperlukan untuk melihat sumber daya terkait Akselerasi AMS.

```
AWSTemplateFormatVersion: 2010-09-09
Description: AMSAccelerateCustomerAccessPolicies

Resources:
  AMSAccelerateAdminAccess:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateAdminAccess
      Path: /
      PolicyDocument:
        Fn::Sub:
        - |
          {
            "Version": "2012-10-17",
            "Statement": [
              {
                 "Sid": "AmsSelfServiceReport",
                 "Effect": "Allow",
                 "Action": "amsssrv:*",
                 "Resource": "*"
              },
              {
                "Sid": "AmsBackupPolicy",
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/ams-backup-iam-role"
              },
              {
                "Sid": "AmsChangeRecordKMSPolicy",
                "Effect": "Allow",
```

```
                "Action": [
                  "kms:Encrypt",
                  "kms:Decrypt",
                  "kms:GenerateDataKey"
                ],
                "Resource": [
                  "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
                ],
                "Condition": {
                  "ForAnyValue:StringLike": {
                    "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
                  }
                }
              },
              {
                "Sid": "AmsChangeRecordAthenaReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "athena:BatchGetNamedQuery",
                  "athena:Get*",
                  "athena:List*",
                  "athena:StartQueryExecution",
                  "athena:UpdateWorkGroup",
                  "glue:GetDatabase*",
                  "glue:GetTable*",
                  "s3:GetAccountPublicAccessBlock",
                  "s3:ListAccessPoints",
                  "s3:ListAllMyBuckets"
                ],
                "Resource": "*"
              },
              {
                "Sid": "AmsChangeRecordS3ReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "s3:Get*",
                  "s3:List*"
                ],
                "Resource": [
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/
*",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
```

```
        ]
      },
      {
        "Sid": "AmsChangeRecordS3WritePolicy",
        "Effect": "Allow",
        "Action": [
          "s3:PutObject",
          "s3:PutObjectLegalHold",
          "s3:PutObjectRetention"

        ],
        "Resource": [
          "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
        ]
      },
      {
        "Sid": "MaciePolicy",
        "Effect": "Allow",
        "Action": [
          "macie2:GetFindingStatistics"
        ],
        "Resource": "*"
      },
      {
        "Sid": "GuardDutyPolicy",
        "Effect": "Allow",
        "Action": [
          "guardduty:GetFindingsStatistics",
          "guardduty:ListDetectors"
        ],
        "Resource": "*"
      },
      {
        "Sid": "SupportPolicy",
        "Effect": "Allow",
        "Action": "support:*",
        "Resource": "*"
      },
      {
        "Sid": "ConfigPolicy",
        "Effect": "Allow",
        "Action": [
          "config:Get*",
          "config:Describe*",
```

```
                "config:Deliver*",
                "config:List*",
                "config:StartConfigRulesEvaluation"
              ],
              "Resource": "*"
            },
            {
              "Sid": "AppConfigReadPolicy",
              "Effect": "Allow",
              "Action": [
                "appconfig:List*",
                "appconfig:Get*"
              ],
              "Resource": "*"
            },
            {
              "Sid": "AppConfigPolicy",
              "Effect": "Allow",
              "Action": [
                "appconfig:StartDeployment",
                "appconfig:StopDeployment",
                "appconfig:CreateHostedConfigurationVersion",
                "appconfig:ValidateConfiguration"
              ],
              "Resource": [
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/configurationprofile/
${AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/environment/*",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/configurationprofile/
${AMSResourceTaggerConfigurationCustomerManagedTagsProfileID}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/environment/*",
                "arn:aws:appconfig:*:${AWS::AccountId}:deploymentstrategy/*"
              ]
            },
            {
              "Sid": "CloudFormationStacksPolicy",
```

```
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EC2Policy",
      "Action": [
        "ec2:DescribeInstances"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "SSMPolicy",
      "Effect": "Allow",
      "Action": [
        "ssm:AddTagsToResource",
        "ssm:CancelCommand",
        "ssm:CancelMaintenanceWindowExecution",
        "ssm:CreateAssociation",
        "ssm:CreateAssociationBatch",
        "ssm:CreateMaintenanceWindow",
        "ssm:CreateOpsItem",
        "ssm:CreatePatchBaseline",
        "ssm:DeleteAssociation",
        "ssm:DeleteMaintenanceWindow",
        "ssm:DeletePatchBaseline",
        "ssm:DeregisterPatchBaselineForPatchGroup",
        "ssm:DeregisterTargetFromMaintenanceWindow",
        "ssm:DeregisterTaskFromMaintenanceWindow",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "ssm:PutConfigurePackageResult",
        "ssm:RegisterDefaultPatchBaseline",
        "ssm:RegisterPatchBaselineForPatchGroup",
        "ssm:RegisterTargetWithMaintenanceWindow",
        "ssm:RegisterTaskWithMaintenanceWindow",
        "ssm:RemoveTagsFromResource",
        "ssm:SendCommand",
        "ssm:StartAssociationsOnce",
        "ssm:StartAutomationExecution",
```

```
                "ssm:StartSession",
                "ssm:StopAutomationExecution",
                "ssm:TerminateSession",
                "ssm:UpdateAssociation",
                "ssm:UpdateAssociationStatus",
                "ssm:UpdateMaintenanceWindow",
                "ssm:UpdateMaintenanceWindowTarget",
                "ssm:UpdateMaintenanceWindowTask",
                "ssm:UpdateOpsItem",
                "ssm:UpdatePatchBaseline"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AmsPatchRestrictAMSResources",
            "Effect": "Deny",
            "Action": [
                "ssm:DeletePatchBaseline",
                "ssm:UpdatePatchBaseline"
            ],
            "Resource": [
                "arn:aws:ssm:${AWS::Region}:${AWS::AccountId}:patchbaseline/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/ams:resourceOwner": "*"
                }
            }
        },
        {
            "Sid": "AmsPatchRestrictAmsTags",
            "Effect": "Deny",
            "Action": [
                "ssm:AddTagsToResource",
                "ssm:RemoveTagsFromResource"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "aws:TagKeys": [
                        "AMS*",
                        "Ams*",
                        "ams*"
                    ]
```

```
        }
      }
    },
    {
      "Sid": "TagReadPolicy",
      "Effect": "Allow",
      "Action": [
        "tag:GetResources",
        "tag:GetTagKeys"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudtrailReadPolicy",
      "Effect": "Allow",
      "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EventBridgePolicy",
      "Effect": "Allow",
      "Action": [
        "events:Describe*",
        "events:List*",
        "events:TestEventPattern"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMReadOnlyPolicy",
      "Action": [
          "iam:ListRoles",
          "iam:GetRole"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "AmsResourceSchedulerPassRolePolicy",
      "Effect": "Allow",
```

```
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/
ams_resource_scheduler_ssm_automation_role",
                "Condition": {
                    "StringEquals": {
                        "iam:PassedToService": "ssm.amazonaws.com"
                    }
                }
              }
            ]
          }
        - AMSAlarmManagerConfigurationApplicationId: !ImportValue "AMS-Alarm-Manager-
Configuration-ApplicationId"
          AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID: !ImportValue
 "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID"
          AMSResourceTaggerConfigurationApplicationId: !ImportValue "AMS-
ResourceTagger-Configuration-ApplicationId"
          AMSResourceTaggerConfigurationCustomerManagedTagsProfileID: !ImportValue
 "AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID"

  AMSAccelerateReadOnly:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateReadOnly
      Path: /
      PolicyDocument: !Sub |
        {
          "Version": "2012-10-17",
          "Statement": [
          {
                 "Sid": "AmsSelfServiceReport",
                 "Effect": "Allow",
                 "Action": "amsssrv:*",
                 "Resource": "*"
              },
            {
               "Sid": "AmsBackupPolicy",
               "Effect": "Allow",
               "Action": [
                 "backup:Describe*",
                 "backup:Get*",
                 "backup:List*"
               ],
               "Resource": "*"
```

```
            },
            {
                "Action": [
                    "rds:DescribeDBSnapshots",
                    "rds:ListTagsForResource",
                    "rds:DescribeDBInstances",
                    "rds:describeDBSnapshots",
                    "rds:describeDBEngineVersions",
                    "rds:describeOptionGroups",
                    "rds:describeOrderableDBInstanceOptions",
                    "rds:describeDBSubnetGroups",
                    "rds:DescribeDBClusterSnapshots",
                    "rds:DescribeDBClusters",
                    "rds:DescribeDBParameterGroups",
                    "rds:DescribeDBClusterParameterGroups",
                    "rds:DescribeDBInstanceAutomatedBackups"
                ],
                "Effect": "Allow",
                "Resource": "*"
            },
            {
                "Action": [
                    "dynamodb:ListBackups",
                    "dynamodb:ListTables"
                ],
                "Effect": "Allow",
                "Resource": "*"
            },
            {
                "Action": [
                    "elasticfilesystem:DescribeFilesystems"
                ],
                "Resource": "arn:aws:elasticfilesystem:*:*:file-system/*",
                "Effect": "Allow"
            },
            {
                "Action": [
                    "ec2:DescribeSnapshots",
                    "ec2:DescribeVolumes",
                    "ec2:describeAvailabilityZones",
                    "ec2:DescribeVpcs",
                    "ec2:DescribeAccountAttributes",
                    "ec2:DescribeSecurityGroups",
                    "ec2:DescribeImages",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:GetResources"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeCachediSCSIVolumes",
                "storagegateway:DescribeStorediSCSIVolumes"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*/volume/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Resource": "arn:aws:storagegateway:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeGatewayInformation",
                "storagegateway:ListVolumes",
                "storagegateway:ListLocalDisks"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*"
        },
        {
            "Action": [
                "iam:ListRoles",
```

```
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "organizations:DescribeOrganization",
            "Resource": "*"
        },
        {
            "Action": "fsx:DescribeBackups",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:backup/*"
        },
        {
            "Action": "fsx:DescribeFileSystems",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:file-system/*"
        },
        {
            "Action": "ds:DescribeDirectories",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
          "Sid": "AmsChangeRecordKMSPolicy",
          "Effect": "Allow",
          "Action": [
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:GenerateDataKey"
          ],
          "Resource": [
            "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
          ],
          "Condition": {
            "ForAnyValue:StringLike": {
              "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
            }
          }
        },
        {
          "Sid": "AmsChangeRecordAthenaReadPolicy",
```

```
            "Effect": "Allow",
            "Action": [
              "athena:BatchGetNamedQuery",
              "athena:Get*",
              "athena:List*",
              "athena:StartQueryExecution",
              "athena:UpdateWorkGroup",
              "glue:GetDatabase*",
              "glue:GetTable*",
              "s3:GetAccountPublicAccessBlock",
              "s3:ListAccessPoints",
              "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
          },
          {
            "Sid": "AmsChangeRecordS3ReadPolicy",
            "Effect": "Allow",
            "Action": [
              "s3:Get*",
              "s3:List*"
            ],
            "Resource": [
              "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
              "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*",
              "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
              "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
            ]
          },
          {
            "Sid": "AmsChangeRecordS3WritePolicy",
            "Effect": "Allow",
            "Action": [
              "s3:PutObject",
              "s3:PutObjectLegalHold",
              "s3:PutObjectRetention"
            ],
            "Resource": [
              "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
            ]
          },
          {
            "Sid": "MaciePolicy",
            "Effect": "Allow",
```

```
            "Action": [
              "macie2:GetFindingStatistics"
            ],
            "Resource": "*"
          },
          {
            "Sid": "GuardDutyReadPolicy",
            "Effect": "Allow",
            "Action": [
              "guardduty:GetFindingsStatistics",
              "guardduty:ListDetectors"
            ],
            "Resource": "*"
          },
          {
            "Sid": "SupportReadPolicy",
            "Effect": "Allow",
            "Action": "support:Describe*",
            "Resource": "*"
          },
          {
            "Sid": "ConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "config:Get*",
              "config:Describe*",
              "config:List*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "AppConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "appconfig:List*",
              "appconfig:Get*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "CloudFormationReadPolicy",
            "Effect": "Allow",
            "Action": [
              "cloudformation:DescribeStacks"
```

```
        ],
        "Resource": "*"
      },
      {
        "Sid": "EC2ReadPolicy",
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeInstances"
        ],
        "Resource": "*"
      },
      {
        "Sid": "SSMReadPolicy",
        "Effect": "Allow",
        "Action": [
          "ssm:Describe*",
          "ssm:Get*",
          "ssm:List*"
        ],
        "Resource": "*"
      },
      {
        "Sid": "TagReadPolicy",
        "Effect": "Allow",
        "Action": [
          "tag:GetResources",
          "tag:GetTagKeys"
        ],
        "Resource": "*"
      },
      {
        "Sid": "CloudtrailReadPolicy",
        "Effect": "Allow",
        "Action": [
          "cloudtrail:DescribeTrails",
          "cloudtrail:GetTrailStatus",
          "cloudtrail:LookupEvents"
        ],
        "Resource": "*"
      },
      {
        "Sid": "EventBridgePolicy",
        "Effect": "Allow",
        "Action": [
```

```
                "events:Describe*",
                "events:List*",
                "events:TestEventPattern"
            ],
            "Resource": "*"
        }
    ]
}
```

Mengapa dan kapan AMS mengakses akun Anda

Operator AMS Accelerate (Accelerate) dapat mengakses konsol dan instans akun Anda, dalam keadaan tertentu, untuk mengelola sumber daya Anda. Peristiwa akses ini didokumentasikan dalam log AWS CloudTrail (CloudTrail) Anda. Untuk detail tentang cara meninjau aktivitas di akun Anda oleh tim Operasi Akselerasi AMS dan otomatisasi Akselerasi AMS, lihatMelacak perubahan di akun AMS Accelerate.

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
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)
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

Operator AMS memerlukan peran berikut untuk melayani akun Anda.

> **Note**
>
> Peran akses AMS memungkinkan operator AMS mengakses sumber daya Anda untuk menyediakan kemampuan AMS (lihatDeskripsi layanan). Mengubah peran ini dapat menghambat kemampuan kita untuk menyediakan kemampuan ini. Jika Anda perlu mengubah peran akses AMS, konsultasikan dengan Cloud Architect Anda.

Peran IAM untuk akses AMS ke akun pelanggan

Nama Peran	Deskripsi
ams-access-admin	Peran ini memiliki akses administratif penuh ke akun Anda tanpa batasan. Layanan AMS menggunak an peran ini dengan kebijakan sesi terbatas yang membatasi akses untuk menerapkan infrastruktur AMS dan mengoperasikan akun Anda.
ams-access-admin-operations	Peran ini memberikan izin administratif kepada operator AMS untuk mengoperasikan akun Anda. Peran ini tidak memberikan izin baca, tulis, atau hapus ke konten pelanggan dalam AWS layanan yang biasa digunakan sebagai penyimpanan data, seperti Amazon Simple Storage Service, Amazon Relational Database

Nama Peran	Deskripsi
	Service, Amazon DynamoDB, Amazon Redshift, dan Amazon. ElastiCache Hanya operator AMS yang memenuhi syarat yang memiliki pemahaman dan latar belakang yang kuat dalam manajemen akses yang dapat mengambil peran ini. Operator ini berfungsi sebagai titik eskalasi untuk masalah manajemen akses dan mengakses akun Anda untuk memecahkan masalah akses operator AMS.
ams-access-management	Diterapkan secara manual selama orientasi. Sistem AMS Access memerlukan peran ini untuk mengelola `ams-access-roles` dan `ams-access-managed-policies` menumpuk.
ams-access-operations	Peran ini memiliki izin untuk melakukan tugas administratif di akun Anda. Peran ini tidak memiliki izin membaca, menulis, atau menghapus konten pelanggan dalam AWS layanan yang biasa digunakan sebagai penyimpanan data, seperti Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift, dan Amazon. ElastiCache Izin untuk melakukan operasi AWS Identity and Access Management penulisan juga dikecualikan dari peran ini. Staf operasi AMS Accelerate dan arsitek cloud (CAs) dapat mengambil peran ini.
ams-access-read-only	Peran ini memiliki akses hanya-baca ke akun Anda. Staf operasi AMS Accelerate dan arsitek cloud (CAs) dapat mengambil peran ini. Izin membaca konten pelanggan dalam AWS layanan yang biasa digunakan sebagai penyimpanan data, seperti Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift, dan, tidak diberikan peran ini. ElastiCache

Nama Peran	Deskripsi
ams-access-security-analyst	Peran keamanan AMS ini memiliki izin di akun AMS Anda untuk melakukan pemantauan peringata n keamanan khusus dan penanganan insiden keamanan. Hanya sedikit individu AMS Security terpilih yang dapat mengambil peran ini.
ams-access-security-analyst-baca-saja	Peran keamanan AMS ini terbatas pada izin hanya-baca di akun AMS Anda untuk melakukan pemantauan peringatan keamanan khusus dan penanganan insiden keamanan.

> **Note**
>
> Ini adalah template untuk ams-access-management peran tersebut. Ini adalah tumpukan yang diterapkan oleh arsitek cloud (CAs) secara manual di akun Anda pada waktu orientasi: management-role.yaml.
> Ini adalah template untuk peran akses yang berbeda untuk tingkat akses yang berbeda: ams-access-read-only,, ams-access-operations ams-access-admin-operations, ams-access-admin: accelerate-roles.yaml.

Bagaimana AMS mengakses akun Anda

Operator AMS Accelerate dapat mengakses konsol dan instans akun Anda, dalam keadaan tertentu.

Operator AMS menggunakan layanan akses Akselerasi AMS internal untuk mengakses akun Anda dengan cara yang aman dan diaudit. Untuk mengakses instans Anda, operator AMS menggunakan layanan akses AMS internal yang sama dengan broker dan, setelah akses diberikan, operator AMS Accelerate menggunakan manajer sesi SSM untuk mendapatkan akses dengan menggunakan kredenal sesi. Akses RDP untuk instance Windows disediakan dengan membuat penerusan port ke instance dan membuat pengguna lokal menggunakan SSM. Kredensi pengguna lokal digunakan untuk akses RDP dan dihapus pada akhir sesi.

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.

Root dengan AMS Accelerate:

AMS tidak melarang Anda menggunakan akun pengguna root Anda. Namun, Operasi dan Keamanan AMS memperlakukan penggunaannya sebagai masalah untuk diselidiki dan kami akan menghubungi tim Keamanan Anda setiap kali digunakan.

Kami menyarankan Anda menghubungi CSDM dan CA Anda dua puluh empat jam sebelumnya, untuk memberi tahu mereka tentang pekerjaan akses root yang ingin Anda lakukan.

Operasi AMS dan respons keamanan terhadap penggunaan root:

AMS menerima alarm saat akun pengguna root digunakan. Jika penggunaan kredensional 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.

Manajemen keamanan di AMS Accelerate

AWS Managed Services menggunakan beberapa kontrol untuk melindungi aset informasi Anda dan membantu menjaga AWS infrastruktur tetap aman. AMS Accelerate mengelola pustaka Aturan AWS Config dan tindakan remediasi untuk memastikan bahwa semua akun Anda mematuhi standar industri untuk keamanan dan integritas operasional. Aturan AWS Config terus melacak perubahan konfigurasi di antara sumber daya yang Anda rekam. Jika perubahan melanggar ketentuan aturan apa pun, AMS melaporkan temuannya, dan memungkinkan Anda untuk memulihkan pelanggaran secara otomatis atau berdasarkan permintaan, sesuai dengan tingkat keparahan pelanggaran. Aturan AWS Config memfasilitasi kepatuhan terhadap standar yang ditetapkan oleh: Center for Internet Security (CIS), National Institute of Standards and Technology (NIST) Cloud Security Framework (CSF), Health Insurance Portability and Accountability Act (HIPAA), dan Payment Card Industry (PCI) Standar Keamanan Data (DSS).

Selain itu, AMS memanfaatkan Amazon GuardDuty untuk mengidentifikasi aktivitas yang berpotensi tidak sah atau berbahaya di lingkungan Anda AWS . AMS memantau GuardDuty temuan 24x7. AMS bekerja sama dengan Anda untuk memahami dampak temuan dan mengidentifikasi remediasi berdasarkan rekomendasi praktik terbaik. AMS juga menggunakan Amazon Macie untuk melindungi data sensitif Anda seperti informasi kesehatan pribadi (PHI), informasi identitas pribadi (PII), dan data keuangan.

> **Note**
>
> Amazon Macie adalah layanan opsional dan tidak diaktifkan secara default.

AMS Accelerate menyediakan berbagai layanan operasional untuk membantu Anda mencapai keunggulan operasional AWS. Untuk mempelajari lebih lanjut tentang bagaimana AMS membantu tim Anda mencapai keunggulan operasional secara keseluruhan AWS Cloud dengan kemampuan operasional utama AMS termasuk helpdesk 24x7, pemantauan proaktif, keamanan, penambalan, pencatatan, dan pencadangan, lihat Diagram Arsitektur Referensi AMS.

Topik

- Gunakan Dokumen SSM Log4j untuk menemukan kejadian di Accelerate
- Pemantauan keamanan infrastruktur di AMS
- Perlindungan data di Accelerate

- AWS Identity and Access Management di AMS Accelerate
- Respon Insiden Keamanan di AMS
- Pencatatan dan pemantauan peristiwa keamanan di Accelerate
- Kepatuhan konfigurasi di Accelerate
- Respon Insiden di Accelerate
- Ketahanan dalam Mempercepat
- Kontrol keamanan untuk sistem end-of-support operasi
- Praktik terbaik keamanan di Accelerate
- Ubah ulasan keamanan permintaan
- FAQ Keamanan

Gunakan Dokumen SSM Log4j untuk menemukan kejadian di Accelerate

Dokumen Log4j (AWS Systems Manager dokumen SSM) membantu Anda mencari pustaka Apache Log4j2 dalam beban kerja yang dicerna. Dokumen otomatisasi menyediakan laporan ID Proses aplikasi Java tempat pustaka Log4j2 aktif.

Laporan ini mencakup informasi tentang Java Archives (JAR Files), ditemukan dalam lingkungan tertentu yang berisi JndiLookup kelas. Ini adalah praktik terbaik untuk meningkatkan pustaka yang ditemukan ke versi terbaru yang tersedia. Peningkatan ini mengurangi Eksekusi Kode Jarak Jauh (RCE) yang diidentifikasi melalui CVE-2021-44228. Unduh versi terbaru perpustakaan Log4j dari Apache. Untuk informasi lebih lanjut, lihat Unduh Apache Log4j 2.

Dokumen ini dibagikan ke semua Wilayah yang terhubung ke Accelerate,. Untuk mengakses dokumen, lengkapi langkah-langkah berikut:

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Di panel navigasi, pilih Dokumen.
3. Pilih Berbagi dengan saya.
4. Di kotak pencarian, masukkan AWSManagedServices-GatherLog4JInformation.
5. Gunakan kontrol tingkat untuk menjalankan dokumen dalam skala besar.

Dokumen AWSManagedServices-GatherLog 4JInformation mengumpulkan parameter berikut:

- InstanceId: (Wajib) ID EC2 instans Anda.
- S3Bucket: (Opsional) URL S3 yang telah ditandatangani sebelumnya atau URI S3 (s3://BUCKET_NAME) untuk mengunggah hasilnya.
- AutomationAssumeRole: (Wajib) ARN dari peran yang memungkinkan autoomasi untuk melakukan tindakan atas nama Anda.

Ini adalah praktik terbaik untuk menjalankan dokumen ini menggunakan kontrol tingkat. Anda dapat mengatur parameter kontrol laju menjadi InstanceId, dan menetapkan daftar instance ke dalamnya, atau menerapkan kombinasi tombol tag untuk menargetkan semua EC2 instance yang memiliki tag tertentu. AWS Managed Services juga merekomendasikan agar Anda menyediakan bucket Amazon Simple Storage Service (Amazon S3) untuk mengunggah hasilnya, sehingga Anda dapat membuat laporan dari data yang disimpan di S3. Untuk contoh cara menggabungkan hasil di S3, lihat Stack EC2 Instans | Kumpulkan Informasi Log4j.

Jika Anda tidak dapat memutakhirkan paket, ikuti panduan yang diuraikan oleh AWS Security at Using AWS security services untuk melindungi, mendeteksi, dan merespons kerentanan Log4j. Untuk mengurangi kerentanan dengan menghapus fungsionalitas JndiLookup kelas, jalankan hot patch Log4j sebaris dengan aplikasi Java Anda. Untuk informasi lebih lanjut tentang hot patch, lihat Hotpatch untuk Apache Log4j.

Untuk pertanyaan tentang output otomatisasi atau bagaimana melanjutkan dengan mitigasi tambahan, kirimkan permintaan layanan.

Pemantauan keamanan infrastruktur di AMS

Saat Anda melakukan onboard ke AMS Accelerate, AWS menerapkan infrastruktur AWS Config dasar berikut dan seperangkat aturan, AMS Accelerate menggunakan aturan ini untuk memantau akun Anda.

- AWS Config peran terkait layanan: AMS Accelerate menerapkan peran terkait layanan bernama AWSServiceRoleForConfig, yang digunakan oleh AWS Config untuk menanyakan status layanan lain. AWS Peran AWSServiceRoleForConfigterkait layanan mempercayai AWS Config layanan untuk mengambil peran tersebut. Kebijakan izin untuk AWSServiceRoleForConfigperan tersebut berisi izin hanya-baca dan hanya tulis pada sumber daya dan izin hanya-baca untuk AWS Config sumber daya di layanan lain yang mendukung. AWS Config Jika Anda sudah memiliki peran yang dikonfigurasi dengan AWS Config Recorder, AMS Accelerate memvalidasi bahwa peran

yang ada memiliki kebijakan terkelola AWS Config yang dilampirkan. Jika tidak, AMS Accelerate menggantikan peran dengan peran terkait layanan. AWSServiceRoleForConfig

- AWS Config perekam dan saluran pengiriman: AWS Config menggunakan perekam konfigurasi untuk mendeteksi perubahan dalam konfigurasi sumber daya Anda dan menangkap perubahan ini sebagai item konfigurasi. AMS Accelerate menyebarkan perekam konfigurasi di semua layanan Wilayah AWS, dengan perekaman terus menerus dari semua sumber daya. AMS Accelerate juga membuat saluran pengiriman konfigurasi, bucket Amazon S3, yang digunakan untuk merekam perubahan yang terjadi di AWS sumber daya Anda. Perekam konfigurasi memperbarui status konfigurasi melalui saluran pengiriman. Perekam konfigurasi dan saluran pengiriman diperlukan AWS Config untuk bekerja. AMS Accelerate membuat perekam di semua Wilayah AWS, dan saluran pengiriman dalam satu Wilayah AWS. Jika Anda sudah memiliki perekam dan saluran pengiriman Wilayah AWS, AMS Accelerate tidak menghapus AWS Config sumber daya yang ada, sebaliknya AMS Accelerate menggunakan perekam dan saluran pengiriman yang ada setelah memvalidasi bahwa mereka telah dikonfigurasi dengan benar. Untuk informasi lebih lanjut tentang cara mengurangi AWS Config biaya, lihatMengurangi AWS Config biaya di Accelerate.
- AWS Config aturan: AMS Accelerate memelihara perpustakaan Aturan AWS Config dan tindakan remediasi untuk membantu Anda mematuhi standar industri untuk keamanan dan integritas operasional. Aturan AWS Config terus melacak perubahan konfigurasi di antara sumber daya yang Anda rekam. Jika perubahan melanggar ketentuan aturan apa pun, AMS melaporkan temuannya, dan memungkinkan Anda untuk memulihkan pelanggaran secara otomatis atau berdasarkan permintaan, sesuai dengan tingkat keparahan pelanggaran. Aturan AWS Config memfasilitasi kepatuhan terhadap standar yang ditetapkan oleh: Center for Internet Security (CIS), National Institute of Standards and Technology (NIST) Cloud Security Framework (CSF), Health Insurance Portability and Accountability Act (HIPAA), dan Payment Card Industry (PCI) Standar Keamanan Data (DSS).
- AWS Config otorisasi agregator: Agregator adalah jenis AWS Config sumber daya yang mengumpulkan data AWS Config konfigurasi dan kepatuhan dari beberapa akun dan beberapa Wilayah. AMS Mempercepat onboard akun Anda ke agregator konfigurasi tempat AMS Accelerate mengumpulkan informasi konfigurasi sumber daya akun Anda dan data kepatuhan konfigurasi serta menghasilkan laporan kepatuhan. Jika ada agregator yang ada yang dikonfigurasi di akun milik AMS, AMS Accelerate akan menerapkan agregator tambahan dan agregator yang ada tidak dimodifikasi.

> **Note**
>
> Agregator Config tidak diatur di akun Anda; melainkan, ini diatur di akun milik AMS dan akun Anda dimasukkan ke dalamnya.

Untuk mempelajari lebih lanjut tentang AWS Config, 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 Agregator: Agregasi Data Multi-Wilayah Multi-Akun

Untuk informasi tentang laporan, lihatAWS Config Laporan Kepatuhan Kontrol.

Menggunakan peran terkait layanan untuk AMS Accelerate

AMS Accelerate menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Service-linked role (SLR) adalah tipe unik dari peran IAM yang ditautkan langsung ke AMS Accelerate. Peran terkait layanan telah ditentukan sebelumnya oleh AMS Accelerate dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan AMS Accelerate lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AMS Accelerate mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AMS Accelerate yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWS layanan yang bekerja dengan IAM dan cari layanan yang memiliki Ya di kolom Peran terkait layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Peran terkait layanan toolkit penerapan untuk AMS Accelerate

AMS Accelerate menggunakan peran terkait layanan (SLR) bernama AWSServiceRoleForAWSManagedServicesDeploymentToolkit— peran ini menyebarkan infrastruktur AMS Accelerate ke akun pelanggan.

> **Note**
>
> Kebijakan ini baru saja diperbarui; untuk detailnya, lihatMempercepat pembaruan ke peran terkait layanan.

AMS Mempercepat penerapan toolkit SLR

Peran AWSService RoleFor AWSManaged ServicesDeploymentToolkit terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `deploymenttoolkit.managedservices.amazonaws.com`

Kebijakan yang diberi nama AWSManagedServicesDeploymentToolkitPolicymemungkinkan AMS Accelerate untuk melakukan tindakan pada sumber daya berikut:

- `arn:aws*:s3:::ams-cdktoolkit*`
- `arn:aws*:cloudformation:*:*:stack/ams-cdk-toolkit*`
- `arn:aws:ecr:*:*:repository/ams-cdktoolkit*`

SLR ini memberikan izin Amazon S3 untuk membuat dan mengelola bucket penerapan yang digunakan oleh AMS untuk mengunggah sumber daya, seperti CloudFormation template atau bundel aset Lambda, ke dalam akun untuk penerapan komponen. SLR ini memberikan CloudFormation izin untuk menyebarkan CloudFormation tumpukan yang mendefinisikan bucket penerapan. Untuk detail atau mengunduh kebijakan, lihat AWSManagedServices_DeploymentToolkitPolicy.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran yang terkait dengan layanan dalam Panduan Pengguna IAM.

Membuat toolkit penerapan SLR untuk AMS Accelerate

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda Onboard ke AMS di AWS Management Console, the AWS CLI, atau AWS API, AMS Accelerate membuat peran terkait layanan untuk Anda.

> **Important**
>
> Peran terkait layanan ini dapat muncul di akun Anda jika Anda menggunakan layanan AMS Accelerate sebelum 09 Juni 2022, ketika mulai mendukung peran terkait layanan, kemudian AMS Accelerate membuat AWSService RoleFor AWSManaged ServicesDeploymentToolkit peran tersebut di 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 Accelerate membuat peran terkait layanan untuk Anda lagi.

Mengedit toolkit penerapan SLR untuk AMS Accelerate

AMS Accelerate tidak memungkinkan Anda mengedit peran AWSService RoleFor AWSManaged ServicesDeploymentToolkit 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 toolkit penerapan SLR untuk AMS Accelerate

Anda tidak perlu menghapus AWSService RoleFor AWSManaged ServicesDeploymentToolkit peran secara manual. Saat Anda Offboard dari AMS di AWS Management Console, the AWS CLI, atau AWS API, AMS Accelerate 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 tertaut layanan terlebih dahulu, lalu Anda dapat menghapusnya secara manual.

> **Note**
>
> Jika layanan AMS Accelerate 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 Accelerate yang digunakan oleh AWSService RoleFor AWSManaged ServicesDeploymentToolkit peran terkait layanan

Hapus `ams-cdk-toolkit` tumpukan dari semua Wilayah yang di-onboard akun Anda di AMS (Anda mungkin harus mengosongkan bucket S3 secara manual terlebih dahulu).

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSService RoleFor AWSManaged ServicesDeploymentToolkit terkait layanan. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan di Panduan Pengguna IAM.

Detektif mengontrol peran terkait layanan untuk AMS Accelerate

AMS Accelerate menggunakan peran terkait layanan (SLR) bernama AWSServiceRoleForManagedServices_DetectiveControlsConfig— AWS Managed Services menggunakan peran terkait layanan ini untuk menerapkan perekam konfigurasi, aturan konfigurasi, dan kontrol detektif bucket S3..

Terlampir pada peran AWSServiceRoleForManagedServices_DetectiveControlsConfigterkait layanan adalah kebijakan terkelola berikut: AWSManagedServices_DetectiveControlsConfig _. ServiceRolePolicy Untuk pembaruan kebijakan ini, silakan lihat Mempercepat pembaruan kebijakan AWS terkelola.

Izin untuk kontrol detektif SLR untuk AMS Accelerate

Peran AWSServiceRoleForManagedServices_DetectiveControlsConfig terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `detectivecontrols.managedservices.amazonaws.com`

Terlampir pada peran ini adalah kebijakan `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS terkelola (lihat AWS kebijakan terkelola: AWSManagedServices_DetectiveControlsConfig _ ServiceRolePolicy Layanan menggunakan peran untuk membuat konfigurasi Kontrol Detektif AMS di akun Anda, yang memerlukan penerapan sumber daya seperti bucket s3, aturan konfigurasi, dan agregator. Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin Peran Tertaut Layanan di Panduan Pengguna AWS Identity and Access Management.

Membuat detektif mengontrol SLR untuk AMS Accelerate

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda Onboard ke AMS di AWS Management Console, the AWS CLI, atau AWS API, AMS Accelerate membuat peran terkait layanan untuk Anda.

> **Important**
>
> Peran terkait layanan ini dapat muncul di akun Anda jika Anda menggunakan layanan AMS Accelerate sebelum 09 Juni 2022, ketika mulai mendukung peran terkait layanan, AMS Accelerate membuat AWSServiceRoleForManagedServices_DetectiveControlsConfig peran tersebut di 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 Accelerate membuat peran terkait layanan untuk Anda lagi.

Mengedit detektif mengontrol SLR untuk AMS Accelerate

AMS Accelerate tidak memungkinkan Anda mengedit peran AWSServiceRoleForManagedServices_DetectiveControlsConfig 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 yang terkait dengan layanan dalam Panduan Pengguna IAM.

Menghapus kontrol detektif SLR untuk AMS Accelerate

Anda tidak perlu menghapus AWSServiceRoleForManagedServices_DetectiveControlsConfig peran secara manual. Saat Anda Offboard dari AMS di AWS Management Console, the AWS CLI, atau AWS API, AMS Accelerate 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 tertaut layanan terlebih dahulu, lalu Anda dapat menghapusnya secara manual.

> **Note**
>
> Jika layanan AMS Accelerate 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 Accelerate yang digunakan oleh AWSServiceRoleForManagedServices_DetectiveControlsConfig peran terkait layanan

Hapus`ams-detective-controls-config-recorder`, `ams-detective-controls-config-rules-cdk` dan `ams-detective-controls-infrastructure-cdk` tumpukan dari semua Wilayah yang dimasukkan ke akun Anda di AMS (Anda mungkin harus mengosongkan bucket S3 secara manual terlebih dahulu).

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForManagedServices_DetectiveControlsConfig terkait layanan. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

Peran terkait layanan EventBridge aturan Amazon untuk AMS Accelerate

AMS Accelerate menggunakan peran terkait layanan (SLR) bernama. AWSServiceRoleForManagedServices_Events Peran ini mempercayai salah satu prinsip layanan AWS Managed Services (events.managedservices.amazonaws.com) untuk mengambil peran tersebut bagi Anda. Layanan ini menggunakan peran untuk membuat aturan EventBridge terkelola Amazon. Aturan ini adalah infrastruktur yang diperlukan di akun AWS Anda untuk mengirimkan informasi perubahan status alarm dari akun Anda ke AWS Managed Services.

Izin untuk EventBridge SLR untuk AMS Accelerate

Peran AWSServiceRoleForManagedServices_Events terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `events.managedservices.amazonaws.com`

Terlampir pada peran ini adalah kebijakan `AWSManagedServices_EventsServiceRolePolicy` AWS terkelola (lihatAWS kebijakan terkelola: AWSManagedServices_EventsServiceRolePolicy).

Layanan menggunakan peran untuk mengirimkan informasi perubahan status alarm dari akun Anda ke AMS. 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 Accelerate

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda Onboard ke AMS di AWS Management Console, the AWS CLI, atau AWS API, AMS Accelerate membuat peran terkait layanan untuk Anda.

> **Important**
>
> Peran terkait layanan ini dapat muncul di akun Anda jika Anda menggunakan layanan AMS Accelerate sebelum 7 Februari 2023, ketika mulai mendukung peran terkait layanan, 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 Accelerate membuat peran terkait layanan untuk Anda lagi.

Mengedit EventBridge SLR untuk AMS Accelerate

AMS Accelerate tidak memungkinkan 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 Accelerate

Anda tidak perlu menghapus AWSServiceRoleForManagedServices_Events peran secara manual. Saat Anda Offboard dari AMS di AWS Management Console, the AWS CLI, atau AWS API, AMS Accelerate 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 tertaut layanan terlebih dahulu, lalu Anda dapat menghapusnya secara manual.

> **Note**
>
> Jika layanan AMS Accelerate 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 Accelerate yang digunakan oleh AWSServiceRoleForManagedServices_Events peran terkait layanan

Untuk menghapus peran tertaut 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.

Menghubungi peran terkait layanan untuk AMS Accelerate

AMS Accelerate menggunakan peran terkait layanan (SLR) bernama AWSServiceRoleForManagedServices_Contacts— Peran ini memfasilitasi pemberitahuan otomatis ketika insiden terjadi dengan mengizinkan layanan membaca tag yang ada dari sumber daya yang terpengaruh dan mengambil email yang dikonfigurasi dari titik kontak yang sesuai.

Ini adalah satu-satunya layanan yang menggunakan peran terkait layanan ini.

Terlampir pada peran AWSServiceRoleForManagedServices_Contactsterkait layanan adalah kebijakan terkelola berikut:. AWSManagedServices_ContactsServiceRolePolicy Untuk pembaruan kebijakan ini, silakan lihat Mempercepat pembaruan kebijakan AWS terkelola.

Izin untuk Kontak SLR untuk AMS Accelerate

Peran AWSServiceRoleForManagedServices_Contacts terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `contacts-service.managedservices.amazonaws.com`

Terlampir pada peran ini adalah kebijakan terkelola `AWSManagedServices_ContactsServiceRolePolicy` AWS (lihatAWS kebijakan terkelola: AWSManagedServices_ContactsServiceRolePolicy). Layanan menggunakan peran untuk membaca tag pada AWS sumber daya apa pun dan menemukan email yang terkandung dalam tag, dari titik kontak yang sesuai ketika insiden terjadi. Peran ini memfasilitasi pemberitahuan otomatis ketika insiden terjadi dengan mengizinkan AMS membaca tag tersebut pada sumber daya yang terpengaruh dan mengambil email. Untuk informasi selengkapnya, lihat Izin Peran Tertaut Layanan di Panduan Pengguna AWS Identity and Access Management.

> **Important**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. AMS menggunakan tag untuk memberi Anda layanan administrasi. Tag tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Kebijakan izin peran bernama AWSManagedServices_ContactsServiceRolePolicy memungkinkan AMS Accelerate untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: Memungkinkan Layanan Kontak membaca tag yang diatur secara khusus agar berisi email bagi AMS untuk mengirim pemberitahuan insiden pada sumber daya AWS apa pun.

Anda dapat mengunduh JSON AWSManagedServices_ContactsServiceRolePolicy di ZIP ini: ContactsServicePolicy.zip.

Membuat SLR Kontak untuk AMS Accelerate

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda Onboard ke AMS di AWS Management Console, the AWS CLI, atau AWS API, AMS Accelerate membuat peran terkait layanan untuk Anda.

> **Important**
>
> Peran terkait layanan ini dapat muncul di akun Anda jika Anda menggunakan layanan AMS Accelerate sebelum 16 Februari 2023, ketika mulai mendukung peran terkait layanan, AMS Accelerate membuat peran tersebut di AWSServiceRoleForManagedServices_Contacts 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 Accelerate membuat peran terkait layanan untuk Anda lagi.

Mengedit Kontak SLR untuk AMS Accelerate

AMS Accelerate tidak memungkinkan Anda mengedit peran AWSServiceRoleForManagedServices_Contacts 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 Kontak SLR untuk AMS Accelerate

Anda tidak perlu menghapus AWSServiceRoleForManagedServices_Contacts peran secara manual. Saat Anda Offboard dari AMS di AWS Management Console, the AWS CLI, atau AWS API, AMS Accelerate 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 tertaut layanan terlebih dahulu, lalu Anda dapat menghapusnya secara manual.

> **Note**
>
> Jika layanan AMS Accelerate 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 Accelerate yang digunakan oleh AWSServiceRoleForManagedServices_Contacts peran terkait layanan

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForManagedServices_Contacts terkait layanan. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

Wilayah yang didukung untuk AMS Mempercepat peran terkait layanan

AMS Accelerate mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi selengkapnya, silakan lihat Wilayah AWS dan titik akhir.

Mempercepat pembaruan ke peran terkait layanan

Lihat detail tentang pembaruan untuk Mempercepat peran terkait layanan sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman AccelerateRiwayat dokumen untuk Panduan Pengguna AMS Accelerate.

Ubah	Deskripsi	Tanggal

Kebijakan yang diperbarui - Deployment Toolkit	• Izin baru ini ditambahkan untuk sumber daya`arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		April 4, 2024

Kebijakan yang diperbarui - Deployment Toolkit	• Izin baru ini ditambahkan untuk sumber daya`arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*` :
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
	• Izin baru ini ditambahkan untuk sumber daya`arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :
	`ecr:CreateRepository`
	`ecr:DeleteLifecyclePolicy`
	`ecr:DeleteRepository`
	`ecr:DeleteRepositoryPolicy`
		09 Mei 2023

Ubah	Deskripsi	Tanggal
	ecr:DescribeRepositories ecr:GetLifecyclePolicy ecr:ListTagsForResource ecr:PutImageTagMutability ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy ecr:TagResource ecr:UntagResource • Juga, beberapa tindakan yang ada dengan wildcard dicakup ke tindakan individu: - s3:DeleteObject* + s3:DeleteObject + s3:DeleteObjectTagging + s3:DeleteObjectVersion + s3:DeleteObjectVersionTagging - s3:GetObject* + s3:GetObject + s3:GetObjectAcl + s3:GetObjectAttributes + s3:GetObjectLegalHold + s3:GetObjectRetention + s3:GetObjectTagging + s3:GetObjectVersion + s3:GetObjectVersionAcl + s3:GetObjectVersionAttributes + s3:GetObjectVersionForReplication + s3:GetObjectVersionTagging + s3:GetObjectVersionTorrent - cloudformation:UpdateTermination* + cloudformation:UpdateTerminationProtection	
Kebijakan yang diperbarui — Detective Controls	• CloudFormation Tindakan telah dicakup lebih lanjut setelah konfirmasi dengan tim keamanan dan akses • Tindakan Lambda telah dihapus dari kebijakan karena tidak berdampak pada boarding onboarding/off	10 April 2023

Ubah	Deskripsi	Tanggal
Kebijakan yang diperbarui — Detective Controls	Memperbarui kebijakan dan menambahkan kebijakan batas izin.	21 Maret 2023
Peran terkait layanan baru - Kontak SLR	Accelerate menambahkan peran terkait layanan baru untuk layanan Kontak. Peran ini memfasilitasi pemberitahuan otomatis ketika insiden terjadi dengan mengizinkan layanan membaca tag yang ada dari sumber daya yang terpengaruh dan mengambil email yang dikonfigurasi dari titik kontak yang sesuai.	16 Februari 2023
Peran terkait layanan baru — EventBridge	Accelerate menambahkan peran terkait layanan baru untuk aturan Amazon EventBridge . Peran ini mempercayai salah satu prinsip layanan AWS Managed Services (events.managedservices.amazonaws.com) untuk mengambil peran tersebut bagi Anda. Layanan ini menggunakan peran untuk membuat aturan EventBridge terkelola Amazon. Aturan ini adalah infrastruktur yang diperlukan di akun AWS Anda untuk mengirimkan informasi perubahan status alarm dari akun Anda ke AWS Managed Services.	7 Februari 2023

Ubah	Deskripsi	Tanggal
Peran terkait layanan yang diperbarui — Deployment Toolkit	Mempercepat diperbarui AWSService RoleFor AWSManaged ServicesDeploymentToolkit dengan izin S3 baru. Izin baru ini ditambahkan: `"s3:GetLifecycleConfiguration", "s3:GetBucketLogging", "s3:ListBucket", "s3:GetBucketVersioning", "s3:PutLifecycleConfiguration", "s3:GetBucketLocation", "s3:GetObject*"`	30 Januari 2023
Mempercepat mulai melacak perubahan	Accelerate mulai melacak perubahan untuk peran terkait layanannya.	30 November 2022
Peran terkait layanan baru — Detective Controls	Accelerate menambahkan peran terkait layanan baru untuk menerapkan Accelerate detective controls. AWS Managed Services menggunakan peran terkait layanan ini untuk menerapkan perekam konfigurasi, aturan konfigurasi, dan kontrol detektif bucket S3.	13 Oktober 2022
Peran terkait layanan baru — Deployment Toolkit	Accelerate menambahkan peran terkait layanan baru untuk menerapkan infrastruktur Accelerate. peran ini menyebarkan infrastruktur AMS Accelerate ke dalam akun pelanggan.	Juni 09, 2022

AWS kebijakan terkelola untuk AMS Accelerate

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

Untuk tabel perubahan, lihatMempercepat pembaruan kebijakan AWS terkelola.

AWS kebijakan terkelola: AWSManagedServices_AlarmManagerPermissionsBoundary

AWS Managed Services (AMS) menggunakan kebijakan `AWSManagedServices_AlarmManagerPermissionsBoundary` AWS terkelola. Kebijakan AWS-managed ini digunakan di AWSManagedServices_AlarmManager _ ServiceRolePolicy untuk membatasi izin peran IAM yang dibuat oleh. AWSServiceRoleForManagedServices_AlarmManager

Kebijakan ini memberikan peran IAM yang dibuat sebagai bagian dariBagaimana Manajer Alarm bekerja, izin untuk melakukan operasi seperti evaluasi Config AWS , AWS Config read untuk mengambil konfigurasi Alarm Manager, dan pembuatan alarm Amazon yang diperlukan. CloudWatch

`AWSManagedServices_AlarmManagerPermissionsBoundary`Kebijakan ini dilampirkan pada peran `AWSServiceRoleForManagedServices_DetectiveControlsConfig` terkait layanan. Untuk pembaruan peran ini, lihatMempercepat pembaruan ke peran terkait layanan.

Anda dapat melampirkan kebijakan ini ke identitas IAM Anda.

Detail izin

Kebijakan ini mencakup izin berikut.

- `AWS Config`— Memungkinkan izin untuk mengevaluasi aturan konfigurasi dan memilih konfigurasi sumber daya.
- `AWS AppConfig`— Memungkinkan izin untuk mengambil konfigurasi AlarmManager .

- `Amazon S3`— Memungkinkan izin untuk mengoperasikan AlarmManager ember dan objek.
- `Amazon CloudWatch`— Memungkinkan izin untuk membaca dan menempatkan alarm dan metrik yang AlarmManager dikelola.
- `AWS Resource Groups and Tags`— Memungkinkan izin untuk membaca tag sumber daya.
- `Amazon EC2`— Memungkinkan izin untuk membaca EC2 sumber daya Amazon.
- `Amazon Redshift`— Memungkinkan izin untuk membaca instance dan cluster Redshift.
- `Amazon FSx`— Memungkinkan izin untuk menggambarkan sistem file, volume, dan tag sumber daya.
- `Amazon CloudWatch Synthetics`— Memungkinkan izin untuk membaca sumber daya Synthetics.
- `Amazon Elastic Kubernetes Service`— Memungkinkan izin untuk mendeskripsikan kluster Amazon EKS.
- `Amazon ElastiCache`— Memungkinkan izin untuk menggambarkan sumber daya.

Anda dapat mengunduh file kebijakan di ZIP ini: RecommendedPermissionBoundary.zip.

AWS kebijakan terkelola: AWSManagedServices_DetectiveControlsConfig _ ServiceRolePolicy

AWS Managed Services (AMS) menggunakan kebijakan `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS terkelola. Kebijakan AWS-managed ini dilampirkan ke peran `AWSServiceRoleForManagedServices_DetectiveControlsConfig` terkait layanan, (lihat). Detektif mengontrol peran terkait layanan untuk AMS Accelerate Untuk pembaruan peran `AWSServiceRoleForManagedServices_DetectiveControlsConfig` terkait layanan, lihat. Mempercepat pembaruan ke peran terkait layanan

Kebijakan ini memungkinkan peran terkait layanan untuk menyelesaikan tindakan untuk Anda.

Anda dapat melampirkan ServiceRolePolicy kebijakan AWSManagedServices_DetectiveControlsConfig _ ke entitas IAM Anda.

Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AMS Accelerate.

Detail izin

Kebijakan ini memiliki izin berikut untuk mengizinkan Kontrol AWS Managed Services Detektif menerapkan dan mengonfigurasi semua sumber daya yang diperlukan.

- `CloudFormation`— Memungkinkan Kontrol Detektif AMS untuk menyebarkan CloudFormation tumpukan dengan sumber daya seperti bucket s3, aturan konfigurasi, dan perekam konfigurasi.
- `AWS Config`— Memungkinkan Kontrol Detektif AMS untuk membuat aturan konfigurasi AMS, mengonfigurasi agregator, dan menandai sumber daya.
- `Amazon S3`— memungkinkan AMS Detective Controls untuk mengelola bucket s3-nya.

Anda dapat mengunduh file kebijakan JSON di ZIP ini: DetectiveControlsConfig_ ServiceRolePolicy .zip.

AWS kebijakan terkelola: AWSManaged ServicesDeploymentToolkitPolicy

AWS Managed Services (AMS) menggunakan kebijakan `AWSManagedServicesDeploymentToolkitPolicy` AWS terkelola. Kebijakan AWS-managed ini dilampirkan ke peran `AWSServiceRoleForAWSManagedServicesDeploymentToolkit` terkait layanan, (lihat). Peran terkait layanan toolkit penerapan untuk AMS Accelerate Kebijakan ini memungkinkan peran terkait layanan untuk menyelesaikan tindakan untuk Anda. Anda tidak dapat melampirkan kebijakan ini ke entitas IAM Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AMS Accelerate.

Untuk pembaruan peran `AWSServiceRoleForManagedServicesDeploymentToolkitPolicy` terkait layanan, lihat. Mempercepat pembaruan ke peran terkait layanan

Detail izin

Kebijakan ini memiliki izin berikut untuk mengizinkan Kontrol AWS Managed Services Detektif menerapkan dan mengonfigurasi semua sumber daya yang diperlukan.

- `CloudFormation`— Memungkinkan AMS Deployment Toolkit untuk menyebarkan tumpukan CFN dengan sumber daya S3 yang dibutuhkan oleh CDK.
- `Amazon S3`— memungkinkan AMS Deployment Toolkit untuk mengelola bucket S3-nya.
- `Elastic Container Registry`— memungkinkan AMS Deployment Toolkit untuk mengelola repositori ECR yang digunakan untuk menyebarkan aset yang dibutuhkan oleh aplikasi AMS CDK.

Anda dapat mengunduh file kebijakan JSON di ZIP ini: AWSManagedServicesDeploymentToolkitPolicy.zip.

AWS kebijakan terkelola: AWSManagedServices_EventsServiceRolePolicy

AWS Managed Services (AMS) menggunakan kebijakan terkelola `AWSManagedServices_EventsServiceRolePolicy` AWS. Kebijakan AWS-managed ini dilampirkan ke peran `AWSServiceRoleForManagedServices_Events`terkait layanan. Kebijakan ini memungkinkan peran terkait layanan untuk menyelesaikan tindakan untuk Anda. Anda tidak dapat melampirkan kebijakan ini ke entitas IAM Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AMS Accelerate.

Untuk pembaruan peran `AWSServiceRoleForManagedServices_Events` terkait layanan, lihat. Mempercepat pembaruan ke peran terkait layanan

Detail izin

Kebijakan ini memiliki izin berikut untuk mengizinkan Amazon EventBridge mengirimkan informasi perubahan status alarm dari akun Anda ke AWS Managed Services.

- `events`— Memungkinkan Accelerate untuk membuat aturan EventBridge terkelola Amazon. Aturan ini adalah infrastruktur yang diperlukan dalam Anda Akun AWS untuk mengirimkan informasi perubahan status alarm dari akun Anda ke AWS Managed Services.

Anda dapat mengunduh file kebijakan JSON di ZIP ini: EventsServiceRolePolicy.zip.

AWS kebijakan terkelola: AWSManagedServices_ContactsServiceRolePolicy

AWS Managed Services (AMS) menggunakan kebijakan terkelola `AWSManagedServices_ContactsServiceRolePolicy` AWS. Kebijakan AWS-managed ini dilampirkan ke peran `AWSServiceRoleForManagedServices_Contacts` terkait layanan, (lihat). Membuat SLR Kontak untuk AMS Accelerate Kebijakan ini memungkinkan AMS Contacts SLR untuk melihat tag sumber daya Anda, dan nilainya, pada sumber daya AWS. Anda tidak dapat melampirkan kebijakan ini ke entitas IAM Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AMS Accelerate.

> **Important**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. AMS menggunakan tag untuk memberi Anda layanan administrasi. Tag tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Untuk pembaruan peran `AWSServiceRoleForManagedServices_Contacts` terkait layanan, lihat. Mempercepat pembaruan ke peran terkait layanan

Detail izin

Kebijakan ini memiliki izin berikut untuk mengizinkan SLR Kontak membaca tag sumber daya Anda untuk mengambil informasi kontak sumber daya yang telah Anda siapkan sebelumnya.

- `IAM`— Memungkinkan layanan Kontak untuk melihat tag pada Peran IAM dan pengguna IAM.
- `Amazon EC2`— Memungkinkan layanan Kontak untuk melihat tag pada EC2 sumber daya Amazon.
- `Amazon S3`— Memungkinkan Layanan Kontak untuk melihat tag di ember Amazon S3. Tindakan ini menggunakan Kondisi untuk memastikan AMS mengakses tag bucket Anda menggunakan header Otorisasi HTTP, menggunakan protokol tanda tangan SiGv4, dan menggunakan HTTPS dengan TLS 1.2 atau yang lebih baru. Untuk informasi selengkapnya, lihat Metode Otentikasi dan Kunci Kebijakan Khusus Autentikasi Amazon S3 Signature Version 4.
- `Tag`— Memungkinkan layanan Kontak untuk melihat tag pada AWS sumber daya lain.

- “saya: ListRoleTags “, “saya: “, ListUserTags “tag: “, GetResources “tag: “, GetTagKeys “tag: “, GetTagValues “ec2: “, DescribeTags “s3:” GetBucketTagging

Anda dapat mengunduh file kebijakan JSON di ZIP ini: ContactsServicePolicy.zip.

Mempercepat pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Accelerate sejak layanan ini mulai melacak perubahan ini.

Ubah	Deskripsi	Tanggal

Kebijakan yang diperbarui - Deployment Toolkit	• Izin baru ini ditambahkan untuk sumber daya`aarn:aws:ecr:*:*:repository/ams-cdktoolkit*` :
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		April 4, 2024

Ubah	Deskripsi	Tanggal

Kebijakan yang diperbarui - Deployment Toolkit	• Izin baru ini ditambahkan untuk sumber daya `arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*` :
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
	• Izin baru ini ditambahkan untuk sumber daya `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :
	`ecr:CreateRepository`
	`ecr:DeleteLifecyclePolicy`
	`ecr:DeleteRepository`
	`ecr:DeleteRepositoryPolicy`
	`ecr:DescribeRepositories`
	`ecr:GetLifecyclePolicy`
	`ecr:ListTagsForResource`
	`ecr:PutImageTagMutability`
	`ecr:PutLifecyclePolicy`
	`ecr:SetRepositoryPolicy`
	`ecr:TagResource`
	`ecr:UntagResource`
	• Juga, beberapa tindakan yang ada dengan wildcard dicakup ke tindakan individu:
	`- s3:DeleteObject*`
	`+ s3:DeleteObject`
	`+ s3:DeleteObjectTagging`
	`+ s3:DeleteObjectVersion`
	`+ s3:DeleteObjectVersionTagging`
	`- s3:GetObject*`
		9 Mei 2023

Ubah	Deskripsi	Tanggal

	<pre>+ s3:GetObject
	+ s3:GetObjectAcl
	+ s3:GetObjectAttributes
	+ s3:GetObjectLegalHold
	+ s3:GetObjectRetention
	+ s3:GetObjectTagging
	+ s3:GetObjectVersion
	+ s3:GetObjectVersionAcl
	+ s3:GetObjectVersionAttributes
	+ s3:GetObjectVersionForReplication
	+ s3:GetObjectVersionTagging
	+ s3:GetObjectVersionTorrent
	
	- cloudformation:UpdateTermination*
	+ cloudformation:UpdateTerminationProtection</pre>	

Kebijakan yang diperbarui — Detective Controls	• CloudFormation Tindakan telah dicakup lebih lanjut setelah konfirmasi dengan tim keamanan dan akses • Tindakan Lambda telah dihapus dari kebijakan karena tidak berdampak pada boarding onboarding/off	10 April 2023
Kebijakan yang diperbarui — Detective Controls	`ListAttachedRolePolicies` Tindakan dihapus dari kebijakan. Tindakan tersebut memiliki Resource sebagai wildcard (*). Karena “daftar” adalah tindakan non-mutatif, itu diberikan akses ke semua sumber daya, dan wildcard tidak diizinkan.	Maret 28, 2023
Kebijakan yang diperbarui — Detective Controls	Memperbarui kebijakan dan menambahkan kebijakan batas izin.	21 Maret 2023

Ubah	Deskripsi	Tanggal
Kebijakan baru - Layanan Kontak	Accelerate menambahkan kebijakan baru untuk melihat informasi kontak akun Anda dari tag sumber daya Anda. Accelerate menambahkan kebijakan baru untuk membaca tag sumber daya Anda sehingga dapat mengambil informasi kontak sumber daya yang telah Anda siapkan sebelumnya.	16 Februari 2023
Kebijakan baru - Layanan Acara	Accelerate menambahkan kebijakan baru untuk mengirimkan informasi perubahan status alarm dari akun Anda ke AWS Managed Services. Memberikan peran IAM yang dibuat sebagai bagian dari Bagaimana Manajer Alarm bekerja izin untuk membuat aturan terkelola Amazon EventBridge yang diperlukan.	Februari 07, 2023
Kebijakan yang diperbarui - Deployment Toolkit	Menambahkan izin S3 untuk mendukung offboarding pelanggan dari Accelerate.	30 Januari 2023
Kebijakan baru — Detective Controls	Memungkinkan peran terkait layanan,Detektif mengontrol peran terkait layanan untuk AMS Accelerate, untuk menyelesaikan tindakan bagi Anda untuk menerapkan Mempercepat kontrol detektif.	19 Desember 2022
Kebijakan baru - Manajer Alarm	Accelerate menambahkan kebijakan baru untuk mengizinkan izin menjalankan tugas pengelola alarm. Memberikan peran IAM yang dibuat sebagai bagian dari Bagaimana Manajer Alarm bekerja izin untuk melakukan operasi seperti evaluasi Config AWS , AWS Config read to fetch alarm manager configuration, pembuatan alarm Amazon yang diperlukan. CloudWatch	30 November 2022

Ubah	Deskripsi	Tanggal
Mempercepat mulai melacak perubahan	Accelerate mulai melacak perubahan untuk kebijakan yang AWS dikelola.	30 November 2022
Kebijakan baru - Deployment Toolkit	Accelerate menambahkan kebijakan ini untuk tugas penerapan. Memberikan AWSServiceRoleForAWSManagedServicesDeploymentToolkitizin peran terkait layanan untuk mengakses dan memperbarui bucket dan tumpukan Amazon S3 terkait penerapan. AWS CloudFormation	Juni 09, 2022

Perlindungan data di Accelerate

AMS Accelerate memanfaatkan native Layanan AWS seperti Amazon GuardDuty, Amazon Macie (opsional), dan alat dan proses kepemilikan internal lainnya, untuk terus memantau akun terkelola Anda. Setelah alarm dipicu, AMS Accelerate bertanggung jawab atas triase awal dan respons terhadap alarm. Proses respons AMS didasarkan pada standar NIST. AMS Accelerate secara teratur menguji proses respons menggunakan Simulasi Respons Insiden Keamanan dengan Anda untuk menyelaraskan alur kerja Anda dengan program respons keamanan pelanggan yang ada.

