Informasi Orientasi Akun Tingkat Lanjut AMS

Panduan Orientasi Tingkat Lanjut AMS

Versi September 25, 2025

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Panduan Orientasi Tingkat Lanjut AMS: Informasi Orientasi Akun Tingkat Lanjut AMS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

AWS Managed Services Onboarding Pendahuluan 1
Belajar tentang AMS 1
Istilah kunci 2
Mode AMS 9
Mode dan aplikasi AMS atau beban kerja 9
Panduan preskriptif pasca-akun AMS 17
Apa yang kita lakukan, apa yang tidak kita lakukan 17
Manajemen lalu lintas jalan keluar AMS 19
Peran pengguna IAM 20
MALZ: Peran Pengguna IAM Default 21
SALZ: Peran Pengguna IAM Default 34
Aturan Firewall Akses Default 41
Port Instans Tumpukan Linux 42
Port Instans Stack Windows 42
Manajemen layanan 44
Tata kelola akun 44
Dimulainya layanan 45
Manajemen hubungan pelanggan (CRM) 45
Proses CRM 46
Rapat CRM 47
Pengaturan Rapat CRM 48
Laporan bulanan CRM 49
Optimalisasi biaya 50
Kerangka kerja pengoptimalan biaya 50
Matriks tanggung jawab optimasi biaya 52
Jam layanan 54
Mendapatkan bantuan 55
Ubah mode manajemen 56
Ikhtisar mode 57
Jenis mode dan akun di AMS 58
Mode dan aplikasi AMS atau beban kerja 61
Kasus penggunaan dunia nyata untuk mode AMS 69
Modus RFC 72
Pelajari tentang RFCs 73

Apa itu jenis perubahan? 113
Memecahkan masalah kesalahan RFC 126
Mode Ubah Langsung 136
Memulai dengan mode Perubahan Langsung 137
Keamanan dan kepatuhan 140
Ubah manajemen dalam mode Perubahan Langsung 145
Membuat tumpukan menggunakan mode Perubahan Langsung 148
Kasus penggunaan Mode Perubahan Langsung 151
Mode pengembang 152
Memulai dengan mode Pengembang 153
Keamanan dan kepatuhan 155
Manajemen perubahan 157
Penyediaan infrastruktur 162
Kontrol detektif 163
Pencatatan, pemantauan, dan manajemen acara 163
Manajemen insiden 163
Manajemen tambalan 164
Manajemen kontinuitas 164
Keamanan dan manajemen akses 164
Mode Penyediaan Layanan Mandiri di AMS 165
Memulai dengan mode SSP di AMS 166
Amazon API Gateway 166
Alexa for Business 167
Amazon AppStream 2.0 169
Amazon Athena 171
Amazon Bedrock 172
Amazon CloudSearch 174
Amazon CloudWatch Synthetics 175
Amazon Cognito 176
Amazon Comprehend 178
Amazon Connect 179
Amazon Data Firehose 181
DevOpsGuru Amazon 182
Amazon DocumentDB (dengan kompatibilitas MongoDB) 183
Amazon DynamoDB 184
Amazon Elastic Container Registry 185

EC2 Image Builder 186
Amazon ECS aktif AWS Fargate 188
Amazon EKS di AWS Fargate 191
Amazon EMR 194
Amazon EventBridge 197
Amazon Forecast 199
Amazon FSx 202
Amazon FSx untuk OpenZFS 203
Amazon FSx untuk NetApp ONTAP 205
Amazon Inspector Klasik 206
Amazon Kendra 208
Amazon Kinesis Data Streams 208
Amazon Kinesis Video Streams 209
Amazon Lex 210
Amazon MQ 211
Layanan Terkelola Amazon untuk Apache Flink 212
Amazon Managed Streaming untuk Apache Kafka 213
Layanan Terkelola Amazon untuk Prometheus 215
Amazon Personalize 216
Amazon QuickSight 219
Amazon Rekognition 220
Amazon SageMaker AI 221
Layanan Email Sederhana Amazon 225
Layanan Alur Kerja Sederhana Amazon 226
Amazon Textract 227
Amazon Transcribe 228
Amazon WorkSpaces 229
Layanan Kode AMS 231
AWS Amplify 234
AWS AppSync 235
AWS App Mesh 236
AWS Audit Manager 237
AWS Batch 238
AWS Certificate Manager 240
AWS Private Certificate Authority 241
AWS CloudEndure 244

AWS CloudHSM 245
AWS CodeBuild 247
AWS CodeCommit 248
AWS CodeDeploy 250
AWS CodePipeline 251
AWS Compute Optimizer 253
AWS DataSync 254
AWS Device Farm 255
AWS Elastic Disaster Recovery 256
AWS Elemental MediaConvert 257
AWS Elemental MediaLive 258
AWS Elemental MediaPackage 259
AWS Elemental MediaStore 260
AWS Elemental MediaTailor 261
AWS Global Accelerator 262
AWS Glue 263
AWS Lake Formation 264
AWS Lambda 266
AWS License Manager 267
AWS Migration Hub 268
AWS Outposts 269
AWS Resilience Hub 270
AWS Secrets Manager 271
AWS Security Hub CSPM 274
AWS Service Catalog AppRegistry 275
AWS Shield 276
AWS Snowball Edge 277
AWS Step Functions 279
AWS Systems Manager Toko Parameter 280
AWS Systems Manager Otomasi 281
AWS Transfer Family 284
AWS Transit Gateway 286
AWS WAF 287
AWS Well-Architected Tool 288
AWS X-Ray 289
VM Import/Export 290

Modus Dikelola Pelanggan 291
Memulai mode Customer Managed 292
AMS dan AWS Service Catalog 292
Memulai Service Catalog 293
Service Catalog di AMS sebelum Anda mulai 293
Orientasi AMS Multi-akun landing zone (MALZ) 297
Arsitektur jaringan MALZ 297
Tentang arsitektur jaringan landing zone multi-akun 297
Memilih MALZ tunggal atau ganda MALZs 299
Akun Zona Pendaratan Multi-Akun 305
MALZ: Orientasi akun inti 338
Buat AWS akun inti landing zone multi-akun 339
Buat peran IAM untuk AMS untuk mengakses akun Anda 340
Amankan akun baru dengan otentikasi multi-faktor (MFA) untuk pengguna root 342
Berlangganan AWS Marketplace untuk EPS 342
Mengatur jaringan 343
Mengatur manajemen akses 347
MALZ: Orientasi akun aplikasi 352
Meminta akun aplikasi baru 353
Menyiapkan Active Directory untuk mengfederasi akses ke peran AMS IAM 354
Menyiapkan jaringan dengan akun Aplikasi baru 357
Menyiapkan tambahan VPCs di akun Aplikasi 359
Lampiran: daftar pertimbangan orientasi multi-akun landing zone (MALZ) 359
Konfigurasi akun 360
Peringatan pemantauan landing zone multi-akun AMS 360
Konfigurasi jaringan 361
Konfigurasi Direktori Aktif 362
Perlindungan Titik Akhir Trend Micro (EPS) 362
Akses: Bastion, SSH dan RDP 363
Federation 364
Orientasi AMS Single-account landing zone (SALZ) 365
Proses orientasi AMS SALZ 365
Arsitektur jaringan SALZ 366
Layanan bersama landing zone akun tunggal AMS 367
SALZ: Buat AWS akun baru untuk AMS 368
Buat sebuah Akun AWS 368

Siapkan tagihan konsolidasan—tautkan akun baru ke akun Pembayar 371
Konfigurasikan Akun AWS akses AMS Anda 371
Berlangganan AWS Marketplace untuk EPS 373
Berlangganan AWS Marketplace untuk CentOS 7.6 375
Amankan akun baru dengan otentikasi multi-faktor (MFA) untuk pengguna root 375
SALZ: Mengatur jaringan 375
Alokasikan Ruang IP untuk Lingkungan AMS Anda 375
Membangun Konektivitas Jaringan Pribadi ke AWS 377
Siapkan Firewall Anda 378
Opsi AMS Bastion selama Migrasi/Orientasi Aplikasi 378
SALZ: Mengatur manajemen akses 379
Membangun kepercayaan Active Directory (AD) 380
Federasi Direktori Aktif Anda dengan peran AMS AWS Identity and Access Management ... 386
SALZ: Pengaturan default 392
Keamanan Titik Akhir (EPS) 392
Grup keamanan 397
EC2 Profil instans IAM 402
Metrik yang dipantau secara default 410
Retensi log dan default rotasi 427
Default manajemen kontinuitas 428
Menambal default 429
Validasi layanan AMS (SALZ) 430
Temukan pengaturan akun 431
Menemukan ID instans atau alamat IP 435
Nama benteng ramah DNS 437
Menemukan alamat IP benteng 439
EC2 contoh: Membuat 439
Akses, meminta 449
Lainnya | RFC lainnya, membuat (CLI) 456
Tumpukan apa pun: menghapus, me-reboot, memulai, menghentikan 458
Contoh akses 470
Melaporkan insiden 480
Membuat permintaan layanan 483
Langkah pasca-orientasi 486
Tutorial 486
Lampiran: Kuesioner orientasi SALZ 513

Ringkasan penyebaran 513
Pertimbangan arsitektur lingkungan 514
Peringatan Pemantauan Zona Pendaratan Akun Tunggal 515
Jendela Pemeliharaan 515
Langkah Berikutnya 515
Lampiran: Aturan klaim ActiveDirectory Federation Services (ADFS) dan pengaturan SAMP 517
Konfigurasi aturan klaim ADFS 517
Konsol web 518
Akses API dan CLI dengan SAMP 518
Konfigurasi skrip 518
Konfigurasi Windows 518
Konfigurasi Linux 520
Riwayat dokumen 522
..... dxxv

AWS Managed Services Onboarding Pendahuluan

Selamat datang di AWS Managed Services (AMS). AMS adalah layanan perusahaan yang menyediakan pengelolaan infrastruktur AWS Anda secara berkelanjutan. Panduan ini dirancang untuk membantu Anda mulai menggunakan AMS, termasuk cara menyiapkan akun baru untuk AMS, menyiapkan jaringan dan akses ke AMS, dan memvalidasi pengaturan orientasi Anda.

Ini ditujukan untuk administrator TI yang bertugas mempersiapkan dan melaksanakan tugas yang diperlukan untuk onboard layanan AMS ke akun AWS baru. Orientasi layanan AMS memerlukan hak istimewa khusus untuk menyiapkan trust Active Directory dan menyelesaikan tugas tingkat jaringan lainnya. Untuk mendapatkan bantuan dalam memutuskan apakah akan menggunakan akun landing zone multi-akun atau akun landing zone akun tunggal, kunjungi Memilih MALZ tunggal atau beberapa. MALZs

> **Important**
>
> Panduan ini dibagi menjadi dua bagian setelah pengenalan ini: Satu untuk akun landing zone multi-akun dan satu untuk akun landing zone akun tunggal. Orientasinya sangat berbeda untuk keduanya, silakan pergi ke bagian panduan yang berlaku untuk situasi Anda.

Topik

- Belajar tentang AMS
- Istilah kunci AMS
- Mode AMS
- Panduan preskriptif pasca-akun AMS
- Apa yang kita lakukan, apa yang tidak kita lakukan
- Manajemen lalu lintas jalan keluar AMS
- Peran pengguna IAM di AMS
- Aturan Firewall Akses Default

Belajar tentang AMS

Untuk memahami AMS dengan lebih baik, lihat bagian Panduan Pengguna AMS ini:

- What Is AWS Managed Services memperkenalkan layanan AMS dan menjelaskan fitur utama, operasi, dan antarmuka serta arsitektur jaringan yang dikelola AMS yang khas. Bab ini juga menyediakan informasi tentang manajemen akses termasuk cara mengakses sumber daya yang dikelola AMS dan menggunakan benteng.
- Istilah Kunci memberikan definisi dan penjelasan untuk terminologi AMS.
- Memahami Default AMS memberikan nilai default yang digunakan AMS, termasuk default untuk komponen lingkungan dasar, IAM dan, proxy, metrik yang dipantau, logging EC2, keamanan titik akhir (EPS), pencadangan, dan penambalan.
- Change Management memberikan rincian tentang cara kerja request for change (RFCs) dan change types (CTs) dan menyertakan contoh penggunaan AMS RFCs.
- Beberapa chapter tambahan mencakup mengakses konsol AWS, AMS CLI, menggunakan sistem manajemen perubahan AMS, SKMS AMS, keamanan, permintaan layanan, insiden, pemantauan, log, EPS, backup, dan manajemen patch.

Untuk mempelajari lebih lanjut tentang arsitektur landing zone multi-akun AMS, lihat Arsitektur jaringan Zona Pendaratan Multi-Akun

Untuk mempelajari lebih lanjut tentang arsitektur landing zone akun tunggal AMS, lihat Arsitektur jaringan Zona Pendaratan Akun Tunggal

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.

Mode AMS

Gunakan ini untuk membantu Anda memilih mode AWS Managed Services (AMS) yang sesuai untuk hosting aplikasi Anda, berdasarkan kombinasi fleksibilitas dan tata kelola preskriptif yang Anda inginkan untuk mencapai hasil bisnis Anda.

Audiens yang dituju untuk informasi ini adalah:

- Tim pelanggan yang bertanggung jawab atas strategi dan tata kelola landing zone mereka. Informasi ini akan membantu tim menyusun fondasi landing zone yang dikelola AMS, dengan mode AMS yang ingin mereka tawarkan kepada pelanggan internal dan eksternal mereka.
- Pemilik bisnis dan aplikasi ditugaskan untuk memigrasikan aplikasi mereka ke AMS. Informasi ini akan membantu merencanakan migrasi aplikasi, dengan mode AMS yang sesuai untuk aplikasi migrate/host mereka. Catatan, aplikasi yang sama dapat di-host di lebih dari satu mode AMS selama fase siklus hidup Siklus Hidup Pengembangan Perangkat Lunak (SDLC) yang berbeda.
- Mitra AMS bertugas membimbing pelanggan tentang berbagai opsi untuk membangun dan bermigrasi ke AMS.

Informasi ini mengasumsikan bahwa Anda telah membuat keputusan untuk memanfaatkan AMS untuk mempercepat perjalanan Anda ke cloud. Lihat paper ini di dua titik dalam perjalanan migrasi cloud Anda: Pertama, selama fase dasar menyiapkan platform yang dikelola AMS. Kedua, ketika Anda beralih dari fondasi ke fase migrasi dari perjalanan adopsi cloud Anda, tepat setelah orientasi ke AMS selesai dan Anda berfokus pada tata kelola dan operasi aplikasi.

Mode dan aplikasi AMS atau beban kerja

Pertimbangkan persyaratan operasional dan tata kelola untuk aplikasi Anda saat memilih mode yang tepat, baik dengan meminta akun aplikasi baru atau menghosting aplikasi di akun aplikasi yang ada. Pemilihan mode AMS yang sesuai untuk setiap aplikasi atau beban kerja tergantung pada faktor-faktor berikut:

- Jenis fungsi siklus hidup SDLC yang akan disediakan lingkungan (misalnya, kotak pasir dengan perubahan yang tidak dimoderasi, UAT dengan beberapa perubahan yang sering, produksi dengan perubahan minimal dan sangat diatur)
- Kebijakan tata kelola yang diperlukan (ditegakkan melalui SCPs di tingkat OU)
- Model Operasional (jika Anda ingin memiliki tanggung jawab operasional atau ingin mengalihdayakannya ke AMS)

- Hasil bisnis yang diinginkan, seperti waktu untuk beroperasi di cloud, dan biaya operasi.

> **Note**
>
> Untuk deskripsi jenis mode per layanan AMS, lihat Jenis mode dan akun di AMS.
> Untuk kasus penggunaan dunia nyata dari berbagai mode, lihat Kasus penggunaan dunia nyata untuk mode AMS

Tabel berikut menguraikan pertimbangan utama bagi pemilik aplikasi untuk membantu memutuskan mode AMS yang paling sesuai. Pemilik aplikasi harus menyertakan fase penilaian sebelum migrasi aplikasi untuk sepenuhnya memahami mode mana yang berlaku untuk aplikasi spesifik mereka. Contoh: Untuk aplikasi berbasis layanan cloud-native atau arsitektur tanpa server, opsi terbaik adalah mulai membangun dan mengulangi dalam mode Pengembang dan menerapkan Infrastruktur akhir sebagai Kode menggunakan mode AMS Managed — SSP. Dalam hal ini, pemfaktoran ulang ringan mungkin diperlukan untuk memastikan bahwa CloudFormation templat apa pun yang dibuat untuk penerapan otomatis memenuhi pedoman konsumsi yang ditetapkan oleh AMS. Selain itu, izin IAM apa pun harus disetujui oleh AMS Security untuk memastikan mereka mengikuti model hak istimewa paling sedikit.

Mode AMS yang dipilih untuk meng-host aplikasi, dapat membantu Anda membangun model operasi cloud yang Anda inginkan.

> **Note**
>
> Lebih dari satu model operasi cloud dapat ada dalam satu Zona Pendaratan Terkelola AMS berdasarkan berbagai mode AMS yang dipilih untuk meng-host aplikasi.

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
Kesiapan operasional						
Logging, Monitorin	AMS bertanggung jawab atas semua infrastruktur yang dikelola			Pelanggan yang	Pelanggan bertanggu	Pelanggan yang

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
g dan Manajemen Acara				bertanggung jawab atas Layanan Penyediaan Layanan Mandiri (SSP)	ng jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar sistem AMS CM	
Manajemen Kontinuitas	Tanggung jawab AMS untuk melaksanakan rencana cadangan yang dipilih oleh pelanggan			Pelanggan yang bertanggung jawab atas Layanan Penyediaan Layanan Mandiri (SSP)	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar sistem AMS CM	bertanggung jawab

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
Manajemen Akses Tingkat Instans	Dikelola AMS melalui kepercayaan AD satu arah dengan domain on-prem. Memerlukan infrastruktur terkelola untuk bergabung dengan domain AMS			Tidak berlaku	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar sistem AMS CM	
Manajemen Keamanan dan Manajemen Akses Tingkat Akun	Tanggung jawab AMS untuk semua akun terkelola			AMS bertanggung jawab atas semua akun yang dikelola	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar sistem AMS CM	

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
Manajemen Patch	Tanggung jawab AMS untuk semua akun terkelola			Pelanggan yang bertanggung jawab atas Layanan Penyediaan Layanan Mandiri (SSP)	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar sistem AMS CM	
Manajemen Perubahan	Tanggung jawab AMS untuk semua akun terkelola			Pelanggan yang bertanggung jawab atas Layanan Penyediaan Layanan Mandiri (SSP)	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar sistem AMS CM	

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
Manajemen Penyediaan	Preskriptif dan standar untuk opsi penyediaan yang ditawarkan di AMS	Fleksibilitas untuk langsung menggunakan AWS service API untuk AWS Service Catalog mengikuti standar preskriptif AMS	Fleksibilitas untuk langsung menggunakan AWS service API mengikuti standar preskriptif AMS	Fleksibilitas untuk langsung menggunakan layanan AWS APIs untuk layanan SSP	Fleksibilitas untuk langsung menggunakan AWS service API untuk penyediaan	
Manajemen Insiden dan Audit	Tanggung jawab AMS untuk semua akun terkelola				Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar AMS Change Management System	

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
GuardRails Infrastruktur Bersama (Jaringan) dan Kerangka Keamanan	Memanfaatkan Akun Inti AMS yang preskriptif dan standar					Memanfaatkan Akun Inti AMS yang fleksibel dan dipesan lebih dahulu
Kesiapan aplikasi						
Aplikasi refactoring	Diperlukan refactoring ringan				Diperlukan refactoring ringan (jika disediakan menggunakan AMS Standard CM)	Tidak perlu refactoring
Support untuk layanan AWS	Terbatas pada apa yang didukung oleh AMS					Tidak terbatas
Pertimbangan bisnis						

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
Saatnya kesiapan operasional	Tiga sampai enam bulan			6 bulan+tergantung pada kompetensi operasi aplikasi pelanggan		6-18 bulan tergantung pada infrastruktur pelanggan dan kompetensi operasi aplikasi
Biaya	$$$$			$$$	$$	$
Contoh aplikasi	Server web dengan tumpukan 3 tingkat, aplikasi dengan kepatuhan dan persyaratan peraturan			Server web menggunakan API Gateway, aplikasi kontainer yang memanfaatkan ECS/EKS	Mengiterasi/mengoptimalkan aplikasi Data Lake yang menggunakan Lambda, Glue, Athena, dll	De-sentralisasi accounts/applications seperti kotak pasir, aplikasi yang dikelola pihak ketiga

* Operations On Demand (OOD) memiliki penawaran untuk pelanggan yang menggunakan mode CM Standar untuk mengelola perubahan mereka melalui sumber daya khusus. Untuk detail selengkapnya, lihat katalog penawaran Operations on Demand dan hubungi manajer pengiriman layanan cloud (CSDM) Anda.

> **Note**
>
> Perbandingan harga antara mode SSP dan mode Pengembang mengasumsikan bahwa layanan AWS yang sama disediakan.

Membandingkan Mode AMS dengan tujuan bisnis dan TI

Seperti yang ditunjukkan, jika Anda mencari model tata kelola yang sangat terkontrol dan terstandarisasi untuk aplikasi Anda, maka mode Perubahan Standar yang dikelola AMS, AWS Service Catalog, atau Direct Change adalah yang paling cocok. Jika Anda memerlukan model tata kelola yang dipesan lebih dahulu dengan fokus pada inovasi aplikasi tanpa perlu kesiapan operasional, pilih mode Customer Managed. Dengan mode Customer Managed, Anda bisa membutuhkan waktu lebih lama untuk mengoperasionalkan aplikasi Anda karena Anda memikul tanggung jawab untuk menetapkan orang, proses, dan alat untuk mendukung kemampuan operasional seperti Manajemen Insiden, Manajemen Konfigurasi, Manajemen Penyediaan, Manajemen Keamanan, Manajemen Patch, dll.

Panduan preskriptif pasca-akun AMS

Ketika organisasi mengadopsi operasi dan DevOps praktik terdistribusi, ada seperangkat inti kemampuan operasional yang harus diterapkan ke setiap akun sebelum penyebaran beban kerja untuk memenuhi pilar Well Architected.

Tautan ini mengunduh file ZIP yang berisi dokumen Word, dan file ZIP dengan skrip dan contoh. Pengaturan Akun Otomatis adalah seperangkat skrip untuk mengotomatiskan, atau bootstrap, pengaturan akun aplikasi baru.

Setelah akun baru dijual, dan sebelum beban kerja apa pun diterapkan, untuk membuat akun siap dari sudut pandang operasional, keamanan, dan manajemen, Anda mengatur rencana cadangan default, jendela tambalan, dan enkripsi (dan banyak lagi). Untuk membantu meningkatkan kelincahan, konsistensi, dan daya tanggap untuk pengaturan akun aplikasi, contoh berikut “Cara” disediakan untuk referensi Anda.

Pengaturan Akun Otomatis.

Apa yang kita lakukan, apa yang tidak kita lakukan

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

> **Note**
>
> Untuk meminta agar AMS menyediakan layanan AWS tambahan, ajukan permintaan layanan. Untuk informasi selengkapnya, lihat Membuat Permintaan Layanan.

- Apa yang kita lakukan:

  Setelah Anda menyelesaikan orientasi, lingkungan AMS tersedia untuk menerima permintaan perubahan (RFCs), insiden, dan permintaan layanan. Interaksi Anda dengan layanan AMS berkisar pada siklus hidup tumpukan aplikasi. Tumpukan baru diurutkan dari daftar templat yang telah dikonfigurasi sebelumnya, diluncurkan ke subnet virtual private cloud (VPC) tertentu, dimodifikasi selama masa operasionalnya melalui permintaan perubahan (RFCs), dan dipantau untuk kejadian dan insiden 24/7.

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

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

- Apa yang tidak kita lakukan:

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

Manajemen lalu lintas jalan keluar AMS

Secara default, rute dengan CIDR tujuan 0.0.0.0/0 untuk subnet pribadi AMS dan aplikasi pelanggan memiliki gateway terjemahan alamat jaringan (NAT) sebagai target. Layanan AMS, TrendMicro dan patching, adalah komponen yang harus memiliki akses keluar ke Internet sehingga AMS dapat menyediakan layanannya, dan TrendMicro dan sistem operasi dapat memperoleh pembaruan.

AMS mendukung pengalihan lalu lintas keluar ke internet melalui perangkat jalan keluar yang dikelola pelanggan selama:

- Ini bertindak sebagai proxy implisit (misalnya, transparan).

  and

- Ini memungkinkan dependensi AMS HTTP dan HTTPS (tercantum di bagian ini) untuk memungkinkan penambalan dan pemeliharaan infrastruktur terkelola AMS yang sedang berlangsung.

Beberapa contohnya adalah:

- Gateway transit (TGW) memiliki rute default yang menunjuk ke firewall lokal yang dikelola pelanggan melalui koneksi AWS Direct Connect di akun Jaringan Zona Pendaratan Multi-Akun.
- TGW memiliki rute default yang menunjuk ke titik akhir AWS di VPC keluar Zona Pendaratan Multi-Akun yang memanfaatkan AWS PrivateLink, menunjuk ke proxy yang dikelola pelanggan di akun AWS lain.
- TGW memiliki rute default yang menunjuk ke firewall yang dikelola pelanggan di akun AWS lain, dengan koneksi site-to-site VPN sebagai lampiran ke Multi-Account Landing Zone TGW.

AMS telah mengidentifikasi dependensi HTTP dan HTTPS AMS yang sesuai, dan mengembangkan serta menyempurnakan dependensi ini secara berkelanjutan. Lihat egressMgmt.zip. Seiring dengan file JSON, ZIP berisi README.

> **Note**
>
> - Informasi ini tidak komprehensif - beberapa situs eksternal yang diperlukan tidak tercantum di sini.
> - Jangan gunakan daftar ini di bawah daftar penolakan atau strategi pemblokiran.

- Daftar ini dimaksudkan sebagai titik awal untuk set aturan penyaringan jalan keluar, dengan harapan bahwa alat pelaporan akan digunakan untuk menentukan dengan tepat di mana lalu lintas aktual menyimpang dari daftar.

Untuk meminta informasi tentang memfilter lalu lintas jalan keluar, kirim email ke CSDM Anda: ams-csdm@amazon.com.

Peran pengguna IAM di AMS

Peran IAM mirip dengan pengguna IAM, karena itu adalah AWS identitas dengan kebijakan izin yang menentukan apa yang dapat dan tidak dapat dilakukan identitas. AWS Namun, alih-alih secara unik terkait dengan satu orang, peran dimaksudkan untuk menjadi dapat diambil oleh siapa pun yang membutuhkannya.

Saat ini ada satu peran pengguna default AMS`Customer_ReadOnly_Role`, untuk akun AMS standar dan peran tambahan, `customer_managed_ad_user_role` untuk akun AMS dengan Direktori Aktif Terkelola.

Kebijakan peran menetapkan izin untuk CloudWatch dan tindakan log Amazon S3, akses konsol AMS, pembatasan hanya-baca pada Layanan AWS sebagian besar, akses terbatas ke konsol S3 akun, dan akses tipe perubahan AMS.

Selain itu, `Customer_ReadOnly_Role` memiliki izin instans cadangan mutatif yang memungkinkan Anda untuk memesan instance. Ini memiliki beberapa nilai penghematan biaya, jadi, jika Anda tahu bahwa Anda akan memerlukan sejumlah EC2 instans Amazon untuk jangka waktu yang lama, Anda dapat memanggilnya. APIs Untuk mempelajari lebih lanjut, lihat Instans EC2 Cadangan Amazon.

> **Note**
>
> Tujuan tingkat layanan AMS (SLO) untuk membuat kebijakan IAM khusus untuk pengguna IAM adalah empat hari kerja, kecuali kebijakan yang ada akan digunakan kembali. Jika Anda ingin mengubah peran pengguna IAM yang ada, atau menambahkan yang baru, kirimkan IAM: Update Entity atau IAM: Create Entity RFC, masing-masing.

Jika Anda tidak terbiasa dengan peran Amazon IAM, lihat Peran IAM untuk informasi penting.

Zona Pendaratan Multi-Akun (MALZ): Untuk melihat kebijakan peran pengguna default, tanpa penyesuaian, zona pendaratan multi-akun AMS, lihat, selanjutnya. MALZ: Peran Pengguna IAM Default

MALZ: Peran Pengguna IAM Default

Pernyataan kebijakan JSON untuk peran pengguna landing zone multi-akun AMS multi-akun default.

> **Note**
>
> Peran pengguna dapat disesuaikan dan mungkin berbeda berdasarkan per akun. Petunjuk untuk menemukan peran Anda disediakan.

Ini adalah contoh peran pengguna MALZ default. Untuk memastikan bahwa Anda memiliki kebijakan yang ditetapkan yang Anda butuhkan, jalankan perintah AWS `get-role`atau masuk ke AWS Management -> konsol IAM dan pilih Peran di panel navigasi.

Peran akun inti OU

Akun inti adalah akun infrastruktur yang dikelola Malz. Akun inti zona pendaratan multi-akun AMS mencakup akun manajemen dan akun jaringan.

Akun Core OU: Peran dan kebijakan umum

Peran	Kebijakan atau kebijakan
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Kebijakan Terkelola AWS Publik).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAkses (Kebijakan Terkelola AWS Publik).
AWSManagedServicesChangeManagementRole (Versi akun inti)	ReadOnlyAccess
	AWSSupportAkses
	AMSChangeManagementReadOnlyPolicy

Peran	Kebijakan atau kebijakan
	AMSChangeManagementInfrastructurePolicy

Akun Core OU: Peran dan kebijakan akun manajemen

Peran	Kebijakan atau kebijakan
AWSManagedServicesBillingRole	AMSBillingKebijakan (AMSBillingKebijakan).
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Kebijakan Terkelola AWS Publik).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAkses (Kebijakan Terkelola AWS Publik).
AWSManagedServicesChangeManagementRole (Versi akun manajemen)	ReadOnlyAccess
	AWSSupportAkses
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

Akun Core OU: Peran dan kebijakan akun jaringan

Peran	Kebijakan atau kebijakan
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Kebijakan Terkelola AWS Publik).
AWSManagedServicesCaseRole	ReadOnlyAccess

Peran	Kebijakan atau kebijakan
	AWSSupportAkses (Kebijakan Terkelola AWS Publik).
AWSManagedServicesChangeManagementRole (Versi akun jaringan)	ReadOnlyAccess
	AWSSupportAkses
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

Peran Akun Aplikasi

Peran akun aplikasi diterapkan ke akun khusus aplikasi Anda.

Akun aplikasi: Peran dan kebijakan

Peran	Kebijakan atau kebijakan
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Kebijakan Terkelola AWS Publik).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAkses (Kebijakan Terkelola AWS Publik). Kebijakan ini menyediakan akses ke semua operasi dan sumber daya pendukung. Untuk selengkapnya, lihat Memulai dengan AWS Support.
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess
	AWSSupportContoh Akses

Peran	Kebijakan atau kebijakan
	Kebijakan ini menyediakan akses ke semua operasi dan sumber daya pendukung.
	AWSCertificateManagerFullAccess informasi, (Kebijakan Terkelola AWS Publik)
	AWSWAFFullAccess informasi, (Kebijakan AWS Terkelola Publik). Kebijakan ini memberikan akses penuh ke sumber daya AWS WAF.
	AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole (Versi akun aplikasi)	ReadOnlyAccess
	AWSSupportAkses (Kebijakan Terkelola AWS Publik). Kebijakan ini menyediakan akses ke semua operasi dan sumber daya pendukung. Untuk selengkapnya, lihat Memulai dengan AWS Support.
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AMSReservedInstancesPolicy
	AMSS3Kebijakan
AWSManagedServicesAdminRole	ReadOnlyAccess
	AWSSupportAkses
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions

Peran	Kebijakan atau kebijakan
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFullAkses
	AMSS3Kebijakan
	AMSReservedInstancesPolicy

Contoh Kebijakan

Contoh disediakan untuk sebagian besar kebijakan yang digunakan. Untuk melihat ReadOnlyAccess kebijakan (yang merupakan halaman selama menyediakan akses hanya-baca ke semua AWS layanan), Anda dapat menggunakan tautan ini, jika Anda memiliki akun AWS aktif:. ReadOnlyAccess Juga, versi kental disertakan di sini.

AMSBillingKebijakan

`AMSBillingPolicy`

Peran Penagihan baru dapat digunakan oleh departemen akuntansi Anda untuk melihat dan mengubah informasi penagihan atau pengaturan akun di akun Manajemen. Untuk mengakses informasi seperti Kontak Alternatif, melihat penggunaan sumber daya akun, atau menyimpan tab penagihan Anda atau bahkan mengubah metode pembayaran, Anda menggunakan peran ini. Peran baru ini terdiri dari semua izin yang tercantum di halaman web tindakan AWS Billing IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ModifyBilling"
```

```
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToBilling"
        },
        {
            "Action": [
                "aws-portal:ViewAccount",
                "aws-portal:ModifyAccount"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountSettings"
        },
        {
            "Action": [
                "budgets:ViewBudget",
                "budgets:ModifyBudget"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountBudget"
        },
        {
            "Action": [
                "aws-portal:ViewPaymentMethods",
                "aws-portal:ModifyPaymentMethods"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPaymentMethods"
        },
        {
            "Action": [
                "aws-portal:ViewUsage"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToUsage"
        },
        {
            "Action": [
                "cur:DescribeReportDefinitions",
                "cur:PutReportDefinition",
```

```
                "cur:DeleteReportDefinition",
                "cur:ModifyReportDefinition"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostAndUsageReport"
        },
        {
            "Action": [
                "pricing:DescribeServices",
                "pricing:GetAttributeValues",
                "pricing:GetProducts"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPricing"
        },
        {
            "Action": [
                "ce:*",
                "compute-optimizer:*"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostExplorerComputeOptimizer"
        },
        {
            "Action": [
                "purchase-orders:ViewPurchaseOrders",
                "purchase-orders:ModifyPurchaseOrders"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPurchaseOrders"
        },
        {
            "Action": [
                "redshift:AcceptReservedNodeExchange",
                "redshift:PurchaseReservedNodeOffering"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToRedshiftAction"
        },
```

```
        {
            "Action": "savingsplans:*",
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AWSSavingsPlansFullAccess"
        }
    ]
}
```

AMSChangeManagementReadOnlyPolicy

`AMSChangeManagementReadOnlyPolicy`

Izin untuk melihat semua jenis perubahan AMS, dan riwayat jenis perubahan yang diminta.

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

`AMSMasterAccountSpecificChangeManagementInfrastructurePolicy`

Izin untuk meminta Deployment | Managed landing zone | Akun manajemen | Buat akun aplikasi (dengan VPC) mengubah jenis.

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

`AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy`

Izin untuk meminta Deployment | Managed landing zone | Akun jaringan | Buat jenis perubahan tabel rute aplikasi.

AMSChangeManagementInfrastructurePolicy

`AMSChangeManagementInfrastructurePolicy`(untuk Manajemen | Lainnya | Lainnya CTs)

Izin untuk meminta Manajemen | Lainnya | Lainnya | Buat, dan Manajemen | Lainnya | Lainnya | Perbarui jenis perubahan.

AMSSecretsManagerSharedPolicy

`AMSSecretsManagerSharedPolicy`

Izin untuk melihat rahasia yang passwords/hashes dibagikan oleh AMS melalui AWS Secrets Manager (misalnya kata sandi ke infrastruktur untuk audit).

Izin untuk membuat rahasia password/hashes untuk dibagikan dengan AMS. (misalnya, kunci lisensi untuk produk yang perlu digunakan).

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
   "Sid": "AllowAccessToSharedNameSpaces",
   "Effect": "Allow",
   "Action": "secretsmanager:*",
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
   ]
  },
  {
   "Sid": "DenyGetSecretOnCustomerNamespace",
   "Effect": "Deny",
   "Action": "secretsmanager:GetSecretValue",
   "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
   "Sid": "AllowReadAccessToAMSNameSpace",
   "Effect": "Deny",
   "NotAction": [
    "secretsmanager:Describe*",
    "secretsmanager:Get*",
    "secretsmanager:List*"
   ],
   "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
 ]
}
```

AMSChangeManagementPolicy

`AMSChangeManagementPolicy`

Izin untuk meminta dan melihat semua jenis perubahan AMS, dan riwayat jenis perubahan yang diminta.