Ketika AMS Accelerate mendeteksi pelanggaran, atau ancaman pelanggaran yang akan segera terjadi, AWS atau kebijakan keamanan Anda, Accelerate mengumpulkan informasi, termasuk sumber daya yang terkena dampak dan perubahan terkait konfigurasi apa pun. AMS Accelerate 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. Accelerate menyelidiki temuan dengan pakar keamanan internal untuk menganalisis aktivitas dan memberi tahu Anda melalui kontak eskalasi keamanan yang tercantum di akun Anda.

Berdasarkan temuan, Accelerate secara proaktif terlibat dengan Anda. Jika Anda menemukan bahwa 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 Accelerate 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.

Monitor dengan Amazon Macie

AMS Accelerate mendukung, dan merupakan praktik terbaik untuk digunakan, Amazon Macie untuk mendeteksi daftar data sensitif yang besar dan komprehensif, seperti informasi kesehatan pribadi (PHI), informasi identitas pribadi (PII), dan data keuangan.

Anda dapat mengonfigurasi Macie untuk berjalan secara berkala di bucket Amazon S3 apa pun. Ini mengotomatiskan evaluasi objek baru atau yang dimodifikasi dalam ember dari waktu ke waktu. Saat temuan keamanan dihasilkan, AMS memberi tahu Anda dan bekerja sama dengan Anda untuk memulihkan temuan sesuai kebutuhan.

Untuk informasi lebih lanjut, lihat Menganalisis temuan Amazon Macie.

Monitor dengan 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 di lingkungan Anda. AWS Ini mungkin termasuk masalah seperti eskalasi hak istimewa, penggunaan kredensional yang terbuka, atau komunikasi dengan alamat IP berbahaya, atau domain. GuardDuty memantau perilaku Akun AWS akses untuk tanda-tanda kompromi, seperti penerapan infrastruktur yang tidak sah, instance yang diterapkan di Wilayah yang belum pernah Anda gunakan. AWS GuardDuty juga mendeteksi panggilan API yang tidak biasa, seperti perubahan kebijakan kata sandi untuk mengurangi kekuatan kata sandi. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna GuardDuty .

Untuk melihat dan menganalisis GuardDuty temuan Anda, selesaikan langkah-langkah berikut:

1. Buka GuardDuty konsol di https://console.aws.amazon.com/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.

Gunakan aturan GuardDuty penekanan untuk memfilter temuan

Aturan penekanan adalah seperangkat kriteria yang terdiri dari atribut filter yang dipasangkan dengan nilai. Anda dapat menggunakan aturan penekanan untuk menyaring temuan bernilai rendah yang tidak ingin Anda tindaklanjuti, seperti temuan positif palsu, atau aktivitas yang diketahui. Memfilter temuan Anda membantu mempermudah mengenali ancaman keamanan yang mungkin berdampak paling besar terhadap lingkungan Anda.

Untuk memfilter temuan, aturan penekanan secara otomatis mengarsipkan temuan baru yang sesuai dengan kriteria yang Anda tentukan. Temuan yang diarsipkan tidak dikirim ke AWS Security Hub, Amazon S3, CloudTrail atau Acara. Jadi, filter penekanan mengurangi data yang tidak dapat ditindaklanjuti jika Anda menggunakan temuan melalui GuardDuty Security Hub atau aplikasi peringatan dan tiket SIEM pihak ketiga.

AMS memiliki serangkaian kriteria yang ditentukan untuk mengidentifikasi aturan penekanan untuk akun terkelola Anda. Ketika akun terkelola memenuhi kriteria ini, AMS menerapkan filter dan membuat permintaan layanan (SR) kepada Anda yang merinci filter penekanan yang diterapkan.

Anda dapat berkomunikasi dengan AMS melalui SR untuk memodifikasi atau mengembalikan filter penekanan.

Lihat temuan yang diarsipkan

GuardDuty terus menghasilkan temuan bahkan ketika temuan tersebut sesuai dengan aturan penindasan Anda. Temuan yang ditekan ditandai sebagai diarsipkan. GuardDuty menyimpan temuan yang diarsipkan selama 90 hari. Anda dapat melihat temuan yang diarsipkan di GuardDuty konsol selama 90 hari tersebut dengan memilih Diarsipkan dari tabel temuan. Atau, lihat temuan yang diarsipkan melalui GuardDuty API menggunakan ListFindingsAPI dengan FindingCriteria of service.archived sama dengan true.

Kasus penggunaan umum untuk aturan penindasan

Jenis temuan berikut memiliki kasus penggunaan umum untuk menerapkan aturan penekanan.

- Recon: EC2 /Portscan: Gunakan aturan penekanan untuk mengarsipkan temuan secara otomatis saat menggunakan pemindai kerentanan resmi.
- UnauthorizedAccess:EC2/SSHBrutePaksa: Gunakan aturan penekanan untuk mengarsipkan temuan secara otomatis saat ditargetkan ke instance benteng.
- Recon:EC2/PortProbeUnprotectedPort: Gunakan aturan penekanan untuk mengarsipkan temuan secara otomatis ketika ditargetkan ke instance yang sengaja diekspos.

Monitor dengan 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 diaktifkan. Wilayah AWS
- Satu aturan bernama `DefaultSecurityMonitoringRule` dengan prioritas 1 dalam grup `DefaultSecurityMonitoringRule` aturan, menggunakan daftar Domain `AWSManagedDomainsAggregateThreatList` 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 layanan.

Enkripsi data di AMS Accelerate

AMS Accelerate menggunakan beberapa Layanan AWS untuk enkripsi data.

Amazon Simple Storage Service menawarkan beberapa opsi enkripsi objek yang melindungi data saat transit dan saat istirahat. 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.

AWS Identity and Access Management di AMS Accelerate

AWS Identity and Access Management 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 orientasi AMS Accelerate, Anda bertanggung jawab untuk membuat peran administrator IAM lintas akun dalam setiap akun terkelola Anda.

Di AMS Accelerate, Anda bertanggung jawab untuk mengelola akses ke sumber daya Anda Akun AWS dan sumber daya dasarnya, seperti solusi manajemen akses, kebijakan akses, dan

proses terkait. Ini berarti Anda mengelola siklus hidup pengguna, izin dalam layanan direktori, dan sistem otentikasi federasi, untuk mengakses konsol atau. AWS AWS APIs Untuk membantu Anda mengelola solusi akses, AMS Accelerate menerapkan AWS Config aturan yang mendeteksi kesalahan konfigurasi IAM yang umum, dan mengirimkan pemberitahuan remediasi. Untuk informasi selengkapnya, lihat AWS Config Managed Rules.

Mengautentikasi dengan identitas di AMS Accelerate

AMS menggunakan peran IAM, yang merupakan jenis identitas IAM. Peran IAM 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, dapat 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. AMS menggunakan peran IAM berikut.

> **Note**
>
> Peran akses AMS memungkinkan operator AMS mengakses sumber daya Anda untuk menyediakan kemampuan AMS (lihatDeskripsi layanan). Mengubah peran ini dapat menghambat kemampuan kita untuk menyediakan kemampuan ini. Jika Anda perlu mengubah peran akses AMS, konsultasikan dengan Cloud Architect Anda.

Nama peran	Deskripsi
Digunakan oleh (entitas): Hanya Layanan Akses AMS	
ams-access-management	Digunakan secara manual oleh Anda selama orientasi. Diasumsikan hanya oleh akses AMS untuk menyebarkan atau memperbarui peran akses. Tetap berada di akun Anda setelah melakukan onboarding untuk pembaruan masa depan untuk peran akses.
Digunakan oleh (entitas): Operasi AMS	

Nama peran	Deskripsi
ams-access-admin-operations	Peran ini memiliki izin administratif untuk beroperasi di akun, tetapi tidak memiliki izin untuk membaca, menulis, atau menghapus konten pelanggan dalam AWS layanan yang biasa digunakan sebagai penyimpanan data, seperti Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift, dan Amazon. ElastiCache Hanya sedikit individu AMS terpilih yang dapat mengambil peran ini.
ams-access-operations	Peran Operasi AMS ini memiliki izin untuk melakukan tugas administratif di akun Anda. Peran ini tidak memiliki izin membaca, menulis, atau menghapus konten pelanggan dalam AWS layanan yang biasa digunakan sebagai penyimpanan data, seperti Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift, dan Amazon. ElastiCache Izin untuk melakukan operasi AWS Identity and Access Management penulisan juga dikecualikan dari peran ini.
ams-access-read-only	Peran hanya-baca AMS ini terbatas pada izin hanya-baca di akun AMS Anda. Izin membaca konten pelanggan dalam AWS layanan yang biasa digunakan sebagai penyimpanan data, seperti Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift, dan, tidak diberikan oleh peran ElastiCache ini.
Digunakan oleh (entitas): Operasi AMS dan Layanan AMS	

Nama peran	Deskripsi
ams_ssm_automation_role	Diasumsikan oleh AWS Systems Manager untuk mengeksekusi dokumen SSM Automatio n dalam akun Anda.
ams_ssm_automation_role	
Digunakan oleh (entitas): AMS Security	
ams-access-security-analyst	Peran keamanan AMS ini memiliki izin di akun AMS Anda untuk melakukan pemantauan peringatan keamanan khusus dan penangana n insiden keamanan. Hanya sedikit individu AMS Security terpilih yang dapat mengambil peran ini. Izin membaca konten pelanggan di AWS layanan yang biasa digunakan sebagai penyimpanan data, seperti Amazon S3;, Amazon RDS;, Amazon DynamoDB, Amazon Redshift, dan, tidak diberikan oleh peran ini. ElastiCache
ams-access-security-analyst-baca-saja	Peran keamanan AMS ini terbatas pada izin hanya-baca di akun AMS Anda untuk melakukan pemantauan peringatan keamanan khusus dan penanganan insiden keamanan. Izin membaca konten pelanggan di AWS layanan yang biasa digunakan sebagai penyimpanan data, seperti Amazon S3;, Amazon RDS;, Amazon DynamoDB, Amazon Redshift, dan, tidak diberikan oleh peran ini. ElastiCache
Digunakan oleh (entitas): AWS Services	
ams-access-admin	Peran admin AMS ini memiliki izin penuh untuk beroperasi di akun tanpa batasan. Hanya layanan internal AMS (dengan kebijakan sesi tertutup) yang dapat mengambil peran admin.

Nama peran	Deskripsi
ams-opscenter-eventbridge-role	Diasumsikan oleh Amazon EventBridge untuk membuat AWS Systems Manager OpsItems sebagai bagian dari alur kerja Aturan AWS Config remediasi khusus AMS.
AMSOSConfigurationCustomerInstanceRole	Peran IAM ini diterapkan ke EC2 instans Amazon Anda ketika layanan konfigurasi OS AMS menemukan bahwa kebijakan IAM yang diperlukan tidak ada. Ini memungkinkan EC2 instans Amazon Anda berinteraksi dengan AWS Systems Manager, Amazon CloudWatc h, dan EventBridge layanan Amazon. Ini juga telah melampirkan kebijakan AMS yang dikelola khusus untuk mengaktifkan akses RDP ke instance Windows Anda.
mc-patch-glue-service-peran	Diasumsikan oleh alur kerja AWS Glue ETL untuk melakukan transformasi data dan mempersiapkannya untuk generator laporan AMS Patch.
Digunakan oleh (entitas): Layanan AMS	
ams-alarm-manager- AWSManaged ServicesA larmManagerDe - <8-digit hash>	Diasumsikan oleh infrastruktur manajer alarm AMS dalam akun AMS Anda untuk melakukan Aturan AWS Config evaluasi AWS AppConfig penerapan baru.
ams-alarm-manager- AWSManaged ServicesA larmManagerRe - <8-digit hash>	Diasumsikan oleh infrastruktur remediasi manajer alarm AMS dalam akun AMS Anda untuk memungkinkan pembuatan atau penghapusan alarm untuk perbaikan.
ams-alarm-manager- AWSManaged ServicesA larmManager SS- <8-digit hash>	Diasumsikan oleh AWS Systems Manager untuk memanggil layanan remediasi manajer alarm AMS dalam akun AMS Anda.

Nama peran	Deskripsi
ams-alarm-manager- AWSManaged ServicesAlarmManagerTr - <8-digit hash>	Diasumsikan oleh infrastruktur manajer alarm AMS dalam AWS akun Anda untuk melakukan Aturan AWS Config evaluasi AMS berkala.
ams-alarm-manager- AWSManaged ServicesAlarmManagerVa - <8-digit hash>	Diasumsikan oleh infrastruktur manajer alarm AMS dalam akun AMS Anda untuk memastikan bahwa alarm yang diperlukan ada di AWS akun.
ams-backup-iam-role	Peran ini digunakan untuk berjalan AWS Backup di dalam akun Anda.
ams-pemantauan- - AWSManaged ServicesLogGroupLimitLamb <8-digit hash>	Diasumsikan oleh infrastruktur AMS Logging & Monitoring di akun AMS Anda untuk mengevaluasi batas grup Amazon CloudWatch Logs dan membandingkannya dengan kuota layanan.
ams-monitoring- AWSManaged Layanan RDSMonitoring RDSE- <8-digit hash>	Diasumsikan oleh infrastruktur AMS Logging & Monitoring di akun AMS Anda untuk meneruskan peristiwa Amazon RDS ke Amazon CloudWatch Events.
ams-pemantauan- - AWSManaged ServicesRedshiftMonitorin <8-digit hash>	Diasumsikan oleh infrastruktur Pencatatan & Pemantauan AMS di akun AMS Anda untuk meneruskan peristiwa Amazon Redshift (CreateCluster dan DeleteCuster) ke Acara Amazon CloudWatch .
ams-monitoring-infrastruc- AWSManaged ServicesMonito - <8-digit hash>	Diasumsikan oleh infrastruktur AMS Logging & Monitoring di akun AMS Anda untuk mempublikasikan pesan ke Amazon Simple Notification Service untuk memvalidasi bahwa akun tersebut melaporkan semua data yang diperlukan.

Nama peran	Deskripsi
ams-opscenter-role	Diasumsikan oleh sistem Manajemen Pemberitahuan AMS di akun AMS Anda untuk mengelola AWS Systems Manager OpsItems terkait dengan peringatan di akun Anda.
ams-opsitem-autoexecution-role	Diasumsikan oleh sistem Manajemen Pemberitahuan AMS untuk menangani remediasi otomatis menggunakan dokumen SSM untuk memantau peringatan yang terkait dengan sumber daya di akun Anda.
ams-patch-infrastructure-amspatchconfigrulero leC1- <8-digit hash>	Diasumsikan oleh AWS Config untuk mengevaluasi sumber daya patch AMS dan mendeteksi penyimpangan di AWS CloudForm ation tumpukannya.
ams-patch-infrastructure-amspatchcwruleopsite mams- <8-digit hash>	Diasumsikan oleh Amazon EventBridge AWS Systems Manager OpsItems untuk membuat kegagalan penambalan.
ams-patch-infrastructure-amspatchser vicebusamspat- <8-digit hash>	Diasumsikan oleh Amazon EventBridge untuk mengirim acara ke bus acara orkestrator AMS Patch untuk AWS Systems Manager Pemeliharaan Pemberitahuan perubahan status Windows.
ams-patch-reporting-infra-amspatchreportingco nfigr- <8-digit hash>	Diasumsikan oleh AWS Config untuk mengevaluasi sumber daya pelaporan AMS Patch dan mendeteksi penyimpangan di AWS CloudFormation tumpukannya.
ams-resource-tagger- AWSManaged ServicesR esourceTagg - <8-digit hash>	Diasumsikan oleh infrastruktur AMS Resource Tagger dalam akun AMS Anda untuk melakukan Aturan AWS Config evaluasi pada AWS AppConfig penerapan baru.

Nama peran	Deskripsi
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Diasumsikan oleh infrastruktur AMS Resource Tagger dalam akun AMS Anda untuk memvalidasi bahwa AWS tag yang diperlukan ada untuk sumber daya terkelola.
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Diasumsikan oleh AWS Systems Manager untuk menjalankan alur kerja remediasi AMS Resource Tagger di akun AMS Anda.
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Diasumsikan oleh infrastruktur remediasi AMS Resource Tagger dalam akun AMS Anda untuk membuat atau menghapus AWS tag untuk sumber daya terkelola.
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Diasumsikan oleh infrastruktur AMS Resource Tagger dalam AWS akun Anda untuk melakukan evaluasi Aturan Konfigurasi AMS secara berkala.
ams_os_configuration_event_rule_role- <AWS Region>	Diasumsikan oleh Amazon EventBridge untuk meneruskan peristiwa dari akun Anda ke layanan konfigurasi OS AMS EventBus di Wilayah yang benar.
mc-patch-reporting-service	Diasumsikan oleh agregator data patch AMS dan generator laporan.

Note

Ini adalah template untuk ams-access-management peran tersebut. Ini adalah tumpukan yang diterapkan oleh arsitek cloud (CAs) secara manual di akun Anda saat onboarding: management-role.yaml.
Ini adalah template untuk berbagai peran akses dan tingkat akses: ams-access-read-only,, ams-access-operations ams-access-admin-operations, ams-access-admin: accelerate-roles.yaml.

Untuk mempelajari lebih lanjut tentang AWS Cloud Development Kit (AWS CDK) (AWS CDK) pengidentifikasi, termasuk hash, lihat Unik. IDs

Layanan fitur AMS Accelerate ams-access-adminberperan untuk akses terprogram ke akun, tetapi dengan kebijakan sesi yang dicakup untuk masing-masing layanan fitur (misalnya, tambalan, cadangan, pemantauan, dan sebagainya).

AMS Accelerate mengikuti praktik terbaik industri untuk memenuhi dan mempertahankan kelayakan kepatuhan. AMS Mempercepat akses ke akun Anda dicatat CloudTrail dan juga tersedia untuk ditinjau melalui pelacakan perubahan. Untuk informasi tentang kueri yang dapat Anda gunakan untuk mendapatkan informasi ini, lihatMelacak perubahan di akun AMS Accelerate.

Mengelola akses menggunakan kebijakan

Berbagai tim dukungan AMS Accelerate seperti Operations Engineers, Cloud Architects, dan Cloud Service Delivery Manager (CSDMs), terkadang memerlukan akses ke akun Anda untuk menanggapi permintaan dan insiden layanan. Akses mereka diatur oleh layanan akses AMS internal yang memberlakukan kontrol, seperti pembenaran bisnis, permintaan layanan, item operasi, dan kasus dukungan. Akses default hanya baca, dan semua akses dilacak dan direkam; lihat juga. Melacak perubahan di akun AMS Accelerate

Validasi sumber daya IAM

Sistem akses Akselerasi AMS secara berkala mengambil peran dalam akun Anda (setidaknya setiap 24 jam) dan memvalidasi bahwa semua sumber daya IAM kami sesuai dengan yang diharapkan.

Untuk melindungi akun Anda, AMS Accelerate memiliki “kenari” yang memantau dan mengkhawatirkan keberadaan dan status peran IAM, serta kebijakan terlampirnya, yang disebutkan di atas. Secara berkala, kenari mengambil ams-access-read-onlyperan dan memulai CloudFormation dan panggilan API IAM terhadap akun Anda. Kenari mengevaluasi status peran akses Akselerasi AMS untuk memastikan peran tersebut selalu tidak dimodifikasi dan. up-to-date Aktivitas ini membuat CloudTrail log di akun.

Nama sesi AWS Security Token Service (AWS STS) kenari adalah AMS-access-roles-auditor- {uuid4 ()} seperti yang terlihat di dan panggilan API berikut terjadi: CloudTrail

- Panggilan API Pembentukan Awan: `describe_stacks()`
- Panggilan API IAM:
  - `get_role()`

- `list_attached_role_policies()`
- `list_role_policies()`
- `get_policy()`
- `get_policy_version()`
- `get_role_policy()`

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 ditambal 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 kredenal 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 kredenal 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 ditambal dan dipelihara secara berkelanjutan oleh AMS.

Selama pengoperasian instance, AMS memantau anomali perilaku atau aktivitas melalui berbagai kontrol deteksi keamanan, termasuk Amazon, Network Traffic GuardDuty, dan Amazon internal Threat Intelligence feed.

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 acara pada instance dengan GuardDuty. 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.

Pencatatan dan pemantauan peristiwa keamanan di Accelerate

Akun yang terdaftar di AMS Accelerate dikonfigurasi dengan penerapan dasar CloudWatch Peristiwa dan Alarm yang telah dioptimalkan untuk mengurangi kebisingan dan untuk mengidentifikasi indikasi insiden yang sebenarnya. AMS Accelerate juga digunakan GuardDuty untuk pemantauan akun. Lihat informasi yang lebih lengkap di Monitor dengan GuardDuty.

Kepatuhan konfigurasi di Accelerate

AMS Accelerate membantu Anda mengonfigurasi sumber daya Anda dengan standar tinggi untuk keamanan dan integritas operasional, serta mematuhi standar industri berikut:

- Pusat Keamanan Internet (CIS)
- Institut Nasional Standar dan Teknologi (NIST) Kerangka Keamanan Cloud (CSF)
- Undang-Undang Akuntabilitas dan Portabilitas Asuransi Kesehatan (HIPAA)
- Standar Keamanan Data Industri Kartu Pembayaran (PCI) (DSS)

Kami melakukan ini dengan menerapkan seluruh AWS Config aturan kepatuhan kami yang ditetapkan ke akun Anda, lihatPustaka Aturan Konfigurasi AMS. AWS Config Aturan mewakili konfigurasi yang diinginkan untuk sumber daya dan dievaluasi terhadap perubahan konfigurasi pada pengaturan sumber daya Anda AWS . Setiap perubahan konfigurasi memicu sejumlah besar aturan untuk menguji kepatuhan. Misalnya, Anda membuat bucket Amazon S3, dan mengonfigurasinya agar dapat dibaca publik, yang melanggar standar NIST. bucket-public-read-prohibited Aturan ams-nist-cis-s 3 mendeteksi pelanggaran dan memberi label bucket S3 Anda Tidak Sesuai dalam Laporan

Konfigurasi Anda. Karena aturan ini termasuk dalam kategori remediasi Insiden Otomatis, ia segera membuat Laporan Insiden, memperingatkan Anda tentang masalah tersebut. Pelanggaran aturan lain yang lebih parah dapat menyebabkan AMS memperbaiki masalah secara otomatis. Lihat Tanggapan terhadap pelanggaran di Accelerate.

> **Important**
>
> Jika Anda ingin kami berbuat lebih banyak, misalnya, jika Anda ingin AMS memulihkan pelanggaran untuk Anda, terlepas dari kategori remediasinya, kirimkan Permintaan Layanan yang meminta AMS untuk memulihkan sumber daya yang tidak sesuai untuk Anda. Dalam Permintaan Layanan, sertakan komentar seperti “Sebagai bagian dari perbaikan aturan konfigurasi AMS, harap pulihkan sumber daya non-keluhan*RESOURCE_ARNS_OR_IDs*, aturan konfigurasi *CONFIG_RULE_NAME* di akun” dan tambahkan masukan yang diperlukan untuk memulihkan pelanggaran.
> Jika Anda ingin kami melakukan lebih sedikit, misalnya, jika Anda tidak ingin kami mengambil tindakan pada bucket S3 tertentu yang memerlukan akses publik berdasarkan desain, Anda dapat membuat pengecualian, lihat. Membuat pengecualian aturan di Accelerate

Pustaka Aturan Konfigurasi AMS

Accelerate menerapkan pustaka aturan konfigurasi AMS untuk melindungi akun Anda. Aturan konfigurasi ini dimulai dengan`ams-`. Anda dapat melihat aturan dalam akun Anda, dan status kepatuhannya, baik dari AWS Config konsol, AWS CLI, atau API. AWS Config Untuk informasi umum tentang penggunaan AWS Config, lihat ViewingConfiguration Kepatuhan.

> **Note**
>
> Untuk keikutsertaan Wilayah AWS, dan Wilayah cloud gov, kami hanya menerapkan subset aturan konfigurasi karena pembatasan Wilayah. Periksa ketersediaan aturan di Wilayah dengan memeriksa tautan yang terkait dengan pengenal di tabel aturan konfigurasi AMS Accelerate.
> Anda tidak dapat menghapus Aturan Konfigurasi AMS yang diterapkan.

Tabel Aturan

Unduh sebagai ams_config_rules.zip.

Aturan Konfigurasi AMS

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-guardduty-diaktifkan-terpusat	GuardDuty	Berkala	Remediasi	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 2.2,3.4,8.2.1;
ams-nist-cis-vpc-flow-logs-enabled	VPC	Berkala	Remediasi	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A) ,164.312 (b); PCI: 2.2,10.1,10.3.3.2,10.3.3,10.3.4,10.3.5,10.3.6;
ams-eks-secrets-encrypted	EKS	Berkala	Insiden	CIS: NA; NIST-CSF: NA; HIPAA: NA; PCI: NA;
ams-eks-endpoint-no-akses publik	EKS	Berkala	Insiden	CIS: NA; NIST-CSF: NA; HIPAA: NA; PCI: NA;
ams-nist-cis-vpc-default-security-group-closed	VPC	Perubahan Config	Insiden	CIS: CIS.11 , CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.312 (e) (1); PCI: 1.2,1.3,2.1,2.2,1.2.1,1.3.2.2.2.2;
ams-nist-cis-iam-katasandi-kebijakan	IAM	Berkala	Insiden	CIS: NA; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (3) (ii) (A) ,164.308 (a) (3) (ii) (B),

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
				164.308 (a) (4) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (B) ,164.308 (a) (4) (ii) (C) ,164.312 (a) (1); PCI: 7.1.2,7.1.3,7.2.1. 1.7.2.2;
ams-nist-cis-iam-root-access-key-check	IAM	Berkala	Insiden	CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (3) (ii) (A), 164.308 (a) (3) (ii) (B) ,164.308 (a) (4) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (B) ,164.308 (a) (4) (ii) (C) ,164.312 (a) (1); PCI: 2.2,7.1.2,7.1.3.7.2.1.7.2.2;
ams-nist-cis-iam-user-mfa-enabled	IAM	Berkala	Insiden	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (3) (ii) (A) ,164.308 (a) (3) (ii) (B) ,164.308 (a) (4) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (B) ,164.308 (a) (4) (ii) (C) ,164.312 (a) (1); PCI: 2.2,7.1.2,7.1.1.3.7.2.1.1.7 .2.2;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-restricted-ssh	Grup Keamanan	Perubahan Config	Insiden	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (b) ,164.308 (a) (4) (ii) (c), 164.308 312 (a) (1); PCI: 2.2,7.2.1,8.1.4;
ams-nist-cis-restricted-pelabuhan umum	Grup Keamanan	Perubahan Config	Insiden	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (3) (ii) (B) ,164.308 (a) (4) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (B) ,164.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,2.2,1.2.1.1.1.1.3.2 ,2,2.2.2;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-s3- account-level-public-access -blok	S3	Perubahan Config	Insiden	CIS: CIS.9, CIS.12, CIS.14; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 4.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.2.1,1.3,1.3.1,1.3.2,1 .3.4,1.3.6.2.2.2.2.2;
ams-nist-cis-s3- bucket-public-read-prohibited	S3	Perubahan Config	Insiden	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 4.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,2.2,1.2.1,1.3.1,1.3 .2,1.3.4,1.3.3.6.2.2.2;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-s3- bucket-public-write-prohibited	S3	Perubahan Config	Insiden	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 4.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,2.2,1.2.1,1.3.1,1.3 .2,1.3.4,1.3.3.6.2.2.2;
ams-nist-cis-s3 bucket-server-side-encryption - diaktifkan	S3	Perubahan Config	Insiden	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (c) (2) ,164.312 (e) (2) (ii); PCI: 2.2,3.4,10.5,8.2.1;
ams-nist-cis-securityhub-diaktifkan	Security Hub	Berkala	Insiden	CIS: CIS.3 , CIS.4, CIS.6, CIS.12, CIS.16, CIS.19; NIST-CSF: PR.DS-5, PR.PT-1; HIPAA: 164.312 (b); PCI: NA;
ams-nist-cis-ec2- instance-managed-by-systems - manajer	EC2	Perubahan Config	Laporan	CIS: CIS.2, CIS.5; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: 164.308 (a) (5) (ii) (B); PCI: 2.4;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-cloudtrail-diaktifkan	CloudTrail	Berkala	Laporan	CIS: CIS.16, CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.MA-2, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A), 164.308 (a) (5) (ii) (c), 164.312 (b); PCI: 10.1,10.2.1,10.2.2 ,10.2.3,10.2.4,10.2.5,10.2.6,10.2.7,10.3.1,10.3.3.2,10.3.3,10.3.3.4,10.3.3.5,10.3.6;
ams-nist-cis-access-kunci-diputar	IAM	Berkala	Laporan	CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164.308 (a) (4) (ii) (B); PCI: 2.2;
ams-nist-cis-acm-certificate-expiration-check	Certificate Manager	Perubahan Config	Laporan	CIS: CIS.13 , CIS.14; NIST-CSF: PR.AC-5, PR.PT-4; HIPAA: NA; PCI: 4.1;
ams-nist-cis-alb- http-to-https-redirection-periksa	ALB	Berkala	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (1) ,164.312 (e) (2) (i) ,164.312 (e) (2) (ii); PCI: 2.3,4.1,8.2.1;
ams-nist-cis-api- gw-cache-enabled-and -dienkripsi	API Gateway	Perubahan Config	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 3.4;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-api-gw-execution-logging-enabled	API Gateway	Perubahan Config	Laporan	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164.312 (b); PCI: 10.1,10.3 .1,10.3.2,10.3.3,10.3.4,10. 3.5,10.3.6,10.5.4;
ams-nist-autoscaling-group-elb-healthcheck-required	ELB	Perubahan Config	Laporan	CIS: NA; NIST-CSF: PR.PT-1, PR.PT-5; HIPAA: 164.312 (b); PCI: 2.2;
ams-nist-cis-cloud-trail-encryption-enabled	CloudTrail	Berkala	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 2.2,3.4,10.5;
ams-nist-cis-cloud- trail-log-file-validation - diaktifkan	CloudTrail	Berkala	Laporan	CIS: CIS.6; NIST-CSF: PR.DS-6; HIPAA: 164.312 (c) (1) ,164.312 (c) (2); PCI: 2.2,10.5,11.5,10.5 .2,10.5.5;
ams-nist-cis-cloudtrail-s3-dataevents-diaktifkan	CloudTrail	Berkala	Laporan	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A) ,164.312 (b); PCI: 2.2,10.1,10.2.1,10.2.2,10.2 .3,10.2.5,10.3.1,10.3.2.2,1 0.3.3,10.3.4,10.3.5,10.3.6;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-cloudwatch-alarm-action-check	CloudWatch	Perubahan Config	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: NA; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 3.4;
ams-nist-cis-cloudwatch-log-group-encrypted	CloudWatch	Berkala	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: NA; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 3.4;
ams-nist-cis-codebuild-project-envvar-awscred-check	CodeBuild	Perubahan Config	Laporan	CIS: CIS.18; NIST-CSF: PR.DS-5; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (C) ,164.312 (a) (1); PCI: 8.2.1;
ams-nist-cis-codebuild- project-source-repo-url-periksa	CodeBuild	Perubahan Config	Laporan	CIS: CIS.18; NIST-CSF: PR.DS-5; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (C) ,164.312 (a) (1); PCI: 8.2.1;
ams-nist-cis-db-instance-backup-enabled	RDS	Perubahan Config	Laporan	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i) ,164.308 (a) (7) (ii) (ii) (ii); PCI: NA;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-dms-replication-not-public	DMS	Berkala	Laporan	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 4.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.3.6,2.2.2;
ams-nist-dynamodb-autoscaling-diaktifkan	DynamoDB	Berkala	Laporan	CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i) ,164.308 (a) (7) (ii) (C); PCI: NA;
ams-nist-cis-dynamodb-pitr-diaktifkan	DynamoDB	Berkala	Laporan	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i) ,164.308 (a) (7) (ii) (ii) (ii); PCI: NA;
ams-nist-dynamodb-throughput-cek batas	DynamoDB	Berkala	Laporan	CIS: NA; NIST-CSF: NA; HIPPER: 164.312 (b); PCI: NA;
ams-nist-ebs-optimized-contoh	EBS	Perubahan Config	Laporan	CIS: NA; NIST-CSF: NA; HIPAA: 164.308 (a) (7) (i); PCI: NA;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-ebs-snapshot-public-restorable-check	EBS	Berkala	Laporan	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 4.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.3.6,2.2.2;
ams-nist-ec2- instance-detailed-monitoring-enabled	EC2	Perubahan Config	Laporan	CIS: NA; NIST-CSF: DE.AE-1, PR.PT-1; HIPAA: 164.312 (b); PCI: NA;
ams-nist-cis-ec2- instance-no-public-ip	EC2	Perubahan Config	Laporan	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6.2.2.2;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-ec2-managedinstance-association-compliance-status -periksa	EC2	Perubahan Config	Laporan	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii)) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2;
ams-nist-cis-ec2-managedinstance-patch-compliance-status -periksa	EC2	Perubahan Config	Laporan	CIS: CIS.2, CIS.5; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: 164.308 (a) (5) (ii) (B); PCI: 6.2;
ams-nist-cis-ec2-stopped-instance	EC2	Berkala	Laporan	CIS: CIS.2 ; NIST-CSF: ID.AM-2, PR.IP-1; HIPA: NA; PCI: NA;
ams-nist-cis-ec2- volume-in use-check	EC2	Perubahan Config	Laporan	CIS: CIS.2 ; NIST-CSF: PR.IP-1; HIPA: NA; PCI: NA;
ams-nist-cis-efs-terenkripsi-periksa	EFS	Berkala	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 3.4,8.2.1;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-eip-Terlampir	EC2	Perubahan Config	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 3.4,8.2.1;
ams-nist-cis-elasticache-redis-cluster-automatic-backup -periksa	ElastiCache	Berkala	Laporan	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i) ,164.308 (a) (7) (ii) (ii) (ii); PCI: NA;
ams-nist-cis-opensearch-encrypted-at-rest	OpenSearch	Berkala	Laporan	CIS: CIS.14, CIS.13; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 3.4,8.2.1;
ams-nist-cis-opensearch-in-vpc-only	OpenSearch	Berkala	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 3.4,8.2.1;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-elb-acm-certificate-required	Certificate Manager	Perubahan Config	Laporan	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2;
ams-nist-elb-deletion-proteksi-diaktifkan	ELB	Perubahan Config	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (1) ,164.312 (e) (2) (i) ,164.312 (e) (2) (ii); PCI: 4.1,8.2.1;
ams-nist-cis-elb-logging-diaktifkan	ELB	Perubahan Config	Laporan	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164.312 (b); PCI: 10.1,10.3.1,10.3.2,10.3.3,10.3.4,10.3.5,10.3.6,10.5.4;
ams-nist-cis-emr-kerberos-diaktifkan	EMR	Berkala	Laporan	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164.312 (b); PCI: 10.1,10.3.1,10.3.2,10.3.3,10.3.4,10.3.5,10.3.6,10.5.4;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-emr-master-no-public-ip	EMR	Berkala	Laporan	CIS: CIS.14, CIS.16; NIST-CSF: PR.AC-1, PR.AC-4, PR.AC-6; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (3) (ii) (A), 164.308 (a) (3) (ii) (B) ,164.308 (a) (4) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (B) ,164.308 (a) (4) (ii) (C) ,164.312 (a) (1); PCI: 7.2.1;
ams-nist-cis-encrypted-volume	EBS	Perubahan Config	Laporan	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii)) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2;
ams-nist-cis-guardduty-non-archived-findings	GuardDuty	Berkala	Laporan	CIS: CIS.12 , CIS.13, CIS.16, CIS.19, CIS.3, CIS.4, CIS.6, CIS.8; NIST-CSF: DE.AE-2, DE.AE-3, DE.CM-4, DE.DP-5, ID.RA-1, ID.RA-3, PR.DS-5, PR.PT-1; HIPAA: 164.308 (a) (5) (ii) (C) ,164.308 (a) (6) (ii) ,164.312 (b); PCI: 6.1,11.4,5.1.2;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-iam-group-has-users-check	IAM	Perubahan Config	Laporan	CIS: NA; NIST-CSF: PR.AC-4, PR.AC-1; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (3) (ii) (A) ,164.308 (a) (3) (ii) (B), 164.308 (a) (4) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (B) ,164.308 (a) (4) (ii) (C) ,164.312 (a) (1); PCI: 7.1.2,7.1.3,7.2.1. 1.7.2.2;
ams-nist-cis-iam- policy-no-statements-with -akses admin	IAM	Perubahan Config	Laporan	CIS: CIS.16; NIST-CSF: PR.AC-6, PR.AC-7; HIPAA: 164.308 (a) (4) (ii) (B) ,164.308 (a) (5) (ii) (D) ,164.312 (d); PCI: 8.2.3,8.2.4,8.2.5;
ams-nist-cis-iam-user-group-membership-check	IAM	Perubahan Config	Laporan	CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (B) ,164.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (a) (2) (i); PCI: 2.2,7.1.2,7.2.1,8.1.1;
ams-nist-cis-iam-user-no-policies-check	IAM	Perubahan Config	Laporan	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-7; HIPAA: 164.308 (a) (4) (ii) (B) ,164.312 (d); PCI: 8.3;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-iam-user-unused-credentials-check	IAM	Berkala	Laporan	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (3) (ii) (A) ,164.308 (a) (3) (ii) (B) ,164.308 (a) (4) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (B) ,164.308 (a) (4) (ii) (C) ,164.312 (a) (1); PCI: 2.2,7.1.2,7.1.3,7.2.2.1,7.2.2;
ams-nist-cis-ec2- instances-in-vpc	EC2	Perubahan Config	Laporan	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (3) (ii) (B) ,164.308 (a) (4) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (B) ,164.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,2.2,1.2.1.1.1.1.3.2,2,2.2.2;
ams-nist-cis-internet-gateway-authorized-vpc-only	Internet Gateway	Berkala	Laporan	CIS: CIS.9 , CIS.12; NIST-CSF: NA; HIPAA: NA; PCI: NA;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-kms- cmk-not-scheduled-for-penghapusan	KMS	Berkala	Laporan	CIS: CIS.13 , CIS.14; NIST-CSF: PR.DS-1; HIPA: NA; PCI: 3.5,3.6;
ams-nist-lambda-concurrency-periksa	Lambda	Perubahan Config	Laporan	CIS: NA; NIST-CSF: NA; HIPPER: 164.312 (b); PCI: NA;
ams-nist-lambda-dlq-periksa	Lambda	Perubahan Config	Laporan	CIS: NA; NIST-CSF: NA; HIPPER: 164.312 (b); PCI: NA;
ams-nist-cis-lambda-function-public-access-prohibited	Lambda	Perubahan Config	Laporan	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,2.2.2;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-lambda-dalam-vpc	Lambda	Perubahan Config	Laporan	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii)) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1 .3.4,2.2.2;
ams-nist-cis-mfa- enabled-for-iam-console-akses	IAM	Berkala	Laporan	CIS: CIS.16 ; NIST-CSF: PR.AC-7; HIPA: 164.312 (d); PCI: 2.2,8.3;
ams-nist-cis-multi-region-cloudtrail-enabled	CloudTrail	Berkala	Laporan	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.MA-2, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A) ,164.312 (b); PCI: 2.2,10.1,10.1.1,10 .2.2.2,10.2.3,10.2.4,10.0.0 .2.5,10.2.6,10.2.7,10.3.1,1 0.3.3.2,10.3.3,10.3.4,10.3. 5,10.3.6;
ams-nist-rds-enhanced-pemantauan-diaktifkan	RDS	Perubahan Config	Laporan	CIS: NA; NIST-CSF: PR.PT-1; HIPA: 164.312 (b); PCI: NA;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-rds-instance-public-access-check	RDS	Perubahan Config	Laporan	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 4.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.3.6,2.2.2;
ams-nist-rds-multi-az-dukungan	RDS	Perubahan Config	Laporan	CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i) ,164.308 (a) (7) (ii) (C); PCI: NA;
ams-nist-cis-rds-snapshots-public-prohibited	RDS	Perubahan Config	Laporan	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 4.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.3.6,2.2.2;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-rds-penyimpanan-dienkripsi	RDS	Perubahan Config	Laporan	CIS: CIS.13, CIS.5, CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-1, PR.PT-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (b) ,164.312 (e) (2) (ii); PCI: 3.4,10.1,10.1,10.0 .2.1,10.2.2,10.2.3,10.2.4,1 0.2.5,10.3.1,10.3.3.2,10.3. 3,10.3.4,10.3.5,10.3.6.8.2. 1;
ams-nist-cis-redshift-cluster-configuration-check	RedShift	Perubahan Config	Laporan	CIS: CIS.6, CIS.13, CIS.5; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-1, PR.PT-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (b) ,164.312 (e) (2) (ii); PCI: 3.4,8.1,12.2.0.1,1 0.2.1,10.2.2,10.2.3,10.2.4, 10.2.5,10.3.1,10.3.3.2,10.3 .3,10.3.3.4,10.3.5,10.3.6;
ams-nist-cis-redshift-cluster-public-access-check	RedShift	Perubahan Config	Laporan	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 4.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1 .3.4,1.3.3.6,2.2.2;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-redshift-require-tls-ssl	RedShift	Berkala	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (1) ,164.312 (e) (2) (i) ,164.312 (e) (2) (ii); PCI: 2.3,4.1;
ams-nist-cis-root-account-hardware-mfa-enabled	IAM	Berkala	Laporan	CIS: CIS.16 , CIS.4; NIST-CSF: PR.AC-7; HIPAA: 164.312 (d); PCI: 2.2,8.3;
ams-nist-cis-root-account-mfa-enabled	IAM	Berkala	Laporan	CIS: CIS.16 , CIS.4; NIST-CSF: PR.AC-7; HIPAA: 164.312 (d); PCI: 2.2,8.3;
ams-nist-cis-s3- bucket-default-lock-enabled	S3	Perubahan Config	Laporan	CIS: CIS.14 , CIS.13; NIST-CSF: ID.BE-5, PR.PT-5, RC.RP-1; HIPA: NA; PCI: NA;
ams-nist-cis-s3- bucket-logging-enabled	S3	Perubahan Config	Laporan	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A) ,164.312 (b); PCI: 2.2,10.1,10.2.1,10.2.2,10.2.3,10.2.4,10.2.5,10.2.2.7,10.3.1,10.3.2,10.3.3,10.3.4, 10.3.3.5,10.3.6;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-s3- bucket-replication-enabled	S3	Perubahan Config	Laporan	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i) ,164.308 (a) (7) (ii) (ii) (ii); PCI: 2.2,10.5.3;
ams-nist-cis-s3- bucket-ssl-requests-only	S3	Perubahan Config	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv) ,164.312 (c) (2) ,164.312 (e) (1) ,164.312 (e) (2) (i) ,164.312 (e) (2) (ii); PCI: 2.2,4.1,8.2.1;
ams-nist-cis-s3- bucket-versioning-enabled	S3	Berkala	Laporan	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.DS-6, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i) ,164.308 (a) (7) (ii) (A) ,164.308 (a) (7) (ii) (B) ,164.312 (c) (1) ,164.312 (c) (2); PCI: 10.5.3;
ams-nist-cis-sagemaker-endpoint-configuration-kms-key - dikonfigurasi	SageMaker	Berkala	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 3.4,8.2.1;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-sagemaker-notebook-instance-kms-key -dikonfigurasi	SageMaker	Berkala	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 3.4,8.2.1;
ams-nist-cis-sagemaker-notebook-no-direct-internet-akses	SageMaker	Berkala	Laporan	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C) ,164.312 (a) (1) ,164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2;
ams-nist-cis-secretsmanager-rotation-enabled-check	Secrets Manager	Perubahan Config	Laporan	CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164.308 (a) (4) (ii) (B); PCI: NA;
ams-nist-cis-secretsmanager-scheduled-rotation-success-check	Secrets Manager	Perubahan Config	Laporan	CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164.308 (a) (4) (ii) (B); PCI: NA;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-nist-cis-sns-terenkripsi-kms	SNS	Perubahan Config	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 8.2.1;
ams-nist-cis-vpc- sg-open-only-to -port resmi	VPC	Perubahan Config	Laporan	CIS: CIS.11 , CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3. 1.2.2.2.2;
ams-nist-vpc-vpn-2-terowongan	VPC	Perubahan Config	Laporan	CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i); PCI: NA;
ams-cis-ec2-ebs-encryption-by-default	EC2	Berkala	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 2.2,3.4,8.2.1;
ams-cis-rds-snapshot-dienkripsi	RDS	Perubahan Config	Laporan	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 3.4,8.2.1;

Nama Aturan	Layanan	Pemicu	Tindakan	Kerangka Kerja
ams-cis-redshift-cluster-pengaturan pemeliharaan-periksa	RedShift	Perubahan Config	Laporan	CIS: CIS.5; NIST-CSF: PR.DS-4, PR.IP-1, PR.IP-4; HIPAA: 164.308 (a) (5) (ii) (A) ,164.308 (a) (7) (ii) (A); PCI: 6.2;

Tanggapan terhadap pelanggaran di Accelerate

Semua pelanggaran Aturan Config muncul di Laporan Konfigurasi Anda. Ini adalah respons universal. Bergantung pada Kategori Remediasi (tingkat keparahan) aturan, AMS mungkin mengambil tindakan tambahan, dirangkum dalam tabel berikut. Untuk detail tentang cara menyesuaikan Kode Tindakan untuk aturan tertentu, lihatTanggapan temuan yang disesuaikan.

Tindakan Remediasi

Kode Aksi	Tindakan AMS
Laporan	1. Tambahkan ke Config Report
Insiden	1. Tambahkan ke Config Report 2. Laporan insiden otomatis di Accelerate
Remediasi	1. Tambahkan ke Config Report 2. Laporan insiden otomatis di Accelerate 3. Remediasi otomatis di Accelerate

Meminta Bantuan Tambahan

> **Note**
>
> AMS dapat memulihkan pelanggaran apa pun untuk Anda, terlepas dari kategori remediasinya. Untuk meminta bantuan, kirimkan Permintaan Layanan, dan tunjukkan sumber daya mana yang Anda ingin AMS perbaiki dengan komentar seperti “Sebagai bagian dari perbaikan aturan konfigurasi AMS, harap pulihkan *RESOURCE_ARNS_OR_IDs* sumber daya

non-keluhan ARNs/IDs>, aturan konfigurasi *CONFIG_RULE_NAME* di akun" dan tambahkan input yang diperlukan untuk memulihkan pelanggaran.

AMS Accelerate memiliki perpustakaan dokumen AWS Systems Manager otomatisasi dan runbook untuk membantu memulihkan sumber daya yang tidak sesuai.

Tambahkan ke Config Report

AMS menghasilkan Laporan Config yang melacak status kepatuhan semua aturan dan sumber daya di akun Anda. Anda dapat meminta laporan dari CSDM Anda. Anda juga dapat meninjau status kepatuhan dari konsol AWS Config, AWS CLI, atau Config API. AWS Laporan Config Anda meliputi:

- Sumber daya teratas yang tidak patuh di lingkungan Anda, untuk menemukan potensi ancaman dan kesalahan konfigurasi
- Kepatuhan sumber daya dan aturan konfigurasi dari waktu ke waktu
- Deskripsi aturan konfigurasi, tingkat keparahan aturan, dan langkah-langkah perbaikan yang disarankan untuk memperbaiki sumber daya yang tidak sesuai

Ketika sumber daya apa pun masuk ke status tidak patuh, status sumber daya (dan status aturan) menjadi Tidak Sesuai dalam Laporan Config Anda. Jika aturan tersebut termasuk dalam kategori remediasi Config Report Only, secara default, AMS tidak akan mengambil tindakan lebih lanjut. Anda selalu dapat membuat Permintaan Layanan untuk meminta bantuan atau perbaikan tambahan dari AMS.

Untuk detail selengkapnya, lihat AWS Pelaporan Config.

Laporan insiden otomatis di Accelerate

Untuk pelanggaran aturan yang cukup berat, AMS secara otomatis membuat Laporan Insiden untuk memberi tahu Anda bahwa sumber daya telah masuk ke status tidak patuh, dan menanyakan tindakan mana yang ingin Anda lakukan. Anda memiliki opsi berikut saat menanggapi suatu insiden:

- Minta AMS memulihkan sumber daya yang tidak sesuai yang tercantum dalam insiden tersebut. Kemudian, kami mencoba untuk memulihkan sumber daya yang tidak patuh, dan memberi tahu Anda setelah insiden yang mendasarinya diselesaikan.
- Anda dapat menyelesaikan item yang tidak sesuai secara manual di konsol atau melalui sistem penerapan otomatis Anda (misalnya, pembaruan template CI/CD Pipeline); kemudian, Anda dapat

menyelesaikan insiden tersebut. Sumber daya yang tidak patuh dievaluasi kembali sesuai jadwal aturan dan, jika sumber daya dievaluasi sebagai tidak sesuai, laporan insiden baru dibuat.

- Anda dapat memilih untuk tidak menyelesaikan sumber daya yang tidak patuh dan hanya menyelesaikan insiden tersebut. Jika Anda memperbarui konfigurasi sumber daya nanti, AWS Config akan memicu evaluasi ulang dan Anda akan diperingatkan lagi untuk mengevaluasi ketidakpatuhan sumber daya tersebut.

Remediasi otomatis di Accelerate

Aturan paling kritis termasuk dalam kategori Auto Remediate. Ketidakpatuhan terhadap aturan ini dapat sangat memengaruhi keamanan dan ketersediaan akun Anda. Ketika sumber daya melanggar salah satu aturan ini:

1. AMS secara otomatis memberi tahu Anda dengan Laporan Insiden.
2. AMS memulai remediasi otomatis menggunakan dokumen SSM otomatis kami.
3. AMS memperbarui Laporan Insiden dengan keberhasilan atau kegagalan remediasi otomatis.
4. Jika remediasi otomatis gagal, insinyur AMS menyelidiki masalah ini.

Membuat pengecualian aturan di Accelerate

Fitur pengecualian Aturan AWS Config sumber daya memungkinkan Anda menekan pelaporan sumber daya tertentu yang tidak sesuai untuk aturan tertentu.

> **Note**
>
> Sumber daya yang dikecualikan masih muncul sebagai Tidak Sesuai di konsol Layanan Config AWS Anda. Sumber daya yang dikecualikan muncul dengan tanda khusus di Config Reports (Resource_exception:true). Anda CSDMs dapat memfilter sumber daya tersebut sesuai dengan kolom itu saat membuat laporan.

Jika Anda memiliki sumber daya yang Anda tahu tidak sesuai, Anda dapat menghilangkan sumber daya tertentu untuk aturan konfigurasi tertentu dalam Laporan Config mereka. Untuk melakukannya:

Kirim permintaan layanan ke Accelerate terhadap akun Anda, dengan daftar aturan konfigurasi dan sumber daya yang akan dikecualikan dari laporan. Anda harus memberikan justifikasi bisnis eksplisit (seperti, tidak perlu melaporkannya *`resource_name_1`* dan tidak *`resource_name_2`*

didukung karena kami tidak ingin mereka didukung). Untuk bantuan mengirimkan permintaan layanan Accelerate, lihat. Membuat permintaan layanan di Accelerate

Tempelkan ke permintaan input berikut (untuk setiap sumber daya tambahkan blok terpisah dengan semua bidang yang diperlukan, seperti yang ditunjukkan), lalu kirimkan:

```
[
    {
        "resource_name": "resource_name_1",
        "config_rule_name": "config_rule_name_1",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    },
    {
        "resource_name": "resource_name_2",
        "config_rule_name": "config_rule_name_2",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    }
]
```

Mengurangi AWS Config biaya di Accelerate

Anda dapat mengurangi biaya AWS Config dengan menggunakan opsi untuk merekam jenis `AWS::EC2::Instance` sumber daya secara berkala. Perekaman berkala menangkap perubahan konfigurasi terbaru dari sumber daya Anda setiap 24 jam sekali, mengurangi jumlah perubahan yang dikirimkan. Saat diaktifkan, AWS Config hanya mencatat konfigurasi sumber daya terbaru pada akhir periode 24 jam. Hal ini memungkinkan Anda untuk menyesuaikan data konfigurasi dengan perencanaan operasional tertentu, kepatuhan, dan penggunaan audit kasus yang tidak memerlukan pemantauan berkelanjutan. Perubahan ini direkomendasikan hanya jika Anda memiliki aplikasi yang bergantung pada arsitektur fana, yang berarti Anda terus-menerus menskalakan jumlah instance ke atas atau ke bawah.

Untuk ikut serta dalam perekaman berkala untuk jenis `AWS::EC2::Instance` sumber daya, hubungi Tim Pengiriman AMS Anda.

Tanggapan temuan yang disesuaikan

Anda dapat memilih cara AMS Accelerate merespons beberapa temuan (aturan Config yang tidak sesuai). Anda dapat mengonfigurasi AMS untuk menanggapi temuan itu dengan memulihkan

temuan, meminta persetujuan Anda untuk memulihkan, atau hanya melaporkan kepada Anda dalam Tinjauan Bisnis Bulanan (MBR) berikutnya. Anda dapat mengubah respons default untuk aturan AMS Accelerate Config. Untuk melihat aturan, buka Kepatuhan Konfigurasi > Tabel aturan atau unduh tabel aturan sebagai file ZIP ams_config_rules.zip.

Mengubah respons default membantu Anda meningkatkan status keamanan dan kepatuhan akun Anda dengan memungkinkan lebih banyak temuan untuk diperbaiki. Ketika Anda memulihkan lebih banyak temuan, Anda memiliki lebih sedikit kasus yang perlu menunggu peninjauan dan persetujuan manual. Perpustakaan ekstensif runbook remediasi AMS terus-menerus memperbaiki sumber daya yang tidak sesuai dan Anda dihubungi hanya jika diperlukan.

Respons yang disesuaikan hanya digunakan dengan sumber daya baru atau sumber daya yang ada dengan acara baru. Misalnya, sumber daya yang menjadi tidak sesuai setelah perubahan. Ini karena sumber daya yang lebih tua cenderung memerlukan pemeriksaan lebih dalam sebelum remediasi dan lebih mudah untuk menegakkan remediasi sumber daya saat dibuat atau diubah. Untuk meminta perbaikan temuan untuk sumber daya apa pun kapan saja, kirimkan permintaan layanan.

Meminta perubahan dalam tanggapan default

Cloud Architects (CAs) bekerja dengan Anda selama on-boarding untuk mengumpulkan preferensi Anda. CAskemudian atur konfigurasi awal pada sistem AMS internal. Setelah onboard, buat Permintaan Layanan untuk meminta pembaruan konfigurasi Anda. Anda dapat meminta pembaruan konfigurasi sebanyak yang diperlukan. Harap dicatat bahwa Operasi hanya memperbarui konfigurasi untuk akun tempat permintaan layanan dibuat. Jika Anda perlu memperbarui beberapa akun secara bersamaan, hubungi Cloud Architect Anda. CA Anda akan meminta Anda untuk memotong permintaan layanan dengan preferensi Anda untuk tujuan audit.

Mengubah tanggapan default untuk temuan dan akun Anda

Anda selalu membutuhkan preferensi respons untuk setiap akun dan temuan. AMS menyediakan respons default (lihat Kepatuhan Konfigurasi), jadi konfigurasi ini bersifat opsional. Anda dapat mengubah respons default untuk setiap temuan ke opsi berikut:

- Remediasi: AMS secara manual atau otomatis memulihkan temuan. AMS meninjau remediasi dan memberi tahu Anda jika gagal.
- Minta persetujuan: AMS membuat kasus keluar untuk memberi tahu Anda tentang temuan tersebut. Gunakan opsi ini ketika Anda ingin meninjau temuan sebelum menyetujui remediasi atau mengecualikannya. AMS kemudian mengeksekusi tindakan yang Anda inginkan.

- Tidak ada tindakan (hanya laporan): AMS tidak mengambil tindakan untuk memulihkan atau meningkatkan temuan. Temuan mungkin masih muncul di konsol dan laporan yang disajikan selama MBRs.

> **Note**
>
> Anda tidak dapat mengubah konfigurasi aturan yang harus diperbaiki oleh AMS. Misalnya, mengaktifkan Amazon GuardDuty dan VPC Flow Logs.

Mengubah respons default berdasarkan sumber daya

Anda selanjutnya dapat mengonfigurasi respons terhadap sumber daya tertentu menggunakan tag. Anda dapat menggunakan tag atau sumber daya tag yang sudah ada sebelumnya menggunakan Resource Tagger. Untuk detailnya, lihatMempercepat Tagger Sumber Daya). Konfigurasi untuk sumber daya dengan tag lebih diutamakan daripada tindakan default untuk temuan. Jika sumber daya memiliki beberapa tag dengan konfigurasi terkait yang berbeda, AMS tidak dapat menjalankan remediasi yang disesuaikan. Sebagai gantinya, AMS mengirimi Anda Permintaan Layanan keluar untuk memberi tahu Anda tentang situasinya. Misalnya, untuk temuan yang bucket-server-side-encryptiondiaktifkan s3, Anda dapat:

- Ubah respons ke bucket S3 yang tidak terenkripsi 'remediate' dengan pasangan nilai kunci tag “Regulated: True”
- Ubah respons menjadi 'tidak ada tindakan' saat bucket S3 yang tidak terenkripsi memiliki tag “Regulated: False”, dan
- Ubah respons default bucket S3 yang tidak terenkripsi menjadi 'minta persetujuan. Ini berlaku untuk semua bucket S3 yang tidak memiliki tag “Regulated: True” atau “Regulated: False”

Anda juga dapat menambahkan input yang diperlukan untuk menjalankan respons pencarian kustom. Misalnya, untuk remediasi yang memerlukan kunci enkripsi, Anda dapat memberikan kunci Anda IDs ke AMS. Anda dapat mengubah parameter input dari runbook remediasi, tetapi AMS tidak mendukung integrasi dengan runbook kustom. Untuk deskripsi runbook remediasi AMS di Laporan Config, lihat. AWS Config Laporan Kepatuhan Kontrol

Respon Insiden di Accelerate

Setelah menerima peringatan, tim AMS menggunakan remediasi otomatis dan manual untuk mengembalikan sumber daya ke keadaan sehat. Jika remediasi gagal, AMS memulai proses manajemen insiden untuk berkolaborasi dengan tim Anda. Anda dapat mengubah garis dasar dengan memperbarui konfigurasi default dalam file konfigurasi.

Respons insiden dan orientasi di AMS Accelerate

Selama orientasi, AMS Accelerate menekan pembuatan insiden otomatis untuk sumber daya yang tidak sesuai; sebagai gantinya, Cloud Service Deliver Manager (CSDM) memberi Anda laporan yang berisi semua aturan dan sumber daya ketidakpatuhan untuk peninjauan Anda. Setelah mengidentifikasi aturan yang ingin diperbaiki AMS, buat permintaan layanan di konsol Dukungan Tengah yang menunjukkan aturan dan sumber daya tersebut. Templat Permintaan Layanan berikut adalah contoh permintaan pelanggan ke AMS untuk memulihkan sumber daya yang tidak sesuai secara manual. Jika AMS memiliki pertanyaan tambahan, kami bekerja sama dengan Anda dalam Permintaan Layanan untuk mengumpulkan informasi yang diperlukan.

```
Hello,
Please remediate the following resources for the Config Rule "ENCRYPTED_VOLUMES".
Resource List:
    "Vol-12345678"
    "Vol-87654312"
Thank you
```

Setelah proses orientasi selesai, AMS Accelerate secara otomatis membuat insiden untuk setiap sumber daya yang tidak sesuai untuk aturan yang ditandai sebagai Insiden Otomatis.

Ketahanan dalam Mempercepat

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan zona ketersediaan. Wilayah AWS menyediakan beberapa zona ketersediaan yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan zona ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan database yang secara otomatis gagal di antara zona tanpa interupsi. zona ketersediaan lebih tersedia, toleran kesalahan, dan skalabel daripada infrastruktur pusat data tunggal atau ganda tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan zona ketersediaan, lihat infrastruktur AWS global.

Untuk informasi tentang AMS Mempercepat manajemen kontinuitas, lihatManajemen kontinuitas di AMS Accelerate.

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.

Praktik terbaik keamanan di Accelerate

AMS Accelerate menggunakan paket kesesuaian, yang menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan tindakan terkelola atau kustom dan remediasi. Aturan AWS Config AWS Config Untuk informasi tentang cara terbaik mengonfigurasi paket kesesuaian ini, lihat AWS ConfigPraktik Terbaik Operasional untuk CSF NIST dan Praktik Terbaik Operasional untuk 20 Teratas CIS.

Ubah ulasan keamanan permintaan

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 Mempercepat standar teknistentukan 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 Accelerate 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 Mempercepat standar teknis

Berikut ini adalah Mempercepat kategori standar teknis:

ID	Kategori
AMS-STD-X002	AWS Identity and Access Management
AMS-STD-X003	Keamanan Jaringan
AMS-STD-X004	Pengujian Penetrasi
AMS-STD-X005	Amazon GuardDuty
AMS-STD-X007	Pencatatan

Kontrol standar di AMS Accelerate

Berikut ini adalah kontrol standar di AMS:

AMS-STD-X002 - (IAM) AWS Identity and Access Management

ID	Standar teknis
1.0	Durasi Batas Waktu
1.1	Sesi batas waktu default pengguna federasi adalah satu jam dan dapat ditingkatkan hingga empat jam.

ID	Standar teknis
1.2	Batas waktu sesi RDP untuk Microsoft Windows Server diatur ke 15 menit dan dapat diperpanjang berdasarkan kasus penggunaan.
2.0	AWS Penggunaan Akun Root
2.1	Jika ada penggunaan akun root karena alasan apa pun, Amazon GuardDuty harus dikonfigu rasi untuk menghasilkan temuan yang relevan.
2.2	Kunci akses untuk akun root tidak boleh dibuat.
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.
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/r enewal/extension Namun, izin untuk mengizink an pembacaan objek (misalnya, S3:GetObject) di semua ember S3 di akun tidak diizinkan.

ID	Standar teknis
3.2	Pengguna IAM dan peran untuk konsol dan akses terprogram dengan izin mutasi infrastru ktur 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	Di Server Microsoft Windows, hanya Akun Layanan Terkelola grup Microsoft (GMSA) yang harus dibuat.
4.0	Kebijakan, Tindakan, dan APIs
4.4	Kebijakan tidak boleh memberikan akses administrator dengan pernyataan yang setara dengan “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*” tanpa penerimaan risiko.
4.6	Panggilan API terhadap kebijakan kunci KMS untuk kunci infrastruktur AMS dalam kebijakan IAM pelanggan tidak boleh diizinkan.
4.8	Tindakan, yang mengubah 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.

ID	Standar teknis
4.10	Profil EC2 instans Amazon dengan akses baca ke rahasia atau namespace tertentu di AWS Secrets Manager dalam akun yang sama dapat dibuat.
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	Akses ke bucket S3 ARN yang belum dibuat di akun pelanggan dapat disediakan dengan membatasi akses ke bucket ke akun pelanggan dengan menentukan nomor akun menggunak an kunci kondisi S3 khusus layanan s3:. ResourceAccount
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.
4.18	Peran IAM dengan AWS layanan sebagai prinsipal tepercaya juga harus sejalan dengan standar teknis IAM.

ID	Standar teknis
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 seharusnya tidak mengizinkan pembacaan objek (misalnya, S3:GetObject) di semua bucket S3 di akun.
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, dll) secara manual di salah satu layanan penyimpanan data seperti Amazon S3, Amazon Relational Database Service, Amazon DynamoDB, dan sebagainya, atau dalam sistem file OS.
6.0	Kebijakan Lintas Akun
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).

ID	Standar teknis
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.
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.

ID	Standar teknis
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 dikonfigu rasi hanya jika akun non-AMS dimiliki oleh pelanggan AMS yang sama (dengan mengonfir masi 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.
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

ID	Standar teknis
7.1	Grup IAM dengan izin readonly dan non mutatif diizinkan.
8.0	Kebijakan berbasis sumber daya
8.4	Sumber daya infrastruktur AMS harus dilindungi dari manajemen oleh identitas yang tidak sah dengan lampiran kebijakan berbasis sumber daya.
8.2	Sumber daya pelanggan harus dikonfigurasi dengan kebijakan berbasis sumber daya dengan hak istimewa terkecil, kecuali pelanggan secara eksplisit menentukan kebijakan yang berbeda.

AMS-STD-X003 - Keamanan Jaringan

Berikut ini adalah kontrol standar untuk X003 - Keamanan Jaringan:

ID	Standar teknis
	Jaringan
1.0	Dicadangkan untuk kontrol masa depan
2.0	IP elastis pada EC2 instans diizinkan
3.0	Bidang kontrol AMS dan dengan ekstensi di bidang data TLS 1.2+ harus digunakan.
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

ID	Standar teknis
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
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.

ID	Standar teknis
12.0	AMS Security akan merujuk standar setiap kali grup keamanan diminta untuk dilampirkan ke sebuah instans.
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.
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

ID	Standar teknis
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	Permintaan ICMP masuk ke Amazon EC2 dari infra pelanggan akan memerlukan pemberita huan risiko.
24.0	Permintaan masuk dari publik yang IPs dialihkan ke Amazon VPC melalui DX, VPC-peer, atau VPN melalui grup keamanan diperbolehkan.
25.0	Permintaan masuk dari publik yang IPs tidak diarahkan ke Amazon VPC melalui DX, VPC-peer, atau VPN melalui grup keamanan akan memerlukan penerimaan risiko.
26.0	Permintaan ICMP keluar dari Amazon EC2 ke tujuan mana pun diizinkan.
27.0	Berbagi kelompok keamanan
27.1	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.

ID	Standar teknis
27.2	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-X004 - Pengujian Penetrasi

Berikut ini adalah kontrol standar untuk X004 - 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-X005 - GuardDuty

Berikut ini adalah kontrol standar untuk X005 - GuardDuty

1. GuardDuty harus diaktifkan di semua akun pelanggan setiap saat.
2. GuardDuty peringatan harus disimpan dalam akun yang sama atau akun terkelola lainnya di bawah organisasi yang sama.
3. Fitur daftar IP tepercaya tidak GuardDuty boleh digunakan. Sebaliknya pengarsipan otomatis dapat digunakan sebagai alternatif, yang berguna untuk tujuan audit.

AMS-STD-X007 - Penebangan

Berikut ini adalah kontrol standar untuk X007 - 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.
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.
1.7	Log Aplikasi: Pelanggan diberdayakan untuk mengaktifkan pencatatan di aplikasi mereka dan menyimpannya di grup CloudWatch log Log atau bucket S3.

ID	Standar teknis
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.
1.10	Log Elastic Load Balancing (Classic/Application Load Balancer/NetworkLoad Balancer): Entri akses dan log kesalahan harus disimpan di bucket S3 yang dikelola AMS 2.0.
2.0	Kontrol akses
2.3	Bucket S3 yang diamanatkan 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 pelanggan.
3.0	Retensi log
3.1	Grup CloudWatch log log yang diamanatkan AMS harus memiliki periode retensi minimum 90 hari pada log.
3.2	Ember S3 yang diamanatkan 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. Itu berarti konfigurasikan “Validasi file log” 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 (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.

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 (tulis, 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

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
- High_risk-log-002: Nonaktifkan Log Aliran VPC.
- 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

Lain-lain

- High_risk-enc-001: Nonaktifkan enkripsi di sumber daya apa pun jika diaktifkan

FAQ Keamanan

AMS menyediakan dukungan 24/7/365 follow-the-sun melalui pusat operasi global. Insinyur operasi AMS yang berdedikasi secara aktif memantau dasbor dan antrian insiden. Biasanya, AMS mengelola akun Anda melalui otomatisasi. Dalam keadaan langka yang memerlukan keahlian pemecahan masalah atau penerapan khusus, insinyur operasi AMS dapat mengakses akun Anda. AWS

Berikut ini adalah pertanyaan umum tentang praktik terbaik keamanan, kontrol, model akses, dan mekanisme audit yang digunakan AMS Accelerate saat insinyur operasi AMS atau otomatisasi mengakses akun Anda.

Kapan insinyur operasi AMS mengakses lingkungan saya?

Insinyur operasi AMS tidak memiliki akses terus-menerus ke akun atau instans Anda. Akses ke akun pelanggan diberikan kepada operator AMS hanya untuk kasus penggunaan bisnis yang dapat dibenarkan, seperti peringatan, insiden, permintaan perubahan, dan sebagainya. Akses didokumentasikan dalam AWS CloudTrail log.

Untuk pembenaran akses, pemicu, dan inisiator pemicu, lihat. Pemicu akses akun pelanggan AMS

Peran apa yang diasumsikan oleh insinyur operasi AMS saat mereka mengakses akun saya?

Dalam kasus yang jarang terjadi (~ 5%) yang memerlukan intervensi manusia di lingkungan Anda, insinyur operasi AMS masuk ke akun Anda dengan peran akses default, baca saja. Peran default

tidak memiliki akses ke konten apa pun yang biasanya disimpan di penyimpanan data, seperti Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift, dan Amazon. ElastiCache

Untuk daftar peran yang diperlukan oleh insinyur operasi dan sistem AMS untuk menyediakan layanan di akun Anda, lihatAkun pelanggan AMS mengakses peran IAM.

Bagaimana cara insinyur operasi AMS mengakses akun saya?

Untuk mengakses akun pelanggan, insinyur operasi AMS menggunakan layanan akses AMS AWS internal. Layanan internal ini hanya tersedia melalui saluran pribadi yang aman sehingga akses ke akun Anda aman dan diaudit.

1. Insinyur operasi AMS menggunakan otentikasi layanan akses AMS internal bersama dengan otentikasi dua faktor. Dan, insinyur operasi harus memberikan justifikasi bisnis (tiket insiden atau ID permintaan layanan) yang menguraikan kebutuhan untuk mengakses akun Anda AWS .
2. Berdasarkan otorisasi insinyur operasi, layanan akses AMS memberi insinyur peran yang sesuai (Baca-only/Operator/Admin) dan URL login ke AWS konsol Anda. Akses ke akun Anda berumur pendek dan terikat waktu.
3. Untuk mengakses EC2 instans Amazon, insinyur operasi AMS menggunakan layanan akses AMS internal yang sama dengan broker. Setelah akses diberikan, teknisi operasi AMS menggunakannya AWS Systems Manager Session Manager untuk mengakses instans Anda dengan kredensyal sesi yang berumur pendek.

   Untuk menyediakan akses RDP untuk instans Windows, insinyur operasi menggunakan Amazon EC2 Systems Manager untuk membuat pengguna lokal pada instance dan membuat penerusan port ke instance. Insinyur operasi menggunakan kredensyal pengguna lokal untuk akses RDP ke instance. Kredensi pengguna lokal akan dihapus pada akhir sesi.

Diagram berikut menguraikan proses yang digunakan oleh insinyur operasi AMS untuk mengakses akun Anda:

Bagaimana cara melacak perubahan yang dibuat oleh AMS di AWS akun terkelola AMS saya?

Akses akun

Untuk membantu Anda melacak perubahan yang dibuat oleh otomatisasi atau oleh tim operasi AMS Accelerate, AMS menyediakan antarmuka Ubah catatan SQL di konsol Amazon Athena dan log AMS Accelerate. Sumber daya ini memberikan informasi berikut:

- Siapa yang mengakses akun Anda.
- Ketika akun diakses.
- Hak istimewa apa yang digunakan untuk mengakses akun Anda.
- Perubahan apa yang dilakukan oleh AMS Accelerate di akun Anda.
- Mengapa perubahan dilakukan di akun Anda.

Konfigurasi sumber daya

Lihat CloudTrail log untuk melacak konfigurasi dalam AWS sumber daya Anda selama 90 hari terakhir. Jika konfigurasi Anda lebih tua dari 90 hari, maka akses log di Amazon S3.

Log contoh

CloudWatch Agen Amazon mengumpulkan log sistem operasi. Lihat CloudWatch log untuk melihat login dan log tindakan lain yang didukung sistem operasi Anda.

Untuk informasi selengkapnya, lihat Melacak perubahan di akun AMS Accelerate.

Apa saja kontrol proses untuk akses insinyur operasi AMS ke akun saya?

Sebelum bergabung dengan AMS, insinyur operasi menjalani pemeriksaan latar belakang kriminal. Karena insinyur AMS mengelola infrastruktur pelanggan, mereka juga memiliki pemeriksaan latar belakang tahunan wajib. Jika seorang insinyur gagal dalam pemeriksaan latar belakang, maka akses dicabut.

Semua insinyur operasi AMS harus menyelesaikan pelatihan keamanan wajib, seperti keamanan infrastruktur, keamanan data, dan respons insiden sebelum mereka diberikan akses ke sumber daya.

Bagaimana akses istimewa dikelola?

Sebagian pengguna harus menyelesaikan pelatihan tambahan dan mempertahankan hak akses istimewa untuk akses yang lebih tinggi. Akses dan penggunaan diperiksa dan diaudit. AMS membatasi akses istimewa ke keadaan luar biasa atau ketika akses hak istimewa paling sedikit tidak dapat memenuhi permintaan Anda. Akses istimewa juga terikat waktu.

Apakah insinyur operasi AMS menggunakan MFA?

Ya. Semua pengguna harus menggunakan MFA dan Bukti Kehadiran untuk memberikan layanan kepada Anda.

Apa yang terjadi pada akses mereka ketika karyawan AMS meninggalkan organisasi atau mengubah peran pekerjaan?

Akses ke akun pelanggan dan sumber daya disediakan melalui keanggotaan grup internal. Keanggotaan didasarkan pada kriteria ketat termasuk peran pekerjaan tertentu, manajer pelaporan, dan status pekerjaan di AMS. Jika keluarga pekerjaan insinyur operasi berubah atau ID pengguna mereka dinonaktifkan, maka akses dicabut.

Kontrol akses apa yang mengatur akses insinyur operasi AMS ke akun saya?

Ada beberapa lapisan kontrol teknis untuk menegakkan prinsip “kebutuhan untuk mengetahui” dan “hak istimewa paling kecil” untuk akses ke lingkungan Anda. Berikut ini adalah daftar kontrol akses:

- Semua insinyur operasi harus menjadi bagian dari AWS grup internal tertentu untuk mengakses akun dan sumber daya pelanggan. Keanggotaan grup secara ketat didasarkan pada kebutuhan untuk mengetahui dasar dan otomatis dengan kriteria yang telah ditentukan.
- AMS mempraktikkan akses “non-persistensi” ke lingkungan Anda. Ini berarti bahwa akses ke AWS akun Anda dengan operasi AMS adalah "just-in-time" dengan kredensyal berumur pendek. Akses ke akun Anda diberikan hanya setelah pembenaran kasus bisnis internal (permintaan layanan, insiden, permintaan manajemen perubahan, dan sebagainya) diajukan dan ditinjau.
- AMS mengikuti prinsip hak istimewa paling sedikit. Jadi, insinyur operasi resmi mengasumsikan akses Read-Only secara default. Akses tulis hanya digunakan oleh teknisi ketika perubahan pada lingkungan Anda diperlukan karena insiden atau permintaan perubahan.
- AMS menggunakan AWS Identity and Access Management peran standar dan mudah diidentifikasi yang menggunakan awalan “ams” untuk memantau dan mengelola akun Anda. Semua akses masuk AWS CloudTrail untuk Anda audit.
- AMS menggunakan alat backend otomatis untuk mendeteksi perubahan yang tidak sah pada akun Anda selama fase validasi informasi pelanggan dari eksekusi perubahan.

Bagaimana AMS memantau akses pengguna root?

Akses root selalu memicu proses respons insiden. AMS menggunakan GuardDuty deteksi Amazon untuk memantau aktivitas pengguna root. Jika GuardDuty menghasilkan peringatan, AMS membuat acara untuk penyelidikan lebih lanjut. AMS memberi tahu Anda jika aktivitas akun root yang tidak terduga terdeteksi, dan tim AMS Security memulai penyelidikan.

Bagaimana AMS menanggapi insiden keamanan?

AMS menyelidiki peristiwa keamanan yang dihasilkan dari layanan deteksi seperti Amazon GuardDuty, Amazon Macie, dan dari masalah keamanan yang dilaporkan pelanggan. AMS bekerja sama dengan tim respons keamanan Anda untuk menjalankan proses Security Incident Response (SIR). Proses AMS SIR didasarkan pada kerangka kerja NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide dan memberikan respons keamanan 24/7/365. follow-the-sun AMS bekerja dengan Anda untuk menganalisis dan menahan insiden keamanan dengan cepat.

Sertifikasi dan kerangka kerja standar industri apa yang dipatuhi AMS?

Seperti AWS layanan lainnya, AWS Managed Services disertifikasi untuk OSPAR, HIPAA, HITRUST, GDPR, SOC*, ISO*, FedRAMP (Medium/High), IRAP, dan PCI. Untuk informasi selengkapnya tentang sertifikasi, peraturan, dan kerangka kerja kepatuhan pelanggan yang AWS selaras dengannya, lihat Kepatuhan AWS.

Pagar keamanan

AWS Managed Services menggunakan beberapa kontrol untuk melindungi aset informasi Anda dan membantu menjaga AWS infrastruktur tetap aman. AMS Accelerate mengelola pustaka AWS Config aturan dan tindakan remediasi untuk membantu Anda memastikan bahwa akun Anda mematuhi standar industri untuk keamanan dan integritas operasional. AWS Config aturan terus melacak perubahan konfigurasi pada sumber daya yang Anda rekam. Jika perubahan melanggar ketentuan aturan, maka AMS melaporkan temuannya kepada Anda. Anda dapat memulihkan pelanggaran secara otomatis atau berdasarkan permintaan, sesuai dengan tingkat keparahan pelanggaran.

AMS menggunakan AWS Config aturan untuk membantu memenuhi persyaratan standar berikut:

- Pusat Keamanan Internet (CIS)
- Institut Nasional Standar dan Teknologi (NIST) Kerangka Keamanan Cloud (CSF)
- Undang-Undang Akuntabilitas dan Portabilitas Asuransi Kesehatan (HIPAA)
- Standar Keamanan Data Industri Kartu Pembayaran (PCI) (DSS)

Untuk informasi selengkapnya, lihat Manajemen keamanan di AMS Accelerate

Bagaimana saya bisa mendapatkan akses ke laporan terbaru tentang sertifikasi keamanan, kerangka kerja, dan kepatuhan? AWS

Anda dapat menemukan laporan keamanan dan kepatuhan saat ini untuk AWS layanan menggunakan metode berikut:

- Anda dapat menggunakan AWS Artifactuntuk mengunduh laporan terbaru tentang keamanan, ketersediaan, dan kerahasiaan AWS layanan.
- Untuk daftar sebagian besar AWS layanan, termasuk AWS Managed Services, yang sesuai dengan kerangka kerja kepatuhan global, lihat. https://aws.amazon.com/compliance/services-in-scope/ Misalnya, pilih PCI dan cari AWS Managed Services.

  Anda dapat mencari “AMS” untuk menemukan artefak keamanan khusus AMS dari AWS akun terkelola AMS. AWS Managed Services berada dalam lingkup SOC 3.
- Laporan AWS SOC 2 (System and Organizations Controls) diterbitkan ke AWS Artifact repositori. Laporan ini mengevaluasi AWS kontrol yang memenuhi kriteria keamanan, ketersediaan, dan kerahasiaan di American Institute of Certified Public Accountants (AICPA) TSP bagian 100, Trust Services Criteria.

Apakah AMS berbagi diagram arsitektur referensi dari berbagai aspek fitur AMS?

Untuk melihat arsitektur referensi AMS, unduh AWS Managed Services for Proactive Monitoring PDF.

Bagaimana AMS melacak siapa yang mengakses akun saya dan apa kebutuhan bisnis untuk akses?

Untuk mendukung kelangsungan layanan dan keamanan akun Anda, AMS mengakses akun atau instans Anda hanya sebagai tanggapan terhadap kesehatan atau pemeliharaan proaktif, acara kesehatan atau keamanan, aktivitas yang direncanakan, atau permintaan pelanggan. Akses ke akun Anda diotorisasi melalui proses AMS sebagaimana diuraikan dalam model akses untuk AMS Accelerate. Aliran otorisasi ini berisi pagar pembatas untuk mencegah akses yang tidak disengaja atau tidak pantas. Sebagai bagian dari aliran akses, AMS memasok sistem otorisasi dengan kebutuhan bisnis. Kebutuhan bisnis ini mungkin merupakan item pekerjaan yang terkait

dengan akun Anda, seperti kasus yang Anda buka dengan AMS. Atau, kebutuhan bisnis mungkin berupa alur kerja resmi, seperti solusi Patching. Semua akses memerlukan pembenaran yang divalidasi, diverifikasi, dan diotorisasi secara real time oleh sistem AMS internal berdasarkan aturan bisnis untuk menyelaraskan permintaan akses dengan kebutuhan bisnis.

Insinyur operasi AMS tidak diberi jalur untuk mengakses akun Anda tanpa kebutuhan bisnis yang valid. Semua akses akun dan kebutuhan bisnis terkait dipancarkan ke AWS CloudTrail entri di dalam akun Anda. AWS Ini memberikan transparansi penuh dan kesempatan bagi Anda untuk melakukan audit dan inspeksi Anda sendiri. Selain inspeksi Anda, AMS memiliki inspeksi otomatis, dan melakukan inspeksi manual sesuai kebutuhan, permintaan akses dan melakukan audit perkakas dan akses manusia untuk meninjau akses anomali.

Apakah teknisi AMS memiliki akses ke data saya yang disimpan dalam layanan penyimpanan AWS data, seperti Amazon S3, Amazon RDS, DynamoDB, dan Amazon Redshift?

Insinyur AMS tidak memiliki akses ke konten pelanggan yang disimpan dalam AWS layanan yang biasa digunakan untuk penyimpanan data. Akses yang AWS APIs digunakan untuk membaca, menulis, memodifikasi, atau menghapus data dalam layanan ini dibatasi oleh kebijakan penolakan IAM eksplisit yang terkait dengan peran IAM yang digunakan untuk akses insinyur AMS. Selain itu, pagar pembatas dan otomatisasi AMS internal mencegah insinyur operasi AMS menghapus atau memodifikasi kondisi penolakan.

Apakah insinyur AMS memiliki akses ke data pelanggan yang disimpan di Amazon EBS, Amazon EFS, dan Amazon? FSx

Insinyur AMS dapat masuk ke EC2 instans Amazon sebagai administrator. Akses administrator diperlukan untuk remediasi dalam skenario tertentu yang mencakup, tetapi tidak terbatas pada, masalah sistem operasi (OS) dan kegagalan tambalan. Insinyur AMS biasanya mengakses volume sistem untuk memulihkan masalah yang terdeteksi. Namun, akses untuk insinyur AMS tidak terbatas atau terbatas pada volume sistem.

Bagaimana akses dibatasi atau dikontrol untuk peran otomatisasi yang memiliki hak istimewa tinggi untuk lingkungan saya?

`ams-access-admin`Peran ini digunakan secara eksklusif oleh otomatisasi AMS. Otomatisasi ini menyebarkan, mengelola, dan memelihara sumber daya yang diperlukan yang digunakan oleh

AMS untuk menyebarkan ke lingkungan Anda untuk pengumpulan data telemetri, kesehatan, dan keamanan guna menjalankan fungsi operasional. Insinyur AMS tidak dapat mengambil peran otomatisasi dan dibatasi oleh pemetaan peran dalam sistem internal. Saat runtime, AMS secara dinamis menerapkan kebijakan sesi hak istimewa terkecil yang tercakup ke setiap otomatisasi. Kebijakan sesi ini membatasi kemampuan dan izin otomatisasi.

Bagaimana AMS menerapkan prinsip hak istimewa paling sedikit seperti yang dianjurkan dalam Kerangka Kerja AWS Well-Architected untuk peran otomatisasi?

Saat runtime, AMS menerapkan kebijakan sesi tanpa hak istimewa yang tercakup ke setiap otomatisasi. Kebijakan sesi tertutup ini membatasi kemampuan dan izin otomatisasi. Kebijakan sesi yang memiliki izin untuk membuat sumber daya IAM juga memiliki persyaratan untuk melampirkan batas izin. Batas izin ini mengurangi risiko eskalasi hak istimewa. Setiap tim menerapkan kebijakan sesi yang hanya digunakan oleh tim itu.

Sistem pencatatan dan pemantauan apa yang digunakan untuk mendeteksi upaya akses yang tidak sah atau aktivitas mencurigakan yang melibatkan peran otomatisasi?

AWS memelihara repositori terpusat yang menyediakan fungsionalitas arsip log inti untuk penggunaan internal oleh tim layanan. AWS Log ini disimpan di Amazon S3 untuk skalabilitas, daya tahan, dan ketersediaan yang tinggi. AWS Tim layanan kemudian dapat mengumpulkan, mengarsipkan, dan melihat log layanan di layanan log pusat.

Host produksi di AWS digunakan menggunakan gambar dasar master. Gambar dasar dilengkapi dengan seperangkat konfigurasi dan fungsi standar yang mencakup pencatatan dan pemantauan untuk tujuan keamanan. Log ini disimpan dan dapat diakses oleh tim AWS keamanan untuk analisis akar penyebab jika terjadi insiden keamanan yang dicurigai.

Log untuk host tertentu tersedia untuk tim yang memiliki host tersebut. Tim dapat mencari log mereka untuk analisis operasional dan keamanan.

Bagaimana insiden keamanan atau pelanggaran terkait infrastruktur otomatisasi ditangani, dan protokol apa yang membantu respons dan mitigasi yang cepat?

AWS Rencana darurat dan pedoman respons insiden telah menentukan dan menguji alat dan proses untuk mendeteksi, mengurangi, menyelidiki, dan menilai insiden keamanan. Rencana dan buku pedoman ini mencakup pedoman untuk menanggapi potensi pelanggaran data sesuai dengan persyaratan kontrak dan peraturan.

Apakah penilaian keamanan reguler, pemindaian kerentanan, dan tes penetrasi dilakukan pada infrastruktur otomatisasi?

AWS Keamanan melakukan pemindaian kerentanan reguler pada sistem operasi host, aplikasi web, dan database di AWS lingkungan menggunakan berbagai alat. AWS Tim keamanan juga berlangganan feed berita untuk kelemahan vendor yang berlaku dan secara proaktif memantau situs web vendor dan outlet relevan lainnya untuk tambalan baru.

Bagaimana akses ke infrastruktur otomasi dibatasi hanya untuk personel yang berwenang?

Akses ke AWS sistem dialokasikan berdasarkan hak istimewa yang paling sedikit dan disetujui oleh individu yang berwenang. Tugas dan bidang tanggung jawab (misalnya, permintaan akses dan persetujuan, permintaan dan persetujuan manajemen perubahan, pengembangan perubahan, pengujian dan penyebaran, dan sebagainya) dipisahkan di berbagai individu untuk mengurangi modifikasi atau penyalahgunaan sistem yang tidak sah atau tidak disengaja. AWS Akun grup atau bersama tidak diizinkan dalam batas sistem.

Langkah-langkah apa yang diterapkan untuk menegakkan standar keamanan dan mencegah akses yang tidak sah atau pelanggaran data dalam pipa otomatisasi?

Akses ke sumber daya, termasuk layanan, host, perangkat jaringan, dan grup Windows dan UNIX, disetujui dalam sistem manajemen izin AWS kepemilikan oleh pemilik atau manajer yang sesuai. Log alat manajemen izin menangkap permintaan untuk perubahan akses. Perubahan fungsi Job secara otomatis mencabut akses karyawan ke sumber daya. Akses berkelanjutan untuk karyawan tersebut harus diminta dan disetujui.

AWS memerlukan otentikasi dua faktor melalui saluran kriptografi yang disetujui untuk otentikasi ke AWS jaringan internal dari lokasi terpencil. Perangkat firewall membatasi akses ke lingkungan komputasi, menegakkan batas-batas cluster komputasi, dan membatasi akses ke jaringan produksi.

Proses diimplementasikan untuk melindungi informasi audit dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah. Catatan audit berisi seperangkat elemen data untuk mendukung persyaratan analisis yang diperlukan. Selain itu, catatan audit tersedia bagi pengguna yang berwenang untuk inspeksi atau analisis sesuai permintaan, dan sebagai tanggapan terhadap peristiwa terkait keamanan atau yang berdampak pada bisnis.

Hak akses pengguna ke AWS sistem (misalnya, jaringan, aplikasi, alat, dll.) Dicabut dalam waktu 24 jam setelah penghentian atau penonaktifan. Akun pengguna yang tidak aktif dinonaktifkan and/or dihapus setidaknya setiap 90 hari.

Apakah deteksi atau pemantauan anomali diaktifkan untuk akses atau pencatatan audit guna mendeteksi eskalasi hak istimewa atau penyalahgunaan akses untuk secara proaktif memperingatkan tim AMS?

Host produksi di AWS dilengkapi dengan logging untuk tujuan keamanan. Layanan ini mencatat tindakan manusia pada host, termasuk log on, upaya log on yang gagal, dan log off. Log ini disimpan dan dapat diakses oleh tim AWS keamanan untuk analisis akar penyebab jika terjadi insiden keamanan yang dicurigai. Log untuk host tertentu juga tersedia untuk tim yang memiliki host tersebut. Alat analisis log ujung depan tersedia untuk tim layanan untuk mencari log mereka untuk analisis operasional dan keamanan. Proses diimplementasikan untuk membantu melindungi log dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah. Tim AWS Keamanan melakukan analisis log untuk mengidentifikasi peristiwa berdasarkan parameter manajemen risiko yang ditentukan.

Jenis data pelanggan apa yang diambil dari akun terkelola AMS, dan bagaimana ini digunakan dan disimpan?

AMS tidak mengakses atau menggunakan konten Anda untuk tujuan apa pun. AMS mendefinisikan konten pelanggan sebagai perangkat lunak (termasuk gambar mesin), data, teks, audio, video, atau gambar yang ditransfer oleh pelanggan atau pengguna akhir AWS untuk diproses, disimpan, atau dihosting Layanan AWS sehubungan dengan akun pelanggan, dan hasil komputasi apa pun yang diperoleh pelanggan atau pengguna akhir mereka dari hal tersebut di atas melalui penggunaannya. Layanan AWS

Pemantauan dan manajemen acara di AMS Accelerate

Sistem pemantauan AMS Accelerate memantau AWS sumber daya Anda dari kegagalan, penurunan kinerja, dan masalah keamanan.

Sebagai akun terkelola, AMS Accelerate mengonfigurasi dan menyebarkan alarm untuk AWS sumber daya yang berlaku, memantau sumber daya ini, dan melakukan remediasi bila diperlukan.

Sistem pemantauan AMS Accelerate bergantung pada alat internal, seperti Resource Tagger dan Alarm Manager, dan memanfaatkan Layanan AWS, seperti, AWS AppConfigAmazon ()CloudWatch, Amazon CloudWatch EventBridge (sebelumnya dikenal sebagai), Amazon, Amazon GuardDuty Macie CloudWatch, dan. AWS Health

AMS Accelerate menyediakan berbagai layanan operasional untuk membantu Anda mencapai keunggulan operasional AWS. Untuk mendapatkan pemahaman cepat tentang bagaimana AMS membantu tim Anda mencapai keunggulan operasional secara keseluruhan AWS Cloud dengan beberapa kemampuan operasional utama kami termasuk helpdesk 24x7, pemantauan proaktif, keamanan, penambalan, pencatatan, dan pencadangan, lihat Diagram Arsitektur Referensi AMS.

Topik

- Apa itu pemantauan?
- Cara kerja pemantauan
- Peringatan dari pemantauan dasar di AMS
- Pemberitahuan insiden sadar aplikasi di AMS
- Mempercepat Manajer Alarm
- Remediasi peringatan otomatis AMS
- Menggunakan Aturan EventBridge Terkelola Amazon di AMS
- Remediator Tepercaya di AMS

Untuk informasi tentang pemantauan Amazon EKS, lihat Pemantauan dan manajemen insiden untuk Amazon EKS di AMS Accelerate

Apa itu pemantauan?

AMS Accelerate monitoring memberikan manfaat berikut:

- Konfigurasi default yang membuat, mengelola, dan menerapkan kebijakan di seluruh akun terkelola untuk semua atau AWS sumber daya yang didukung yang Anda pilih.
- Garis dasar pemantauan sehingga Anda memiliki tingkat perlindungan default, bahkan jika Anda tidak mengonfigurasi pemantauan lain untuk akun terkelola Anda. Untuk informasi selengkapnya, lihat Peringatan dari pemantauan dasar di AMS.
- Kemampuan untuk menyesuaikan alarm sumber daya dasar untuk memenuhi kebutuhan Anda.
- Remediasi otomatis peringatan oleh Operasi AMS, 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.
- Visibilitas ke 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. Untuk informasi selengkapnya, lihat Manajemen insiden di AMS Accelerate.
- 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, lihatPeringatan 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, Acara, atau Temuan dari AWS layanan, seperti GuardDuty atau AWS Health.

Cara kerja pemantauan

Lihat grafik berikut tentang arsitektur pemantauan di AWS Managed Services (AMS).

Diagram berikut menggambarkan arsitektur pemantauan AMS Accelerate.

Setelah sumber daya Anda diberi tag berdasarkan kebijakan yang ditentukan menggunakan tagger Resource, dan definisi alarm diterapkan, daftar berikut menjelaskan proses pemantauan 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: 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 Amazon bersama-sama. 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.
- 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.

    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 konfigurasikan 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, konfigurasikan 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 diCara 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

Peringatan dari pemantauan dasar di AMS

Pelajari tentang default pemantauan AMS Mempercepat. Untuk informasi selengkapnya, lihat Pemantauan dan manajemen acara di AMS Accelerate.

Tabel berikut menunjukkan apa yang dipantau dan ambang batas peringatan default. Anda dapat mengubah ambang peringatan dengan dokumen konfigurasi khusus, atau mengirimkan permintaan layanan. Untuk petunjuk tentang mengubah konfigurasi alarm kustom Anda, lihatMengubah konfigurasi Accelerate alarm. Untuk menerima pemberitahuan saat alarm melewati ambang batas, selain proses peringatan standar AMS, Anda dapat menimpa konfigurasi alarm. Untuk petunjuk, lihat Mempercepat Manajer Alarm.

Amazon CloudWatch menyediakan retensi metrik yang diperpanjang. Untuk informasi selengkapnya, lihat CloudWatch Batasan-batasan.

> **Note**
>
> AMS Accelerate mengkalibrasi pemantauan baseline secara berkala. Akun baru selalu disertakan dengan pemantauan dasar terbaru dan tabel menjelaskan pemantauan dasar untuk akun yang baru di-onboard. AMS Accelerate memperbarui pemantauan dasar di akun yang ada secara berkala dan Anda mungkin mengalami penundaan sebelum pembaruan dilakukan.

Peringatan dari pemantauan dasar

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
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, jika Anda ikut serta dalam topik Direct-Customer-Alerts SNS, maka peringatan ini dikirim langsung ke email Anda.		
Contoh Application Load Balancer	ApplicationLoadBalancerErrorCount (HTTPCode_elb_5xx_count/) *100 RequestCount jumlah> 15% untuk 1 menit, 5 kali berturut-turut.	Aplikasi LoadBalancer HTTP 5XX Error Count CloudWatch alarm pada kelebihan jumlah kode respons HTTP 5XX yang dihasilkan oleh Loadbalancer.
Contoh Application Load Balancer	RejectedConnectionCount jumlah> 0% selama 1 menit, 5 kali berturut-turut.	Jumlah Koneksi yang LoadBalancer Ditolak Aplikasi CloudWatch alarm jika jumlah koneksi yang ditolak karena load balancer mencapai maksimum
Target Application Load Balancer	TargetConnectionErrorCount	$ {ElasticLoadBalancingV2:::TargetGroup:FullName} -

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
	(HTTPCode_target_5xx_count/) RequestCount *100 jumlah> 15% untuk 1 menit, 5 kali berturut-turut.	Jumlah Kesalahan Koneksi LoadBalancer Target Aplikasi - $ {ElasticLoadBalancingV2::TargetGroup: :UUID} CloudWatch alarm pada kelebihan jumlah kode respons HTTP 5XX yang dihasilkan oleh target.
Target Application Load Balancer	ApplicationLoadBalancerTargetGroupErrorCount jumlah> 0% selama 1 menit, 5 kali berturut-turut.	$ {ElasticLoadBalancingV2:::TargetGroup:FullName} - LoadBalancer Target Aplikasi HTTP 5XX Jumlah Kesalahan - $ {ElasticLoadBalancingV2::TargetGroup: :UUID} CloudWatch alarm jika jumlah koneksi tidak berhasil dibuat antara penyeimbang beban dan instans terdaftar.
EC2 Contoh Amazon - semua OSs	CPUUtilization* > 95% selama 5 menit, 6 kali berturut-turut.	$ {EC2::InstanceId}: CPU Terlalu Tinggi CloudWatch alarm. Pemanfaatan CPU yang tinggi adalah indikator perubahan status aplikasi seperti kebuntuan, loop tak terbatas, serangan berbahaya, dan anomali lainnya. Ini adalah Direct-Customer-Alerts alarm.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
EC2 Contoh Amazon - semua OSs	StatusCheckFailed > 0% selama 5 menit, 3 kali berturut-turut.	$ {EC2::InstanceId}: Pemeriksaan Status Gagal CloudWatch alarm. Pemeriksaan Status Gagal menunjukkan bahwa EC2 instans Amazon dengan ID yang ditentukan telah gagal satu atau beberapa pemeriksaan status otomatisnya. Ini berarti instance mengalami masalah yang mencegahnya beroperasi dengan benar atau dapat dijangkau.
EC2 Contoh Amazon - Linux	Minimum mem_used_percent >= 95% selama 5 menit, 6 kali berturut-turut.	$ {EC2::InstanceId}: Bebas memori CloudWatch alarm. Memory Free menunjukkan bahwa memori yang tersedia (RAM) pada EC2 instans Amazon yang ditentukan telah turun di bawah ambang batas yang ditentukan. Hal ini dapat menyebabkan masalah memori, sistem crash, dan menunjukkan bahwa instance mungkin membutuhkan lebih banyak RAM. Ini adalah Direct-Customer-Alerts alarm.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
EC2 Contoh Amazon - Linux	Rata-rata swap_used_percent >= 95% selama 5 menit, 6 kali berturut-turut.	$ {EC2::InstanceId}: Swap Gratis CloudWatch alarm. Rata-rata swap_used_percent pada instance EC2 Amazon menunjukkan bahwa persentase rata-rata ruang swap yang dialokasikan saat ini digunakan telah melewati ambang batas yang telah ditentukan. Hal ini dapat menyebabkan degradasi kinerja, kemacetan, dan masalah memori. Ini adalah Direct-Customer-Alerts alarm.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
EC2 Contoh Amazon - Linux	Disk_used_percent maksimum >= 95% selama 5 menit, 6 kali berturut-turut.	$ {EC2::InstanceId}: Penggunaan Disk Terlalu Tinggi - $ {EC2: :Disk: :UUID} CloudWatch alarm. Penggunaan Disk Terlalu Tinggi berarti bahwa penggunaan disk pada Amazon tertentu EC2 atau pada disk yang diidentifikasi, mendekati kapasitasnya. Hal ini dapat menyebabkan degradasi kinerja, kesalahan aplikasi, dan ketidakstabilan sistem. Ini adalah Direct-Customer-Alerts alarm.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
EC2 Contoh Amazon - Windows	Memori Minimum% Byte Berkomitmen dalam Penggunaan >= 95% selama 5 menit, 6 kali berturut-turut.	$ {EC2::InstanceId}: Bebas memori CloudWatch alarm. Memory Free menunjukkan bahwa memori yang tersedia (RAM) pada EC2 instans Amazon yang ditentukan telah turun di bawah ambang batas yang ditentukan. Hal ini dapat menyebabkan masalah memori, sistem crash, dan menunjukkan bahwa instance mungkin membutuhkan lebih banyak RAM. Ini adalah Direct-Customer-Alerts alarm.
EC2 Contoh Amazon - Windows	LogicalDisk Maksimum% Ruang Bebas <= 5% selama 5 menit, 6 kali berturut-turut.	$ {EC2::InstanceId}: Penggunaan Disk Terlalu Tinggi - $ {EC2: :Disk: :UUID} CloudWatch alarm. Menunjukkan bahwa persentase ruang kosong pada disk logis (partisi sistem file) dalam instance Amazon EC2 Windows telah melewati ambang batas yang telah ditentukan. Kekurangan ruang disk dapat menyebabkan kekurangan ruang disk Ini adalah Direct-Customer-Alerts alarm.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
Amazon EFS	AMSEFSBurstCreditBalanceExhausted. BurstCreditBalance kurang dari 1000 selama lima belas menit.	$ {EFS::FileSystemId}: EFS: Saldo Kredit Burst CloudWatch alarm pada BurstCreditBalance sistem file Amazon EFS.
Amazon EFS	AMSEFSClientConnectionsLimit. ClientConnections > 24.000 selama lima belas menit.	$ {EFS::FileSystemId}: EFS: Batas Koneksi Klien CloudWatch alarm pada ClientConnections sistem file Amazon EFS.
Amazon EFS	AMSEFSThroughputUtilizationLimit. Pemanfaatan Throughput EFS > 80% selama satu jam.	$ {EFS::FileSystemId}: EFS: Batas Pemanfaatan Throughput CloudWatch alarm pada Pemanfaatan Throughput dari sistem file Amazon EFS.
Amazon EFS	AMSEFSPercentIOLimit. Persen IOLimit > 95 selama tujuh puluh lima menit.	$ {EFS::FileSystemId}: EFS: Persen IOLimit CloudWatch alarm pada Persentase IOLimit sistem file Amazon EFS.
Amazon EKS	Lihat Amazon EKSPeringatan dasar dalam pemantauan dan manajemen insiden untuk Amazon EKS di AMS Accelerate.	

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
Contoh Elastic Load Balancing	SpilloverCountBack endConnectionErrors > 1 selama 1 menit, 15 kali berturut-turut.	Alarm LoadBalancer Hitungan Spillover Klasik CloudWatch alarm jika kelebihan jumlah permintaa n yang ditolak karena antrian lonjakan penuh.
Contoh Elastic Load Balancing	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.
Contoh Elastic Load Balancing	SurgeQueueLength > 100 selama 1 menit, 15 kali berturut-turut.	Alarm Panjang Antrian LoadBalancer Lonjakan Klasik. CloudWatch alarm jika kelebihan jumlah permintaan sedang menunggu perutean.
FSx untuk ONTAP	AMSFSXONTAPIOPSUti lization. FSX: ONTAP IOPS Utilization > 80% selama dua jam.	$ {FSx::FileSystemId}: FSX:ONTAP IOPS Pemanfaat an CloudWatch alarm pada batas pemanfaatan IOPS FSx untuk instance ONTAP.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
FSx untuk ONTAP	AMSFSXONTAPThroughputPemanfaatan. FSX: ONTAP Throughput Utilization > 80% selama dua jam.	$ {FSx::FileSystemId}: FSX:ONTAP Pemanfaatan Throughput CloudWatch alarm pada batas throughput FSx untuk volume ONTAP.
FSx untuk ONTAP	AMSFSXONTAPVolumeInodeUtilization. FSX: ONTAP Pemanfaatan Inode> 80% selama dua jam.	$ {FSx::FileSystemId} :$ {: :ONTAPFSx::} FSX:ONTAP Pemanfaatan VolumeId Inode CloudWatch alarm pada batas pemanfaatan kapasitas file FSx untuk volume ONTAP.
FSx untuk ONTAP	AMSFSXONTAPVolumeCapacityUtilization. FSX: Pemanfaatan Kapasitas Volume ONTAP> 80% selama dua jam.	$ {FSx::FileSystemId} :$ {: :ONTAPFSx::} VolumeId CloudWatch alarm pada batas pemanfaatan kapasitas volume FSx untuk volume ONTAP.
FSx untuk Windows File Server	AMSFSXWindowsThroughputUtilization. FSX: Pemanfaatan Throughput Windows> 80% selama dua jam.	$ {FSx::FileSystemId}: FSX:Pemanfaatan Throughput Windows CloudWatch alarm pada batas throughput FSx untuk instance Windows File Server.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
FSx untuk Windows File Server	AMSFSXWindowsIOPSUtilization. FSX: Pemanfaatan Windows IOPS > 80% selama dua jam.	$ {FSx::FileSystemId}: FSX:Pemanfaatan IOPS Windows CloudWatch alarm pada batas pemanfaatan IOPS FSx untuk instance Server File Windows.
GuardDuty Layanan	Tidak berlaku; semua temuan (tujuan ancaman) dipantau. Setiap temuan sesuai dengan peringatan. Perubahan GuardDuty temuan. Perubahan ini termasuk temuan yang baru dihasilkan atau kejadian selanjutnya dari temuan yang ada.	Untuk daftar jenis GuardDuty temuan yang didukung, lihat Jenis Pencarian GuardDuty Aktif.
Kondisi	AWS Health Dashboard	Pemberitahuan dikirim ketika ada perubahan status AWS Health Dashboard (AWS Health) peristiwa sehubungan dengan layanan yang dipantau oleh AMS. Untuk informasi selengkapnya, lihat Layanan yang didukung.
IAM	Profil Instans Amazon EC2 IAM tidak ada. Profil instans IAM tidak ada.	Untuk petunjuk cara mengganti profil instans Amazon EC2 IAM, lihat dokumentasi IAM di Ganti peran IAM.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
IAM	Profil Instans Amazon EC2 IAM memiliki terlalu banyak kebijakan. Profil instans IAM memiliki 10 kebijakan dan kebijakan tambahan tidak dapat ditambahkan.	• Ubah Kuota AWS Layanan IAM untuk meningkatkan jumlah kebijakan terkelola per peran menjadi 20. Untuk informasi tentang kuota layanan, lihat Melihat kuota layanan. • Turunkan jumlah kebijakan terkelola di bawah kuota IAM saat ini dengan menghapus kebijakan terkelola yang tidak perlu untuk Peran IAM yang terkait dengan instans ini. Pastikan untuk menjaga kebijakan yang diperlukan AMS. • Turunkan jumlah kebijakan terkelola di bawah kuota IAM saat ini dengan mengkonsolidasikan kebijakan untuk Peran IAM yang terkait dengan instans ini. Pastikan untuk menjaga kebijakan yang diperlukan AMS. Untuk kebijakan yang diperlukan AMS, lihat Panduan Pengguna Akseleras i AMS:Izin IAM mengubah detail.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
Macie	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 Amazon Macie yang didukung, lihat Menganalisis temuan Amazon Macie. Perhatikan bahwa Macie tidak diaktifkan untuk semua akun.
NATGateways	PacketsDropCount : Alarm jika packetsdropcount> 0 selama periode 15 menit	NatGateway PacketsDr opCount Nilai yang lebih besar dari nol dapat menunjukkan masalah sementara yang sedang berlangsung dengan gateway NAT.
NATGateways	ErrorPortAllocation : Alarm jika NAT Gateways tidak dapat mengalokasikan port selama lebih dari 15 menit periode evaluasi	NatGateway ErrorPortAllocatio n Berapa kali gateway NAT tidak dapat mengalokasikan port sumber. Nilai yang lebih besar dari nol menunjukkan bahwa terlalu banyak koneksi bersamaan yang terbuka.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
OpenSearch kluster	ClusterStatus maksimum merah adalah >= 1 selama 1 menit, 1 kali berturut-turut.	ClusterStatus Merah CloudWatch alarm. Kunci AWS KMS enkripsi yang digunakan untuk mengenkripsi data saat istirahat di domain Anda dinonaktifkan. Aktifkan kembali untuk mengembal ikan operasi normal. Untuk mempelajari lebih lanjut, lihat Status Cluster Merah.
OpenSearch domain	KMSKeyKesalahan >= 1 selama 1 menit, 1 kali berturut-turut.	Kesalahan kunci KMS CloudWatch alarm. Setidakny a satu serpihan utama dan replika yang tidak dialokasi kan untuk simpul. Untuk mempelajari lebih lanjut, lihat Enkripsi Data saat Istirahat untuk OpenSearch Layanan Amazon.
OpenSearch domain	KMSKeyTidak dapat diakses >= 1 selama 1 menit, 1 kali berturut-turut.	Kunci KMS Kesalahan Tidak Dapat Diakses CloudWatch alarm. Setidakny a satu serpihan utama dan replika yang tidak dialokasi kan untuk simpul. Untuk mempelajari lebih lanjut, lihat Enkripsi Data saat Istirahat untuk OpenSearch Layanan Amazon.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
OpenSearch domain	ClusterStatus maksimum kuning adalah >= 1 selama 1 menit, 1 kali berturut-turut.	ClusterStatus Kuning Setidaknya satu serpihan replika tidak dialokasikan ke simpul. Untuk mempelajari lebih lanjut, lihat Status Cluster Kuning.
OpenSearch domain	FreeStorageSpace minimum adalah <= 20480 selama 1 menit, 1 kali berturut-turut.	Ruang penyimpanan gratis yang rendah Sebuah simpul di klaster Anda turun ke 20 GiB ruang penyimpanan gratis. Untuk mempelajari lebih lanjut, lihat Kurangnya Ruang Penyimpanan yang Tersedia.
OpenSearch domain	ClusterIndexWritesBlocked >= 1 selama 5 menit, 1 kali berturut-turut.	Indeks Cluster Menulis Diblokir Cluster memblokir permintaan tulis. Untuk mempelajari selengkapnya, lihat ClusterBlockException.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
OpenSearch domain	Simpul minimal < x selama 1 hari, 1 kali berturut-turut.	Node Turun x adalah jumlah simpul dalam klaster Anda. Alarm ini menunjukkan bahwa setidakny a satu simpul di klaster Anda telah tidak terjangkau untuk satu hari. Untuk mempelaja ri selengkapnya, lihat Node Cluster Gagal.
OpenSearch domain	CPUUtilization rata-rata> = 80% selama 15 menit, 3 kali berturut-turut.	Penggunaan CPU yang tinggi di node data Pemanfaatan CPU 100% tidak jarang, tetapi rata-rata tinggi yang berkelanjutan bermasala h. Pertimbangkan ukuran kanan jenis instance yang ada atau menambahkan instance.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
OpenSearch domain	JVMMemoryTekanan maksimal> = 80% selama 5 menit, 3 kali berturut-turut.	Penggunaan memori yang tinggi di node data Klaster bisa mengalami kesalahan kehabisan memori jika penggunaan meningkat . Pertimbangkan penskalaa n secara vertikal. OpenSearc h menggunakan setengah dari RAM instance untuk heap Java, hingga ukuran heap 32 GiB. Anda dapat menskalak an instans secara vertikal hingga 64 GiB RAM, di mana Anda dapat menskalakan secara horizontal dengan menambahkan instans.
OpenSearch domain	Menguasai CPUUtilization rata-rata> = 50% selama 15 menit, 3 kali berturut-turut.	Master Nodes Penggunaan CPU yang tinggi Pertimbangkan untuk menggunakan tipe instans yang lebih besar untuk node master khusus Anda. Karena perannya dalam stabilitas cluster dan penerapan biru/ hijau, node master khusus harus memiliki penggunaa n CPU rata-rata yang lebih rendah daripada node data.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
OpenSearch domain	JVMMemoryTekanan Master maksimal> = 80% selama 15 menit, 1 kali berturut-turut.	Master Node Tekanan Memori JVM Tinggi Pertimbangkan untuk menggunakan tipe instans yang lebih besar untuk node master khusus Anda. Karena perannya dalam stabilitas cluster dan penerapan biru/hijau, node master khusus harus memiliki penggunaa n CPU rata-rata yang lebih rendah daripada node data.
OpenSearch contoh	AutomatedSnapshotFailure maksimum adalah >= 1 selama 1 menit, 1 kali berturut-turut.	Kegagalan snapshot otomatis CloudWatch alarm. Sebuah snapshot otomatis gagal. Kegagalan ini sering merupakan hasil dari status kesehatan klaster merah. Untuk mempelajari lebih lanjut, lihat Status Cluster Merah.
Amazon RDS	Pemanfaatan CPU rata-rata > 90% selama 15 menit, 2 kali berturut-turut.	$ {RDS:: DBInstance Pengidentifikasi}: CPUUtiliz ation CloudWatch alarm.
Amazon RDS	Jumlah DiskQueueDepth > 75% selama 1 menit, 15 kali berturut-turut.	$ {RDS:: DBInstance Pengidentifikasi}: DiskQueue CloudWatch alarm.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
Amazon RDS	Rata-rata FreeStorageSpace < 1.073.741.824 byte selama 5 menit, 2 kali berturut-turut.	$ {RDS:: DBInstance Pengidentifikasi}: FreeStorageSpace CloudWatch alarm.
Amazon RDS	Peringatan Penyimpanan Rendah Pemicu ketika penyimpanan yang dialokasikan untuk instans DB telah habis.	RDS-EVENT-0007, lihat detail di Menggunakan pemberitahuan acara Amazon RDS.
Amazon RDS	Instans DB gagal Instans DB gagal karena konfigurasi tidak kompatibel atau masalah penyimpanan yang mendasarinya. Mulailah a point-in-time-restore untuk instance DB.	RDS-EVENT-0031, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
Amazon RDS	RDS -0034 failover tidak dicoba. Amazon RDS tidak mencoba failover yang diminta karena failover baru-baru ini terjadi pada instans DB.	RDS-EVENT-0034, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
Amazon RDS	RDS - 0035 DB instans parameter tidak valid Misalnya, MySQL tidak dapat memulai karena parameter terkait memori disetel terlalu tinggi untuk kelas instance ini, jadi tindakan Anda adalah memodifikasi parameter memori dan me-reboot instance DB.	RDS-EVENT-0035, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
Amazon RDS	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, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
Amazon RDS	Kesalahan replika baca instans RDS-0045 DB 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.	RDS-EVENT-0045, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
Amazon RDS	RDS-0057 Kesalahan membuat akun pengguna statspack Replikasi pada Read Replica telah berakhir.	Acara layanan. RDS-EVENT -0057, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
Amazon RDS	Replikasi baca instans RDS-0058 DB berakhir Terjadi kesalahan saat membuat akun pengguna Statspack PERFSTAT. Jatuhkan akun sebelum menambahkan opsi Statspack.	Acara layanan. RDS-EVENT -0058, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
Amazon RDS	Pemulihan instans DB dimulai Instans DB SQL Server membangun ulang cerminnya . Performa akan diturunka n 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>[,...])	Acara layanan. RDS-EVENT -0066 lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
Amazon RDS	Failover untuk klaster DB telah gagal.	RDS-EVENT-0069, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
Amazon RDS	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 lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
Amazon RDS	Aurora tidak dapat menyalin data cadangan dari bucket Amazon S3.	RDS-EVENT-0082, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
Amazon RDS	Peringatan penyimpanan rendah ketika instans DB telah mengkonsumsi lebih dari 90% penyimpanan yang dialokasikan.	Acara layanan. RDS-EVENT-0089 lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
Amazon RDS	Layanan notifikasi saat penskalaan gagal untuk klaster DB Tanpa Server Aurora.	Acara layanan. RDS-EVENT-0143 lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
Amazon RDS	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.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
Amazon RDS	Instans DB telah mencapai ambang penyimpanan penuh, dan database telah dimatikan.	RDS-EVENT-0221, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
Amazon RDS	Peristiwa ini menunjukk an penskalaan otomatis penyimpanan instans Amazon 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.
Amazon RDS	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.
Amazon RDS	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.
Amazon RDS	Amazon RDS tidak dapat menyediakan kapasitas untuk proxy karena tidak ada cukup alamat IP yang tersedia di subnet Anda.	RDS-EVENT-0243, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
Amazon RDS	Penyimpanan untuk Anda Akun AWS telah melebihi kuota penyimpanan yang diizinkan.	RDS-EVENT-0254, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.