AMSReservedInstancesPolicy

`AMSReservedInstancesPolicy`

Izin untuk mengelola instans EC2 cadangan Amazon; untuk informasi harga, lihat Instans EC2 Cadangan Amazon.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Sid": "AllowReservedInstancesManagement",
  "Effect": "Allow",
  "Action": [
   "ec2:ModifyReservedInstances",
   "ec2:PurchaseReservedInstancesOffering"
  ],
  "Resource": [
   "*"
  ]
 }]
}
```

AMSS3Kebijakan

`AMSS3Policy`

Izin untuk membuat dan menghapus file dari bucket Amazon S3 yang ada.

> **Note**
>
> Izin ini tidak memberikan kemampuan untuk membuat bucket S3; yang harus dilakukan dengan Deployment | Komponen tumpukan lanjutan | Penyimpanan S3 | Buat jenis perubahan.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:PutObject"
            ],
            "Resource": "*"
        }
    ]
}
```

AWSSupportAkses

`AWSSupportAccess`

Akses penuh ke Dukungan. Untuk selengkapnya, lihat Memulai dengan Dukungan. Untuk informasi Dukungan Premium, lihat Dukungan.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "support:*"
  ],
  "Resource": "*"
 }]
}
```

AWSMarketplaceManageSubscriptions

`AWSMarketplaceManageSubscriptions`(Kebijakan yang AWS Dikelola Publik)

Izin untuk berlangganan, berhenti berlangganan, dan melihat AWS Marketplace langganan.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "aws-marketplace:ViewSubscriptions",
   "aws-marketplace:Subscribe",
   "aws-marketplace:Unsubscribe"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

AWSCertificateManagerFullAccess

`AWSCertificateManagerFullAccess`

Akses penuh ke AWS Certificate Manager. Untuk informasi selengkapnya, lihat AWS Certificate Manager.

`AWSCertificateManagerFullAccess`informasi, (Kebijakan Terkelola AWS Publik).

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "acm:*"
  ],
  "Resource": "*"
 }]
}
```

AWSWAFFullAkses

`AWSWAFFullAccess`

Akses penuh ke AWS WAF. Untuk informasi selengkapnya, lihat AWS WAF - Firewall Aplikasi Web.

`AWSWAFFullAccess`informasi, (Kebijakan yang AWS Dikelola Publik). Kebijakan ini memberikan akses penuh ke AWS WAF sumber daya.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "waf:*",
   "waf-regional:*",
   "elasticloadbalancing:SetWebACL"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

ReadOnlyAccess

`ReadOnlyAccess`

Akses hanya-baca ke semua AWS layanan dan sumber daya di konsol. AWS Saat AWS meluncurkan layanan baru, AMS memperbarui ReadOnlyAccess kebijakan untuk menambahkan izin hanya-baca untuk layanan baru. Izin yang diperbarui diterapkan pada semua entitas prinsipal yang kebijakannya dilampirkan.

Ini tidak memberikan kemampuan untuk masuk ke EC2 host atau host database.

Jika Anda aktif Akun AWS, maka Anda dapat menggunakan tautan ini ReadOnlyAccessuntuk melihat seluruh ReadOnlyAccess kebijakan. Seluruh ReadOnlyAccess kebijakan sangat panjang karena menyediakan akses hanya-baca ke semua. Layanan AWS Berikut ini adalah kutipan sebagian dari kebijakan tersebut. ReadOnlyAccess

Zona Pendaratan Akun Tunggal (SALZ): Untuk melihat kebijakan peran pengguna default, tidak disesuaikan, zona pendaratan akun tunggal AMS, lihat, selanjutnya. SALZ: Peran Pengguna IAM Default

SALZ: Peran Pengguna IAM Default

Pernyataan kebijakan JSON untuk peran pengguna landing zone akun tunggal AMS default.

> **Note**
>
> Peran pengguna default SALZ dapat disesuaikan dan mungkin berbeda berdasarkan per akun. Petunjuk untuk menemukan peran Anda disediakan.

Berikut ini adalah contoh peran pengguna SALZ default. Untuk memastikan bahwa Anda memiliki kebijakan yang ditetapkan untuk Anda, jalankan `get-role`perintah. Atau, masuk ke AWS Identity and Access Management konsol di https://console.aws.amazon.com/iam/, lalu pilih Peran.

Peran read-only pelanggan adalah kombinasi dari beberapa kebijakan. Rincian peran (JSON) mengikuti.

Kebijakan Audit Managed Services:

Kebijakan IAM ReadOnly Managed Services

Kebijakan Pengguna Managed Services

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "AllowCustomerToListTheLogBucketLogs",
     "Effect": "Allow",
     "Action": [
       "s3:ListBucket"
     ],
     "Resource": [
       "arn:aws:s3:::mc-a*-logs-*"
     ],
     "Condition": {
       "StringLike": {
         "s3:prefix": [
           "aws/*",
           "app/*",
           "encrypted",
```

```
            "encrypted/",
            "encrypted/app/*"
          ]
        }
      }
    },
    {
      "Sid": "BasicAccessRequiredByS3Console",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid": "AllowCustomerToGetLogs",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/aws/*",
        "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
      ]
    },
    {
      "Sid": "AllowAccessToOtherObjects",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCustomerToListTheLogBucketRoot",
      "Effect": "Allow",
```

```
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:prefix": [
            "",
            "/"
          ]
        }
      }
    },
    {
      "Sid": "AllowCustomerCWLConsole",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "AllowCustomerCWLAccessLogs",
      "Effect": "Allow",
      "Action": [
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:/infra/*",
        "arn:aws:logs:*:*:log-group:/app/*",
        "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
      ]
    },
    {
      "Sid": "AWSManagedServicesFullAccess",
      "Effect": "Allow",
      "Action": [
```

```
        "amscm:*",
        "amsskms:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "ModifyAWSBillingPortal",
      "Effect": "Allow",
      "Action": [
        "aws-portal:Modify*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "DenyDeleteCWL",
      "Effect": "Deny",
      "Action": [
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "DenyMCCWL",
      "Effect": "Deny",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/mc/*"
      ]
    },
    {
```

```
      "Sid": "DenyS3MCNamespace",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
        "arn:aws:s3:::mc-a*-logs-*/mc/*",
        "arn:aws:s3:::mc-a*-logs-*-audit/*",
        "arn:aws:s3:::mc-a*-internal-*/*",
        "arn:aws:s3:::mc-a*-internal-*"
      ]
    },
    {
      "Sid": "ExplicitDenyS3CfnBucket",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::cf-templates-*"
      ]
    },
    {
      "Sid": "DenyListBucketS3LogsMC",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "auditlog/*",
            "encrypted/mc/*",
            "mc/*"
          ]
        }
      }
    },
    {
      "Sid": "DenyS3LogsDelete",
```

```
      "Effect": "Deny",
      "Action": [
        "s3:Delete*",
        "s3:Put*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/*"
      ]
    },
    {
      "Sid": "DenyAccessToKmsKeysStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "kms:*"
      ],
      "Resource": [
        "arn:aws:kms::*:key/mc-*",
        "arn:aws:kms::*:alias/mc-*"
      ]
    },
    {
      "Sid": "DenyListingOfStacksStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "cloudformation:*"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/mc-*"
      ]
    },
    {
      "Sid": "AllowCreateCWMetricsAndManageDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCreateandDeleteCWDashboards",
      "Effect": "Allow",
      "Action": [
```

```
        "cloudwatch:DeleteDashboards",
        "cloudwatch:PutDashboard"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Kebijakan Bersama Manajer Rahasia Pelanggan

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
        "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
        "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
      ]
    },
   {
      "Sid": "DenyCustomerGetSecretCustomerNamespace",
      "Effect": "Deny",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    },
    {
      "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
      "Effect": "Deny",
      "NotAction": [
        "secretsmanager:Describe*",
```

```
        "secretsmanager:Get*",
        "secretsmanager:List*"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
    }
  ]
}
```

Kebijakan Berlangganan Marketplace Pelanggan

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Aturan Firewall Akses Default

Ini adalah aturan firewall default yang diperlukan untuk mengakses instance Anda.

> **Note**
>
> Untuk informasi tentang aturan firewall dan port yang diperlukan untuk membangun kepercayaan satu arah AD, lihat Panduan Keamanan AMS dengan membuka konsol AWS Artifact -> tab Laporan dan cari AWS Managed Services.

Port Instans Tumpukan Linux

Aturan ini diperlukan untuk otentikasi Anda ke tumpukan AMS Linux.

Aturan Port Instance Linux DARI: Instans Tumpukan Linux KE: Pengontrol Domain CORP

Port	Protokol	Layanan	Arahan
389	TCP	LDAP	Ingress
389	UDP	LDAP	Ingress
88	TCP	Kerberos	Ingress
88	UDP	Kerberos	Ingress

Port Instans Stack Windows

Aturan ini diperlukan untuk otentikasi Anda ke tumpukan AMS Windows.

DARI: Instans Tumpukan Windows KE: Pengontrol Domain CORP

Port	Protokol	Layanan	Arahan
88	TCP | UDP	Kerberos	Masuknya dan Jalan keluar
135	TCP | UDP	Layanan Pencari Lokasi DCE/RPC	Masuknya dan Jalan keluar
389	TCP | UDP	LDAP	Masuknya dan Jalan keluar
3268	TCP | UDP	msft-gc, Microsoft Global Catalog (layanan LDAP yang berisi data dari hutan Active Directory)	Masuknya dan Jalan keluar
445	TCP	Direktori Aktif Microsoft-DS, berbagi Windows	Masuknya dan Jalan keluar

Port	Protokol	Layanan	Arahan
49152 - 65535	TCP	Port dinamis atau pribadi yang tidak dapat didaftarkan dengan IANA. Rentang ini digunakan untuk layanan pribadi, atau khusus atau tujuan sementara dan untuk alokasi otomatis port sementara.	Masuknya dan Jalan keluar

Manajemen layanan di AWS Managed Services

Topik

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

Bagaimana layanan AMS bekerja untuk Anda.

Tata kelola akun di AWS Managed Services

Bagian ini mencakup tata kelola akun AMS.

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

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

Dimulainya layanan di AWS Managed Services

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

Dimulainya Layanan

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

Dimulainya layanan

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

Manajemen hubungan pelanggan (CRM)

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

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

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

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

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

Proses CRM

Proses CRM mencakup kegiatan-kegiatan ini:

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

Rapat CRM

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

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

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

Pengaturan Rapat CRM

AMS CSDM bertanggung jawab untuk mendokumentasikan pertemuan, termasuk:

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

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

> **Note**
>
> CSDM Anda bekerja sama dengan Anda untuk menetapkan tata kelola akun Anda.

Laporan bulanan CRM

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

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

> **Note**
>
> Selain informasi yang dijelaskan, CSDM Anda juga memberi tahu Anda tentang perubahan material dalam ruang lingkup atau ketentuan, termasuk penggunaan subkontraktor oleh AMS untuk kegiatan operasional.
> AMS menghasilkan laporan tentang penambalan dan pencadangan yang disertakan CSDM Anda dalam laporan bulanan Anda. Sebagai bagian dari sistem pembuatan laporan, AMS menambahkan beberapa infrastruktur ke akun Anda yang tidak dapat diakses oleh Anda:
>
> - Bucket S3, dengan data mentah dilaporkan
> - Contoh Athena, dengan definisi kueri untuk menanyakan data
> - Glue Crawler untuk membaca data mentah dari bucket S3

Optimalisasi biaya di AWS Managed Services

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

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

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

Kerangka kerja pengoptimalan biaya

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

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

Identifikasi jalan optimasi biaya di lingkungan yang dikelola

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

Beberapa rekomendasi pengoptimalan meliputi yang berikut ini.

Rekomendasi optimasi arsitektur:

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

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

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

EC2 rekomendasi yang berfokus pada contoh

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

Rekomendasi yang berfokus pada akun

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

Hadir untuk pelanggan dan membantu dalam perencanaan

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

Membantu dalam implementasi rekomendasi dan mengukur dampak biaya

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

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

Matriks tanggung jawab optimasi biaya

Tanggung jawab dalam optimasi biaya AMS.

Optimalisasi biaya RACI

Aktifitas	Pelanggan	AMS
Menyusun rekomendasi penghemat	I	R

Aktifitas	Pelanggan	AMS
an biaya dan menyiapkan laporan		
Menyajikan laporan penghematan biaya	C	R
Perubahan perencanaan yang terkait dengan penghematan biaya	R	C
Menilai dampak dan risiko perubahan	R	C
Meningkatkan RFCs untuk menerapkan perubahan	R	C

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

Jam layanan di AWS Managed Services

Fitur	AMS Lanjutan
	Tingkat Premium
Permintaan layanan	24/7

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

Mendapatkan bantuan di AWS Managed Services

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

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

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

Ubah mode manajemen

AWS Managed Services (AMS) menggunakan mode manajemen perubahan untuk perubahan pagar pembatas di AMS Advanced. Mode manajemen perubahan membantu Anda mempertahankan standar operasional yang tinggi untuk lingkungan, dan untuk mengendalikan risiko dan mencegah dampak buruk. AMS Advanced memiliki mode berbeda yang memberikan tingkat kontrol dan risiko yang berbeda. Semua mode, kecuali mode yang dikelola pelanggan, dikelola oleh AMS. Berikut ini adalah mode manajemen perubahan yang tersedia:

- Mode RFC (sebelumnya mode CM Standar): Menyediakan sistem “permintaan untuk perubahan” (RFC) dan jenis perubahan kustom AMS () CTs
- Mode Perubahan Langsung: Sama seperti mode RFC ditambah penggunaan AWS APIs dan konsol untuk membuat sumber daya yang dikelola AMS
- AWS Service Catalog di AMS: Mirip dengan mode Direct Change, tetapi alih-alih menggunakan sistem manajemen perubahan AMS (RFCs), Anda menggunakan AWS Service Catalog untuk membuat sumber daya yang kemudian dikelola AMS.
- Mode pengembang: Sama seperti mode Perubahan Langsung, hanya sumber daya yang Anda buat dengan AWS APIs dan konsol yang tidak dikelola AMS—Anda bertanggung jawab atas pengelolaannya
- Mode Penyediaan Layanan Mandiri (SSP): Sama seperti mode Pengembang kecuali tidak ada akses ke sistem manajemen perubahan AMS (tidak) RFCs
- Mode Terkelola Pelanggan: AMS memberi Anda landing zone landing zone multi-akun tetapi semua manajemen sumber daya adalah tanggung jawab Anda

Sistem manajemen perubahan AWS Managed Services (AMS), menggunakan Change Management (CM) API, menyediakan operasi untuk membuat dan mengelola request for change (RFCs) untuk akun multi-account landing zone (MALZ) dan single-account landing zone (SALZ).

Permintaan untuk perubahan (RFC) adalah permintaan yang dibuat oleh Anda atau AMS melalui antarmuka AMS untuk membuat perubahan pada lingkungan terkelola Anda dan menyertakan ID tipe perubahan (CT) untuk operasi tertentu.

AMS change management (CM) API menyediakan operasi untuk membuat dan mengelola permintaan untuk change (RFCs). Anda dapat membuat, memperbarui, mengirimkan, menyetujui, menolak, dan membatalkan. RFCs Operator AMS dapat membuat, memperbarui, mengirimkan, menyetujui, menolak, membatalkan, dan menandai RFCs sebagai ditutup.

Untuk daftar awalan cadangan AMS yang tidak digunakan dalam tag atau nama lain, lihat Awalan cadangan.

Untuk informasi tentang setiap jenis perubahan, termasuk skema dan contoh, lihat Referensi Jenis Perubahan AMS.

> **Note**
>
> Semua panggilan API manajemen perubahan direkam di AWS CloudTrail. Untuk informasi selengkapnya, lihat Mengakses log Anda.

Ikhtisar mode

Gunakan informasi ini untuk membantu Anda memilih mode AWS Managed Services (AMS) yang sesuai untuk hosting aplikasi Anda, berdasarkan kombinasi fleksibilitas dan tata kelola preskriptif yang Anda inginkan untuk mencapai hasil bisnis Anda.

Audiens yang dituju untuk informasi ini adalah:

- Tim pelanggan yang bertanggung jawab atas strategi dan tata kelola landing zone mereka. Informasi ini akan membantu tim menyusun fondasi landing zone yang dikelola AMS, dengan mode AMS yang ingin mereka tawarkan kepada pelanggan internal dan eksternal mereka.
- Pemilik bisnis dan aplikasi ditugaskan untuk memigrasikan aplikasi mereka ke AMS. Informasi ini akan membantu merencanakan migrasi aplikasi, dengan mode AMS yang sesuai untuk aplikasi migrate/host mereka. Catatan, aplikasi yang sama dapat di-host di lebih dari satu mode AMS selama fase siklus hidup Siklus Hidup Pengembangan Perangkat Lunak (SDLC) yang berbeda.
- Mitra AMS bertugas membimbing pelanggan tentang berbagai opsi untuk membangun dan bermigrasi ke AMS.

Informasi ini paling berguna selama fase dasar menyiapkan platform yang dikelola AMS Anda, dan ketika Anda beralih dari fondasi ke fase migrasi perjalanan adopsi cloud Anda, tepat setelah orientasi ke AMS selesai dan Anda berfokus pada tata kelola dan operasi aplikasi.

Jenis mode dan akun di AMS

Mode AWS Managed Services (AMS) dapat didefinisikan sebagai cara berinteraksi dengan layanan AMS di bawah kerangka tata kelola khusus untuk setiap mode. Perbedaan landing zone, multi-account landing zone atau MALZ dan single-account landing zone atau SALZ dicatat.

> **Note**
>
> Untuk detail tentang penerapan aplikasi dan memilih mode AMS yang tepat, lihat mode AMS dan aplikasi atau beban kerja.
> Untuk kasus penggunaan dunia nyata dari berbagai mode, lihat Kasus penggunaan dunia nyata untuk mode AMS

Tabel berikut memberikan deskripsi mode per layanan AMS.

Fitur AMS	Mode RFC (sebelumnya mode CM Standar) / OOD *	Mode Ubah Langsung	AWS Service Catalog	Penyediaan layanan mandiri/Mode pengembang	Pelanggan Dikelola
Konfigurasi Zona Pendaratan	MALZ dan SALZ	MALZ dan SALZ	MALZ dan SALZ		
Manajemen Perubahan	Mengubah penjadwalan, meninjau perubahan manual, dan mengubah catatan	Sama seperti mode RFC untuk perubahan berisiko tinggi seperti IAM atau grup keamanan	Tidak ada		
Logging, Monitorin	Ya (sumber daya yang didukung)			Tidak	

Fitur AMS	Mode RFC (sebelumnya mode CM Standar) / OOD *	Mode Ubah Langsung	AWS Service Catalog	Penyediaan layanan mandiri/Mode pengembang	Pelanggan Dikelola
g, Guardrails, dan Manajemen Acara					
Manajemen kontinuitas	Ya (sumber daya yang didukung)			Tidak berlaku/Tidak	Tidak
Manajemen keamanan	Kontrol keamanan tingkat instans dan kontrol tingkat akun			Kontrol tingkat akun	Kontrol tingkat AWS Org
Manajemen tambalan	Ya			Tidak berlaku/Tidak	Tidak
Insiden dan manajemen masalah	Respons dan resolusi SLA untuk sumber daya yang didukung AMS			Respon SLA untuk sumber daya yang dihasilkan	Tidak
Pelaporan	Ya			Tidak	
Manajemen permintaan layanan	Ya			Hanya permintaan Support	Tidak

* Operations On Demand (OOD) memiliki penawaran untuk pelanggan yang menggunakan mode RFC untuk mengelola perubahan mereka melalui sumber daya khusus. Untuk detail selengkapnya, lihat katalog penawaran Operations on Demand dan hubungi manajer pengiriman layanan cloud (CSDM) Anda.

> **Note**
>
> Mode Penyediaan Layanan Mandiri di AMSdan Mode Pengembang AMS Lanjutan mungkin keduanya tampak cocok untuk aplikasi yang memiliki arsitektur kompleks yang berakar pada Layanan AWS asli. Saat merancang beban kerja, Anda membuat trade-off antara keunggulan operasional dan kelincahan, berdasarkan konteks bisnis Anda. Ini adalah cara yang baik untuk berpikir tentang memilih mode SSP atau mode Pengembang untuk aplikasi Anda. Pemilihan juga dapat berubah berdasarkan fase SDLC aplikasi. Misalnya: Ketika aplikasi siap produksi, maka mode SSP mungkin opsi yang lebih tepat karena pagar pembatas AMS yang lebih ketat dalam mode ini. Pagar pembatas diberlakukan dalam bentuk kontrol pencegahan seperti kontrol perubahan berbasis RFC untuk pembaruan IAM dan pada tingkat OU aplikasi. SCPs Keputusan bisnis ini dapat mendorong prioritas rekayasa Anda. Anda dapat mengoptimalkan untuk meningkatkan fleksibilitas bagi pemilik aplikasi dalam fase “pra-prod” dengan mengorbankan tata kelola dan dukungan operasional.

Arsitektur MALZ dan mode AMS terkait

AMS multi-account landing zone (MALZ) memberi Anda opsi untuk secara otomatis menyediakan akun aplikasi (atau akun sumber daya) di bawah Unit Organisasi (OU) default: OU yang Dikelola Pelanggan, OU Terkelola, atau OU Pengembangan. Infrastruktur yang disediakan dalam akun aplikasi yang dibuat di bawah masing-masing OUs ini tunduk pada mode AMS spesifik yang ditawarkan oleh yayasan tersebut. OUs Adalah umum untuk menemukan campuran dua atau lebih mode di akun aplikasi yang sama. Misalnya: Mode RFC dan mode SSP dapat hidup berdampingan dalam akun terkelola AMS yang menghosting arsitektur pipeline yang terdiri dari API Gateway dan Lambda untuk fungsi pemicu, dan, S3 EC2, dan SQS untuk konsumsi dan orkestrasi. Dalam hal ini, mode SSP akan berlaku untuk Lambda dan API Gateway.

Gambar 1 menyajikan bagaimana mode yang berbeda ditawarkan melalui fondasi OUs di AMS. Saat meminta akun aplikasi baru di AMS, Anda harus memilih OU untuk akun tersebut.

Arsitektur MALZ dan mode AMS terkait

AMS memanfaatkan dasar OUs berdasarkan praktik terbaik AWS sebagai cara untuk mengelola akun secara logis menggunakan Kebijakan Kontrol Layanan ()SCPs. Ini berfungsi sebagai cara untuk menegakkan kerangka tata kelola dengan setiap mode AMS. Setiap tata kelola dan pagar pembatas keamanan (dalam bentuk SCPs) yang diterapkan pada yayasan OUs juga diterapkan

secara otomatis. custom/child OUs Tambahan SCPs dapat diminta untuk anak OUs. Penting untuk dipahami bahwa akun aplikasi tidak sama dengan mode. Mode diterapkan pada infrastruktur yang disediakan dalam akun dan menentukan tanggung jawab operasional antara AMS dan pelanggan.

Gambar 1: Arsitektur MALZ dan mode AMS terkait

> **Note**
>
> “Pembatasan” menyiratkan bahwa Anda dapat meminta kebijakan khusus untuk ini OUs, kebijakan tersebut disetujui oleh AMS atas case-by-case dasar untuk memastikan kebijakan tersebut tidak mengganggu kemampuan AMS untuk memberikan keunggulan operasional. Untuk daftar rinci pagar pembatas AMS, lihat AMS Guardrails di panduan pengguna.

Mode dan aplikasi AMS atau beban kerja

Pertimbangkan persyaratan operasional dan tata kelola untuk aplikasi Anda saat memilih mode yang tepat, baik dengan meminta akun aplikasi baru atau menghosting aplikasi di akun aplikasi yang ada. Pemilihan mode AMS yang sesuai untuk setiap aplikasi atau beban kerja tergantung pada faktor-faktor berikut:

- Jenis fungsi siklus hidup SDLC yang akan disediakan lingkungan (misalnya, kotak pasir dengan perubahan yang tidak dimoderasi, UAT dengan beberapa perubahan yang sering, produksi dengan perubahan minimal dan sangat diatur)
- Kebijakan tata kelola yang diperlukan (ditegakkan melalui SCPs di tingkat OU)
- Model Operasional (jika Anda ingin memiliki tanggung jawab operasional atau ingin mengalihdayakannya ke AMS)
- Hasil bisnis yang diinginkan, seperti waktu untuk beroperasi di cloud, dan biaya operasi.

> **Note**
>
> Untuk deskripsi jenis mode per layanan AMS, lihat Jenis mode dan akun di AMS.
> Untuk kasus penggunaan dunia nyata dari berbagai mode, lihat Kasus penggunaan dunia nyata untuk mode AMS

Tabel berikut menguraikan pertimbangan utama bagi pemilik aplikasi untuk membantu memutuskan mode AMS yang paling sesuai. Pemilik aplikasi harus menyertakan fase penilaian sebelum migrasi aplikasi untuk sepenuhnya memahami mode mana yang berlaku untuk aplikasi spesifik mereka. Contoh: Untuk aplikasi berbasis layanan cloud-native atau arsitektur tanpa server, opsi terbaik adalah mulai membangun dan mengulangi dalam mode Pengembang dan menerapkan Infrastruktur akhir sebagai Kode menggunakan mode AMS Managed — SSP. Dalam hal ini, pemfaktoran ulang ringan mungkin diperlukan untuk memastikan bahwa CloudFormation templat apa pun yang dibuat untuk penerapan otomatis memenuhi pedoman konsumsi yang ditetapkan oleh AMS. Selain itu, izin IAM apa pun harus disetujui oleh AMS Security untuk memastikan mereka mengikuti model hak istimewa paling sedikit.

Mode AMS yang dipilih untuk meng-host aplikasi, dapat membantu Anda membangun model operasi cloud yang Anda inginkan.

> **Note**
>
> Lebih dari satu model operasi cloud dapat ada dalam satu Zona Pendaratan Terkelola AMS berdasarkan berbagai mode AMS yang dipilih untuk meng-host aplikasi.

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
Kesiapan operasional						
Logging, Monitoring dan Manajemen Acara	AMS bertanggung jawab atas semua infrastruktur yang dikelola			Pelanggan yang bertanggung jawab atas Layanan Penyediaan Layanan Mandiri (SSP)	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar	Pelanggan yang bertanggung jawab

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
					sistem AMS CM	
Manajemen Kontinuitas	Tanggung jawab AMS untuk melaksanakan rencana cadangan yang dipilih oleh pelanggan			Pelanggan yang bertanggung jawab atas Layanan Penyediaan Layanan Mandiri (SSP)	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar sistem AMS CM	
Manajemen Akses Tingkat Instans	Dikelola AMS melalui kepercayaan AD satu arah dengan domain on-prem. Memerlukan infrastruktur terkelola untuk bergabung dengan domain AMS			Tidak berlaku	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar sistem AMS CM	

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
Manajemen Keamanan dan Manajemen Akses Tingkat Akun	Tanggung jawab AMS untuk semua akun terkelola			AMS bertanggung jawab atas semua akun yang dikelola	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar sistem AMS CM	
Manajemen Patch	Tanggung jawab AMS untuk semua akun terkelola			Pelanggan yang bertanggung jawab atas Layanan Penyediaan Layanan Mandiri (SSP)	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar sistem AMS CM	

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
Manajemen Perubahan	Tanggung jawab AMS untuk semua akun terkelola			Pelanggan yang bertanggung jawab atas Layanan Penyediaan Layanan Mandiri (SSP)	Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar sistem AMS CM	
Manajemen Penyediaan	Preskriptif dan standar untuk opsi penyediaan yang ditawarkan di AMS	Fleksibilitas untuk langsung menggunakan AWS service API untuk AWS Service Catalog mengikuti standar preskriptif AMS	Fleksibilitas untuk langsung menggunakan AWS service API mengikuti standar preskriptif AMS	Fleksibilitas untuk langsung menggunakan layanan AWS APIs untuk layanan SSP	Fleksibilitas untuk langsung menggunakan AWS service API untuk penyediaan	

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
Manajemen Insiden dan Audit	Tanggung jawab AMS untuk semua akun terkelola				Pelanggan bertanggung jawab atas sumber daya yang disediakan menggunakan peran IAM pengembang di luar AMS Change Management System	
GuardRails Infrastruktur Bersama (Jaringan) dan Kerangka Keamanan	Memanfaatkan Akun Inti AMS yang preskriptif dan standar					Memanfaatkan Akun Inti AMS yang fleksibel dan dipesan lebih dahulu
Kesiapan aplikasi						

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
Aplikasi refactoring	Diperlukan refactoring ringan				Diperlukan refactoring ringan (jika disediakan menggunakan AMS Standard CM)	Tidak perlu refactoring
Support untuk layanan AWS	Terbatas pada apa yang didukung oleh AMS					Tidak terbatas
Pertimbangan bisnis						
Saatnya kesiapan operasional	Tiga sampai enam bulan			6 bulan+tergantung pada kompetensi operasi aplikasi pelanggan		6-18 bulan tergantung pada infrastruktur pelanggan dan kompetensi operasi aplikasi
Biaya	$$$$			$$$	$$	$

Masalah keputusan	Mode CM standar/OOD *	AWS Service Catalog	Mode Ubah Langsung	Penyediaan layanan mandiri	Mode pengembang	Pelanggan Dikelola
Contoh aplikasi	Server web dengan tumpukan 3 tingkat, aplikasi dengan kepatuhan dan persyaratan peraturan			Server web menggunakan API Gateway, aplikasi kontainer yang memanfaatkan ECS/EKS	Mengiterasi/mengoptimalkan aplikasi Data Lake yang menggunakan Lambda, Glue, Athena, dll	De-sentralisasi accounts/applications seperti kotak pasir, aplikasi yang dikelola pihak ketiga

* Operations On Demand (OOD) memiliki penawaran untuk pelanggan yang menggunakan mode CM Standar untuk mengelola perubahan mereka melalui sumber daya khusus. Untuk detail selengkapnya, lihat katalog penawaran Operations on Demand dan hubungi manajer pengiriman layanan cloud (CSDM) Anda.

> **Note**
>
> Perbandingan harga antara mode SSP dan mode Pengembang mengasumsikan bahwa layanan AWS yang sama disediakan.

Membandingkan Mode AMS dengan tujuan bisnis dan TI

Seperti yang ditunjukkan, jika Anda mencari model tata kelola yang sangat terkontrol dan terstandarisasi untuk aplikasi Anda, maka mode Perubahan Standar yang dikelola AMS, AWS Service Catalog, atau Direct Change adalah yang paling cocok. Jika Anda memerlukan model tata kelola yang dipesan lebih dahulu dengan fokus pada inovasi aplikasi tanpa perlu kesiapan operasional, pilih mode Customer Managed. Dengan mode Customer Managed, Anda bisa membutuhkan waktu lebih lama untuk mengoperasionalkan aplikasi Anda karena Anda memikul tanggung jawab untuk menetapkan orang, proses, dan alat untuk mendukung kemampuan

operasional seperti Manajemen Insiden, Manajemen Konfigurasi, Manajemen Penyediaan, Manajemen Keamanan, Manajemen Patch, dll.

Kasus penggunaan dunia nyata untuk mode AMS

Periksa ini untuk membantu menentukan cara menggunakan mode AMS.

- Gunakan Kasus 1, keharusan bisnis untuk menurunkan biaya dengan keluar pusat data yang sensitif terhadap waktu: Perusahaan dengan acara bisnis yang menarik, seperti pintu keluar pusat data, tertarik untuk menghosting ulang aplikasi on-prem mereka di cloud. Sebagian besar inventaris on-prem terdiri dari server Windows dan Linux dengan campuran versi sistem operasi. Dengan melakukan itu, pelanggan juga ingin memanfaatkan penghematan biaya yang pindah ke penawaran cloud dan meningkatkan postur teknis dan keamanan aplikasi mereka. Pelanggan ingin bergerak cepat tetapi belum memiliki keahlian operasi cloud internal yang dibangun. Pelanggan harus menemukan keseimbangan refactoring, terlalu banyak refactoring dapat berisiko terhadap garis waktu yang ketat. Namun, dengan beberapa refactoring, seperti memperbarui versi OS dan mengoptimalkan database, aplikasi dapat mencapai tingkat kinerja berikutnya. Dalam contoh ini, pelanggan dapat memilih mode RFC yang dikelola AMS untuk meng-host kembali sebagian besar aplikasi mereka. AMS menyediakan operasi infrastruktur, sekaligus memandu tim operasi pelanggan tentang praktik terbaik dalam pengoperasian cloud dengan aman.

  AWS Service Catalog yang dikelola AMS dan mode Perubahan Langsung yang dikelola AMS memberi pelanggan fleksibilitas ekstra sambil mencapai hasil dan sasaran bisnis yang sama. Selain itu, pelanggan dapat menggunakan penawaran AMS Operations On Demand (OOD) untuk memiliki insinyur operasi AMS khusus untuk memprioritaskan pelaksanaan permintaan perubahan ()RFCs.

  Saat membongkar tugas operasional infrastruktur yang tidak terdiferensiasi (patching, backup, manajemen akun, dll) ke AMS, pelanggan dapat terus fokus pada pengoptimalan aplikasi mereka dan meningkatkan tim internal mereka pada operasi cloud. AMS memberikan laporan bulanan kepada pelanggan tentang penghematan biaya, dan membuat rekomendasi tentang pengoptimalan sumber daya. Dalam kasus penggunaan ini, jika ada end-of-life aplikasi yang di-host pada versi OS lama seperti Windows 2003 dan 2008, bahwa pelanggan memutuskan untuk tidak memfaktorkan ulang, itu juga dapat dimigrasikan ke AMS dan dihosting di akun yang memanfaatkan mode Dikelola Pelanggan.
- Gunakan Kasus 2, membangun data lake dengan Lambda, Glue, Athena dalam batas AMS yang aman: Perusahaan ingin menyiapkan Data Lake untuk memenuhi kebutuhan pelaporan untuk beberapa aplikasi di AMS. Pelanggan ingin menggunakan bucket S3 untuk penyimpanan

kumpulan data dan AWS Athena untuk melakukan kueri terhadap kumpulan data untuk setiap laporan. S3 dan AWS Athena akan digunakan di akun AMS Managed terpisah. Akun dengan S3 juga memiliki layanan lain seperti Glue, Lambda, dan Step Functions untuk membangun pipeline konsumsi data. Glue, Lambda, Athena, dan Step Functions dianggap sebagai layanan Penyediaan Layanan Mandiri (SSP) dalam hal ini. Pelanggan juga menyebarkan EC2 instance di akun yang bertindak sebagai server ad hoc tooling/scripting . Pelanggan memulai dengan meminta AMS untuk mengaktifkan layanan SSP di akun AMS Managed mereka. AMS memberikan peran IAM untuk setiap layanan yang dapat diasumsikan oleh pelanggan, setelah peran tersebut dimasukkan ke dalam solusi federasi pelanggan. Untuk kemudahan manajemen, pelanggan juga dapat menggabungkan kebijakan untuk peran IAM terpisah menjadi satu peran khusus, sehingga mengurangi kebutuhan untuk beralih peran saat bekerja di antara layanan AWS. Setelah peran diaktifkan di akun, pelanggan dapat mengonfigurasi layanan sesuai kebutuhan mereka. Namun, pelanggan harus bekerja dengan sistem manajemen perubahan AMS untuk meminta izin tambahan, tergantung pada kasus penggunaannya.

Misalnya, untuk akses ke Glue Crawler, izin tambahan diperlukan oleh Glue. Izin tambahan juga akan diperlukan untuk membuat sumber acara untuk Lambda. Pelanggan akan bekerja dengan AMS untuk memperbarui peran IAM guna memungkinkan akses lintas akun bagi Athena untuk menanyakan bucket S3. Pembaruan untuk peran layanan atau peran terkait layanan juga akan diperlukan melalui manajemen perubahan AMS agar Lambda memanggil layanan Step Functions, dan Glue untuk membaca dan menulis ke semua bucket S3. AMS bekerja dengan pelanggan untuk memastikan bahwa model akses hak istimewa paling sedikit diikuti dan perubahan IAM yang diminta tidak terlalu permisif dan membuka lingkungan terhadap risiko yang tidak perlu. Tim data lake pelanggan menghabiskan waktu merencanakan semua izin IAM yang diperlukan untuk layanan khusus untuk arsitektur pelanggan dan meminta AMS untuk mengaktifkannya. Ini karena semua perubahan IAM diproses secara manual dan menjalani peninjauan dari tim AMS Security. Waktu untuk memproses permintaan ini harus diperhitungkan dalam jadwal penerapan aplikasi.

Karena layanan SSP beroperasi di akun, pelanggan dapat meminta dukungan dan melaporkan masalah melalui manajemen insiden AMS dan permintaan layanan. Namun, AMS tidak akan secara aktif memantau metrik kinerja dan konkurensi untuk Lambda, atau metrik pekerjaan untuk Glue. Adalah tanggung jawab pelanggan untuk memastikan pencatatan dan pemantauan yang tepat diaktifkan untuk layanan SSP. EC2 Instance dan bucket S3 di akun dikelola sepenuhnya oleh AMS.

- Gunakan Kasus 3, penyiapan pipeline penerapan CICD yang cepat dan fleksibel di AMS: Seorang pelanggan ingin menyiapkan pipeline CICD berbasis Jenkins untuk menyebarkan pipeline kode ke semua akun aplikasi di AMS. Pelanggan mungkin merasa paling cocok untuk meng-host pipeline

CICD ini dalam mode Perubahan Langsung (DCM) yang dikelola AMS atau mode Pengembang yang dikelola AMS karena memberi mereka fleksibilitas untuk mengatur server Jenkins dengan konfigurasi khusus yang diperlukan EC2, dengan izin IAM yang diinginkan untuk mengakses dan ember S3 yang menampung repositori artefak. CloudFormation Meskipun ini juga dapat dilakukan dalam mode RFC yang dikelola AMS, tim pelanggan perlu membuat beberapa manual untuk peran IAM RFCs untuk mengulangi set izin yang disetujui yang paling tidak permisif, yang ditinjau secara manual oleh AMS. DCM memungkinkan pelanggan untuk mencapai tujuan operasional mereka di AWS sambil menghindari kebutuhan untuk membuat beberapa manual RFCs untuk peran IAM, saat menggunakan mode RFC yang dikelola AMS, untuk mengulangi serangkaian izin yang disetujui yang paling tidak permisif, yang ditinjau secara manual oleh AMS. Ini akan membutuhkan waktu serta pendidikan di pihak pelanggan untuk meningkatkan proses dan alat AMS. Bekerja dengan mode Pengembang, pelanggan dapat memulai dengan “peran pengembang” untuk menyediakan infrastruktur menggunakan AWS asli APIs. Cara tercepat dan paling fleksibel untuk mengatur pipeline ini adalah dengan menggunakan mode AMS Managed-Developer. Mode pengembang memberikan cara tercepat dan termudah, sambil mengorbankan integrasi operasional, sementara DCM kurang fleksibel tetapi memberikan tingkat dukungan operasional yang sama dengan mode RFC.

- Gunakan Kasus 4, model operasi yang dipesan lebih dahulu dalam yayasan AMS: Seorang pelanggan melihat keluar pusat data berdasarkan tenggat waktu dan salah satu aplikasi perusahaan mereka sepenuhnya dikelola oleh MSP pihak ketiga, termasuk operasi aplikasi dan operasi infrastruktur. Dengan asumsi bahwa pelanggan tidak memiliki waktu dalam jadwal untuk memfaktorkan ulang aplikasi ini sehingga dapat dioperasikan oleh AMS, mode Customer Managed adalah opsi yang cocok. Pelanggan dapat memanfaatkan pengaturan otomatis dan cepat dari Zona Pendaratan yang dikelola AMS. Mereka dapat memanfaatkan manajemen akun terpusat yang mengontrol penjual akun dan konektivitas melalui akun jaringan terpusat. Ini juga menyederhanakan penagihan mereka dengan mengkonsolidasikan biaya untuk semua akun yang dikelola pelanggan melalui akun Pembayar AMS. Pelanggan memiliki fleksibilitas untuk mengatur model manajemen akses yang dipesan lebih dahulu dengan MSP terpisah dari manajemen akses standar yang digunakan untuk akun Terkelola AMS. Dengan cara ini, menggunakan mode Customer Managed, mereka dapat mengatur lingkungan yang dikelola AMS sambil memenuhi persyaratan bisnis mereka untuk mengosongkan lingkungan di prem mereka. Dalam hal ini, jika pelanggan juga memiliki aplikasi berbasis Windows yang mereka migrasi ke cloud, dan memilih untuk memindahkannya ke akun Customer Managed, pelanggan bertanggung jawab untuk membuat model operasi cloud. Ini bisa rumit, mahal, dan memakan waktu tergantung pada kemampuan pelanggan untuk mengubah proses TI tradisional dan melatih orang. Pelanggan dapat

menghemat waktu dan biaya dengan “mengangkat dan memindahkan” beban kerja tersebut ke akun AMS Managed dan menurunkan operasi infrastruktur ke AMS.

> **Note**
>
> Pelanggan terkadang merasa perlu untuk memindahkan akun aplikasi antara kerangka tata kelola mode RFC atau SSP dan mode Pengembang. Misalnya, pelanggan dapat meng-host aplikasi dalam mode terkelola AMS sebagai bagian dari migrasi lift dan shift awal, tetapi lembur ingin menulis ulang aplikasi untuk mengoptimalkannya untuk layanan AWS cloud-native. Mereka dapat mengubah mode akun pra-prod dari RFC yang dikelola AMS ke mode Pengembang yang dikelola AMS, memberi mereka fleksibilitas dan kelincahan untuk penyediaan infrastruktur. Namun, setelah perubahan penyediaan infrastruktur dibuat menggunakan “peran pengembang”, infrastruktur yang sama tidak dapat dipindahkan kembali ke mode RFC yang dikelola AMS. Ini karena AMS tidak dapat menjamin operasi infrastruktur yang disediakan di luar sistem manajemen perubahan AMS. Pelanggan mungkin perlu membuat akun aplikasi baru yang menawarkan mode RFC yang dikelola AMS dan kemudian menerapkan kembali konfigurasi infrastruktur yang “dioptimalkan” melalui CloudFormation templat atau kustom yang dimasukkan ke dalam akun yang dikelola AMS AMIs . Ini adalah cara bersih untuk menerapkan konfigurasi siap produksi. Setelah digunakan, aplikasi akan berada di bawah tata kelola dan operasi AMS preskriptif. Hal yang sama berlaku untuk beralih mode antara mode Customer Managed dan AMS-managed.

Modus RFC

Mode RFC adalah mode default untuk pelanggan rencana operasi AMS Advanced. Ini mencakup sistem manajemen perubahan dengan permintaan perubahan atau RFCs dan katalog jenis perubahan yang akan digunakan untuk meminta penambahan atau perubahan yang Anda butuhkan ke akun Anda. Sistem manajemen perubahan ini memberikan tingkat keamanan dalam membatasi siapa yang dapat melakukan perubahan pada akun Anda.

Untuk detail tentang jenis perubahan AMS Advanced, lihat Apa itu Jenis Perubahan AMS? .

Untuk detail tentang orientasi ke AMS Advanced, lihat AWS Managed Services Onboarding Introduction.

Untuk contoh penelusuran jenis perubahan, lihat bagian “Informasi Tambahan” untuk jenis perubahan yang relevan di bagian AMS Advanced Change Type Reference Change Type by Classification.

> **Note**
>
> Mode RFC sebelumnya disebut “Mode Manajemen Ubah” atau “Mode CM Standar.”

Topik

- Pelajari tentang RFCs
- Apa itu jenis perubahan?
- Memecahkan masalah kesalahan RFC di AMS

Pelajari tentang RFCs

Permintaan perubahan, atau RFCs, bekerja dengan cara dua kali lipat. Pertama, ada parameter yang diperlukan untuk RFC itu sendiri. Ini adalah opsi di `CreateRfc` API. Dan kedua, ada parameter yang diperlukan untuk aksi RFC (parameter eksekusi). Untuk mempelajari `CreateRfc` opsi, lihat CreateRfcbagian Referensi AMS API. Opsi ini biasanya muncul di area Konfigurasi tambahan pada halaman Buat RFC.

Anda dapat membuat dan mengirimkan RFC dengan `CreateRfc` API, `aws amscm create-rfc` CLI, atau menggunakan konsol AMS Buat halaman RFC. Untuk tutorial tentang membuat RFC, lihatBuat RFC.

Topik

- Apa itu RFCs?
- Mengautentikasi saat menggunakan AMS API/CLI
- Memahami ulasan keamanan RFC
- Memahami klasifikasi tipe perubahan RFC
- Memahami tindakan RFC dan status aktivitas
- Memahami kode status RFC
- Memahami pembaruan RFC CTs dan deteksi drift CloudFormation template
- Jadwal RFCs
- Menyetujui atau menolak RFCs

- Minta periode berjalan terbatas RFC
- Buat, kloning, perbarui, temukan, dan batalkan RFCs
- Gunakan konsol AMS dengan RFCs
- Pelajari tentang parameter RFC umum
- Mendaftar untuk email harian RFC

Apa itu RFCs?

Permintaan perubahan, atau RFC, adalah cara Anda membuat perubahan di lingkungan yang dikelola AMS, atau meminta AMS untuk membuat perubahan atas nama Anda. Untuk membuat RFC, Anda memilih dari jenis perubahan AMS, pilih parameter RFC (seperti jadwal), lalu kirimkan permintaan menggunakan konsol AMS atau perintah CreateRfcAPI dan. SubmitRfc

RFC berisi dua spesifikasi, satu untuk RFC itu sendiri, dan satu untuk parameter tipe perubahan (CT). Pada baris perintah, Anda dapat menggunakan perintah Inline RFC, atau CreateRfc template standar dalam format JSON, yang Anda isi dan kirimkan bersama dengan file skema CT JSON yang Anda buat (berdasarkan parameter CT). Nama CT adalah deskripsi informal dari CT. CSIO (kategori, subkategori, item, operasi) adalah deskripsi yang lebih formal dari CT. Hanya ID CT yang harus ditentukan saat membuat RFC.

AMS memberi tahu Anda ketika perubahan telah berhasil diselesaikan (Sukses) atau tidak berhasil (Kegagalan).

> **Note**
>
> Untuk informasi tentang pemecahan masalah kegagalan RFC, lihat. Memecahkan masalah kesalahan RFC di AMS

Grafik berikut menggambarkan alur kerja RFC yang dikirimkan oleh Anda.

Mengautentikasi saat menggunakan AMS API/CLI

Saat Anda menggunakan AMS API/CLI, Anda harus mengautentikasi dengan kredensi sementara. Untuk meminta kredensil keamanan sementara untuk pengguna federasi, cal,, AssumeRoleWithSALL GetFederationTokenAssumeRole, atau AssumeRoleWithWebIdentityAWS security token service (STS). APIs

Pilihan umum adalah SAFL. Setelah disiapkan, Anda menambahkan argumen ke setiap operasi yang Anda panggil. Sebagai contoh: `aws --profile saml amscm list-change-type-categories`.

Pintasan untuk profil SAFL 2.0 adalah mengatur variabel profil di awal masing-masing API/CLI dengan `set AWS_DEFAULT_PROFILE=saml` (untuk Windows; untuk Linux itu akan`export AWS_DEFAULT_PROFILE=saml`). Untuk informasi tentang menyetel variabel lingkungan CLI, lihat Mengonfigurasi Antarmuka Baris Perintah AWS, Variabel Lingkungan.

Memahami ulasan keamanan RFC

Proses persetujuan manajemen perubahan AWS Managed Services (AMS) memastikan bahwa kami melakukan tinjauan keamanan terhadap perubahan yang kami buat di akun Anda.

AMS mengevaluasi semua permintaan untuk perubahan (RFCs) terhadap standar teknis AMS. Setiap perubahan yang mungkin menurunkan postur keamanan akun Anda dengan menyimpang dari standar teknis, akan melalui tinjauan keamanan. Selama tinjauan keamanan, AMS menyoroti risiko yang relevan dan, dalam kasus risiko keamanan tinggi atau sangat tinggi, petugas keamanan resmi Anda menerima atau menolak RFC. Semua perubahan juga dievaluasi untuk menilai dampak buruk pada kemampuan AMS untuk beroperasi. Jika potensi dampak buruk ditemukan, maka tinjauan dan persetujuan tambahan diperlukan dalam AMS.

Standar teknis AMS

Standar Teknis AMS menentukan kriteria keamanan minimum, konfigurasi, dan proses untuk menetapkan keamanan dasar akun Anda. Standar ini harus diikuti oleh AMS dan Anda.

Setiap perubahan yang berpotensi menurunkan postur keamanan akun Anda dengan menyimpang dari standar teknis, akan melalui proses Penerimaan Risiko, di mana risiko yang relevan disorot oleh AMS dan diterima atau ditolak oleh petugas keamanan yang berwenang dari pihak Anda. Semua perubahan tersebut juga dievaluasi untuk menilai apakah akan ada dampak buruk pada kemampuan AMS untuk mengoperasikan akun dan, jika demikian, ulasan dan persetujuan tambahan diperlukan dalam AMS.

Proses manajemen risiko keamanan pelanggan (CSRM) RFC

Ketika seseorang dari organisasi Anda meminta perubahan pada lingkungan terkelola Anda, AMS meninjau perubahan tersebut untuk menentukan apakah permintaan tersebut dapat memperburuk postur keamanan akun Anda dengan berada di luar standar teknis. Jika permintaan menurunkan

postur keamanan akun, AMS memberi tahu kontak tim keamanan Anda dengan risiko yang relevan, dan mengeksekusi perubahan; atau, jika perubahan tersebut menimbulkan risiko keamanan yang tinggi atau sangat tinggi di lingkungan, AMS meminta persetujuan eksplisit dari kontak tim keamanan Anda dalam bentuk penerimaan risiko (dijelaskan selanjutnya). Proses Penerimaan Risiko Pelanggan AMS dirancang untuk:

- Memastikan risiko diidentifikasi dan dikomunikasikan dengan jelas kepada pemilik yang tepat
- Minimalkan risiko yang teridentifikasi terhadap lingkungan Anda
- Mendapatkan dan mendokumentasikan persetujuan dari kontak keamanan yang ditunjuk yang memahami profil risiko organisasi Anda
- Mengurangi overhead operasional yang sedang berlangsung untuk risiko yang teridentifikasi

Cara mengakses standar teknis dan risiko tinggi atau sangat tinggi

Kami telah membuat dokumentasi Standar Teknis AMS tersedia untuk referensi Anda dalam https://console.aws.amazon.com/artifact/sebagai laporan. Gunakan dokumentasi Standar Teknis AMS untuk memahami apakah perubahan akan memerlukan penerimaan risiko dari kontak keamanan resmi Anda sebelum mengirimkan permintaan perubahan (RFC).

Temukan laporan Standar Teknis dengan menelusuri “Standar Teknis AWS Managed Services (AMS)” di bilah pencarian tab AWS Artifact Laporan setelah masuk dengan default AWSManagedServicesChangeManagementRole.

> **Note**
>
> Dokumen standar teknis AMS dapat diakses oleh Customer_ ReadOnly _Role di landing zone akun tunggal. Di landing zone multi-akun, yang AWSManaged ServicesAdminRole digunakan oleh admin keamanan dan AWSManaged ServicesChangeManagementRole digunakan oleh tim aplikasi, dapat digunakan untuk mengakses dokumen. Jika tim Anda menggunakan peran kustom, buat Other | Other RFC untuk meminta akses dan kami akan memperbarui peran kustom yang ditentukan.

Memahami klasifikasi tipe perubahan RFC

Jenis perubahan yang Anda gunakan saat mengirimkan RFC dibagi menjadi dua kategori besar:

- Deployment: Klasifikasi ini untuk membuat sumber daya.

- Manajemen: Klasifikasi ini untuk memperbarui atau menghapus sumber daya. Kategori Manajemen juga berisi jenis perubahan untuk mengakses instance, mengenkripsi atau berbagi, dan memulai, menghentikan AMIs, me-reboot, atau menghapus tumpukan.

Memahami tindakan RFC dan status aktivitas

`RfcActionState`(API)/Status Aktivitas (konsol) membantu Anda memahami status intervensi manusia, atau tindakan, pada RFC. Digunakan terutama untuk manual RFCs, `RfcActionState` membantu Anda memahami kapan ada tindakan yang diperlukan oleh Anda atau operasi AMS, dan membantu Anda melihat kapan Operasi AMS secara aktif mengerjakan RFC Anda. Ini memberikan peningkatan transparansi ke dalam tindakan yang diambil pada RFC selama siklus hidupnya.

`RfcActionState`Definisi (API)/Status Aktivitas (konsol):

- AwsOperatorAssigned: Operator AWS secara aktif mengerjakan RFC Anda.
- AwsActionPending: Respons atau tindakan dari AWS diharapkan.
- CustomerActionPendingRespons atau tindakan dari pelanggan diharapkan.
- NoActionPending: Tidak ada tindakan yang diperlukan dari AWS atau pelanggan.
- NotApplicable: Status ini tidak dapat diatur oleh operator AWS atau pelanggan, dan hanya digunakan untuk RFCs yang dibuat sebelum fungsionalitas ini dirilis.

Status tindakan RFC berbeda tergantung pada apakah jenis perubahan yang dikirimkan memerlukan peninjauan manual dan penjadwalan disetel ke ASAP atau tidak.

- ActionStatePerubahan RFC selama peninjauan, persetujuan, dan dimulainya jenis perubahan manual dengan penjadwalan yang ditangguhkan:
  - Setelah Anda mengirimkan manual, terjadwal, RFC, ActionStatesecara otomatis berubah AwsActionPendinguntuk menunjukkan bahwa operator perlu meninjau dan menyetujui RFC.
  - Ketika operator mulai secara aktif meninjau RFC Anda, ActionStateperubahan menjadi. AwsOperatorAssigned
  - Ketika operator menyetujui RFC Anda, Status RFC berubah menjadi Terjadwal, dan ActionStatesecara otomatis berubah menjadi. NoActionPending
  - Ketika waktu mulai yang dijadwalkan dari RFC tercapai, Status RFC berubah menjadi InProgress, dan ActionStatesecara otomatis berubah AwsActionPendinguntuk menunjukkan bahwa operator perlu ditugaskan untuk meninjau RFC.

- Ketika operator mulai aktif menjalankan RFC, mereka mengubah ActionStateke AwsOperatorAssigned.
- Setelah selesai, Operator menutup RFC. Ini secara otomatis mengubah ActionStateke NoActionPending.

> ⚠ Important
>
> - Status tindakan tidak dapat diatur oleh Anda. Mereka diatur secara otomatis berdasarkan perubahan dalam RFC, atau diatur secara manual oleh operator AMS.
> - Jika Anda menambahkan korespondensi ke RFC, secara otomatis ActionStatediatur ke. AwsActionPending
> - Ketika RFC dibuat, secara otomatis ActionStatediatur ke NoActionPending.
> - Ketika RFC dikirimkan, secara otomatis ActionStatediatur ke AwsActionPending.
> - Ketika RFC Ditolak, Dibatalkan, atau dilengkapi dengan status Sukses atau Kegagalan, secara otomatis ActionStatediatur ulang ke. NoActionPending
> - Status tindakan diaktifkan untuk otomatis dan manual RFCs, tetapi sebagian besar penting untuk manual RFCs karena jenis tersebut RFCs sering memerlukan komunikasi.

Tinjau contoh kasus penggunaan status tindakan RFC

Kasus Penggunaan: Visibilitas pada Proses RFC Manual

- Setelah Anda mengirimkan RFC manual, status tindakan RFC secara otomatis berubah `AwsActionPending` untuk menunjukkan bahwa operator perlu meninjau dan menyetujui RFC. Ketika operator mulai secara aktif meninjau RFC Anda, status tindakan RFC berubah menjadi. `AwsOperatorAssigned`
- Pertimbangkan RFC manual yang telah disetujui dan dijadwalkan dan siap untuk mulai berjalan. Setelah status RFC berubah`InProgress`, status tindakan RFC secara otomatis berubah menjadi. `AwsActionPending` Ini berubah lagi menjadi `AwsOperatorAssigned` setelah operator mulai aktif menjalankan RFC.
- Ketika RFC manual selesai (ditutup sebagai “Sukses” atau “Kegagalan”), status Tindakan RFC berubah `NoActionPending` untuk menunjukkan bahwa tidak ada tindakan lebih lanjut yang diperlukan baik dari pelanggan atau operator.

Kasus penggunaan: korespondensi RFC

- Ketika RFC manual`Pending Approval`, Operator AMS mungkin memerlukan informasi lebih lanjut dari Anda. Operator akan memposting korespondensi ke RFC dan mengubah status tindakan RFC menjadi. `CustomerActionPending` Saat Anda merespons dengan menambahkan korespondensi RFC baru, status tindakan RFC secara otomatis berubah menjadi. `AwsActionPending`
- Ketika RFC otomatis atau manual gagal, Anda dapat menambahkan korespondensi ke detail RFC, menanyakan kepada Operator AMS mengapa RFC gagal. Ketika korespondensi Anda ditambahkan, status tindakan RFC secara otomatis diatur ke. `AwsActionPending` Saat operator AMS mengambil RFC untuk melihat korespondensi Anda, status tindakan RFC berubah menjadi. `AwsOperatorAssigned` Ketika operator merespons dengan menambahkan korespondensi RFC baru, status tindakan RFC dapat diatur`CustomerActionPending`, menunjukkan bahwa ada respons lain dari pelanggan yang diharapkan, atau ke`NoActionPending`, yang menunjukkan bahwa tidak ada respons dari pelanggan yang diperlukan atau diharapkan.

Memahami kode status RFC

Kode status RFC membantu Anda melacak permintaan Anda. Anda dapat mengamati kode status ini selama RFC berjalan di output CLI, atau dengan menyegarkan halaman daftar RFC di konsol.

Anda juga dapat melihat kode untuk RFC di halaman detail untuk RFC itu, yang mungkin terlihat seperti ini:

Anda mungkin melihat RFC dalam daftar yang tidak Anda kirimkan. Ketika operator AMS menggunakan CT internal saja, mereka mengirimkannya dalam RFC dan ditampilkan dalam daftar RFC Anda. Untuk informasi selengkapnya, lihat Jenis perubahan hanya internal.

> **Important**
>
> Anda dapat meminta pemberitahuan perubahan status RFC. Untuk detailnya, lihat Pemberitahuan Perubahan Status RFC.

Kode status RFC

Berhasil	Kegagalan
Pengeditan: RFC telah dibuat tetapi tidak dikirimkan PendingApproval /Dikirim: RFC telah diserahkan dan sistem menentukan apakah memerlukan persetujuan, dan mendapatkan persetujuan itu, jika diperlukan Disetujui oleh AWS/Disetujui oleh pelanggan : RFC telah disetujui. Otomatis RFCs disetujui oleh AWS, manual RFCs disetujui oleh Operator dan, terkadang, pelanggan Dijadwalkan: RFC telah lulus sintaks dan pemeriksaan persyaratan dan dijadwalkan untuk berjalan InProgress: RFC sedang dijalankan, perhatikan RFCs bahwa penyediaan banyak sumber daya atau telah berjalan lama UserData, membutuhkan waktu lebih lama untuk dijalankan Dieksekusi: RFC telah dijalankan Sukses/Berhasil: RFC telah berhasil diselesaikan	Ditolak: ditolak RFCs biasanya karena gagal validasi; misalnya, sumber daya yang tidak dapat digunakan, yaitu subnet, ditentukan Dibatalkan: RFCs biasanya dibatalkan karena tidak lulus validasi sebelum waktu mulai yang dikonfigurasi berlalu Kegagalan: RFC telah gagal; lihat output untuk alasan kegagalan, dan operasi AMS secara otomatis membuat tiket masalah dan berkomunikasi dengan Anda sesuai kebutuhan StatusReason

> **Note**
>
> Dibatalkan atau ditolak RFCs dapat dikirimkan kembali menggunakan UpdateRfc; lihat juga. Perbarui RFCs

Jika RFC melewati semua kondisi yang diperlukan (misalnya, semua parameter yang diperlukan ditentukan), status berubah menjadi `PendingApproval` (bahkan otomatis CTs memerlukan

persetujuan, yang terjadi secara otomatis jika sintaks dan pemeriksaan parameter lulus). Jika tidak lulus, statusnya berubah menjadi`Rejected`. `StatusReason`Memberikan informasi tentang penolakan; `ExecutionOutput` bidang memberikan informasi tentang persetujuan dan penyelesaian. Kode kesalahan meliputi:

- InvalidRfcStateException: RFC berada dalam status yang tidak mengizinkan operasi yang dipanggil. Misalnya, jika RFC telah pindah ke status Kirim, itu tidak dapat lagi dimodifikasi.
- InvalidRfcScheduleException: StartTime, EndTime, atau TimeoutInMinutes parameter dilanggar.
- InternalServerError: Kesulitan dengan sistem ditemui.
- InvalidArgumentException: Parameter salah ditentukan; misalnya, nilai yang tidak dapat diterima digunakan.
- ResourceNotFoundException: Nilai, seperti ID tumpukan, tidak dapat ditemukan.

Jika waktu mulai dan akhir yang dijadwalkan yang diminta (juga dikenal sebagai jendela jalankan perubahan) terjadi sebelum perubahan disetujui, status RFC akan berubah menjadi`Canceled`. Jika perubahan disetujui, status RFC berubah menjadi`Scheduled`. Jendela change run untuk ASAP RFCs adalah waktu yang dikirimkan ditambah `ExpectedExecutionDuration` nilai untuk CT.

Kapan saja sebelum kedatangan jendela run perubahan, perubahan terjadwal (dikirimkan dengan a `RequestedStartTime` di CLI) dapat dimodifikasi atau dibatalkan. Jika perubahan yang dijadwalkan diubah, maka harus dikirimkan kembali.

Ketika waktu mulai perubahan tiba (dijadwalkan atau ASAP) dan setelah persetujuan selesai, status berubah `InProgress` dan tidak ada modifikasi yang dapat dilakukan. Jika perubahan selesai dalam jendela run perubahan yang ditentukan, status berubah menjadi`Success`. Jika ada bagian dari perubahan yang gagal, atau jika perubahan masih berlangsung saat jendela run change berakhir, status akan berubah menjadi`Failure`.

> **Note**
>
> Selama`InProgress`,`Success`, atau `Failure` mengubah status, RFC tidak dapat dimodifikasi atau dibatalkan.

Diagram berikut mengilustrasikan status RFC dari panggilan CreateRFC hingga resolusi.

Memahami pembaruan RFC CTs dan deteksi drift CloudFormation template

Sumber daya yang disediakan di AMS menggunakan templat yang dimodifikasi CloudFormation . Jika sumber daya memiliki parameter yang diubah secara langsung melalui Konsol AWS Manajemen layanan, maka catatan CloudFormation pembuatan sumber daya tersebut menjadi tidak sinkron. Jika ini terjadi dan Anda mencoba menggunakan jenis perubahan pembaruan AMS untuk memperbarui sumber daya di AMS, AMS mereferensikan konfigurasi sumber daya asli dan berpotensi menyetel ulang parameter yang diubah. Reset ini mungkin merusak, jadi AMS melarang RFCs dengan jenis perubahan pembaruan jika ada perubahan konfigurasi AMS tambahan yang terdeteksi.

Untuk daftar jenis perubahan pembaruan, gunakan filter konsol.

Remediasi drift FAQs

Pertanyaan dan jawaban tentang remediasi drift AMS. Ada dua jenis perubahan yang dapat Anda gunakan untuk memulai remediasi drift, satu adalah mode eksekusi = manual atau “review required,” yang lainnya adalah mode eksekusi = otomatis.

Sumber daya yang didukung remediasi drift (ct-3kinq0u4l33zf)

Ini adalah sumber daya yang didukung oleh tipe perubahan remediasi drift, (ct-3kinq0u4l33zf). Untuk perbaikan sumber daya apa pun, gunakan jenis perubahan “diperlukan tinjauan” (ct-34sxfo53yuzah) sebagai gantinya.

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
```

```
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

Jenis perubahan remediasi drift

Pertanyaan dan jawaban tentang penggunaan jenis perubahan remediasi drift AMS.

Untuk daftar sumber daya yang didukung untuk fitur remediasi drift, lihat. Sumber daya yang didukung remediasi drift (ct-3kinq0u4l33zf)

Important

Remediasi drift memodifikasi and/or parameter template tumpukan dan wajib untuk memperbarui repositori template lokal Anda atau otomatisasi apa pun yang memperbarui tumpukan ini untuk menggunakan templat dan parameter tumpukan terbaru. Menggunakan and/or parameter template lama tanpa sinkronisasi dapat menyebabkan perubahan merusak pada sumber daya yang mendasarinya.
Tidak diperlukan tinjauan, otomatis, CT (ct-3kinq0u4l33zf) hanya mendukung remediasi 10 sumber daya per RFC. Untuk memulihkan sumber daya yang tersisa dalam batch 10 buat yang baru RFCs sampai semua sumber daya diperbaiki.

Jenis perubahan remediasi drift mana yang harus saya gunakan?

Kami merekomendasikan untuk menggunakan CT otomatis (ct-3kinq0u4l33zf) tanpa ulasan saat:

- Anda mencoba melakukan pembaruan ke sumber daya tumpukan yang ada menggunakan CT otomatis dan RFC ditolak sebagai tumpukan. `DRIFTED`
- Anda menggunakan Update CT di masa lalu dan gagal karena tumpukannya DRIFTED. Anda tidak perlu mencoba pembaruan lagi dan dapat menggunakan ulasan yang diperlukan, manual, CT sebagai gantinya.

Kami merekomendasikan penggunaan tinjauan yang diperlukan, CT manual (ct-34sxfo53yuzah) hanya jika jenis sumber daya yang hanyut tidak didukung oleh remediasi drift tidak diperlukan tinjauan, otomatis, CT (ct-3kinq0u4l33zf), atau ketika remediasi drift tidak diperlukan tinjauan, otomatis, CT gagal.

Perubahan apa yang dilakukan pada tumpukan selama remediasi?

Remediasi memerlukan pembaruan ke and/or parameter template tumpukan tergantung pada properti yang hanyut. Remediasi juga memperbarui kebijakan tumpukan tumpukan selama remediasi dan mengembalikan kebijakan tumpukan ke nilai sebelumnya setelah remediasi selesai.

Bagaimana kita bisa melihat perubahan yang dilakukan pada and/or parameter template tumpukan?

Dalam menanggapi RFC, ringkasan perubahan disediakan dengan informasi berikut:

- `ChangeSummaryJson`: Berisi ringkasan perubahan and/or Parameter Template Stack sebagai bagian dari remediasi drift. Remediasi dilakukan dalam beberapa fase. Ringkasan perubahan ini terdiri dari perubahan untuk fase individu. Jika Remediasi berhasil periksa perubahan fase terakhir. Lihat ExecutionPlan di JSON untuk fase yang dieksekusi secara berurutan. Misalnya, RestoreReferences bagian saat hadir selalu dieksekusi di akhir dan berisi JSON untuk perubahan pasca remediasi. Jika remediasi dijalankan dalam DryRun mode, tidak satu pun dari perubahan ini akan diterapkan ke tumpukan.
- `PreRemediationStackTemplateAndConfigurationJson`: Berisi snapshot konfigurasi CloudFormation Stack termasuk Template, Parameter, Output, StackPolicyBody sebelum remediasi dipicu pada tumpukan.

Apa yang harus saya lakukan setelah remediasi dilakukan?

> **Important**
>
> Anda perlu memperbarui repositori template lokal Anda, atau otomatisasi apa pun, yang akan memperbarui tumpukan yang diperbaiki, dengan templat dan parameter terbaru yang disediakan dalam ringkasan RFC. Hal ini sangat penting untuk melakukan ini karena menggunakan and/or parameter template lama dapat menyebabkan perubahan destruktif lebih lanjut pada sumber daya stack.

Apakah aplikasi saya akan diterapkan selama remediasi ini?

Remediasi adalah proses offline yang dilakukan hanya pada konfigurasi CloudFormation tumpukan. Tidak ada pembaruan yang dilakukan pada sumber daya yang mendasarinya.

Dapatkah saya terus menggunakan Manajemen | Lainnya | Lainnya RFCs untuk melakukan pembaruan sumber daya setelah perbaikan?

Kami menyarankan agar Anda selalu melakukan pembaruan untuk menumpuk sumber daya menggunakan Pembaruan otomatis yang tersedia CTs. Jika Pembaruan yang tersedia CTs tidak mendukung kasus penggunaan Anda, gunakan Manajemen | Lainnya | Permintaan lainnya.

Apakah remediasi membuat sumber daya baru di tumpukan?

Remediasi tidak membuat sumber daya baru di tumpukan. Namun, remediasi membuat output baru dan memperbarui bagian metadata template tumpukan untuk menyimpan ringkasan remediasi untuk referensi Anda.

Akankah remediasi selalu berhasil?

Remediasi memerlukan analisis dan validasi konfigurasi template yang cermat untuk menentukan apakah itu dapat dilakukan. Dalam skenario di mana validasi ini gagal, proses remediasi dihentikan dan tidak ada perubahan yang dilakukan pada template tumpukan atau parameter. Selain itu, remediasi hanya dapat dilakukan pada jenis sumber daya yang didukung.

Bagaimana saya bisa melakukan pembaruan untuk menumpuk sumber daya jika remediasi tidak berhasil?

Anda dapat menggunakan Manajemen | Lainnya | Lainnya | Perbarui CT (ct-0xdawir96cy7k) untuk meminta perubahan. AMS memantau skenario tersebut dan bekerja untuk meningkatkan solusi remediasi.

Dapatkah saya memulihkan tumpukan yang memiliki tipe sumber daya yang didukung dan tidak didukung?

Ya. Namun, remediasi dilakukan hanya jika jenis sumber daya yang didukung ditemukan DRIFTED di tumpukan. Jika ada jenis sumber daya yang tidak didukung DRIFTED, remediasi tidak akan dilanjutkan.

Dapatkah saya meminta remediasi untuk tumpukan yang dibuat melalui non-CFN Ingest? CTs

Ya. Remediasi dapat dilakukan pada tumpukan terlepas dari jenis perubahan yang digunakan untuk membuat tumpukan.

Dapatkah saya mengetahui perubahan yang akan dilakukan pada tumpukan sebelum perbaikan?

Ya. Kedua jenis perubahan menyediakan DryRunopsi yang dapat Anda gunakan untuk meminta perubahan yang akan dilakukan jika tumpukan diperbaiki. Namun, perubahan remediasi akhir mungkin berbeda tergantung pada penyimpangan yang ada pada tumpukan pada saat remediasi.

Jadwal RFCs

Fitur Penjadwalan memungkinkan Anda memilih waktu mulai untuk RFCs. Opsi berikut tersedia di fitur Penjadwalan:

- Jalankan perubahan ini secepatnya: AMS menjalankan RFC segera setelah disetujui. Sebagian CTs besar disetujui secara otomatis. Gunakan opsi ini jika tidak ingin RFC dimulai pada waktu tertentu.
- Jadwalkan perubahan ini: Tetapkan hari, waktu, dan zona waktu agar RFC berjalan. Untuk jenis perubahan otomatis, ini adalah praktik terbaik untuk meminta waktu mulai yang setidaknya 10 menit setelah Anda berencana untuk mengirimkan RFC. Untuk meninjau jenis perubahan yang diperlukan, Anda harus meminta waktu mulai setidaknya 24 jam setelah Anda berencana mengirimkan RFC. Jika RFC tidak disetujui oleh waktu mulai yang dikonfigurasi, maka RFC ditolak.

Tetapkan jadwal RFC

Untuk menjadwalkan RFC, gunakan salah satu metode berikut:

Jalankan perubahan ini secepatnya:

- Konsol: Jangan lakukan apa-apa. Ini menggunakan jadwal RFC default.
- API atau CLI: Hapus `RequestedEndTime` opsi `RequestedStartTime` dan dalam operasi Buat RFC.

ASAP “diperlukan peninjauan” ditolak RFCs secara otomatis jika tidak disetujui dalam waktu tiga puluh hari sejak pengajuan.

Jadwalkan perubahan ini:

- Konsol: Pilih tombol Jadwalkan perubahan radio ini. Area waktu mulai terbuka. Ketik secara manual dalam sehari atau gunakan widget kalender untuk memilih hari. Masukkan waktu, dalam UTC, dinyatakan dalam format ISO 8601, dan gunakan daftar drop-down untuk memilih lokasi. Secara default, AMS menggunakan format ISO 8601 Z atau:MM: YYYYMMDDThhmmss YYYY-MM-DDThh SSZ, salah satu format diterima.

> **Note**
>
> Waktu Akhir Default adalah 4 jam dari waktu Mulai yang Anda masukkan. Untuk mengatur Waktu Akhir perubahan terjadwal Anda melebihi 4 jam, gunakan API atau CLI untuk menjalankan perubahan.

- API atau CLI: Kirim nilai untuk `RequestedStartTime` dan `RequestedEndTime` parameter dalam operasi Buat RFC. Melewati konfigurasi `RequestedEndTime` tidak menghentikan proses untuk jenis perubahan otomatis yang telah dimulai. Untuk jenis perubahan “wajib ditinjau”, jika `RequestedEndTime` tercapai saat penelitian Operasi AMS masih berlangsung, dan Anda berkomunikasi dengan AMS, maka Anda dapat meminta ekstensi, atau Anda mungkin diminta untuk mengirimkan ulang RFC.

> **Tip**
>
> Untuk contoh pembacaan waktu UTC, lihat UTC di situs web Time-is. Contoh format ISO 8601 untuk date/time nilai 2016-12-05 pada 2:20pm: 2016-12-05T 14:20:00 Z atau 20161205T142000Z.

Jika Anda memberikan...

- hanya a`RequestedStartTime`, RFC dianggap dijadwalkan dan `RequestedEndTime` diisi menggunakan nilai. `ExecutionDurationInMinutes`
- hanya a`RequestedEndTime`, kami melempar InvalidArgumentException.
- keduanya `RequestedStartTime` dan`RequestedEndTime`, kami menimpa `RequestedEndTime` dengan waktu mulai yang ditentukan ditambah `ExecutionDurationInMinutes` nilainya.
- baik `RequestedStartTime` maupun`RequestedEndTime`, kami mempertahankan nilai-nilai itu sebagai nol dan RFC diperlakukan sebagai ASAP RFC.

> **Note**
>
> Untuk semua yang dijadwalkan RFCs, waktu akhir yang tidak ditentukan ditulis sebagai waktu yang ditentukan `RequestedStartTime` ditambah `ExpectedExecutionDurationInMinutes` atribut dari jenis perubahan yang dikirimkan. Misalnya, jika “60" (menit), dan yang ditentukan `RequestedStartTime`

adalah `2016-12-05T14:20:00Z` (5 Desember 2016 pukul 4:20 pagi), waktu akhir yang sebenarnya akan ditetapkan ke 5 Desember 2016 pukul 5:20 pagi. `ExpectedExecutionDurationInMinutes` Untuk menemukan tipe perubahan tertentu, jalankan perintah ini: `ExpectedExecutionDurationInMinutes`

```
aws amscm --profile saml get-change-type-version --
change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.
{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Gunakan opsi Prioritas RFC

Gunakan opsi Prioritas dalam jenis `execution mode = manual` perubahan untuk mengingatkan Operasi AMS tentang urgensi permintaan.