Jenis Layanan/Sumber Daya	Sumber peringatan dan kondisi pemicu	Nama dan catatan peringatan
Klaster Amazon Redshift	Kesehatan cluster saat tidak dalam mode pemeliharaan < 1 selama 5 menit	RedshiftClusterHealthStatus Untuk informasi selengkap nya, lihat Memantau Amazon Redshift menggunakan CloudWatch metrik.
Site-to-Site VPN	VPNTunnelBawah TunnelState <= 0 selama 1 menit, 20 kali berturut-turut.	$ {AWS::EC2::VpnConn ectionId} - VPNTunnel Turun TunnelState adalah 0 ketika kedua terowongan turun, .5 ketika satu terowongan naik, dan 1.0 ketika kedua terowongan naik.
Agen Systems Manager	EC2 Instans Tidak Dikelola oleh Systems Manager Agen SSM tidak diinstal. Agen SSM diinstal pada instance, tetapi layanan agen tidak berjalan. Agen SSM tidak memiliki rute jaringan ke layanan AWS Systems Manager.	Ada kondisi tambahan yang menyebabkan gangguan pada Agen Systems Manager; untuk informasi selengkapnya, lihat Memecahkan masalah ketersediaan node terkelola.

Untuk informasi tentang upaya remediasi, lihatRemediasi peringatan otomatis AMS.

Tonton video Andrew untuk mempelajari lebih lanjut (7:03)

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 AppRegistryuntuk 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 onboard ke AWS Service Catalog AppRegistry.

Untuk mempelajari selengkapnya tentang AMS Mempercepat pemantauan default, lihat. Pemantauan dan manajemen acara di AMS Accelerate

Onboard ke AppRegistry dan membuat aplikasi

Untuk onboard AppRegistry, lihat Memulai AppRegistry di Panduan AWS Service Catalog AppRegistry Administrator. Setelah onboarding, gunakan salah satu metode berikut untuk membuat aplikasi:

1. AWS konsol: Untuk mempelajari selengkapnya tentang membuat aplikasi AppRegistry melalui AWS konsol, 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.
3. Otomatisasi AMS: Untuk menyederhanakan proses pendaftaran aplikasi, AMS memberi Anda dokumen otomatisasi SSM. `AWSManagedServices-CreateAppRegistryApplication` Untuk menggunakan metode ini, panggil dokumen dari AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/, atau dengan AWS CLI seperti yang dijelaskan dalam contoh berikut.

```
# The following registers a new application with customized severity
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["normal"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# The following registers a new application with no customizations
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
```

```
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# You can also register applications using CloudFormation stacks
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["STACKS"],"AppTagValue":
[""],"CFNStackNames":["arn:aws:cloudformation:us-east-1:123456789012:stack/
stack-2343eddq/1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p"],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
```

Buat tag untuk mengaktifkan pengayaan kasus

Anda harus menandai aplikasi Anda sebelum AMS dapat mengakses metadata aplikasi. Tabel berikut mencantumkan tag yang diperlukan.

Tag dengan awalan `ams:rt:` diterapkan melalui Resource Tagger.

Kunci tanda	Nilai tanda
ams-dikelola	true
ams:rt: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 SeverityLeveldi 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-*
```

Mempercepat Manajer Alarm

AMS Accelerate menerapkan alarm ke AWS sumber daya Anda menggunakan Manajer Alarm berbasis tag untuk menerapkan strategi pemantauan dasar dan memastikan bahwa semua AWS sumber daya Anda dipantau dan dilindungi. Dengan mengintegrasikan dengan Manajer Alarm berbasis tag, Anda dapat menyesuaikan konfigurasi AWS sumber daya Anda berdasarkan jenis, platform, dan tag lainnya, untuk memastikan sumber daya dipantau. Manajer Alarm diterapkan ke akun Accelerate Anda selama orientasi.

Bagaimana Manajer Alarm bekerja

Saat akun Anda di-onboard ke AMS Accelerate, dua dokumen JSON, yang disebut profil konfigurasi, akan digunakan di akun Anda. AWS AppConfig Kedua dokumen profil berada di aplikasi Alarm Manager dan di lingkungan infrastruktur AMS Accelerate.

Kedua profil konfigurasi diberi nama AMSManagedAlarm (profil konfigurasi default) dan CustomerManagedAlarms(profil konfigurasi kustomisasi).

- Profil konfigurasi default:
  - Konfigurasi yang ditemukan di profil ini berisi konfigurasi default yang digunakan AMS Accelerate di semua akun pelanggan. Konfigurasi ini berisi kebijakan pemantauan AMS Accelerate default, yang tidak boleh Anda ubah karena AMS Accelerate dapat memperbarui profil ini kapan saja, menghapus setiap perubahan yang telah Anda buat.

  - Jika Anda ingin memodifikasi atau menonaktifkan salah satu definisi ini, lihat Memodifikasi konfigurasi default Accelerate alarm danMenonaktifkan konfigurasi alarm Percepat default.
- Profil konfigurasi kustomisasi:
  - Setiap konfigurasi dalam profil ini sepenuhnya dikelola oleh Anda; AMS Accelerate tidak menimpa profil ini, kecuali jika Anda secara eksplisit memintanya.
  - Anda dapat menentukan definisi alarm kustom apa pun yang Anda inginkan di profil ini, dan Anda juga dapat menentukan modifikasi pada konfigurasi default AMS Accelerate-managed. Untuk informasi selengkapnya, lihat Memodifikasi konfigurasi default Accelerate alarm dan Menonaktifkan konfigurasi alarm Percepat default.
  - Jika Anda memperbarui profil ini, Manajer Alarm secara otomatis memberlakukan perubahan Anda di semua sumber daya yang relevan di AWS akun Anda. Perhatikan bahwa meskipun perubahan Anda diberlakukan secara otomatis, perubahan tersebut dapat memakan waktu hingga 60 menit untuk diterapkan.
  - Anda dapat memperbarui profil ini menggunakan CLI/SDK alat AWS AWS Management Console atau AWS. Lihat Panduan AWS AppConfig Pengguna untuk petunjuk tentang memperbarui konfigurasi.
  - Profil kustomisasi awalnya kosong; Namun, definisi alarm apa pun yang ditempatkan di dokumen profil diberlakukan, selain konfigurasi default.

Semua CloudWatch alarm yang dibuat oleh Manajer Alarm berisi kunci tag ams:alarm-manager:managed dan tag value true. Ini untuk memastikan bahwa Manajer Alarm hanya mengelola alarm yang dibuatnya, dan tidak akan mengganggu alarm Anda sendiri. Anda dapat melihat tag ini menggunakan Amazon CloudWatch ListTagsForResourceAPI.

> **Important**
>
> Jika definisi alarm khusus dan definisi alarm default ditentukan dengan ConfigurationId yang sama (lihatMempercepat profil Konfigurasi: pemantauan), definisi kustom akan diprioritaskan daripada aturan default.

Memulai dengan Accelerate Alarm Manager

Secara default, saat Anda melakukan onboard dengan AMS Accelerate, konfigurasi Anda diterapkan AWS AppConfig, menentukan garis dasar alarm untuk sumber daya Anda. Definisi alarm hanya

diterapkan pada sumber daya dengan tag ams:rt: *. Kami menyarankan agar tag ini diterapkan menggunakanMempercepat Tagger Sumber Daya: Anda menyiapkan konfigurasi Tagger Sumber Daya dasar agar AMS Accelerate mengetahui sumber daya mana yang ingin Anda kelola.

Gunakan Resource Tagger untuk menerapkan kunci tag ams:rt:ams-managed dengan nilai tag true ke sumber daya apa pun yang ingin dipantau AMS Accelerate.

Berikut ini adalah contoh profil kustomisasi Resource Tagger yang dapat Anda gunakan untuk ikut serta dalam memantau semua EC2 instans Amazon Anda. Untuk informasi umum, lihatMempercepat Tagger Sumber Daya.

```
{
    "AWS::EC2::Instance": {
        "AMSManageAllEC2Instances": {
            "Enabled": true,
            "Filter": {
                "InstanceId": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

Untuk informasi tentang cara menerapkan konfigurasi Resource Tagger ini, lihatMelihat atau membuat perubahan pada konfigurasi Resource Tagger.

Mempercepat tag Manajer Alarm

Secara default, saat Anda melakukan onboard dengan AMS Accelerate, konfigurasi Anda akan diterapkan AWS AppConfig, menentukan garis dasar alarm untuk sumber daya Anda. Definisi alarm hanya diterapkan pada sumber daya dengan tag ams:rt: *. Kami menyarankan agar tag ini diterapkan menggunakanMempercepat Tagger Sumber Daya: Anda menyiapkan konfigurasi Tagger Sumber Daya dasar agar AMS Accelerate mengetahui sumber daya mana yang ingin Anda kelola.

Gunakan Resource Tagger untuk menerapkan kunci tag ams:rt:ams-managed dengan nilai tag true ke sumber daya apa pun yang ingin dipantau AMS Accelerate.

Topik

- Mempercepat tag menggunakan Resource Tagger
- Mempercepat tag tanpa Resource Tagger
- Mempercepat tag menggunakan AWS CloudFormation
- Mempercepat tag menggunakan Terraform

Mempercepat tag menggunakan Resource Tagger

Manajer Alarm berbasis tag mengelola siklus hidup alarm per sumber daya; namun, hal ini mengharuskan sumber daya CloudWatch terkelola memiliki tag spesifik yang ditentukan oleh AMS Accelerate. Untuk menggunakan Resource Tagger untuk menerapkan set default alarm yang dikelola AMS ke instance berbasis Linux dan Windows, ikuti langkah-langkah berikut.

1. Jelajahi AppConfigkonsol di dalam akun Anda.
2. Pilih ResourceTagger aplikasi.
3. Pilih tab Profil konfigurasi, lalu pilih CustomerManagedTags.
4. Klik Buat untuk membuat profil baru.
5. Pilih JSON dan tentukan konfigurasi Anda. Untuk lebih banyak contoh definisi filter dan platform, lihatMempercepat Tagger Sumber Daya.

```
{
"AWS::EC2::Instance": {
   "MonitorAllInstances": {
       "Enabled": true,
       "Filter": {
           "Platform": "*"
       },
       "Tags": [
           {
               "Key": "ams:rt:ams-managed",
               "Value": "true"
           }
       ]
   }
}
}
```

6. Klik Buat versi konfigurasi yang dihosting.

7. Klik Mulai penerapan.
8. Tentukan detail penerapan berikut:

```
Environment: AMSInfrastructure Hosted configuration version: <Select the version
 that you have just created>
              Deployment Strategy: AMSNoBakeDeployment
```

9. Klik Mulai penerapan.

Instance Anda ditandai dengan `"ams:rt:ams-managed": "true"` yang memastikan bahwa tambahan `"ams:rt:ams-monitoring-policy": "ams-monitored"` dan `"ams:rt:ams-monitoring-policy-platform": "ams-monitored-linux"` diterapkan ke instance. Tag ini kemudian menghasilkan alarm yang sesuai yang dibuat untuk instance tersebut. Untuk informasi lebih lanjut tentang proses ini, lihatPemantauan dalam Mempercepat.

Tonton video Himanshu untuk mempelajari lebih lanjut (11:04)

Mempercepat tag tanpa Resource Tagger

Manajer Alarm berbasis tag mengelola siklus hidup alarm per sumber daya; namun, hal ini mengharuskan sumber daya CloudWatch terkelola memiliki tag spesifik yang ditentukan oleh AMS Accelerate. AMS Accelerate menyediakan profil konfigurasi default yang mengasumsikan bahwa tag Anda telah diterapkan oleh Resource Tagger.

Jika Anda ingin menggunakan metode alternatif untuk menerapkan tag ke sumber daya Anda, seperti AWS CloudFormation atau Terraform, dan bukan Resource Tagger, Anda perlu menonaktifkan Resource Tagger sehingga tidak menerapkan tag ke sumber daya Anda dan bersaing dengan metode penandaan yang Anda pilih. Untuk petunjuk tentang mengubah profil konfigurasi Resource Tagger kustom Anda agar mengaktifkan mode hanya-baca, lihat. Mencegah Resource Tagger dari memodifikasi sumber daya

Setelah Resource Tagger disetel ke mode hanya-baca, dan profil konfigurasi diterapkan, gunakan metode penandaan yang Anda pilih untuk menerapkan tag ke sumber daya Anda sesuai dengan pedoman berikut:

Jenis sumber daya	Kunci tanda	Nilai tanda
Semua sumber daya yang didukung (dijelaskan dalam tabel ini)	am: rt: ams-monitoring-policy	ams-dipantau
EC2 contoh (Linux)	am: rt: ams-monitoring-policy-platform	ams-monitored-linux
EC2 contoh (Windows)	am: rt: ams-monitoring-policy-platform	ams-monitored-windows
OpenSearch Domain dengan KMS	am: rt: ams-monitoring-with-kms	ams-monitored-with-kms
OpenSearch Domain dengan Dedicated Master Node	am: rt: ams-monitoring-with-master	ams-monitored-with-master

Sumber daya yang memiliki kunci dan nilai tag ini dikelola oleh AMS Accelerate Alarm Manager.

Mempercepat tag menggunakan AWS CloudFormation

> **Note**
>
> Pastikan Anda telah mengatur Resource Tagger ke mode read-only terlebih dahulu sebelum menerapkan tag menggunakan AWS CloudFormation, jika tidak Resource Tagger dapat memodifikasi tag berdasarkan profil konfigurasi. Untuk informasi tentang pengaturan Resource Tagger ke mode hanya-baca, dan panduan tentang penyediaan tag Anda sendiri, lihat. Mempercepat tag tanpa Resource Tagger

Untuk menerapkan tag menggunakan AWS CloudFormation, Anda dapat menerapkan tag di tingkat tumpukan (lihat Tag CloudFormation Sumber Daya) atau, pada tingkat sumber daya individual, (misalnya, lihat Membuat Tag EC2 Instance).

Berikut ini adalah contoh bagaimana Anda dapat menerapkan tag manajemen alarm AMS Accelerate ke EC2 instans Amazon yang dikelola oleh AWS CloudFormation:

```
Type: AWS::EC2::Instance
Properties:
 InstanceType: "t3.micro"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

Berikut ini adalah contoh bagaimana Anda dapat menerapkan tag manajemen alarm AMS Accelerate ke grup Auto Scaling yang dikelola oleh. AWS CloudFormation Perhatikan bahwa grup Auto Scaling akan menyebarkan tag ke EC2 instans Amazon yang dibuat olehnya:

```
Type: AWS::AutoScaling::AutoScalingGroup
Properties:
 AutoScalingGroupName: "TestASG"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

Mempercepat tag menggunakan Terraform

> **Note**
>
> Pastikan Anda telah mengatur Resource Tagger ke mode read-only terlebih dahulu sebelum menerapkan tag menggunakan AWS CloudFormation, jika tidak Resource Tagger dapat memodifikasi tag berdasarkan profil konfigurasi. Untuk informasi tentang pengaturan Resource Tagger ke mode hanya-baca, dan panduan tentang penyediaan tag Anda sendiri, lihat. Mempercepat tag tanpa Resource Tagger

Untuk deskripsi tentang cara mengelola tag sumber daya menggunakan Terraform, lihat Penandaan Sumber Daya dokumentasi Terraform.

Berikut ini adalah contoh bagaimana Anda dapat menerapkan tag manajemen alarm AMS Accelerate ke EC2 instans Amazon yang dikelola oleh Terraform.

```
resource "aws_instance" "test_linux_instance" {
     # ...ami and other properties...

     instance_type = "t3.micro"

     tags = {
       "aws:rt:ams-monitoring-policy" = "ams-monitored"
       "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
     }
   }
```

Berikut ini adalah contoh bagaimana Anda dapat menerapkan tag manajemen alarm AMS ke grup Auto Scaling yang dikelola oleh Terraform. Perhatikan bahwa grup Auto Scaling menyebarkan tag ke EC2 instance yang dibuat olehnya:

```
 resource "aws_autoscaling_group" "test_asg" {
 name = "terraform-test"
 # ...other properties...

 tags = {
   "aws:rt:ams-monitoring-policy" = "ams-monitored"
   "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
 }
}
```

Mempercepat profil konfigurasi Manajer Alarm

Saat akun Anda di-onboard ke AMS Accelerate, dua dokumen JSON, yang disebut profil konfigurasi, akan digunakan di akun Anda dengan AWS AppConfig (lihat Apa adanya). AWS AppConfig Kedua dokumen profil berada di aplikasi Alarm Manager dan di lingkungan infrastruktur AMS Accelerate.

Topik

- Mempercepat profil Konfigurasi: pemantauan
- Mempercepat profil Konfigurasi: substitusi pseudoparameter

- Mempercepat contoh konfigurasi alarm
- Melihat konfigurasi Accelerate Alarm Manager
- Mengubah konfigurasi Accelerate alarm
- Memodifikasi konfigurasi default Accelerate alarm
- Menyebarkan Mempercepat perubahan konfigurasi alarm
- Menggulung kembali Mempercepat perubahan alarm
- Mempertahankan Mempercepat alarm
- Menonaktifkan konfigurasi alarm Percepat default

Mempercepat profil Konfigurasi: pemantauan

Baik dokumen profil konfigurasi default dan dokumen profil konfigurasi kustomisasi mengikuti struktur yang sama:

```
  {
    "<ResourceType>": {
        "<ConfigurationID>": {
            "Enabled": true,

            "Tag": {
                "Key": "...",
                "Value": "..."
            },
            "AlarmDefinition": {
                ...
            }
        },
        "<ConfigurationID>": {
            ...
        }
    },
    "<ResourceType>": {
        ...
    }
}
```

- ResourceType: Kunci ini harus menjadi salah satu string yang didukung berikut. Konfigurasi dalam objek JSON ini hanya akan berhubungan dengan jenis AWS sumber daya yang ditentukan. Jenis sumber daya yang didukung:

```
AWS::EC2::Instance
AWS::EC2::Instance::Disk
AWS::RDS::DBInstance
AWS::RDS::DBCluster
AWS::Elasticsearch::Domain
AWS::OpenSearch::Domain
AWS::Redshift::Cluster
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::ElasticLoadBalancingV2::LoadBalancer::TargetGroup
AWS::ElasticLoadBalancing::LoadBalancer
AWS::FSx::FileSystem::ONTAP
AWS::FSx::FileSystem::ONTAP::Volume
AWS::FSx::FileSystem::Windows
AWS::EFS::FileSystem
AWS::EC2::NatGateway
AWS::EC2::VPNConnection
```

- ConfigurationId: Kunci ini harus unik di profil, dan secara unik menamai blok konfigurasi berikut. Jika dua blok konfigurasi di blok yang sama memiliki ConfigurationId yang sama, ResourceTypeblok yang muncul terbaru di profil akan berlaku. Jika Anda menentukan ConfigurationId di profil penyesuaian Anda yang sama dengan yang ditentukan dalam profil default, blok konfigurasi yang ditentukan dalam profil penyesuaian akan berlaku.
  - Diaktifkan: (opsional, default=true) Tentukan apakah blok konfigurasi akan berlaku. Setel ini ke false untuk menonaktifkan blok konfigurasi. Blok konfigurasi yang dinonaktifkan berperilaku seolah-olah tidak ada di profil.
  - Tag: Tentukan tag yang berlaku untuk definisi alarm ini. Sumber daya apa pun (dari jenis sumber daya yang sesuai) yang memiliki kunci dan nilai tag ini akan memiliki CloudWatch alarm yang dibuat dengan definisi yang diberikan. Bidang ini adalah objek JSON dengan bidang berikut:
    - Kunci: Kunci tag yang cocok. Perlu diingat bahwa jika Anda menggunakan Resource Tagger untuk menerapkan tag ke sumber daya, kunci untuk tag akan selalu dimulai dengan ams:rt:.
    - Nilai: Nilai tag yang cocok.
  - AlarmDefinition: Mendefinisikan alarm yang akan dibuat. Ini adalah objek JSON yang bidangnya diteruskan sebagaimana adanya ke panggilan CloudWatch `PutMetricAlarm` API (dengan pengecualian pseudoparameter; untuk informasi lebih lanjut, lihat). Mempercepat profil Konfigurasi: substitusi pseudoparameter Untuk informasi tentang bidang apa yang diperlukan, lihat PutMetricAlarmdokumentasi.

    ATAU

CompositeAlarmDefinition: Mendefinisikan alarm komposit yang akan dibuat. Saat Anda membuat alarm komposit, Anda menentukan ekspresi aturan untuk alarm yang memperhitungkan status alarm alarm lain yang telah Anda buat. Ini adalah objek JSON yang bidangnya diteruskan apa adanya ke. `CloudWatchPutCompositeAlarm` Alarm gabungan tersebut akan beralih ke status ALARM hanya jika semua ketentuan yang ada dalam aturan itu terpenuhi. Alarm yang ditentukan dalam sebuah ekspresi aturan alarm gabungan dapat mencakup alarm-alarm metrik dan alarm-alarm gabungan lainnya. Untuk informasi tentang bidang apa yang diperlukan, lihat PutCompositeAlarmdokumentasi.

Kedua opsi menyediakan bidang berikut:

- AlarmName: Tentukan nama alarm yang ingin Anda buat untuk sumber daya. Bidang ini memiliki semua aturan yang sama seperti yang ditentukan dalam PutMetricAlarmdokumentasi; Namun, karena nama alarm harus unik di Wilayah, Manajer Alarm memiliki satu persyaratan tambahan: Anda harus menentukan pseudoparameter pengidentifikasi unik dalam nama alarm (jika tidak, Manajer Alarm menambahkan pengenal unik sumber daya ke bagian depan nama alarm). Misalnya, untuk jenis AWS::EC2::Instancesumber daya, Anda harus menentukan `${EC2::InstanceId}` dalam nama alarm, atau secara implisit ditambahkan pada awal nama alarm. Untuk daftar pengidentifikasi, lihatMempercepat profil Konfigurasi: substitusi pseudoparameter.

  Semua bidang lainnya adalah seperti yang ditentukan dalam PutMetricAlarmatau PutCompositeAlarmdokumentasi.
- AlarmRule: Tentukan alarm lain mana yang akan dievaluasi untuk menentukan status alarm komposit ini. Untuk setiap alarm yang Anda referensikan, alarm tersebut harus ada di CloudWatch atau ditentukan dalam profil konfigurasi Manajer Alarm di akun Anda.

> **Important**
>
> Anda dapat menentukan salah satu AlarmDefinitionatau CompositeAlarmDefinitiondalam dokumen konfigurasi Manajer Alarm Anda, tetapi keduanya tidak dapat digunakan pada saat yang sama.

Dalam contoh berikut, sistem membuat alarm ketika dua alarm metrik yang ditentukan melebihi ambang batasnya:

```
{
  "AWS::EC2::Instance": {
    "LinuxResourceAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:mylinuxinstance",
        "Value": "true"
      },
      "CompositeAlarmDefinition": {
        "AlarmName": "${EC2::InstanceId} Resource Usage High",
        "AlarmDescription": "Alarm when a linux EC2 instance is using too much CPU and
 too much Disk",
        "AlarmRule": "ALARM(\"${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}\") AND ALARM(\"${EC2::InstanceId}: CPU Too High\")"
      }
    }
  }
}
```

Important

Ketika Manajer Alarm tidak dapat membuat atau menghapus alarm karena konfigurasi rusak, ia mengirimkan pemberitahuan ke topik SNS Direct-Customer-Alerts. Alarm ini disebut AlarmDependencyError.
Kami sangat menyarankan agar Anda mengonfirmasi langganan Anda ke topik SNS ini. Untuk menerima pesan yang dipublikasikan ke suatu topik, Anda harus berlangganan titik akhir ke topik tersebut. Untuk detailnya, lihat Langkah 1: Membuat topik.

Note

Saat alarm Deteksi Anomali dibuat, Manajer Alarm secara otomatis membuat Model Deteksi Anomali yang diperlukan untuk metrik yang ditentukan. Saat alarm Deteksi Anomali dihapus, Manajer Alarm tidak menghapus Model Deteksi Anomali terkait.
Amazon CloudWatch membatasi jumlah Model Deteksi Anomali yang dapat Anda miliki di Wilayah tertentu AWS . Jika Anda melebihi kuota model, maka Alarm Manager tidak akan membuat Alarm Deteksi Anomali baru. Anda harus menghapus model yang tidak digunakan, atau bekerja dengan mitra AMS Anda untuk meminta peningkatan batas.

Banyak definisi alarm dasar yang disediakan AMS Accelerate mencantumkan topik SNS, topik MMS, sebagai target. Ini untuk digunakan dalam layanan pemantauan AMS Accelerate, dan merupakan mekanisme transportasi untuk pemberitahuan alarm Anda untuk sampai ke AMS Accelerate. Jangan tentukan topik MMS sebagai target untuk alarm apa pun selain yang disediakan di baseline (dan penggantian yang sama), karena layanan mengabaikan alarm yang tidak diketahui. Ini tidak mengakibatkan AMS Accelerate bekerja pada alarm khusus Anda.

Mempercepat profil Konfigurasi: substitusi pseudoparameter

Di salah satu profil konfigurasi, Anda dapat menentukan pseudoparameter yang diganti sebagai berikut:

- Global - di mana saja di profil:
  - $ {AWS::AccountId}: Diganti dengan ID AWS akun Anda
  - $ {AWS::Partition}: Diganti dengan partisi sumber daya di (ini adalah 'aws' untuk sebagian besar Wilayah); untuk informasi lebih lanjut, lihat entri untuk partisi di referensi ARN. Wilayah AWS
  - $ {AWS::Region}: Diganti dengan nama Wilayah Wilayah tempat sumber daya Anda digunakan (misalnya us-east-1)
- Di blok tipe AWS::EC2::Instancesumber daya:
  - $ {EC2::InstanceId}: (identifier) diganti dengan ID instans Amazon EC2 Anda.
  - $ {EC2::InstanceName}: diganti dengan nama EC2 instans Amazon Anda.
- Dalam blok tipe sumber daya AWS::EC2::Instance: :Disk:
  - $ {EC2::InstanceId}: (identifier) Diganti dengan ID instans Amazon EC2 Anda.
  - $ {EC2::InstanceName}: Diganti dengan nama EC2 instans Amazon Anda.
  - $ {EC2: :Disk: :Device}: (identifier) Diganti dengan nama disk. (Hanya Linux, pada instance yang dikelola oleh CloudWatch Agen).
  - $ {EC2: :Disk::FSType}: (identifier) Digantikan oleh jenis sistem file disk. (Hanya Linux, pada instance yang dikelola oleh CloudWatchAgent).
  - $ {EC2: :Disk: :Path}: (identifier) Digantikan oleh jalur disk. Di Linux, ini adalah titik pemasangan disk (misalnya,/), sedangkan di Windows ini adalah label drive (misalnya, c:/) (hanya pada instance yang dikelola oleh CloudWatch Agen).
  - $ {EC2: :Disk: :UUID}: (identifier) Digantikan oleh UUID yang dihasilkan yang secara unik mengidentifikasi disk, ini harus ditentukan dalam nama alarm, karena alarm di bawah tipe

sumber daya akan membuat satu alarm per volume. AWS::EC2::Instance::Disk Menentukan $ {EC2: :Disk: :UUID} akan mempertahankan keunikan nama alarm.

- Di blok tipe AWS::EKS::Clustersumber daya:
  - $ {EKS::ClusterName}: (identifier) diganti dengan nama EKS Cluster Anda.
- Di blok tipe AWS::OpenSearch::Domainsumber daya:
  - $ {OpenSearch::DomainName}: (pengenal) diganti dengan nama Domain EKS Anda.
- Di blok tipe AWS::ElasticLoadBalancing::LoadBalancersumber daya:
  - $ {ElasticLoadBalancing::LoadBalancer: :Name}: (identifier) diganti dengan nama Load Balancer V1 Anda.
- Di blok tipe AWS::ElasticLoadBalancingV2::LoadBalancersumber daya:
  - $ {ElasticLoadBalancingV2::LoadBalancer: :Arn}: (identifier) digantikan oleh ARN Load Balancer V2 Anda.
  - $ {ElasticLoadBalancingV2::LoadBalancer: :Name}: (identifier) diganti dengan nama Load Balancer V2 Anda.
  - $ {ElasticLoadBalancingV2::LoadBalancer::FullName}: (identifier) diganti dengan nama lengkap Load Balancer V2 Anda.
- Dalam blok tipe TargetGroup sumber daya AWS::ElasticLoadBalancingV2::LoadBalancer::
  - $ {ElasticLoadBalancingV2::TargetGroup::FullName}: (identifier) diganti dengan nama grup target Load Balancer V2 Anda.
  - $ {ElasticLoadBalancingV2::TargetGroup: :UUID}: (identifier) diganti dengan UUID yang dihasilkan untuk Load Balancer V2 Anda.
- Di blok tipe AWS::EC2::NatGatewaysumber daya:
  - $ {NatGateway::NatGatewayId}: (identifier) digantikan oleh NAT Gateway ID.
- Dalam blok tipe DBInstance sumber daya AWS: :RDS:::
  - $ {RDS:: DBInstance Identifier}: (identifier) diganti dengan pengidentifikasi instans RDS DB Anda.
- Dalam blok tipe DBCluster sumber daya AWS: :RDS:::
  - $ {RDS:: DBCluster Identifier}: (identifier) digantikan oleh pengidentifikasi cluster RDS DB Anda.
- Di blok tipe AWS::Redshift::Clustersumber daya:
  - $ {Redshift::ClusterIdentifier}: (identifier) diganti dengan pengidentifikasi cluster Redshift Anda.
- Di blok tipe AWS::Synthetics::Canarysumber daya:

  - $ {Synthetics::CanaryName}: (identifier) diganti dengan nama kenari CloudWatch Synthetics Anda.
- Dalam blok tipe VPNConnection sumber daya AWSEC2::::::
  - $ {AWS::EC2::VpnConnectionId}: (pengenal) diganti dengan ID VPN Anda.
- Di blok tipe AWS::EFS::FileSystemsumber daya:
  - $ {EFS::FileSystemId}: (identifier) Digantikan oleh ID sistem file dari sistem file EFS Anda.
- Dalam blok tipe sumber daya AWS::FSx::FileSystem: :ONTAP:
  - $ {FSx::FileSystemId}: (identifier) Digantikan oleh ID sistem file file FSX Anda.
  - $ {FSx::FileSystem: :Throughput}: Digantikan oleh throughput sistem file FSX Anda.
  - $ {FSx::FileSystem: :Iops}: Digantikan oleh IOPS dari sistem file FSX.
- Dalam blok tipe sumber daya AWS::FSx::FileSystem: :ONTAP: :Volume:
  - $ {FSx::FileSystemId}: (identifier) Digantikan oleh ID sistem file dari sistem file FSX Anda.
  - $ {FSx: :ONTAP::VolumeId}: (identifier) Diganti dengan ID volume.
- Dalam blok tipe sumber daya AWS::FSx::FileSystem: :Windows:
  - $ {FSx::FileSystemId}: (identifier) Digantikan oleh ID sistem file dari sistem file FSX Anda.
  - $ {FSx::FileSystem: :Throughput}: Digantikan oleh throughput sistem file FSX Anda.

> **Note**
>
> Semua parameter yang ditandai dengan pengenal digunakan sebagai awalan untuk nama alarm yang dibuat, kecuali Anda menentukan pengenal itu dalam nama alarm.

Mempercepat contoh konfigurasi alarm

Dalam contoh berikut, sistem membuat alarm untuk setiap disk yang terpasang pada instance Linux yang cocok.

```
{
    "AWS::EC2::Instance::Disk": {
        "LinuxDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mylinuxinstance",
                "Value": "true"
            },
```

```
            "AlarmDefinition": {
                "MetricName": "disk_used_percent",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "device",
                        "Value": "${EC2::Disk::Device}"
                    },
                    {
                        "Name": "fstype",
                        "Value": "${EC2::Disk::FSType}"
                    },
                    {
                        "Name": "path",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

Dalam contoh berikut, sistem membuat alarm untuk setiap disk yang terpasang pada instance Windows yang cocok.

```
{
     "AWS::EC2::Instance::Disk": {
        "WindowsDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mywindowsinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "LogicalDisk % Free Space",
                "Namespace": "CWAgent",
                "Dimensions": [
```

```
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "objectname",
                        "Value": "LogicalDisk"
                    },
                    {
                        "Name": "instance",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

Melihat konfigurasi Accelerate Alarm Manager

Baik AMSManagedAlarm dan CustomerManagedAlarmsdapat ditinjau AppConfig dengan GetConfiguration.

Berikut ini adalah contoh `GetConfiguration` panggilan:

```
aws appconfig get-configuration --application AMSAlarmManager --environment
 AMSInfrastructure --configuration AMSManagedAlarms --client-id
      any-string outfile.json
```

- Aplikasi: ini adalah AppConfig unit logis untuk menyediakan kemampuan; untuk Manajer Alarm, ini `AMSAlarmManager`
- Lingkungan: ini adalah AMSInfrastructure lingkungan
- Konfigurasi: untuk melihat AMS Mempercepat alarm dasar, nilainya adalah`AMSManagedAlarms`; untuk melihat definisi alarm pelanggan, konfigurasinya adalah `CustomerManagedAlarms`
- ID Klien: ini adalah pengidentifikasi instance aplikasi unik, yang dapat berupa string apa pun
- Definisi alarm dapat dilihat dalam file output yang ditentukan, yang dalam hal ini `outfile.json`

Anda dapat melihat versi konfigurasi mana yang digunakan ke akun Anda dengan melihat penerapan sebelumnya di lingkungan. AMSInfrastructure

Mengubah konfigurasi Accelerate alarm

Untuk menambahkan atau memperbarui definisi alarm baru, Anda dapat menerapkan dokumen konfigurasiMenggunakan AWS CloudFormation untuk menerapkan Mempercepat perubahan konfigurasi, atau menjalankan API. CreateHostedConfigurationVersion

Ini adalah perintah baris perintah Linux yang menghasilkan nilai parameter di base64, yang diharapkan oleh perintah AppConfig CLI. Untuk informasi, lihat AWS CLI dokumentasi, Binary/Blob (objek besar biner).

Sebagai contoh:

```
aws appconfig create-hosted-configuration-version --application-id application-id --
configuration-profile-id configuration-profile-id --content base64-string
      --content-type application/json
```

- ID Aplikasi: ID aplikasi AMS AlarmManager; Anda dapat menemukannya dengan panggilan ListApplicationsAPI.
- ID Profil Konfigurasi: ID konfigurasi CustomerManagedAlarms; Anda dapat menemukannya dengan panggilan ListConfigurationProfilesAPI.
- Konten: String Base64 dari konten, yang akan dibuat dengan membuat dokumen dan menyandikannya di base64: cat alarms-v2.json | base64 (lihat Binary/Blob (objek besar biner)).

  Jenis Konten: Jenis MIME, `application/json` karena definisi alarm ditulis dalam JSON.

> **Important**
>
> Batasi akses ke tindakan StopDeploymentAPI StartDeploymentdan pengguna tepercaya yang memahami tanggung jawab dan konsekuensi penerapan konfigurasi baru ke target Anda.

Untuk mempelajari lebih lanjut tentang cara menggunakan AppConfig fitur AWS untuk membuat dan menerapkan konfigurasi, lihat Bekerja dengan AWS AppConfig.

Memodifikasi konfigurasi default Accelerate alarm

Meskipun Anda tidak dapat mengubah profil konfigurasi default, Anda dapat memberikan penggantian ke default dengan menentukan blok konfigurasi di profil penyesuaian Anda dengan ConfigurationId yang sama dengan blok konfigurasi default. Jika Anda melakukan ini, seluruh blok konfigurasi Anda akan menimpa blok konfigurasi default untuk konfigurasi penandaan yang akan diterapkan.

Misalnya, pertimbangkan profil konfigurasi default berikut:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 5,
                ...
            }
        }
    }
}
```

Untuk mengubah ambang alarm ini menjadi 10, Anda harus memberikan seluruh definisi alarm, tidak hanya bagian yang ingin Anda ubah. Misalnya, Anda dapat memberikan profil penyesuaian berikut:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
```

```
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 10,
                ...
            }
        }
    }
}
```

Important

Ingatlah untuk menerapkan perubahan konfigurasi Anda setelah Anda membuatnya. Di SSM AppConfig, Anda harus menerapkan versi konfigurasi baru setelah membuatnya.

Menyebarkan Mempercepat perubahan konfigurasi alarm

Setelah Anda menyelesaikan kustomisasi, Anda perlu menerapkannya, baik dengan AppConfig atau AWS CloudFormation.

Topik

- Menggunakan AppConfig untuk menyebarkan Mempercepat perubahan konfigurasi alarm
- Menggunakan AWS CloudFormation untuk menerapkan Mempercepat perubahan konfigurasi

Menggunakan AppConfig untuk menyebarkan Mempercepat perubahan konfigurasi alarm

Setelah kustomisasi selesai, gunakan AppConfig untuk menyebarkan perubahan Anda dengan StartDeployment.

```
  aws appconfig start-deployment --application-id application_id
   --environment-id environment_id Vdeployment-strategy-id
   deployment_strategy_id --configuration-profile-id configuration_profile_id --
configuration-version 1
```

- ID Aplikasi: ID aplikasi`AMSAlarmManager`, Anda dapat menemukan ini dengan panggilan ListApplicationsAPI.
- ID Lingkungan: Anda dapat menemukan ini dengan panggilan ListEnvironmentsAPI.
- ID Strategi Penerapan: Anda dapat menemukannya dengan panggilan ListDeploymentStrategiesAPI.
- ID Profil Konfigurasi: ID dari`CustomerManagedAlarms`; Anda dapat menemukan ini dengan panggilan ListConfigurationProfilesAPI.
- Versi Konfigurasi: Versi profil konfigurasi yang akan digunakan.

> **Important**
>
> Manajer Alarm menerapkan definisi alarm sebagaimana ditentukan dalam profil konfigurasi. Setiap modifikasi manual yang Anda buat dengan AWS Management Console atau CloudWatch CLI/SDK ke CloudWatch alarm secara otomatis dikembalikan kembali, jadi pastikan perubahan Anda ditentukan melalui Manajer Alarm. Untuk memahami alarm mana yang dibuat oleh Manajer Alarm, Anda dapat mencari `ams:alarm-manager:managed` tag dengan nilai`true`.
>
> Batasi akses ke tindakan StopDeploymentAPI StartDeploymentdan pengguna tepercaya yang memahami tanggung jawab dan konsekuensi penerapan konfigurasi baru ke target Anda.

Untuk mempelajari lebih lanjut tentang cara menggunakan AppConfig fitur AWS untuk membuat dan menerapkan konfigurasi, lihat AppConfig dokumentasi AWS.

Menggunakan AWS CloudFormation untuk menerapkan Mempercepat perubahan konfigurasi

Jika Anda ingin menerapkan profil `CustomerManagedAlarms` konfigurasi Anda menggunakan AWS CloudFormation, Anda dapat menggunakan AWS CloudFormation template berikut. Letakkan konfigurasi JSON yang Anda inginkan di `AMSAlarmManagerConfigurationVersion.Content` lapangan.

Saat Anda menerapkan template dalam AWS CloudFormation Stack atau Stack Set, penyebaran `AMSResourceTaggerDeployment` sumber daya akan gagal jika Anda belum mengikuti format JSON yang diperlukan untuk konfigurasi. Lihat Mempercepat profil Konfigurasi: pemantauan detail tentang format yang diharapkan.

Untuk bantuan dalam menerapkan templat ini sebagai kumpulan CloudFormation tumpukan atau tumpukan, lihat CloudFormation dokumentasi AWS yang relevan di bawah ini:

- Membuat tumpukan di CloudFormation konsol AWS
- Membuat tumpukan dengan AWS CLI
- Membuat set tumpukan

> **Note**
>
> Jika Anda menerapkan versi konfigurasi menggunakan salah satu templat ini, dan kemudian menghapus kumpulan CloudFormation tumpukan/tumpukan, versi konfigurasi templat akan tetap sebagai versi yang diterapkan saat ini, dan tidak ada penerapan tambahan yang akan dilakukan. Jika Anda ingin kembali ke konfigurasi default, Anda harus menerapkan konfigurasi kosong secara manual (yaitu hanya {}), atau memperbarui tumpukan Anda ke konfigurasi kosong, daripada menghapus tumpukan.

JSON

```
{
  "Description": "Custom configuration for the AMS Alarm Manager.",
  "Resources": {
    "AMSAlarmManagerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "Content": "{}",
        "ContentType": "application/json"
```

```
      }
    },
    "AMSAlarmManagerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSAlarmManagerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Alarm Manager.
Resources:
  AMSAlarmManagerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      Content: |
        {

        }
      ContentType: application/json
  AMSAlarmManagerDeployment:
```

```
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      ConfigurationVersion:
        !Ref AMSAlarmManagerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-Alarm-Manager-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-Alarm-Manager-Configuration-EnvironmentId
```

Menggulung kembali Mempercepat perubahan alarm

Anda dapat memutar kembali definisi alarm melalui mekanisme penerapan yang sama dengan menentukan versi profil konfigurasi sebelumnya dan menjalankannya. StartDeployment

Mempertahankan Mempercepat alarm

Ketika sumber daya yang dipantau oleh AMS dihapus, alarm apa pun yang dibuat oleh Manajer Alarm untuk sumber daya tersebut akan dihapus secara otomatis oleh Manajer Alarm. Jika Anda perlu menyimpan alarm tertentu untuk tujuan audit, kepatuhan, atau historis, gunakan kemampuan penandaan tetap Manajer Alarm.

Untuk mempertahankan alarm bahkan setelah sumber daya yang dipantau dihapus, tambahkan `"ams:alarm-manager:retain"` tag ke konfigurasi kustom alarm seperti yang ditunjukkan pada contoh berikut.

```
{
  "AWS::EC2::Instance": {
    "AMSCpuAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:ams-monitoring-policy",
        "Value": "ams-monitored"
      },
      "AlarmDefinition": {
        "AlarmName": "${EC2::InstanceId}: CPU Too High",
        "AlarmDescription": "AMS Baseline Alarm for EC2 CPUUtilization",
        [...]
        "Tags": [
```

```
          {
            "Key": "ams:alarm-manager:retain",
            "Value": "true"
          }
        ]
      }
    }
  }
}
```

Alarm yang dikonfigurasi dengan `"ams:alarm-manager:retain"` tag, tidak secara otomatis dihapus oleh Manajer Alarm ketika sumber daya yang dipantau dihentikan. Alarm yang dipertahankan tetap ada CloudWatch tanpa batas waktu sampai Anda menghapusnya secara manual menggunakan. CloudWatch

Menonaktifkan konfigurasi alarm Percepat default

AMS Accelerate menyediakan profil konfigurasi default di akun Anda berdasarkan alarm dasar. Namun, konfigurasi default ini dapat dinonaktifkan dengan mengesampingkan salah satu definisi alarm. Anda dapat menonaktifkan aturan konfigurasi default dengan mengganti ConfigurationId aturan di profil konfigurasi kustomisasi Anda dan menentukan bidang yang diaktifkan dengan nilai false.

Misalnya, jika konfigurasi berikut hadir dalam profil konfigurasi default:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                ...
            }
        }
    }
```

Anda dapat menonaktifkan aturan penandaan ini dengan memasukkan yang berikut dalam profil konfigurasi kustomisasi Anda:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": false
        }
    }
}
```

Untuk membuat perubahan ini, CreateHostedConfigurationVersionAPI harus dipanggil dengan dokumen profil JSON (lihatMengubah konfigurasi Accelerate alarm) dan selanjutnya harus diterapkan (lihatMenyebarkan Mempercepat perubahan konfigurasi alarm). Perhatikan bahwa ketika Anda membuat versi konfigurasi baru, Anda juga harus menyertakan alarm kustom yang dibuat sebelumnya yang Anda inginkan dalam dokumen profil JSON.

> **Important**
>
> Saat AMS Accelerate memperbarui profil konfigurasi default, itu tidak dikalibrasi terhadap alarm kustom yang dikonfigurasi, jadi tinjau perubahan pada alarm default saat Anda menggantikannya di profil konfigurasi kustomisasi.

Membuat CloudWatch alarm tambahan untuk Accelerate

Anda dapat membuat CloudWatch alarm tambahan untuk AMS Accelerate menggunakan CloudWatch metrik dan alarm khusus untuk instans Amazon. EC2

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 untuk EC2 instans Amazon Linux menunjukkan cara memproduksi dan menggunakan metrik khusus CloudWatch . Sampel skrip Perl ini terdiri atas contoh yang berfungsi penuh yang melaporkan metrik pemanfaatan memori, swap, dan ruang disk untuk instans Linux.

> **Important**
>
> AMS Accelerate tidak memantau CloudWatch alarm yang dibuat oleh Anda.

Melihat jumlah sumber daya yang dipantau oleh Manajer Alarm untuk Mempercepat

Manajer Alarm mengirimkan metrik setiap jam ke Amazon CloudWatch, di `AMS/AlarmManager` namespace. Metrik dipancarkan hanya untuk jenis sumber daya yang didukung oleh Manajer Alarm.

Nama Metrik	Dimensi	Deskripsi
ResourceCount	Komponen, ResourceType	Jumlah sumber daya (dari jenis sumber daya yang ditentukan) yang digunakan di Wilayah ini. Unit: Hitungan
ResourcesMissingManagedAlarms	Komponen, ResourceType	Jumlah sumber daya (dari jenis sumber daya tertentu) yang memerlukan alarm terkelola, tetapi Manajer Alarm belum menerapkan alarm. Unit: Hitungan
UnmanagedResources	Komponen, ResourceType	Jumlah sumber daya (dari jenis sumber daya yang ditentukan) yang tidak memiliki alarm terkelola yang diterapkan padanya oleh Manajer Alarm. Biasanya, sumber daya ini tidak cocok dengan blok konfigurasi Alarm Manager, atau secara eksplisit dikecualikan dari blok konfigurasi. Unit: Hitungan
MatchingResourceCount	Komponen, ResourceType, ConfigClauseName	Jumlah sumber daya (dari jenis sumber daya yang ditentukan) yang cocok dengan blok konfigurasi Manajer Alarm. Agar sumber daya cocok dengan blok konfigurasi, blok harus diaktifkan, dan sumber daya harus memiliki tag yang sama yang ditentukan dalam blok konfigurasi. Unit: Hitungan

Metrik ini juga dapat dilihat sebagai grafik, di dasbor AMS-Alarm-Manager-Reporting-. Untuk melihat dasbor, dari konsol AWS CloudWatch manajemen, pilih AMS-Alarm-Manager-Reporting-Dashboard. Secara default, grafik di dasbor ini menampilkan data untuk periode 12 jam sebelumnya.

AMS Accelerate menyebarkan CloudWatch alarm ke akun Anda untuk mendeteksi peningkatan signifikan dalam jumlah sumber daya yang tidak dikelola, misalnya, sumber daya yang dikecualikan dari manajemen oleh AMS Alarm Manager. Operasi AMS akan menyelidiki peningkatan sumber daya yang tidak dikelola yang melebihi: baik tiga sumber daya dari jenis yang sama, atau peningkatan 50% atas semua sumber daya dari jenis yang sama. Jika perubahan tampaknya tidak disengaja, Operasi AMS dapat menghubungi Anda untuk meninjau perubahan tersebut.

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
Pemeriksaan Status Gagal	Kemungkinan kegagalan perangkat keras atau keadaan kesalahan instance.	Sistem telah mendeteksi status gagal setidaknya a 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	Ambang batas berada di atas nilai yang ditentuka	Remediasi otomatis AMS pertama menghapus

Nama peringatan	Deskripsi	Ambang batas	Tindakan
	pemasangan (ruang yang ditentukan pada volume) pada EC2 instans Anda terisi.	n 6 kali pada 30 menit terakhir.	file sementara. Jika itu tidak membebaskan ruang disk yang cukup, itu memperpanjang volume untuk mencegah downtime jika volume menjadi penuh.
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: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

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 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: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

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: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

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 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: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

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.

Menggunakan Aturan EventBridge Terkelola Amazon di AMS

AMS Accelerate 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 Akselerasi AMS ditautkan ke prinsipal `events.managedservices.amazonaws.com` layanan. Aturan Terkelola ini dikelola melalui peran `AWSServiceRoleForManagedServices_Events`terkait 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

AmsAccessRolesRule	Aturan ini mendengarkan modifikasi dalam peran dan kebijakan Akselerasi AMS tertentu.	<pre>{
		"source": ["aws.iam"],
		"detail-type": ["AWS API Call via CloudTrail"],
		"detail": {
		"eventName": [
		"DeleteRole",
		"DeletePolicy",
		"CreatePolicyVersion",
		"AttachRolePolicy",
		"DetachRolePolicy"
		],
		"requestParameters": {
		"$or": [
		{
		"roleName": [
		"ams-access-admin",
		"ams-access-admin-operations",
		"ams-access-operations",
		"ams-access-read-only",
		"ams-access-security-analyst",
		"ams-access-security-analyst-read-only"
		]
		},
		{
		"policyArn": [
		"arn:*:iam::*:policy/ams-access-allow-pass-role",
		"arn:*:iam::*:policy/ams-access-deny-cloudshell-policy",
		"arn:*:iam::*:policy/ams-access-deny-operations-policy",</pre>

Nama Aturan	Deskripsi	Definisi

```
                    "arn:*:iam::*:policy/ams-ac
cess-deny-update-iam-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-ssr-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-read-only-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-extended-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-operations-policy"
                ]
            },
        ]
      },
   },
}
```

Nama Aturan	Deskripsi	Definisi

AMSCoreAturan	Aturan ini meneruskan AWS Config dan CloudWatch peristiwa Amazon ke remediasi AMS Config dan layanan pemantauan AMS dengan hormat. AWS Config Peristiwa membuat dan menyelesaikan AWS Systems Manager OpsItems. CloudWatch Acara Amazon memantau CloudWatch Alarm.	<pre>{
		    {
		        "source": ["aws.config", "aws.cloudwatch"],
		        "detail-type": ["Config Rules Compliance Change", "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 AdvisorAWS 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 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 Anda meninjau, Anda memulai dokumen otomatisasi.

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. Untuk informasi selengkapnya, lihat Laporan Remediator Tepercaya.

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 Tepercaya: Solusi remediasi AMS untuk Trusted Advisorpemeriksaan dan AWS Compute Optimizerrekomendasi. 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 OpsItemSumber 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. Anda dapat menggunakan AWS AppConfig konsol atau API untuk mengedit konfigurasi.
- 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 Tepercaya. 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 Accelerate 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. Setelah onboard, Anda dapat menggunakan AWS AppConfig konsol atau API untuk mengelola konfigurasi. 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 Konfigurasikan remediasi Trusted Advisor cek di 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. Perbarui konfigurasi Anda untuk mengaktifkan remediasi untuk Trusted Advisor pemeriksaan yang Anda pilih. Untuk petunjuk tentang cara memilih cek, lihatKonfigurasikan 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, lihatLacak remediasi di Remediator Tepercaya.

Jalankan remediasi manual di Remediator Tepercaya

Anda dapat memulihkan Trusted Advisor pemeriksaan secara manual. Saat Anda memulai remediasi manual, Trusted Remediator membuat eksekusi manual. OpsItem Anda harus meninjau dan memulai dokumen otomatisasi SSM untuk memulihkan. OpsItems Untuk informasi selengkapnya, lihat 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 pengoptimalan	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Pengukuran Hak		

Opsi pengoptimalan	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
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

Opsi pengoptimalan	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
Rekomendasi volume Amazon EBS	AWSManagedServices-ModifyEBSVolume Volume Amazon EBS dimodifikasi sesuai dengan rekomendasi Compute Optimizer. Modifikasi dapat mencakup jenis volume, ukuran, IOPS, generasi volume (gp2, gp3 dll).	• CreateSnapshot: Untuk membuat snapshot sebelum memodifikasi volume, atur ke 'Benar.' Untuk 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.

Opsi pengoptim alan	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasi sebelumnya yang didukung
		Tidak ada kendala • 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 menganggur		
Volume Amazon EBS yang menganggur	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 dikonfigurasikan 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-TerminateEC2 InstanceStoppedForPeriodOfTime - EC2 Instans Amazon dihentikan selama beberapa hari dihentikan.	• Buat AMIBefore Pengakhiran: Untuk membuat instance AMI sebagai cadangan sebelum menghentikan EC2 instans Amazon, pilih`true`. Untuk tidak membuat cadangan sebelum mengakhiri, pilih`false`. Nilai default-nya `true`. • 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 dikonfigurasikan sebelumnya yang didukung
Siklus Hidup Dikonfigurasi		
DAvU99Dc4C Volume Amazon EBS yang Kurang Digunakan	AWSManagedServices-DeleteUnusedEBSVolume Menghapus volume Amazon EBS yang kurang dimanfaatkan jika volume tidak terhubung selama 7 hari terakhir. Snapshot Amazon EBS dibuat secara default.	• CreateSnapshot: Jika disetel `ketrue`, maka otomatisasi akan membuat snapshot volume Amazon EBS sebelum dihapus. Pengaturan default-nya adalah `true`. Nilai yang valid adalah `true` dan `false` (peka huruf besar/kecil). • MinimumUnattachedDays: Minimum hari yang tidak terikat dari volume EBS untuk dihapus, hingga 62 hari. Jika disetel ke`0`, maka dokumen SSM tidak memeriksa periode yang tidak terpasang dan menghapus volume jika volume saat ini tidak terpasang. Defaultnya adalah nilai7. Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasikan 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 dikonfigurasikan 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: Setel `true` untuk memaksa instance berhenti menggunakan penyimpanan instance. Jika tidak, atur ke`false`. Nilai default `false` mencegah instance berhenti. Nilai yang valid adalah true atau false (case-sensitive). Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasikan 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. `true` Untuk tidak membuat cadangan, pilih`false`. Nilai default-nya `false`. Nilai yang valid adalah `true` dan `false` (peka huruf besar/kecil). • ResizeIfStopped: Untuk melanjutkan dengan perubahan ukuran instance, bahkan jika instance dalam keadaan berhenti, pilih`true`. Untuk tidak mengubah ukuran instance secara otomatis jika dalam keadaan berhenti, pilih`false`. Nilai yang valid adalah `true` dan `false` (peka huruf besar/kecil). Tidak ada kendala

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasikan 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 `false` ke `true` atau untuk membuat instance AMI sebagai cadangan sebelum menghentikan EC2 instance. Nilai default-nya `true`. Nilai yang valid adalah `true` dan `false` (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 dikonfigurasikan sebelumnya yang didukung
c1z7kmr00n Rekomendasi pengoptimalan EC2 biaya Amazon untuk instans	Gunakan rekomendasi EC2 instans Amazon dan EC2 instans Amazon Idle dariRekomendasi 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 dikonfigurasikan 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 dikonfigurasikan 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-TrustedRemediatorEnableAutoScalingGroupELBHealthCheck 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 pengganti an 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 dikonfigurasikan 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 dikonfigurasikan 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 dikonfigurasikan 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 dikonfigurasikan 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 Neptunus 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 dikonfigurasikan sebelumnya yang didukung
Hs4Ma3G308 - Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan AWS Security Hub Pemeriksaan yang sesuai: DocumentDB.5	AWSManagedServices-TrustedRemediatorEnableDocumentDBClusterDeletionProtection 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-TrustedRemediatorEnableDynamoDBTableDeletionProtection 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-TrustedRemediatorDisablePublicAccessOnEBSSnapshot 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 dikonfigurasikan 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 dikonfigurasikan 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`true`. Untuk tidak membuat cadangan sebelum mengakhiri, pilih`false`. Nilai default-nya `true`. 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`true`. Untuk tidak membuat cadangan sebelum mengakhiri, pilih`false`. Nilai default-nya `true`. Tidak ada kendala
Hs4Ma3G121 - Enkripsi default EBS harus diaktifkan AWS Security Hub Cek yang sesuai: EC2.7	AWSManagedServices-EncryptEBSByDefault 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 dikonfigurasikan 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 dikonfigurasikan 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 dikonfigurasikan 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 dikonfigurasikan 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 dikonfigurasikan 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 dikonfigurasikan 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 string`AWSLogs`. 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 dikonfigurasikan 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-TrustedRemediatorEnableEMRBlockPublicAccess 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 dikonfigurasikan 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 Neptunus.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
Hs4Ma3G319 - Firewall 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 dikonfigurasikan 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 dikonfigurasikan sebelumnya harus disediakan:. CloudWatchLogGroup Arn Kebijakan CloudWatch sumber daya Amazon harus dikonfigurasi dengan izin. Untuk informasi selengkap nya, 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 dikonfigurasikan 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 dikonfigurasikan sebelumnya harus disediakan: CloudWatchLogGroupArn 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 dikonfigurasikan 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-TrustedRemediatorDisablePublicAccessOnRDSInstance 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 dikonfigurasikan 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 `rds-monitoring-role` 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 dikonfigurasikan sebelumnya yang didukung
Hs4Ma3G190 - Cluster Amazon RDS harus mengaktifkan perlindungan penghapusan AWS Security Hub Pemeriksaan yang sesuai: RDS.7	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection 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-TrustedRemediatorEnableRDSDeletionProtection 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-TrustedRemediatorEnableRDSLogExports 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 dikonfigurasikan 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. `true` Untuk menjadwalkan perubahan untuk jendela pemeliharaan berikutnya, pilih`false`. 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. `true` Untuk menjadwalkan perubahan untuk jendela pemeliharaan berikutnya, pilih`false`. 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 `available` keadaan agar remediasi ini terjadi.