Opsi prioritas di`execution mode = manual`:

Tentukan prioritas RFC manual sebagai Tinggi, Sedang, atau Rendah. RFCs diklasifikasikan sebagai Tinggi ditinjau dan disetujui sebelum RFCs diklasifikasikan sebagai Medium, tunduk pada tujuan tingkat layanan RFC (SLOs) dan waktu pengajuannya. RFCs dengan Prioritas rendah atau tidak ada prioritas yang ditentukan diproses sesuai urutan yang dikirimkan.

Menyetujui atau menolak RFCs

RFCs diserahkan dengan persetujuan yang diperlukan (manual) CTs harus disetujui oleh Anda atau AMS. Pra-persetujuan CTs diproses secara otomatis. Untuk informasi selengkapnya, lihat Persyaratan persetujuan CT.

> **Note**
>
> Saat menggunakan “review required” CTs, AMS merekomendasikan agar Anda menggunakan opsi Penjadwalan ASAP (pilih ASAP di konsol, biarkan waktu mulai dan berakhir kosong di API/CLI) karena ini CTs memerlukan operator AMS untuk memeriksa RFC, dan mungkin berkomunikasi dengan Anda sebelum dapat disetujui dan dijalankan. Jika Anda menjadwalkan ini RFCs, pastikan untuk mengizinkan setidaknya 24 jam. Jika persetujuan tidak terjadi sebelum waktu mulai yang dijadwalkan, RFC ditolak secara otomatis.

Jika RFC yang diperlukan persetujuan berhasil dikirimkan oleh AMS, maka RFC tersebut harus disetujui secara eksplisit oleh Anda. Atau, jika Anda mengirimkan RFC yang diperlukan persetujuan, maka itu harus disetujui oleh AMS. Jika Anda diminta untuk menyetujui RFC yang dikirimkan AMS, maka email atau komunikasi lain yang telah ditentukan dikirimkan kepada Anda untuk meminta persetujuan. Komunikasi termasuk ID RFC. Setelah komunikasi dikirim, lakukan salah satu hal berikut:

- Menyetujui atau Menolak Konsol: Gunakan halaman detail RFC untuk RFC yang relevan:

- API/CLI Approve: ApproveRfcmenandai perubahan sebagai disetujui. Tindakan harus diambil oleh pemilik dan operator, jika keduanya diperlukan. Berikut ini adalah contoh CLI menyetujui perintah. Dalam contoh berikut, ganti RFC_ID dengan ID RFC yang sesuai.

  ```
  aws amscm approve-rfc --rfc-id RFC_ID
  ```

- API/CLI Reject: RejectRfcmenandai perubahan sebagai ditolak. Berikut ini adalah contoh perintah CLI reject. Dalam contoh berikut, ganti RFC_ID dengan ID RFC yang sesuai.

  ```
  aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
  ```

Minta periode berjalan terbatas RFC

Sebelumnya dikenal sebagai hari pemadaman, Anda dapat meminta untuk membatasi periode waktu tertentu. Tidak ada perubahan yang dapat dijalankan selama waktu-waktu tersebut.

Untuk menetapkan periode berjalan terbatas, gunakan operasi UpdateRestrictedExecutionTimesAPI dan tetapkan periode waktu tertentu, di UTC. Periode yang Anda tentukan mengesampingkan periode sebelumnya yang ditentukan. Jika Anda mengirimkan RFC selama waktu berjalan terbatas yang ditentukan, pengiriman gagal dengan kesalahan Jadwal RFC Tidak Valid. Anda dapat menentukan hingga 200 periode waktu terbatas. Secara default, tidak ada periode terbatas yang ditetapkan. Berikut ini adalah contoh perintah permintaan (dengan otentikasi SAM dikonfigurasi):

```
aws amscm  --profile saml update-restricted-execution-times --restricted-execution-
times="[{\"TimeRange\":{\"StartTime\":\"2018-01-01T12:00:00Z\",\"EndTime\":
\"2018-01-01T12:00:01Z\"}}]"
```

Anda juga dapat melihat RestrictedExecutionTimes setelan Anda saat ini dengan menjalankan operasi ListRestrictedExecutionTimesAPI. Contoh:

```
aws amscm  --profile saml list-restricted-execution-times
```

Jika Anda ingin mengirimkan RFC selama waktu eksekusi terbatas yang ditentukan, tambahkan RestrictedExecutionTimesOverrideIddengan nilai OverrideRestrictedTimeRanges, dan kemudian kirimkan RFC seperti biasa. Ini adalah praktik terbaik untuk hanya menggunakan metode ini untuk RFC kritis atau darurat. Untuk informasi selengkapnya, lihat referensi API untuk SubmitRfc.

Buat, kloning, perbarui, temukan, dan batalkan RFCs

Contoh berikut memandu Anda melalui berbagai operasi RFC.

Topik

- Buat RFC
- Kloning RFCs (buat ulang) dengan konsol AMS
- Perbarui RFCs
- Menemukan RFCs
- Batalkan RFCs

Buat RFC

Membuat RFC dengan konsol

Berikut ini adalah halaman pertama proses RFC Create di konsol AMS, dengan kartu Quick terbuka dan Browse change types aktif:

Berikut ini adalah halaman pertama proses RFC Create di konsol AMS, dengan Pilih berdasarkan kategori aktif:

Cara kerjanya:

1. Arahkan ke halaman Buat RFC: Di panel navigasi kiri konsol AMS klik RFCsuntuk membuka halaman RFCs daftar, lalu klik Buat RFC.
2. Pilih jenis perubahan populer (CT) di tampilan default Jelajahi jenis perubahan, atau pilih CT dalam tampilan Pilih menurut kategori.

- Jelajahi berdasarkan jenis perubahan: Anda dapat mengklik CT populer di area Buat cepat untuk segera membuka halaman Jalankan RFC. Perhatikan bahwa Anda tidak dapat memilih versi CT yang lebih lama dengan pembuatan cepat.

  Untuk mengurutkan CTs, gunakan area Semua jenis perubahan dalam tampilan Kartu atau Tabel. Di kedua tampilan, pilih CT dan kemudian klik Buat RFC untuk membuka halaman Jalankan RFC. Jika berlaku, opsi Buat dengan versi yang lebih lama muncul di sebelah tombol Buat RFC.
- Pilih berdasarkan kategori: Pilih kategori, subkategori, item, dan operasi dan kotak detail CT terbuka dengan opsi untuk Membuat dengan versi yang lebih lama jika berlaku. Klik Buat RFC untuk membuka halaman Jalankan RFC.

3. Pada halaman Jalankan RFC, buka area nama CT untuk melihat kotak detail CT. Subjek diperlukan (ini diisi untuk Anda jika Anda memilih CT Anda di tampilan jenis perubahan Jelajahi). Buka area konfigurasi tambahan untuk menambahkan informasi tentang RFC.

   Di area konfigurasi Eksekusi, gunakan daftar drop-down yang tersedia atau masukkan nilai untuk parameter yang diperlukan. Untuk mengkonfigurasi parameter eksekusi opsional, buka area konfigurasi tambahan.
4. Setelah selesai, klik Jalankan. Jika tidak ada kesalahan, halaman RFC berhasil dibuat ditampilkan dengan detail RFC yang dikirimkan, dan output Run awal.
5. Buka area parameter Jalankan untuk melihat konfigurasi yang Anda kirimkan. Segarkan halaman untuk memperbarui status eksekusi RFC. Secara opsional, batalkan RFC atau buat salinannya dengan opsi di bagian atas halaman.

Membuat RFC dengan CLI

Cara kerjanya:

1. Gunakan Inline Create (Anda mengeluarkan `create-rfc` perintah dengan semua RFC dan parameter eksekusi disertakan), atau Template Create (Anda membuat dua file JSON, satu untuk parameter RFC dan satu untuk parameter eksekusi) dan mengeluarkan `create-rfc` perintah dengan dua file sebagai input. Kedua metode tersebut dijelaskan di sini.
2. Kirim `aws amscm submit-rfc --rfc-id` *`ID`* perintah RFC: dengan ID RFC yang dikembalikan.

   Pantau `aws amscm get-rfc --rfc-id` *`ID`* perintah RFC:.

Untuk memeriksa versi jenis perubahan, gunakan perintah ini:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Anda dapat menggunakan `CreateRfc` parameter apa pun dengan RFC apa pun apakah itu bagian dari skema untuk jenis perubahan atau tidak. Misalnya, untuk mendapatkan pemberitahuan ketika status RFC berubah, tambahkan baris ini, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` ke bagian parameter RFC dari permintaan (bukan parameter eksekusi). Untuk daftar semua CreateRfc parameter, lihat Referensi AMS Change Management API.

BUAT SEBARIS:

Keluarkan perintah create RFC dengan parameter eksekusi yang disediakan sebaris (tanda kutip saat memberikan parameter eksekusi sebaris), lalu kirimkan ID RFC yang dikembalikan. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini::

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title
 "TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

TEMPLATE MEMBUAT:

> **Note**
>
> Contoh pembuatan RFC ini menggunakan tipe perubahan tumpukan Load Balancer (ELB).

1. Temukan CT yang relevan. Perintah berikut mencari ringkasan klasifikasi CT untuk yang berisi “ELB” di Nama Item dan membuat output dari Kategori, Item, Operasi, dan ChangeType ID dalam bentuk tabel (Subkategori untuk keduanya). `Advanced stack components`

   ```
   aws amscm list-change-type-classification-summaries --query
    "ChangeTypeClassificationSummaries[?contains(Item,'ELB')].
   [Category,Item,Operation,ChangeTypeId]" --output table
   ```

```
-------------------------------------------------------------------
|                            CtSummaries                          |
+-----------+--------------------------+-------------------------+
| Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7jl |
| Management| Load balancer (ELB) stack | Update | ct-0ltm873rsebx9 |
+-----------+--------------------------+-------------------------+
```

2. Temukan versi terbaru dari CT:

   `ChangeTypeIddanChangeTypeVersion`: ID tipe perubahan untuk panduan ini adalah `ct-123h45t6uz7jl` (buat ELB), untuk mengetahui versi terbaru, jalankan perintah ini:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-123h45t6uz7jl
```

3. Pelajari opsi dan persyaratannya. Perintah berikut output skema ke file JSON bernama .json. CreateElbParams

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. Memodifikasi dan menyimpan parameter eksekusi file JSON. Contoh ini menamai file CreateElbParams .json.

   Untuk CT penyediaan, termasuk dalam skema dan harus diserahkan dalam parameter eksekusi. StackTemplateId

   Untuk TimeoutInMinutes, berapa menit yang diizinkan untuk pembuatan tumpukan sebelum RFC gagal, pengaturan ini tidak akan menunda eksekusi RFC, tetapi Anda harus memberikan waktu yang cukup (misalnya, jangan tentukan “5"). Nilai yang valid adalah “60" hingga “360,” untuk CTs dengan jangka panjang UserData: Buat EC2 dan Buat ASG. Kami merekomendasikan maksimum yang diizinkan “60" untuk semua penyediaan CTs lainnya.

   Berikan ID VPC tempat Anda ingin tumpukan dibuat; Anda bisa mendapatkan ID VPC dengan perintah CLI. `aws amsskms list-vpc-summaries`

```
{
"Description":      "ELB-Create-RFC",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-sdhopv00000000000",
```

```
"Name":             "MyElbInstance",
"TimeoutInMinutes": 60,
"Parameters":   {
    "ELBSubnetIds":                     ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold":   4,
    "ELBHealthCheckInterval":           5,
    "ELBHealthCheckTarget":             "HTTP:80/",
    "ELBHealthCheckTimeout":            60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":                        false
    }
}
```

5. Keluarkan template RFC JSON ke file di folder Anda saat ini bernama CreateElbRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. Ubah dan simpan CreateElbRfc file.json. Karena Anda membuat parameter eksekusi dalam file terpisah, hapus `ExecutionParameters` baris. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```
{
"ChangeTypeVersion":    "2.0",
"ChangeTypeId":         "ct-123h45t6uz7jl",
"Title":                "Create ELB"
}
```

7. Buat RFC. Perintah berikut menentukan file parameter eksekusi dan file template RFC:

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-
parameters file://CreateElbParams.json
```

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

Kiat

> **Note**
>
> Anda dapat menggunakan AMS API/CLI untuk membuat RFC tanpa membuat file JSON RFC atau file JSON parameter eksekusi CT. Untuk melakukan ini, Anda menggunakan `create-rfc` perintah dan menambahkan parameter RFC dan eksekusi yang diperlukan ke perintah, ini disebut “Buat Sebaris”. Perhatikan bahwa semua penyediaan CTs telah terkandung dalam `execution-parameters` blok `Parameters` array dengan parameter untuk sumber daya. Parameter harus memiliki tanda kutip yang lolos dengan garis miring belakang (\).
> Metode terdokumentasi lainnya untuk membuat RFC disebut “Template Create.” Di sinilah Anda membuat file JSON untuk parameter RFC dan file JSON lain untuk parameter eksekusi, dan mengirimkan dua file dengan perintah. `create-rfc` File-file ini dapat berfungsi sebagai template dan digunakan kembali untuk masa depan RFCs.
> Saat membuat RFCs dengan template, Anda dapat menggunakan perintah untuk membuat file JSON dengan konten yang Anda inginkan dengan mengeluarkan perintah seperti yang ditunjukkan. Perintah membuat file bernama “parameters.json” dengan konten yang ditampilkan; Anda juga bisa menggunakan perintah ini untuk membuat file RFC JSON.

Kloning RFCs (buat ulang) dengan konsol AMS

Anda dapat menggunakan konsol AMS untuk mengkloning RFC yang ada.

Untuk mengkloning, atau membuat ulang, RFC menggunakan konsol AMS, ikuti langkah-langkah berikut:

1. Temukan RFC yang relevan. Dari navigasi kiri, klik RFCs.

   RFCs Dasbor terbuka.

2. Gulir halaman sampai Anda menemukan RFC yang ingin Anda kloning. Gunakan opsi Filter untuk mempersempit daftar. Pilih RFC yang ingin Anda kloning.

   Halaman detail RFC terbuka.

3. Klik Buat Salinan.

   Halaman Buat permintaan untuk perubahan terbuka dengan semua opsi yang ditetapkan seperti pada RFC asli.

4. Buat perubahan yang Anda inginkan. Untuk mengatur opsi tambahan, ubah opsi Basic ke Advanced. Setelah Anda mengatur semua opsi, pilih Kirim.

   Halaman detail RFC aktif terbuka dengan ID RFC baru untuk RFC kloning dan RFC kloning muncul di dasbor RFC.

Perbarui RFCs

Anda dapat mengirimkan ulang RFC yang telah ditolak atau yang belum dikirimkan, dengan memperbarui RFC dan kemudian mengirimkannya, atau mengirimkannya kembali. Perhatikan bahwa sebagian besar ditolak karena RFCs yang ditentukan `RequestedStartTime` telah berlalu sebelum pengiriman atau yang TimeoutInMinutes ditentukan tidak memadai untuk menjalankan RFC (karena TimeoutInMinutes tidak memperpanjang RFC yang berhasil, kami sarankan untuk selalu menyetel ini ke setidaknya “60" dan hingga “360" untuk Amazon atau grup Auto Scaling EC2 Amazon dengan jangka panjang). EC2 UserData Bagian ini menjelaskan cara menggunakan versi CLI dari `UpdateRfc` perintah untuk memperbarui RFC dengan parameter RFC baru, atau parameter baru menggunakan JSON stringified atau file parameter yang diperbarui.

Contoh ini menjelaskan penggunaan AMS UpdateRfc API versi CLI (lihat Perbarui RFC). Meskipun ada jenis perubahan untuk memperbarui beberapa sumber daya (DNS pribadi dan publik, tumpukan penyeimbang beban, dan konfigurasi tambalan tumpukan), tidak ada CT untuk memperbarui RFC.

Kami menyarankan Anda mengirimkan satu UpdateRfc operasi pada satu waktu. Jika Anda mengirimkan beberapa pembaruan, misalnya pada tumpukan DNS, pembaruan mungkin gagal mencoba memperbarui DNS secara bersamaan.

DATA YANG DIPERLUKAN:`RfcId`: RFC yang Anda perbarui.

DATA OPSIONAL`ExecutionParameters`:: Kecuali Anda memperbarui bidang yang tidak wajib`Description`, seperti, Anda akan mengirimkan parameter eksekusi yang dimodifikasi untuk mengatasi masalah yang menyebabkan RFC ditolak atau dibatalkan. Semua nilai non-null yang dikirimkan menimpa nilai-nilai tersebut di RFC asli.

1. Temukan RFC yang ditolak atau dibatalkan yang relevan, Anda dapat menggunakan perintah ini (Anda dapat mengganti nilainya dengan`Canceled`):

   ```
   aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
   ```

2. Anda dapat memodifikasi salah satu parameter RFC berikut:

```
{
    "Description": "string",
    "ExecutionParameters": "string",
    "ExpectedOutcome": "string",
    "ImplementationPlan": "string",
    "RequestedEndTime": "string",
    "RequestedStartTime": "string",
    "RfcId": "string",
    "RollbackPlan": "string",
    "Title": "string",
    "WorstCaseScenario": "string"}
```

Contoh perintah memperbarui bidang Deskripsi:

```
aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
 --region us-east-1
```

Contoh perintah memperbarui ExecutionParameters VpcId bidang:

```
aws amscm update-rfc  --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id
 "RFC_ID" --region us-east-1
```

Contoh perintah memperbarui RFC dengan file parameter eksekusi yang berisi pembaruan; lihat contoh file parameter eksekusi di langkah 2 dari: EC2 stack | Buat:

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --
rfc-id "RFC_ID" --region us-east-1
```

3. Kirim ulang RFC menggunakan `submit-rfc` dan ID RFC yang sama dengan yang Anda miliki saat RFC pertama kali dibuat:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Jika RFC berhasil, Anda tidak menerima konfirmasi atau pesan kesalahan di baris perintah.

4. Untuk memantau status permintaan dan untuk melihat Output Eksekusi, jalankan perintah berikut.

```
aws amscm get-rfc --rfc-id RFC_ID
```

Menemukan RFCs

Temukan permintaan perubahan (RFC) dengan konsol

Untuk menemukan RFC menggunakan konsol AMS, ikuti langkah-langkah berikut.

> **Note**
>
> Prosedur ini hanya berlaku untuk yang dijadwalkan RFCs, RFCs yaitu, yang tidak menggunakan opsi ASAP.

1. Dari navigasi kiri, klik RFCs.

   RFCs Dasbor terbuka.
2. Gulir daftar atau gunakan opsi Filter untuk memperbaiki daftar.

   Daftar RFC berubah per kriteria filter.
3. Pilih tautan Subjek untuk RFC yang Anda inginkan.

   Halaman detail RFC terbuka untuk RFC itu dengan informasi termasuk ID RFC.
4. Jika ada banyak RFCs di dasbor, Anda dapat menggunakan opsi Filter untuk mencari berdasarkan RFC:

   - Subjek: Baris subjek, atau judul (dalam API/CLI) diberikan kepada RFC saat dibuat.
   - ID RFC: Pengidentifikasi untuk RFC.
   - Status aktivitas: Jika Anda mengetahui status RFC, Anda dapat memilih antara AwsOperatorAssignedarti operator sedang melihat RFC, yang AwsActionPendingberarti bahwa operator AMS harus melakukan sesuatu sebelum eksekusi RFC dapat dilanjutkan atau CustomerActionPendingartinya Anda perlu mengambil beberapa tindakan sebelum eksekusi RFC dapat dilanjutkan.
   - Status: Jika Anda mengetahui status RFC, Anda dapat memilih antara:
     - Dijadwalkan: RFCs yang dijadwalkan.
     - Dibatalkan: RFCs yang dibatalkan.
     - Sedang berlangsung: RFCs sedang berlangsung.
     - Sukses: RFCs yang dieksekusi dengan sukses.
     - Ditolak: RFCs yang ditolak.

    - Pengeditan: RFCs yang sedang diedit.
    - Kegagalan: RFCs itu gagal.
    - Persetujuan yang tertunda: RFCs yang tidak dapat dilanjutkan sampai AMS atau Anda menyetujui. Biasanya, ini menunjukkan bahwa Anda perlu menyetujui RFC. Anda akan mendapatkan pemberitahuan layanan ini di daftar Permintaan Layanan Anda.
  - Ubah jenis: Pilih Kategori, Subkategori, Item, dan Operasi, dan ID jenis perubahan diambil untuk Anda.
  - Waktu mulai yang diminta atau Waktu akhir yang diminta: Opsi filter ini memungkinkan Anda memilih Sebelum atau Setelah, lalu masukkan Tanggal dan, secara opsional, Waktu (hh: mm dan zona waktu). Filter ini beroperasi dengan sukses hanya pada jadwal RFCs (tidak ASAP RFCs).
  - Status: Baik Dijadwalkan, Dibatalkan, Sedang berlangsung, Sukses, Ditolak, Mengedit, atau Kegagalan.
  - Subjek: Subjek (atau judul, jika RFC dibuat dengan API/CLI) yang Anda berikan RFC.
  - Ubah tipe ID: Gunakan pengenal untuk jenis perubahan yang dikirimkan dengan RFC.

  Pencarian memungkinkan Anda untuk menambahkan filter, seperti yang ditunjukkan pada gambar berikut.

5. Klik tautan Subjek untuk RFC yang Anda inginkan.

   Halaman detail RFC terbuka untuk RFC itu dengan informasi termasuk ID RFC.

Menemukan permintaan perubahan (RFC) dengan CLI

Anda dapat menggunakan beberapa filter untuk menemukan RFC.

Untuk memeriksa versi jenis perubahan, gunakan perintah ini:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Anda dapat menggunakan `CreateRfc` parameter apa pun dengan RFC apa pun apakah itu bagian dari skema untuk jenis perubahan atau tidak. Misalnya, untuk mendapatkan

pemberitahuan ketika status RFC berubah, tambahkan baris ini, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` ke bagian parameter RFC dari permintaan (bukan parameter eksekusi). Untuk daftar semua CreateRfc parameter, lihat Referensi AMS Change Management API.

Jika Anda tidak menuliskan ID RFC, dan perlu menemukannya nanti, Anda dapat menggunakan sistem manajemen perubahan AMS (CM) untuk mencarinya dan mempersempit hasilnya dengan filter atau kueri.

1. ListRfcSummariesOperasi CM API memiliki filter. Anda dapat Memfilter hasil berdasarkan `Attribute` dan `Value` digabungkan dalam operasi AND logis, atau berdasarkan`Attribute`, a`Condition`, dan`Values`.

   Penyaringan RFC

Atribut	Nilai valid	Ketentuan yang valid	Kondisi default	Catatan
ActualEndTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , “20170101 T000000Z”)	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua
ActualStartTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , “20170101 T000000Z”)	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara

Atribut	Nilai valid	Ketentuan yang valid	Kondisi default	Catatan
				harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua
AutomationStatusId	Manual, Otomatis	Setara	Setara	Hanya ada dua status otomatisasi
ChangeTypeId	Setiap ID jenis perubahan yang valid; misalnya, ct-123h45t6uz7jl	Setara	Setara	Menemukan Jenis Perubahan atau CSIO
ChangeTypeVersion	Setiap ID tipe perubahan yang valid; misalnya, 1.0	Setara	Setara	Menemukan Jenis Perubahan atau CSIO
CreatedBy	String apa pun (panjang maksimum yang diizinkan adalah 2048 karakter)	Contains	Contains	CreatedBy Bidang RFC berisi ARN pengguna yang membuatnya

Atribut	Nilai valid	Ketentuan yang valid	Kondisi default	Catatan
CreatedTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , “20170101 T000000Z”)	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua
LastModifiedTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , “20170101 T000000Z”)	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua

Atribut	Nilai valid	Ketentuan yang valid	Kondisi default	Catatan
LastSubmittedTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , “20170101 T000000Z”)	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua
RequestedEndTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , “20170101 T000000Z”)	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua

Atribut	Nilai valid	Ketentuan yang valid	Kondisi default	Catatan
RequestedStartTime	String apa pun yang mewakili tanggal ISO86 01 (misalnya , “20170101 T000000Z”)	Sebelum, Setelah, Antara	Tidak ada	Kondisi Sebelum atau Setelah hanya menerima satu nilai di bidang Nilai. Kondisi Antara harus memiliki tepat dua nilai di bidang Nilai, di mana nilai pertama harus mewakili tanggal yang terjadi sebelum nilai kedua
RfcStatusId	Dibatalkan, Mengedit, Kegagalan ,, InProgress, Ditolak PendingApproval, Dijadwalkan, Sukses	Setara	Setara	Segarkan daftar RFC di konsol AMS atau jalankan GetRfc
Judul	Setiap judul RFC yang valid	Contains	Contains	Ekspresi reguler di setiap bidang individu tidak didukung. Pencarian yang tidak peka huruf besar/kecil

Contoh:

Untuk menemukan semua IDs yang RFCs terkait dengan SQS (di mana SQS terkandung dalam bagian Item CT), Anda dapat menggunakan perintah ini:

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

Yang mengembalikan sesuatu seperti ini:

```
-------------------------------------------------------------------------
|                          ListRfcSummaries                             |
+----------+---------------------------------+-------+-------+---------------+
|Deployment| Advanced Stack Components      |SQS    |Create |ct-123h45t6uz7jl|
|Management| Monitoring & Notification  |SQS    |Update |ct-123h45t6uz7jl|
+----------+---------------------------------+-------+-------+---------------+
```

Filter lain yang tersedia `list-rfc-summaries` adalah`AutomationStatusId`, untuk mencari RFCs yang otomatis atau manual:

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

Filter lain yang tersedia `list-rfc-summaries` adalah `Title` (Subjek di konsol):

```
 Attribute=Title,Value=RFC-TITLE
```

Contoh struktur permintaan baru di JSON yang mengembalikan RFCs where:

- (Judul BERISI frasa “Windows 2012" ATAU “Amazon Linux”) DAN
- (RfcStatusId SAMA DENGAN “Sukses” ATAU "InProgress“) DAN
- (20170101T000000Z <= <= 20170103T000000Z) DAN (<= 20170103T000000Z) RequestedStartTime ActualEndTime

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
```

```
      "Attribute": "RequestedStartTime",
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

> **Note**
>
> Dengan lebih lanjut`Filters`, AMS bermaksud untuk menghentikan bidang berikut dalam rilis mendatang:
>
> - Nilai: Bidang Nilai adalah bagian dari bidang Filter. Gunakan bidang Nilai yang mendukung fungsionalitas yang lebih canggih.
> - RequestedEndTimeRange: Gunakan bagian RequestedEndTime dalam bidang Filter yang mendukung fungsionalitas yang lebih canggih
> - RequestedStartTimeRange: Gunakan bagian RequestedStartTime dalam bidang Filter yang mendukung fungsionalitas yang lebih canggih.

Untuk informasi tentang penggunaan kueri CLI, lihat Cara Memfilter Output dengan Opsi --query dan referensi bahasa kueri, Spesifikasi. JMESPath

2. Jika Anda menggunakan konsol AMS:

   Pergi ke halaman RFCsdaftar. Jika diperlukan, Anda dapat memfilter pada Subjek RFC, yang Anda masukkan sebagai RFC `Title` saat Anda membuatnya.

Kiat

> **Note**
>
> Prosedur ini hanya berlaku untuk yang dijadwalkan RFCs, RFCs yaitu, yang tidak menggunakan opsi ASAP.

Batalkan RFCs

Anda dapat membatalkan RFC menggunakan Konsol atau AMS API/CLI.

Untuk membatalkan RFC dengan konsol, temukan RFC di daftar RFC Anda, buka, klik Batal.

Data yang Diperlukan:

- `Reason`: Mengapa Anda membatalkan RFC.
- `RfcId`: RFC yang Anda batalkan.

1. Biasanya Anda akan membatalkan RFC segera setelah mengirimkannya (jadi ID RFC harus berguna); jika tidak, Anda tidak akan dapat membatalkannya kecuali Anda menjadwalkannya dan itu sebelum waktu mulai yang ditentukan. Jika Anda perlu menemukan ID RFC, Anda dapat menggunakan perintah ini (Anda dapat mengganti `Value` dengan `PendingApproval` RFC yang disetujui secara manual):

   ```
   aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
   ```

2. Contoh perintah untuk membatalkan RFC:

   ```
   aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --
   region us-east-1
   ```

Gunakan konsol AMS dengan RFCs

Konsol AMS menyediakan fitur untuk membantu Anda berhasil membuat dan mengirimkan RFCs.

Gunakan halaman Daftar RFC (Konsol)

Halaman RFCsdaftar konsol AMS memberi Anda opsi berikut:

- Pencarian RFC tingkat lanjut melalui Filter. Untuk informasi, lihat Menemukan RFCs.
- Menemukan terakhir kali RFC Dimodifikasi. Nilai ini menunjukkan bahwa terakhir kali status RFC diubah.
- Melihat detail RFC dengan Subjek RFC. Memilih tautan ini membuka halaman detail untuk RFC itu.
- Melihat status RFC. Untuk informasi, lihat Memahami kode status RFC

Gunakan RFC quick create (konsol)

Gunakan kartu cepat RFC, atau daftar tabel, atau pilih jenis perubahan RFCs berdasarkan klasifikasi.

Untuk mempelajari selengkapnya, lihat Buat RFC.

Tambahkan korespondensi dan lampiran RFC (konsol)

Anda dapat menambahkan korespondensi ke RFC setelah dikirimkan dan sebelum disetujui; misalnya, saat berada dalam keadaan ""PendingApproval. Setelah RFC disetujui (dalam keadaan “Terjadwal” atau "InProgress“), korespondensi tidak dapat ditambahkan, karena dapat ditafsirkan sebagai perubahan pada permintaan. Setelah RFC selesai (dalam keadaan “Dibatalkan”, “Ditolak”, “Sukses”, atau “Kegagalan”), korespondensi sekali lagi diaktifkan, meskipun korespondensi dinonaktifkan setelah RFC ditutup selama lebih dari 30 hari.

> **Note**
>
> Setiap korespondensi dibatasi hingga 5.000 karakter.

Batasan untuk lampiran:

- Hanya tiga lampiran per korespondensi.
- Batasi lima puluh lampiran per RFC.
- Setiap lampiran harus berukuran kurang dari 5 MB.
- Hanya file teks yang diterima seperti plaintext (`.txt`), nilai yang dipisahkan koma (), JSON (`.csv`), atau YAMB (`.json`). `.yaml` Dalam kasus format YAMAL, file harus dilampirkan menggunakan ekstensi `.yaml` file.

  > **Note**
  >
  > File teks yang memiliki konten XMLdilarang. Jika Anda memiliki konten XMLuntuk dibagikan dengan AMS, gunakan permintaan layanan.

- Nama file dibatasi hingga 255 karakter, dengan hanya angka, huruf, spasi, tanda hubung (-), garis bawah (_), dan titik (.).
- Memperbarui dan menghapus lampiran pada RFC saat ini tidak didukung.

Untuk menambahkan korespondensi dan lampiran ke RFC, ikuti langkah-langkah berikut:

1. Di konsol AMS, pada halaman detail RFC untuk RFC, temukan bagian Korespondensi di bagian bawah halaman.

   Sebelum korespondensi apa pun:

   Setelah beberapa korespondensi:

2. Untuk menambahkan korespondensi baru, ketik pesan Anda di kotak teks Balas. Untuk melampirkan file yang terkait dengan korespondensi, pilih Tambahkan Lampiran, lalu pilih file yang Anda inginkan.

3. Setelah selesai, pilih Kirim.

   Korespondensi baru, bersama dengan tautan ke file terlampir, muncul di daftar korespondensi di halaman detail RFC.

Konfigurasikan pemberitahuan email RFC (konsol)

Halaman pembuatan Permintaan Perubahan konsol AMS memberi Anda opsi untuk menambahkan alamat email guna menerima pemberitahuan perubahan status RFC:

Selain itu, Anda dapat menambahkan alamat email untuk pemberitahuan ke jenis perubahan apa pun, misalnya:

```
aws amscm create-rfc --change-type-id <Change type ID>
                    --change-type-version 1.0 --title "TITLE"
                    --notification "{\"Email\": {\"EmailRecipients\" :
 [\"email@example.com\"]}}"
```

Tambahkan baris serupa (`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`) ke setiap jenis perubahan inline atau permintaan template di bagian parameter RFC dari permintaan, bukan bagian parameter.

Pelajari tentang parameter RFC umum

Berikut ini adalah parameter RFC yang harus Anda kirimkan, dan parameter yang biasa digunakan di RFCs:

- Ubah informasi jenis: ChangeTypeId dan ChangeTypeVersion. Dengan daftar jenis perubahan IDs dan nomor versi, lihat Mengubah Referensi Jenis.

  Jalankan `list-change-type-classification-summaries` di CLI dengan `query` argumen untuk mempersempit hasil. Misalnya, mempersempit hasil untuk mengubah jenis yang berisi "Akses" dalam `Item` nama.

  ```
  aws amscm list-change-type-classification-summaries --query
   "ChangeTypeClassificationSummaries [?contains (Item, 'access')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
  ```

  Jalankan `get-change-type-version` dan tentukan ID tipe perubahan. Perintah berikut mendapatkan versi CT untuk ct-2tylseo8rxfsc.

  ```
  aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
  ```

- Judul: Nama untuk RFC; ini menjadi Subjek RFC di daftar RFC konsol AMS dan Anda dapat mencarinya dengan `GetRfc` perintah dan filter `Title`
- Penjadwalan: Jika Anda menginginkan RFC terjadwal, Anda harus menyertakan `RequestedEndTime` parameter `RequestedStartTime` dan, atau gunakan opsi Jadwalkan konsol perubahan ini. Untuk ASAP RFC (yang berjalan segera setelah disetujui), saat menggunakan CLI, `RequestedStartTime` tinggalkan `RequestedEndTime` dan null. Saat menggunakan konsol, terima opsi ASAP.

  Jika `RequestedStartTime` terlewatkan, RFC ditolak.
- Penyediaan CTs: Parameter eksekusi, atau pengaturan khusus `Parameters` yang diperlukan untuk menyediakan sumber daya. Mereka sangat bervariasi tergantung pada CT.
- Non-penyediaan CTs: CTs yang tidak menyediakan sumber daya, seperti akses CTs atau Lainnya | Lainnya, atau menghapus tumpukan, memiliki parameter eksekusi minimal dan tidak ada blok. `Parameters`
- Beberapa RFCs juga mengharuskan Anda menentukan`TimeoutInMinutes`, atau berapa menit yang diizinkan untuk pembuatan tumpukan sebelum RFC gagal. Nilai yang valid adalah 60 (menit) hingga 360, untuk jangka panjang UserData. Jika eksekusi tidak dapat diselesaikan sebelum

`TimeoutInMinutes` terlampaui, RFC gagal. Namun, pengaturan ini tidak menunda eksekusi RFC.

- RFCs yang membuat instance, seperti bucket S3 atau ELB, umumnya menyediakan skema yang memungkinkan Anda menambahkan hingga tujuh tag (pasangan kunci/nilai). Anda dapat menambahkan lebih banyak tag ke bucket S3 Anda dengan mengirimkan RFC menggunakan Deployment | Advanced stack components | Tag | Create change type (ct-3cx7we852p3af). EC2, EFS, RDS, dan skema multi-tier (HA Two-Tiered dan HA One-Tiered) memungkinkan hingga lima puluh tag. Tag ditentukan di `ExecutionParameters` bagian skema. Memberikan tag bisa sangat berharga. Untuk informasi selengkapnya, lihat Menandai EC2 Sumber Daya Amazon Anda.

  Saat menggunakan konsol AMS, Anda harus membuka area konfigurasi tambahan untuk menambahkan tag.

> **Tip**
>
> Banyak skema CT memiliki `Name` bidang `Description` dan di dekat bagian atas skema. Bidang tersebut digunakan untuk memberi nama komponen tumpukan atau tumpukan, mereka tidak memberi nama sumber daya yang Anda buat. Beberapa skema menawarkan parameter untuk memberi nama sumber daya yang Anda buat, dan beberapa tidak. Misalnya, skema CT untuk EC2 tumpukan Create tidak menawarkan parameter untuk menamai EC2 instance. Untuk melakukannya, Anda harus membuat tag dengan kunci “Nama” dan nilai dari nama yang Anda inginkan. Jika Anda tidak membuat tag seperti itu, EC2 instance Anda akan ditampilkan di EC2 konsol tanpa atribut name.

Gunakan opsi AWS Wilayah RFC

Titik akhir AMS API dan CLI (`amscmdanamsskms`) ada di. `us-east-1` Jika Anda berfederasi dengan Security Assertion Markup Language (SAMP), maka skrip diberikan kepada Anda saat orientasi yang mengatur Wilayah Anda ke us-east-1. AWS Jika Anda menggunakan SAMP, maka Anda tidak perlu menentukan `--region` opsi saat Anda mengeluarkan perintah. Jika SAMP Anda dikonfigurasi untuk menggunakan us-east-1 tetapi akun Anda tidak berada di Wilayah itu, maka Anda harus menentukan Wilayah AWS yang dionboard akun saat Anda mengeluarkan perintah lain (misalnya,). AWS `aws s3`

> **Note**
>
> Sebagian besar contoh perintah yang disediakan dalam panduan ini tidak menyertakan `--region` opsi.

Mendaftar untuk email harian RFC

Anda dapat mendaftar untuk email harian yang merangkum aktivitas RFC di akun Anda selama 24 jam terakhir menggunakan fitur RFC digest. Fitur RFC digest adalah proses efisien yang mengurangi jumlah notifikasi email yang Anda terima terkait akun Anda. RFCs Intisari RFC dapat mengurangi kemungkinan Anda melewatkan tindakan yang menunggu respons Anda.

Untuk mengaktifkan fitur RFC digest, hubungi AMS Cloud Service Delivery Manager (CSDM). CSDM berlangganan Anda. Anda dapat meminta hingga 20 alamat email (atau alias) untuk disertakan dalam daftar email intisari RFC Anda. Jadwal email saat ini ditetapkan pada pukul 09:00 UTC-8.

Untuk mematikan fitur RFC digest, hubungi CSDM Anda dengan permintaan Anda.

Jika Anda tidak mengatur intisari RFC dan menginginkan pemberitahuan mengenai Anda RFCs, atau jika Anda ingin informasi lebih rinci tentang Anda RFCs daripada apa yang disediakan oleh intisari RFC, gunakan Sistem Manajemen Perubahan untuk mengatur pemberitahuan CloudWatch Acara atau pemberitahuan email untuk setiap RFC individu yang Anda inginkan informasi. Untuk informasi tentang cara menyiapkan notifikasi RFC, lihat Pemberitahuan Perubahan Status RFC.

Topik yang terkandung dalam intisari RFC meliputi:

- Persetujuan Pelanggan Tertunda: Daftar RFCs yang PendingApprovalberstatus, menunggu persetujuan Anda
- Balasan Pelanggan Tertunda: Daftar RFCs yang menunggu balasan Anda pada korespondensi RFC
- Persetujuan atau Balasan AWS RFCs yang Tertunda: Daftar yang menunggu di AMS untuk balasan atau persetujuan
- Selesai: Daftar RFCs dalam status Sukses, Kegagalan, Dibatalkan dan Ditolak

Berikut ini adalah contoh RFC digest:

Apa itu jenis perubahan?

Jenis perubahan mengacu pada tindakan yang dilakukan oleh permintaan perubahan (RFC) AWS Managed Services (AMS) dan mencakup tindakan perubahan itu sendiri, dan jenis perubahan — manual vs otomatis. AMS memiliki banyak koleksi jenis perubahan yang tidak digunakan oleh layanan web Amazon lainnya. Anda menggunakan jenis perubahan ini saat mengirimkan permintaan untuk perubahan (RFC) untuk menyebarkan, atau mengelola, atau mendapatkan akses ke, sumber daya.

Topik

- Otomatis dan manual CTs
- Persyaratan persetujuan CT
- Ubah versi tipe
- Buat jenis perubahan
- Perbarui jenis perubahan
- Jenis perubahan hanya internal
- Ubah skema tipe
- Mengelola izin untuk jenis perubahan
- Menyunting informasi sensitif dari jenis perubahan
- Menemukan jenis perubahan, menggunakan opsi kueri

Otomatis dan manual CTs

Batasan pada jenis perubahan adalah apakah mereka otomatis atau manual, ini adalah `AutomationStatusId` atribut tipe perubahan, yang disebut mode Eksekusi di konsol AMS.

Jenis perubahan otomatis memiliki hasil dan waktu eksekusi yang diharapkan dan dijalankan melalui sistem otomatis AMS, umumnya dalam waktu satu jam atau kurang (ini sangat tergantung pada sumber daya apa yang disediakan CT). Jenis perubahan manual jarang terjadi, tetapi diperlakukan berbeda karena mengharuskan operator AMS bertindak pada RFC sebelum dapat dijalankan. Itu terkadang berarti berkomunikasi dengan pengirim RFC, jadi, jenis perubahan manual memerlukan waktu yang bervariasi untuk menyelesaikannya.

Untuk semua yang dijadwalkan RFCs, waktu akhir yang tidak ditentukan ditulis sebagai waktu yang ditentukan `RequestedStartTime` ditambah `ExpectedExecutionDurationInMinutes`

atribut dari jenis perubahan yang dikirimkan. Misalnya, jika “60" (menit), dan yang ditentukan `RequestedStartTime` adalah `2016-12-05T14:20:00Z` (5 Desember 2016 pukul 4:20 pagi), waktu akhir yang sebenarnya akan ditetapkan ke 5 Desember 2016 pukul 5:20 pagi. `ExpectedExecutionDurationInMinutes` Untuk menemukan tipe perubahan tertentu, jalankan perintah ini: `ExpectedExecutionDurationInMinutes`

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

> **Note**
>
> Dijadwalkan RFCs dengan mode Eksekusi = Manual, di Konsol, harus diatur untuk berjalan setidaknya 24 jam di masa mendatang. Peringatan ini tidak berlaku untuk AMS API/CLI, tetapi masih penting untuk menjadwalkan manual RFCs setidaknya 8 jam ke depan.

> **Note**
>
> Saat menggunakan “review required” CTs, AMS merekomendasikan agar Anda menggunakan opsi Penjadwalan ASAP (pilih ASAP di konsol, biarkan waktu mulai dan berakhir kosong di API/CLI) karena ini CTs memerlukan operator AMS untuk memeriksa RFC, dan mungkin berkomunikasi dengan Anda sebelum dapat disetujui dan dijalankan. Jika Anda menjadwalkan ini RFCs, pastikan untuk mengizinkan setidaknya 24 jam. Jika persetujuan tidak terjadi sebelum waktu mulai yang dijadwalkan, RFC ditolak secara otomatis.

AMS bertujuan untuk menanggapi CT manual dalam waktu empat jam, dan akan berkorespondensi sesegera mungkin, tetapi bisa memakan waktu lebih lama bagi RFC untuk benar-benar dijalankan.

Untuk daftar yang Manual dan memerlukan tinjauan AMS, lihat file CSV Ubah Jenis, yang tersedia di halaman Sumber Daya Pengembang di Konsol. CTs

YouTube Video: Bagaimana cara menemukan jenis perubahan otomatis untuk AMS RFCs?

Untuk menemukan mode Eksekusi untuk CT di konsol AMS, Anda harus menggunakan opsi pencarian jenis perubahan Jelajahi. Hasilnya menunjukkan mode eksekusi dari jenis perubahan yang cocok atau jenis perubahan.

Untuk menemukan tipe perubahan tertentu dengan menggunakan AMS CLI, jalankan perintah ini: `AutomationStatus`

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

Anda juga dapat mencari jenis perubahan di Referensi Jenis Perubahan AMS, yang menyediakan informasi tentang semua jenis perubahan AMS.

> **Note**
>
> AMS saat API/CLI ini bukan bagian dari AWSAPI/CLI. To access the AMS API/CLI, Anda mengunduh AMS SDK melalui konsol AMS.

Persyaratan persetujuan CT

AMS CTs selalu memiliki dua kondisi persetujuan, AwsApprovalIddan CustomerApprovalIditu menunjukkan apakah RFC memerlukan AMS atau Anda, atau siapa pun, untuk menyetujui eksekusi.

Kondisi persetujuan agak terkait dengan mode eksekusi; untuk detailnya, lihatOtomatis dan manual CTs.

Untuk mengetahui kondisi persetujuan untuk CT, Anda dapat melihat di AMS Change Type Reference, atau menjalankannya GetChangeTypeVersion. Keduanya juga akan memberi Anda mode CT **`AutomationStatusId`** atau Eksekusi.

Anda dapat menyetujui RFCs dengan menggunakan konsol AMS atau dengan perintah berikut:

```
aws amscm approve-rfc --rfc-id RFC_ID
```

Kondisi persetujuan CT

Jika kondisi persetujuan CT adalah	Hal ini membutuhkan persetujuan dari	Dan
`AwsApprovalId: Required`	Sistem tipe perubahan AMS,	Tidak ada tindakan yang diperlukan. Kondisi ini khas untuk otomatis CTs.
`AwsApprovalId: NotRequiredIfSubmitter`	Sistem jenis perubahan AMS dan tidak ada orang lain, jika RFC yang dikirimkan adalah untuk akun yang diserahkan,	Tidak ada tindakan yang diperlukan. Kondisi ini khas untuk manual CTs karena akan selalu ditinjau oleh operator AMS.
`CustomerApprovalId: NotRequired`	Sistem tipe perubahan AMS,	Jika RFC melewati pemeriksaan sintaks dan parameter, itu disetujui secara otomatis.
`CustomerApprovalId: Required`	Sistem tipe perubahan AMS dan Anda,	Pemberitahuan dikirimkan kepada Anda, dan Anda harus secara eksplisit menyetujui RFC, baik dengan menanggapi pemberitahuan, atau menjalankan operasi. ApproveRfc
`CustomerApprovalId: NotRequiredIfSubmitter`	Sistem tipe perubahan AMS dan tidak ada orang lain, jika Anda mengirimkan RFC.	Jika RFC melewati pemeriksaan sintaks dan parameter, itu disetujui secara otomatis.

Jika kondisi persetujuan CT adalah	Hal ini membutuhkan persetujuan dari	Dan
Insiden Keamanan Mendesak atau Patch	AMS	Apakah auto disetujui dan diimplementasikan.

Ubah versi tipe

Jenis perubahan diberi versi dan versi berubah saat pembaruan besar dibuat untuk jenis perubahan.

Setelah memilih jenis perubahan menggunakan konsol AMS, Anda memiliki opsi untuk membuka area konfigurasi tambahan dan memilih versi jenis perubahan. Anda juga dapat menentukan versi jenis perubahan pada baris API/CLI perintah. Anda mungkin ingin melakukan ini karena berbagai alasan, termasuk:

- Anda tahu bahwa versi jenis perubahan Pembaruan yang Anda inginkan harus cocok dengan versi jenis Buat perubahan yang Anda gunakan untuk membuat sumber daya yang sekarang ingin Anda perbarui. Misalnya, Anda mungkin memiliki instance Elastic Load Balancer (ELB) yang dibuat dengan ELB Create change type versi 1. Untuk memperbaruinya, pilih ELB Update versi 1.
- Anda ingin menggunakan versi jenis perubahan yang memiliki opsi berbeda di dalamnya daripada jenis perubahan terbaru. Kami tidak merekomendasikan hal ini karena pembaruan AMS mengubah jenis terutama untuk alasan keamanan dan kami menyarankan Anda untuk selalu memilih versi terbaru.

Buat jenis perubahan

Buat jenis perubahan dicocokkan version-to-version dengan jenis perubahan Perbarui. Artinya, versi tipe perubahan yang Anda gunakan untuk menyediakan sumber daya harus sesuai dengan versi jenis perubahan Perbarui yang akan Anda gunakan nanti untuk memodifikasi sumber daya tersebut. Misalnya, jika Anda membuat bucket S3 dengan Create S3 Bucket change type versi 2.0, dan kemudian ingin mengirimkan RFC untuk memodifikasi bucket S3 tersebut, Anda harus menggunakan Update S3 Bucket change type versi 2.0 juga, meskipun ada jenis perubahan Update S3 Bucket dengan versi 3.0.

Sebaiknya simpan catatan ID tipe perubahan dan versi yang Anda gunakan saat menyediakan sumber daya dengan tipe Buat perubahan jika nanti Anda ingin menggunakan jenis perubahan Pembaruan untuk memodifikasinya.

Perbarui jenis perubahan

AMS menyediakan jenis perubahan Pembaruan untuk memperbarui sumber daya yang dibuat dengan tipe Buat perubahan. Jenis perubahan Perbarui harus dicocokkan version-to-version dengan jenis Buat perubahan yang awalnya digunakan untuk menyediakan sumber daya.

Sebaiknya simpan catatan ID tipe perubahan dan versi yang Anda gunakan saat menyediakan sumber daya agar mudah memperbaruinya.

YouTube Video: Bagaimana cara menggunakan pembaruan CTs untuk mengubah sumber daya di akun AWS Managed Services (AMS)?

Jenis perubahan hanya internal

Anda dapat melihat jenis perubahan yang hanya untuk penggunaan internal. Ini agar Anda tahu tindakan apa yang dapat atau dilakukan AMS. Jika ada jenis perubahan internal saja yang ingin Anda miliki untuk digunakan, kirimkan permintaan layanan.

Misalnya, ada Manajemen | Pemantauan dan pemberitahuan | penindasan CloudWatch alarm | Perbarui CT yang hanya internal. AMS menggunakannya untuk menyebarkan pembaruan infrastruktur (seperti menambal) untuk mematikan pemberitahuan alarm yang mungkin dipicu oleh pembaruan secara keliru. Ketika CT ini dikirimkan, Anda akan melihat RFC untuk CT dalam daftar RFC Anda. CT internal apa pun yang digunakan dalam RFC akan muncul di daftar RFC Anda.

Ubah skema tipe

Semua jenis perubahan menyediakan skema JSON untuk masukan Anda dalam pembuatan, modifikasi, atau akses, sumber daya. Skema menyediakan parameter, dan deskripsinya, bagi Anda untuk membuat permintaan perubahan (RFC).

Keberhasilan eksekusi RFC menghasilkan output eksekusi. Untuk penyediaan RFCs, output eksekusi menyertakan “stack_id” yang mewakili tumpukan CloudFormation dan dapat dicari di konsol. CloudFormation Output eksekusi terkadang menyertakan output ID dari instance yang dibuat dan ID tersebut dapat digunakan untuk mencari instance di konsol AWS yang sesuai. <stack-xxxx>Misalnya, output eksekusi Create ELB CT menyertakan “stack_id” yang dapat dicari CloudFormation dan

mengeluarkan nilai key=ELB = yang dapat dicari di konsol Amazon untuk Elastic Load Balancing. EC2

Mari kita periksa skema CT. Ini adalah skema untuk CodeDeploy Application Create, skema yang cukup kecil. Beberapa skema memiliki `Parameter` area yang sangat luas.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
  resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
 vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv00000000000",
      "type": "string",
      "enum": ["stm-sft6rv00000000000"]
    },
    "Name":{
      "description": "A name for the stack or stack component
;
      this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "Tags": {
      "description": "Up to seven tags (key/value pairs) to
      categorize the resource.",
```

Bagian pertama dari skema memberikan informasi kepada AMS tentang jenis perubahan yang diminta.

```
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "Key": {
            "type": "string",
            "minLength": 1,
            "maxLength": 127
          },
          "Value": {
            "type": "string",
            "minLength": 1,
            "maxLength": 255
          }
        },
        "additionalProperties": false,
        "required": [
          "Key",
          "Value"
        ]
      },
      "minItems": 1,
      "maxItems": 7
    },
    "TimeoutInMinutes": {
      "description": "The maximum amount of time, in minutes,
to
      allow for execution of the change. This will not prolong
execution,
      but the RFC fails if the change is not completed in the
specified time.
      Valid values are 60 up to 360, for long-running
UserData.",
      "type": "number",
      "minimum": 0,
      "maximum": 60
    },
    "Parameters": {
      "description": "Specifications for the stack.",
      "type": "object",
      "properties": {
        "CodeDeployApplicationName": {
          "description": "The name of an AWS CodeDeploy
application.",
```

TimeoutInMinutes Parameter ini memungkinkan Anda untuk menunjukkan waktu batas untuk menjalankan jenis perubahan. Nilai yang valid adalah 60 hingga 360, untuk jangka panjang UserData.

Bagian Parameter adalah tempat Anda menentukan pengaturan untuk sumber daya yang Anda buat, atau tindakan yang Anda minta.

Bagian “properti tambahan” memberi

```
          "type": "string",
          "minLength": 1,
          "maxLength": 100,
          "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
        }
      },
      "additionalProperties": false,
      "required": [
        "CodeDeployApplicationName"
      ]
    }
  },
  "additionalProperties": false,
  "required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
  ]
}
```

tahu Anda parameter apa yang diperluka n dan mana yang opsional.

> **Note**
>
> Skema ini memungkinkan hingga tujuh tag; namun, EFS EC2, RDS, dan skema pembuatan multi-tier memungkinkan hingga 50 tag.

Mengelola izin untuk jenis perubahan

Anda dapat menggunakan kebijakan khusus untuk membatasi jenis perubahan (CTs) yang tersedia untuk grup atau pengguna yang berbeda.

Untuk mempelajari lebih lanjut tentang melakukan hal ini, lihat bagian Panduan Pengguna AMS Menyetel Izin.

Menyunting informasi sensitif dari jenis perubahan

Skema jenis perubahan AMS menawarkan atribut parameter, `"metadata":"ams:sensitive":"true"` yang digunakan untuk parameter yang berisi informasi

sensitif, seperti kata sandi. Ketika atribut ini disetel, masukan yang diberikan dikaburkan. Perhatikan bahwa Anda tidak dapat menyetel atribut parameter ini; namun, jika Anda bekerja dengan AMS untuk membuat tipe perubahan dan memiliki parameter yang ingin dikaburkan pada input, Anda dapat meminta ini.

Menemukan jenis perubahan, menggunakan opsi kueri

Contoh ini menunjukkan cara menggunakan Konsol AMS untuk menemukan jenis perubahan yang sesuai untuk RFC yang ingin Anda kirimkan.

Anda dapat menggunakan konsol atau API/CLI untuk menemukan perubahan jenis ID (CT) atau versi. Ada dua metode, baik pencarian atau memilih klasifikasi. Untuk kedua jenis pilihan, Anda dapat mengurutkan pencarian dengan memilih Paling sering digunakan, Paling baru digunakan, atau Alfabetis.

YouTube Video: Bagaimana cara membuat RFC menggunakan AWS Managed Services CLI dan di mana saya dapat menemukan Skema CT?

Di konsol AMS, pada halaman RFCs-> Buat RFC:

- Dengan Browse by change type yang dipilih (default), baik:
  - Gunakan area Quick create untuk memilih dari AMS yang paling populer CTs. Klik pada label dan halaman Jalankan RFC terbuka dengan opsi Subjek diisi otomatis untuk Anda. Selesaikan opsi yang tersisa sesuai kebutuhan dan klik Jalankan untuk mengirimkan RFC.
  - Atau, gulir ke bawah ke Semua jenis perubahan area dan mulai mengetik nama CT di kotak opsi, Anda tidak harus memiliki nama jenis perubahan yang tepat atau lengkap. Anda juga dapat mencari CT dengan mengubah jenis ID, klasifikasi, atau mode eksekusi (otomatis atau manual) dengan memasukkan kata-kata yang relevan.

    Dengan tampilan Kartu default yang dipilih, kartu CT yang cocok muncul saat Anda mengetik, pilih kartu dan klik Buat RFC. Dengan tampilan Tabel dipilih, pilih CT yang relevan dan klik Buat RFC. Kedua metode membuka halaman Run RFC.
- Atau, dan untuk menjelajahi pilihan jenis perubahan, klik Pilih berdasarkan kategori di bagian atas halaman untuk membuka serangkaian kotak opsi drop-down.
- Pilih Kategori, Subkategori, Item, dan Operasi. Kotak informasi untuk jenis perubahan itu muncul panel muncul di bagian bawah halaman.
- Saat Anda siap, tekan Enter, dan daftar jenis perubahan yang cocok akan muncul.

- Pilih jenis perubahan dari daftar. Kotak informasi untuk jenis perubahan itu muncul di bagian bawah halaman.
- Setelah Anda memiliki jenis perubahan yang benar, pilih Buat RFC.

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

> **Note**
>
> Titik akhir AMS API/CLI (amscm dan amsskms) berada di Wilayah AWS N. Virginia,. `us-east-1` Bergantung pada cara autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan`--profile saml`, jika itu adalah metode otentikasi Anda.

Untuk mencari jenis perubahan menggunakan AMS CM API (lihat ListChangeTypeClassificationSummaries) atau CLI:

Anda dapat menggunakan filter atau kueri untuk mencari. ListChangeTypeClassificationSummaries Operasi memiliki opsi Filter untuk`Category`,`Subcategory`,`Item`, dan`Operation`, tetapi nilainya harus sama persis dengan nilai yang ada. Untuk hasil yang lebih fleksibel saat menggunakan CLI, Anda dapat menggunakan opsi. `--query`

Ubah jenis penyaringan dengan AMS CM API/CLI

Atribut	Nilai valid	Kondisi valid/default	Catatan
ChangeTypeId	String apa pun yang mewakili ChangeTypeId (Misalnya: ct-abc123xyz7890)	Setara	Untuk jenis perubahan IDs, lihat Referensi Ubah Jenis. Untuk jenis perubahan IDs, lihat Menemukan Jenis Perubahan atau CSIO.
Kategori	Teks bentuk bebas apa pun	Contains	Ekspresi reguler di setiap bidang individu tidak didukung. Pencarian yang tidak peka huruf besar/kecil
Subkategori			
Item			
Operasi			

1. Berikut adalah beberapa contoh klasifikasi jenis perubahan daftar:

   Perintah berikut mencantumkan semua kategori jenis perubahan.

   ```
   aws amscm list-change-type-categories
   ```

   Perintah berikut mencantumkan subkategori milik kategori tertentu.

   ```
   aws amscm list-change-type-subcategories --category CATEGORY
   ```

   Perintah berikut mencantumkan item milik kategori dan subkategori tertentu.

   ```
   aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
   ```

2. Berikut adalah beberapa contoh pencarian jenis perubahan dengan kueri CLI:

Perintah berikut mencari ringkasan klasifikasi CT untuk yang berisi “S3" di Nama item dan membuat output dari kategori, subkategori, item, operasi, dan mengubah ID tipe dalam bentuk tabel.

```
aws amscm list-change-type-classification-summaries --query
 "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

```
+-------------------------------------------------------------+
|              ListChangeTypeClassificationSummaries          |
+----------+-------------------------+--+------+--------------+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+----------+-------------------------+--+------+--------------+
```

3. Anda kemudian dapat menggunakan ID tipe perubahan untuk mendapatkan skema CT dan memeriksa parameternya. Perintah berikut output skema ke file JSON bernama creates3params.schema.json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3Params.schema.json
```

Untuk informasi tentang penggunaan kueri CLI, lihat Cara Memfilter Output dengan Opsi --query dan referensi bahasa kueri, Spesifikasi. JMESPath

4. Setelah Anda memiliki ID tipe perubahan, kami sarankan untuk memverifikasi versi untuk jenis perubahan untuk memastikan itu adalah versi terbaru. Gunakan perintah ini untuk menemukan versi untuk jenis perubahan tertentu:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

Untuk menemukan tipe perubahan tertentu, jalankan perintah ini: `AutomationStatus`

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

Untuk menemukan tipe perubahan tertentu, jalankan perintah ini: `ExpectedExecutionDurationInMinutes`

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h
 --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Memecahkan masalah kesalahan RFC di AMS

Banyak kegagalan RFC penyediaan AMS dapat diselidiki melalui dokumentasi. CloudFormation Lihat Pemecahan Masalah AWS CloudFormation: Kesalahan Pemecahan Masalah

Saran pemecahan masalah tambahan disediakan di bagian berikut.

Kesalahan RFC “Manajemen” di AMS

AMS “Manajemen” Jenis perubahan kategori (CTs) memungkinkan Anda untuk meminta akses ke sumber daya serta mengelola sumber daya yang ada. Bagian ini menjelaskan beberapa masalah umum.

Kesalahan akses RFC

- Pastikan Username dan FQDN yang Anda tentukan di RFC sudah benar dan ada di domain. Untuk bantuan menemukan FQDN Anda, lihat Menemukan FQDN Anda.
- Pastikan ID tumpukan yang Anda tentukan untuk akses adalah tumpukan EC2 -related. Tumpukan seperti ELB dan Amazon Simple Storage Service (S3) bukan kandidat untuk RFCs akses, sebagai gantinya, gunakan peran akses baca saja untuk mengakses sumber daya tumpukan ini. Untuk bantuan menemukan ID tumpukan, lihat Menemukan tumpukan IDs
- Pastikan ID tumpukan yang Anda berikan sudah benar dan milik akun yang relevan.

Untuk bantuan terkait kegagalan akses RFC lainnya, lihat Manajemen akses.

YouTube Video: Bagaimana cara mengajukan Request for Change (RFC) dengan benar untuk menghindari penolakan dan kegagalan?

Kesalahan penjadwalan CT RFC (manual)

Sebagian besar jenis perubahan adalah ExecutionMode = Otomatis, tetapi beberapa ExecutionMode = Manual dan itu memengaruhi cara Anda menjadwalkannya untuk menghindari kegagalan RFC.

Dijadwalkan RFCs dengan ExecutionMode =Manual, harus diatur untuk mengeksekusi setidaknya 24 jam di masa mendatang jika Anda menggunakan Konsol AMS untuk membuat RFC. Peringatan ini

tidak berlaku untuk AMS API/CLI, tetapi masih penting untuk menjadwalkan Manual RFCs setidaknya 8 jam ke depan.

AMS bertujuan untuk menanggapi CT manual dalam waktu empat jam, dan akan berkorespondensi sesegera mungkin, tetapi bisa memakan waktu lebih lama bagi RFC untuk benar-benar dieksekusi.

Menggunakan RFCs dengan pembaruan manual CTs

Operasi AMS menolak Manajemen | Lainnya | Lainnya RFCs untuk pembaruan tumpukan, ketika ada jenis perubahan Pembaruan untuk jenis tumpukan yang ingin Anda perbarui.

Kesalahan tumpukan hapus RFC

Kegagalan tumpukan penghapusan RFC: Jika Anda menggunakan Manajemen | Tumpukan standar | Tumpukan | Hapus CT, Anda akan melihat peristiwa terperinci di CloudFormation Konsol untuk tumpukan dengan nama tumpukan AMS. Anda dapat mengidentifikasi tumpukan Anda dengan memeriksanya terhadap nama yang ada di Konsol AMS. CloudFormation Konsol memberikan rincian lebih lanjut tentang penyebab kegagalan.

Sebelum menghapus tumpukan, Anda harus mempertimbangkan bagaimana tumpukan dibuat. Jika Anda membuat tumpukan menggunakan AMS CT dan tidak menambahkan atau mengedit sumber daya tumpukan, Anda dapat menghapusnya tanpa masalah. Namun, itu adalah ide yang baik untuk Anda menghapus sumber daya yang ditambahkan secara manual dari tumpukan sebelum mengirimkan tumpukan hapus RFC terhadapnya. Misalnya, jika Anda membuat tumpukan menggunakan tumpukan penuh CT (HA Two Tier), itu termasuk grup keamanan - SG1. Jika Anda kemudian menggunakan AMS untuk membuat grup keamanan lain - SG2, dan mereferensikan yang baru SG2 di SG1 dibuat sebagai bagian dari tumpukan penuh, dan kemudian menggunakan CT tumpukan hapus untuk menghapus tumpukan, tidak SG1 akan dihapus seperti yang direferensikan oleh SG2.

> **Important**
>
> Menghapus tumpukan dapat memiliki konsekuensi yang tidak diinginkan dan tidak terduga. AMS lebih suka *tidak* menghapus tumpukan atau menumpuk sumber daya atas nama pelanggan karena alasan ini. Perhatikan, AMS hanya akan menghapus sumber daya atas nama Anda (melalui Mangement yang dikirimkan | Lainnya | Lainnya | Jenis perubahan pembaruan) yang tidak mungkin dihapus menggunakan jenis perubahan yang sesuai, otomatis, untuk dihapus. Pertimbangan tambahan:

- Jika sumber daya diaktifkan untuk 'hapus perlindungan', AMS dapat membantu membuka blokir ini jika Anda mengirimkan Manajemen | Lainnya | Lainnya | Perbarui jenis perubahan dan, setelah perlindungan penghapusan dihapus, Anda dapat menggunakan CT otomatis untuk menghapus sumber daya tersebut.
- Jika ada beberapa sumber daya dalam tumpukan, dan Anda hanya ingin menghapus sebagian dari sumber daya tumpukan, gunakan jenis perubahan CloudFormation Pembaruan (lihat CloudFormation Ingest Stack: Update). Anda juga dapat mengirimkan Manajemen | Lainnya | Lainnya | Perbarui jenis perubahan dan insinyur AMS dapat membantu Anda menyusun set perubahan, jika diperlukan.
- Jika ada masalah dalam menggunakan CT CloudFormation Pembaruan karena drift, AMS dapat membantu jika Anda mengirimkan Manajemen | Lainnya | Lainnya | Pembaruan untuk menyelesaikan penyimpangan (sejauh yang didukung oleh CloudFormation Layanan AWS) dan memberikan ChangeSet yang kemudian dapat Anda validasi dan jalankan menggunakan CT, Management/Custom Stack/Stack From CloudFormation Template/ Approve Changeset, dan Pembaruan otomatis.

AMS mempertahankan pembatasan di atas untuk membantu memastikan tidak ada penghapusan sumber daya yang tidak terduga atau tidak terduga.

Untuk informasi selengkapnya, lihat Pemecahan Masalah AWS CloudFormation: menghapus tumpukan gagal.

Kesalahan DNS pembaruan RFC

Beberapa RFCs untuk memperbarui zona yang dihosting DNS dapat gagal, beberapa tanpa alasan. Membuat beberapa RFCs sekaligus untuk memperbarui zona yang dihosting DNS (pribadi atau publik) dapat menyebabkan beberapa RFCs gagal karena mereka mencoba memperbarui tumpukan yang sama pada saat yang bersamaan. Manajemen perubahan AMS menolak atau gagal RFCs yang tidak dapat memperbarui tumpukan karena tumpukan sudah diperbarui oleh RFC lain. AMS merekomendasikan agar Anda membuat satu RFC sekaligus dan menunggu RFC berhasil sebelum menaikkan yang baru untuk tumpukan yang sama.

Kesalahan entitas IAM RFC

AMS menyediakan sejumlah peran dan profil IAM default ke dalam akun AMS yang dirancang untuk memenuhi kebutuhan Anda. Namun, Anda mungkin perlu meminta sumber daya IAM tambahan sesekali.

Proses untuk mengirimkan RFCs permintaan sumber daya IAM kustom mengikuti alur kerja standar untuk manual RFCs, tetapi proses persetujuan juga mencakup tinjauan keamanan untuk memastikan kontrol keamanan yang tepat ada. Oleh karena itu, prosesnya biasanya memakan waktu lebih lama daripada manual lainnya RFCs. Untuk mengurangi waktu siklus ini RFCs, ikuti panduan berikut.

Untuk informasi tentang apa yang kami maksud dengan tinjauan IAM dan cara memetakannya ke Standar Teknis dan proses Penerimaan Risiko kami, lihatMemahami ulasan keamanan RFC.

Permintaan sumber daya IAM umum:

- Jika Anda meminta kebijakan yang berkaitan dengan aplikasi utama yang kompatibel dengan cloud, misalnya CloudEndure, lihat CloudEndure kebijakan IAM AMS yang telah disetujui sebelumnya: Buka paket file Contoh Zona Pendaratan WIGs Cloud Endure dan buka file `customer_cloud_endure_policy.json`

  > **Note**
  >
  > Jika Anda menginginkan kebijakan yang lebih permisif, diskusikan kebutuhan Anda dengan Anda CloudArchitect/CSDM dan dapatkan, jika diperlukan, AMS Security Review and Signoff sebelum mengirimkan RFC yang menerapkan kebijakan tersebut.

- Jika Anda ingin mengubah sumber daya yang digunakan oleh AMS di akun Anda secara default, sebaiknya Anda meminta salinan sumber daya yang dimodifikasi, bukan perubahan pada yang sudah ada.
- Jika Anda meminta izin untuk pengguna manusia (alih-alih melampirkan izin ke pengguna) lampirkan izin ke peran, lalu berikan izin kepada pengguna untuk mengambil peran tersebut. Untuk detail tentang hal ini, lihat Akses konsol AMS Advanced sementara.
- Jika Anda memerlukan izin luar biasa untuk migrasi sementara atau alur kerja, berikan tanggal akhir untuk izin tersebut dalam permintaan Anda.
- Jika Anda telah mendiskusikan subjek permintaan Anda dengan tim keamanan Anda, berikan bukti persetujuan mereka kepada CSDM Anda dengan sedetail mungkin.

Jika AMS menolak IAM RFC, kami memberikan alasan yang jelas untuk penolakan tersebut. Misalnya, kami mungkin menolak permintaan pembuatan kebijakan IAM dan menjelaskan kebijakan yang tidak pantas. Dalam hal ini, Anda dapat membuat perubahan yang diidentifikasi dan mengirimkan kembali permintaan. Jika kejelasan tambahan tentang status permintaan diperlukan, kirimkan permintaan layanan, atau hubungi CSDM Anda.

Daftar berikut menjelaskan risiko umum yang AMS coba mitigasi saat kami meninjau IAM Anda. RFCs Jika IAM RFC Anda memiliki salah satu risiko ini, itu dapat mengakibatkan penolakan RFC. Dalam kasus di mana Anda memerlukan pengecualian, AMS meminta persetujuan dari tim keamanan Anda. Untuk mencari pengecualian seperti itu, koordinasikan dengan CSDM Anda.

> **Note**
>
> AMS dapat, dengan alasan apa pun, menolak perubahan apa pun pada sumber daya IAM di dalam akun. Untuk masalah mengenai penolakan RFC, hubungi Operasi AMS melalui permintaan layanan, atau hubungi CSDM Anda.

- Eskalasi hak istimewa, seperti izin yang memungkinkan Anda mengubah izin Anda sendiri, atau untuk mengubah izin sumber daya lain di dalam akun. Contoh:
  - Penggunaan `iam:PassRole` dengan peran lain yang lebih istimewa.
  - Izin untuk kebijakan attach/detach IAM dari peran atau pengguna.
  - Modifikasi kebijakan IAM di akun.
  - Kemampuan untuk melakukan panggilan API dalam konteks infrastruktur manajemen.
- Izin untuk mengubah sumber daya atau aplikasi yang diperlukan untuk menyediakan layanan AMS kepada Anda. Contoh:
  - Modifikasi infrastruktur AMS seperti benteng, host manajemen, atau infrastruktur EPS.
  - Penghapusan fungsi AWS Lambda manajemen log, atau aliran log.
  - Penghapusan atau modifikasi aplikasi CloudTrail pemantauan default.
  - Modifikasi Direktori Layanan Direktori Aktif (AD).
  - Menonaktifkan alarm CloudWatch (CW).
  - Modifikasi prinsip, kebijakan, dan ruang nama yang digunakan di akun sebagai bagian dari landing zone.
- Penyebaran infrastruktur di luar praktik terbaik, seperti izin yang memungkinkan pembuatan infrastruktur dalam keadaan yang membahayakan keamanan informasi Anda. Contoh:

  - Pembuatan bucket S3 publik, atau tidak terenkripsi, atau berbagi volume EBS secara publik.
  - Penyediaan alamat IP publik.
  - Modifikasi kelompok keamanan untuk memungkinkan akses luas.
- Izin yang terlalu luas yang dapat menyebabkan dampak aplikasi, seperti izin yang dapat mengakibatkan kehilangan data, kehilangan integritas, konfigurasi yang tidak tepat, atau gangguan layanan untuk infrastruktur Anda dan aplikasi di dalam akun. Contoh:
  - Menonaktifkan, atau mengarahkan, lalu lintas jaringan melalui suka atau. APIs `ModifyNetworkInterfaceAttribute` `UpdateRouteTable`
  - Menonaktifkan infrastruktur terkelola dengan melepaskan volume dari host yang dikelola.
- Izin untuk layanan bukan bagian dari deskripsi layanan AMS dan tidak didukung oleh AMS.

  Layanan yang tidak tercantum dalam deskripsi Layanan AMS tidak dapat digunakan di akun AMS. Untuk meminta dukungan untuk fitur atau layanan, silakan hubungi CSDM Anda.
- Izin yang tidak memenuhi tujuan yang Anda nyatakan karena terlalu murah hati, atau terlalu konservatif, atau diterapkan pada sumber daya yang salah. Contoh:
  - Permintaan `s3:PutObject` izin ke bucket S3 yang memiliki enkripsi KMS wajib, tanpa `KMS:Encrypt` izin ke kunci yang relevan.
  - Izin yang berkaitan dengan sumber daya yang tidak ada di akun.
  - IAM RFCs di mana deskripsi RFC tampaknya tidak cocok dengan permintaan.

Kesalahan RFC “Penerapan”

AMS “Deployment” Jenis perubahan kategori (CTs) memungkinkan Anda untuk meminta berbagai sumber daya yang didukung AMS ditambahkan ke akun Anda.

Sebagian besar AMS CTs yang membuat sumber daya didasarkan pada CloudFormation templat. Sebagai pelanggan, Anda memiliki akses hanya-baca ke semua layanan AWS termasuk CloudFormation, Anda dapat dengan cepat mengidentifikasi CloudFormation tumpukan yang mewakili tumpukan Anda berdasarkan deskripsi tumpukan menggunakan CloudFormation Konsol. Tumpukan yang gagal kemungkinan akan berada dalam keadaan DELETE_COMPLETE. Setelah Anda mengidentifikasi CloudFormation tumpukan, peristiwa akan menunjukkan sumber daya spesifik yang gagal dibuat, dan mengapa.

Menggunakan CloudFormation dokumentasi untuk memecahkan masalah

Sebagian besar penyediaan AMS RFCs menggunakan CloudFormation templat dan dokumentasi tersebut dapat membantu pemecahan masalah. Lihat dokumentasi untuk CloudFormation template itu:

- Buat kegagalan penyeimbang beban aplikasi: AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer)
- Buat grup penskalaan Otomatis: AWS::AutoScaling::AutoScalingGroup (Grup Auto Scaling)
- Buat cache memcache: AWS::ElastiCache::CacheCluster (Cache Cluster)
- Buat cache Redis: AWS::ElastiCache::CacheCluster (Cache Cluster)
- Buat DNS Hosted Zone (digunakan dengan Create DNS private/public): AWS::Route53::HostedZone (R53 Hosted Zone)
- Buat DNS Record Set (digunakan dengan Create DNS private/public): AWS::Route53::RecordSet (Resource Record Set)
- Buat EC2 tumpukan: AWS::EC2::Instance (Elastic Compute Cloud)
- Buat Sistem File Elastis (EFS): AWS::EFS::FileSystem (Sistem File Elastis)
- Buat Load balancer: AWS::ElasticLoadBalancing::LoadBalancer (Elastic Load Balancer)
- Buat RDS DB: AWS::RDS::DBInstance (Database Relasional)
- Buat Amazon S3: AWS::S3::Bucket (Layanan Penyimpanan Sederhana)
- Buat Antrian: AWS::SQS::Queue (Layanan Antrian Sederhana)

RFC membuat kesalahan AMIs

Amazon Machine Image (AMI) adalah templat yang berisi konfigurasi perangkat lunak (misalnya, sistem operasi, server aplikasi, dan aplikasi). Dari AMI, Anda meluncurkan instance, yang merupakan salinan AMI yang berjalan sebagai server virtual di cloud. AMIs sangat berguna, dan diperlukan untuk membuat EC2 instance atau grup Auto Scaling; namun, Anda harus mematuhi beberapa persyaratan:

- Instance yang Anda tentukan `Ec2InstanceId` harus dalam keadaan berhenti agar RFC berhasil. Jangan gunakan instans Auto Scaling group (ASG) untuk parameter ini karena ASG akan menghentikan instance yang dihentikan.
- Untuk membuat AMS Amazon Machine Image (AMI), Anda harus memulai dengan instance AMS. Sebelum Anda dapat menggunakan instance untuk membuat AMI, Anda harus menyiapkannya

dengan memastikan bahwa instans tersebut dihentikan dan tidak bergabung dari domainnya. Untuk detailnya, lihat Membuat Gambar Mesin Amazon Standar Menggunakan Sysprep

- Nama yang Anda tentukan untuk AMI baru harus unik di dalam akun atau RFC gagal. Cara melakukannya dijelaskan dalam AMI | Buat, dan untuk detail selengkapnya, lihat dan AWS AMI Design.

> **Note**
>
> Untuk informasi tambahan tentang persiapan pembuatan AMI, lihat AMI | Buat.

RFCs membuat EC2s atau ASGs kesalahan

Untuk EC2 atau kegagalan ASG dengan batas waktu, AMS menyarankan Anda mengonfirmasi apakah AMI yang digunakan disesuaikan. Jika ya, silakan lihat langkah-langkah pembuatan AMI yang disertakan dalam panduan ini (lihat AMI | Buat) untuk memastikan bahwa AMI dibuat dengan benar. Kesalahan umum saat membuat AMI kustom adalah tidak mengikuti langkah-langkah dalam panduan untuk mengganti nama atau memanggil Sysprep.

RFCs membuat kesalahan RDS

Kegagalan Amazon Relational Database Service (RDS) dapat terjadi karena berbagai alasan karena Anda dapat menggunakan banyak mesin yang berbeda saat membuat RDS, dan setiap mesin memiliki persyaratan dan keterbatasannya sendiri. Sebelum mencoba membuat tumpukan AMS RDS, tinjau nilai parameter AWS RDS dengan cermat, lihat Membuat. DBInstance

Untuk mempelajari lebih lanjut tentang Amazon RDS secara umum, termasuk rekomendasi ukuran, lihat Dokumentasi Layanan Amazon Relational Database Service.

RFCs membuat kesalahan Amazon S3

Satu kesalahan umum saat membuat bucket penyimpanan S3 adalah tidak menggunakan nama unik untuk bucket. Jika Anda mengirimkan bucket S3 Create CT dengan nama yang sama dengan yang dikirimkan sebelumnya, itu akan gagal karena bucket S3 sudah ada dengan itu. BucketName Ini akan dirinci di CloudFormation Konsol, di mana Anda akan melihat bahwa peristiwa tumpukan menunjukkan bahwa nama bucket sudah digunakan.

Validasi RFC versus kesalahan eksekusi

Kegagalan RFC dan pesan terkait berbeda dalam pesan keluaran pada halaman detail RFC konsol AMS untuk RFC yang dipilih:

- Alasan Kegagalan Validasi hanya tersedia di Bidang Status
- Alasan Kegagalan Eksekusi tersedia di Output Eksekusi serta Bidang Status.

Pesan kesalahan RFC

Ketika Anda menemukan kesalahan berikut untuk jenis perubahan yang tercantum (CTs), Anda dapat menggunakan solusi ini untuk membantu Anda menemukan sumber masalah dan memperbaikinya.