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasikan sebelumnya yang didukung
Hs4Ma3G163 - 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.
Hs4Ma3G164 - 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 dikonfigurasikan 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 dikonfigurasikan sebelumnya yang didukung
Hs4Ma3G105 - Amazon Redshiftharus 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 pemeliharaannya 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-TrustedRemediatorEnableRedshiftClusterEnhancedVPCRouting 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 dikonfigurasikan 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 dikonfigurasikan 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 dikonfigurasikan 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 dikonfigurasikan 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 dikonfigurasikan 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 TargetBucketTagValueuntuk 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 TargetBucketTagKeyuntuk 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. PartitionedPrefixDeliveryTi

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasikan 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 RwqBli 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 dikonfigurasikan sebelumnya yang didukung
Hs4Ma3G272 - 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
Hs4Ma3G179 - 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 `kealias/aws/sns` . 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 dikonfigurasikan 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 dikonfigurasikan 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.	• SqsManagedSseEnabled: Setel `true` untuk mengaktifkan enkripsi antrian sisi server menggunakan kunci enkripsi milik Amazon SQS, setel `false` untuk mengaktifkan enkripsi antrian sisi server menggunakan kunci. AWS KMS • KMSKeyId: 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, alias/aws/sqs digunakan. • KmsDataKeyReusePeriodSeconds: 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 `SqsManagedSseEnabled` disetel `ketrue`. Anonim SendMessage dan ReceiveMessage 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 dikonfigurasikan 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 dikonfigurasikan 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).
BueAdJ7nrp 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 dikonfigurasikan 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 dikonfigurasikan sebelumnya yang didukung
		Mengaktifkan pencatatan akses server Amazon S3.
F2ik5r6dep Amazon RDS Multi-AZ	AWSManagedServices-TrustedRemediatorEnableRDSMultiAZ 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-TrustedRemediatorCreateEBSSnapshot 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 dikonfigurasikan 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 `true` untuk segera menerapkan perubahan, atau `false` untuk menjadwalkan perubahan untuk jendela pemeliharaan berikutnya. Jika `ApplyImmediately` parameter disetel ke`true`, 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 dikonfigurasikan sebelumnya yang didukung
c1qf5bt013 Instans Amazon RDS DB memiliki penyimpanan autoscaling dimatikan	AWSManagedServices-TrustedRemediatorEnableRDSInstanceStorageAutoScaling- Penskalaan otomatis penyimpanan diaktifkan untuk instans Amazon RDS DB.	• MaxAllocatedStorageIncrease Percentage: Persentase kenaikan arus AllocatedStorage, untuk mengatur MaxAllocatedStorage. Default diatur ke26. 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-TrustedRemediatorEnableCLBConnectionDraining Pengurasan 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 dikonfigurasikan 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 dikonfigurasikan 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 dikonfigurasikan sebelumnya yang didukung
c1qf5bt030 `innodb_flush_log_at_trx_commit` Parameter Amazon RDS tidak 1	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter 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-TrustedRemediatorRemediateRDSParameterGroupParameter 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-TrustedRemediatorRemediateRDSParameterGroupParameter 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 dikonfigurasikan 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
ZRxQlPsb6c 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, pilih`false`. Nilai default-nya `false`. Nilai yang valid adalah `true` dan `false` (peka huruf besar/kecil). • ResizeIfStopped: Untuk melanjutkan dengan perubahan ukuran

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasikan sebelumnya yang didukung
		instance, bahkan jika instance dalam keadaan berhenti, pilih`true`. Untuk tidak mengubah ukuran instance secara otomatis jika dalam keadaan berhenti, pilih`false`. Nilai yang valid adalah `true` dan `false` (peka huruf besar/kecil). Tidak ada kendala
c1qf5bt021 `innodb_change_buffering` Parameter Amazon RDS menggunakan nilai kurang dari optimal	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter 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-TrustedRemediatorRemediateRDSParameterGroupParameter 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 dikonfigurasikan sebelumnya yang didukung
c1qf5bt028 enable_indexonlyscan Parameter Amazon RDS dimatikan	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Parameter enable_indexonlyscan dihidupkan untuk Amazon RDS.	Tidak ada parameter yang telah dikonfigurasi sebelumnya yang diizinkan. Tidak ada kendala
c1qf5bt029 enable_indexscan Parame Amazon RDS dimatikan	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter 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-TrustedRemediatorRemediateRDSParameterGroupParameter 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-TrustedRemediatorRemediateRDSParameterGroupParameter 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 dikonfigurasikan 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 0K 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 0K 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 0K 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 dikonfigurasikan 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-IncreaseServiceQuota 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-IncreaseServiceQuota 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 dikonfigurasikan sebelumnya yang didukung
8WiQ YSt25 K Penyeimbang Beban Jaringan ELB	AWSManagedServices-IncreaseServiceQuota 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 dikonfigurasikan 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 penghapus	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 dikonfigurasikan 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-TrustedRemediatorEnableRDSPerformanceInsights 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) atau731. • PerformanceInsightsKMSKeyId: Id AWS KMS kunci untuk enkripsi data Performance Insights. Jika Anda tidak menentukan nilai untuk PerformanceInsights KMSKey Id, 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 dikonfigurasikan 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, 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

Periksa ID dan nama	Nama dokumen SSM dan hasil yang diharapkan	Parameter dan kendala yang telah dikonfigurasikan 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.

Konfigurasikan remediasi Trusted Advisor cek di Remediator Tepercaya

Konfigurasi disimpan AWS AppConfig sebagai bagian dari aplikasi Remediator Tepercaya. Setiap kategori Trusted Advisor cek memiliki profil konfigurasi terpisah. Untuk informasi selengkapnya tentang Trusted Advisor kategori, lihat Lihat kategori cek.

Anda dapat 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-percentagePeluang 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 dan menjalankan dokumen SSM secara manual dari OpsItem AWS Systems Manager OpsCenter konsol.
  - 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 danSesuaikan 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 diTrusted Advisor cek yang didukung oleh Trusted Remediator.

Misalnya, untuk cek`Qch7DwouX1`, ada tiga dokumen SSM terkait: AWSManagedServices-StopEC 2Instance, AWSManagedServices-ResizeInstanceByOneLevel, dan. AWSManagedServices-TerminateInstance Nilai untuk `alternative-automation-document` dapat berupa AWSManagedServices-ResizeInstanceByOneLevel atau AWSManagedServices-TerminateInstance (AWSManagedServices-StopEC2Instance adalah dokumen SSM default untuk diperbaiki`Qch7DwouX1`).

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 didukungTrusted Advisor cek yang didukung oleh Trusted Remediator.
3. Tambahkan tag ke sumber daya dengan kunci dan nilai berikut:
    - 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 secara manual dari. OpsItem
  - 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).

Konfigurasikan remediasi manual untuk volume Amazon EBS dengan cek ID U99Dc4C DAv

1. Buka AWS AppConfig konsol di https://console.aws.amazon.com/systems-manager/appconfig.

   Pastikan Anda masuk sebagai akun Administrator Delegasi.

2. Pilih Trusted Remediator dari daftar aplikasi.
3. Pilih profil konfigurasi Pengoptimalan Biaya.
4. Pilih bendera Volume Amazon EBS yang Kurang Digunakan.
5. Untuk mode eksekusi, pilih Manual.
6. Pastikan manual-for-tagged-onlyatribut automated-for-tagged-onlydan kosong. Atribut ini digunakan untuk mengganti mode eksekusi default untuk sumber daya dengan tag yang cocok.

   Berikut ini adalah contoh bagian Atribut dengan nilai kosong untuk automated-for-tagged-onlydan manual-for-tagged-onlydan Manual untuk mode eksekusi:

7. Pilih Simpan untuk memperbarui nilai, lalu pilih Simpan versi baru untuk menerapkan perubahan. Anda harus memilih Simpan versi baru untuk Remediator Tepercaya untuk mengenali perubahan.
8. Pastikan volume Amazon EBS Anda tidak memiliki tag dengan kuncinya`TR-DAvU99Dc4C-Execution-Mode`. Kunci tag ini mengganti mode eksekusi default untuk Volume EBS tersebut.

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.

Konfigurasikan remediasi otomatis untuk volume Amazon EBS dengan cek ID DAv U99Dc4C, dengan pengecualian sumber daya tidak aktif yang dipilih

1. Buka AWS AppConfig konsol di https://console.aws.amazon.com/systems-manager/appconfig.

   Pastikan Anda masuk sebagai akun Administrator Delegasi.
2. Pilih Trusted Remediator dari daftar aplikasi.
3. Pilih profil konfigurasi Pengoptimalan Biaya.
4. Pilih bendera Volume Amazon EBS yang Kurang Digunakan.
5. Untuk mode eksekusi, pilih Otomatis.
6. Pastikan manual-for-tagged-onlyatribut automated-for-tagged-onlydan kosong. Atribut ini digunakan untuk mengganti mode eksekusi default untuk sumber daya dengan tag yang cocok.

Berikut ini adalah contoh bagian Atribut dengan nilai kosong untuk automated-for-tagged-onlydan manual-for-tagged-onlydan Automated for execution-mode:

7. Pilih Simpan untuk memperbarui nilai, lalu pilih Simpan versi baru untuk menerapkan perubahan. Anda harus memilih Simpan versi baru untuk Remediator Tepercaya untuk mengenali perubahan.

   Pada titik ini, semua volume Amazon EBS diatur untuk remediasi otomatis.

8. Ganti remediasi otomatis untuk volume Amazon EBS yang dipilih:

   a. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.

   b. Pilih Elastic Block Store, Volume.

   c. Pilih Tanda.

   d. Pilih Kelola tanda.

   e. Tambahkan tag berikut:

      - Kunci: Mode Eksekusi TR- DAv U99Dc4C
      - Nilai: Tidak aktif

      Berikut ini adalah contoh bagian Tag yang menunjukkan bidang Kunci dan Nilai:

   f. Ulangi langkah 2 hingga 5 untuk semua volume Amazon EBS yang ingin Anda kecualikan dari remediasi.

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. Buka AWS AppConfig konsol di https://console.aws.amazon.com/systems-manager/appconfig.

   Pastikan Anda masuk sebagai akun Administrator Delegasi.

2. Pilih Trusted Remediator dari daftar aplikasi.
3. Pilih profil konfigurasi Pengoptimalan Biaya.
4. Pilih bendera Volume Amazon EBS yang Kurang Digunakan.
5. Untuk mode eksekusi, pilih Bersyarat.
6. Atur automated-for-tagged-only ke `Stage=NonProd` . Atribut ini mengesampingkan default `execution-mode` untuk sumber daya dengan tag yang cocok. Pastikan manual-for-tagged-onlyatributnya kosong.

   Berikut ini adalah contoh dari bagian Atribut dengan automated-for-tagged-onlyset ke Stage = NonProd dan Conditional for execution-mode:

7. Secara opsional, setel parameter yang telah dikonfigurasi ke salah satu dari berikut ini:

   - `CreateSnapshot=false`untuk tidak membuat snapshot dari volume Amazon EBS sebelum dihapus
   - `MinimumUnattachedDays=10`untuk menetapkan hari minimum yang tidak terikat dari volume Amazon EBS yang akan dihapus menjadi 10 hari
   - `CreateSnapshot=false`, `MinimumUnattachedDays=10` untuk kedua hal di atas
8. Pilih Simpan untuk memperbarui nilai, lalu pilih Simpan versi baru untuk menerapkan perubahan. Anda harus memilih Simpan versi baru untuk Remediator Tepercaya untuk mengenali perubahan.
9. Pastikan volume Amazon EBS Anda tidak memiliki tag dengan kuncinya`TR-DAvU99Dc4C-Execution-Mode`. Kunci tag ini mengganti mode eksekusi default untuk Volume EBS tersebut.

Bekerja dengan remediasi di Remediator Tepercaya

Lacak remediasi di Remediator Tepercaya

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 Tepercaya untuk menyertakan hanya Remediator Tepercaya 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 Tepercaya.

Jalankan remediasi manual di Remediator Tepercaya

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 Tepercaya untuk menyertakan hanya Remediator Tepercaya 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.
6. Untuk memulihkan secara manual OpsItem, selesaikan langkah-langkah berikut:
   a. Dari Runbook, pilih salah satu runbook terkait (dokumen SSM).
   b. Pilih Eksekusi.
   c. Untuk AutomationAssumeRole , pilih `arn:aws:iam::`*`Akun AWS ID`*`:role/ams_ssm_automation_role`. Ganti Akun AWS ID dengan ID akun tempat remediasi berjalan. Untuk nilai parameter lainnya, lihat Data operasi.

Untuk memulihkan sumber daya secara manual, peran atau pengguna yang digunakan untuk mengautentikasi ke Akun AWS harus memiliki `iam:PassRole` izin untuk peran IAM. `ams-ssm-automation-role` Untuk informasi selengkapnya, lihat Memberikan izin pengguna untuk meneruskan peran ke Layanan AWS atau menghubungi Cloud Architect Anda.

d. Pilih Eksekusi.

e. Pantau progres eksekusi dokumen SSM di kolom status dan hasil terbaru.

f. Setelah dokumen selesai, pilih Setel Status, Diselesaikan untuk menyelesaikan secara manual. OpsItem Jika dokumen gagal, tinjau detailnya dan jalankan kembali. SSMdocument Untuk dukungan pemecahan masalah tambahan, buat permintaan layanan.

Untuk menyelesaikan OpsItem tanpa remediasi, pilih Setel Status ke Terselesaikan.

7. Ulangi langkah 3 dan 4 untuk semua remediasi OpsItems manual yang tersisa.

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 DocumentNamedan Parameter sudah benar. Untuk nilai yang benar, tinjau Konfigurasikan remediasi Trusted Advisor cek di Remediator Tepercaya 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, jalankan dokumen SSM secara manual lagi.
5. Untuk mencegah kesalahan ini terulang, pastikan Anda mengonfigurasi remediasi dengan nilai parameter yang benar dalam konfigurasi Anda. Untuk informasi selengkapnya, lihat Konfigurasikan remediasi Trusted Advisor cek di Remediator Tepercaya

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 Exection 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 Tepercaya

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.

Untuk informasi selengkapnya, lihat Integrasi Remediator tepercaya dengan QuickSight.

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`*`-`*`Trusted 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"}
```

Log akun anggota

Trusted Remediator membuat `Member accounts log` saat akun Anda di-onboard atau di-offboard. Anda dapat menggunakan `Member accounts log` untuk menemukan ID akun, onboard Wilayah AWS, dan waktu eksekusi setiap akun anggota.

Lokasi log akun anggota

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/configuration_logs/member_accounts.json`

URL file contoh log akun anggota

`s3://ams-trusted-remediator-`*`111122223333`*`-logs/configuration_logs/member_accounts.json`

Format log akun anggota

```
{
    "delegated_administrator_account_id": Delegated Administrator account id,
    "appconfig_configuration_region": Trusted Remediator AppConfig Region,
    "member_accounts": [
        {
            "account_id": Member account id
            "account_partition": Member account partition (for example, aws),
            "regions": [
                {
                    "execution_time": Remediation execution time in cron schedule
 expression,
                    "execution_timezone": Timezone for the remediation execution time,
                    "region_name": Wilayah AWS name
                }
                ...
            ]
        }
        ...
    ],
    "updated_at": Log update time,
```

```
}
```

Akun anggota log format sampel konten

```
{
    "delegated_administrator_account_id": "111122223333",
    "appconfig_configuration_region": "ap-southeast-2",
    "member_accounts": [
        {
            "account_id": "222233334444",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 9 * * 6",
                    "execution_timezone": "Australia/Sydney",
                    "region_name": "ap-southeast-2"
                },
                {
                    "execution_time": "0 5 * * 7",
                    "execution_timezone": "UTC",
                    "region_name": "us-east-1"
                }
            ]
        },
        {
            "account_id": "333344445555",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 1 * * 5",
                    "execution_timezone": "Asia/Seoul",
                    "region_name": "ap-northeast-2"
                }
            ]
        }
    ],
    "updated_at": "1730869607"
}
```

Integrasi Remediator tepercaya dengan QuickSight

Anda dapat mengintegrasikan log Remediator Tepercaya yang disimpan di Amazon S3 QuickSight untuk membuat laporan remediasi yang disesuaikan. QuickSight Integrasi bersifat opsional. Fitur

ini memungkinkan Anda menggunakan log untuk membuat dasbor pelaporan khusus. Untuk mendapatkan laporan berdasarkan permintaan untuk Trusted Remediator, hubungi CSDM Anda. Untuk informasi selengkapnya tentang laporan Remediator Tepercaya yang tersedia, lihatLaporan Remediator Tepercaya.

Untuk informasi selengkapnya tentang memvisualisasikan data QuickSight, lihat Memvisualisasikan data di. QuickSight

Tambahkan kumpulan data QuickSight untuk log item Remediasi

Untuk menambahkan kumpulan data ke QuickSight log item Remediasi, ikuti langkah-langkah berikut:

1. Masuk ke QuickSight konsol. Anda dapat membuat QuickSight laporan di semua Wilayah AWS yang QuickSight mendukung. Namun, untuk kinerja yang lebih baik dan biaya yang lebih rendah, sebaiknya buat laporan di Wilayah tempat bucket logging Remediator Tepercaya berada.
2. Pilih Datasets.
3. Pilih S3.
4. Di sumber data New S3, masukkan nilai berikut:

   - Nama sumber data: `trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-items`.
   - Unggah file manifes: Buat file JSON dengan konten berikut, dan gunakan. Saat membuat file, ganti `logging_bucket_name` URIPrefixes kunci.

```
{
    "fileLocations": [
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_items/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
```

```
}
```

- Pilih Hubungkan.
- Dari jendela Selesai pembuatan kumpulan data, pilih Visualisasikan.
- QuickSight membuka halaman lembar analisis baru. Anda sekarang siap untuk membuat analisis baru menggunakan log item Remediation.

Berikut ini adalah analisis sampel:

Menambahkan kumpulan data QuickSight untuk log eksekusi remediasi otomatis

1. Masuk ke QuickSight konsol. Anda dapat membuat QuickSight laporan di semua Wilayah AWS yang QuickSight mendukung. Namun, untuk kinerja yang lebih baik dan biaya yang lebih rendah, sebaiknya buat laporan di Wilayah tempat bucket logging Remediator Tepercaya berada.
2. Pilih Datasets.
3. Pilih S3.
4. Di sumber data New S3, masukkan nilai berikut:

   - Nama sumber data:`trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-executions`.
   - Unggah file manifes: Buat file JSON dengan konten berikut, lalu gunakan file ini. Saat membuat file, ganti `logging_bucket_name` URIPrefixes kunci.

```
{
    "fileLocations": [
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_executions/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
```

```
}
```

- Pilih Hubungkan.
- Dari jendela Selesai pembuatan kumpulan data, pilih Visualisasikan.
- QuickSight membuka halaman lembar analisis baru. Anda sekarang siap untuk membuat analisis baru menggunakan log item Remediation.

Berikut ini adalah analisis sampel:

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 dapat menghubungi CA atau CDSM Anda untuk bantuan mengelola konfigurasi Anda. Anda juga dapat menghubungi AMS melalui permintaan layanan untuk dukungan konfigurasi, remediasi manual, dan kegagalan remediasi pemecahan masalah.

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 Accelerate. 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?

Anda dapat mematikan Remediator Tepercaya melalui AWS AppConfig aplikasi. Untuk menjeda atau menghentikan Trusted Remediator, selesaikan langkah-langkah berikut:

1. Buka AWS AppConfig konsol di https://console.aws.amazon.com/systems-manager/appconfig.
2. Pilih Remediator Tepercaya.
3. Pilih Pengaturan pada profil konfigurasi.
4. Pilih bendera Tangguhkan Remediator Tepercaya.
5. Tetapkan valueof `suspended` atribut ke. `true`

> **Note**
>
> Berhati-hatilah saat menggunakan prosedur ini karena ini menghentikan Remediator Tepercaya untuk semua akun yang ditautkan ke akun administrator yang didelegasikan.

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.

Apa bedanya Trusted Remediator dengan AWS Config remediasi?

AWS Config Remediasi adalah solusi lain yang membantu Anda mengoptimalkan sumber daya cloud dan menjaga kepatuhan terhadap praktik terbaik. Berikut ini adalah beberapa perbedaan operasional antara kedua solusi tersebut:

- Trusted Remediator menggunakan Trusted Advisor dan Compute Optimizer sebagai mekanisme deteksi. AWS Config Remediasi menggunakan AWS Config aturan sebagai mekanisme deteksi.
- Untuk Remediator Tepercaya, remediasi terjadi pada jadwal remediasi yang telah ditentukan sebelumnya. Dalam AWS Config, remediasi terjadi secara real time.

- Parameter untuk setiap remediasi di Trusted Remediator mudah disesuaikan berdasarkan kasus penggunaan Anda dan remediasi dapat diotomatisasi atau dibuat manual dengan menambahkan tag pada sumber daya.
- Trusted Remediator menyediakan fungsionalitas pelaporan.
- Trusted Remediator mengirimkan pemberitahuan email kepada Anda dengan daftar remediasi dan status remediasi.

Beberapa Trusted Advisor pemeriksaan dan rekomendasi Compute Optimizer mungkin memiliki aturan yang sama. AWS Config Ini adalah praktik terbaik untuk mengaktifkan hanya satu remediasi jika ada AWS Config aturan dan Trusted Advisor pemeriksaan yang cocok. Untuk informasi tentang AWS Config aturan untuk setiap Trusted Advisor pemeriksaan, lihatTrusted Advisor cek yang didukung oleh Trusted Remediator.

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.

Pemantauan dan manajemen insiden untuk Amazon EKS di AMS Accelerate

Pemantauan dan Manajemen Insiden untuk Amazon EKS memantau sumber daya Amazon EKS Anda untuk kegagalan, penurunan kinerja, dan masalah keamanan. AMS Accelerate mengonfigurasi dan menerapkan Layanan Terkelola Amazon untuk aturan manajer peringatan Prometheus, memantau peringatan, dan kemudian melakukan manajemen insiden saat peringatan ini dipicu. Pemantauan dan manajemen insiden untuk Amazon EKS bergantung pada AMS Alarm Manager dan memanfaatkan AWS layanan asli, seperti Amazon Managed Service untuk Prometheus, Amazon Managed Grafana, Amazon, dan. GuardDuty AWS LambdaAWS Config

> **Note**
>
> Pemantauan dan manajemen insiden untuk Amazon EKS tidak mendukung AWS GovCloud (US), node Windows, atau wadah Windows.

Apa itu pemantauan dan manajemen insiden untuk Amazon EKS di AMS Accelerate?

Pemantauan dan manajemen insiden untuk Amazon EKS memberikan yang berikut:

- Konfigurasi default yang membuat, mengelola, dan menyebarkan monitor dan kebijakan di seluruh akun terkelola untuk klaster Amazon EKS yang Anda pilih.
- Garis dasar pemantauan untuk memungkinkan beban kerja Amazon EKS Anda meningkatkan ketersediaan, bahkan jika Anda tidak mengonfigurasi pemantauan lain untuk kluster Amazon EKS Anda. Untuk informasi selengkapnya, lihat Peringatan dasar dalam pemantauan dan manajemen insiden untuk Amazon EKS di AMS Accelerate.
- Pemberitahuan yang dihasilkan oleh pemantauan dasar yang dikonfigurasi untuk kluster Amazon EKS Anda. Notifikasi ini dikenal sebagai peringatan. Peringatan dihasilkan ketika ada yang akan segera terjadi, sedang berlangsung, surut, atau potensi kegagalan, penurunan kinerja, atau masalah keamanan. Contoh peringatan termasuk peringatan Prometheus, acara, atau temuan dari layanan, seperti Amazon. AWS GuardDuty

- Investigasi peringatan dengan panduan tentang tindakan remediasi yang tepat yang dapat Anda ambil. Untuk informasi selengkapnya, lihat Laporan insiden dan permintaan layanan di AMS Accelerate.
- Remediasi peringatan dan insiden oleh operasi AMS, bila memungkinkan dan dengan persetujuan Anda, untuk mencegah atau mengurangi dampak pada aplikasi Anda. Untuk informasi selengkapnya, lihat Laporan insiden dan permintaan layanan di AMS Accelerate.
- Dasbor Grafana Terkelola Amazon opsional yang telah ditentukan sebelumnya yang memberikan visibilitas ke pemanfaatan sumber daya, kinerja, kesehatan CoreDNS, peringatan aktif, dan peringatan yang telah diselesaikan sebelumnya. Jika Anda mengonfigurasi Grafana Terkelola Amazon menggunakan templat yang disediakan AMS, Anda dapat membuka konsol Grafana Terkelola Amazon untuk melihat metrik dan peringatan untuk klaster Amazon EKS Anda.

Cara kerja pemantauan dan manajemen insiden untuk Amazon EKS di AMS Accelerate

Generasi: Sebagai bagian dari pemantauan orientasi dan manajemen insiden untuk EKS, AMS mengonfigurasi pemantauan dasar untuk kluster Amazon EKS yang Anda pilih di akun terkelola. AMS menggunakan kombinasi Layanan Terkelola Amazon untuk aturan manajer peringatan Prometheus dan aturan peristiwa CloudWatch Amazon untuk mengonfigurasi pemantauan dasar. Server Prometheus yang dikonfigurasi AMS di kluster Anda akan menggores dan menulis metrik Prometheus dari jarak jauh ke Layanan Terkelola Amazon untuk titik akhir Prometheus di Wilayah yang sama. Konfigurasi pemantauan dasar menghasilkan peringatan ketika aturan manajer peringatan Prometheus dipicu atau peristiwa dihasilkan. CloudWatch

Agregasi: AMS mengirimkan semua peringatan yang dihasilkan sumber daya Anda ke sistem pemantauan AMS dengan mengarahkannya ke topik Layanan Pemberitahuan Sederhana Amazon yang dikelola oleh AMS.

Pemrosesan dan analisis dampak: AMS menganalisis peringatan dan kemudian memprosesnya berdasarkan potensi dampaknya. AMS mengklasifikasikan peringatan sebagai berikut:

- Peringatan dengan dampak pelanggan yang diketahui: Untuk peringatan ini, AMS membuat laporan insiden baru menggunakan proses manajemen insiden.
- Peringatan dengan dampak pelanggan yang tidak pasti: Untuk peringatan ini, AMS mengirimkan laporan insiden. Dalam banyak kasus, peringatan ini meminta Anda untuk memverifikasi dampaknya sebelum AMS dapat mengambil tindakan. Untuk peringatan semacam itu, AMS

mengirimkan pemberitahuan peringatan dengan detailnya dan memeriksa apakah peringatan memerlukan tindakan mitigasi. AMS menyediakan opsi untuk mengurangi tindakan dalam notifikasi. Jika balasan Anda mengonfirmasi bahwa peringatan tersebut adalah insiden, AMS kemudian memicu pembuatan laporan insiden baru dan memulai proses manajemen insiden. Setiap pemberitahuan layanan yang menerima tanggapan “tidak ada dampak pelanggan” atau tidak ada tanggapan sama sekali selama tiga hari ditandai sebagai diselesaikan. Juga, peringatan yang sesuai ditandai sebagai diselesaikan.

- Peringatan tanpa dampak pelanggan: Jika, setelah evaluasi, AMS menentukan bahwa peringatan tidak memiliki dampak pelanggan, peringatan ditutup.

Matriks tanggung jawab AMS (RACI)

Matriks AMS yang bertanggung jawab, bertanggung jawab, dikonsultasikan, dan diinformasikan, atau RACI memberikan tanggung jawab utama kepada pelanggan atau AMS untuk berbagai kegiatan. Tabel f ollowing memberikan gambaran umum tentang tanggung jawab pelanggan dan AMS untuk aktivitas dalam aplikasi yang menggunakan Pemantauan dan Manajemen Insiden untuk Amazon EKS.

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

Aktifitas	Pelanggan	AMS
Penemuan untuk persyaratan AMS	I	R
Aktifkan izin AMS (RBAC) untuk akses klaster	R	C

Aktifitas	Pelanggan	AMS
Instal Amazon EC2 Systems Manager Agent di node pekerja jika belum ada	R	C
Terapkan komponen on-cluste r AMS, seperti Prometheus, Prometheus Node Exporter, dan di namespace AMS, sesuai kebutuhan. kube-state-metrics	C	R
Menyediakan Layanan Terkelola Amazon untuk Prometheus di bidang kontrol AMS	I	R
Konfigurasikan manajer peringatan Prometheus di bidang kontrol AMS	I	R
Menyediakan template Grafana yang Dikelola Amazon dan bantu konfigurasi	C	R
Aktifkan Pemantauan Log Audit GuardDuty EKS	C	R
Aktifkan pencatatan pesawat kontrol Amazon EKS	I	R
Pantau kesehatan dan kinerja pesawat kontrol Amazon EKS	I	R

Aktifitas	Pelanggan	AMS
Pantau kesehatan dan kinerja klaster Amazon EKS Anda (cluster, node, beban kerja, pod, API Server, dan CoreDNS)	I	R
Peringatan triase dan berikan respons insiden untuk Amazon EKS	I	R
Jalankan perintah diagnostik selama insiden	I	R
Menganalisis log selama insiden (bidang kontrol dan log pod)	I	R
Respons insiden untuk masalah AWS jaringan	I	R
Menanggapi temuan GuardDuty EKS Audit Log Monitoring	I	R
Memberikan panduan pelanggan tentang tindakan untuk memulihkan insiden jika memungkinkan	I	R

Peringatan dasar dalam pemantauan dan manajemen insiden untuk Amazon EKS di AMS Accelerate

Setelah memverifikasi peringatan, AMS mengaktifkan peringatan berikut untuk Amazon EKS dan kemudian terlibat dalam pemantauan dan manajemen insiden untuk kluster Amazon EKS pilihan Anda. Waktu respons Perjanjian Tingkat Layanan (SLAs) dan Tujuan Tingkat Layanan

(SLOs) bergantung pada Tingkat Layanan akun yang Anda pilih (Plus, Premium). Untuk informasi selengkapnya, lihat Laporan insiden dan permintaan layanan di AMS Accelerate.

Peringatan dan tindakan

Tabel berikut mencantumkan peringatan Amazon EKS dan tindakan masing-masing yang dilakukan AMS:

Pemberitahuan	Ambang batas	Tindakan
Kontainer OOM terbunuh	Jumlah kontainer yang dimulai ulang dalam 10 menit terakhir setidaknya 1 dan kontainer Kubernetes dalam sebuah pod telah dihentikan dengan alasan “OOMKilled” dalam 10 menit terakhir.	AMS menyelidiki apakah pembunuhan OOM disebabkan karena mencapai batas kontainer atau batas memori yang berlebihan, dan kemudian memberi tahu Anda tentang tindakan korektif.
Pod Job Gagal	Pekerjaan Kubernetes gagal diselesaikan. Kegagalan ditunjukkan dengan adanya setidaknya satu status pekerjaan yang gagal.	AMS menyelidiki mengapa pekerjaan Kubernetes atau pekerjaan cron terkait gagal, dan kemudian memberi tahu Anda tentang tindakan korektif.
StatefulSet Bawah	Jumlah replika yang siap melayani lalu lintas tidak sesuai dengan jumlah replika yang ada saat ini per StatefulSet setidaknya 1 menit.	AMS menentukan mengapa pod tidak siap dengan meninjau pesan kesalahan dalam peristiwa pod dan cuplikan log kesalahan di log pod, dan kemudian memberi tahu Anda tentang tindakan korektif.
Kemampuan Penskalaan HPA	Horizontal Pod Autoscaler (HPA) tidak dapat menskalakan karena kondisi status	AMS menentukan Kubernetes Horizontal Pod Autoscaler (HPA) mana yang tidak dapat menskalakan Pod untuk

Pemberitahuan	Ambang batas	Tindakan
	“AbleToScale” salah setidakny a selama 2 menit.	sumber daya beban kerja berikutnya, seperti Deploymen t atau. StatefulSet
Ketersediaan Metrik HPA	Horizontal Pod Autoscaler (HPA) tidak dapat mengumpul kan metrik karena kondisi status “ScalingActive” salah setidaknya selama 2 menit.	AMS menentukan mengapa HPA tidak dapat mengumpul kan metrik, seperti metrik yang terkait dengan masalah konfigurasi server atau masalah otorisasi RBAC.
Pod Belum Siap	Pod Kubernetes tetap dalam keadaan tidak berjalan (seperti Pending, Unknown, atau Failed) selama lebih dari 15 menit.	AMS menyelidiki pod yang terpengaruh untuk detailnya , meninjau log pod untuk kesalahan dan peristiwa terkait, dan kemudian memberi tahu Anda tentang tindakan korektif.
Perulangan Kecelakaan Pod	Kontainer pod dimulai ulang setidaknya sekali setiap 15 menit selama periode 1 jam.	AMS menyelidiki alasan pod tidak dimulai, seperti sumber daya yang tidak mencukupi, file yang dikunci oleh wadah lain, database dikunci oleh kontainer lain, dependensi layanan gagal, masalah DNS untuk layanan eksternal, dan kesalahan konfigurasi.

Pemberitahuan	Ambang batas	Tindakan
Daemonset Salah terjadwal	Setidaknya ada satu pod Kubernetes Daemonset yang salah dalam jangka waktu 10 menit.	AMS menentukan mengapa Daemonset dijadwalkan pada node di mana mereka tidak seharusnya berjalan. Ini mungkin terjadi ketika pod yang salah diterapkan ke pod nodeSelector/taints/affinities Daemonset atau ketika node (kumpulan node) tercemar dan pod yang ada tidak dijadwalk an untuk penggusuran.
Kesalahan API Kubernetes	Tingkat kesalahan server API Kubernetes melebihi 3% selama periode 2 menit.	AMS menganalisis log bidang kontrol untuk menentukan volume dan jenis kesalahan yang menyebabkan peringata n ini, dan mengidentifikasi masalah pertentangan sumber daya apa pun untuk grup penskalaan otomatis node master atau etcd. Jika server API tidak pulih, AMS melibatka n tim layanan Amazon EKS.
Latensi API Kubernetes	Latensi persentil ke-99 dari permintaan ke server API Kubernetes melebihi 1 detik selama periode 2 menit.	AMS menganalisis log bidang kontrol untuk menentukan volume dan jenis kesalahan yang menyebabkan latensi dan mengidentifikasi masalah pertentangan sumber daya untuk grup auto-scaling node master atau etcd. Jika server API tidak pulih, AMS melibatka n tim layanan Amazon EKS.

Pemberitahuan	Ambang batas	Tindakan
Sertifikat Klien Kubernetes Kedaluwarsa	Sertifikat klien yang digunakan untuk mengautentikasi ke server API Kubernetes akan kedaluwarsa dalam waktu kurang dari 24 jam.	AMS mengirimkan pemberita huan ini untuk memberi tahu Anda bahwa sertifikat klaster Anda akan kedaluwarsa dalam 24 jam.
Node Tidak Siap	Status kondisi Node “Siap” salah setidaknya selama 10 menit.	AMS menyelidiki kondisi dan peristiwa node, seperti masalah jaringan, yang mencegah akses kubelet ke server API.
Node CPU Tinggi	Beban CPU melebihi 80% selama periode 5 menit.	AMS menentukan apakah satu atau lebih pod mengkonsumsi CPU dalam jumlah yang luar biasa tinggi. Kemudian, AMS memverifikasi dengan Anda bahwa permintaan, batasan, dan aktivitas pod Anda seperti yang diharapkan.
Node OOM Bunuh Terdeteksi	Setidaknya ada satu host OOM kill yang dilaporkan oleh node dalam jendela 4 menit.	AMS menentukan apakah pembunuhan OOM disebabka n karena mencapai batas kontainer atau komit berlebih node. Jika aktivitas aplikasi normal, AMS memberi tahu Anda tentang permintaan dan batasan untuk overcommit dan merevisi batas pod.

Pemberitahuan	Ambang batas	Tindakan
Batas Node Conntrack	Rasio jumlah entri pelacakan koneksi saat ini hingga batas maksimum melebihi 80% selama periode 5 menit.	AMS memberi tahu Anda tentang nilai conntrack yang direkomendasikan per inti. Node Kubernetes menetapkan nilai conntrack max sebanding dengan total kapasitas memori node. Aplikasi beban tinggi, terutama pada node yang lebih kecil, dapat dengan mudah melebihi nilai max conntrack, menghasilkan reset koneksi dan batas waktu.
Jam Node Tidak Sinkronisasi	Status sinkronisasi minimum selama periode 2 menit adalah 0, dan kesalahan maksimum dalam hitungan detik adalah 16 atau lebih tinggi.	AMS menentukan apakah Network Time Protocol (NTP) diinstal dan berfungsi dengan baik.
CPU Pod Tinggi	Penggunaan CPU kontainer melebihi 80% lebih dari 3 menit untuk periode minimal 2 menit.	AMS menyelidiki log pod untuk menentukan tugas pod yang mengkonsumsi CPU dalam jumlah tinggi.
Memori Pod Tinggi	Penggunaan memori wadah melebihi 80% dari batas memori yang ditentukan selama periode 2 menit.	AMS menyelidiki log pod untuk menentukan tugas pod yang mengkonsumsi memori dalam jumlah tinggi.

Pemberitahuan	Ambang batas	Tindakan
CoreDNS Turun	CoreDNS telah menghilang dari penemuan target Prometheus selama lebih dari 15 menit.	Ini adalah peringatan kritis yang menunjukkan bahwa resolusi nama domain untuk layanan klaster internal atau eksternal dihentikan. AMS memeriksa status pod CoreDNS, memverifikasi konfigurasi CoreDNS, memverifikasi titik akhir DNS yang mengarah ke pod CoreDNS, memverifikasi batas CoreDNS, dan dengan persetujuan Anda, mengaktifkan logging debug CoreDNS.
Kesalahan CoreDNS	CoreDNS mengembalikan kesalahan SERVFAIL untuk lebih dari 3% permintaan DNS selama periode 10 menit.	Peringatan ini mungkin menandakan masalah dengan aplikasi atau kesalahan konfigurasi. AMS memeriksa status pod CoreDNS, memverifikasi konfigurasi CoreDNS, memverifikasi titik akhir DNS yang mengarah ke pod CoreDNS, memverifikasi batas CoreDNS, dan dengan persetujuan Anda, mengaktifkan logging debug CoreDNS.

Pemberitahuan	Ambang batas	Tindakan
Latensi CoreDNS	Persentil ke-99 dari durasi permintaan DNS melebihi 4 detik selama 10 menit.	Peringatan ini menandakan bahwa CoreDNS mungkin kelebihan beban. AMS memeriksa status pod CoreDNS, memverifikasi konfigurasi CoreDNS, memverifikasi titik akhir DNS yang mengarah ke pod CoreDNS, memverifikasi batas CoreDNS, dan dengan persetujuan Anda, mengaktifkan logging debug CoreDNS.
Latensi Penerusan CoreDNS	Persentil ke-99 dari waktu respons untuk permintaan penerusan CoreDNS ke kube-dns melebihi 4 detik selama periode 10 menit.	Ketika CoreDNS bukan server otoritatif atau tidak memiliki entri cache untuk nama domanin, CoreDNS meneruskan permintaan DNS ke server DNS hulu. Peringatan ini menandakan bahwa CoreDNS mungkin kelebihan beban atau mungkin ada masalah dengan server DNS hulu. AMS memeriksa status pod CoreDNS, memverifikasi konfigurasi CoreDNS, memverifikasi titik akhir DNS yang mengarah ke pod CoreDNS, memverifikasi batas CoreDNS, dan dengan persetujuan Anda, mengaktifkan logging debug CoreDNS.

Pemberitahuan	Ambang batas	Tindakan
Kesalahan Penerusan CoreDNS	Lebih dari 3% kueri DNS gagal selama periode 5 menit.	Ketika CoreDNS bukan server otoritatif atau tidak memiliki entri cache untuk nama domanin, CoreDNS meneruskan permintaan DNS ke server DNS hulu. Peringatan ini menandakan kemungkinan kesalahan konfigurasi atau masalah dengan server DNS hulu. AMS memeriksa status pod CoreDNS, memverifikasi konfigurasi CoreDNS, memverifikasi titik akhir DNS yang mengarah ke pod CoreDNS, memverifikasi batas CoreDNS, dan dengan persetujuan Anda, mengaktifkan logging debug CoreDNS.

Persyaratan untuk pemantauan dan manajemen insiden untuk Amazon EKS di AMS Accelerate

Ini adalah sumber daya yang and/or diperlukan yang didukung untuk pemantauan dan manajemen insiden untuk Amazon EKS untuk AMS Accelerate

- Versi Kubernetes yang didukung: Lihat versi Amazon EKS Kubernetes di Panduan Pengguna Amazon EKS.
- Jenis node: Node terkelola Amazon EKS didukung. Node dan wadah Windows tidak didukung.
- Akses klaster Kubernetes: AMS membutuhkan system:master peran cluster RBAC dan pengguna cluster.
- Agen SSM di EC2 node Amazon: Baik Bottle Rocket dan Amazon EKS AMIs memiliki Agen SSM yang sudah diinstal sebelumnya. Pastikan Agen SSM diinstal pada EC2 node kustom AMIs dan Amazon Anda.

- Service Quotas Untuk informasi selengkapnya, lihat kuota layanan untuk Amazon Managed Service for Prometheus dan Amazon Managed Grafana.
- AWS Wilayah yang Didukung:

Nama wilayah	Wilayah	Wilayah penyimpanan metrik
AS Timur (Ohio)	us-east-2	us-east-2
US East (N. Virginia)	us-east-1	us-east-1
AS Barat (Oregon)	us-west-2	us-west-2
Asia Pasifik (Tokyo)	ap-northeast-1	ap-northeast-1
Asia Pasifik (Seoul)	ap-northeast-2	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2	ap-southeast-2
Europe (Frankfurt)	eu-central-1	eu-central-1
Europe (Ireland)	eu-west-1	eu-west-1
Europe (London)	eu-west-2	eu-west-2
Afrika (Cape Town)	af-south-1	eu-west-1 eu-west-2
Asia Pasifik (Hong Kong)	ap-east-1	ap-northeast-1 ap-northeast-2

> **Note**
>
> Metrik untuk kluster Amazon EKS di af-south-1, Afrika (Cape Town) dan ap-east-1, Asia Pasifik (Hong Kong) diekspor ke layanan pemantauan AMS masing-masing. Wilayah AWS Metrik untuk ini kemudian Wilayah AWS diangkut dalam layanan pemantauan AMS ke

Wilayah yang berbeda di mana mereka diproses dan disimpan. Lihat tabel sebelumnya untuk Wilayah yang digunakan layanan pemantauan AMS untuk menyimpan metrik.

Onboard untuk pemantauan dan manajemen insiden untuk Amazon EKS di AMS Accelerate

Lakukan langkah-langkah berikut untuk melakukan onboard ke pemantauan dan manajemen insiden untuk Amazon EKS.

1. Mengaktifkan tag pengoptimalan biaya Amazon EKS: Lihat Menandai sumber daya Anda untuk penagihan di Panduan Pengguna Amazon EKS.
2. Memulai orientasi pemantauan dan manajemen insiden untuk EKS: Hubungi Cloud Service Delivery Manager (CSDM) Anda dengan nama akun IDs dan klaster untuk onboard.
3. Validasi persyaratan: Cloud Architect (CA) Anda memvalidasi bahwa semua persyaratan terpenuhi sebelum orientasi dimulai.
4. Update Kubernetes role-based access control (RBAC): AMS membagikan perintah untuk mengimplementasikan perubahan ini. `eksctl` Anda dapat meninjau perubahan ini dan kemudian menerapkan. Anda harus menerapkan pembaruan RBAC sehingga AMS memiliki izin untuk menjalankan perintah atas nama Anda. Pembaruan ini termasuk memetakan peran AMS IAM ke pengguna Kubernetes, membuat peran klaster Kubernetes baru untuk AMS, dan mengikat peran klaster AMS Kubernetes ke pengguna.
5. Menerapkan komponen cluster: AMS menerapkan komponen berikut dalam namespace yang dikelola AMS di klaster Anda:
   - Server Prometheus
   - Eksportir simpul Prometheus (tidak berlaku untuk) AWS Fargate
   - kube-state-metrics
6. Lakukan pembaruan konfigurasi Prometheus: AMS mengonfigurasi Prometheus untuk mengaktifkan penulisan jarak jauh untuk metrik.
7. (Opsional) Konfigurasikan dasbor: CA membantu mengonfigurasi dasbor Grafana Terkelola Amazon di akun Anda.

> **Note**
>
> Setelah klaster Amazon EKS Anda di-onboard, AMS menganalisis sinyal peringatan dan melakukan penilaian dasar untuk mengidentifikasi masalah yang ada di klaster Anda. Setelah penilaian dasar selesai, AMS membagikan temuan dan rekomendasi remediasi melalui Trusted Advisor dan permintaan layanan yang dapat Anda gunakan untuk mengatasi masalah di klaster Anda. Dari penilaian, AMS membuat garis dasar pemantauan Amazon EKS khusus untuk kluster EKS Anda dengan menyesuaikan ambang batas alarm tingkat akun kami. Untuk menghilangkan duplikat respons AMS terhadap temuan ini, kami menyesuaikan pemantauan kami untuk mengecualikan sinyal peringatan tersebut. Kami menyesuaikan kembali pemantauan kami untuk menyertakan sinyal ketika CSDM Anda memberi tahu kami bahwa masalah mendasar telah diperbaiki.

Offboard dari Pemantauan dan Manajemen Insiden untuk Amazon EKS di AMS Accelerate

Beri tahu manajer pengiriman layanan cloud (CSDM) Anda dengan nama akun IDs dan klaster untuk memulai proses offboarding. Setelah Anda offboard, pemrosesan peringatan, penyimpanan metrik, dan kueri metrik ditangguhkan dan metrik dihapus sesuai dengan kebijakan penyimpanan data Amazon Managed Service for Prometheus default.

AMS melakukan langkah-langkah offboarding berikut:

1. AMS menonaktifkan peringatan yang dikirimkan kepada Anda dan Operasi AMS.
2. AMS menghapus instans Prometheus dari cluster Amazon EKS Anda.
3. AMS menghapus AWS sumber daya lain yang diinstal di akun Anda, seperti peran dan AWS Config aturan IAM.

Setelah langkah-langkah ini selesai, Anda harus menyelesaikan langkah-langkah offboarding berikut:

1. Gunakan `eksctl` untuk menghapus izin Kubernetes RBAC dari. `aws-auth ConfigMap`
2. Jika sebelumnya Anda menginstalnya, hapus instans Grafana Terkelola Amazon yang Anda konfigurasikan untuk disambungkan ke AMS.

Manajemen kontinuitas di AMS Accelerate

AMS memanfaatkan AWS Backup untuk memusatkan dan mengotomatiskan pencadangan data Anda di seluruh layanan. AWS Paket cadangan AMS memberikan praktik terbaik untuk berbagai kasus penggunaan; namun, Anda dipersilakan untuk terus menggunakan paket cadangan yang ada. Setelah Anda melakukan onboard ke manajemen cadangan AMS, AMS menyediakan laporan cadangan, dan pakar AMS terus memantau tugas pencadangan Anda untuk memastikan Anda memiliki solusi pencadangan yang andal.

Untuk mempelajari lebih lanjut, lihat AWS Backup: Cara Kerjanya dan AWS Sumber daya yang didukung serta aplikasi pihak ketiga.

AMS Accelerate menyediakan berbagai layanan operasional untuk membantu Anda mencapai keunggulan operasional AWS. Untuk mendapatkan pemahaman cepat tentang bagaimana AMS membantu tim Anda mencapai keunggulan operasional secara keseluruhan AWS Cloud dengan beberapa kemampuan operasional utama kami termasuk helpdesk 24x7, pemantauan proaktif, keamanan, penambalan, pencatatan, dan pencadangan, lihat Diagram Arsitektur Referensi AMS.

Tonton video Carl untuk mempelajari lebih lanjut (9:29)

Topik

- Bagaimana manajemen kontinuitas bekerja di AMS
- Pilih paket cadangan AMS
- Tandai sumber daya Anda untuk menerapkan paket cadangan AMS
- Lihat cadangan di brankas AMS
- Pemantauan dan pelaporan cadangan AMS

Bagaimana manajemen kontinuitas bekerja di AMS

Paket cadangan AMS menentukan seberapa sering data Anda dicadangkan dan kebijakan penyimpanan untuk cadangan Anda. Brankas cadangan AMS menjaga data cadangan Anda tetap terorganisir. Setelah sumber daya dikaitkan dengan rencana cadangan, sumber daya yang kompatibel secara bertahap dicadangkan. Cadangan pertama adalah salinan lengkap dan cadangan berikutnya menangkap perubahan tambahan. Bergantung pada sumber daya dan paket cadangan AMS yang dipilih, Point-in-time restore (PITR) memungkinkan Anda memundurkan sumber daya

Anda dengan memilih waktu untuk pemulihan Anda. Untuk memulai Manajemen Cadangan AMS, cukup pilih paket cadangan AMS dan beri tag sumber daya Anda.

> **Note**
>
> Pastikan bahwa AWS Backup diaktifkan untuk setiap akun Wilayah AWS, dan jenis sumber daya dengan mengikuti langkah-langkah di sini: Memulai 1: Keikutsertaan Layanan.
> Anda tidak perlu melanjutkan untuk Memulai 2: Buat cadangan berdasarkan permintaan.

Topik Terkait dari AWS Backup

- Bekerja dengan backup (Buat, Edit, Salin, Pulihkan, Hapus)
- Buat cadangan sesuai permintaan
- Membuat salinan cadangan di seluruh Wilayah AWS
- AWS Backup Layanan yang Didukung
- Point-in-time mengembalikan
- AWS Backup Fitur

Pilih paket cadangan AMS

AMS menyediakan tiga paket cadangan berbeda dengan rencana cadangan keempat untuk meminimalkan biaya selama orientasi. Untuk memilih paket cadangan AMS untuk setiap sumber daya yang didukung, beri tag sumber daya dengan tag terkait paket. Saat Anda bergabung dengan Accelerate, AMS akan bekerja sama dengan Anda untuk mengidentifikasi paket cadangan yang paling sesuai dengan kebutuhan Anda.

> **Important**
>
> Jangan mengedit paket cadangan default AMS Anda karena perubahan Anda mungkin hilang. Sebagai gantinya, buat paket baru untuk konfigurasi kustom Anda. Untuk informasi selengkapnya, lihat Membuat paket cadangan.

Paket cadangan AMS default

AWS Backup Pencadangan berkelanjutan tidak diaktifkan untuk rencana pencadangan ini; untuk detailnya, lihat Memulihkan ke waktu tertentu menggunakan point-in-time pemulihan (PITR).

Kunci TAG: `ams:rt:backup-orchestrator`

Nilai TAG: `true`

Paket cadangan AMS default	Waktu Mulai	Penyimpanan
cadangan per jam	N/A	N/A
cadangan harian	setiap hari 4:00 UTC	7 hari
cadangan mingguan	Sabtu, 2:00 UTC	4 minggu
cadangan bulanan	1 bulan ini, 2:00 UTC	26 minggu
cadangan tahunan	1 Januari, 2:00 UTC	2 tahun

Paket cadangan yang disempurnakan

AWS Backup Pencadangan berkelanjutan diaktifkan dengan retensi maksimum (31 hari) pada sumber daya yang didukung; untuk detailnya, lihat Memulihkan ke waktu tertentu menggunakan point-in-time pemulihan (PITR) dan Layanan dan aplikasi yang didukung untuk point-in-time pemulihan (PITR).

Kunci TAG: `ams:rt:backup-orchestrator-enhanced`

Nilai TAG: `true`

Paket cadangan yang disempurnakan	Waktu Mulai	Penyimpanan
cadangan per jam	N/A	N/A
cadangan harian	setiap hari 4:00 UTC	31 hari

Paket cadangan yang disempurnakan	Waktu Mulai	Penyimpanan
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 pencadangan Data Sensitif

AWS Backup Pencadangan berkelanjutan diaktifkan dengan retensi maksimum (31 hari) pada sumber daya yang didukung; untuk detailnya, lihat Memulihkan ke waktu tertentu menggunakan point-in-time pemulihan (PITR) dan Layanan dan aplikasi yang didukung untuk point-in-time pemulihan (PITR).

Kunci TAG: `ams:rt:backup-orchestrator-data-sensitive`

Nilai TAG: `true`

Rencana pencadangan Data Sensitif	Waktu Mulai	Penyimpanan
cadangan per jam	setiap 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

AMS Mempercepat rencana cadangan orientasi

AWS Backup Pencadangan berkelanjutan tidak diaktifkan untuk rencana pencadangan ini; untuk detailnya, lihat Memulihkan ke waktu tertentu menggunakan point-in-time pemulihan (PITR).

Kunci TAG: `ams:rt:backup-orchestrator-onboarding`

Nilai TAG: `true`

AMS Mempercepat rencana cadangan orientasi	Waktu Mulai	Penyimpanan
cadangan per jam	setiap jam	2 minggu
cadangan harian	N/A	N/A
cadangan mingguan	N/A	N/A
cadangan bulanan	N/A	N/A
cadangan tahunan	N/A	N/A

AWS Backup Topik Terkait

- Membuat rencana cadangan
- Point-in-time restore (PITR) memungkinkan pencadangan berkelanjutan dari sumber daya yang didukung dan memungkinkan Anda memilih waktu tertentu untuk pemulihan Anda. Untuk daftar sumber daya yang didukung, lihat Ketersediaan fitur berdasarkan sumber daya.

Tandai sumber daya Anda untuk menerapkan paket cadangan AMS

Untuk menetapkan sumber daya ke paket cadangan AMS, beri tag sumber daya dengan pasangan nilai kunci tag paket. Anda dapat menggunakan AMS Resource Tagger untuk menerapkan paket cadangan AMS ke subset sumber daya Anda atau untuk semua sumber daya yang didukung di akun Anda. Jika Anda ingin menggunakan metode alternatif untuk menerapkan tag ke sumber daya Anda, seperti AWS CloudFormation atau Terraform, matikan Resource Tagger agar tidak bersaing dengan metode penandaan yang Anda pilih. Untuk informasi selengkapnya, lihat Mencegah Resource Tagger dari memodifikasi sumber daya.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan Resource Tagger untuk menerapkan paket cadangan AMS default pada instans Amazon Elastic Compute Cloud di akun Anda. Untuk paket cadangan ini, terapkan kunci tag `ams:rt:backup-orchestrator` dan nilai`true`. Untuk menggunakan paket cadangan yang berbeda, ubah kunci agar sesuai dengan kunci

tag paket cadangan yang Anda inginkan. Untuk mempelajari tentang AMS Resource Tagger dan memahami cara mengintegrasikan profil yang direferensikan berikut dengan profil saat ini (sudah dikonfigurasi) di akun Accelerate Anda, lihat. Mempercepat Tagger Sumber Daya

1. Buka AWS AppConfig konsol di https://console.aws.amazon.com/systems-manager/appconfig.
2. Pilih ResourceTaggeraplikasinya.
3. Pilih tab Profil Konfigurasi, lalu pilih CustomerManagedTags
4. Pilih Buat untuk membuat versi baru.
5. Pilih JSON, lalu salin dan tempel objek JSON berikut:

```
{
    "AWS::EC2::Instance": {
        "AccelerateBackupPlan": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "*"
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:backup-orchestrator",
                    "Value": "true"
                }
            ]
        }
    }
}
```

6. Pilih Buat versi konfigurasi yang dihosting.
7. Pilih Mulai penerapan.
8. Tentukan detail penerapan berikut:

```
Environment: AMSInfrastructure
Hosted configuration version: Select the version that you have just created.
Deployment Strategy: AMSNoBakeDeployment
```

9. Pilih Mulai penerapan. Resource Tagger menandai instans Andaams:rt:backup-orchestrator: true, memastikan bahwa instans Anda dicadangkan sesuai dengan paket cadangan AMS default.

Lihat cadangan di brankas AMS

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	Kunci Tag Paket Cadangan AMS
ams-automated-backups	ams:rt:backup-orkestrator
ams-automated-enhanced-backups	am: rt: backup-orchestrator-enhanced
ams-automated-data-sensitive-cadangan	am: rt: backup-orchestrator-data-sensitive
ams-onboarding-backups	am: rt: backup-orchestrator-onboarding

AMS Vaults lainnya

Nama AMS Vault	Deskripsi
ams-manual-backups	Vault ini berisi pencadangan yang dimulai secara manual yang dibuat oleh dokumen AWSManagedServices-StartBackupJob SSM Automation dan pencadang

Nama AMS Vault	Deskripsi
	an pra-tambalan yang dibuat oleh otomatisasi patch AMS sebelum menambal.
ams-custom-backups	Ini adalah brankas yang direkomendasikan untuk cadangan yang dibuat di luar paket cadangan AMS.

AWS Backup Topik Terkait

- Lihat Cadangan berdasarkan Sumber Daya
- Bekerja dengan 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 Laporan cadangan harian Laporan .

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.

Memahami manajemen tambalan di AMS Accelerate

Important

Mempercepat pelaporan Patch secara berkala menerapkan kebijakan berbasis AWS Glue sumber daya. Harap diperhatikan bahwa pembaruan AMS ke sistem penambalan menimpa kebijakan berbasis sumber daya yang ada AWS Glue .

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

Anda dapat menggunakan sistem patching AMS Accelerate, Patch Add-On, untuk menambal instans Anda dengan pembaruan terkait keamanan dan jenis pembaruan lainnya. Accelerate Patch Add-On adalah fitur yang menyediakan penambalan berbasis tag untuk instance AMS. Ini memanfaatkan fungsionalitas AWS Systems Manager (SSM) sehingga Anda dapat menandai instance dan menambal instance tersebut menggunakan baseline dan jendela yang Anda konfigurasikan. AMS Accelerate Patch Add-On adalah opsi orientasi, jika Anda tidak mendapatkannya saat melakukan onboarding akun Accelerate, hubungi manajer pengiriman layanan cloud (CSDM) Anda untuk mendapatkannya.

AMS Accelerate patch management menggunakan fungsionalitas dasar patch Systems Manager untuk mengontrol definisi patch yang diterapkan pada instance. Patch baseline berisi daftar patch yang telah disetujui sebelumnya; misalnya, semua patch keamanan. Kepatuhan instance diukur terhadap baseline patch yang terkait dengannya. AMS Accelerate, secara default, menginstal semua patch yang tersedia untuk menjaga instance tetap up to date.

> **Note**
>
> AMS Accelerate hanya menerapkan patch sistem operasi (OS). Misalnya, untuk Windows, hanya pembaruan Windows yang diterapkan, bukan pembaruan Microsoft.

Untuk informasi tentang laporan, lihatLaporan manajemen host AMS.

AMS Accelerate menyediakan berbagai layanan operasional untuk membantu Anda mencapai keunggulan operasional AWS. Untuk mendapatkan pemahaman cepat tentang bagaimana AMS membantu tim Anda mencapai keunggulan operasional secara keseluruhan AWS Cloud dengan beberapa kemampuan operasional utama kami termasuk helpdesk 24x7, pemantauan proaktif, keamanan, penambalan, pencatatan, dan pencadangan, lihat Diagram Arsitektur Referensi AMS.

Topik

- Rekomendasi penambalan
- Buat jendela pemeliharaan tambalan di AMS
- Patch dengan kait
- AMS Mempercepat garis dasar tambalan
- Membuat peran IAM untuk patching sesuai permintaan AMS Accelerate
- Memahami notifikasi tambalan dan kegagalan tambalan di AMS Accelerate

Rekomendasi penambalan

Jika Anda terlibat dalam operasi aplikasi atau infrastruktur, Anda memahami pentingnya solusi patching sistem operasi (OS) yang fleksibel dan cukup skalabel untuk memenuhi beragam persyaratan dari tim aplikasi Anda. Dalam organisasi tipikal, beberapa tim aplikasi menggunakan arsitektur yang melibatkan instance yang tidak dapat diubah sedangkan yang lain menyebarkan aplikasi mereka pada instance yang dapat berubah.

Untuk informasi selengkapnya tentang Panduan AWS Preskriptif untuk penambalan, lihat Penambalan otomatis untuk instance yang dapat berubah di cloud hybrid menggunakan. AWS Systems Manager

> **Note**
>
> Accelerate Patch Add-On adalah fitur yang menyediakan penambalan berbasis tag untuk instance AMS. Ini memanfaatkan fungsionalitas AWS Systems Manager (SSM) sehingga Anda dapat menandai instance dan menambal instance tersebut menggunakan baseline dan jendela yang Anda konfigurasikan. AMS Accelerate Patch Add-On adalah opsi orientasi, jika Anda tidak mendapatkannya saat melakukan onboarding akun Accelerate, hubungi manajer pengiriman layanan cloud (CSDM) Anda untuk mendapatkannya.

Rekomendasi tanggung jawab tambalan

Proses patching untuk instance persisten harus melibatkan tim dan tindakan berikut:

- Tim aplikasi (DevOps) mendefinisikan grup patch untuk server mereka berdasarkan lingkungan aplikasi, jenis OS, atau kriteria lainnya. Mereka juga mendefinisikan jendela pemeliharaan khusus untuk setiap grup patch. Informasi ini harus disimpan pada tag yang dilampirkan pada instance. Nama tag yang disarankan adalah 'Patch Group' dan 'Maintenance Window'. Selama setiap siklus patch, tim aplikasi bersiap untuk menambal, menguji aplikasi setelah menambal, dan memecahkan masalah apa pun dengan aplikasi dan OS mereka selama penambalan.
- Tim operasi keamanan mendefinisikan baseline patch untuk berbagai jenis OS yang digunakan oleh tim aplikasi, dan membuat patch tersedia melalui Systems Manager Patch Manager.
- Solusi patching otomatis berjalan secara teratur dan menyebarkan patch yang ditentukan dalam baseline patch, berdasarkan grup patch yang ditentukan pengguna dan jendela pemeliharaan.
- Tim tata kelola dan kepatuhan menentukan pedoman penambalan dan proses & mekanisme pengecualian.

Untuk informasi selengkapnya, lihat Desain solusi Penambalan untuk instance yang dapat berubah EC2 .

Panduan untuk tim aplikasi

- Tinjau dan menjadi akrab dengan membuat dan mengelola jendela pemeliharaan; lihat Windows AWS Systems Manager Pemeliharaan dan Membuat jendela Pemeliharaan SSM untuk ditambal untuk mempelajari lebih lanjut. Memahami struktur umum dan penggunaan jendela pemeliharaan membantu Anda memahami informasi apa yang harus diberikan jika Anda bukan orang yang membuatnya.

- Untuk pengaturan Ketersediaan Tinggi (HA), rencanakan untuk memiliki satu jendela pemeliharaan per zona ketersediaan dan per lingkungan ()Dev/Test/Prod. Ini akan memastikan ketersediaan berkelanjutan selama penambalan.
- Pemeliharaan yang Direkomendasikan Durasi jendela adalah 4 jam dengan cutoff 1 jam, ditambah 1 jam tambahan per 50 instans
- Versi Patch Dev dan Test dengan waktu yang cukup di antara masing-masing untuk memungkinkan Anda mengidentifikasi potensi masalah sebelum penambalan Produksi.
- Otomatiskan tugas pra dan sesudah penambalan umum melalui otomatisasi SSM dan jalankan sebagai tugas jendela pemeliharaan. Perhatikan bahwa untuk tugas pasca-penambalan Anda harus memastikan bahwa ada cukup waktu yang dialokasikan, karena tugas tidak akan diluncurkan setelah batas tercapai.
- Kenali Patch Baseline dan fitur-fiturnya — terutama seputar penundaan persetujuan otomatis untuk jenis keparahan tambalan yang dapat digunakan untuk memastikan bahwa hanya tambalan yang diterapkan yang diterapkan di Produksi di Dev/Test kemudian hari. Lihat Tentang garis dasar tambalan untuk detailnya.

Panduan untuk tim operasi keamanan

- Tinjau dan menjadi akrab dengan garis dasar tambalan. Persetujuan patch ditangani secara otomatis dan memiliki opsi aturan yang berbeda. Lihat Tentang garis dasar tambalan untuk informasi lebih lanjut.
- Diskusikan kebutuhan seputar penambalan Dev/Test/Prod dengan tim aplikasi dan kembangkan beberapa garis dasar untuk mengakomodasi kebutuhan ini.

Panduan untuk tim tata kelola dan kepatuhan

- Patching harus menjadi fungsi “Opt Out”. Jendela pemeliharaan default dan penandaan otomatis harus ada untuk memastikan tidak ada yang belum ditambal. AMS Resource Tagger dapat membantu dalam hal ini; diskusikan opsi ini dengan arsitek cloud (CA) atau manajer pengiriman layanan cloud (CSDM) Anda untuk panduan implementasi.
- Permintaan pembebasan dari penambalan harus memerlukan dokumentasi yang membenarkan pengecualian. Seorang Chief Information Security Officer (CISO) atau petugas persetujuan lainnya harus menyetujui atau menolak permintaan tersebut.

- Kepatuhan patching harus ditinjau pada jadwal reguler melalui konsol Patch Manager, Security Hub, atau scanner kerentanan.

Contoh desain untuk aplikasi Windows ketersediaan tinggi

Ikhtisar:

- Satu Jendela Pemeliharaan per AZ.
- Satu Set Windows Pemeliharaan per Lingkungan.
- Satu Patch Baseline per Lingkungan:
  - Dev: Menyetujui semua tingkat keparahan dan klasifikasi setelah 0 hari.
  - Tes: Menyetujui patch pembaruan keamanan kritis setelah 0 hari dan semua tingkat keparahan dan klasifikasi lainnya setelah 7 hari.
  - Prod: Menyetujui patch pembaruan keamanan kritis setelah 0 hari dan semua tingkat keparahan dan klasifikasi lainnya setelah 14 hari.

CloudFormation Skrip:

Skrip ini disiapkan untuk membangun jendela pemeliharaan, garis dasar, dan tugas penambalan untuk dua zona ketersediaan EC2 aplikasi Windows HA menggunakan pengaturan persetujuan dasar yang dijelaskan di atas.

- Contoh Tumpukan CFN Windows Dev: HA-Patching-dev-Stack.json
- Contoh Tumpukan CFN Uji Windows: HA-Patching-test-Stack.json
- Contoh Tumpukan CFN Prod Windows: HA-Patching-Prod-Stack.json

Rekomendasi tambalan FAQs

T: Bagaimana cara menangani patching tak terjadwal untuk eksploitasi “0" hari?

J: SSM mendukung fitur Patch Now yang menggunakan baseline default saat ini untuk OS instans. AMS menerapkan set default Patch Baseline yang menyetujui semua patch setelah 0 hari. Namun, saat menggunakan fitur Patch Now, snapshot pra-tambalan tidak diambil, karena perintah ini

menjalankan dokumen AWS- RunPatchBaseline SSM. Kami menyarankan Anda mengambil cadangan manual sebelum menambal.

T: Apakah AMS mendukung penambalan untuk instance di Grup Penskalaan Otomatis ()? ASGs

A: Tidak. Saat ini, penambalan ASG tidak didukung untuk pelanggan Accelerate.

T: Apakah ada batasan untuk Pemeliharaan Windows yang perlu diingat?

A: Ya, ada beberapa batasan yang harus Anda waspadai.

- Pemeliharaan Windows per Akun: 50
- Tugas per Jendela Pemeliharaan: 20
- Jumlah maksimum otomatisasi bersamaan per Jendela Pemeliharaan: 20
- Jumlah maksimum Windows Pemeliharaan bersamaan: 5

Untuk daftar lengkap batas SSM default, lihat AWS Systems Manager titik akhir dan kuota.

Buat jendela pemeliharaan tambalan di AMS

Jendela pemeliharaan tambalan menjalankan otomatisasi patch AMS pada jadwal yang ditetapkan untuk EC2 instans Amazon yang ditargetkan. Target ditentukan oleh tag atau tag untuk sekelompok instance. Anda dapat mengatur jadwal berdasarkan hari dan waktu di sekitar Patch Tuesday, atau Anda dapat menentukan jadwal menggunakan ekspresi cron. Untuk informasi selengkapnya, lihat Referensi: Cron dan ekspresi tingkat untuk Systems Manager di Panduan AWS Systems Manager Pengguna. Sebelum menambal, AMS membuat snapshot dari setiap volume root instance. Jika AMS mendeteksi bahwa penambalan memengaruhi kesehatan instans, atau jika Anda memberi tahu AMS tentang dampak aplikasi dari penambalan, AMS menggunakan snapshot ini untuk mengembalikan volume root ke status pra-tambalan.

AMS Mempercepat batas jendela pemeliharaan tambalan

Penggunaan patch AMS AWS Systems Manager (Systems Manager). Selain batas layanan Systems Manager, penambalan AMS memiliki batas 300 instans target per jendela pemeliharaan patch. Mengingat waktu penyelesaian patch umum 30 menit per instance, tabel berikut memberikan contoh untuk jumlah jendela pemeliharaan dan durasi.

Contoh untuk ditambal	Durasi jendela pemeliharaan (jam)	Diperlukan jendela pemeliharaan bersamaan
100	1	1
200	1	1
300	2	1
600	3	2
800	4	3
1200	6	4
1500	8	5

> **Important**
>
> Contoh-contoh ini mengasumsikan tidak ada jendela pemeliharaan Systems Manager lainnya yang aktif dan tidak ada otomatisasi lain yang berjalan.

Untuk informasi lebih lanjut tentang batas, lihat AWS Systems Manager titik akhir dan kuota.

Topik

- Buat jendela pemeliharaan “Patch Tuesday” berulang dari konsol AMS (disarankan)
- Buat jendela pemeliharaan tambalan menggunakan AMS AWS CloudFormation Accelerate
- Membuat jendela pemeliharaan dari konsol Systems Manager untuk AMS Accelerate
- Buat jendela pemeliharaan dengan antarmuka baris perintah Systems Manager (CLI) untuk AMS Accelerate

Buat jendela pemeliharaan “Patch Tuesday” berulang dari konsol AMS (disarankan)

Microsoft merilis patch untuk sistem operasinya pada Selasa kedua setiap bulan, juga dikenal sebagai Patch Tuesday. Adalah umum untuk menjadwalkan penambalan untuk instance Windows dan Linux relatif terhadap Patch Tuesday. Untuk menjadwalkan jendela pemeliharaan patch berulang pada akhir pekan pertama atau kedua setelah Patch Tuesday, kunjungi konsol AMS dan ikuti langkah-langkah berikut:

1. Berikan nama untuk jendela pemeliharaan tambalan Anda.
2. [opsional] Berikan deskripsi untuk jendela pemeliharaan tambalan.
3. Pilih hari relatif terhadap Patch Tuesday.
4. Masukkan waktu untuk jendela pemeliharaan tambalan untuk memulai dalam hh:mm. Misalnya, tengah malam adalah 00:00 dan 11pm adalah 23:00. Kemudian pilih zona waktu.
5. [opsional] Ubah durasi agar sesuai dengan kebutuhan Anda. AMS merekomendasikan durasi minimum empat jam.
6. Masukkan kunci tag patch dan nilai untuk target. Untuk selengkapnya, lihat Apa itu tag? .
7. [opsional] Perluas parameter opsional untuk menyesuaikan konkurensi, tingkat kesalahan, dan batas jendela pemeliharaan.

    1. Concurrency mengontrol berapa banyak instance target yang ditambal pada saat yang bersamaan. Misalnya, konkurensi 50% untuk 10 instance target tidak akan menambal lebih dari 5 instance sekaligus, sementara 100% konkurensi akan menambal semua 10 sekaligus.
    2. Tingkat kesalahan mengontrol toleransi untuk kesalahan sebelum penambalan ditangguhkan. Misalnya, tingkat kesalahan 100% untuk 10 instance target akan menambal semua instance terlepas dari berapa banyak yang gagal, sementara tingkat kesalahan 50% akan menangguhkan penambalan setelah 5 instance gagal ditambal. AMS merekomendasikan tingkat kesalahan 100%.
    3. Pemutusan jendela pemeliharaan tambalan mencegah pelanggaran jendela pemeliharaan tambalan dengan menangguhkan dimulainya aktivitas penambalan baru pada jam yang ditentukan sebelum akhir jendela pemeliharaan tambalan. Misalnya cutoff 1 jam (disarankan), menghentikan aktivitas patch baru 1 jam sebelum akhir jendela pemeliharaan patch.

> **Important**
>
> Verifikasi waktu eksekusi berikutnya.
> Kunjungi konsol Jendela Pemeliharaan SSM, cari jendela pemeliharaan patch yang baru dibuat, dan verifikasi waktu eksekusi berikutnya. Jika Anda memiliki pertanyaan atau perlu mengedit jendela pemeliharaan tambalan Anda, buat permintaan layanan untuk berbicara dengan pakar patch AMS

Untuk menjadwalkan jendela pemeliharaan patch berbasis Cron menggunakan CloudFormation, lihat. Buat jendela pemeliharaan tambalan menggunakan AMS AWS CloudFormation Accelerate

Buat jendela pemeliharaan tambalan menggunakan AMS AWS CloudFormation Accelerate

Untuk membuat jendela pemeliharaan patch AMS Accelerate menggunakan AWS CloudFormation, pertama-tama masuk ke akun Accelerate Anda dan pilih Wilayah AWS tempat instance target Anda berada. Kemudian ikuti langkah-langkah ini di https://console.aws.amazon.com/cloudformation:

1. Pilih salah satu dari dua CloudFormation template patch Accelerate kustom.

   - Penjadwalan Patch Tuesday: Microsoft merilis tambalan untuk sistem operasinya pada hari Selasa kedua setiap bulan, juga dikenal sebagai Patch Tuesday, untuk menjadwalkan jendela pemeliharaan tambalan pada akhir pekan pertama atau kedua setelah Patch Tuesday: Setelah masuk ke konsol Accelerate, gunakan templat tautan ini. PatchTuesdayScheduling CloudFormation
   - Penjadwalan CRON: Untuk membuat jendela pemeliharaan patch menggunakan CRON untuk menentukan hari mulai, gunakan templat tautan ini. CRONScheduling CloudFormation Ingat bahwa Systems Manager CRON menghitung hari 1-7 (untuk detail tentang Systems Manager CRON, lihat Referensi: Cron dan ekspresi tingkat untuk Systems Manager).

   Memilih salah satu tautan ini menyebabkan templat dimuat secara otomatis di CloudFormation konsol. Kemudian klik Selanjutnya.
2. Pada halaman Tentukan detail tumpukan (langkah 2 dari halaman Buat Tumpukan), masukkan nama tumpukan dan parameter templat (parameter default yang ditampilkan adalah default yang direkomendasikan AMS, pilih hari dan waktu untuk kasus penggunaan Anda). Setelah selesai, klik Selanjutnya.

3. Konfigurasikan Opsi Tumpukan (Opsional). Untuk informasi tentang opsi, lihat Menyetel opsi CloudFormation tumpukan AWS. Setelah selesai, klik Selanjutnya.
4. Tinjau nilai tumpukan Anda (Opsional). Untuk informasi tentang meninjau detail tumpukan untuk memperkirakan biaya, lihat Meninjau tumpukan Anda dan memperkirakan biaya tumpukan. Saat siap, klik Buat tumpukan.

   Tumpukan mungkin memakan waktu hingga satu menit untuk dibuat. Setelah tumpukan berhasil dibuat, jendela pemeliharaan patch Anda berjalan pada waktu yang ditentukan. Anda dapat membuat perubahan pada jendela pemeliharaan tambalan dengan membuat dan mengeksekusi set CloudFormation perubahan (disarankan) (untuk detail tentang melakukan hal ini, lihat Membuat tumpukan menggunakan set perubahan), atau dengan memperbarui jendela pemeliharaan patch pada konsol jendela Systems Manager Maintenance (). https://console.aws.amazon.com/systems-manager/maintenance-windows

Tonton video Namrata untuk mempelajari lebih lanjut (5:41)

Membuat jendela pemeliharaan dari konsol Systems Manager untuk AMS Accelerate

Untuk membuat jendela pemeliharaan AMS Accelerate dari konsol Systems Manager, ikuti langkah-langkah berikut:

1. Di bilah navigasi kiri di area Change management, klik Maintenance Windows, lalu klik Create Maintenance Window di kanan atas layar. Isi formulir. Untuk detail tentang salah satu opsi, lihat Membuat jendela pemeliharaan (konsol). Setelah selesai, klik Buat jendela pemeliharaan.

   Halaman daftar jendela pemeliharaan terbuka.
2. Pilih jendela pemeliharaan yang baru dibuat.

   Halaman detail jendela pemeliharaan terbuka.
3. Buka tab Target dan pilih Daftarkan target.

   Halaman target Register terbuka.
4. Tambahkan target Accelerate Anda. Untuk informasi tentang target, lihat Menetapkan target ke jendela pemeliharaan (konsol). Setelah selesai, klik Daftarkan target. Catat target saat Anda membutuhkannya nanti.

Halaman detail jendela pemeliharaan terbuka kembali di tab Target dengan daftar termasuk target baru.

5. Pada tab Tugas pada halaman detail jendela pemeliharaan, pilih Daftarkan Tugas, lalu pilih Daftarkan tugas Otomasi dari daftar drop-down. Isi formulir. Mempercepat catatan:

   - Berikan nama tugas yang berarti. Misalnya: AcceleratePatch.
   - Di area dokumen otomatisasi klik di kotak pencarian, pilih Pemilik, lalu Dokumen bersama.
   - Pilih dokumen otomatisasi dengan mengklik di kotak pencarian dan memilih Awalan nama dokumen -> Sama dengan lalu mengetik:. AWSManagedServices-PatchInstance Kemudian pilih AWSManagedServices-PatchInstancedokumen dengan memilih tombol radionya.
   - Di bawah versi dokumen, pilih Versi default saat runtime.
   - Di bagian Target:
     - Tetapkan Target dengan: untuk Memilih grup target terdaftar.
     - Dalam daftar target, pilih target yang Anda daftarkan di tab Target.
   - Di bagian Parameter input, isi formulir.
     - InstanceId: `{{TARGET_ID}}`
     - StartInactiveInstances: `True` untuk memulai instance jika dihentikan selama jendela pemeliharaan tambalan.

     > **Note**
     >
     > Nilai InstanceIdparameter peka huruf besar/kecil dan nilai StartInactiveInstancesparameter dapat berupa True atau False.
     > Instance yang dihentikan tidak dapat dimulai saat ditargetkan oleh tag. Untuk informasi selengkapnya, lihat No Invocations to Execute.

   - Di bagian Rate control, pilih persentase. AMS Accelerate merekomendasikan 100% untuk Concurrency dan 100% for Error threshold untuk mencoba menambal semua instance secara bersamaan, terlepas dari kesalahan otomatisasi. Jika Anda ingin menambal setengah target Anda sekaligus, misalnya, untuk menjaga setengah dari instance target di belakang keseimbangan beban berjalan, atur Concurrency ke 50%.
   - Di bagian peran layanan IAM, pilih Gunakan peran layanan kustom, lalu pilih ams_ssm_automation_role.

Klik Daftarkan tugas Otomasi.

Jendela pemeliharaan tambalan dibuat. Di bawah tab Deskripsi, Anda dapat melihat Waktu eksekusi berikutnya.

Buat jendela pemeliharaan dengan antarmuka baris perintah Systems Manager (CLI) untuk AMS Accelerate

Untuk membuat jendela pemeliharaan AMS Accelerate dengan antarmuka baris perintah:

1. Ikuti Tutorial SSM: Buat dan konfigurasikan jendela pemeliharaan (AWS CLI). Untuk setiap langkah tutorial, berikut adalah contoh perintah CLI untuk menambal.

> **Note**
>
> Contoh-contoh ini khusus untuk Linux atau macOS. Perintah juga dapat dijalankan dari AWS CloudShell yang mungkin lebih sederhana daripada mengkonfigurasi `awscli` pada mesin lokal. Untuk detailnya, lihat Bekerja dengan AWS CloudShell.

   a. Pada langkah 1 tutorial, untuk membuat jendela pemeliharaan:

```
aws ssm create-maintenance-window \
                --name Sample-Maintenance-Window \
                --schedule "cron(0 30 23 ? * TUE#2 *)" \
                --duration 4 \
                --cutoff 1 \
                --allow-unassociated-targets \
                --tags "Key=Environment,Value=Production"
```

   Setelah berhasil diselesaikan, `window-id` dikembalikan.

   b. Pada langkah 2 tutorial, untuk mendaftarkan node target:

```
aws ssm register-target-with-maintenance-window \
                --window-id "mw-xxxxxxxxx" \
                --resource-type "INSTANCE" \
                --target "Key=tag:Environment,Values=Prod"
```

Setelah berhasil diselesaikan, `WindowTargetID` s dikembalikan.

c. Pada langkah 3 tutorial, untuk mendaftarkan tugas:

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-xxxxxx" \
    --targets "Key=WindowTargetIds,Values=63d4f63c-xxxxxx-9b1d-xxxxxfff" \
    --task-arn "AWSManagedServices-PatchInstance" \
    --service-role-arn "arn:aws:iam::AWS-Account-ID:role/ams_ssm_automation_role"
 \
    --task-invocation-parameters "{\"Automation\":{\"DocumentVersion\":\"\$DEFAULT
\",\"Parameters\":{\"InstanceId\":[\"{{TARGET_ID}}\"],\"StartInactiveInstances\":
[\"True\"]}}}" \
    --max-concurrency 50 \
    --max-errors 50 \
    --name "AutomationExample" \
    --description "Sample Description" \
    --task-type=AUTOMATION
```

Patch dengan kait

Anda dapat mengonfigurasi patch AMS untuk menjalankan perintah level operating-system (OS) sebelum dan sesudah menambal, menggunakan kait patch AMS. Gunakan kait patch AMS untuk menjalankan dokumen Perintah SSM untuk menghentikan layanan sebelum menambal dan kemudian memulai layanan setelah menambal, atau menjalankan perintah untuk mengonfirmasi bahwa aplikasi Anda sehat setelah ditambal.

Untuk menggunakan kait patch AMS, Anda perlu melakukan hal berikut:

1. Buat dokumen SSM Command untuk digunakan sebagai patch hook.
2. Buat jendela pemeliharaan patch AMS, atau gunakan jendela pemeliharaan patch AMS yang ada. Untuk detailnya, lihat jendela pemeliharaan tambalan AMS.
3. Konfigurasikan jendela pemeliharaan patch AMS untuk menggunakan dokumen Perintah SSM Anda untuk kait patch AMS.

Kait tambalan AMS RACI

Matriks yang bertanggung jawab, akuntabel, dikonsultasikan, dan diinformasikan, atau RACI, memberikan tanggung jawab utama kepada pelanggan atau AMS untuk berbagai kegiatan. Tabel berikut memberikan gambaran umum tentang tanggung jawab pelanggan dan AMS untuk aktivitas dalam aplikasi yang menggunakan kait patch AMS.

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

Aktifitas	Pelanggan	AMS
Buat pre/post patch SSM Command dokumen dan konten dokumen	R	C
Konfigurasikan parameter kait patch untuk penambalan AMS	R	C
Jalankan pre/post dokumen Patch SSM Command	I	R
Triase dan tanggapi kegagalan patch hook	I	R
Beri tahu pelanggan tentang kegagalan patch hook	I	R
Kembalikan ke status pra-tambalan jika diminta oleh pelanggan	C	R

Buat dokumen SSM untuk kait patch

Kait patch AMS menggunakan dokumen Amazon EC2 Systems Manager (SSM) selama penambalan. Buat dokumen SSM Command, atau bagikan dokumen SSM Command yang ada, dengan akun tempat penambalan terjadi. Untuk informasi tentang dokumen SSM, termasuk batasan, lihat Berbagi dokumen SSM.

Untuk membuat dokumen SSM Command, ikuti langkah-langkah berikut:

1. Buat dokumen SSM dengan Document Type = “Command”.
2. Masukkan perintah Anda di bagian Konten. Untuk informasi selengkapnya, lihat Membuat konten dokumen SSM.

> **Note**
>
> Dokumen SSM untuk kait patch AMS juga dapat dibuat dengan AWS CLI atau. AWS CloudFormation Jika Anda memerlukan bantuan untuk membuat dokumen SSM untuk kait patch AMS Anda, hubungi Cloud Architect Anda.

Konfigurasikan jendela pemeliharaan patch AMS untuk menggunakan dokumen Perintah SSM Anda sebagai kait patch AMS

Jendela pemeliharaan patch AMS adalah jendela pemeliharaan Systems Manager yang menjalankan otomatisasi patch AMS yang dikonfigurasi.

Untuk mengedit jendela pemeliharaan tambalan AMS agar menggunakan kait tambalan, ikuti langkah-langkah berikut:

1. Pada https://console.aws.amazon.com/systems-manager/, di bawah Change Management Tools di panel navigasi kiri, pilih Maintenance Windows.

   Halaman yang mencantumkan jendela pemeliharaan yang ada terbuka.
2. Pilih ID Jendela yang dimulai dengan mw-.

   Halaman detail untuk jendela pemeliharaan itu terbuka.
3. Pilih tab Tugas dan ID Tugas Jendela dengan ARN Tugas AMS- PatchInstance dan klik Edit.

4. Gulir ke bawah ke bagian Parameter dan perbarui parameter berikut.

Parameter kait patch AMS:

- PrePatchHook: Nama dokumen SSM dengan tipe “Command” yang ingin Anda jalankan sebelum menambal. Biarkan ini kosong atau ketik “AWS-noop” (peka huruf besar/kecil) jika Anda tidak menjalankan perintah sebelum menambal.
- PostPatchHook: Nama dokumen SSM dengan tipe “Command” yang ingin Anda jalankan setelah menambal. Biarkan ini kosong atau ketik “AWS-noop” (peka huruf besar/kecil) jika Anda tidak menjalankan perintah setelah menambal.
- ExecutePatchBasedOnPreHookStatus: Jalankan patching berdasarkan keberhasilan atau kegagalan PrePatchHook lari, pilih salah satu:
  - OnPreHookSuccess: Hanya jalankan otomatisasi patch AMS ketika berhasil. PrePatchHook
  - Selalu: Jalankan otomatisasi patch AMS ketika berhasil dan ketika gagal. PrePatchHook
  - OnPreHookFailure- Jalankan otomatisasi patch AMS hanya ketika PrePatchHook gagal.
  - Tidak pernah: Jangan jalankan otomatisasi patch AMS. Ini mungkin berguna saat menguji Anda PrePatchHook.
- ExecutePostHookBasedOnPatchStatus: Jalankan hook pasca-patch berdasarkan keberhasilan atau kegagalan otomatisasi patch AMS, pilih salah satu:
  - OnPatchSuccess: Jalankan hanya PostPatchHook ketika otomatisasi patch AMS berjalan dengan sukses.
  - Selalu: Jalankan PostPatchHook ketika otomatisasi patch AMS berhasil dan ketika gagal.
  - OnPatchFailure- Jalankan PostPatchHook satu-satunya ketika otomatisasi patch AMS gagal.

> **Note**
>
> Jika salah satu variabel ini kehilangan kotak teksnya, perbaiki ini dengan menggulir ke bagian dokumen Otomasi pada halaman yang sama dan memilih dokumen yang berbeda dan kemudian memilih kembali dokumen asli. Ini menyegarkan parameter input sehingga Anda dapat mengeditnya.

AMS Mempercepat garis dasar tambalan

Suatu dasar patch mendefinisikan patch mana yang disetujui untuk instalasi pada instans Anda. Anda dapat menentukan patch yang disetujui atau ditolak satu per satu. Anda juga dapat membuat aturan persetujuan otomatis untuk menentukan bahwa jenis pembaruan tertentu (misalnya, pembaruan penting) harus disetujui secara otomatis. Daftar yang ditolak menggantikan aturan dan daftar persetujuan.

Garis dasar tambalan default

Saat Anda melakukan onboard ke patch AMS Accelerate, baseline patch default akan diganti oleh baseline patch default AMS Accelerate untuk sistem operasi berikut.

- Windows
- Amazon Linux 1
- Amazon Linux 2
- CentOS
- Suse
- Rhel
- Ubuntu

Important

Garis dasar patch default dikelola oleh AMS. Jangan mengedit baseline patch default karena perubahan Anda mungkin hilang. Sebagai gantinya, buat baseline patch kustom. Lihat Garis dasar patch khusus dengan AMS Accelerate

Note

Garis dasar patch AMS Accelerate yang didefinisikan sebagai product = * berarti bahwa semua tambalan diterapkan pada instance semua keamanan dan klasifikasi.

Garis dasar patch khusus dengan AMS Accelerate

Untuk menggunakan baseline patch kustom dengan AMS Accelerate, pertama-tama pastikan bahwa Anda memiliki grup patch, lalu buat baseline kustom.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Bekerja dengan grup patch
- Membuat baseline patch kustom (Windows)
- Membuat baseline patch kustom (Linux)
- Memperbarui atau menghapus baseline patch khusus (konsol)

Membuat peran IAM untuk patching sesuai permintaan AMS Accelerate

Setelah akun Anda di-onboard ke patch AMS Accelerate, AMS Accelerate akan menerapkan kebijakan terkelola, amspatchmanagedpolicy. Kebijakan ini berisi izin yang diperlukan untuk patching sesuai permintaan menggunakan dokumen otomatisasi AMS. `AWSManagedServices-PatchInstance` Untuk menggunakan dokumen otomatisasi ini, administrator akun membuat peran IAM untuk pengguna. Ikuti langkah-langkah ini:

Buat peran menggunakan AWS Management Console:

1. Masuk ke AWS Management Console dan buka konsol IAM.
2. Di panel navigasi konsol, pilih Peran, lalu Buat peran.
3. Pilih jenis Akun AWS peran lain.
4. Untuk ID Akun, masukkan ID AWS akun yang ingin Anda berikan akses ke sumber daya Anda.

   Administrator akun yang ditentukan dapat memberikan izin untuk mengasumsikan peran ini kepada setiap pengguna IAM dalam akun tersebut. Untuk melakukan ini, administrator melampirkan kebijakan ke pengguna, atau grup, yang memberikan izin untuk tindakan sts: AssumeRole. Kebijakan tersebut harus menentukan Nama Sumber Daya Amazon (ARN) peran sebagai sumber daya. Perhatikan hal berikut:

   - Jika Anda memberikan izin kepada pengguna dari akun yang tidak Anda kendalikan, dan pengguna akan mengambil peran ini secara terprogram, lalu pilih Memerlukan ID eksternal. ID eksternal dapat berupa kata atau nomor apa pun yang disepakati antara Anda dan administrator

akun pihak ketiga. Opsi ini secara otomatis menambahkan kondisi ke kebijakan kepercayaan yang memungkinkan pengguna untuk mengambil peran hanya jika permintaan menyertakan STS:externalid yang benar. Untuk informasi selengkapnya, lihat Cara menggunakan ID eksternal saat memberikan akses ke AWS sumber daya Anda kepada pihak ketiga.

- Jika Anda ingin membatasi peran untuk pengguna yang masuk dengan otentikasi multi-faktor (MFA), pilih Memerlukan MFA. Ini menambahkan persyaratan ke kebijakan kepercayaan peran yang memeriksa masuk MFA. Seorang pengguna yang ingin mengasumsikan peran tersebut harus masuk dengan kata sandi satu kali sementara dari perangkat MFA yang dikonfigurasi. Pengguna tanpa otentikasi MFA tidak dapat mengambil peran. Untuk informasi selengkapnya tentang MFA, lihat Menggunakan otentikasi multi-faktor (MFA) di. AWS

5. Pilih Berikutnya: Izin.

   IAM menyertakan daftar kebijakan di akun. Di bawah Tambahkan Izin, masukkan amspatchmanagedpolicy di kotak filter dan pilih kotak centang untuk kebijakan izin ini. Klik Berikutnya.

6. Di bawah Rincian peran, masukkan nama Peran seperti PatchRole, tambahkan deskripsi untuk peran (disarankan), juga tambahkan tag untuk membantu Anda mengidentifikasi peran ini. Nama peran tidak peka huruf besar/kecil, tetapi harus unik di dalam Akun AWS. Setelah selesai, klik Buat Peran.

> **Note**
>
> Nama peran tidak dapat diedit setelah dibuat.

Memahami notifikasi tambalan dan kegagalan tambalan di AMS Accelerate

> **Important**
>
> Mulai 1 Februari 2025, pelanggan AMS tidak akan lagi menerima pemberitahuan untuk Windows Pemeliharaan Patch kosong di akun terkelola mereka.

Permintaan layanan patch dan pemberitahuan email

AMS membuat permintaan layanan baru empat hari sebelum Jendela Pemeliharaan Patch berikutnya. Misalnya, empat hari sebelum Jendela Pemeliharaan Patch bernama App1 PROD berjalan, AMS membuat permintaan layanan berjudul Jendela Pemeliharaan Patch April untuk App1 Prod for Account [id akun]. Gunakan permintaan layanan tambalan untuk berkomunikasi dengan AMS jika Anda memerlukan penyesuaian pada patch terjadwal, atau untuk melewati tambalan yang akan datang. Saat permintaan layanan dibuat, email dikirim ke alamat notifikasi tambalan Anda dengan tautan ke permintaan layanan. Anda menerima email tambahan setiap kali AMS memperbarui permintaan layanan.

> **Note**
>
> AMS membuat permintaan layanan baru, meskipun Jendela Pemeliharaan Patch dibuat kurang dari empat hari sebelum dijadwalkan untuk dijalankan.
> Jendela Patch Maintenance harus dalam status “diaktifkan” untuk menerima pemberitahuan Permintaan Layanan.

Satu jam sebelum penambalan dimulai, AMS memberi tahu Anda melalui permintaan layanan patch. Setelah patch selesai, AMS memperbarui permintaan layanan patch dengan link ke konsol Patch Manager. Gunakan tautan untuk melihat kepatuhan patch untuk instance yang ditargetkan oleh Jendela Pemeliharaan Patch.

> **Note**
>
> Tautan di konsol Patch Manager menunjukkan kepatuhan instans saat ini. Patch Manager menunjukkan instance sebagai tidak sesuai jika tambalan baru dirilis antara waktu AMS menyelesaikan penambalan dan Anda mengakses tautan.

Pemberitahuan tambalan melalui CloudWatch Acara

AMS mengirimkan CloudWatch Peristiwa tiga kali selama proses tambalan termasuk yang berikut:

- Empat hari sebelum Patch Maintenance Window berjalan.
- Satu jam sebelum Patch Maintenance Window berjalan.
- Saat Jendela Pemeliharaan Patch selesai.

Berikut ini adalah skema acara pemberitahuan lanjutan Patch Maintenance Window:

```
{
    "version": "0",
    "id": "37004d81-458d-2cef-fe1c-8afa8af30406",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "145917996532",
    "time": "2021-05-20T02:00:00Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {
        "State": "PREEMPTIVE",
        "StartTime": "2021-05-24T02:00:00.000000",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\"}, {\"instanceId\":
 \"i-0000000aaaaaaaaab\"}]"
    }
}
```

Tabel berikut menjelaskan skema acara pemberitahuan awal Patch Maintenance Window:

Detail pemberitahuan tambalan

Nama properti	Deskripsi	Nilai sampel
Status	Keadaan jendela pemeliharaan tambalan	PREEMPTIVE - Jendela patching dijadwalkan akan segera dimulai
Status	Status jendela pemeliharaan tambalan	SUKSES - Semua contoh ditambal tanpa kegagalan GAGAL - Setidaknya satu instance gagal menambal

Nama properti	Deskripsi	Nilai sampel
StartTime	Waktu mulai, dalam format ISO, dari jendela pemeliharaan tambalan	2021-02-03T 22:14:05.814 308
WindowArn	Pengidentifikasi unik dari Jendela Pemeliharaan Patching	arn:aws:ssm:us-timur-1:1234 56789012: maintenancewindow/mw-00000001235
Hasil	Daftar instance yang ditargetkan oleh jendela patch	InstanceId — ID instance dari instance yang ditargetkan

Berikut ini adalah skema acara akhir Patch Maintenance Window:

```
{"version": "0",
    "id": "0f25add5-44a9-0702-d2bc-bd2102affefe",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "123456789012",
    "time": "2021-02-03T22:14:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {"State": "[COMPLETED]",
        "Status": "SUCCESS",
        "StartTime": "2021-02-03T22:12:00.814308",
        "EndTime": "2021-02-03T22:14:05.814309",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "WindowExecutionId": "e32088eb-c05f-4c63-b766-6866e163c818",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\", \"status\":
 \"Success\", \"missing_critical_patch_count\": 0, \"missing_total_patch_count
\": 0} }, {\"instanceId\": \"i-0000000aaaaaaaaab\", \"status\": Success},
 \"missing_critical_patch_count\": 0, \"missing_total_patch_count\": 0}]"
    }
}
```

Tabel berikut menjelaskan skema acara akhir Patch Maintenance Window:

Detail akhir jendela tambalan

Nama properti	Deskripsi	Nilai sampel
Status	Keadaan jendela pemeliharaan tambalan	SELESAI - Jendela tambalan selesai
Status	Status jendela pemeliharaan tambalan	SUKSES - Semua contoh ditambal tanpa kegagalan GAGAL - Setidaknya satu instance gagal menambal
StartTime	Waktu mulai, dalam format ISO, dari jendela pemeliharaan tambalan	2021-02-03T 22:14:05.814 308
EndTime	Waktu akhir, dalam format ISO, dari jendela pemeliharaan tambalan	2021-02-03T 23:14:05.814 308
WindowArn	Pengidentifikasi unik dari jendela pemeliharaan tambalan.	arn:aws:ssm:us-timur-1:1234 56789012: maintenan cewindow/mw-00000001235
WindowExecutionId	ID eksekusi jendela, yang dapat dilihat dari Konsol Jendela Pemeliharaan SSM	e32088eb-c05f-4c63-b766-6866e163c818
Hasil	Daftar instance yang akan ditargetkan oleh jendela patch	InstanceId — ID instance yang ditargetkan status - status patch instance missing_critical_patch_count - jumlah tambalan kritis yang hilang pada instance

Nama properti	Deskripsi	Nilai sampel
		missing_total_patch_count - jumlah total patch yang hilang pada instance

Anda dapat menggunakan CloudWatch acara Acara untuk memicu CloudWatch aturan yang memberi tahu Anda saat pemberitahuan terlebih dahulu Jendela Pemeliharaan Patching dikirim. Untuk melakukan ini, konfigurasikan CloudWatch aturan dengan konfigurasi berikut:

```
{
    "source": [
        "aws.managedservices"
    ],
    "detail-type": [
        "AMS Patch Window Execution State Change"
    ],
    "detail": {
        "State": ["PREEMPTIVE"]
    }
}
```

> **Note**
>
> Peringatan kegagalan patch tidak dibuat untuk instance yang memiliki sistem operasi yang tidak didukung, atau yang dihentikan selama jendela pemeliharaan.

Investigasi kegagalan tambalan di AMS

AWS Managed Services (AMS) mengelola patching dan menyertakan remediasi kegagalan patch. Saat tambalan gagal, Operasi AMS diperingatkan dan mencoba perbaikan dengan mengikuti AWS dan praktik terbaik AMS untuk mengatasi masalah tersebut.

<instance-id>Jika tambalan gagal, AMS akan membuat SSM OpsItem di akun dengan judul berikut: AWS Managed Services — Kegagalan Instans Patch misalnya.

AMS kemudian menyelidiki. OpsItem Jika AMS dapat memperbaiki kegagalan tanpa intervensi Anda, maka AMS menyelesaikannya. OpsItem Jika intervensi Anda diperlukan, AMS akan memberi tahu

Anda melalui permintaan layanan yang berisi hasil investigasi dan langkah-langkah perbaikan yang disarankan. Jika Anda tidak mengambil tindakan untuk menyelesaikan masalah, AMS mencoba menambal instance selama Jendela Pemeliharaan Patch terjadwal berikutnya.

> **Note**
>
> Kegagalan patch OpsItems tidak dibuat untuk instance yang memiliki sistem operasi yang tidak didukung, atau yang berada dalam status Berhenti selama Jendela Pemeliharaan Patch.

Optimalisasi biaya dengan Penjadwal Sumber Daya AMS

AWS Solusi AMS Resource Scheduler on membantu Anda mengurangi biaya AWS dan AMS dengan menghentikan sumber daya yang tidak digunakan dan memulai sumber daya saat kapasitas diperlukan. Misalnya, Anda dapat menggunakan Penjadwal Sumber Daya AMS AWS di lingkungan pengembangan untuk menghentikan instans secara otomatis di luar jam kerja setiap hari. Jika Anda membiarkan semua instans Anda berjalan pada pemanfaatan penuh, solusi ini dapat mengurangi penggunaan instans, yang mengurangi biaya keseluruhan berdasarkan jadwal yang Anda konfigurasi.

Gunakan Penjadwal Sumber Daya AWS Managed Services (AMS) untuk menjadwalkan mulai dan berhenti otomatis grup Auto Scaling, instans EC2 Amazon, dan instans Amazon RDS di akun Anda. Ini membantu mengurangi biaya infrastruktur di mana sumber daya tidak dimaksudkan untuk berjalan 24/7. Solusinya dibangun di atas Penjadwal AWS Instance tetapi berisi fitur dan penyesuaian tambahan khusus untuk kebutuhan pelanggan AMS. Kustomisasi mencakup dukungan untuk penjadwalan grup Auto Scaling CloudWatch , penekan alarm untuk alarm Elastic Load Balancing, dukungan untuk beberapa jendela AWS Systems Manager pemeliharaan untuk EC2 Amazon, estimator penghematan biaya, dan dukungan operasional dari AMS.

Penjadwal Sumber Daya AMS menggunakan periode dan jadwal. Periode menentukan waktu sumber daya harus dijalankan, seperti waktu mulai, waktu akhir, dan hari dalam sebulan. Jadwal berisi periode yang Anda tentukan, bersama dengan konfigurasi tambahan—jendela pemeliharaan SSM, zona waktu, hibernasi, dll—dan tentukan kapan sumber daya harus dijalankan. Anda dapat mengonfigurasi periode dan jadwal ini menggunakan runbook otomatisasi yang disediakan AMS AWS Systems Manager . Setiap jadwal harus berisi setidaknya satu periode yang menentukan waktu (s) instance harus dijalankan. Jadwal dapat berisi lebih dari satu periode. Ketika lebih dari satu periode digunakan dalam jadwal, Penjadwal Instance menerapkan tindakan awal yang sesuai ketika setidaknya salah satu aturan periode benar. Untuk detail selengkapnya tentang jadwal dan periode, lihat Komponen Solusi Penjadwal Instans AWS.

Penjadwal Sumber Daya AMS menggunakan tag AWS sumber daya untuk mengaitkan jadwal ke satu atau beberapa sumber daya untuk menargetkannya untuk tindakan mulai dan berhenti yang dijadwalkan. Anda menandai sumber daya Anda dengan kunci tag (default`Schedule`) dikonfigurasi di Scheduler dengan nama jadwal sebagai nilai. Anda mengonfigurasi kunci tag yang sama dengan tag alokasi biaya AWS Cost Explorer untuk fitur penaksir biaya Penjadwal untuk melacak dan melaporkan penghematan biaya.

Penjadwal Sumber Daya AMS adalah fitur ikut serta yang dapat Anda aktifkan per akun.

Menggunakan sumber daya dengan Penjadwal Sumber Daya AMS

Amazon EC2

- EC2 Instans Amazon yang merupakan bagian dari grup Auto Scaling tidak diproses secara individual dan dilewati oleh Penjadwal Sumber Daya AMS, meskipun ditandai.
- Jika volume root instans target dienkripsi dengan kunci master AWS KMS pelanggan (CMK), `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, Anda dapat menambahkan izin dengan memperbarui CloudFormation tumpukan,`ams-resource-scheduler`, dengan daftar CMK sebagai nilai ke `UseCMK` parameter (gunakan satu atau lebih Kunci CMK ARNs dalam format `arn:`*`partition`*`:kms:`*`region`*`:`*`account-id`*`:key/`*`key-id`* alih-alih alias KMS).
- Jika EC2 instans Amazon Anda dikonfigurasi dengan perangkat lunak tertentu, atau lisensi vendor yang dikelola oleh AWS License Manager, Resource Scheduler memerlukan izin ke AWS License Manager lisensi tertentu agar dapat memulai instance. Anda dapat memberikan Resource Scheduler izin yang diperlukan dengan menambahkan daftar ARN lisensi ke AWS License Manager lisensi manajer Lisensi untuk parameter EC2 instance stack (). CloudFormation `ams-resource-scheduler`

EC2 Auto Scaling Amazon

- 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 grup Auto Scaling 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.

Amazon RDS

- Penjadwal dapat mengambil snapshot sebelum menghentikan instance RDS (tidak berlaku untuk cluster Aurora DB). Fitur ini diaktifkan secara default dengan parameter CloudFormation template Create RDS Instance Snapshot AWS 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.

> **Note**
>
> Resource Scheduler tidak memvalidasi bahwa sumber daya dimulai atau dihentikan. Itu membuat panggilan API untuk layanan yang relevan dan melanjutkan. Jika panggilan API gagal, ia mencatat kesalahan untuk penyelidikan.
> Penjadwal Sumber Daya AMS tidak mendukung AWS Backup jendela. Jika Anda memetakan instans RDS yang AWS Backup diaktifkan dengan jadwal Resource Scheduler, agar cadangan berfungsi seperti yang diharapkan, jendela cadangan harus berada di dalam jendela jadwal yang sedang berjalan.

Penjadwal Sumber Daya AMS Orientasi

Akun Anda tidak secara otomatis masuk ke Penjadwal Sumber Daya AMS saat akun Anda dionboard ke paket operasi Akselerasi AMS. Namun, sebagai bagian dari orientasi akun ke paket operasi AMS Accelerate, atau kapan saja setelahnya, Anda dapat meminta Cloud Service Delivery Manager (CSDM) untuk memasukkan akun ke Penjadwal Sumber Daya AMS. Setelah CSDM Anda masuk ke akun, CloudFormation tumpukan yang berisi sumber daya Penjadwal Sumber Daya AMS dengan konfigurasi default, secara otomatis disediakan ke akun Anda.

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, lihatMenyesuaikan Penjadwal Sumber Daya AMS, selanjutnya.

Menyesuaikan Penjadwal Sumber Daya AMS

Saat onboard, Penjadwal Sumber Daya AMS diterapkan sebagai CloudFormation tumpukan, dengan nama`aams-resource-scheduler`, di wilayah AWS utama untuk akun AMS Accelerate Anda. Anda dapat mengonfigurasi properti Penjadwal Sumber Daya AMS berdasarkan preferensi Anda melalui parameter CloudFormation tumpukan dan melakukan pembaruan tumpukan. Untuk informasi tentang memperbarui CloudFormation tumpukan, lihat Memperbarui tumpukan secara langsung.

Kami menyarankan Anda menyesuaikan properti berikut dan membiarkan sisanya secara default untuk fungsionalitas optimal.

- Nama tag: Nama tag yang akan digunakan Resource Scheduler untuk mengaitkan jadwal instance dengan sumber daya. Nilai default-nya adalah `Schedule`.
- Layanan untuk menjadwalkan: Daftar layanan yang dipisahkan koma yang dapat dikelola oleh Resource Scheduler. Nilai defaultnya adalah "`ec2,rds,autoscaling`". Nilai yang valid adalah “ec2", “rds” dan “autoscaling”.
- Zona waktu default: Tentukan zona waktu default untuk Resource Scheduler untuk digunakan. Nilai default-nya adalah `UTC`.
- CMK untuk volume EBS terenkripsi: Daftar Amazon KMS Customer Managed Key (CMK ARNs) yang dipisahkan koma yang dapat diberikan izin kepada Resource Scheduler.
- Lisensi manajer lisensi EC2 misalnya: Daftar AWS Licence Manager yang dipisahkan koma ARNs untuk Resource Scheduler tersebut dapat diberikan izin untuk.

> **Note**
>
> AMS terkadang merilis fitur dan perbaikan agar AMS Resource Scheduler tetap up to date di akun Anda. Ketika ini terjadi, kustomisasi apa pun yang Anda buat pada tumpukan Penjadwal Sumber Daya AMS melalui parameter tumpukan dipertahankan.
> Kami sangat menyarankan agar tidak melakukan penyesuaian apa pun secara langsung ke salah satu sumber daya komponen Penjadwal Sumber Daya AMS. Melakukan hal itu memengaruhi fungsionalitas Resource Scheduler dan kemampuan AMS untuk tetap up to date.

Menggunakan Penjadwal Sumber Daya AMS

Cara menggunakan periode Penjadwal Sumber Daya AMS di akun AMS Accelerate.

Gunakan kumpulan runbook AWS Systems Manager otomatisasi berikut untuk mengelola jadwal dan periode yang diperlukan di Penjadwal Sumber Daya AMS.

> **Note**
>
> Runbook otomatisasi SSM ini tersedia di Wilayah AWS utama akun Anda.

- `AWSManagedServices-AddOrUpdatePeriod`
- `AWSManagedServices-AddOrUpdateSchedule`
- `AWSManagedServices-DeleteScheduleOrPeriod`
- `AWSManagedServices-DescribeScheduleOrPeriods`
- `AWSManagedServices-EnableOrDisableAMSResourceScheduler`

Selain itu, AMS AWS Identity and Access Management menyediakan peranams_resource_scheduler_ssm_automation_role,, yang AWS Systems Manager membutuhkan dan mengasumsikan untuk menggunakan runbook. Peran IAM dicakup dengan kebijakan sebaris hak istimewa paling sedikit yang memberikan izin SSM yang diperlukan untuk fungsionalitas runbook.

Prasyarat

Lakukan langkah-langkah berikut sebelum Anda mulai menggunakan runbook otomatisasi SSM dan Penjadwal Sumber Daya AMS.

Lampirkan kebijakan berikut ke entitas IAM yang sesuai (pengguna, grup, atau peran) yang ingin Anda izinkan untuk menggunakan runbook otomatisasi untuk mengelola jadwal dan periode di Penjadwal Sumber Daya AMS. Kebijakan ini tidak diperlukan jika entitas IAM Anda memiliki Administrator atau PowerUser izin di akun Anda.

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowPassingResourceSchedulerRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/
ams_resource_scheduler_ssm_automation_role",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "ListAndDescribeAutomationExecutions",
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:DescribeAutomationStepExecutions"
            ],
            "Resource": "arn:aws:ssm:*:111122223333:automation-execution/*"
        },
        {
            "Sid": "ListAndDescribeResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocumentVersions",
                "ssm:DescribeDocument",
                "ssm:ListDocumentMetadataHistory",
                "ssm:DescribeDocumentParameters",
                "ssm:GetDocument",
                "ssm:DescribeDocumentPermission"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdatePeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdateSchedule",
                "arn:aws:ssm:*::document/AWSManagedServices-
DeleteScheduleOrPeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-
DescribeScheduleOrPeriods",
                "arn:aws:ssm:*::document/AWSManagedServices-
EnableOrDisableAMSResourceScheduler"
            ]
        },
```

```
        {
            "Sid": "AllowExecutionOfResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdatePeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdateSchedule:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DeleteScheduleOrPeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DescribeScheduleOrPeriods:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
EnableOrDisableAMSResourceScheduler:*"
            ]
        },
        {
            "Sid": "AllowListingAllDocuments",
            "Effect": "Allow",
            "Action": "ssm:ListDocuments",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingAllSSMExecutions",
            "Effect": "Allow",
            "Action": "ssm:DescribeAutomationExecutions",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingIAMRolesForStartingExecutionViaConsole",
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        }
    ]
}
```

Anda dapat menjalankan otomatisasi baik dari AWS Systems Manager konsol atau menggunakan AWS CLI. Jika menggunakan AWS CLI, Anda mungkin perlu menginstal dan mengkonfigurasinya

atau AWS alat untuk PowerShell, jika Anda belum melakukannya. Untuk selengkapnya, lihat Menginstal atau memutakhirkan alat baris AWS perintah.

Tonton video Navish untuk mempelajari lebih lanjut (4:52)

Bekerja dengan periode dan jadwal di AWS Managed Services Resource Scheduler

Anda dapat menggunakan Penjadwal Sumber Daya AMS untuk menambah, memperbarui, atau menghapus jadwal atau periode di akun AMS Accelerate.

Menambahkan atau memperbarui periode di Penjadwal Sumber Daya AMS

Tambahkan atau perbarui periode Resource Scheduler di akun AMS Anda.

Data yang Anda perlukan:

- Tindakan: Jenis operasi yang harus dilakukan. Gunakan “tambah” jika Anda ingin menambahkan periode atau “pembaruan” jika Anda ingin memperbarui periode yang ada.
- Nama: Nama periode. Anda harus menentukan nilai unik jika Anda menambahkan periode baru.
- AutomationAssumeRole: ARN peran AWS Identity and Access Management (IAM) yang memungkinkan runbook menambah atau memperbarui periode atas nama Anda. Tentukan peran sebagai`ams_resource_scheduler_ssm_automation_role`.
- Deskripsi (Opsional): Deskripsi yang bermakna untuk periode tersebut.
- BeginTime(Opsional): Waktu dalam format HH: MM ketika Anda ingin memulai sumber daya.
- EndTime(Opsional): Waktu dalam format HH: MM ketika Anda ingin menghentikan sumber daya.
- Bulan (Opsional): Daftar bulan yang dibatasi koma atau rentang bulan dengan tanda hubung selama sumber daya harus dijalankan.
- MonthDays(Opsional): Daftar hari dalam sebulan yang dibatasi koma atau rentang hari dengan tanda hubung selama sumber daya harus dijalankan.
- WeekDays(Opsional): Daftar hari dalam seminggu yang dibatasi koma atau rentang hari dalam seminggu di mana sumber daya harus dijalankan.

Cara melakukannya:

- Lihat dokumen di AWSManagedServices-AddOrUpdatePeriod(Anda mungkin harus memilih Region onboard Anda).

Tentukan persyaratan di bagian Parameter input, lalu pilih Jalankan. Setelah operasi selesai, lihat hasil di Output tab.

- AWS CLI:

  Jalankan perintah berikut untuk memulai otomatisasi. Ganti *placeholders* dengan informasi Anda sendiri.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdatePeriod" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"],
    "Description":["DESCRIPTION"],"BeginTime":["TIME"], "EndTime":["TIME"],
    "Months":["MONTH"],"MonthDays":["DAY"], "WeekDays":["DAY"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

Contoh:

Contoh berikut menunjukkan bagaimana Anda dapat menambahkan periode baru menggunakan AWS Systems Manager konsol. Kami telah menamai periode Period-Name dan mengonfigurasinya untuk mencakup 9AM-6PM dari Senin-Jumat selama 15 hari pertama setiap bulan.

1. Lihat dokumen AWS Systems Manager otomatisasi di AWSManagedServices-AddOrUpdatePeriod(Anda mungkin harus memilih Region onboard Anda).

2. Berikan nilai untuk parameter.

3. Klik Execute dan tunggu otomatisasi selesai.

Menambahkan atau memperbarui jadwal di Penjadwal Sumber Daya AMS

Menambahkan atau memperbarui jadwal Resource Scheduler di akun AMS Accelerate.

Data yang Anda perlukan:

- Tindakan: Jenis operasi yang harus dilakukan. Gunakan “add” jika Anda ingin menambahkan jadwal atau “update” jika Anda ingin memperbarui jadwal yang ada.
- Nama: Nama jadwal. Anda harus menentukan nilai unik jika Anda menambahkan jadwal baru.

- AutomationAssumeRole: ARN dari peran AWS Identity and Access Management (IAM) yang memungkinkan runbook untuk menambah atau memperbarui jadwal atas nama Anda. Tentukan perannya`aams_resource_scheduler_ssm_automation_role`.
- Deskripsi (Opsional): Deskripsi yang bermakna untuk jadwal.
- Jadwal (Opsional): Tentukan daftar periode yang dibatasi koma yang akan digunakan dengan jadwal ini. Setiap periode pasti sudah dibuat.
- RetainRunning(Opsional): Tentukan “true” untuk mencegah Resource Scheduler menghentikan sumber daya yang berjalan pada akhir periode berjalan jika sumber daya dimulai secara manual sebelum awal perod yang sedang berjalan. Secara default, Resource Scheduler menghentikan sumber daya.
- StopNewInstances(Opsional): Tentukan “false” untuk mencegah Resource Scheduler menghentikan sumber daya saat pertama kali diberi tag jika berjalan di luar periode berjalan. Secara default, Resource Scheduler menghentikan sumber daya.
- SSMMaintenanceWindow (Opsional): Tentukan daftar jendela pemeliharaan AWS Systems Manager (SSM) yang dibatasi koma yang ingin Anda tambahkan sebagai periode berjalan untuk jadwal. Anda juga harus menentukan properti UseMaintenanceWindow "" menjadi “true.”
- TimeZone(Opsional): Tentukan zona waktu yang Anda inginkan Resource Scheduler untuk digunakan. Secara default, Resource Scheduler menggunakan UTC.
- UseMaintenanceWindow(Opsional): Tentukan “true” jika Anda ingin Resource Scheduler untuk mempertimbangkan jendela pemeliharaan Amazon Relational Database Service (RDS) sebagai periode berjalan ke jadwal instans Amazon RDS, atau untuk menambahkan jendela pemeliharaan AWS Systems Manager (SSM) sebagai periode berjalan ke jadwal instans Amazon. EC2
- UseMetrics(Opsional): Tentukan “true” untuk mengaktifkan CloudWatch metrik pada tingkat jadwal dan “false” untuk menonaktifkan CloudWatch metrik. Menentukan properti ini akan mengesampingkan pengaturan CloudWatch metrik yang ditetapkan pada tingkat tumpukan.

Cara melakukannya:

- Lihat dokumen di AWSManagedServices-AddOrUpdateSchedule(Anda mungkin harus memilih Region onboard Anda).

  Tentukan persyaratan di bagian Parameter input, lalu pilih Jalankan. Setelah operasi selesai, lihat hasil di Output tab.
- AWS CLI:

Jalankan perintah berikut untuk memulai otomatisasi. Ganti *placeholders* dengan informasi Anda sendiri.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdateSchedule" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"], "Description":
["DESCRIPTION"],
    "Hibernate":["true or false"],"Enforced":["true or false"],
    "OverrideStatus":["running or stopped"],"Periods":["PERIOD-A, PERIOD-B"],
    "RetainRunning":["true or false"],"StopNewInstances":["true or false"],
    "SSMMaintenanceWindow":["WINDOW-NAME"],"TimeZone":["TIMEZONE"],
    "UseMaintenanceWindow":["true or false"],"UseMetrics":["true or false"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

Contoh:

Contoh berikut menunjukkan cara menambahkan jadwal untuk Penjadwal Sumber Daya AMS. Dalam contoh ini Anda menambahkan jadwal bernama CustomSchedule menggunakan CustomPeriod.

1. Lihat dokumen AWS Systems Manager otomatisasi di AWSManagedServices-AddOrUpdateSchedule(Anda mungkin harus memilih Region onboard Anda).

2. Berikan nilai untuk parameter.

3. Klik Execute dan tunggu otomatisasi selesai.

Menghapus periode atau jadwal di Penjadwal Sumber Daya AMS

Untuk menghapus periode atau jadwal Resource Scheduler di akun AMS Accelerate, Anda memerlukan data berikut:

- ConfigurationType: Jenis konfigurasi yang ingin Anda hapus. Gunakan “periode” jika Anda ingin menghapus periode atau “jadwal” jika Anda ingin menghapus jadwal.
- Nama: Nama jadwal atau periode yang ingin Anda hapus.

- AutomationAssumeRole: ARN peran AWS Identity and Access Management (IAM) yang memungkinkan runbook menghapus jadwal atau periode atas nama Anda. Tentukan perannyaams_resource_scheduler_ssm_automation_role.

Cara melakukannya:

- Lihat dokumen di AWSManagedServices-DeleteScheduleOrPeriod(Anda mungkin3harus memilih Wilayah onboard Anda).

  Tentukan persyaratan di bagian Parameter input, lalu pilih Jalankan. Setelah operasi selesai, lihat hasil di Output tab.
- AWS CLI:

  Jalankan perintah berikut untuk memulai otomatisasi. Ganti *placeholders* dengan informasi Anda sendiri.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DeleteScheduleOrPeriod" --document-version "\$DEFAULT"
--parameters '{"ConfigurationType":["period" or "schedule"],"Name":["NAME"],
    "AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}' --region ONBOARDED_REGION
```

Contoh:

Contoh berikut menunjukkan bagaimana Anda dapat menghapus periode menggunakan AWS Systems Manager konsol.