```
{"errorMessage":"An error has occurred during RFC execution. We are
investigating the issue.","errorType":"InternalError"}
```

Jika Anda memerlukan bantuan lebih lanjut setelah merujuk pada opsi pemecahan masalah berikut, maka libatkan AMS melalui korespondensi RFC atau buat permintaan layanan. Lihat Korespondensi dan Lampiran RFC (Konsol) dan Membuat Permintaan Layanan di AMS untuk detail selengkapnya.

Kesalahan konsumsi beban kerja (WIGS)

> **Note**
>
> Alat validasi untuk Windows dan Linux dapat diunduh dan dijalankan langsung di server lokal Anda, serta EC2 instance di AWS. Hal ini dapat ditemukan melalui Panduan Pengembang Aplikasi AMS Advanced Migrating workloads: Linux pre-ingestion validation dan Migrating workloads: Windows pre-ingestion validation.

- Pastikan EC2 instance ada di akun AMS target. Misalnya, jika Anda telah membagikan AMI dari akun non-AMS ke akun AMS, Anda harus membuat EC2 instance di akun AMS dengan AMI bersama sebelum dapat mengirimkan RFC Workload Ingest.
- Periksa untuk melihat apakah grup keamanan yang dilampirkan pada instance memiliki lalu lintas jalan keluar yang diizinkan. Agen SSM harus dapat terhubung ke titik akhir publiknya.

- Periksa untuk melihat apakah instance memiliki izin yang tepat untuk terhubung dengan agen SSM. Izin ini disertakan dengan`customer-mc-ec2-instance-profile`, Anda dapat memeriksanya di EC2 konsol:

EC2 kesalahan penghentian tumpukan contoh

- Periksa untuk melihat apakah instance sudah dalam keadaan berhenti atau dihentikan.
- Jika EC2 instans sedang online dan Anda melihat `InternalError` kesalahan, maka kirimkan permintaan layanan untuk diselidiki AMS.
- Perhatikan bahwa Anda tidak dapat menggunakan tipe perubahan Management | Advanced stack components | EC2 instance stack | Stop ct-3mvvt2zkyveqj untuk menghentikan instance Auto Scaling group (ASG). Jika Anda perlu menghentikan instans ASG, maka kirimkan permintaan layanan.

EC2 instance stack membuat kesalahan

`InternalError`Pesannya berasal dari CloudFormation; alasan status CREATION_FAILED. Anda dapat menemukan detail tentang kegagalan tumpukan dalam peristiwa CloudWatch tumpukan dengan mengikuti langkah-langkah berikut:

- Di konsol AWS Management, Anda dapat melihat daftar peristiwa tumpukan saat tumpukan dibuat, diperbarui, atau dihapus. Dari daftar ini, temukan peristiwa kegagalan dan kemudian lihat alasan status untuk peristiwa tersebut.

  Alasan status mungkin berisi pesan kesalahan dari AWS CloudFormation atau dari layanan tertentu yang dapat membantu Anda memahami masalah tersebut.
- Untuk informasi selengkapnya tentang melihat peristiwa tumpukan, lihat Melihat Data dan Sumber Daya AWS CloudFormation Stack di AWS Management Console.

EC2 kesalahan pemulihan volume instance

AMS membuat RFC pemecahan masalah internal saat pemulihan volume EC2 instans gagal. Ini dilakukan karena pemulihan volume EC2 instans merupakan bagian penting dari pemulihan bencana (DR) dan AMS membuat RFC pemecahan masalah internal ini untuk Anda secara otomatis.

Saat RFC pemecahan masalah internal dibuat, spanduk ditampilkan memberi Anda tautan ke RFC. Pemecahan masalah internal RFC ini memberi Anda lebih banyak visibilitas ke kegagalan RFC dan, daripada mengirimkan percobaan ulang yang RFCs mengarah ke kesalahan yang sama, atau membuat Anda secara manual menjangkau AMS untuk kegagalan ini, Anda dapat melacak perubahan Anda dan mengetahui bahwa kegagalan sedang dikerjakan oleh AMS. Ini juga mengurangi metrik time-to-recovery (TTR) untuk perubahannya karena Operator AMS secara proaktif bekerja pada kegagalan RFC alih-alih menunggu permintaan Anda.

Cara mendapatkan bantuan dengan RFC

Anda dapat menghubungi AMS untuk mengidentifikasi akar penyebab kegagalan Anda. Jam kerja AMS adalah 24 jam sehari, 7 hari seminggu, 365 hari setahun.

AMS menyediakan beberapa jalan bagi Anda untuk meminta bantuan atau membuat permintaan layanan.

- Untuk meminta informasi atau saran, atau akses ke layanan TI yang dikelola AMS, atau meminta layanan tambahan dari AMS, gunakan konsol AMS dan kirimkan permintaan layanan. Untuk detailnya, lihat Membuat Permintaan Layanan. Untuk informasi umum tentang permintaan layanan AMS, lihat Manajemen Permintaan Layanan.
- Untuk melaporkan masalah kinerja layanan AWS atau AMS yang memengaruhi lingkungan terkelola Anda, gunakan konsol AMS dan kirimkan laporan insiden. Untuk detailnya, lihat Melaporkan Insiden. Untuk informasi umum tentang manajemen insiden AMS, lihat Respons insiden.
- Untuk pertanyaan spesifik tentang bagaimana Anda atau sumber daya atau aplikasi Anda bekerja dengan AMS, atau untuk meningkatkan insiden, kirim email ke satu atau beberapa hal berikut:
  1. Pertama, jika Anda tidak puas dengan permintaan layanan atau tanggapan laporan insiden, kirimkan email ke CSDM Anda: ams-csdm@amazon.com
  2. Selanjutnya, jika eskalasi diperlukan, Anda dapat mengirim email ke Manajer Operasi AMS (tetapi CSDM Anda mungkin akan melakukannya): ams-opsmanager@amazon.com
  3. Eskalasi lebih lanjut akan ke Direktur AMS: ams-director@amazon.com
  4. Akhirnya, Anda selalu dapat menghubungi AMS VP: ams-vp@amazon.com

Mode Perubahan Langsung di AMS

Topik

- Memulai dengan mode Perubahan Langsung
- Keamanan dan kepatuhan
- Ubah manajemen dalam mode Perubahan Langsung
- Membuat tumpukan menggunakan mode Perubahan Langsung
- Kasus penggunaan Mode Perubahan Langsung

AWS Managed Services (AMS) Direct Change mode (DCM) memperluas manajemen perubahan AMS Advanced dengan menyediakan AWS akses asli ke akun AMS Advanced Plus dan Premium untuk menyediakan dan memperbarui AWS sumber daya. Dengan DCM, Anda memiliki opsi untuk menggunakan AWS API asli (konsol atau CLI/SDK) atau permintaan manajemen perubahan AMS Advanced untuk perubahan (RFCs), dan dalam kedua kasus sumber daya dan perubahannya sepenuhnya didukung oleh AMS, termasuk pemantauan, tambalan, cadangan, manajemen respons insiden. Sumber daya yang disediakan melalui DCM terdaftar di sistem manajemen pengetahuan layanan AMS (SKMS), bergabung dengan domain Active Directory yang dikelola AMS (bila berlaku), dan menjalankan agen manajemen AMS. Gunakan perkakas yang ada (misalnya, AWS SDK CloudFormation, dan CDK) untuk mengembangkan dan menerapkan tumpukan yang dikelola AMS. CloudFormation

> **Note**
>
> Mode Perubahan Langsung tidak menghapus manajemen perubahan AMS RFCs. Anda memiliki akses penuh ke AMS RFCs dengan DCM.

Tonton video Akash untuk mempelajari lebih lanjut (6:30)

Memulai dengan mode Perubahan Langsung

Mulailah dengan memeriksa prasyarat dan kemudian mengirimkan permintaan perubahan (RFC) di akun AMS Advanced Anda yang memenuhi syarat.

1. Konfirmasikan bahwa akun yang ingin Anda gunakan dengan DCM memenuhi persyaratan:

   - Akun tersebut adalah AMS Advanced Plus atau Premium.
   - Akun tidak mengaktifkan Service Catalog. Saat ini kami tidak mendukung akun orientasi ke DCM dan Service Catalog secara bersamaan. Jika Anda sudah onboard ke Service Catalog tetapi tertarik dengan DCM, diskusikan kebutuhan Anda dengan manajer pengiriman layanan

cloud (CSDM) Anda. Jika Anda memutuskan untuk beralih dari Service Catalog ke DCM, offboard Service Catalog, untuk melakukan itu, sertakan permintaan dalam permintaan perubahan di bawah ini. Untuk detail tentang Service Catalog di AMS, lihat AMS dan Service Catalog.

2. Kirim permintaan perubahan (RFC) menggunakan Manajemen | Akun terkelola | Mode Perubahan Langsung | Aktifkan jenis perubahan (ct-3rd4781c2nnhp). Untuk contoh panduan, lihat Mode Perubahan Langsung | Aktifkan.

   Setelah CT diproses, peran IAM yang telah ditentukan sebelumnya, `AWSManagedServicesCloudFormationAdminRole` dan `AWSManagedServicesUpdateRole` disediakan dalam akun yang ditentukan.

3. Tetapkan peran yang sesuai untuk pengguna yang memerlukan akses DCM menggunakan proses federasi internal Anda.

> **Note**
>
> Anda dapat menentukan sejumlah SAMLIdentity Penyedia, AWS Layanan, dan Entitas IAM (Peran, Pengguna, dll) untuk mengambil peran. Anda harus memberikan setidaknya satu:`SAMLIdentityProviderARNs`,`IAMEntityARNs`, atau`AWSServicePrincipals`. Untuk informasi lebih lanjut, konsultasikan dengan departemen IAM perusahaan Anda atau dengan arsitek cloud AMS (CA) Anda.

Mode Perubahan Langsung peran dan kebijakan IAM

Saat mode Perubahan Langsung diaktifkan di akun, entitas IAM baru ini diterapkan:

`AWSManagedServicesCloudFormationAdminRole`: Peran ini memberikan akses ke CloudFormation konsol, membuat dan memperbarui CloudFormation tumpukan, melihat laporan drift, dan membuat dan mengeksekusi. CloudFormation ChangeSets Akses ke peran ini dikelola melalui penyedia SAMP Anda.

Kebijakan terkelola yang diterapkan dan dilampirkan pada peran `AWSManagedServicesCloudFormationAdminRole` adalah:

- Akun aplikasi AMS Advanced multi-account landing zone (MALZ)
  - AWSManagedServices_CloudFormationAdminPolicy1

  - AWSManagedServices_CloudFormationAdminPolicy2
    - Kebijakan ini mewakili izin yang diberikan kepada. `AWSManagedServicesCloudFormationAdminRole` Anda dan mitra menggunakan kebijakan ini untuk memberikan akses ke peran yang ada di akun dan mengizinkan peran tersebut untuk meluncurkan dan memperbarui CloudFormation tumpukan di akun. Ini mungkin memerlukan pembaruan kebijakan kontrol layanan AMS (SCP) tambahan untuk mengizinkan entitas IAM lainnya meluncurkan CloudFormation tumpukan.
- Akun landing zone (SALZ) akun AMS Advanced single-account
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
  - cdk-legacy-mode-s3-akses [kebijakan in-line]
  - AWS ReadOnlyAccess kebijakan

`AWSManagedServicesUpdateRole`: Peran ini memberikan akses terbatas ke layanan hilir AWS . APIs Peran ini diterapkan dengan kebijakan terkelola yang menyediakan operasi API yang bermutasi dan tidak bermutasi, tetapi secara umum membatasi operasi mutasi (sepertiCreate/Delete/PUT), terhadap layanan tertentu seperti IAM, KMS,, VPC, sumber daya dan konfigurasi infrastruktur AMSGuardDuty, dan sebagainya. Akses ke peran ini dikelola melalui penyedia SAMP Anda.

Kebijakan terkelola yang diterapkan dan dilampirkan pada peran `AWSManagedServicesUpdateRole` adalah:

- Akun aplikasi landing zone multi-akun AMS tingkat lanjut
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyPolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2dan RDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraKebijakan
- Akun landing zone akun tunggal AMS Advanced
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2dan RDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraKebijakan1

- AWSManagedServicesUpdateDenyActionsOnAMSInfraKebijakan2

Selain itu, `AWSManagedServicesUpdateRole` peran kebijakan terkelola juga memiliki kebijakan AWS terkelola yang `ViewOnlyAccess` melekat padanya.

Keamanan dan kepatuhan

Keamanan dan kepatuhan adalah tanggung jawab bersama antara AMS Advanced dan Anda, sebagai pelanggan kami. Mode AMS Advanced Direct Change tidak mengubah tanggung jawab bersama ini.

Keamanan dalam mode Perubahan Langsung

AMS Advanced menawarkan nilai tambahan dengan landing zone preskriptif, sistem manajemen perubahan, dan manajemen akses. Saat menggunakan mode Perubahan Langsung, model tanggung jawab ini tidak berubah. Namun, Anda harus mewaspadai risiko tambahan.

Peran “Perbarui” Mode Perubahan Langsung (lihatMode Perubahan Langsung peran dan kebijakan IAM) memberikan izin tinggi yang memungkinkan entitas mengaksesnya, untuk membuat perubahan pada sumber daya infrastruktur layanan yang didukung AMS dalam akun Anda. Dengan izin yang tinggi, beragam risiko ada tergantung pada sumber daya, layanan, dan tindakan, terutama dalam situasi di mana perubahan yang salah dibuat karena pengawasan, kesalahan, atau kurangnya kepatuhan terhadap proses internal dan kerangka kontrol Anda.

Sesuai Standar Teknis AMS, risiko berikut telah diidentifikasi dan rekomendasi dibuat sebagai berikut. Informasi terperinci tentang Standar Teknis AMS tersedia melalui AWS Artifact. Untuk mengakses AWS Artifact, hubungi CSDM Anda untuk instruksi atau pergi ke Memulai dengan. AWS Artifact

AMS-STD-001: Penandaan

Standar	Apakah itu rusak	Risiko	Rekomendasi
Semua sumber daya yang dimiliki AMS harus memiliki pasangan nilai kunci berikut	Ya. Istirahat untuk CloudFormationCloudTrail,, EFS OpenSearch,, CloudWatch Logs,	Penandaan sumber daya AMS yang salah dapat berdampak buruk pada operasi pelaporan, peringata	Akses harus dibatasi untuk membuat perubahan apa pun pada persyaratan penandaan default

Standar	Apakah itu rusak	Risiko	Rekomendasi
Semua tag milik AMS selain yang tercantum di atas harus memiliki awalan seperti `AMS*` atau dalam kasus. `MC*` upper/lower/mix	SQS, SSM, Tagging api - karena layanan ini tidak mendukung `aws:TagsKey` kondisi untuk membatasi penandaan untuk namespace AMS. Standar yang diberikan dalam tabel AMS-STD-003, berikut, menyatakan bahwa Anda dapat mengubah, Lingkungan dan AppId AppName, tetapi tidak untuk sumber daya milik AMS. Tidak dapat dicapai melalui izin IAM.	n, dan penambalan sumber daya Anda, di sisi AMS.	AMS untuk siapa pun selain tim AMS.
Tag apa pun pada tumpukan milik AMS tidak boleh dihapus berdasarkan permintaan perubahan Anda.	Ya. CloudFormation tidak mendukung `aws:TagsKey` kondisi untuk membatasi tag untuk namespace AMS.		

Standar	Apakah itu rusak	Risiko	Rekomendasi
Anda tidak diizinkan untuk menggunakan konvensi penamaan tag AMS di infrastru ktur Anda seperti yang disebutkan dalam tabel AMS-STD-002, selanjutnya.	Ya. Istirahat untuk CloudFormation CloudTrail, Amazon Elastic File System (EFS), OpenSearc h, CloudWatch Log, Amazon Simple Queue Service (SQS), Amazon EC2 Systems Manager (SSM), API Tagging; layanan ini tidak `aws:TagsKey` mendukung kondisi untuk membatasi penandaan pada namespace AMS.		

AMS-STD-002: Identity and Access Management (IAM)

Standar	Apakah itu rusak	Risiko	Rekomendasi
4.7 Tindakan, yang melewati proses manajemen perubahan (RFC), tidak boleh diizinkan seperti memulai atau menghentikan instance, pembuatan bucket S3 atau instans RDS, dan sebagainya. Akun mode pengembang	Ya. Tujuan tindakan layanan mandiri memungkinkan Anda melakukan tindakan melewati sistem AMS RFC.	Model akses aman adalah aspek teknis inti AMS dan pengguna IAM untuk konsol atau akses terprogra m menghindari kontrol akses ini. Akses pengguna IAM tidak dipantau oleh manajemen perubahan AMS.	Pengguna IAM harus dibatasi waktu dan diberikan izin berdasarkan hak istimewa paling sedikit dan. need-to-know

Standar	Apakah itu rusak	Risiko	Rekomendasi
dan layanan mode Penyediaan Layanan Mandiri (SSPS) dikecualikan selama tindakan dilakukan dalam batas-batas peran yang ditugaska n.		Akses CloudTrail hanya login.	

AMS-STD-003: Keamanan Jaringan

Standar	Apakah itu rusak	Risiko	Rekomendasi
S2. IP elastis pada EC2 instans harus digunakan hanya dengan perjanjian penerimaan risiko formal, atau dengan kasus penggunaan yang valid oleh tim internal.	Ya. Tindakan layanan mandiri memungkin kan Anda untuk mengaitkan dan memisahkan alamat IP elastis (EIP).	Menambahkan IP elastis ke sebuah instance memaparka nnya ke Internet. Hal ini meningkatkan risiko pengungkapan informasi dan aktivitas yang tidak sah.	Blokir lalu lintas yang tidak perlu ke instans itu melalui grup keamanan, dan verifikasi bahwa grup keamanan Anda dilampirkan dengan instans untuk memastikan bahwa itu memungkinkan lalu lintas hanya sesuai kebutuhan untuk alasan bisnis.
S14. VPC Peering dan koneksi endpoint antar akun milik pelanggan yang sama dapat diizinkan.	Ya. Tidak mungkin melalui kebijakan IAM.	Lalu lintas yang meninggalkan akun AMS Anda tidak dipantau setelah keluar dari batas akun.	Kami merekomen dasikan mengintip hanya dengan akun AMS yang Anda miliki. Jika kasus penggunaan Anda mengharuskan ini, gunakan grup

Standar	Apakah itu rusak	Risiko	Rekomendasi
			keamanan dan tabel rute untuk membatasi rentang lalu lintas, sumber daya, dan jenis apa yang dapat keluar melalui koneksi yang relevan.
Basis AMS AMIs dapat dibagi antara akun yang dikelola AMS dan tidak dikelola selama kami dapat memverifikasi bahwa akun tersebut dimiliki oleh organisasi yang sama. AWS		AMIs mungkin berisi data sensitif dan mungkin terpapar ke akun yang tidak diinginkan.	Bagikan hanya AMIs dengan akun yang dimiliki oleh organisasi Anda atau validasi kasus penggunaan dan informasi akun sebelum berbagi di luar organisasi.

AMS-STD-007: Penebangan

Standar	Apakah itu rusak	Risiko	Rekomendasi
19. Setiap log dapat diteruskan dari satu akun AMS ke akun AMS lain dari pelanggan yang sama.	Ya. Potensi ketidakamanan untuk log pelanggan karena verifikasi akun pelanggan berada di organisasi yang sama tidak dapat dicapai melalui kebijakan IAM.	Log mungkin berisi data sensitif dan mungkin terpapar ke akun yang tidak diinginkan.	Bagikan log hanya dengan akun yang dikelola oleh AWS Org Anda, atau validasi kasus penggunaan dan informasi akun sebelum berbagi di luar organisasi Anda. Kami dapat memverifikasi ini melalui berbagai
20. Setiap log dapat diteruskan dari AMS ke akun non-AMS hanya jika akun non-AMS dimiliki oleh pelanggan			

Standar	Apakah itu rusak	Risiko	Rekomendasi
AMS yang sama (dengan mengonfir masi bahwa mereka berada di bawah AWS Organizations akun yang sama atau dengan mencocokkan domain email dengan nama perusahaa n pelanggan dan akun terkait PAYER) menggunakan alat internal.			cara, periksa dengan manajer pengirima n layanan cloud (CSDM) Anda.

Bekerja dengan tim otorisasi dan otentikasi internal Anda untuk mengontrol izin ke peran mode Perubahan Langsung yang sesuai.

Kepatuhan dalam mode Perubahan Langsung

Mode Perubahan Langsung kompatibel dengan beban kerja produksi dan non-produksi. Anda bertanggung jawab untuk memastikan kepatuhan terhadap standar kepatuhan apa pun (misalnya, PHI, HIPAA, PCI), dan untuk memastikan bahwa penggunaan mode Perubahan Langsung sesuai dengan kerangka kerja dan standar kontrol internal Anda.

Ubah manajemen dalam mode Perubahan Langsung

Manajemen perubahan adalah proses yang digunakan AMS Advanced untuk mengimplementasikan permintaan perubahan. Permintaan untuk perubahan (RFC) adalah permintaan yang dibuat oleh Anda, atau AMS Advanced melalui antarmuka AMS Advanced untuk membuat perubahan pada lingkungan terkelola Anda dan menyertakan ID AMS Advanced change type (CT) untuk operasi tertentu. Untuk informasi selengkapnya, lihat Mengubah manajemen.

> **Note**
>
> Mode Perubahan Langsung tidak menghapus manajemen perubahan AMS RFCs, Anda masih memiliki akses penuh ke AMS RFCs dengan DCM.

Mode Perubahan Langsung AMS (DCM) memperluas manajemen perubahan AMS Advanced dengan menyediakan AWS akses asli ke akun AMS Advanced Plus dan Premium untuk menyediakan dan memperbarui AWS sumber daya. Pengguna yang telah diberikan izin mode Perubahan Langsung melalui peran IAM, dapat menggunakan akses AWS API asli ke penyediaan dan membuat perubahan pada sumber daya di akun AMS Advanced mereka. Pengguna masih dapat menggunakan manajemen perubahan AMS Advanced RFCs menggunakan peran IAM yang sama. Dalam kedua kasus, sumber daya dan perubahannya sepenuhnya didukung oleh AMS, termasuk pemantauan, tambalan, cadangan, manajemen respons insiden. Pengguna yang tidak memiliki peran yang sesuai dalam akun ini harus menggunakan proses RFC manajemen perubahan AMS Advanced untuk melakukan perubahan.

Ubah kasus penggunaan manajemen

Untuk alasan keamanan, beberapa perubahan pada AMS Advanced hanya dapat dilakukan melalui proses Change Management Request for Change (RFC). `AWSManagedServicesCloudFormationAdminRole`Ini terbatas pada tindakan yang diambil melalui CloudFormation (CFN). Untuk selengkapnya tentang cara membuat tumpukan melalui DCM, lihat Membuat tumpukan menggunakan mode Perubahan Langsung. `AWSManagedServicesUpdateRole`Ini dibatasi untuk tindakan berikut.

Misalnya penelusuran untuk setiap jenis perubahan, termasuk jenis perubahan Manajemen | Akun terkelola | Mode Perubahan Langsung | Aktifkan (ct-3rd4781c2nnhp), lihat bagian “Informasi Tambahan” untuk jenis perubahan yang relevan di bagian AMS Advanced Change Type Reference Change Type by Classification.

Layanan	Tindakan
AWS Key Management Service (AWS KMS)	Perbarui
AWS Certificate Manager	Buat
AWS Identity and Access Management (IAM)	Setiap

Layanan	Tindakan
Site-to-Site VPN	Setiap
Penjadwal Sumber Daya AMS	
AWS Backup	Buat rencana cadangan
Konsumsi Beban Kerja AMS () WIGs	Setiap
Penyaringan Jalan Masuk AMS (Palo Alto Terkelola)	
Perubahan akun AMS Advanced MALZ	
Amazon GuardDuty	
Akses Stack Tingkat Lanjut AMS	Setiap
Volume Amazon Elastic Block Store (EBS)	Hapus
Enkripsi default Amazon Elastic Block Store (EBS)	Aktifkan enkripsi default
Amazon Elastic Compute Cloud (Amazon EC2)	Ubah nama host
Amazon Machine Image (AMI)	Hapus, bagikan
Grup EC2 Keamanan Amazon	Setiap
AMS SSPS Tingkat Lanjut	
AWS Microsoft AD yang dikelola	
Mode pengembang AMS Lanjutan	
Amazon Simple Storage Service (Amazon S3)	Buat kebijakan bucket S3
AWS Systems Manager	Buat

Membuat tumpukan menggunakan mode Perubahan Langsung

Ada dua persyaratan saat meluncurkan tumpukan dalam CloudFormation menggunakan`AWSManagedServicesCloudFormationAdminRole`, agar tumpukan dikelola oleh AMS:

- Template harus berisi file`AmsStackTransform`.
- Nama tumpukan harus dimulai dengan awalan `stack-` diikuti oleh string alfanumerik 17 karakter.

> **Note**
>
> Agar berhasil menggunakan`AmsStackTransform`, Anda harus mengakui bahwa template tumpukan Anda berisi `CAPABILITY_AUTO_EXPAND` kemampuan agar CloudFormation (CFN) membuat atau memperbarui tumpukan. Anda melakukan ini dengan meneruskan `CAPABILITY_AUTO_EXPAND` sebagai bagian dari permintaan create-stack Anda. CFN menolak permintaan jika kemampuan ini tidak diakui ketika disertakan dalam template. `AmsStackTransform` Konsol CFN memastikan bahwa Anda melewati kemampuan ini jika Anda memiliki transformasi di template Anda, tetapi ini dapat dilewatkan ketika Anda berinteraksi dengan CFN melalui mereka. APIs
> Anda harus meneruskan kemampuan ini setiap kali Anda menggunakan panggilan API CFN berikut:
>
> - CreateChangeSet
> - CreateStack
> - UpdateStack

Saat membuat atau memperbarui tumpukan dengan DCM, validasi dan augmentasi CFN Ingest dan Pembaruan CTs Tumpukan yang sama dilakukan di tumpukan, untuk informasi selengkapnya lihat Pedoman CloudFormation Ingest, Praktik Terbaik, dan Batasan. Pengecualian untuk ini adalah bahwa grup keamanan default AMS (SGs) tidak akan dilampirkan ke instance atau EC2 EC2 instance yang berdiri sendiri di grup Auto Scaling (). ASGs Saat Anda membuat CloudFormation template, dengan EC2 instance yang berdiri sendiri atau ASGs, Anda dapat melampirkan default. SGs

> **Note**
>
> Peran IAM sekarang dapat dibuat dan dikelola dengan. `AWSManagedServicesCloudFormationAdminRole`

Default AMS SGs memiliki aturan masuk dan keluar yang memungkinkan instans berhasil diluncurkan dan diakses nanti melalui SSH atau RDP oleh operasi AMS dan Anda. Jika Anda menemukan bahwa grup keamanan default AMS terlalu permisif, Anda dapat membuat sendiri SGs dengan aturan yang lebih ketat dan melampirkannya ke instans Anda, asalkan masih memungkinkan Anda dan operasi AMS untuk mengakses instans selama insiden.

Grup keamanan default AMS adalah sebagai berikut:

- SentinelDefaultSecurityGroupPrivateOnly: Dapat diakses di template CFN melalui parameter SSM ini `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- SentinelDefaultSecurityGroupPrivateOnlyEgressAll: Dapat diakses di template CFN melalui parameter SSM ini `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

Transformasi AMS

Tambahkan `Transform` pernyataan ke CloudFormation template Anda. Ini menambahkan CloudFormation makro yang memvalidasi dan mendaftarkan tumpukan dengan AMS pada waktu peluncuran.

Contoh JSON

```
"Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
  }
```

Contoh YAMM

```
Transform:
  Name: AmsStackTransform
```

```
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

Tambahkan juga `Transform` pernyataan saat memperbarui template tumpukan yang ada.