1. Lihat dokumen AWS Systems Manager otomatisasi di AWSManagedServices-DeleteScheduleOrPeriod(Anda mungkin harus memilih Region onboard Anda).

2. Berikan nilai untuk parameter.

3. Klik Execute dan tunggu otomatisasi selesai.

Menjelaskan periode atau jadwal dalam Penjadwal Sumber Daya AMS

Untuk menjelaskan (melihat detail tentang) periode atau jadwal Resource Scheduler di akun AMS Accelerate, Anda memerlukan data berikut:

- ConfigurationType: Jenis konfigurasi yang ingin Anda jelaskan. Gunakan “periode” jika Anda ingin menggambarkan semua periode atau “jadwal” jika Anda ingin menggambarkan semua jadwal.
- AutomationAssumeRole: ARN dari peran AWS Identity and Access Management (IAM) yang memungkinkan runbook untuk menggambarkan jadwal atau periode atas nama Anda. Tentukan perannyaams_resource_scheduler_ssm_automation_role.

Cara melakukannya:

- Lihat dokumen di AWSManagedServices-DescribeScheduleOrPeriods(Anda mungkin harus memilih Region onboard Anda):
  1. Tentukan persyaratan di bagian Parameter input dan kemudian pilih Jalankan.
  2. Setelah operasi selesai, lihat hasil di Output tab.
- AWS CLI:
  1. Jalankan perintah berikut untuk memulai otomatisasi. Ganti *placeholders* dengan informasi Anda sendiri.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DescribeScheduleOrPeriods" --document-version "\$DEFAULT"
                --parameters '{"ConfigurationType":["period" or
 "schedule"],"AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}'
                --region ONBOARDED_REGION
```

Contoh:

Contoh berikut menunjukkan bagaimana Anda dapat menggambarkan periode menggunakan AWS Systems Manager konsol.

1. Lihat dokumen AWS Systems Manager otomatisasi di AWSManagedServices-DescribeScheduleOrPeriods(Anda mungkin harus memilih Region onboard Anda).

2. Berikan nilai untuk parameter.

3. Klik Execute dan tunggu otomatisasi selesai.

Menandai sumber daya untuk Penjadwal Sumber Daya AMS

Menandai sumber daya untuk Penjadwal Sumber Daya AMS.

Setelah menambahkan jadwal dan periode ke Jadwal Sumber Daya AMS, Anda perlu menandai sumber daya Anda dengan nama tag Resource Scheduler sebagai kunci tag, atau yang disesuaikan, dan nama jadwal sebagai nilai tag. Untuk detail tentang cara menandai sumber daya Anda di akun AMS Accelerate, lihatMenandai AMS Accelerate.

> **Note**
>
> Jika Resource Tagger digunakan untuk menandai sumber daya, kunci Tag default untuk Resource Scheduler harus disesuaikan agar memiliki awalan '`ams:rt:`' karena semua tag yang diterapkan oleh tagger sumber daya memiliki key prefix ". `ams:rt:` Jika tidak, sumber daya yang ditandai dengan tagger sumber daya tidak akan dikelola oleh Resource Scheduler. Untuk mengetahui selengkapnya tentang menyesuaikan kunci Tag default untuk Resource Scheduler, lihat. Menyesuaikan Penjadwal Sumber Daya AMS

Penaksir biaya di Penjadwal Sumber Daya AMS

Untuk melacak penghematan biaya, AMS Resource Scheduler menampilkan komponen yang menghitung perkiraan penghematan biaya per jam untuk sumber daya Amazon dan EC2 Amazon 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 satu hari 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 24x0,125 = $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, penagihan AWS 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 di`AMS/ResourceScheduler`. CloudWatch

Jika tag alokasi biaya tidak diaktifkan, estimator tidak dapat menghitung penghematan dan menerbitkan metrik, bahkan jika itu diaktifkan.

> **Note**
>
> 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.

Penekan alarm di Penjadwal Sumber Daya AMS

Penjadwal Sumber Daya AMS dilengkapi dengan penekan CloudWatch Alarm, yang digunakan sebagai fungsi Lambda terpisah bernama yang menekan alarm untuk instans `AMSAlarmSuppressor` yang berada di belakang Elastic Load Balancing, Application Load Balancer, atau Network Load Balancer. Fungsi ini berjalan setiap 5 menit, mengambil semua alarm yang ada di akun dan mengelompokkannya berdasarkan namespace; misalnya,,,. `AWS/ELB` `AWS/`

`ApplicationELB` `AWS/NetworkELB` Untuk setiap grup alarm, penekan menemukan grup and/or target nama penyeimbang beban (untuk grup target, dan memeriksa status instans untuk ALB/NLB) from alarm dimensions, finds the instances that are registered with the load balancer and/or mengetahui apakah instance dijadwalkan oleh Penjadwal Sumber Daya AMS. Jika instance dijadwalkan oleh Resource Scheduler, dan dihentikan oleh Resource Scheduler, penekan kemudian menandai alarm untuk menonaktifkannya. Jika setidaknya satu instance dalam daftar instans terdaftar sedang berjalan, penekan menandai alarm yang sesuai untuk mengaktifkan alarm yang ditandai untuk diaktifkan, dan menonaktifkan alarm yang ditandai untuk dinonaktifkan. Log untuk ini disimpan dalam grup `/aws/lambda/AMSAlarmSuppressor` log.

Manajemen log di AMS Accelerate

AMS Accelerate mengonfigurasi AWS layanan yang didukung untuk mengumpulkan log. Log ini digunakan oleh AMS Accelerate untuk memastikan kepatuhan dan audit sumber daya dalam akun Anda.

AMS Accelerate menyediakan berbagai layanan operasional untuk membantu Anda mencapai keunggulan operasional di AWS. Untuk mendapatkan pemahaman cepat tentang bagaimana AMS membantu tim Anda mencapai keunggulan operasional secara keseluruhan di AWS Cloud dengan beberapa kemampuan operasional utama kami termasuk helpdesk 24x7, pemantauan proaktif, keamanan, penambalan, pencatatan, dan pencadangan, lihat Diagram Arsitektur Referensi AMS.

Topik

- Manajemen log - AWS CloudTrail
- Manajemen log - Amazon EC2
- Manajemen log - Log Aliran VPC Amazon

Manajemen log - AWS CloudTrail

AWS CloudTrailadalah layanan yang digunakan untuk tata kelola akun: kepatuhan, audit operasional, dan audit risiko. Dengan CloudTrail, Anda dapat log, terus memantau, dan mempertahankan aktivitas akun yang terkait dengan tindakan di seluruh AWS infrastruktur Anda.

AMS Accelerate memerlukan AWS CloudTrail pencatatan untuk mengelola audit dan kepatuhan untuk semua sumber daya di akun Anda. Saat melakukan orientasi, Anda dapat memilih salah satu opsi berikut:

- Jejak yang diterapkan AMS: Jika Anda memilih opsi ini, AMS membuat, menyebarkan, dan mengelola jejak CloudTrail Multi-wilayah di AWS Wilayah utama Anda, terlepas dari jejak yang ada di akun Anda.
- Bawa jejak Anda sendiri: Jika Anda memilih untuk memberikan CloudTrail jejak akun atau organisasi Anda sendiri, maka Anda harus bekerja dengan Cloud Architect (CA) Anda untuk memastikannya memenuhi konfigurasi yang diperlukan untuk Accelerate. Jika Anda memilih opsi ini tetapi tidak menyediakan jejak Anda sendiri, Accelerate secara otomatis menyebarkan CloudTrail jejaknya sendiri untuk menjaga keamanan dan cakupan audit yang berkelanjutan.

Jika Anda menyediakan jejak Anda sendiri nanti, AMS menghapus jejak yang disebarkannya untuk menghindari redundansi dan biaya tambahan. Pendekatan ini membantu mempertahankan CloudTrail jejak aktif tunggal di akun Anda dan mencegah biaya pencatatan duplikat.

> **Note**
>
> Jika akun Anda memiliki CloudTrail jejak yang ada dan Anda belum secara khusus mengonfigurasi atau meminta jejak terkelola AMS selama orientasi, AMS Accelerate secara otomatis menghapus jejak yang diterapkan AMS dari akun Anda. Ini mencegah pencatatan duplikat, mengoptimalkan penggunaan sumber daya, dan menghemat biaya tambahan.

AMS Accelerate membuat bucket Amazon S3 untuk CloudTrail jejak yang diterapkan Accelerate sebagai tujuan pengiriman peristiwa dan menggunakan enkripsi AWS Key Management Service ()AWS KMS. Acara jejak Anda diakses oleh operator AMS Accelerate untuk tujuan investigasi dan diagnosis. Jika akun sudah mengaktifkan CloudTrail jejak yang ada, jejak ini adalah tambahan untuk itu, jika Anda memilih untuk meminta Accelerate menyebarkan jejak terkelola Accelerate selama orientasi.

AMS Accelerate menerapkan AWS Config aturan untuk memastikan bahwa jejak CloudTrail akun Anda, termasuk jejak yang diterapkan CloudTrail Accelerate telah diatur dan dienkripsi dengan benar. Untuk mempelajari selengkapnya, lihat AWS Config. Ini adalah aturan yang digunakan, disajikan sebagai tautan ke AWS dokumentasi yang menjelaskannya:

- multi-region-cloudtrail-enabled. Memeriksa apakah AMS Accelerate CloudTrail diatur dengan benar dengan konfigurasi yang benar.
- cloud-trail-encryption-enabled. Pemeriksaan yang AWS CloudTrail dikonfigurasi untuk menggunakan enkripsi sisi server (SSE) dengan enkripsi kunci master AWS KMS pelanggan (CMK).
- cloud-trail-log-file-validasi-diaktifkan. Saat diaktifkan, pemeriksaan yang AWS CloudTrail membuat file intisari bertanda tangan dengan log. Kami sangat menyarankan agar Anda mengaktifkan validasi file di semua jalur.
- s3- bucket-default-lock-enabled. Saat diaktifkan, periksa apakah bucket Amazon S3 telah mengaktifkan kunci.
- s3- bucket-logging-enabled. Saat diaktifkan, periksa apakah pencatatan diaktifkan untuk bucket Amazon S3.

AMS Accelerate digunakan AWS KMS untuk mengenkripsi peristiwa yang dicatat untuk Accelerate deployed CloudTrail trail di akun Anda. Kunci ini dikendalikan oleh, dan dapat diakses oleh, administrator akun, operator AMS Accelerate, dan CloudTrail. Untuk informasi selengkapnya AWS KMS, lihat AWS Key Management Service fitur dokumentasi produk.

Mengakses dan mengaudit log CloudTrail

CloudTrail log untuk CloudTrail jejak penerapan AMS Accelerate disimpan di bucket Amazon S3 dalam akun Anda. Data jejak yang disimpan di bucket Amazon S3 dienkripsi menggunakan kunci AWS KMS yang dibuat saat sumber daya disediakan. CloudTrail

Bucket Amazon S3 memanfaatkan pola penamaan ams-a ***`aws account id`*** -cloudtrail-***`AWS Region`***, (contoh: ams-a123456789 - -1a) dan semua peristiwa disimpan dengan awalan AWS/. cloudtrail-us-east CloudTrail Semua akses ke bucket utama dicatat dan objek log dienkripsi dan diversi untuk tujuan audit.

Untuk informasi selengkapnya tentang melacak perubahan dan menanyakan log, lihatMelacak perubahan di akun AMS Accelerate.

Melindungi dan mempertahankan kayu CloudTrail gelondongan

AMS Accelerate memungkinkan penguncian objek Amazon S3 dengan Mode Tata Kelola untuk CloudTrail jejak yang diterapkan Accelerate untuk memastikan bahwa pengguna tidak dapat menimpa atau menghapus versi objek atau mengubah pengaturan pengunciannya tanpa izin khusus. Untuk informasi selengkapnya, lihat penguncian objek Amazon S3.

Secara default, semua log di bucket ini disimpan tanpa batas waktu. Jika ingin mengubah periode penyimpanan, Anda dapat mengirimkan permintaan layanan melalui AWS Dukungan Pusat untuk menyiapkan kebijakan penyimpanan yang berbeda.

Mengakses log Amazon EC2

Anda dapat mengakses log EC2 instans Amazon dengan menggunakan file AWS Management Console. Log yang dihasilkan oleh instans dan AWS layanan tersedia di CloudWatch Log, yang tersedia di setiap akun yang dikelola oleh AMS Accelerate. Untuk informasi tentang mengakses log Anda, lihat dokumentasi CloudWatch Log.

Mempertahankan log Amazon EC2

Log EC2 instans Amazon disimpan tanpa batas waktu, secara default. Jika ingin mengubah periode penyimpanan, Anda dapat mengirimkan permintaan layanan melalui AWS Dukungan Pusat untuk menyiapkan kebijakan penyimpanan yang berbeda.

Manajemen log - Amazon EC2

AMS Accelerate menginstal CloudWatch agen di semua EC2 instans Amazon yang telah Anda identifikasi sebagai AMS Accelerate-managed. Agen ini mengirimkan log tingkat sistem ke Amazon CloudWatch Logs. Untuk selengkapnya, lihat Apa itu CloudWatch Log Amazon?

File log berikut dikirim ke CloudWatch Log, ke dalam grup log dengan nama yang sama dengan log. Dalam setiap grup log, aliran log dibuat untuk setiap EC2 instans Amazon, dinamai sesuai dengan ID EC2 instans Amazon.

Linux

- /var/log/amazon/ssm/amazon-ssm-agent.log
- /var/log/amazon/ssm/errors.log
- /var/log/audit/audit.log
- /var/log/auth.log
- /var/log/cloud-init-output.log
- /var/log/cron
- /var/log/dnf.log
- /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

Untuk informasi selengkapnya, lihat Membuat atau Mengedit File Konfigurasi CloudWatch Agen Secara Manual.

Windows

- SSMAgentLog Amazon
- AmazonCloudWatchAgentLog
- SSMErrorLog Amazon
- AmazonCloudFormationLog
- ApplicationEventLog
- EC2ConfigServiceEventLog
- MicrosoftWindowsAppLockerEXEAndDLLEventLog
- MicrosoftWindowsAppLockerMSIAndScriptEventLog
- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog

Untuk informasi selengkapnya, lihat Mulai Cepat: Aktifkan EC2 Instans Amazon Anda yang Menjalankan Windows Server 2016 untuk Mengirim Log ke CloudWatch Log Menggunakan Agen CloudWatch Log.

Manajemen log - Log Aliran VPC Amazon

VPC Flow Logs adalah fitur yang menangkap informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di VPC Anda. Data log aliran dapat dipublikasikan ke CloudWatch log Amazon atau Amazon S3. Pengumpulan data log aliran tidak mempengaruhi throughput atau latensi jaringan. Anda dapat membuat atau menghapus flow log tanpa mempengaruhi kinerja jaringan.

Log alur dapat membantu Anda dengan sejumlah tugas, seperti:

- Mendiagnosis aturan Grup Keamanan yang terlalu ketat
- Memantau lalu lintas yang mencapai instans Anda
- Menentukan arah lalu lintas ke dan dari antarmuka jaringan

Anda tidak perlu mengaktifkan log aliran VPC untuk setiap VPC yang baru dibuat di akun Accelerate. AMS akan secara otomatis mendeteksi apakah VPC memiliki log aliran menggunakan aturan - ams-nist-cis-vpcConfig flow-logs-enabled. Jika log aliran VPC tidak diaktifkan, AMS akan memperbaikinya secara otomatis dengan membuat log aliran VPC dengan bidang khusus. Memiliki bidang tambahan ini akan memungkinkan AMS dan pelanggan untuk memantau lalu lintas VPC dengan lebih baik, memahami dependensi jaringan, memecahkan masalah konektivitas jaringan, dan mengidentifikasi ancaman jaringan.

Untuk informasi tentang melihat dan mencari log alur, lihat Bekerja dengan log alur.

Melacak perubahan di akun AMS Accelerate

Important

Layanan Change Record tidak digunakan lagi pada 1 Juli 2025.
Akun baru tidak dapat di-onboard ke layanan Change Record.
Untuk melakukan kueri CloudTrail data di akun AMS Accelerate, Anda dapat menggunakan layanan ini:

- Di AWS CloudTrail, pilih Riwayat acara dan filter peristiwa menggunakan atribut Pencarian. Anda dapat menggunakan filter rentang waktu dan memilih untuk memfilter riwayat peristiwa berdasarkan sumber Peristiwa dengan yang `s3.amazon.aws.com` ditentukan, atau memilih untuk memfilter riwayat peristiwa berdasarkan Nama Pengguna. Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail acara.
- Gunakan AWS CloudTrail Lake untuk mengumpulkan data melalui kueri. Dalam AWS CloudTrail memilih Lake, dan kemudian pilih Query. Anda dapat membuat kueri sendiri, menggunakan generator kueri, atau menggunakan kueri sampel untuk mengumpulkan data berbasis peristiwa. Misalnya, Anda dapat bertanya siapa yang menghapus EC2 instans Amazon minggu lalu. Untuk informasi selengkapnya, lihat Membuat data lake dari AWS CloudTrail sumber dan CloudTrailLake kueri.
- Buat tabel Amazon Athena AWS CloudTrail dan atur lokasi penyimpanan sebagai bucket Amazon S3 yang terkait dengan jejak Anda. Verifikasi bahwa wilayah Beranda untuk jejak Anda dan bucket Amazon S3 adalah sama. Di Amazon Athena, gunakan editor Kueri untuk menjalankan kueri default yang disediakan Accelerate untuk digunakan dengan konsol Athena. Untuk informasi selengkapnya tentang cara membuat tabel Athena ke CloudTrail log kueri, lihat Log kueri AWS CloudTrail.

Topik

- Melihat catatan perubahan Anda
- Kueri default
- Ubah izin rekaman

AWS Managed Services membantu Anda melacak perubahan yang dibuat oleh tim Operasi Akselerasi AMS dan otomatisasi AMS Accelerate dengan menyediakan antarmuka yang dapat dikueri menggunakan konsol Amazon Athena (Athena) dan manajemen log AMS Accelerate.

Athena adalah layanan kueri interaktif yang dapat Anda gunakan untuk menganalisis data di Amazon S3 dengan menggunakan Bahasa Kueri Terstruktur standar (SQL) (lihat Referensi SQL untuk Amazon Athena). Athena tidak memiliki server, sehingga tidak ada infrastruktur untuk dikelola dan Anda hanya membayar untuk mengkueri yang Anda jalankan. AMS Accelerate membuat tabel Athena dengan partisi harian di atas CloudTrail log, dan menyediakan kueri di AWS Wilayah utama Anda dan dalam grup kerja. ams-change-record Anda dapat memilih salah satu kueri default dan menjalankannya sesuai kebutuhan. Untuk mempelajari selengkapnya tentang kelompok kerja Athena, lihat Cara Kerja Kelompok Kerja.

> **Note**
>
> Hanya Accelerate yang dapat melakukan kueri CloudTrail peristiwa untuk akun Accelerate Anda menggunakan Athena saat Accelerate terintegrasi dengan jejak CloudTrail Organisasi Anda, kecuali administrator Organisasi Anda menerapkan Peran IAM untuk menggunakan Athena untuk menanyakan dan menganalisis CloudTrail peristiwa di akun Anda, selama orientasi.

Menggunakan catatan perubahan, Anda dapat dengan mudah menjawab pertanyaan seperti:

- Siapa (AMS Accelerate Systems atau AMS Accelerate Operator) telah mengakses akun Anda
- Perubahan apa yang telah dilakukan oleh AMS Accelerate di akun Anda
- Kapan AMS Accelerate melakukan perubahan di akun Anda
- Ke mana harus pergi untuk melihat perubahan yang dibuat di akun Anda
- Mengapa AMS Accelerate diperlukan untuk membuat perubahan di akun Anda
- Cara memodifikasi kueri untuk mendapatkan jawaban atas semua pertanyaan tersebut untuk perubahan non-AMS juga

Melihat catatan perubahan Anda

Untuk menggunakan kueri Athena, masuk ke konsol AWS Manajemen dan arahkan ke konsol Athena di Wilayah utama Anda. AWS

> **Note**
>
> Jika Anda melihat halaman Amazon Athena Memulai saat melakukan salah satu langkah, klik Memulai. Ini mungkin muncul untuk Anda bahkan jika infrastruktur Change Record Anda sudah ada.

1. Pilih Workgroup dari panel navigasi atas di konsol Athena.
2. Pilih ams-change-recordworkgroup, lalu klik Ganti Workgroup.
3. Pilih ams-change-record-databasedari kotak Database Combo. ams-change-record-databaseTermasuk ams-change-record-tabletabel.
4. Pilih Kueri Tersimpan dari panel navigasi atas.
5. Jendela Kueri Tersimpan menampilkan daftar kueri yang disediakan AMS Accelerate, yang dapat Anda jalankan. Pilih kueri yang ingin Anda jalankan dari daftar Kueri Tersimpan. Misalnya, kueri ams_session_accesses_v1.

   Untuk daftar lengkap kueri Akselerasi AMS prasetel, lihat. Kueri default
6. Sesuaikan filter datetime di kotak editor kueri sesuai kebutuhan; secara default, kueri hanya memeriksa perubahan dari hari terakhir.
7. Pilih Run query (Jalankan kueri).

Kueri default

AMS Accelerate menyediakan beberapa kueri default yang dapat Anda gunakan dalam konsol Athena. Kueri default tercantum dalam tabel berikut.

> **Note**
>
> - Semua kueri menerima rentang datetime sebagai filter opsional; semua kueri berjalan selama 24 jam terakhir, secara default. Untuk masukan yang diharapkan, lihat ayat berikut,Memodifikasi filter datetime dalam kueri.
> - Masukan parameter yang dapat atau perlu Anda ubah ditampilkan dalam kueri seperti *<PARAMETER_NAME>* kawat gigi sudut. Ganti placeholder dan kurung gigi sudut dengan nilai parameter Anda.

- Semua filter bersifat opsional. Dalam kueri, beberapa filter opsional dikomentari dengan tanda hubung ganda (--) di awal baris. Semua kueri akan berjalan tanpa mereka, dengan parameter default. Jika Anda ingin menentukan nilai parameter untuk filter opsional ini, hapus tanda hubung ganda (--) di awal baris dan ganti parameter yang Anda inginkan.
- Semua kueri kembali `IAM PincipalId` dan `IAM SessionId` dalam output
- Biaya yang dihitung untuk menjalankan kueri tergantung pada berapa banyak CloudTrail log yang dihasilkan untuk akun tersebut. Untuk menghitung biaya, gunakan Kalkulator Harga AWS Athena.

Kueri kalengan

Tujuan/Deskripsi	Masukan	Output
Nama kueri: `ams_access_session_query_v1`		
Melacak AMS Mempercepat sesi akses Memberikan informasi tentang sesi akses Akselerasi AMS tertentu. Kueri menerima ID Utama IAM sebagai filter opsional dan mengembalikan waktu acara, kebutuhan bisnis untuk mengakses akun, pemohon, dan sebagainya. Anda dapat memfilter ID Utama IAM tertentu dengan menghapus komentar baris dan mengganti placeholder *`IAM PrincipalId`*	(Opsional)`IAM PrincipalId` : Pengenal Utama IAM dari sumber daya yang mencoba mengakses. Formatnya adalah*`UNIQUE_ID ENTIFIER`* :*`RESOURCE_NAME`* . Untuk detailnya lihat pengidentifikasi unik. Anda dapat menjalankan kueri tanpa filter ini untuk menentukan IAM yang tepat PrincipalId yang ingin Anda filter.	• EventTime: Waktu mendapatkan akses • EventName: Nama Acara AWS (AssumeRole) • EventRegion: Wilayah AWS yang mendapatkan permintaan • EventId: ID CloudTrail Acara • BusinessNeed Jenis: Jenis alasan bisnis untuk mengakses akun. Nilai yang diizinkan adalah: SupportCase, OpsItem, Masalah, Teks. • BusinessNeed: Bisnis perlu mengakses akun. Misalnya, Support Case ID, Ops Item ID, dan lain sebagainya. • Pemohon: ID Operator yang mengakses akun, atau sistem Otomasi yang mengakses akun.

Tujuan/Deskripsi	Masukan	Output
dengan ID tertentu di editor kueri. Anda juga dapat mencantumkan sesi akses non-AMS dengan menghapus baris filter agen pengguna di klausa WHERE dari kueri.		• RequestAccessType: Jenis pemohon (Sistem,, Opsapi OpsConsole, Tidak disetel)
Nama kueri: `ams_events_query_v1`		
Lacak semua tindakan mutasi yang dilakukan oleh AMS Accelerate Mengembalikan semua tindakan penulisan yang dilakukan pada akun menggunakan filter peran AMS Accelerate. Anda juga dapat melacak tindakan mutasi yang dilakukan oleh peran non-AMS dengan menghapus baris filter useridentity.arn dari klausa WHERE kueri.	(Opsional) Hanya rentang datetime. Lihat Memodifikasi filter datetime dalam kueri.	• AccountId: AWS ID Akun • RoleArn: RoleArn untuk pemohon • EventTime: Waktu mendapatkan akses • EventName: Nama Acara AWS (AssumeRole) • EventRegion: Wilayah AWS yang mendapatkan permintaan • EventId: ID CloudTrail Acara • RequestParameters : Parameter permintaan untuk permintaan • ResponseElements: Elemen respons untuk respons. • UserAgent: Agen CloudTrail Pengguna AWS
Nama kueri: `ams_instance_access_sessions_query_v1`		

Tujuan/Deskripsi	Masukan	Output
Lacak akses instans oleh AMS Accelerate Mengembalikan daftar akses instans Akseleras i AMS; setiap catatan mencakup waktu acara, Wilayah peristiwa, ID instance, ID Utama IAM, ID Sesi IAM, ID Sesi SSM. Anda dapat menggunakan ID Utama IAM untuk mendapatkan detail lebih lanjut tentang kebutuhan bisnis untuk mengakses instance dengan menggunakan kueri Athena`aams_acces s_session s_query_v1` . Anda dapat menggunakan ID Sesi SSM untuk mendapatkan detail selengkapnya tentang sesi akses instans, termasuk waktu mulai dan akhir sesi, detail log, dan menggunakan konsol Pengelola AWS Sesi di AWS Wilayah instans. Pengguna juga dapat mencantumkan akses instans non-AMS dengan menghapus baris filter	Hanya`datetime range`. Lihat Memodifik asi filter datetime dalam kueri.	• InstanceId: ID Instance • SSMSession Id: ID Sesi SSM • RoleArn: RoleArn untuk pemohon • EventTime: Waktu mendapatkan akses • EventName: Nama Acara AWS (AssumeRole) • EventRegion: Wilayah AWS yang mendapatkan permintaan • EventId: ID CloudTrail Acara

Tujuan/Deskripsi	Masukan	Output
identitas pengguna di klausa WHERE dari kueri.		

Nama kueri: `ams_privilege_escalation_events_query_v1`

Tujuan/Deskripsi	Masukan	Output
Melacak peristiwa izin (eskalasi) untuk pengguna AMS dan non-AMS Menyediakan daftar peristiwa yang dapat secara langsung atau berpotensi menyebabkan eskalasi hak istimewa. Kueri menerima ActionedBy sebagai filter opsional dan mengembalikan EventName, EventId, EventTime, dan sebagainya. Semua bidang yang terkait dengan acara juga dikembalikan. Bidang kosong jika tidak berlaku untuk acara itu. ActionedBy Filter dinonaktifkan, secara default; untuk mengaktifkannya, hapus “-” dari baris itu. Secara default, ActionedBy filter dinonaktifkan (ini akan menampilkan peristiwa eskalasi hak istimewa dari semua pengguna). Untuk menampilkan peristiwa bagi pengguna	(Opsional)`ACTIONEDBY_PUT_USER_NAME` : Nama pengguna untuk pengguna ActionedBy. Ini bisa menjadi pengguna atau peran IAM. Misalnya, ams-access-admin. (Opsional)`datetime range`. Lihat Memodifikasi filter datetime dalam kueri.	• AccountId: Id Akun • ActionedBy: ActionedBy Nama Pengguna • EventTime: Waktu mendapatkan akses • EventName: AWS Nama acara (AssumeRole). • EventRegion: Wilayah AWS yang mendapatkan permintaan • EventId: ID CloudTrail Acara

Tujuan/Deskripsi	Masukan	Output
atau peran tertentu, hapus tanda hubung ganda (--) dari baris filter identitas pengguna di klausa WHERE dan ganti placeholder *ACTIONEDBY_PUT_USER_NAME_HERE* dengan nama pengguna atau peran IAM. Anda dapat menjalankan kueri tanpa filter untuk menentukan pengguna yang tepat yang ingin Anda filter.		
Nama kueri: `ams_resource_events_query_v1`		
Lacak peristiwa penulisan untuk sumber daya tertentu AMS atau non-AMS Menyediakan daftar peristiwa yang dilakukan pada sumber daya tertentu. Kueri menerima ID sumber daya sebagai bagian dari filter (ganti placeholder *RESOURCE_INFO* di klausa WHERE dari kueri), dan mengembalikan semua tindakan tulis yang dilakukan pada sumber daya tersebut.	(Wajib)`RESOURCE_INFO` : Pengidentifikasi sumber daya, dapat berupa ID untuk sumber daya AWS apa pun di akun. Jangan bingung ini dengan sumber daya ARNs. Misalnya, ID instance untuk sebuah EC2 instance, nama tabel untuk tabel DynamoDB logGroupName , untuk Log, dll CloudWatch . (Opsional)`datetime range`. Lihat Memodifikasi filter datetime dalam kueri.	• AccountId: Id Akun • ActionedBy: ActionedBy Nama Pengguna • EventTime: Waktu mendapatkan akses • EventName: AWS Nama acara (AssumeRole). • EventRegion: Wilayah AWS yang mendapatkan permintaan • EventId: ID CloudTrail Acara

Tujuan/Deskripsi	Masukan	Output
Nama kueri: `ams_session_events_query_v1`		
Melacak tindakan menulis yang dilakukan oleh AMS Accelerate selama sesi tertentu Menyediakan daftar acara yang dilakukan pada sesi tertentu. Kueri menerima ID Utama IAM sebagai bagian dari filter (ganti placeholder *PRINCIPAL_ID* di klausa WHERE dari kueri), dan mengembalikan semua tindakan tulis yang dilakukan pada sumber daya tersebut.	(Wajib)`PRINCIPAL_ID` : ID Utama untuk sesi tersebut. Formatnya adalah*UNIQUE_ID ENTIFIER* :*RESOURCE_NAME* . Untuk detailnya lihat pengidentifikasi unik. Anda dapat menjalankan query “ams_session_ids_by_requester_v1" untuk mendapatkan daftar IAM Principal untuk pemohon. IDs Anda juga dapat menjalankan kueri tanpa filter ini untuk menentukan IAM yang tepat yang ingin Principal Id Anda filter. (Opsional)`datetime range`. Lihat Memodifikasi filter datetime dalam kueri.	• AccountId: Id Akun • ActionedBy: ActionedBy Nama Pengguna • EventTime: Waktu mendapatkan akses • EventName: Nama Acara AWS (AssumeRole) • EventRegion: Wilayah AWS yang mendapatkan permintaan • EventId: ID CloudTrail Acara
Nama kueri: `ams_session_ids_by_requester_v1`		

Tujuan/Deskripsi	Masukan	Output
Lacak IAM Principal /Session IDs untuk pemohon tertentu. Kueri menerima “pemohon” (ganti placeholder *Requester* dalam klausa WHERE dari kueri), dan mengembalikan semua Id Utama IAM oleh pemohon tersebut selama rentang waktu yang ditentukan.	(Wajib)`Requester` : ID Operator yang mengakses akun (misalnya: alias operator) , atau sistem Otomasi yang mengakses akun (misalnya: OsConfiguration, AlarmManager, dll.). (Opsional)`datetime range`. Lihat Memodifikasi filter datetime dalam kueri.	• IAM PrincipalId - IAM Principal Id sesi. Formatnya adalah*UNIQUE_ID ENTIFIER* :*RESOURCE_NAME* . Untuk detailnya lihat pengidentifikasi unik. Anda dapat menjalankan kueri tanpa filter ini untuk menentukan IAM yang tepat yang ingin PrincipalId Anda filter. • IAM SessionId - ID Sesi IAM untuk sesi akses • EventTime: Waktu mendapatkan akses

Memodifikasi filter datetime dalam kueri

Semua kueri menerima rentang datetime sebagai filter opsional. Semua kueri berjalan selama satu hari terakhir secara default.

Format yang digunakan untuk bidang datetime adalah yyyy/MM/dd (misalnya: 2021/01/01). Ingatlah bahwa itu hanya menyimpan tanggal dan bukan seluruh stempel waktu. Untuk seluruh stempel waktu, gunakan field eventime, yang menyimpan stempel waktu dalam format ISO 8601 yyyy-MM-dd T HH: mm: SS Z (misalnya: 2021-01-01T 23:59:59 Z). Namun, karena tabel dipartisi pada bidang datetime, Anda harus meneruskan filter datetime dan eventtime ke kueri. Lihat contoh berikut.

> **Note**
>
> Untuk melihat semua cara yang diterima Anda dapat memodifikasi rentang, lihat dokumentasi fungsi Presto terbaru berdasarkan versi mesin Athena yang saat ini digunakan untuk Fungsi dan Operator Tanggal dan Waktu untuk melihat semua cara yang diterima Anda dapat memodifikasi rentang.

Level Tanggal: 1 hari terakhir atau 24 jam terakhir (Default) Contoh: Jika CURRENT_DATE='2021/01/01', filter akan mengurangi satu hari dari tanggal saat ini dan memformatnya sebagai datetime> '2020/12/31'

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
```

Tingkat Tanggal: Contoh 2 bulan terakhir:

```
datetime > date_format(date_add('month', - 2, CURRENT_DATE), '%Y/%m/%d')
```

Tingkat Tanggal: Antara 2 tanggal contoh:

```
datetime > '2021/01/01'
      AND
      datetime < '2021/01/10'
```

Tingkat Stempel Waktu: Contoh 12 jam terakhir:

Data partisi dipindai hingga 1 hari terakhir dan kemudian memfilter semua peristiwa dalam 12 jam terakhir

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND
      eventtime > date_format(date_add('hour', - 12, CURRENT_TIMESTAMP), '%Y-%m-%dT%H:
%i:%sZ')
```

Tingkat Stempel Waktu: Antara 2 contoh stempel waktu:

Dapatkan acara antara 1 Jan 2021 12:00 PM dan Jan 10, 2021 15.00.

```
datetime > '2021/01/01' AND datetime < '2021/01/10'
      AND
      eventtime > '2021-01-01T12:00:00Z' AND eventtime < '2021-01-10T15:00:00Z'
```

Contoh kueri default

ams_access_session_query_v1

```
Name: ams_access_session_query_v1

Description: >-
```

```
    The query provides more information on specific AMS access session.
    The query accepts IAM Principal Id as an optional filter and returns event time,
  business need for accessing the account, requester, ... etc.
    By default; the query filter last day events only, the user can change the datetime
  filter to search for more wide time range.
    By default; the IAM PrincipalId filter is disabled. To enable it, remove "-- " from
  that line.

AthenaQueryString: |-
    /*
      The query provides list of AMS access sessions during specific time range.
      The query accepts IAM Principal Id as an optional filter and returns event time,
  business need for accessing the account, requester, ... etc.

      By default, the query filters the last day's events only; you can change the
  "datetime" filter to search for a wider time range.

      By default; the IAM Principal ID filter is disabled (it shows access sessions for
  all IAM principals).
      If you want to only show access sessions for a particular IAM principal ID, remove
  the double-dash (--) from
      the "IAM Principal ID" filter line in the WHERE clause of the query, and replace
  the placeholder "<IAM PrincipalId>" with the specific ID that you want.
      You can run the query without the filter to determine the exact IAM PrincipalId
  you want to filter with.

      By default; the query only shows AMS access sessions. If you also want to show
  non-AMS access sessions,
      remove the "useragent" filter in the WHERE clause of the query.

      For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
  in your AMS Accelerate accounts -> Default Queries
    */

    SELECT
       json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
  PrincipalId",
       json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
  SessionId",
       eventtime AS "EventTime",
       eventname AS "EventName",
       awsregion AS "EventRegion",
       eventid AS "EventId",
       json_extract_scalar(requestparameters, '$.tags[0].value') AS "BusinessNeed",
```

```
      json_extract_scalar(requestparameters, '$.tags[1].value') AS "BusinessNeedType",
      json_extract_scalar(requestparameters, '$.tags[2].value') AS "Requester",
      json_extract_scalar(requestparameters, '$.tags[3].value') AS "AccessRequestType"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND eventname = 'AssumeRole'
      AND useragent = 'access.managedservices.amazonaws.com'
      -- AND  json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId')
 = '<IAM PrincipalId>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of AMS access sessions during specific time range.
   # The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   #
   # By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
   # If you want to only show access sessions for a particular IAM principal ID, remove
 the # (#) from
   # the "IAM Principal ID" filter of the query, and replace the placeholder "<IAM
 PrincipalId>" with the specific ID that you want.
   # You can run the query without the filter to determine the exact IAM PrincipalId
 you want to filter with.
   #
   # By default; the query only shows AMS access sessions. If you also want to show
 non-AMS access sessions,
   # remove the "useragent" filter from the query.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter eventName="AssumeRole" AND userAgent="access.managedservices.amazonaws.com"
   # | filter responseElements.assumedRoleUser.assumedRoleId= "<IAM PrincipalId>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
```

```
      requestParameters.tags.0.value as BusinessNeed,
      requestParameters.tags.1.value as BusinessNeedType,
      requestParameters.tags.2.value as Requester,
      requestParameters.tags.3.value as AccessRequestType
```

ams_events_query_v1

```
ams_events_query_v1.yaml
/*
  The query provides list of events to track write actions for all AMS changes.
  The query returns all write actions done on the account using that AMS role filter.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  You can also track mutating actions done by non-AMS roles by removing the
 "useridentity.arn" filter lines from the WHERE clause of the query.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   useridentity.arn AS "RoleArn",
   eventid AS "EventId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventsource AS "EventService",
   eventtime AS "EventTime",
   requestparameters As "RequestParameters",
   responseelements AS "ResponseElements",
   useragent AS "UserAgent"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   readonly <> 'true'
   AND
   (
      LOWER(useridentity.arn) LIKE '%/ams%'
```

```
      OR LOWER(useridentity.arn) LIKE '%/customer_ssm_automation_role%'
   )
ORDER BY eventtime
```

ams_instance_access_sessions_query_v1

```
ams_instance_access_sessions_query_v1
/*
  The query provides list of AMS Instance accesses during specific time range.

  The query returns the list of AMS instance accesses; every record includes the event
 time, the event AWS Region, the instance ID, the IAM session ID, and the SSM session
 ID.
  You can use the IAM Principal ID to get more details on the business need for
 accessing the instance by using ams_access_session_query_v1 athena query.
  You can use the SSM session ID to get more details on the instance access session,
 including the start and end time of the session and log details, using the AWS Session
 Manager Console in the instance's AWS Region.

  You can also list non-AMS instance accesses by removing the "useridentity" filter
 line in the WHERE clause of the query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   json_extract_scalar(requestparameters, '$.target') AS "InstanceId",
   json_extract_scalar(responseelements, '$.sessionId') AS "SSM SessionId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventsource AS "EventService",
   eventtime AS "EventTime"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   useridentity.sessionContext.sessionIssuer.arn like '%/ams_%'
```

```
   AND eventname = 'StartSession'
ORDER BY eventtime
```

ams_privilege_escalation_events_query_v1

```
ams_privilege_escalation_events_query_v1.yaml
/*
  The query provides list of events that can directly or potentially lead to a
 privilege escalation.

  The query accepts ActionedBy as an optional filter and returns EventName, EventId,
 EventTime, ... etc.
  All fields associated with the event are also returned. Some fields are blank if not
 applicable for that event.
  You can use the IAM Session ID to get more details about events happened in that
 session by using ams_session_events_query_v1 query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  By default, the ActionedBy filter is disabled (it shows privilege escalation events
 from all users).
  To show events for a particular user or role, remove the double-dash (--) from the
 useridentity filter line in the WHERE clause of the query
  and replace the placeholder "<ACTIONEDBY_PUT_USER_NAME_HERE>" with an IAM user or
 role name.
  You can run the query without the filter to determine the exact user you want to
 filter with.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventtime AS "EventTime",
   json_extract_scalar(requestparameters, '$.userName') AS "UserName",
```

```
   json_extract_scalar(requestparameters, '$.roleName') AS "RoleName",
   json_extract_scalar(requestparameters, '$.groupName') AS "GroupName",
   json_extract_scalar(requestparameters, '$.policyArn') AS "PolicyArn",
   json_extract_scalar(requestparameters, '$.policyName') AS "PolicyName",
   json_extract_scalar(requestparameters, '$.permissionsBoundary') AS
 "PermissionsBoundary",
   json_extract_scalar(requestparameters, '$.instanceProfileName') AS
 "InstanceProfileName",
   json_extract_scalar(requestparameters, '$.openIDConnectProviderArn') AS
 "OpenIDConnectProviderArn",
   json_extract_scalar(requestparameters, '$.serialNumber') AS "SerialNumber",
   json_extract_scalar(requestparameters, '$.serverCertificateName') AS
 "ServerCertificateName",
   json_extract_scalar(requestparameters, '$.accessKeyId') AS "AccessKeyId",
   json_extract_scalar(requestparameters, '$.certificateId') AS "CertificateId",
   json_extract_scalar(requestparameters, '$.newUserName') AS "NewUserName",
   json_extract_scalar(requestparameters, '$.newGroupName') AS "NewGroupName",
   json_extract_scalar(requestparameters, '$.newServerCertificateName') AS
 "NewServerCertificateName",
   json_extract_scalar(requestparameters, '$.name') AS "SAMLProviderName",
   json_extract_scalar(requestparameters, '$.sAMLProviderArn') AS "SAMLProviderArn",
   json_extract_scalar(requestparameters, '$.sSHPublicKeyId') AS "SSHPublicKeyId",
   json_extract_scalar(requestparameters, '$.virtualMFADeviceName') AS
 "VirtualMFADeviceName"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   (
     -- More event names can be found at https://docs.aws.amazon.com/IAM/latest/
UserGuide/list_identityandaccessmanagement.html
     eventname LIKE 'Add%' OR
     eventname LIKE 'Attach%' OR
     eventname LIKE 'Delete%' AND eventname != 'DeleteAccountAlias' OR
     eventname LIKE 'Detach%' OR
     eventname LIKE 'Create%' AND eventname != 'CreateAccountAlias' OR
     eventname LIKE 'Put%' OR
     eventname LIKE 'Remove%' OR
     eventname LIKE 'Update%' OR
     eventname LIKE 'Upload%' OR
     eventname = 'DeactivateMFADevice' OR
     eventname = 'EnableMFADevice' OR
     eventname = 'ResetServiceSpecificCredential' OR
     eventname = 'SetDefaultPolicyVersion'
   )
```

```
   AND eventsource = 'iam.amazonaws.com'
ORDER BY eventtime
```

ams_resource_events_query_v1

```
Name: ams_resource_events_query_v1

Description: >-
   The query provides list of events done on specific resource.
   The query accepts resource id as part of the filters, and return all write actions
 done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of events done on specific resource.

     The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the WHERE clause of the query),
     and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
     Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventid AS "EventId",
      eventsource AS "EventService",
      eventtime AS "EventTime"
   FROM
```

```
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
      AND
      (
         requestparameters LIKE '%<RESOURCE_INFO>%'
         OR responseelements LIKE '%<RESOURCE_INFO>%'
      )
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of events done on specific resource.
   #
   # The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the filter of the query),
   # and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
   # Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
   # | filter RequestParameters like "RESOURCE_INFO" or ResponseElements like
 "<RESOURCE_INFO>"
   | fields
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
      eventSource as EventService,
      eventTime as EventTime
   | display IAMPrincipalId, IAMSessionId, AccountId, ActionedBy, EventName,
 EventRegion, EventId, EventService, EventTime
   | sort eventTime desc
```

ams_session_events_query_v1

```
Name: ams_session_events_query_v1

Description: >-
   The query provides list of events done on specific session.
   The query accepts IAM Principal Id as part of the filters, and return all write
 actions done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides a list of events executed on a specific session.

     The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the WHERE clause of the query),
     and returns all write actions done on that resource.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventsource AS "EventService",
      eventtime AS "EventTime",
      requestparameters As "RequestParameters",
      responseelements AS "ResponseElements",
      useragent AS "UserAgent"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate   WHERE
      useridentity.principalid = '<PRINCIPAL_ID>'
      AND datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
   ORDER BY eventtime
```

```
InsightsQueryString: |-
   # The query provides a list of events executed on a specific session.
   #
   # The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the filter of the query),
   # and returns all write actions done on that resource.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0 AND userIdentity.principalId = "<IAM Principal>"
   | sort eventTime desc
   | fields
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventSource as EventService,
      eventTime as EventTime,
      userAgent as UserAgent
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
```

ams_session_ids_by_requester_v1

```
Name: ams_session_ids_by_requester_v1

Description: >-
   The query provides list of IAM Principal/Session Ids for specific requester.
   The query accepts requester and return all IAM Principal/Session Ids by that
 requester during specific time range.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of IAM Principal IDs for a specific requester.

     The query accepts the requester (replace placeholder "<Requester>" in the WHERE
 clause of the query),
```

```
     and returns all IAM Principal IDs by that requester during a specific time range.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
      json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionIId",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND json_extract_scalar(requestparameters, '$.tags[2].value') = '<Requester>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of IAM Principal IDs for a specific requester.
   #
   # The query accepts the requester (replace placeholder "<Requester>" in the filter
 of the query),
   # and returns all IAM Principal IDs by that requester during a specific time range.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   filter eventName="AssumeRole" AND requestParameters.tags.2.value="<Requester>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime
```

Ubah izin rekaman

Izin berikut diperlukan untuk menjalankan kueri catatan perubahan:

- Athena

  - Athena: GetWorkGroup
  - Athena: StartQueryExecution
  - Athena: ListDataCatalogs
  - Athena: GetQueryExecution
  - Athena: GetQueryResults
  - Athena: BatchGetNamedQuery
  - Athena: ListWorkGroups
  - Athena: UpdateWorkGroup
  - Athena: GetNamedQuery
  - Athena: ListQueryExecutions
  - Athena: ListNamedQueries
- AWS KMS
  - kms:Decrypt
  - AWS KMS ID kunci AMSCloudTrailLogManagement, atau ID AWS KMS kunci Anda, jika Accelerate menggunakan peristiwa CloudTrail jejak penyimpanan data bucket Amazon S3 menggunakan enkripsi SSE-KMS.
- AWS Glue
  - lem: GetDatabase
  - lem: GetTables
  - lem: GetDatabases
  - lem: GetTable
- Akses baca Amazon S3
  - CloudTrail Data bucket Amazon S3: ams-a *AccountId* -cloudtrail-*primary region*, atau nama bucket Amazon S3 Anda, acara jejak penyimpanan data bucket Amazon S3. CloudTrail
- Akses tulis Amazon S3
  - Hasil kueri acara Athena Bucket Amazon S3: ams-a athena-results- *AccountId primary region*

AWS Systems Manager di Accelerate

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 Amazon. Proses AMS untuk pengembangan dan penerbitan dokumen SSM mengikuti praktik terbaik AWS dan memerlukan beberapa tinjauan sejawat sepanjang siklus hidup dokumen. Untuk informasi selengkapnya tentang praktik terbaik AWS untuk berbagi Dokumen SSM, silakan kunjungi Praktik terbaik untuk dokumen SSM bersama.

Dokumen SSM Akselerasi AMS yang tersedia

Dokumen SSM Akselerasi AMS tersedia secara eksklusif untuk pelanggan AMS Accelerate, dan digunakan untuk mengotomatiskan alur kerja operasional untuk mengoperasikan akun Anda.

Untuk melihat dokumen AMS Accelerate 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 AWS CLI petunjuk, lihat Menggunakan dokumen SSM bersama.

AMS Mempercepat versi dokumen SSM

Dokumen SSM mendukung pembuatan versi. Dokumen SSM AMS Accelerate tidak dapat dimodifikasi dari akun pelanggan dan tidak dapat dibagikan ulang. Mereka dikelola dan dikelola secara terpusat oleh AMS Accelerate untuk mengoperasikan akun.

Nomor versi ditambahkan dengan setiap pembaruan dokumen di Wilayah AWS tertentu. 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 SSM AMS Accelerate, sebaiknya bandingkan hash mereka dengan: AWS CLI

```
aws ssm describe-document \
--name AWSManagedServices-DOCUMENTNAME \
--output text --query "Document.Hash"
```

Dua dokumen SSM identik jika hash mereka cocok.

Harga Systems Manager

Tidak ada biaya yang terkait dengan akses dokumen AMS Accelerate SSM. Biaya runtime bervariasi berdasarkan jenis dokumen SSM, langkah-langkahnya, dan durasi runtime. Untuk informasi lebih lanjut, lihat AWS Systems Manager harga.

Riwayat dokumen untuk Panduan Pengguna AMS Accelerate

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan Pengguna Akselerasi AMS. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Diperbarui manajemen Log - AWS CloudTrail bagian	Informasi dan catatan baru tentang AWS CloudTrail pencatatan.	September 25, 2025
Menambahkan 4 pemeriksaan optimasi Trusted Advisor biaya baru yang didukung oleh Trusted Remediator	Menambahkan pemeriksaan pengoptimalan biaya berikut: • 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	September 22, 2025
Catatan penghentian yang diperbarui untuk layanan Change Record	Catatan penghentian yang diperbarui untuk layanan Ubah Rekaman dengan solusi alternatif.	September 11, 2025
Pemeriksaan Trusted Advisor keamanan yang diperbaru	Memperbarui parameter dan kendala yang telah	September 5, 2025

i didukung oleh Trusted Remediator	dikonfigurasi sebelumnya yang Didukung untuk memeriksa Hs4Ma3G108 - jejak harus diintegrasikan dengan Amazon Logs CloudTrail CloudWatch	
Pemeriksaan Trusted Advisor keamanan yang diperbaru i didukung oleh Trusted Remediator	Pemeriksaan Trusted Advisor keamanan yang diperbarui untuk menambahkan versi 2 dari Hs4Ma3G184 - Applicati on Load Balancers dan Classic Load Balancers logging harus diaktifkan	September 5, 2025
Pemeriksaan keunggulan Trusted Advisor operasional yang diperbarui didukung oleh bagian Remediator Tepercaya	Pemeriksaan keunggulan Trusted Advisor operasion al yang diperbarui didukung oleh Trusted Remediator untuk menambahkan cek baru yang didukung c1fd6b96l4 Amazon S3 Access Logs Diaktifkan.	Agustus 28, 2025
Bagian Remediator Tepercaya yang diperbarui untuk menyertakan konten baru untuk Compute Optimizer	Bagian Remediator Tepercaya 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
Tautan Glosarium TOC dihapus	AWS Glosarium.	Agustus 8, 2025
Bidang baru dalam laporan Patch Daily	Tag Instance: Tag yang terkait dengan ID EC2 instans Amazon.	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-TrustedRemediatorEnableBucketAccessLoggingVAWSManagedServices-TerminateEC InstanceStoppedForPeriodOfTime	Agustus 8, 2025
Memperbarui standar IAM di poin 3.2	Bahasa yang diklarifikasi dan menghapus penyebutan penandaan.	Juli 25, 2025
Profil Konfigurasi Tagger Sumber Daya yang Diperbarui di Accelerate	Menambahkan AvailabilityZone filter baru di Profil Konfigurasi Tagger Sumber Daya di Accelerate.	Juli 25, 2025
Laporan Insiden yang diperbarui, permintaan layanan, dan pertanyaan penagihan di Accelerate.	Mengganti referensi ke tingkatan layanan Plus dan Premium dengan tautan ke layanan SLA.	Juli 25, 2025
Manajemen Insiden yang Diperbarui di Accelerate.	Informasi terbaru tentang pusat operasi.	Juli 25, 2025
Halaman pola AMS yang diperbarui dengan tautan yang benar.	Memperbaiki tautan SLA dan SLO.	Juli 25, 2025

Pembaruan opsi opt-out peringatan	Penambahan tag memungkinkan Anda untuk memilih keluar dari dua peringatan tambahan.	Juli 25, 2025
Fitur baru untuk backup	Sesuaikan notifikasi pada brankas cadangan dengan tag baru.	Juli 25, 2025
Bagian yang diperbarui untuk konfigurasi yang Didukung di Accelerate	Memperbarui Konfigurasi yang didukung untuk sistem operasi yang didukung dan sistem operasi End of Support (EOS) yang Didukung di Accelerate.	Juni 26, 2025
Halaman yang dihapus Mengelola tag untuk manajemen patch di Accelerate	Halaman yang dihapus Mengelola tag untuk manajemen tambalan di Accelerate karena fitur ini tidak digunakan lagi.	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 Accelerate.	Juni 10, 2025
AMS Mempercepat penghentian rekaman perubahan.	Layanan AMS Accelerate Change Record tidak digunakan lagi efektif 1 Juli 2025.	27 Mei 2025
Pembaruan sistem operasi yang didukung.	Sistem operasi yang didukung AMS Accelerate diperbarui, beberapa ditambahkan, beberapa dihapus.	22 Mei 2025
Catatan untuk layanan yang didukung Wilayah Timur Tengah (UEA).	Dukungan terbatas untuk beberapa layanan di Wilayah Timur Tengah (UEA).	22 Mei 2025

Hanya internal. APIs	Hanya internal APIs yang muncul di beberapa CloudWatch log.	22 Mei 2025
Menambahkan lokasi log yang hilang.	Beberapa lokasi log Windows yang hilang ditambahkan.	22 Mei 2025
AMS Mempercepat pembaruan Remediator Tepercaya.	Cara menggunakan parameter baru,`preconfigured-parameters` , untuk menyesuaikan Trusted Advisor cek di Trusted Remediator.	22 Mei 2025
FAQ dan pembaruan AMS Accelerate Remediator Tepercaya.	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
AMS Mempercepat pembaruan kontrol keamanan Standar.	Menambahkan kontrol “Berbagi grup keamanan”.	8 Mei 2025
Mempercepat pembaruan peringatan pemantauan.	Peringatan tambahan ditambahkan, ditambah nama peringatan ditambahkan ke kolom Catatan.	April 28, 2025
Mempercepat inventaris sumber daya.	File spreadsheet inventaris sumber daya (dikompresi) diperbarui.	April 24, 2025

Mempercepat lokasi log.	Lokasi log tambahan ditambahkan.	April 24, 2025
Mempercepat peran dan tanggung jawab baru (RACI) untuk Respons Insiden Keamanan.	RACI untuk Respon Insiden Keamanan.	Maret 27, 2025
Mempercepat peringatan remediasi otomatis Amazon RDS Baru.	ID Peringatan: - 0224, terpicu ketika penyimpanan yang dialokasikan yang diminta mencapai atau melebihi ambang penyimpanan maksimum yang dikonfigurasi.	Maret 27, 2025
Mempercepat pembaruan templat peran Orientasi.	Templat peran orientasi AMS Accelerate telah diperbarui untuk mendukung GovCloud wilayah AWS.	Maret 25, 2025
Mempercepat Peringatan RDS remediasi otomatis baru.	RDS-EVENT-0224 ditambahkan.	Maret 17, 2025
Mempercepat fitur Baru: Pemberitahuan insiden.	Anda dapat menggunakan AppRegistry untuk membuat aplikasi dan menyesuaikan pemberitahuan insiden untuk aplikasi tersebut.	Maret 13, 2025
Mempercepat Pembaruan ke ambang pemantauan alarm RDS.	Ambang alarm Pemanfaatan CPU Rata-rata RDS telah diubah dari 75% menjadi 90%.	Februari 20, 2025
Mempercepat Pembaruan ke AMS remediasi otomatis tabel peringatan.	Tabel remediasi peringatan telah diperluas dengan konten baru.	Februari 20, 2025

Mempercepat fitur Baru: Pertahankan Alarm.	Anda dapat mengonfigurasi Manajer Alarm untuk menyimpan alarm CloudWatch alih-alih penghapusan otomatis.	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: • Laporan patch (harian) • Laporan Backup (harian) • Laporan insiden (mingguan) • Dasbor Tagger Sumber Daya • Dasbor Aturan Konfigurasi Keamanan	Januari 28, 2025

Menambahkan AWS Trusted Advisor pemeriksaan tambahan yang didukung oleh Trusted Remediator	Trusted Advisor Pemeriksaan berikut sekarang didukung oleh Trusted Remediator:
	• Pengoptimalan Biaya
	  • c1cj39rr6v - Konfigurasi Batalkan Unggahan Multipart Amazon S3 Tidak Lengkap
	• Keamanan
	  • Hs4Ma3G199 - Instans RDS DB harus menerbitkan log ke Log CloudWatch
	  • Hs4Ma3G326 - Amazon EMR memblokir pengaturan akses publik harus diaktifkan
	  • Hs4Ma3G272 - Pengguna seharusnya tidak memiliki akses root ke instance notebook AI SageMaker
	  • Hs4Ma3G325 - Kluster EKS harus mengaktifkan pencatatan audit
	  • HHs4Ma3G118 - Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar
	  • Hs4Ma3G127 - API Gateway REST dan pencatatan eksekusi API harus WebSocket diaktifkan
		Januari 28, 2025

    - Hs4Ma3G124 - Instans EC2 Amazon harus menggunakan Layanan Metadata Instance Versi 2 () IMDSv2
- Toleransi kesalahan
    - c1qf5bt013 - Instans Amazon RDS DB memiliki penskalaan otomatis penyimpanan dimatikan
    - 7q GXs KIUw - Classic Load Balancer Connectio n Draining
    - c18d2gz106 - Amazon EBS Tidak Termasuk dalam Paket AWS Backup
    - c18d2gz107 - Amazon DynamoDB Tabel Tidak Termasuk dalam Paket AWS Backup
    - cc18d2gz117 - Amazon EFS Tidak Termasuk dalam Paket AWS Backup
    - c18d2gz105 - Network Load Balancer Cross Load Balancing
    - c1qf5bt026 - Parameter Amazon RDS synchrono us_commit dimatikan
    - c1qf5bt030 - Amazon RDS innodb_flush_log_a t_trx_commit parameter bukan 1

    - c1qf5bt031 - Parameter Amazon RDS sync_binlog dimatikan
    - c1qf5bt036 - Amazon RDS innodb_default_row_format pengaturan parameter tidak aman
    - c18d2gz144 - Pemantauan Rinci Amazon Tidak Diaktifkan EC2
- Keunggulan Operasional
    - c18d2gz125 - Amazon API Gateway Tidak Mencatat Log Eksekusi
    - c18d2gz168 - Perlindungan Beban Elastis Tidak Diaktifkan untuk Load Balancer Balancing Deletion
    - c1qf5bt012 - Amazon RDS Performance Insights dimatikan
- Performa
    - c1qf5bt021 - Amazon RDS innodb_change_buffering parameter menggunakan kurang dari nilai optimal
    - c1qf5bt025 - Parameter autovacuum Amazon RDS dimatikan
    - c1qf5bt028 - Amazon RDS enable_indexonlyscan parameter dimatikan

	• c1qf5bt029 - Amazon RDS enable_indexscan parameter dimatikan • c1qf5bt032 - Amazon RDS innodb_stats_persistent parameter dimatikan • c1qf5bt037 - Parameter _logging Amazon diaktifkan RDSgeneral	
Spreadsheet inventaris sumber daya yang diperbarui	Spreadsheet inventaris sumber daya yang diperbarui.	Januari 23, 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
Fitur patch Accelerate baru: Patch Hooks	Gunakan fitur ini untuk mengonfigurasi “kait” dengan dokumen SSM Command untuk menjalankan perintah tingkat sistem operasi sebelum atau sesudah menambal.	Januari 16, 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

Update ke bagian Orientasi dari EKS Monitoring dan Incident Management	Memperbarui catatan prosedur orientasi untuk mengklari fikasi kapan sinyal peringatan ditangguhkan dan dilanjutkan.	Desember 19, 2024
Log akun anggota ditambahkan ke Remediator Tepercaya	Anda dapat menggunakan log akun Anggota untuk menemukan ID akun, onboard Wilayah AWS, dan waktu eksekusi setiap akun anggota.	Desember 19, 2024
Prasyarat untuk penggunaan Agen SSM	Konten tentang memblokir lalu lintas keluar diperbarui.	Desember 4, 2024
Percepatan Pemantauan dan Manajemen Insiden untuk EKS sekarang didukung di Asia Pasifik (Hong Kong) Wilayah AWS	Asia Pasifik (Hong Kong) sekarang didukung oleh Accelerate Monitoring and Incident Management untuk EKS	November 21, 2024
Tabel penawaran Operasi On Demand yang Diperbarui	Sistem operasi berikut didukung untuk peningkatan di tempat: • Microsoft Windows 2016 ke Microsoft Windows 2022 dan di atasnya	November 11, 2024
Mempercepat Pemantauan dan Manajemen Insiden untuk EKS sekarang didukung di Afrika (Cape Town) Wilayah AWS.	Afrika (Cape Town) sekarang didukung oleh Accelerate Monitoring and Incident Management untuk EKS	November 4, 2024

Tabel penawaran Operasi On Demand yang Diperbarui	Sistem operasi berikut didukung untuk peningkatan di tempat: • 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	November 1, 2024
Template Mulai Cepat Diperbarui	Diagram yang diperbarui, parameter template, dan file template yaml.	Oktober 28, 2024

Trusted Advisor cek ditambahkan ke Remediator Tepercaya di AMS	Trusted Advisor Pemeriksaan berikut sekarang tersedia di Trusted Remediator: • Z4 AUBRNSmz - Alamat IP Elastis yang Tidak Terkait • c18d2gz128 - Amazon ECR Repository Tanpa Kebijakan Siklus Hidup Dikonfigurasi • c18d2gz138 - Pemulihan DynamoDB Point-in-time • Hs4Ma3G323 - Dynamo harus mengaktifkan perlindungan penghapusan DBtables • Hs4Ma3G247 - Amazon EC2 Transit Gateway seharusnya tidak secara otomatis menerima permintaan lampiran VPC • Hs4Ma3G308 - Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan • Hs4Ma3G299 - Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan • Hs4Ma3G306 - Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik • Hs4Ma3G109 - CloudTrail validasi file log harus diaktifkan	Oktober 25, 2024

	• Hs4Ma3G217 - CodeBuild lingkungan proyek harus memiliki AWS Configura tion4 logging • Hs4Ma3G158 - Dokumen SSM seharusnya tidak bersifat publik • Hs4Ma3G319 - Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan	
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
Bagian baru ditambahkan ke Offboard dari AMS Accelerate	Petunjuk tentang cara melakukan offboard dengan dependensi Manajer Alarm dan Tagger Sumber Daya ditambahkan ke Offboard dari AMS Accelerate.	Oktober 24, 2024
Dasbor Resource Tagger sekarang tersedia.	Dasbor Resource Tagger sekarang tersedia dalam pelaporan layanan mandiri.	September 26, 2024
Anda sekarang dapat menyertakan beberapa alamat email dalam peringatan berbasis tag.	Beberapa alamat email sekarang didukung dalam peringatan berbasis tag.	September 20, 2024
Batas Akselerasi AMS sekarang disertakan dalam manajemen patch AMS.	Batas Akselerasi AMS disertakan dalam manajemen Patch - Buat jendela pemeliharaan tambalan.	Agustus 30, 2024

Pembaruan Penemuan Akun AMS Mempercepat	Bagian baru dalam Penemuan Akun telah ditambahkan untuk Evaluasi EC2 Instans Amazon.	Agustus 29, 2024
AMS Accelerate default patch baseline sekarang tersedia untuk sistem operasi Ubuntu.	AMS Accelerate default patch baseline sekarang tersedia untuk sistem operasi Ubuntu.	Agustus 22, 2024
Pembaruan Penemuan Akun AMS Mempercepat	Empat panggilan AWS API baru telah ditambahkan ke bagian AWS CloudTrail Evaluasi di tabel pemeriksaan operasional.	Agustus 2, 2024
Trusted Remediator sekarang mendukung pemeriksaan tambahan	Trusted Remediator sekarang mendukung pemeriksaan keamanan Hs4Ma3G19 2 - Instans RDS DB harus melarang akses publik.	Juli 30, 2024
AMS sekarang mendukung Amazon Route 53 Resolver DNS Firewall	AMS sekarang mendukung Amazon Route 53 Resolver DNS Firewall	Juli 30, 2024
AMS Accelerate onboardin g_role_minimal.zip sekarang berisi kode Terraform	AMS Accelerate onboardin g_role_minimal.zip sekarang berisi kode Terraform.	Juli 30, 2024
Dasbor Aturan Konfigurasi Keamanan	Dasbor Aturan Konfigurasi Keamanan sekarang tersedia dalam pelaporan Layanan Mandiri.	Juli 24, 2024
AMS Accelerate sekarang mendukung Oracle Linux 8.9, RHEL 8.10, dan RHEL 9.4.	AMS Accelerate sekarang mendukung Oracle Linux 8.9, RHEL 8.10, dan RHEL 9.4.	Juli 5, 2024

AMS Mempercepat proses penemuan akun diperbarui.	Proses penemuan akun yang digunakan saat orientasi Akun AWS ke AMS Accelerate diperbarui.	Juli 1, 2024
Remediator Tepercaya sekarang tersedia.	Trusted Remediator, solusi AWS Managed Services yang mengotomatiskan remediasi AWS Trusted Advisor pemeriksaan, kini tersedia.	Juni 24, 2024
Amazon Route 53 Resolver DNS firewall event di Security Incident Response.	AMS sekarang memantau peristiwa firewall DNS Amazon Route 53 Resolver di Respons Insiden Keamanan	Juni 21, 2024
Sistem operasi yang didukung diperbarui	AMS Accelerate sekarang mendukung AlmaLinux 8.3-8.9, 9.0-9.2 (AlmaLinux hanya didukung dengan arsitektur x86)	Juni 19, 2024
Batas profil instans otomatis sekarang meningkat jika default terpenuhi.	AMS sekarang meningkatkan batas profil instans default menjadi 20 jika batas default 10 tercapai.	Juni 18, 2024
Fitur instalasi otomatis Agen SSM AMS sekarang diaktifkan secara default.	Fitur instalasi otomatis Agen SSM AMS diaktifkan secara default untuk akun yang di-onboard setelah 6/03/2024.	Juni 7, 2024

FAQ Keamanan ditambahkan ke manajemen Keamanan.	FAQ Keamanan sekarang tersedia yang mencakup pertanyaan umum tentang praktik terbaik keamanan, kontrol, model akses, dan mekanisme audit yang digunakan saat insinyur operasi AMS atau otomatisasi mengakses akun Anda.	3 Juni 2024
AWS Wilayah Tambahan sekarang didukung oleh Pemantauan dan Manajemen Insiden untuk Amazon EKS.	Tiga AWS Wilayah tambahan sekarang didukung oleh Pemantauan dan Manajemen Insiden untuk Amazon EKS.	23 Mei 2024
Pemberitahuan patch permintaan layanan sekarang dikirim sebelum jendela Patch Maintenance.	AMS Accelerate patching membuat permintaan layanan baru 4 hari sebelum jendela Patch Maintenance. Anda dapat menggunakan permintaan layanan untuk berkomunikasi dengan AMS untuk penyesuaian tambalan atau untuk melewati tambalan.	3 Mei 2024
Ambang batas peringatan ditambahkan ke tabel peringatan dasar pemantauan AMS Accelerate EKS.	Ambang batas peringatan terperinci sekarang tersedia di tabel peringatan Baseline untuk pemantauan Amazon EKS.	3 Mei 2024
Diperbarui: Profil Konfigurasi Manajer Alarm.	Menambahkan catatan tentang membuat alarm Deteksi Anomali dengan Manajer Alarm.	April 25, 2024

Penambahan profil konfigurasi Resource Tagger.	Tabel DynamoDB dan bucket Amazon S3 sekarang tersedia di Resource Tagger	April 25, 2024
Menambahkan bagian informasi Manajemen Acara Terencana (PEM).	Informasi terperinci tentang penawaran layanan PEM sekarang tersedia di Panduan Pengguna Akselerasi AMS.	April 25, 2024
AMS mendukung Red Hat Enterpise Linux (RHEL) 9.x.	AMS mendukung Red Hat Enterprise Linux (RHEL) 9.x.	April 25, 2024
AMS Accelerate mendukung pelaporan untuk semua konfigurasi AWS Wilayah.	AMS Accelerate mendukung Pelaporan Inventaris SSM untuk semua konfigurasi AWS Wilayah.	April 25, 2024
Diperbarui: kebijakan AWS terkelola.	Memperbarui AWSManaged ServicesDeploymentToolkitPolicy dengan izin ECR baru.	April 4, 2024
Diperbarui: Bagian Profil Konfigurasi Tagger Sumber Daya	Ditambahkan `AWS::EFS::FileSystem` ke ResourceTypedaftar.	Maret 21, 2024
Diperbarui: Laporan insiden dan permintaan layanan di bagian Accelerate.	Mengubah judul topik menjadi Laporan insiden, permintaan layanan, dan pertanyaan penagihan di Accelerate. Menambahkan bagian baru, pertanyaan Penagihan.	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: Buat peran aws_managedservices_onboarding_role dengan bagian AWS CloudFormation	Menambahkan perintah untuk membuat peran dari AWS CloudShell.	Maret 21, 2024
Diperbarui: (Opsional) Template Mulai Cepat	Menambahkan perintah untuk mengunduh template dari AWS CloudShell.	Maret 21, 2024
Jenis sumber daya baru tersedia untuk profil konfigurasi Alarm Manager.	Menambahkan jenis sumber daya untuk Amazon FSx, Amazon EFS, dan Elasticsearch ke profil konfigurasi Alarm Manager.	Maret 21, 2024
Substitusi pseudoparameter tambahan tersedia untuk profil konfigurasi.	Menambahkan substitusi FSx pseudoparameter Amazon EFS dan Amazon.	Maret 21, 2024
Menambahkan bagian baru ke Fitur dalam topik Deskripsi Layanan.	Menambahkan bagian baru, Manajemen permintaan layanan di bawah fitur AMS Accelerate.	Maret 21, 2024
Kolom baru ditambahkan ke laporan layanan mandiri laporan Insiden Mingguan	Kolom baru ditambahkan ke laporan Insiden Mingguan sehingga Anda dapat memfilter insiden berdasarkan kuartal, bulan, minggu, atau hari kejadian itu dibuat atau diselesaikan.	Maret 11, 2024

Pembaruan lebih awal

Tabel berikut menjelaskan perubahan penting pada dokumentasi panduan Akselerasi AMS sebelum Maret 2024.

Ubah	Deskripsi	Tanggal
Perbaikan untuk AMS Accelerate CloudTrail trail onboarding	Perbaikan untuk AMS Accelerate CloudTrail trail onboarding: • Kumpulkan semua kebijakan bucket dalam satu blok • Hapus ID AWS Organisasi kedua dalam pernyataan kebijakan • Memperjelas persyaratan lingkungan pelanggan Untuk informasi selengkapnya, lihat Tinjau dan perbarui konfigurasi agar AMS Accelerate dapat menggunakan jejak Anda CloudTrail .	Februari 23, 2024
Diperbarui: Proses orientasi akun.	Merestrukturisasi bagian Proses orientasi Akun untuk membuat langkah-langkahnya lebih jelas. Juga meluncurkan template Mulai Cepat opsional untuk fitur orientasi. Lihat (Opsional) Template Mulai Cepat di Accelerate.	Februari 22, 2024
Diperbarui: Offboarding AMS Accelerate.	Memperbarui bagian pertimbangan offboardi ng AMS Accelerate untuk menunjukkan bahwa peran `ams-access-management` CloudFormation stack dan `ams-access-management` IAM tidak dihapus oleh proses offboarding. Lihat AMS Mempercepat efek offboarding.	Februari 22, 2024
Diperbarui: Kepatuhan konfigurasi di Accelerate.	Mengubah “Laporan Insiden” menjadi “Permintaan Layanan” jika berlaku untuk menghindari kebingungan pada persyaratan ini.	Februari 22, 2024

Ubah	Deskripsi	Tanggal
	Lihat Kepatuhan konfigurasi di Accelerate.	
Diperbarui: Penemuan akun di Accelerate.	Penemuan Akun yang direorganisasi di Accelerate untuk prasyarat grup yang lebih baik dengan bagian yang relevan. Lihat Langkah 1. Penemuan akun di Accelerate.	Februari 22, 2024
Berganti nama: AMS Patch melaporkan ke manajemen host AMS.	Mengganti nama pelaporan AMS Patch menjadi manajemen host AMS dan mengganti nama laporan, laporan Detail Patch, menjadi laporan Cakupan Agen SSM. Lihat Laporan manajemen host AMS.	Februari 22, 2024
Operasi yang Diperbarui pada Katalog Permintaan	Memperbarui katalog tabel penawaran Operations on Demand untuk menghapus referensi ke “kesehatan” di. `Amazon EKS cluster maintenance` Lihat Meminta Operasi AMS Sesuai Permintaan.	Februari 22, 2024
Router Acara AMS yang Diperbarui	Memperbarui bagian `AMSCoreRule` AMS Event Router. Lihat Menggunakan Aturan EventBridge Terkelola Amazon di AMS.	Februari 22, 2024
Sistem Operasi yang Didukung Diperbarui.	Memperbarui Sistem Operasi yang Didukung untuk menyertakan SUSE Linux Enterprise Server 15 SP5. Lihat Konfigurasi yang didukung.	Februari 22, 2024

Ubah	Deskripsi	Tanggal
Otomatisasi remediasi penggunaan EC2 volume yang diperbarui	Memperbarui bagian otomatisasi remdiasi penggunaan EC2 volume dengan jadwal ekspansi kapasitas yang benar. Lihat EC2 otomatisasi remediasi penggunaan volume.	Februari 22, 2024
Diperbarui: Tinjau dan perbarui konfigurasi Anda untuk mengaktifkan Accelerate menggunakan jejak Anda CloudTrail	Memperbarui bagian kebijakan bucket AMS Accelerate Organization CloudTrail S3. Lihat Tinjau dan perbarui konfigurasi agar AMS Accelerate dapat menggunakan jejak Anda CloudTrail	Februari 15, 2024
Ditambahkan fitur baru: Instalasi otomatis Agen SSM	Menambahkan bagian baru untuk instalasi auto SSM Agent Lihat Instalasi otomatis Agen SSM.	Januari 26, 2024
Diperbarui: Konfigurasi yang didukung	Menambahkan informasi mengenai versi yang didukung AWS Control Tower Lihat Konfigurasi yang didukung.	Januari 26, 2024
Diperbarui: Pelaporan AMS Patch.	Menghapus tiga bagian dari pelaporan AMS Patch: • Laporan Ringkasan Detail Instans Patch • Laporan Detail Patch • Contoh yang Dilaporkan Patch Tidak Terjawab Lihat Laporan manajemen host AMS.	22 Desember 2023

Ubah	Deskripsi	Tanggal
Diperbarui: Mempercepat prasyarat orientasi.	Memperbarui rencana dukungan yang diperlukan untuk mengaktifkan AMS Accelerate. Lihat Mempercepat prasyarat orientasi.	15 Desember 2023
Diperbarui: Buat jendela pemeliharaan patch.	Dihapus bagian siklus patch default karena fitur ini tidak digunakan lagi. Lihat Buat jendela pemeliharaan tambalan di AMS.	13 Desember 2023
Diperbarui: Pengaturan pemberitahuan di Accelerate.	Mengklarifikasi email apa yang digunakan untuk notifikasi. Untuk informasi selengkapnya, lihat Pengaturan notifikasi di Accelerate.	Desember 12, 2023
Diperbarui: `AMSAccelerateCustomerAccessPolicies` Template.	Diperbarui `AMSAccelerateCustomerAccessPolicies` template untuk memperbaiki kesalahan sintaks. Untuk informasi selengkapnya, lihat Izin untuk menggunakan fitur AMS.	Desember 12, 2023
Ditambahkan: Ubah ulasan keamanan permintaan	Menambahkan bagian baru Ubah ulasan keamanan permintaan di bawah Manajemen Keamanan. Untuk informasi selengkapnya, lihat Ubah ulasan keamanan permintaan.	Desember 11, 2023
Diperbarui: resource_inventory.xlsx	Memperbarui resource_inventory.xlsx untuk menyertakan peran Analis Keamanan. Untuk informasi selengkapnya, lihat Persediaan sumber daya untuk Accelerate.	17 November 2023

Ubah	Deskripsi	Tanggal
Diperbarui: deskripsi ams-access-admin-operations peran	ams-access-admin-operationsDeskripsi yang diperbarui. Lihat Mengapa dan kapan AMS mengakses akun Anda dan Mengautentikasi dengan identitas di AMS Accelerate untuk informasi lebih lanjut.	17 November 2023
Diperbarui: AMS Mempercepat pertimbangan offboarding	Bagian Keamanan yang Diperbarui untuk mengklarifikasi apa yang tersedia dari Amazon GuardDuty dan AWS Config aturan setelah offboarding. Untuk informasi selengkapnya, lihat AMS Mempercepat efek offboarding.	17 November 2023
Ditambahkan: Pemantauan dan Manajemen Insiden untuk Amazon EKS	Pemantauan dan Manajemen Insiden untuk Amazon EKS memantau sumber daya Amazon EKS Anda untuk kegagalan, penurunan kinerja, dan masalah keamanan. Untuk informasi selengkapnya, lihat Pemantauan dan manajemen insiden untuk Amazon EKS di AMS Accelerate.	14 November 2023
Diperbarui: Menandai	Menambahkan informasi tentang penandaan yang disediakan pelanggan. Untuk informasi selengkapnya, lihat Tag yang disediakan pelanggan di Accelerate.	7 November 2023

Ubah	Deskripsi	Tanggal
Diperbarui: Profil Konfigurasi Tagger Sumber Daya	Ditambahkan AWS::AutoScaling::AutoScaling Group, AWS::EKS::Cluster, AWS::Elasticsearch::Domain, and AWS::FSx::FileSystem ke bagian Filter. Untuk informasi selengkapnya, lihat Profil Konfigurasi Resource Tagger di AMS Accelerate.	Oktober 27, 2023
Diperbarui: Deskripsi Layanan	Menambahkan Ubuntu 22.04 ke Sistem Operasi yang Didukung. Lihat Deskripsi layanan	September 29, 2023
Diperbarui: AMS Mempercepat Prasyarat Orientasi	Menambahkan catatan ke titik akhir AMS Accelerate VPC untuk menyertakan template. CloudFormation Lihat Mempercepat prasyarat orientasi.	September 29, 2023
Diperbarui: Mendeteksi	Jenis perlindungan titik akhir yang dihapus dari respons keamanan AMS Accelerate. Lihat Mendeteksi.	September 29, 2023
Diperbarui: Peringatan dari Pemantauan Dasar di AMS	Ditambahkan AWS Outposts ke Alerts dari tabel Baseline Monitoring. Lihat Mendeteksi monitoring-default-metrics.	September 29, 2023
Diperbarui: Buat peran aws_managedservices_onboarding_role dengan AWS CloudFormation	Tangkapan layar yang diperbarui untuk Tentukan Detail Tumpukan. Lihat Buat `aws_managedservices_onboarding_role` dengan AWS CloudFormation untuk Mempercepat.	September 29, 2023

Ubah	Deskripsi	Tanggal
Diperbarui: Aturan EventBridge Terkelola Amazon yang diterapkan oleh AMS Accelerate	Menambahkan AMS baru Mempercepat Aturan AMSCoreAturan EventBridge Terkelola Amazon. AMS Memperbarui Aturan EventBridge Terkelola Amazon AMSAccessRolesRuleuntuk menambahkan peran baru. Untuk informasi selengkapnya, lihat Aturan EventBridge Terkelola Amazon yang diterapkan oleh AMS .	September 19, 2023
Diperbarui: Profil Konfigurasi Manajer Alarm	Menambahkan pengidentifikasi substitusi pseudoparameter AWS Outposts. Lihat Pemantauan dan manajemen acara di AMS Accelerate.	11 September 2023
Diperbarui: Profil Konfigurasi Tagger Sumber Daya	Menambahkan jenis sumber daya AWS Outposts. Lihat Mempercepat profil Konfigurasi: substitusi pseudoparameter.	11 September 2023
Diperbarui: Layanan yang didukung	Menambahkan Amazon Elastic File System ke bagian Layanan yang dipantau oleh CloudWatch alarm. Untuk informasi selengkapnya, lihat Deskripsi layanan.	September 6, 2023

Ubah	Deskripsi	Tanggal
Diperbarui: Pemantauan patch dan remediasi kegagalan	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” Untuk informasi selengkapnya, lihat Memahami manajemen tambalan di AMS Accelerate.	September 6, 2023
Diperbarui: Tanggapan Klarifikasi terhadap runbook peristiwa malware	Tanggapan Klarifikasi terhadap runbook peristiwa malware untuk respons Insiden Keamanan. Untuk informasi selengkapnya, lihat Respon Insiden Keamanan di AMS .	September 6, 2023
Diperbarui: Menghubungkan akun Accelerate Anda dengan Transit Gateway	Langkah-langkah yang diklarifikasi untuk Menghubungkan VPC Accelerate account baru ke jaringan AMS Multi-Account Landing Zone (membuat lampiran VPC TGW): Lihat Menghubungkan Accelerate account withTransit Gateway untuk informasi selengkapnya.	5 September 2023
Diperbarui: Peringatan dari pemantauan dasar di AMS	Referensi dihapus ke dua alarm usang dan. AMSRead LatencyAlarm AMSWrite LatencyAlarm Untuk informasi selengkapnya, lihat Peringatan dari pemantauan dasar di AMS.	5 September 2023
Ditambahkan: AMS Event Router	Dokumentasi tambahan untuk Router Acara AMS Lihat Menggunakan Aturan EventBridge Terkelola Amazon di AMS untuk informasi selengkapnya.	5 September 2023

Ubah	Deskripsi	Tanggal
Diperbarui: Daftar pseudoparameter Manajer Alarm.	Memperbarui daftar pseudoparameter Manajer Alarm. EC2 parameter nama instance ditambahkan ke konfigurasi alarm EC2 instance dan EC2 disk. Untuk informasi selengkapnya, lihat Mempercepat profil Konfigurasi: substitusi pseudoparameter.	29 Agustus 2023
Ditambahkan: AMS Access Offboarding	Menambahkan pertimbangan saat offboarding AMS Access. Lihat AMS Mempercepat efek offboarding.	24 Agustus 2023
Ditambahkan: Respon Insiden Keamanan AMS	Menambahkan dokumentasi untuk menggunakan AMS Security Incident Response. Lihat Respon Insiden Keamanan di AMS .	18 Agustus 2023
Diperbarui: AMS Mempercepat peran akses	Memperbaiki kesalahan ketik pada nama peran. Lihat AWS Identity and Access Management di AMS Accelerate.	10 Agustus 2023
Diperbarui: Pernyataan kebijakan	Mengganti nama peran hardcode dengan wildcard. Lihat Tinjau dan perbarui konfigurasi agar AMS Accelerate dapat menggunakan jejak Anda CloudTrail .	10 Agustus 2023
Diperbarui: Daftar layanan yang dipantau dengan peringatan EFS.	Memperbarui daftar layanan pemantauan dengan peringatan EFS baru untuk pemantauan dasar AMS. 4 jenis peringatan EFS baru ditambahkan. Untuk informasi selengkapnya, lihat Peringatan dari pemantauan dasar di AMS.	Agustus 03, 2023
Diperbarui: Mempercepat tabel inventaris sumber daya	Dihapus ams-backup-config-rule -stack dan sumber daya terkait. Lihat Persediaan sumber daya untuk Accelerate.	Juli 18, 2023

Ubah	Deskripsi	Tanggal
Diperbarui: AMS Mempercepat peran akses	<8-digit hash>Dihapus peran ams-backup-config-rule -st- amsBackupAlert ConfigRule -<8-digit hash>dan ams-backup-config-rule -st- amsBackupPlan ConfigRule H-. Lihat AWS Identity and Access Management di AMS Accelerate.	Juli 18, 2023
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. Untuk informasi selengkapnya, lihat Peringatan dari pemantauan dasar di AMS.	19 Juni 2023
Baru: AMS Mempercepat peran akses	Menambahkan peran akses baru untuk AMS Security.	Juni 16, 2023
Baru: AMS Mempercepat manajemen CloudTrail log sekarang dapat menggunakan CloudTrail jejak pelanggan.	Diperbarui Mempercepat opsi yang didukung untuk manajemen CloudTrail log, termasuk Mempercepat jejak yang diterapkan atau integrasi dengan CloudTrail akun terkelola pelanggan atau jejak Organisasi. Untuk informasi selengkapnya, lihat Tinjau dan perbarui konfigurasi agar AMS Accelerate dapat menggunakan jejak Anda CloudTrail .	09 Juni 2023
Diperbarui: Laporan Konfigurasi Respons Aturan Konfigurasi AMS Mempercepat Konfigurasi Config.	Memperbarui pelaporan berdasarkan permintaan untuk Laporan Konfigurasi Respons Aturan Konfigurasi AWS Config. Lihat Mempercepat pembaruan untuk pelaporan berdasarkan permintaan. Lihat Laporan Konfigurasi Respons Aturan Konfigurasi AMS Config.	26 Mei 2023
Diperbarui: Kebijakan Tanggal Mulai Penagihan Layanan.	Definisi yang diperbarui dari Tanggal Mulai Penagihan diIstilah kunci AMS.	15 Mei 2023

Ubah	Deskripsi	Tanggal
Diperbarui: kebijakan AWS terkelola.	Memperbarui AWSManaged ServicesDeploymentToolkitPolicy dengan izin CFN dan ECR baru, dan mencakup tindakan yang ada dengan wildcard. Lihat Mempercepat pembaruan ke peran terkait layanan. Lihat Mempercepat pembaruan ke peran terkait layanan.	09 Mei 2023
Diperbarui: Akses tautan kebijakan peran.	Peran akses sekarang dapat diunduh langsung dari lokasi bucket Accelerate S3. Lihat Mengapa dan kapan AMS mengakses akun Anda dan AWS Identity and Access Management di AMS Accelerate.	
Diperbarui: Laporan Layanan Mandiri Penagihan Bulanan.	Catatan tambahan: Laporan Penagihan Bulanan hanya tersedia di akun Management Payer (AMS Advanced multi-account landing zone), tetapi tersedia untuk semua akun terkelola AMS Accelerate yang ditautkan. Lihat Laporan penagihan (bulanan).	13 April 2023
Diperbarui: Daftar Peringatan.	CloudTrail Referensi yang dihapus. Lihat Manajemen log di AMS Accelerate.	13 April 2023
Diperbarui: Daftar Peringatan.	Menambahkan tiga peringatan agen SSM baru. Lihat Peringatan dari pemantauan dasar di AMS.	13 April 2023
Diperbarui: Mempercepat Prasyarat.	Mengklarifikasi bahwa Accelerate memerlukan salah satu dari empat paket AWS Support tersedia dan tidak termasuk paket Developer. Lihat Mempercepat prasyarat orientasi.	13 April 2023

Ubah	Deskripsi	Tanggal
Diperbarui: Mempercepat kebijakan peran terkait layanan.	File zip kebijakan Layanan Kontak telah diperbarui. Lihat AWS kebijakan terkelola untuk AMS Accelerate.	13 April 2023
Diperbarui: Penjadwal Sumber Daya AMS.	Nama peran salah, AWSManagedServices-DescribeScheduleOrPeriod, dikoreksi ke AWSManagedServices-DescribeScheduleOrPeriods. Lihat Optimalisasi biaya dengan Penjadwal Sumber Daya AMS.	13 April 2023
Diperbarui: kebijakan AWS terkelola.	Diperbarui Tanggapan temuan yang disesuaikan dengan instruksi untuk memperbarui tanggapan khusus dalam satu atau beberapa akun.	13 April 2023
Diperbarui: Resource Tagger	Menambahkan peringatan tentang “menentukan nama untuk konfigurasi baru Anda (SampleConfigurationBlock dalam contoh yang disediakan) karena Anda mungkin secara tidak sengaja mengganti konfigurasi yang dikelola AMS dengan nama yang sama”. Lihat Kasus penggunaan Resource Tagger di AMS Accelerate.	16 Maret 2023
Diperbarui: Patch RACI	Beberapa pembaruan dan klarfikasi pada RACI untuk ditambal. Lihat Deskripsi layanan.	16 Maret 2023
Diperbarui: Tindakan dalam penerapan toolkit SLR JSON	Kebijakan dan tindakan yang diperbarui. Lihat:Menggunakan peran terkait layanan untuk AMS Accelerate.	16 Maret 2023
Diperbarui: Remediasi otomatis	Dihapus dukungan LVM untuk otomatisasi EC2 volume. Lihat:Remediasi peringatan otomatis AMS.	16 Maret 2023

Ubah	Deskripsi	Tanggal
Diperbarui: Mempercepat Orientasi.	Penggunaan peran yang diklarifikasi, terutama peran minimal. Template untuk membuat peran AMS	16 Maret 2023
Diperbarui: Pelaporan swalayan.	Laporan cadangan harian sekarang mendukung wilayah primer dan sekunder. Keduanya dilaporkan di bidang Resource RegionLaporan Backup (harian).	16 Maret 2023
Diperbarui: Panduan menambal	Menambahkan peringatan untuk tidak menyesuaikan baseline patching default, yang dikelola oleh AMS. Sebagai gantinya, buat baseline patch kustom baru. Lihat: Garis dasar tambalan default danGaris dasar patch khusus dengan AMS Accelerate.	16 Maret 2023
Kebijakan Penghentian Layanan yang Diperbarui.	Definisi Pemutusan Layanan dan Tanggal Penghentian Layanan yang diperbarui diIstilah kunci AMS. Catatan penghentian harus dikeluarkan pada hari ke-20 bulan sebelum bulan penuh terakhir Anda.	16 Maret 2023
Diperbarui: kebijakan AWS terkelola.	Nama kebijakan yang diklarifikasi:Menghubungi peran terkait layanan untuk AMS Accelerate.	Feb 16, 2023
Baru: kebijakan AWS terkelola .	Ditambahkan kebijakan:Menghubungi peran terkait layanan untuk AMS Accelerate.	Feb 16, 2023
Diperbarui: Kepatuhan konfigurasi.	Memperbaiki kata yang salah eja di:. Kepatuhan konfigurasi di Accelerate	Feb 16, 2023
Konten Baru: Tidak Didukung OSes	Menambahkan informasi tentang layanan apa yang disediakan AMS untuk sistem operasi yang tidak didukung (OSes), lihatKemampuan untuk sistem operasi yang tidak didukung di Accelerate.	Feb 16, 2023

Ubah	Deskripsi	Tanggal
Diperbarui: Buat jendela patch	Menambahkan tautan untuk digunakan CloudShell keBuat jendela pemeliharaan dengan antarmuka baris perintah Systems Manager (CLI) untuk AMS Accelerate.	Feb 16, 2023
Konten yang Diperbarui: Sumber daya manajemen orientasi	Memperbarui template JSON zip di. Template untuk membuat peran AMS	Feb 16, 2023
Konten Baru: Kepatuhan Konfigurasi	Menambahkan topik baru:Tanggapan temuan yang disesuaikan.	Feb 16, 2023
Baru: kebijakan AWS terkelola .	Ditambahkan kebijakan:Peran terkait layanan EventBridge aturan Amazon untuk AMS Accelerate.	07 Feb 2023
Diperbarui: kebijakan AWS terkelola.	Memperbarui `AWSManagedServices DeploymentToolkitPolicy` dengan izin S3 baru. Lihat Mempercepat pembaruan ke peran terkait layanan.	30 Jan 2023
Wilayah keikutsertaan baru: CPT.	AMS Accelerate sekarang tersedia di wilayah opt-in Capetown (CPT). Untuk ikut serta, lihat Mengelola Wilayah AWS.	12 Jan 2023
Diperbarui: Deskripsi Layanan.	Menambahkan FSx layanan yang dipantau oleh CloudWatch alarm ke. Deskripsi layanan	12 Jan 2023
Diperbarui: Memantau metrik default.	Menambahkan 6 FSx alarm kePeringatan dari pemantauan dasar di AMS.	12 Jan 2023
Diperbarui: pola AMS.	Ditambahkan Kustomisasi Pemberitahuan Alarm Cloudwatch ke. Pola AMS	12 Jan 2023

Ubah	Deskripsi	Tanggal
Diperbarui: Sumber daya manajemen orientasi.	Memperbarui tabel template, menambahkan baris untuk `ams-onboarding-ssm-execution-role` in Template untuk membuat peran AMS.	12 Jan 2023
Diperbarui: Kepatuhan konfigurasi.	Detail tambahan untuk meminta perbaikan khusus (di kotak Penting) di. Kepatuhan konfigurasi di Accelerate	12 Jan 2023
Diperbarui: Service-linked-role izin.	Menghapus izin lama atau duplikat. Lihat Menggunakan peran terkait layanan untuk AMS Accelerate.	15 Des 2022
Diperbarui: Manajemen patch, jendela pemeliharaan.	Menambahkan panduan ke instruksi konsol, langkah 5, untuk membuat jendela pemeliharaan. Lihat Membuat jendela pemeliharaan dari konsol Systems Manager untuk AMS Accelerate.	15 Des 2022
Baru: Bagian manajemen patch.	Menambahkan bagian untuk jendela pemeliharaan Patch Tuesday. Lihat Buat jendela pemeliharaan “Patch Tuesday” berulang dari konsol AMS (disarankan).	15 Des 2022
Diperbarui: Penjadwal Sumber Daya AMS.	Memperbarui nama AWS CloudFormation tumpukan. Lihat Menggunakan sumber daya dengan Penjadwal Sumber Daya AMS.	15 Des 2022
Diperbarui: Tandai sumber daya Anda untuk cadangan.	Menambahkan panduan untuk menggunakan AMS Resource Tagger. Lihat Tandai sumber daya Anda untuk menerapkan paket cadangan AMS.	15 Des 2022
Diperbarui: Pilih paket cadangan.	Diindikasikan paket mana yang menawarkan pencadangan berkelanjutan. Lihat Pilih paket cadangan AMS.	15 Des 2022

Ubah	Deskripsi	Tanggal
Diperbarui: Penjadwal Sumber Daya AMS.	Memperbarui contoh AWS CLI untuk menghapus periode atau jadwal. Lihat Bekerja dengan periode dan jadwal di AWS Managed Services Resource Scheduler.	15 Des 2022
Diperbarui: kebijakan AWS terkelola.	Ditambahkan`AWSManagedServices DeploymentToolkitPolicy` . Lihat AWS kebijakan terkelola untuk AMS Accelerate.	15 Des 2022
Baru: Menambahkan bagian yang menjelaskan peran terkait layanan baru AMS,. AWSServiceRoleForManagedServices_DetectiveControlsConfig	Menambahkan GovCloud wilayah dan izin. Lihat Detektif mengontrol peran terkait layanan untuk AMS Accelerate.	15 Des 2022
Kebijakan baru: AWS-managed	Bagian tambahan yang menjelaskan cara kebijakan AWS-managed, AWSManagedServices_AlarmManagerPermissionsBoundary, digunakan dalam kebijakan peran terkait layanan, AWSManagedServices_AlarmManager _ServiceRolePolicy, untuk membatasi izin peran IAM yang dibuat oleh peran terkait layanan. AWSServiceRoleForManagedServices_AlarmManager Lihat AWS kebijakan terkelola untuk AMS Accelerate.	15 Des 2022
Diperbarui: Operasi sesuai Permintaan.	Penawaran tambahan: SQL Server pada Operasi EC2 dan AMI Building and Vending. Lihat Operasi Sesuai Permintaan.	November 10, 2022
Diperbarui: Pemantauan dan manajemen acara.	Penjelasan terbaru tentang pemberitahuan layanan dan laporan insiden. Lihat Cara kerja pemantauan.	November 10, 2022

Ubah	Deskripsi	Tanggal
Diperbarui: Wilayah peran terkait layanan	Menambahkan GovCloud wilayah dan izin. Lihat Menggunakan peran terkait layanan untuk AMS Accelerate.	November 10, 2022
Baru: Peran terkait layanan.	Menambahkan peran baru:`AWSServiceRoleForAMSDetectiveControls` . Lihat Detektif mengontrol peran terkait layanan untuk AMS Accelerate.	November 10, 2022
Diperbarui: Manajemen akses.	Subbagian yang diperbarui dengan instruksi yang ditingkatkan. Lihat Manajemen akses di AMS Accelerate.	November 10, 2022
Diperbarui: Deskripsi layanan.	Pola AMS yang diperbarui dalam matriks RACI. Lihat Deskripsi layanan.	Nov 10, 2022
Diperbarui: pola AMS.	Pelanggan bertanggung jawab atas penerapan pola. Lihat Pola AMS.	Nov 10, 2022
Diperbarui: Offboarding.	Menambahkan rincian tentang apa yang terjadi pada sumber daya Backup dan Monitoring tertentu selama offboarding. Lihat Offboard dari AMS Accelerate.	Nov 10, 2022
Diperbarui: Manajemen patch..	Panduan yang diperbarui dan dipersingkat mengenai kebijakan IAM. Lihat Membuat peran IAM untuk patching sesuai permintaan AMS Accelerate.	Nov 10, 2022
Baru: tautan ke diagram arsitektur.	Menambahkan tautan ke Diagram Arsitektur Referensi AMS ke berbagai topik. Sebagai contoh, lihat Pemantauan dan manajemen acara di AMS Accelerate.	Nov 10, 2022
Baru: Penawaran Operasi sesuai Permintaan	Menambahkan “Operasi Akselerator Zona Pendaratan”. Lihat Operasi Sesuai Permintaan.	Okt 13, 2022

Ubah	Deskripsi	Tanggal
Pembaruan: Manajemen pemantauan. Peringatan menghasilkan laporan insiden, bukan permintaan layanan	Cara kerja pemantauan.	Okt 13, 2022
Baru: Membuat jendela pemeliharaan patch dengan template CFN Accelerate-custom	AWS CloudFormation templat konfigurasi jendela tambalan. Lihat Buat jendela pemeliharaan tambalan di AMS.	September 15, 2022
Diperbarui: Offboarding	Ditekankan bahwa rencana cadangan di Accelerate tidak lagi berfungsi setelah offboarding. Lihat Offboard dari AMS Accelerate.	September 15, 2022
Diperbarui: rincian perubahan CloudWatch konfigurasi	Memperbaiki kesalahan dalam contoh Windows dan Linux. Lihat CloudWatch detail perubahan konfigurasi.	September 15, 2022
Diperbarui: Menggunakan Penjadwal Sumber Daya AMS	Menambahkan panduan tentang Tag Alokasi Biaya. Lihat Penaksir biaya di Penjadwal Sumber Daya AMS.	15 September 2022
Diperbarui: Perpustakaan Aturan AMS Config	Menambahkan dua aturan `ams-eks-` konfigurasi ke Tabel Aturan. Lihat Pustaka Aturan Konfigurasi AMS.	15 September 2022
Diperbarui: Manajemen Backup	Menghapus label PITR (point-in-time-recovery) yang menyesatkan dari judul dan deskripsi rencana cadangan. Lihat Pilih paket cadangan AMS.	15 September 2022
Diperbarui: Mempercepat Deskripsi Layanan	Deskripsi aturan konfigurasi dan kenari yang diperbarui. Lihat Deskripsi layanan.	15 September 2022

Ubah	Deskripsi	Tanggal
Diperbarui: Deskripsi Layanan, Konfigurasi yang Didukung	end-of-serviceTanggal dihapus untuk Windows 2008 R2. Accelerate tidak mendukung Windows 2008. Lihat Konfigurasi yang didukung.	Agustus 11, 2022
Diperbarui: Deskripsi Layanan, Peran dan Tanggung Jawab	Memperbarui tabel RACI. Log akses ELB dihapus dari baris terakhir bagian Jaringan. Kami tidak mengaktifkan log akses ELB untuk pelanggan Accelerate. Lihat Peran dan tanggung jawab.	Agustus 11, 2022
Diperbarui: Kepatuhan Konfigurasi	Memperbaiki kesalahan ketik di kolom Tabel Aturan, Kerangka Kerja. NIST-CSF salah terdaftar sebagai NIST-CIS. Lihat Kepatuhan konfigurasi di Accelerate.	Agustus 11, 2022
Baru: Mempercepat Offboarding	Pertimbangan dan proses untuk offboarding. Lihat Akselerasi AMS Offboarding.	Agustus 11, 2022
Diperbarui: Daftar sistem operasi agen SSM pra-instal	Menambahkan “Ubuntu Linux 18.04 dan 20.04" ke daftar. Lihat EC2 Instans orientasi untuk Mempercepat.	Agustus 11, 2022
Baru: Resource Scheduler	Gunakan Penjadwal Sumber Daya AMS untuk mengoptimalkan biaya dengan menghentikan dan memulai sumber daya hanya jika diperlukan. Lihat Optimalisasi biaya dengan Penjadwal Sumber Daya AMS.	14 Juli 2022
Diperbarui: Deskripsi Layanan untuk Resource Scheduler	Beberapa bagian dari deskripsi layanan diperbarui untuk penawaran Resource Scheduler baru. Lihat Deskripsi layanan.	14 Juli 2022

Ubah	Deskripsi	Tanggal
Baru: Pola AMS	AMS menawarkan template pola, solusi umum yang memecahkan keluarga kasus penggunaan di lingkungan terkelola AMS. Pola pertama yang ditawarkan:Pola AMS.	14 Juli 2022
Baru: Catatan pengoptimalan biaya	Menambahkan catatan yang menjelaskan bagaimana biaya dapat meningkat dengan penggunaan sumber daya. Lihat Persediaan sumber daya untuk Accelerate.	14 Juli 2022
Diperbarui: Aturan AMS Config	Menata ulang tabel di. Pustaka Aturan Konfigurasi AMS Tabel HTML memiliki lebih sedikit kolom, untuk membuatnya lebih mudah dibaca sekilas. Spreadsheet yang dapat diunduh memiliki kolom tambahan untuk memungkinkan penyortiran dan pemfilteran.	14 Juli 2022
Diperbarui: Manajemen Akses	Diperbarui CloudFormation template sampel diIzin untuk menggunakan fitur AMS. `AMSAccelerateAdminAccess` Kebijakan sekarang mencakup `AmsResourceSchedulerPassRolePolicy` dan `IAMReadOnlyPolicy` kebijakan.	14 Juli 2022
Diperbarui: Pelaporan Layanan Mandiri	Menambahkan instruksi untuk mengenkripsi AWS Glue metadata dengan kunci KMS. Lihat kotak berlabel Penting diLaporan layanan mandiri.	14 Juli 2022
Diperbarui: Pemantauan dasar AMS	Menambahkan peringatan DeleteRecoveryPoint cadangan. Peringatan dari pemantauan dasar di AMS	14 Juli 2022
Diperbarui: Sistem operasi yang didukung	Ditambahkan Tanggal Akhir Dukungan untuk Amazon Linux 2. Deskripsi layanan	14 Juli 2022

Ubah	Deskripsi	Tanggal
Diperbarui: Pelaporan AMS	Menambahkan catatan tentang Opt-in Regions. Laporan dan opsi	14 Juli 2022
Penjadwal Sumber Daya	Menambahkan informasi tentang orientasi dan menggunakan Penjadwal Sumber Daya AMS untuk membantu pengoptimalan biaya dengan menjadwalkan waktu berhenti dan mulai sumber daya. Juga, memperbarui deskripsi layanan Accelerate untuk menyertakan penyebutan Resource Scheduler. Selain itu, memperbarui tanggal dukungan akhir dukungan Amazon Linux 2 hingga 2024. Lihat Optimalisasi biaya dengan Penjadwal Sumber Daya AMS dan Deskripsi layanan	30 Juni 2022
Alarm baru	Menambahkan AWS Backup alarm. Peringatan dari pemantauan dasar di AMS	21 Juni 2022
Konten baru	Menambahkan konten peran terkait layanan. Menggunakan peran terkait layanan untuk AMS Accelerate	16 Juni 2022
	AWS Operasi Firewall Jaringan ditambahkan ke katalog penawaran Operations on Demand (OOD). Operasi Sesuai Permintaan	16 Juni 2022
	Menambahkan deskripsi fitur manajemen masalah. Deskripsi layanan	16 Juni 2022
	Menambahkan catatan tentang kumpulan aturan konfigurasi yang tidak mendukung di wilayah keikutsertaan tertentu. Kepatuhan konfigurasi di Accelerate	16 Juni 2022

Ubah	Deskripsi	Tanggal
Konten diperbarui	Kepatuhan konfigurasi. “Perpustakaan Aturan Konfigurasi AMS” -> “Tabel aturan”, diperbarui dan dihapus hanya ke ZIP. Kepatuhan konfigurasi di Accelerate	16 Juni 2022
	Email eskalasi yang dihapus. Jalur eskalasi	16 Juni 2022
	Memindahkan daftar topik ke paragraf pembuka di bawah. Apa itu AMS Accelerate?	16 Juni 2022
	Memperbarui konten auto remeditasi. Remediasi peringatan otomatis AMS	16 Juni 2022
Konten yang diperbarui: Deskripsi Layanan	Menambahkan EKS ke daftar layanan yang dipantau oleh Aturan Konfigurasi AMS di. Layanan yang didukung Deskripsi pemantauan yang diperbarui dalam tabel RACI diPeran dan tanggung jawab.	12 Mei 2022
Konten yang diperbarui: Kepatuhan Konfigurasi	Menambahkan aturan konfigurasi terkait EKS. Lihat Kepatuhan konfigurasi di Accelerate.	12 Mei 2022
Konten yang diperbarui: Memulai, Penemuan Akun	Menambahkan versi AwsAccountDiscoveryCli skrip yang lebih baru (dalam file zip Account Discovery Changelog) di. Langkah 1. Penemuan akun di Accelerate	12 Mei 2022
Konten yang diperbarui: Pemantauan, metrik default	Kondisi pemicu yang diperbarui untuk metrik terkait ALB. Lihat Peringatan dari pemantauan dasar di AMS.	12 Mei 2022
Konten yang diperbarui: Patching onboarding	Menambahkan prasyarat penambalan eksplisit: Anda harus ikut serta ke EBS. Lihat Penambalan orientasi di Accelerate.	12 Mei 2022

Ubah	Deskripsi	Tanggal
Konten yang diperbarui: Mempercepat tabel inventaris sumber daya	Mengubah aturan ams-detective-controls-config -rules-cdk, menambahkan aturan untuk -cdk dan -cdk. ams-detective-controls-recorder ams-detective-controls-infrastructure Lihat Persediaan sumber daya untuk Accelerate.	April 14, 2022
Konten yang diperbarui: Kepatuhan Konfigurasi	Pengantar standar industri, aturan konfigurasi, dan jenis tanggapan. Menekankan bahwa pelanggan tidak memilih aturan atau tanggapan konfigurasi individu. Kepatuhan konfigurasi di Accelerate.	April 14, 2022
Konten yang diperbarui: Deskripsi Layanan	Memindahkan bagian Lingkup Perubahan yang ada di bawah Peran dan Tanggung Jawab. Lihat Peran dan tanggung jawab.	April 14, 2022
Konten yang diperbarui: Tagging dan Monitoring	Ditambahkan `AWS::Synthetics:Canary` ke daftar Jenis Sumber Daya yang diizinkan untuk penandaan dan pemantauan. Lihat Profil Konfigurasi Resource Tagger di AMS Accelerate dan Mempercepat profil Konfigurasi: substitusi pseudoparameter.	April 14, 2022
Konten yang diperbarui: Mempercepat Prasyarat	Menambahkan izin bucket yang diperlukan SSM ke. Amazon EC2 Systems Manager di Accelerate	April 14, 2022
Konten baru: Patching dan Monitoring	Menambahkan kode sampel untuk menggunakan Cloudformation untuk menerapkan konfigurasi penandaan dan pemantauan. Lihat Menerapkan profil konfigurasi dengan AWS CloudFormation untuk Accelerate dan Menggunakan AWS CloudFormation untuk menerapkan Mempercepat perubahan konfigurasi.	10 Maret 2022

Ubah	Deskripsi	Tanggal
Konten yang diperbarui: Konsol pemeliharaan Patch	Langkah yang disusun ulang Membuat jendela pemeliharaan dari konsol Systems Manager untuk AMS Accelerate agar sesuai dengan antarmuka konsol.	10 Maret 2022
Konten yang diperbarui: CLI pemeliharaan Patch	Parameter CLI yang diperbarui (jadwal, durasi, dan batas) untuk Buat jendela pemeliharaan dengan antarmuka baris perintah Systems Manager (CLI) untuk AMS Accelerate	10 Maret 2022
Konten baru: Auto Instance Config	Ditambahkan definisi `AMSInstanceProfile BasePolicy` untuk Izin IAM mengubah detail	10 Maret 2022
Konten baru: Orientasi	Menambahkan contoh perintah Linux ke Konektivitas internet outbound di Accelerate	10 Maret 2022
Konten baru: Orientasi	Menambahkan opsi hak istimewa paling sedikit ke. Template untuk membuat peran AMS	10 Maret 2022
Konten yang diperbarui: Mempercepat instruksi eskalasi	Menambahkan panduan, tautan, dan kontak email ke Jalur eskalasi	10 Maret 2022
Konten yang diperbarui: Konfigurasi yang Didukung	AMS berharap untuk mengakhiri dukungan untuk RHEL 6 dan CentOs pada 14 Maret 2023. Lihat Konfigurasi yang didukung	10 Maret 2022
Konten yang diperbarui: Tabel sumber daya	Menambahkan AMS mengakses peran IAM ke tabel Persediaan sumber daya untuk Accelerate sumber daya	10 Maret 2022
Konten yang diperbarui: Onboarding dan Backup	Menambahkan instruksi AWS Backup untuk Orientasi AWS Backup di Accelerate memilih dan Manajemen kontinuitas di AMS Accelerate	10 Maret 2022

Ubah	Deskripsi	Tanggal
Konten yang diperbarui: Manajemen Akses	Menghapus Instruksi khusus lanjutan dari panduan Accelerate. Bagaimana dan kapan menggunakan akun pengguna root di AMS	10 Maret 2022
Konten yang diperbarui: Konfigurasi yang Didukung	AMS sekarang mendukung Oracle Linux 8.3 dan Ubuntu 18.04 dan 20.04. Lihat Konfigurasi yang didukung.	28 Februari 2022
Konten yang diperbarui: Perjanjian Tingkat Layanan	Memperbarui Perjanjian Tingkat Layanan yang dapat diunduh diLayanan yang didukung.	28 Februari 2022
Konten yang diperbarui: Manajemen Akses	Diperbarui Bagaimana AMS mengakses akun Anda dengan FAQs untuk peran konsol operator AMS dan peringatan untuk tidak memodifikasi atau menghapusnya.	28 Februari 2022
Konten yang diperbarui: Manajer Alarm	DiperbaruiMempercepat profil Konfigurasi: pemantauan. Manajer Alarm tidak lagi terbatas pada alarm metrik tunggal.	28 Februari 2022
Konten yang diperbarui: Memulai	DiperbaruiLangkah 2. Sumber daya manajemen orientasi di Accelerate. Menambahkan peran IAM dengan akses minimal untuk sumber daya orientasi.	28 Februari 2022
Konten baru: Lingkup Perubahan Deskripsi Layanan	Menambahkan bagian baru, Lingkup perubahan yang dilakukan oleh AMS Accelerate yang menekankan batasan dan tindakan yang tidak dilakukan AMS Accelerate.	Februari 10, 2022
Konten yang diperbarui: Memulai	Proses orientasi baru dimulai dengan menyiapkan fitur dan konfigurasi default sebelum menyesuaikan. Subbagian berisi tujuan khusus fitur dan tautan terkait. Lihat Memulai dengan AMS Accelerate.	Februari 10, 2022

Ubah	Deskripsi	Tanggal
Konten yang diperbarui: Manajemen Cadangan AMS.	Mempersingkat dan mengatur ulang Manajemen kontinuitas di AMS Accelerate chapter untuk keterbacaan.	Februari 10, 2022
Konten yang diperbarui: Menandai	Menambahkan bagian Alat Penandaan untuk mengakomodasi sampel kode untuk CloudFormation dan alat lainnya. Lihat Menandai AMS Accelerate.	Februari 10, 2022
Konten yang diperbarui: Baseline Monitoring	Kondisi pemicu yang ditingkatkan untuk alarm RedShift cluster mengurangi alarm palsu selama perawatan. Lihat Peringatan dari pemantauan dasar di AMS.	Februari 10, 2022
Konten yang diperbarui: Patching	Diperbarui perintah CLI sampel untuk mendaftarkan jendela pemeliharaan. Lihat Buat jendela pemeliharaan dengan antarmuka baris perintah Systems Manager (CLI) untuk AMS Accelerate.	Februari 10, 2022
Konten yang diperbarui: AWS Inventaris Aturan Config.	Menghapus aturan konfigurasi usang dari tabel Inventaris `ams-nist-cis-ec2-security-group-attached-to-eni` Aturan Konfigurasi AWS . Lihat Tabel Aturan.	27 Januari 2022
Konten baru: Membuat jendela pemeliharaan patch.	Menambahkan tautan ke tutorial SSM dan contoh perintah untuk membuat jendela pemeliharaan patch dari baris perintah. Lihat Buat jendela pemeliharaan dengan antarmuka baris perintah Systems Manager (CLI) untuk AMS Accelerate.	27 Januari 2022
Konten baru: Resource Tagger mengenali jenis sumber daya Auto Scaling Groups (ASG) baru.	Menambahkan Grup Auto Scaling ke jenis sumber daya yang dapat difilter dengan profil konfigurasi Resource Tagger. Lihat Sintaks dan struktur.	Januari 13, 2022

Ubah	Deskripsi	Tanggal
Konten baru: Paket cadangan tambahan dan brankas.	Menambahkan rencana cadangan dan brankas baru untuk mengurangi skenario berisiko tinggi termasuk serangan ransomware. Lihat Lihat cadangan di brankas AMS dan Lihat cadangan di brankas AMS.	Januari 13, 2022

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.