Contoh JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
    "Transform": {
      "Name": "AmsStackTransform",
      "Parameters": {
        "StackId": {"Ref" : "AWS::StackId"}
     }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

Contoh YAMM

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
```

```
    Default: HelloWorldTopic
Resources:
  SnsTopic:
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Ref TopicName
```

Nama tumpukan

Nama tumpukan harus dimulai dengan awalan `stack-` diikuti oleh string alfanumerik 17 karakter. Ini untuk menjaga kompatibilitas dengan sistem AMS lain yang beroperasi pada tumpukan AMS IDs.

Berikut ini adalah contoh cara untuk menghasilkan tumpukan yang kompatibel IDs:

Bash:

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python:

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

PowerShell:

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17  | %
 {[char]$_}) )
```

Kasus penggunaan Mode Perubahan Langsung

Berikut ini adalah kasus penggunaan untuk Mode Perubahan Langsung:

Penyediaan dan manajemen sumber daya melalui CloudFormation

- Integrasikan perkakas dan proses CloudFormation berbasis yang ada.

Manajemen dan pembaruan sumber daya yang sedang berlangsung

- Perubahan atom kecil dengan risiko rendah.

- Perubahan yang seharusnya berjalan melalui RFC manual atau otomatis.
- Perkakas yang membutuhkan akses AWS API asli.
- Peran DCM dapat digunakan jika Anda berada dalam tahap migrasi. Tim migrasi memanfaatkan izin di DCM untuk membuat atau memodifikasi tumpukan.
- Peran DCM dapat digunakan dalam CI/CD pipeline untuk membangun baru AMIs, membuat tugas Amazon ECS, dan sebagainya.

Mode Pengembang AMS Lanjutan

Topik

- Memulai mode AMS Advanced Developer
- Keamanan dan kepatuhan dalam mode Pengembang
- Ubah manajemen dalam mode Pengembang
- Penyediaan infrastruktur dalam mode Pengembang AMS
- Kontrol Detektif dalam mode Pengembang AMS
- Pencatatan, pemantauan, dan manajemen acara dalam mode Pengembang AMS
- Manajemen insiden dalam mode Pengembang AMS
- Manajemen tambalan dalam mode Pengembang AMS
- Manajemen kontinuitas dalam mode Pengembang AMS
- Keamanan dan manajemen akses dalam mode Pengembang AMS

Mode pengembang AWS Managed Services (AMS) menggunakan izin yang ditingkatkan di akun AMS Advanced Plus dan Premium untuk menyediakan dan memperbarui sumber daya AWS di luar proses manajemen perubahan AMS Advanced. Mode AMS Advanced Developer melakukan ini dengan memanfaatkan panggilan AWS API native dalam AMS Advanced Virtual Private Cloud (VPC), memungkinkan Anda merancang dan mengimplementasikan infrastruktur dan aplikasi di lingkungan terkelola Anda.

Saat menggunakan akun yang mengaktifkan mode Pengembang, manajemen kontinuitas, manajemen tambalan, dan manajemen perubahan disediakan untuk sumber daya yang disediakan melalui proses manajemen perubahan AMS Advanced atau dengan menggunakan AMS Amazon Machine Image (AMI). Namun, fitur manajemen AMS ini tidak ditawarkan untuk sumber daya yang disediakan melalui native. AWS APIs

Anda bertanggung jawab untuk memantau sumber daya infrastruktur yang disediakan di luar proses manajemen perubahan AMS Advanced. Mode pengembang kompatibel dengan beban kerja produksi dan non-produksi. Dengan izin yang tinggi, Anda memiliki tanggung jawab yang meningkat untuk memastikan kepatuhan terhadap kontrol internal.

> **Important**
>
> Sumber daya yang Anda buat menggunakan mode Pengembang dapat dikelola oleh AMS Advanced hanya jika dibuat menggunakan proses manajemen perubahan AMS Advanced.

Mode pengembang adalah salah satu mode AMS Advanced yang dapat Anda gunakan. Lihat informasi yang lebih lengkap di Ikhtisar mode.

Memulai mode AMS Advanced Developer

Pelajari berbagai akun AMS Advanced dengan mode AMS Advanced Developer dan cara mengimplementasikan mode Developer dengan sukses.

Topik

- Sebelum Anda memulai dengan mode AMS Developer
- Prasyarat untuk mode Pengembang AMS
- Cara menerapkan mode AMS Advanced Developer
- Izin mode Pengembang AMS Lanjutan

Sebelum Anda memulai dengan mode AMS Developer

Sebelum menerapkan mode Developer, ada beberapa hal yang harus Anda ketahui.

AMS Advanced tidak dapat mengelola tumpukan atau sumber daya yang ada di DevMode akun yang dibuat di luar proses manajemen perubahan AMS Advanced melalui request for change (RFCs). Namun, saat akun masuk DevMode, AMS Advanced terus mengelola sumber daya yang disediakan melalui proses manajemen perubahan AMS Advanced dengan. RFCs

Anda tidak dapat memulai dengan DevMode akun dan kemudian menutupnya ke akun aplikasi AMS Advanced-managed.

Prasyarat untuk mode Pengembang AMS

Berikut ini adalah prasyarat untuk menerapkan mode Pengembang:

- Anda harus menjadi pelanggan AMS Advanced dengan setidaknya satu akun AMS Advanced Plus atau Premium onboard.
- Akun apa pun yang Anda gunakan harus berupa akun AMS Advanced Plus atau Premium.
- Zona Pendaratan Multi-Akun (MALZ): Anda harus menggunakan peran yang `AWSManagedServicesDevelopmentRole` telah ditentukan AWS Identity and Access Management (IAM). Anda meminta peran ini. Bagian selanjutnya menjelaskan cara memperoleh izin mode Pengembang.
- Single-Account Landing Zone (SALZ): Anda harus menggunakan peran yang `customer_developer_role` telah ditentukan AWS Identity and Access Management (IAM). Anda meminta peran ini. Bagian selanjutnya menjelaskan cara memperoleh izin mode Pengembang.

Cara menerapkan mode AMS Advanced Developer

Anda menerapkan mode Developer dengan meminta agar akun AMS Advanced Anda yang memenuhi syarat disediakan dengan peran IAM yang telah ditentukan sebelumnya:

- MALZ: `AWSManagedServicesDevelopmentRole`
- SALZ: `customer_developer_role`

Anda kemudian menetapkan peran tersebut ke pengguna yang relevan di jaringan federasi Anda.

AMS Advanced merekomendasikan agar Anda memastikan bahwa penggunaan mode Developer sesuai dengan kerangka kerja dan standar kontrol internal Anda karena mode Pengembang menciptakan dua vektor perubahan: Manajemen perubahan AMS Advanced untuk sumber daya yang dikelola AMS Advanced dan federasi peran yang dikelola pelanggan untuk sumber daya yang Anda, sebagai pelanggan kami, kelola. Meskipun proses AMS Advanced tetap sesuai dengan deklarasi kami, proses pelanggan dan kerangka kerja kontrol mungkin perlu diperbarui.

Untuk mengimplementasikan mode Developer di akun AMS Advanced

1. Konfirmasikan akun yang ingin Anda gunakan dengan mode Pengembang memenuhi persyaratan yang tercantum diPrasyarat untuk mode Pengembang AMS.

2. Kirim permintaan perubahan (RFC) menggunakan tipe perubahan (CT) Manajemen | Akun terkelola | Mode pengembang | Aktifkan (diperlukan tinjauan). Untuk contoh cara menggunakan CT ini, lihat Mode Pengembang | Aktifkan (Review Required).

   Setelah CT diproses, peran IAM yang telah ditentukan, (`AWSManagedServicesDevelopmentRole`untuk MALZ, **`customer_developer_role`** untuk SALZ), disediakan di akun yang diminta.
3. Tetapkan peran yang sesuai kepada pengguna yang memerlukan akses mode Pengembang menggunakan proses federasi internal Anda.

   AMS Advanced menyarankan Anda membatasi akses untuk mencegah penyediaan, atau perubahan pada, sumber daya yang tidak diinginkan atau tidak disetujui.

Izin mode Pengembang AMS Lanjutan

Peran yang telah ditentukan sebelumnya (`AWSManagedServicesDevelopmentRole`untuk MALZ, `customer_developer_role` untuk SALZ), memberikan izin untuk membuat sumber daya infrastruktur aplikasi dalam VPC AMS Advanced, termasuk peran IAM, sekaligus membatasi akses ke komponen layanan bersama yang dioperasikan oleh AMS Advanced (misalnya, host manajemen, pengontrol domain, Trend Micro EPS, benteng, dan layanan AWS yang tidak didukung). Peran ini juga membatasi akses ke log Layanan AWS Lanjutan Amazon GuardDuty, AWS Organizations, AWS Directory Service APIs, dan AMS.

Meskipun peran memungkinkan Anda membuat peran IAM tambahan, batas izin yang sama yang disertakan dalam akses mode Pengembang diberlakukan pada peran IAM apa pun yang dibuat oleh. `AWSManagedServicesDevelopmentRole`

Keamanan dan kepatuhan dalam mode Pengembang

Keamanan dan kepatuhan adalah tanggung jawab bersama antara AMS Advanced dan Anda sebagai pelanggan kami. Mode AMS Advanced Developer mengalihkan tanggung jawab bersama kepada Anda atas sumber daya yang disediakan di luar proses manajemen perubahan atau disediakan melalui manajemen perubahan tetapi diperbarui dengan izin mode Pengembang. Untuk informasi selengkapnya tentang tanggung jawab bersama, lihat AWS Managed Services.

Peringatan:

- DevMode memungkinkan Anda dan tim resmi Anda untuk melewati deny-by-default prinsip-prinsip inti keamanan AMS. Keuntungan, swalayan, lebih sedikit waktu menunggu AMS harus ditimbang

terhadap kerugiannya, siapa pun dapat melakukan tindakan tak terduga dan destruktif tanpa sepengetahuan tim keamanan mereka. Jenis perubahan otomatis untuk mengaktifkan mode Dev dan mode Perubahan Langsung diekspos, dan setiap orang yang berwenang di organisasi Anda dapat menjalankannya CTs dan mengaktifkan mode ini.

- Anda bertanggung jawab untuk mengelola izin eksekusi CT dari basis pengguna Anda.
- AMS tidak mengelola izin eksekusi CT

Rekomendasi:

- Lindungi
  - Pelanggan dapat mencegah akses ke CT ini melalui izin, lihat Membatasi izin dengan pernyataan kebijakan peran IAM
  - Mencegah akses ke CT ini dengan menerapkan proxy seperti sistem ITSM
  - Memanfaatkan kebijakan kontrol layanan (SCPs) yang mencegah kebijakan dan perilaku sesuai kebutuhan, lihat Perpustakaan Kontrol Pencegahan dan Detektif AMS
- Mendeteksi
  - Pantau RFC Anda untuk ini CTs (Aktifkan mode pengembang ct-1opjmhuddw194 dan mode perubahan langsung, Aktifkan ct-3rd4781c2nnhp) dieksekusi dan merespons sesuai
  - Tinjau and/or audit akun Anda untuk keberadaan sumber daya IAM untuk mengidentifikasi akun tersebut di mana mode Pengembang atau mode Perubahan Langsung telah diterapkan
- Menanggapi
  - Hapus akun dalam mode Pengembang sesuai kebutuhan

Keamanan dalam mode Pengembang

AMS Advanced menawarkan nilai tambahan dengan landing zone preskriptif, sistem manajemen perubahan, dan manajemen akses. Saat menggunakan mode Pengembang, nilai keamanan AMS Advanced dipertahankan dengan menggunakan konfigurasi akun yang sama dari akun AMS Advanced standar yang menetapkan jaringan pengerasan keamanan AMS Advanced dasar. Jaringan dilindungi oleh batas izin yang diberlakukan dalam peran (`AWSManagedServicesDevelopmentRole`untuk MALZ, **`customer_developer_role`** untuk SALZ), yang membatasi pengguna untuk memecah perlindungan parameter yang ditetapkan saat akun disiapkan.

Misalnya, pengguna dengan peran dapat mengakses Amazon Route 53 tetapi zona host internal AMS Advanced dibatasi. Batas izin yang sama diberlakukan pada peran IAM yang dibuat oleh`AWSManagedServicesDevelopmentRole`, menegakkan batasan izin pada yang membatasi pengguna untuk memecah perlindungan parameter `AWSManagedServicesDevelopmentRole` yang ditetapkan saat akun di-onboard ke AMS Advanced.

Kepatuhan dalam mode Pengembang

Mode pengembang kompatibel dengan beban kerja produksi dan non-produksi. Anda bertanggung jawab untuk memastikan kepatuhan terhadap standar kepatuhan apa pun (misalnya, PHI, HIPAA, PCI), dan untuk memastikan bahwa penggunaan mode Pengembang sesuai dengan kerangka kerja dan standar pengendalian internal Anda.

Ubah manajemen dalam mode Pengembang

Manajemen perubahan adalah proses yang digunakan layanan AMS Advanced untuk mengimplementasikan permintaan perubahan. Permintaan untuk perubahan (RFC) adalah permintaan yang dibuat oleh Anda atau AMS Advanced melalui antarmuka AMS Advanced untuk membuat perubahan pada lingkungan terkelola Anda dan menyertakan ID tipe perubahan (CT) untuk operasi tertentu. Untuk informasi selengkapnya, lihat Ubah mode manajemen.

Manajemen perubahan tidak diberlakukan di akun AMS Advanced di mana izin mode Pengembang diberikan. Pengguna yang telah diberikan izin mode Pengembang dengan peran IAM (`AWSManagedServicesDevelopmentRole`untuk MALZ, **`customer_developer_role`** untuk SALZ), dapat menggunakan akses AWS API asli ke penyediaan dan membuat perubahan pada sumber daya di akun AMS Advanced mereka. Pengguna yang tidak memiliki peran yang sesuai dalam akun ini harus menggunakan proses manajemen perubahan AMS Advanced untuk melakukan perubahan.

> **Important**
>
> Sumber daya yang Anda buat menggunakan mode Pengembang dapat dikelola oleh AMS Advanced hanya jika dibuat menggunakan proses manajemen perubahan AMS Advanced. Permintaan untuk perubahan yang dikirimkan ke AMS Advanced untuk sumber daya yang dibuat di luar proses manajemen perubahan AMS Advanced ditolak oleh AMS Advanced karena harus ditangani oleh Anda.

Pembatasan API layanan penyediaan layanan mandiri

Semua layanan mandiri AMS Advanced didukung dengan mode Pengembang. Akses ke layanan yang disediakan sendiri tunduk pada batasan yang diuraikan di masing-masing bagian panduan pengguna untuk masing-masing. Jika layanan yang disediakan sendiri tidak tersedia dengan peran mode Pengembang, Anda dapat meminta peran yang diperbarui melalui jenis perubahan mode Pengembang.

Layanan berikut tidak menyediakan akses penuh ke layanan APIs:

Layanan Penyediaan Mandiri Dibatasi dalam mode Pengembang

Layanan	Catatan
Amazon API Gateway	Semua APIs panggilan Gateway diperbolehkan kecualiSetWebACL .
Penskalaan Otomatis Aplikasi	Hanya dapat mendaftarkan atau membatalk an pendaftaran target yang dapat diskalakan, dan menempatkan atau menghapus kebijakan penskalaan.
AWS CloudFormation	Tidak dapat mengakses atau memodifikasi CloudFormation tumpukan yang memiliki nama yang diawali dengan. mc-
AWS CloudTrail	Tidak dapat mengakses atau memodifikasi CloudTrail sumber daya yang memiliki nama yang diawali dengan ams- and/or mc-.
Amazon Cognito (Kolam Pengguna)	Tidak dapat mengaitkan token perangkat lunak. Tidak dapat membuat kumpulan pengguna, pekerjaan impor pengguna, server sumber daya, atau penyedia identitas.
AWS Directory Service	Hanya Directory Service tindakan berikut yang diperlukan oleh Connect dan WorkSpaces layanan. Semua tindakan Directory Service

Layanan	Catatan
	lainnya ditolak oleh kebijakan batas izin mode Pengembang: • `ds:AuthorizeApplication` • `ds:CreateAlias` • `ds:CreateIdentityPoolDirectory` • `ds:DeleteDirectory` • `ds:DescribeDirectories` • `ds:GetAuthorizedApplication Details` • `ds:ListAuthorizedApplications` • `ds:UnauthorizeApplication` Dalam akun landing zone akun tunggal, kebijakan batas secara eksplisit menolak akses ke direktori terkelola AMS Advanced yang digunakan oleh AMS Advanced untuk mempertahankan akses ke akun yang diaktifkan mode pengembang.
Amazon Elastic Compute Cloud	Tidak dapat mengakses Amazon EC2 APIs yang berisi string:`DhcpOptions` ,`Gateway`,`Subnet`,`VPC`, dan`VPN`. Tidak dapat mengakses atau memodifikasi EC2 sumber daya Amazon yang memiliki tag yang diawali dengan`AMS`,, `mcManagementHostASG` , and/or `sentinel`.

Layanan	Catatan
Amazon EC2 (Laporan)	Hanya akses tampilan yang diberikan (tidak dapat memodifikasi). Catatan: Amazon EC2 Reports sedang bergerak. Item menu Laporan akan dihapus dari menu navigasi EC2 konsol Amazon. Untuk melihat laporan EC2 penggunaan Amazon setelah dihapus, gunakan konsol AWS Billing dan Manajemen Biaya.
AWS Identity and Access Management (IAM)	Tidak dapat menghapus batas izin yang ada, atau mengubah kebijakan kata sandi pengguna IAM. Tidak dapat membuat atau memodifikasi sumber daya IAM kecuali Anda menggunakan peran IAM yang benar (`AWSManagedServicesDevelopmentRole` untuk MALZ, **`customer_developer_role`** untuk SALZ)). Tidak dapat mengubah sumber daya IAM yang diawali dengan:`ams`,,`mc`,`customer_deny_policy` . and/or `sentinel` Saat membuat sumber daya IAM baru (peran, pengguna, atau grup), batas izin (MALZ:**`AWSManagedServicesDevelopmentRolePermissionsBoundary`** , SALZ:`ams-app-infra-permissions-boundary`) harus dilampirkan.
AWS Key Management Service (AWS KMS)	Tidak dapat mengakses atau memodifikasi kunci KMS yang dikelola lanjutan AMS.
AWS Lambda	Tidak dapat mengakses atau memodifikasi AWS Lambda fungsi yang diawali denganAMS.

Layanan	Catatan
CloudWatch Log	Tidak dapat mengakses aliran CloudWatch log yang nama diawali dengan:`mc`,`aws`,`lambda`. and/or `AMS`
Amazon Relational Database Service (Amazon RDS)	Tidak dapat mengakses atau memodifikasi database Amazon Relational Database Service (Amazon RDS) DBs () yang memiliki nama yang diawali dengan:. `mc-`
AWS Resource Groups	Hanya dapat mengakses`Get`,`List`, dan tindakan API Grup `Search` Sumber Daya.
Amazon Route 53	Tidak dapat mengakses atau memodifikasi sumber daya Route53 AMS yang dikelola lanjutan.
Amazon S3	Tidak dapat mengakses bucket Amazon S3 yang memiliki nama yang diawali dengan:`ams-*`,,, `ams` atau. `ms-a` `mc-a`
AWS Security Token Service	Satu-satunya API layanan token keamanan yang diizinkan adalah`DecodeAuthorizationMessage` .
Amazon SNS	Tidak dapat mengakses topik SNS yang memiliki nama yang diawali dengan:`AMS-`,`Energon-Topic` , atau. `MMS-Topic`
AWS Systems Manager Manajer (SSM)	Tidak dapat mengubah parameter SSM yang diawali dengan`ams`,`mc`, atau. `svc` Tidak dapat menggunakan SSM API `SendCommand` terhadap EC2 instans Amazon yang memiliki tag yang diawali dengan atau. `ams` `mc`

Layanan	Catatan
AWS Menandai	Anda hanya memiliki akses ke tindakan API AWS Tagging yang diawali dengan. `Get`
AWS Lake Formation	Tindakan AWS Lake Formation API berikut ditolak: • `lakeformation:DescribeResource` • `lakeformation:GetDataLakeSettings` • `lakeformation:DeregisterResource` • `lakeformation:RegisterResource` • `lakeformation:UpdateResource` • `lakeformation:PutDataLakeSettings`
Amazon Elastic Inference	Anda hanya dapat memanggil aksi Elastic Inference API. `elastic-inference:Connect` Izin ini termasuk dalam `customer_sagemaker_admin_policy` yang dilampirkan pada`customer_sagemaker_admin_role` . Tindakan ini memberi Anda akses ke akselerator Elastic Inference.
AWS Shield	Tidak ada akses ke salah satu layanan APIs atau konsol ini.
Layanan Alur Kerja Sederhana Amazon	Tidak ada akses ke salah satu layanan APIs atau konsol ini.

Penyediaan infrastruktur dalam mode Pengembang AMS

Pengguna yang tidak memiliki peran IAM mode PengembangAWSManagedServicesDevelopmentRole, di akun tempat mode

Pengembang diaktifkan, diharuskan mengikuti proses manajemen perubahan AMS Advanced yang memanfaatkan AMS Advanced. AMIs Pengguna dengan peran yang benar (MALZ:`AWSManagedServicesDevelopmentRole`, SALZ:`customer_developer_role`) dapat menggunakan sistem manajemen perubahan AMS Advanced dan AMS Advanced AMIs tetapi tidak diharuskan melakukannya.

> **Note**
>
> AWS AMI, yang belum diproses melalui konsumsi beban kerja AMS Advanced, atau dibuat di akun AMS Advanced, tidak akan menyertakan konfigurasi AMS Advanced-required.

Kontrol Detektif dalam mode Pengembang AMS

Bagian ini telah disunting karena berisi informasi sensitif terkait keamanan AMS. Informasi ini tersedia melalui Dokumentasi konsol AMS. Untuk mengakses Artifact AWS, Anda dapat menghubungi CSDM Anda untuk mendapatkan petunjuk atau membuka Memulai dengan Artifact AWS.

Pencatatan, pemantauan, dan manajemen acara dalam mode Pengembang AMS

Pencatatan, pemantauan, dan manajemen peristiwa tidak tersedia untuk sumber daya yang disediakan di luar proses manajemen perubahan AMS Advanced, atau untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang.

Manajemen insiden dalam mode Pengembang AMS

Tidak ada perubahan waktu respons insiden. Resolusi insiden adalah upaya terbaik untuk sumber daya yang disediakan di luar proses manajemen perubahan, atau sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang.

> **Note**
>
> Perjanjian tingkat layanan AMS (SLA) tidak berlaku untuk sumber daya yang dibuat atau diperbarui di luar sistem manajemen perubahan AMS (permintaan untuk perubahan atau

RFCs), termasuk mode Pengembang; oleh karena itu, sumber daya yang diperbarui atau dibuat dalam mode Pengembang secara otomatis terdegradasi ke P3 dan dukungan AMS adalah upaya terbaik.

Manajemen tambalan dalam mode Pengembang AMS

Manajemen tambalan tidak tersedia untuk sumber daya yang disediakan di luar proses manajemen perubahan AMS Advanced, atau untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang. Waktu penambalan:

- Untuk pembaruan keamanan kritis: Dalam waktu 10 hari kerja setelah rilis oleh vendor untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang.
- Untuk pembaruan penting: Dalam waktu 2 bulan setelah rilis oleh vendor untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang.

Manajemen kontinuitas dalam mode Pengembang AMS

Manajemen kontinuitas tidak tersedia untuk sumber daya yang disediakan di luar proses manajemen perubahan AMS Advanced, atau untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang.

Waktu inisiasi pemulihan lingkungan dapat memakan waktu hingga 12 jam untuk sumber daya yang disediakan di luar proses manajemen perubahan AMS Advanced, atau untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang.

Keamanan dan manajemen akses dalam mode Pengembang AMS

Perlindungan anti-malware adalah tanggung jawab Anda atas sumber daya yang disediakan di luar proses manajemen perubahan AMS Advanced, atau untuk sumber daya yang disediakan melalui manajemen perubahan dan kemudian diubah oleh akun menggunakan izin mode Pengembang. Akses ke instans Amazon Elastic Compute Cloud (Amazon EC2) yang tidak disediakan melalui manajemen perubahan AMS Advanced mungkin dikontrol oleh pasangan kunci alih-alih menyediakan akses gabungan.

Mode Penyediaan Layanan Mandiri di AMS

Mode AWS Managed Services (AMS) Self-Service Provisioning (SSP) menyediakan akses penuh ke AWS layanan native dan kemampuan API di akun terkelola AMS. Anda mengakses layanan melalui peran standar, cakupan bawah,. AWS Identity and Access Management AMS menyediakan permintaan layanan dan manajemen insiden. Peringatan, pemantauan, pencatatan, tambalan, cadangan, dan manajemen perubahan adalah tanggung jawab Anda. Dalam banyak kasus, layanan Penyediaan Layanan Mandiri (SSPS) dikelola sendiri, atau tanpa server, dan tidak memerlukan manajemen tugas operasional tertentu seperti patching. Anda mendapat manfaat dari penggunaan layanan ini dalam batas lingkungan yang ditentukan oleh pagar pembatas AMS dan setiap perubahan IAM (termasuk peran terkait layanan, peran layanan, peran lintas akun, atau pembaruan kebijakan) perlu disetujui oleh Operasi AMS untuk menjaga keamanan dasar platform. Anda dapat memanfaatkan CloudFormation template untuk mengotomatiskan penerapan layanan ini, tetapi ini tidak didukung untuk semua layanan SSP.

> **Important**
>
> Gunakan mode SSP di akun AWS Managed Services (AMS) Anda untuk mengakses dan menggunakan AWS layanan, dengan batasan sebagaimana disebutkan.

Ada beberapa Layanan AWS yang dapat Anda gunakan tanpa manajemen AMS, di akun AMS Anda. Layanan mode Penyediaan Layanan Mandiri, atau singkatnya SSPS, cara menambahkannya ke akun AMS Anda dan FAQs untuk masing-masing, dijelaskan di bagian ini.

Layanan penyediaan layanan mandiri ditawarkan apa adanya, dan Anda bertanggung jawab untuk mengelolanya. AMS tidak memberikan peringatan, pemantauan, pencatatan, atau penambalan untuk sumber daya yang terkait dengan layanan tersebut. AMS menyediakan peran IAM yang memungkinkan Anda menggunakan layanan di akun AMS Anda dengan aman. AMS SLAs tidak berlaku.

Untuk sumber daya yang Anda sediakan melalui layanan mandiri, AMS menyediakan manajemen insiden, kontrol detektif dan pagar pembatas, pelaporan, sumber daya yang ditunjuk (Cloud Service Delivery Manager dan Cloud Architect), keamanan dan akses, serta dukungan teknis melalui permintaan layanan. Selain itu, jika berlaku, Anda bertanggung jawab atas manajemen kontinuitas, manajemen patch, pemantauan infrastruktur, dan manajemen perubahan untuk sumber daya yang disediakan atau dikonfigurasi di luar sistem manajemen perubahan AMS.

Memulai dengan mode SSP di AMS

Penyediaan layanan mandiri adalah salah satu mode AMS untuk multi-account landing zone (MALZ) yang dapat Anda gunakan. Untuk informasi selengkapnya, lihat Ikhtisar mode.

Untuk menyediakan kemampuan penyediaan layanan mandiri, AMS telah menciptakan peran IAM yang ditingkatkan dengan batas izin untuk membatasi perubahan yang tidak diinginkan dari akses langsung. Layanan AWS Peran tidak mencegah semua perubahan dan Anda harus mematuhi kontrol internal dan kebijakan kepatuhan Anda, dan memvalidasi bahwa semua yang Layanan AWS digunakan memenuhi sertifikasi yang diperlukan. Ini adalah mode penyediaan swalayan. Untuk detail tentang persyaratan AWS kepatuhan, lihat AWS Kepatuhan.

Untuk menambahkan layanan penyediaan layanan mandiri ke akun Aplikasi landing zone multi-akun Anda, gunakan Manajemen AWS | layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (CT), baik CT yang diperlukan peninjauan atau CT otomatis, seperti yang diinstruksikan untuk layanan.

> **Note**
>
> Untuk meminta agar AMS menyediakan layanan penyediaan layanan mandiri tambahan, ajukan permintaan layanan.

Gunakan AMS SSP untuk menyediakan Amazon API Gateway di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon API Gateway secara langsung di akun terkelola AMS Anda. Amazon API Gateway adalah layanan yang dikelola sepenuhnya yang memudahkan pengembang untuk membuat, menerbitkan, memelihara, memantau, dan mengamankan APIs pada skala apa pun. Dengan menggunakan REST, Konsol Manajemen AWS Anda dapat membuat REST dan WebSocket APIs bertindak sebagai pintu depan bagi aplikasi untuk mengakses data, logika bisnis, atau fungsionalitas dari layanan back-end Anda, seperti beban kerja yang berjalan di Amazon Elastic Compute Cloud (Amazon EC2), kode yang berjalan, aplikasi web apa pun AWS Lambda, atau aplikasi komunikasi real-time.

API Gateway menangani semua tugas yang terlibat dalam menerima dan memproses hingga ratusan ribu panggilan API bersamaan, termasuk manajemen lalu lintas, otorisasi dan kontrol akses, pemantauan, dan manajemen versi API. API Gateway tidak memiliki biaya minimum atau

biaya startup. Anda hanya membayar untuk panggilan API yang Anda terima dan jumlah data yang ditransfer keluar dan, dengan model harga berjenjang API Gateway, Anda dapat mengurangi biaya saat skala penggunaan API Anda. Untuk mempelajari selengkapnya, lihat Amazon API Gateway.

FAQ: API Gateway di AMS

T: Bagaimana cara meminta akses ke Amazon API Gateway di akun AMS saya?

Minta akses ke API Gateway dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_apigateway_author_role` dan. `customer_apigateway_cloudwatch_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon API Gateway di akun AMS saya?

- Konfigurasi API Gateway terbatas pada sumber daya tanpa `AMS-` atau `MC-` awalan untuk mencegah modifikasi apa pun pada infrastruktur AMS.
- `CREATE`hak istimewa untuk VPCLink dinonaktifkan untuk mencegah pembuatan Elastic Load Balancer yang tidak diatur. Jika VPCLinks diperlukan, lihat Application Load Balancer | Buat.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon API Gateway di akun AMS saya?

Itu tergantung pada jenis API Gateway yang ingin Anda terapkan. Ini bisa menjadi layanan mandiri, tetapi juga dapat meminta akses ke layanan yang ada (misalnya, penyeimbang beban jaringan).

Gunakan AMS SSP untuk menyediakan Alexa for Business di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Alexa for Business secara langsung di akun terkelola AMS Anda. Alexa for Business adalah layanan yang memungkinkan organisasi dan karyawan Anda menggunakan Alexa untuk menyelesaikan lebih banyak pekerjaan. Dengan Alexa for Business, Anda dapat menggunakan Alexa sebagai asisten cerdas Anda untuk menjadi lebih produktif di ruang rapat, di meja Anda, dan bahkan dengan perangkat Alexa yang sudah Anda gunakan di rumah atau saat bepergian. Manajer TI dan fasilitas dapat menggunakan Alexa for Business untuk mengukur dan meningkatkan pemanfaatan ruang pertemuan yang ada di tempat kerja mereka.

Untuk mempelajari lebih lanjut, lihat Alexa for Business.

Alexa for Business di AWS Managed Services FAQ

T: Bagaimana cara meminta akses ke Alexa for Business di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_alexa_console_role` A juga `customer_alexa_device_setup_user` dibuat untuk Device Setup Tool yang disediakan oleh Alexa for Business; Alat Pengaturan Perangkat ini kemudian dapat digunakan untuk mengatur perangkat Anda. Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

Gateway Alexa for Business memungkinkan Anda menghubungkan Alexa for Business ke titik akhir Cisco Webex dan Poly Group Series untuk mengontrol rapat dengan suara Anda. Perangkat lunak gateway berjalan pada perangkat keras lokal Anda dan dengan aman proksi arahan konferensi dari Alexa for Business ke titik akhir Cisco Anda. Gateway membutuhkan dua pasang AWS kredensil untuk berkomunikasi dengan Alexa for Business. Kami menyediakan dua pengguna IAM akses terbatas: `customer_alexa_gateway_installer_user` dan `customer_alexa_gateway_execution_user` untuk gateway Alexa for Business Anda, satu untuk menginstal gateway dan satu untuk mengoperasikan gateway; ini dapat diminta dengan mengirimkan RFC dengan Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat entitas atau kebijakan (diperlukan tinjauan) jenis perubahan (ct-3dpd8mdd9dd9jn1r).

> **Note**
>
> Untuk menghasilkan laporan penggunaan dan mengirimkannya ke Amazon S3, tentukan nama bucket Amazon S3 di RFC layanan yang disediakan sendiri.

T: Apa batasan untuk menggunakan Alexa for Business di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Alexa for Business tersedia dengan peran layanan mandiri Alexa for Business.

T: Apa prasyarat atau dependensi untuk menggunakan Alexa for Business di akun AMS saya?

- Jika Anda bermaksud menggunakan WPA2 Enterprise Wi-Fi untuk menyiapkan perangkat bersama, tentukan jenis keamanan jaringan ini di Alat Pengaturan Perangkat, yang AWS Private Certificate Authority diperlukan.

- AMS hanya membuat kunci rahasia yang dimulai dengan namespace “A4B”. Ini hanya terbatas pada namespace ini.

T: Apa fungsi Alexa for Business yang membutuhkan terpisah? RFCs

Untuk mendaftarkan perangkat Alexa Voice Service (AVS) dengan Alexa for Business, berikan akses ke pembuat perangkat bawaan Alexa. Untuk melakukan ini, peran IAM perlu dibuat di konsol Alexa for Business yang dapat digunakan menggunakan Management | Other | Other | Other change type. Hal ini memungkinkan pembuat perangkat AVS untuk mendaftarkan dan mengelola perangkat dengan Alexa for Business atas nama Anda.

Gunakan AMS SSP untuk menyediakan Amazon AppStream 2.0 di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon AppStream 2.0 (AppStream 2.0) secara langsung di akun terkelola AMS Anda. AppStream 2.0 memungkinkan Anda memindahkan aplikasi desktop Anda ke AWS, tanpa menulis ulang. Anda dapat menginstal aplikasi Anda pada AppStream 2.0, mengatur konfigurasi peluncuran, dan membuat aplikasi Anda tersedia untuk pengguna. AppStream 2.0 menawarkan berbagai pilihan opsi mesin virtual sehingga Anda dapat memilih jenis instans yang paling sesuai dengan kebutuhan aplikasi Anda, dan mengatur parameter skala otomatis sehingga Anda dapat dengan mudah memenuhi kebutuhan pengguna akhir Anda. AppStream 2.0 memungkinkan Anda untuk meluncurkan aplikasi di jaringan Anda sendiri, yang berarti aplikasi Anda dapat berinteraksi dengan AWS sumber daya yang ada.

Amazon AppStream 2.0 memungkinkan Anda menginstal, menguji, dan memperbarui aplikasi dengan cepat dan mudah menggunakan pembuat gambar. Aplikasi apa pun yang berjalan di Microsoft Windows Server 2012 R2, Windows Server 2016, atau Windows Server 2019 didukung, dan Anda tidak perlu melakukan modifikasi apa pun. Ketika pengujian selesai, Anda dapat mengatur konfigurasi peluncuran aplikasi, pengaturan pengguna default, dan mempublikasikan gambar Anda untuk diakses pengguna.

Untuk mempelajari lebih lanjut, lihat AppStream 2.0.

AppStream 2.0 di AWS Managed Services FAQ

T: Bagaimana cara meminta akses ke AppStream 2.0 di akun AMS saya?

Minta akses ke AppStream 2.0 dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-3qe6io8t6jtny) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_appstream_console_role`

A juga `customer_appstream_stream_role` digunakan untuk streaming aplikasi yang mengharuskan pengguna untuk diautentikasi menggunakan kredensil login Active Directory mereka.

Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AppStream 2.0 di akun AMS saya?

- Fungsionalitas berikut harus dikonfigurasi oleh tim Dukungan AMS, dan memerlukan spesifik RFCs. Instruksi tentang meminta fungsionalitas tambahan dapat ditemukan di bagian 4.
  - Membuat dan Streaming dari Titik Akhir VPC Antarmuka.
  - Support untuk titik akhir Amazon S3 untuk folder rumah dan persistensi pengaturan aplikasi di jaringan pribadi.
  - Membuat dan memilih peran IAM yang akan tersedia di semua instance streaming armada.
  - Bergabung dengan armada AppStream 2.0 dan pembuat gambar domain Microsoft Active Directory.
  - Membuat Laporan Penggunaan Kustom AppStream 2.0.
  - Custom branding saat ini tidak didukung.

T: Apa prasyarat atau dependensi untuk menggunakan AppStream 2.0 di akun AMS saya?

Saat mengirimkan RFC ke onboard AppStream 2.0, sertakan nama bucket Amazon S3 yang akan digunakan untuk laporan penggunaan 2.0. AppStream Nama bucket ditambahkan ke `customer-appstream-usagereports-policy` yang dibuat saat AppStream 2.0 di-onboard.

T: Fungsionalitas AppStream 2.0 apa yang membutuhkan terpisah RFCs?

- Untuk memilih titik akhir VPC antarmuka untuk AppStream 2.0, kirimkan Manajemen | Lainnya | Lainnya | Perbarui jenis perubahan RFC untuk membuat titik akhir VPC di akun Anda. Untuk langkah-langkah untuk membuat titik akhir khusus untuk AppStream 2.0, lihat Membuat dan Streaming dari Titik Akhir VPC Antarmuka di AppStream panduan pengguna 2.0.
- Support untuk titik akhir Amazon S3 untuk folder rumah dan persistensi pengaturan aplikasi di jaringan pribadi dapat dikonfigurasi dengan meminta titik akhir VPC Amazon S3 dengan Manajemen | Lainnya | Lainnya | Lainnya | Buat jenis perubahan RFC. RFC harus menyertakan bucket Amazon S3 target yang menghosting konten folder beranda, atau pengaturan aplikasi

bucket Amazon S3, masing-masing. RFC ini akan memberikan AppStream 2.0 izin yang diperlukan untuk mengakses titik akhir VPC Amazon S3. Untuk langkah-langkah untuk membuat titik akhir khusus untuk streaming, lihat Menggunakan Titik Akhir VPC Amazon S3 untuk Folder Rumah dan Persistensi Pengaturan Aplikasi dalam panduan pengguna 2.0. AppStream

- Untuk membuat dan memilih peran IAM yang akan tersedia di semua instance streaming armada, kirimkan Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat entitas atau kebijakan (review required) change type (ct-3dpd8mdd9jn1r) RFC yang meminta peran IAM dengan kebijakan yang diperlukan. Nama peran IAM harus selalu dimulai dengan awalan: “customer_appstream”.
- Armada Amazon AppStream 2.0 dan pembuat gambar dapat digabungkan ke domain di Microsoft Active Directory dengan mengirimkan Manajemen | Lainnya | Lainnya | Perbarui jenis perubahan RFC untuk pembuatan Akun Layanan di Active Directory (AD). Izin minimal yang diperlukan untuk bergabung dengan Microsoft Active Directory didefinisikan dalam dokumentasi AppStream 2.0 di Pemberian Izin untuk Membuat dan Mengelola Objek Komputer Direktori Aktif.
- Untuk membuat Laporan Penggunaan AppStream 2.0 kustom, kirimkan Manajemen | Lainnya | Lainnya | Buat jenis perubahan RFC yang meminta berikut:
  - “AppStreamUsageReports” Pembuatan tumpukan CFN
  - “customer_appstream_usagereports_role” disediakan di akun
  - Juga, berikan detail berikut:
    - Berikan ekspresi CRON untuk menjadwalkan Crawler run. Secara default adalah 23:00 UTC setiap hari.
    - Bucket Amazon S3 ARN akan digunakan untuk hasil kueri Athena. Bucket ini harus memiliki awalan: `aws-athena-query-results`
    - Bucket Amazon S3 ARN untuk Log Laporan Penggunaan AppStream 2.0.

  Setelah peran disediakan, masukkan peran ke dalam solusi federasi Anda dan login, lalu akses dan AWS GlueAWS Glue Athena untuk membuat laporan kustom menggunakan peran laporan penggunaan. Untuk detail tentang menggunakan Laporan Penggunaan AppStream 2.0, lihat Membuat Laporan Kustom dan Menganalisis Data Penggunaan AppStream 2.0, dalam dokumentasi AppStream 2.0.

Gunakan AMS SSP untuk menyediakan Amazon Athena di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Athena (Athena) secara langsung di akun terkelola AMS Anda. Athena adalah layanan kueri interaktif

yang membantu Anda menganalisis data di Amazon S3 menggunakan SQL standar. Athena tidak memiliki server, sehingga tidak ada infrastruktur untuk dikelola dan Anda hanya membayar untuk mengkueri yang Anda jalankan. Anda mengarahkan ke data Anda di Amazon S3, menentukan skema, dan mulai melakukan kueri menggunakan SQL standar. Sebagian besar hasil disampaikan dalam hitungan detik. Dengan Athena, tidak perlu pekerjaan kompleks extract-transform-load (ETL) untuk mempersiapkan data Anda untuk analisis. Ini membuatnya mudah bagi siapa pun dengan keterampilan SQL untuk menganalisis kumpulan data skala besar dengan cepat. Untuk mempelajari lebih lanjut, lihat Amazon Athena.

FAQ: Athena di AMS

T: Bagaimana cara meminta akses ke Amazon Athena di akun AMS saya?

Minta akses ke Athena dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_athena_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Athena di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Athena tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Athena di akun AMS saya?

Athena memiliki ketergantungan besar pada AWS Glue layanan, karena menggunakan data catalog/ metastore yang dibuat dengan. AWS Glue Oleh karena itu, AWS Glue izin disertakan dalam Athena RFC yang sukses.

Peran tersebut `customer_athena_console_role` memiliki prasyarat untuk ember Amazon S3. Untuk membuat bucket baru, gunakan CT otomatis `ct-1a68ck03fn98r` (Deployment | Advanced stack components | S3 storage | Create). Saat Anda menggunakan CT otomatis ini untuk membuat bucket S3 untuk Athena, nama bucket harus dimulai dengan awalan. `athena-query-results-*`

Gunakan AMS SSP untuk menyediakan Amazon Bedrock di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon Bedrock secara langsung di akun terkelola AMS Anda. Amazon Bedrock adalah layanan yang dikelola sepenuhnya yang membuat model foundation berkinerja tinggi (FMs) dari startup AI terkemuka dan AWS tersedia untuk Anda gunakan melalui API terpadu. Anda dapat memilih dari

berbagai model pondasi untuk menemukan model yang paling cocok untuk kasus penggunaan Anda. Amazon Bedrock juga menawarkan serangkaian kemampuan yang luas untuk membangun aplikasi AI generatif dengan keamanan, privasi, dan AI yang bertanggung jawab. Menggunakan Amazon Bedrock, Anda dapat dengan mudah bereksperimen dengan dan mengevaluasi model dasar teratas untuk kasus penggunaan Anda, menyesuaikannya secara pribadi dengan data Anda menggunakan teknik seperti fine-tuning dan Retrieval Augmented Generation (RAG), dan membangun agen yang menjalankan tugas menggunakan sistem perusahaan dan sumber data Anda.

Dengan pengalaman tanpa server Amazon Bedrock, Anda dapat memulai dengan cepat, menyesuaikan model foundation secara pribadi dengan data Anda sendiri, serta mengintegrasikan serta menerapkannya dengan mudah dan aman ke dalam aplikasi Anda menggunakan alat AWS tanpa harus mengelola infrastruktur apa pun. Untuk informasi lebih lanjut, lihat Amazon Bedrock.

FAQ: Batuan Dasar Amazon di AMS

T: Bagaimana cara meminta akses ke Amazon Bedrock di akun AMS saya?

Untuk meminta akses ke Amazon Bedrock, kirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) ubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_bedrock_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Bedrock di akun AMS saya?

- Basis pengetahuan Amazon Bedrock tidak didukung secara default sebagai bagian dari peran SSPS karena ketergantungannya pada OpenSearch Amazon Service Serverless yang saat ini tidak didukung di AMS.
- Bedrock Studio tidak didukung karena ketergantungannya pada layanan yang tidak didukung seperti Amazon. DataZone

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Bedrock di akun AMS saya?

- Langganan model pihak ketiga yang memerlukan AWS Marketplace izin harus dilakukan oleh peran default (`AWSManagedServicesAdminRole`di MALZ dan `Customer_ReadOnly_Role` di SALZ). Ini karena peran default menyertakan AWS Marketplace izin.
- Jika enkripsi data digunakan, maka Anda harus memberikan ARN AWS KMS kunci saat Anda meminta pembuatan peran konsol. Selain itu, ember Amazon S3 yang digunakan harus memiliki “batuan dasar” dalam namanya.

Gunakan AMS SSP untuk menyediakan Amazon CloudSearch di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses CloudSearch kapabilitas Amazon secara langsung di akun terkelola AMS Anda. Amazon CloudSearch adalah layanan terkelola di AWS Cloud yang Anda gunakan agar hemat biaya untuk menyiapkan, mengelola, dan menskalakan solusi pencarian untuk situs web atau aplikasi Anda. Amazon CloudSearch mendukung 34 bahasa dan fitur pencarian populer seperti penyorotan, pelengkapan otomatis, dan pencarian geospasial. Untuk mempelajari lebih lanjut, lihat Amazon CloudSearch.

> **Note**
>
> AWS telah menutup akses pelanggan baru ke Amazon CloudSearch, efektif 25 Juli 2024. Pelanggan Amazon CloudSearch yang sudah ada dapat terus menggunakan layanan seperti biasa. AWS terus berinvestasi dalam peningkatan keamanan, ketersediaan, dan kinerja untuk Amazon CloudSearch, tetapi kami tidak berencana untuk memperkenalkan fitur baru. Untuk memahami perbedaan antara Amazon CloudSearch dan Amazon OpenSearch Service, dan bagaimana Anda dapat beralih ke OpenSearch Layanan, hubungi arsitek cloud (CA) Anda untuk mendapatkan panduan. Untuk informasi selengkapnya tentang transisi ke OpenSearch Layanan, lihat Transisi dari layanan Amazon ke CloudSearch Amazon OpenSearch Service.

FAQ Amazon CloudSearch di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon CloudSearch di akun AMS saya?

Minta akses ke Amazon CloudSearch dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_csearch_admin_role` dan. `customer_csearch_dev_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon CloudSearch di akun AMS saya?

Fungsionalitas penuh Amazon CloudSearch tersedia di akun AMS Anda. Semua solusi database yang didukung AMS saat ini didukung di Amazon. CloudSearch Perhatikan bahwa, saat ini, DynamoDB adalah satu-satunya solusi database AWS terkelola yang tidak dapat diindeks.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon CloudSearch di akun AMS saya?

Amazon CloudSearch bergantung pada Amazon S3 yang bekerja dengan Penyedia Identitas untuk menganalisis data input secara otomatis dan menentukan bidang tabel. Akses ke Amazon S3 tidak disediakan dengan RFC ini, dan harus diminta secara terpisah dalam permintaan layanan.

Menggunakan AMS SSP untuk menyediakan Amazon CloudWatch Synthetics di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon CloudWatch Synthetics secara langsung di akun terkelola AMS Anda. Anda dapat menggunakan Amazon CloudWatch Synthetics untuk membuat 'kenari' untuk memantau titik akhir Anda dan. APIs

Canary adalah skrip yang dapat dikonfigurasi, ditulis dalam Node.js atau Python, yang berjalan sesuai jadwal. Mereka membuat fungsi Lambda di akun Anda yang menggunakan Node.js atau Python sebagai kerangka kerja. Canary bekerja di atas protokol HTTP maupun HTTPS. Canary memeriksa ketersediaan dan latensi titik akhir Anda dan dapat menyimpan data waktu buka dan tangkapan layar UI. Mereka memantau REST Anda APIs, URLs, dan konten situs web, dan mereka dapat memeriksa perubahan yang tidak sah dari phishing, injeksi kode, dan skrip lintas situs.

Canary mengikuti rute yang sama dan melakukan tindakan yang sama sebagai pelanggan, sehingga memungkinkan Anda untuk terus memverifikasi pengalaman pelanggan Anda bahkan ketika Anda tidak memiliki lalu lintas pelanggan pada aplikasi Anda. Dengan menggunakan canary, Anda dapat menemukan masalah sebelum para pelanggan Anda menemukannya. Untuk mempelajari lebih lanjut, lihat Amazon CloudWatch: Menggunakan pemantauan sintetis.

FAQ Amazon CloudWatch Synthetics di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon CloudWatch Synthetics di akun AMS saya?

Minta akses ke Amazon CloudWatch Synthetics dengan mengirimkan RFC dengan Management | AWS service | Self-provisioned service | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: 'customer_cw_synthetics_console_role' dan 'customer_cw_synthetics_canary_lambda_role'. Setelah disediakan di akun Anda, Anda harus mengaktifkan peran 'customer_cw_synthetics_console_role' dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon CloudWatch Synthetics di akun AMS saya?

Tidak ada batasan untuk penggunaan Amazon CloudWatch Synthetics di akun AMS Anda. Membuat peran untuk kenari di luar peran layanan yang disediakan AMS 'customer_cw_synthetics_canary_lambda_role' dilarang.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon CloudWatch Synthetics di akun AMS saya?

Canary membuat dan menggunakan bucket Amazon CloudWatch Synthetics S3 default: cw-syn-results "- -" *${accountnumber} ${default-region}*

Gunakan AMS SSP untuk menyediakan kumpulan pengguna Amazon Cognito di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas kumpulan pengguna Amazon Cognito secara langsung di akun terkelola AMS Anda. Kumpulan pengguna Amazon Cognito menyediakan direktori pengguna aman yang menskalakan hingga ratusan juta pengguna. Sebagai layanan yang dikelola sepenuhnya, kumpulan pengguna Amazon Cognito dapat diatur tanpa khawatir tentang infrastruktur server yang berdiri. Layanan ini memungkinkan Anda mengelola kumpulan pengguna akhir yang dapat Anda gunakan untuk berintegrasi dengan aplikasi internal Anda. Layanan ini memberi Anda alternatif untuk database yang disesuaikan atau direktori pengguna akhir untuk aplikasi web atau seluler. Pada saat yang sama, kumpulan pengguna Amazon Cognito menyediakan serangkaian fungsi lengkap dari layanan direktori seperti kebijakan kata sandi, otentikasi multi faktor, pemulihan kata sandi, dan pendaftaran sendiri ke layanan. Ini juga memungkinkan aplikasi untuk menggabungkan akses di layanan publik populer lainnya seperti OpenID, Facebook, Amazon atau Google.

Amazon Cognito dibagi menjadi dua produk utama. Kumpulan pengguna Amazon Cognito dan Penyedia Identitas Amazon Cognito. Bagian ini berfokus pada kumpulan pengguna Amazon Cognito, yang menyediakan akses ke AWS layanan lain seperti Amazon S3 atau DynamoDB. Layanan ini memungkinkan Anda menggunakan kumpulan pengguna Amazon Cognito, atau penyedia identitas pihak ketiga, untuk menyediakan akses ke AWS layanan. Ini juga menyediakan akses ke AWS layanan menggunakan akses tamu anonim. Karena sifat kuat dari kumpulan pengguna Amazon Cognito, itu akan dikelola secara manual case-by-case berdasarkan layanan manual operasi, untuk menghindari potensi kerusakan keamanan ke akun. Untuk mempelajari lebih lanjut, lihat Kumpulan Pengguna Amazon Cognito.

Kumpulan pengguna Amazon Cognito di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke kumpulan pengguna Amazon Cognito di akun AMS saya?

Implementasi kumpulan pengguna Amazon Cognito di AMS adalah proses 2 langkah:

1. Kirim Manajemen | Lainnya | Lainnya | Buat (ct-1e1xtak34nx76) ubah jenis dan minta pembuatan kumpulan pengguna Amazon Cognito di Akun AMS Anda. Sertakan informasi berikut:
   - AWS Wilayah.
   - Nama untuk Kumpulan Pengguna Cognito.
   - Jika Anda ingin menggunakan Amazon Simple Email Service (Amazon SES) untuk mengirim pesan dan notifikasi alih-alih layanan email Cognito internal default, maka pelanggan harus memberikan alamat email yang sudah divalidasi untuk Layanan Amazon SES di akun. Alamat ini akan digunakan untuk bidang “Dari” dan “BALAS-KE” dari pesan. Mereka juga harus menunjukkan Wilayah tempat Amazon SES diaktifkan (us-east-1, eu-west-1 atau us-west-2).
   - Jika Anda ingin menggunakan pesan SMS untuk kata sandi dan verifikasi satu kali, maka pelanggan harus menunjukkannya.
2. Minta akses pengguna dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_cognito_admin_role` dan. `customer_cognito_importjob_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda. Peran ini memungkinkan Anda mengelola kumpulan pengguna Amazon Cognito, mengelola pengguna dan grup di kolam, membuat pekerjaan impor untuk pengguna, memodifikasi pesan notifikasi dan langganan, mengaitkan aplikasi ke kumpulan pengguna, mengelola sendiri menambahkan layanan federasi ke kolam, dan menghapus kumpulan yang sudah dibuat.

T: Apa batasan untuk menggunakan kumpulan pengguna Amazon Cognito di akun AMS saya?

Anda tidak akan dapat membuat kumpulan pengguna Amazon Cognito. Tindakan itu memerlukan pembuatan peran IAM untuk memanfaatkan layanan yang digunakan oleh Amazon Cognito, seperti Amazon SES dan Amazon Simple Notification Service (Amazon SNS).

T: Apa prasyarat atau dependensi untuk menggunakan kumpulan pengguna Amazon Cognito di akun AMS saya?

Jika Anda ingin menggunakan Amazon SES untuk mengirim pesan dan pemberitahuan melalui email ke kumpulan pengguna Anda, mereka seharusnya sudah mengaktifkan layanan Amazon SES di akun, dan sudah memvalidasi alamat email yang harus digunakan di bidang “DARI” dan

“BALAS-KE” dari email yang dikirim. Untuk informasi selengkapnya tentang memvalidasi alamat email menggunakan Amazon SES, lihat Memverifikasi Alamat Email di Amazon SES.

Gunakan AMS SSP untuk menyediakan Amazon Comprehend di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Comprehend secara langsung di akun terkelola AMS Anda. Amazon Comprehend adalah layanan pemrosesan bahasa alami (NLP) yang menggunakan pembelajaran mesin untuk menemukan wawasan dan hubungan dalam teks, tidak diperlukan pengalaman pembelajaran mesin. Amazon Comprehend menggunakan pembelajaran mesin untuk membantu Anda menemukan wawasan dan hubungan dalam data tidak terstruktur Anda. Layanan mengidentifikasi bahasa teks; mengekstrak frasa kunci, tempat, orang, merek, atau peristiwa; memahami seberapa positif atau negatif teks itu; menganalisis teks menggunakan tokenisasi dan bagian pidato; dan secara otomatis mengatur kumpulan file teks berdasarkan topik. Anda juga dapat menggunakan kemampuan AutoML di Amazon Comprehend untuk membuat kumpulan entitas kustom atau model klasifikasi teks yang disesuaikan secara unik dengan kebutuhan organisasi Anda. Untuk mempelajari lebih lanjut, lihat Amazon Comprehend.

FAQ Amazon Comprehend di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon Comprehend di akun AMS saya?

Konsol Amazon Comprehend dan peran akses data dapat diminta melalui pengajuan dua Layanan AMS: RFCs

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_comprehend_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Comprehend di akun AMS saya?

Buat fungsionalitas Peran IAM Baru melalui konsol Amazon Comprehend dibatasi. Jika tidak, fungsionalitas penuh Amazon Comprehend tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Comprehend di akun AMS saya?

Amazon S3 dan AWS Key Management Service (AWS KMS) diperlukan untuk menggunakan Amazon Comprehend, jika bucket Amazon S3 dienkripsi dengan kunci. AWS KMS

Menggunakan AMS SSP untuk menyediakan Amazon Connect di akun AMS

> **Note**
>
> Setelah mempertimbangkan dengan cermat, kami memutuskan untuk mengakhiri dukungan untuk Amazon Connect Voice ID, efektif 20 Mei 2026. Amazon Connect Voice ID tidak akan lagi menerima pelanggan baru mulai 20 Mei 2025. Sebagai pelanggan lama dengan akun yang mendaftar untuk layanan sebelum 20 Mei 2025, Anda dapat terus menggunakan fitur ID Suara Amazon Connect. Setelah 20 Mei 2026, Anda tidak akan lagi dapat menggunakan Amazon Connect Voice ID.

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Connect secara langsung di akun terkelola AMS Anda. Amazon Connect adalah pusat kontak cloud omnichannel yang membantu perusahaan menyediakan layanan pelanggan yang unggul dengan biaya lebih rendah. Amazon Connect memberikan pengalaman yang mulus di seluruh suara dan obrolan untuk pelanggan dan agen. Ini termasuk satu set alat untuk perutean berbasis keterampilan, analitik real-time dan historis yang kuat, dan alat manajemen easy-to-use intuitif — semuanya dengan harga. pay-as-you-go

Anda dapat membuat satu atau beberapa instance instance pusat kontak virtual di akun landing zone multi-akun AMS atau akun landing zone akun tunggal. Anda dapat menggunakan penyedia identitas SAMP 2.0 yang ada untuk akses agen atau menggunakan dukungan asli Amazon Connect untuk manajemen siklus hidup pengguna.

Selain itu, Anda dapat mengklaim nomor telepon free/direct panggilan tol untuk setiap instans Amazon Connect dari konsol Amazon Connect. Anda dapat membuat alur kontak yang kaya untuk mencapai pengalaman dan perutean pelanggan yang diinginkan menggunakan antarmuka pengguna easy-to-use grafis. Alur kontak dapat memanfaatkan AWS Lambda fungsi untuk diintegrasikan dengan penyimpanan data lokal dan API. Anda juga dapat mengaktifkan streaming data menggunakan Kinesis Streams dan Firehose.

Rekaman panggilan, transkrip obrolan, dan laporan, disimpan dalam bucket Amazon S3 yang dienkripsi menggunakan kunci. AWS KMS Log alur kontak dapat disimpan ke grup CloudWatch log.

Untuk mempelajari lebih lanjut, lihat Amazon Connect.

FAQ Amazon Connect di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon Connect di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_connect_console_role` dan. `customer_connect_user_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Connect di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Connect tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Connect di akun AMS saya?

- Anda harus membuat AWS KMS Key dan bucket Amazon S3 menggunakan AMS standar RFCs; bucket Amazon S3 diperlukan untuk menyimpan rekaman panggilan dan transkrip obrolan.
- Jika Anda ingin mengintegrasikan dengan Active Directory (AD), AD Connector diperlukan untuk integrasi antara instans Amazon Connect yang dihosting AMS dan layanan direktori lokal Anda. AD Connector dapat dikonfigurasi di akun Anda dengan meminta RFC 'Manajemen | Lainnya | Lainnya'.
- Anda dapat mengaktifkan layanan mandiri opsional berikut berdasarkan persyaratan alur kontak Anda.
  - AWS Lambda: Anda dapat menggunakan fungsi Lambda untuk memperluas alur kontak guna memanfaatkan penyimpanan data lokal yang ada atau. APIs Anda dapat menggunakan layanan Lambda yang disediakan sendiri untuk membuat fungsi Lambda.
  - Amazon Kinesis Data Streams: Anda dapat membuat aliran data untuk mengaktifkan streaming Data ke aplikasi eksternal. Anda dapat melakukan streaming catatan jejak kontak atau Acara Agen.
  - Amazon Kinesis Data Firehose: Anda dapat membuat Data Firehose untuk mengalirkan catatan jejak kontak volume tinggi ke aplikasi eksternal.
  - Amazon Lex: Anda dapat memanfaatkan Amazon Lex Chatbots untuk menciptakan arus kontak cerdas yang memanfaatkan layanan Amazon Alexa untuk pengalaman dan otomatisasi pelanggan yang kaya.
- T: Bagaimana cara saya meminta untuk menambahkan daftar negara untuk panggilan keluar atau masuk?

Untuk menambahkan daftar negara untuk panggilan keluar atau masuk, kirimkan permintaan layanan ke AMS.

Menggunakan AMS SSP untuk menyediakan Amazon Data Firehose di akun AMS

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Data Firehose secara langsung di akun terkelola AMS Anda. Firehose adalah cara termudah untuk memuat data streaming secara andal ke dalam data lake, penyimpanan data, dan alat analitik. Ini dapat menangkap, mengubah, dan memuat data streaming ke Amazon S3, Amazon Redshift, OpenSearch Amazon Service, dan Splunk, memungkinkan analitik hampir real-time dengan alat intelijen bisnis dan dasbor yang sudah Anda gunakan saat ini. Ini adalah layanan yang dikelola sepenuhnya yang secara otomatis menskalakan agar sesuai dengan throughput data Anda dan tidak memerlukan administrasi berkelanjutan. Ini juga dapat mengumpulkan, mengompres, mengubah, dan mengenkripsi data sebelum memuatnya, meminimalkan jumlah penyimpanan yang digunakan di tempat tujuan dan meningkatkan keamanan. Untuk mempelajari lebih lanjut, lihat Apa itu Amazon Data Firehose?

FAQ Firehose di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Data Firehose di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_kinesis_firehose_user_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan Firehose di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Data Firehose tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Firehose di akun AMS saya?

Peran IAM terkait layanan baru harus diminta untuk setiap aliran pengiriman. Anda juga dapat menggunakan kembali satu peran terkait layanan untuk semua aliran dengan memperbarui kebijakan

peran dengan izin sumber daya yang diperlukan (termasuk ember S3/Kunci KMS/Fungsi Lambda/ aliran Kinesis).

Setelah Anda mengirimkan RFC untuk menambahkan Firehose, insinyur Operasi AMS akan menghubungi Anda melalui Permintaan Layanan untuk sumber daya yang ingin Anda sambungkan dengan Firehose Data (misalnya AWS KMS, Aliran S3, Lambda, dan Kinesis). ARNs

Gunakan AMS SSP untuk menyediakan Amazon DevOps Guru di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon DevOps Guru secara langsung di akun terkelola AMS Anda. Amazon DevOps Guru adalah layanan operasi yang dikelola sepenuhnya yang memudahkan pengembang dan operator untuk meningkatkan kinerja dan ketersediaan aplikasi mereka. DevOpsGuru memungkinkan Anda membongkar tugas administratif yang terkait dengan mengidentifikasi masalah operasional sehingga Anda dapat dengan cepat menerapkan rekomendasi untuk meningkatkan aplikasi Anda. DevOpsGuru menciptakan wawasan reaktif yang dapat Anda gunakan untuk meningkatkan aplikasi Anda sekarang. Ini juga menciptakan wawasan proaktif untuk membantu Anda menghindari masalah operasional yang mungkin memengaruhi aplikasi Anda di masa mendatang. DevOpsGuru menerapkan pembelajaran mesin untuk menganalisis data operasional dan metrik aplikasi serta peristiwa Anda untuk mengidentifikasi perilaku yang menyimpang dari pola operasi normal. Anda akan diberitahu ketika DevOps Guru mendeteksi masalah operasional atau risiko. Untuk setiap masalah, DevOps Guru menyajikan rekomendasi cerdas untuk mengatasi masalah operasional masa depan saat ini dan yang diprediksi.

Untuk mempelajari lebih lanjut, lihat Apa itu Amazon DevOps Guru.

FAQ Amazon DevOps Guru di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon DevOps Guru di akun AMS saya?

Untuk meminta akses, kirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_devopsguru_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon DevOps Guru di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon DevOps Guru tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan DevOps Amazon Guru di akun AMS saya?

Tidak ada prasyarat. DevOpsGuru memanfaatkan AWS layanan berikut: Amazon CloudWatch Logs, RDS Insights, AWS X-Ray, AWS Lambda dan. AWS CloudTrail

Gunakan AMS SSP untuk menyediakan Amazon DocumentDB (dengan kompatibilitas MongoDB) di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon DocumentDB (dengan kompatibilitas MongoDB) secara langsung di akun terkelola AMS Anda. Amazon DocumentDB (dengan kompatibilitas MongoDB) adalah layanan database dokumen yang cepat, terukur, sangat tersedia, dan dikelola sepenuhnya yang mendukung beban kerja MongoDB. Amazon DocumentDB memberi Anda kinerja, skalabilitas, dan ketersediaan yang Anda butuhkan saat mengoperasikan beban kerja MongoDB yang penting dalam skala besar. Amazon DocumentDB mengimplementasikan Apache 2.0 open source MongoDB 3.6 API dengan meniru tanggapan yang diharapkan klien MongoDB dari server MongoDB, memungkinkan Anda untuk menggunakan driver dan alat MongoDB yang ada dengan Amazon DocumentDB. Di Amazon DocumentDB, penyimpanan dan komputasi dipisahkan, memungkinkan masing-masing untuk menskalakan secara independen, dan Anda dapat meningkatkan kapasitas baca hingga jutaan permintaan per detik dengan menambahkan hingga 15 replika baca latensi rendah, terlepas dari ukuran data Anda. Amazon DocumentDB dirancang untuk ketersediaan 99,99% dan mereplikasi enam salinan data Anda di tiga Availability Zone (). AWS AZs Anda dapat menggunakan AWS Database Migration Service (DMS) secara gratis (selama enam bulan) untuk memigrasikan database EC2 MongoDB Amazon Elastic Compute Cloud (Amazon) lokal atau Amazon Elastic Compute Cloud (Amazon) ke Amazon DocumentDB tanpa waktu henti. Untuk mempelajari lebih lanjut, lihat Amazon DocumentDB (dengan kompatibilitas MongoDB).

FAQ Amazon DocumentDB di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon DocumentDB di akun AMS saya?

Konsol Amazon DocumentDB dan peran akses data dapat diminta melalui pengajuan dua RFCs AMS, akses konsol, dan akses data:

Minta akses ke Amazon DocumentDB dengan mengirimkan RFC dengan Manajemen AWS | layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_documentdb_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon DocumentDB di akun AMS saya?

Amazon DocumentDB memerlukan izin khusus Amazon RDS. Karena AMS sepenuhnya mengelola Amazon RDS, peran IAM untuk Amazon DocumentDB mencakup beberapa batasan tindakan di Amazon RDS. Pembatasan berikut berlaku:

- Akses ke `DeleteDBInstance` dan `DeleteDBCluster` APIs telah dibatasi. Untuk menggunakan penghapusan tersebut APIs, kirimkan RFC dengan Manajemen | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Perbarui entitas atau kebijakan (diperlukan tinjauan) jenis perubahan (ct-27tuth19k52b4).
- Anda tidak dapat menambah atau menghapus tag dari instans Amazon RDS.
- Anda tidak dapat membuat instans Amazon DocumentDB Anda menjadi publik.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon DocumentDB di akun AMS saya?

Amazon S3 dan AWS KMS diperlukan untuk menggunakan Amazon DocumentDB, jika bucket Amazon S3 dienkripsi dengan kunci. AWS KMS

Gunakan AMS SSP untuk menyediakan Amazon DynamoDB di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon DynamoDB (DynamoDB) secara langsung di akun terkelola AMS Anda. Amazon DynamoDB adalah nilai kunci dan database dokumen yang memberikan kinerja milidetik satu digit pada skala apa pun. Ini adalah database multi-wilayah, multi-aktif yang dikelola sepenuhnya dengan keamanan bawaan, pencadangan dan pemulihan, dan caching dalam memori untuk aplikasi skala internet. Untuk mempelajari selengkapnya, lihat Amazon DynamoDB.

Amazon DynamoDB Accelerator (DAX) adalah layanan caching write-through yang dirancang untuk memudahkan proses menambahkan cache ke tabel DynamoDB. DAX ditujukan untuk aplikasi yang memerlukan pembacaan performa tinggi.

FAQ DynamoDB di AWS Managed Services

T: Bagaimana cara meminta akses ke DynamoDB dan DAX di akun AMS saya?

Minta akses ke DynamoDB dan DAX dengan mengirimkan RFC dengan Manajemen AWS | layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran dan kebijakan IAM berikut ke akun Anda:

- Nama peran DynamoDB: `customer_dynamodb_role`

  Nama peran layanan DAX: `customer_dax_service_role`
- Nama kebijakan DynamoDB: `customer_dynamodb_policy`

  Kebijakan layanan DAX: `customer_dax_service_policy`

Setelah disediakan di akun Anda, Anda harus memasukkan solusi `customer_dynamodb_role` dalam federasi Anda.

T: Apa batasan untuk menggunakan DynamoDB di akun AMS saya?

Semua fungsi DynamoDB didukung termasuk DynamoDB Accelerator (DAX).

Saat membuat alarm untuk tabel tertentu, nama alarm harus diawali dengan “pelanggan*”; misalnya,. `customer-employee-table-high-put-latency`

Saat membuat topik Amazon SNS untuk DynamoDB, itu harus diberi nama:. `dynamodb`

Untuk menghapus topik Amazon SNS yang dibuat oleh DynamoDB, kirimkan Manajemen | Lainnya | Lainnya | Perbarui jenis perubahan RFC.

T: Apa prasyarat atau dependensi untuk menggunakan DynamoDB di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan DynamoDB di akun AMS Anda.

Gunakan AMS SSP untuk menyediakan Amazon Elastic Container Registry di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Elastic Container Registry (Amazon ECR) Registry ECR) secara langsung di akun terkelola AMS Anda. Amazon Elastic Container Registry adalah registri kontainer Docker yang dikelola sepenuhnya yang memudahkan pengembang untuk menyimpan, mengelola, dan menyebarkan gambar kontainer Docker. Amazon ECR terintegrasi dengan Amazon Elastic Container Service (Amazon ECS), menyederhanakan pengembangan Anda ke alur kerja produksi. Amazon ECR menghilangkan kebutuhan untuk mengoperasikan repositori kontainer Anda sendiri atau khawatir tentang penskalaan infrastruktur yang mendasarinya. Amazon ECS meng-host gambar Anda dalam arsitektur yang sangat tersedia dan dapat diskalakan, memungkinkan Anda untuk menyebarkan kontainer secara andal untuk aplikasi Anda. Integrasi dengan AWS Identity and Access Management (IAM) menyediakan kontrol tingkat sumber daya dari setiap repositori. Dengan Amazon ECR, tidak

ada biaya atau komitmen di muka. Anda hanya membayar untuk jumlah data yang Anda simpan di repositori dan data yang ditransfer ke Internet.

Untuk mempelajari lebih lanjut, lihat Amazon Elastic Container Registry.

FAQ Amazon Elastic Container Registry di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon ECR di akun AMS saya?

Minta akses ke Amazon ECR dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_ecr_console_role`, dan `customer_ecr_poweruser_instance_profile` dengan kebijakan IAM terkait, `customer_ecr_console_policy` dan`customer_ecr_poweruser_instance_profile_policy`, masing-masing. Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon ECR di akun AMS saya?

Ada batasan seputar ruang nama AMS untuk penggunaan Amazon ECR di akun AMS Anda. Gambar kontainer mungkin tidak diawali dengan “AMS-” atau “Sentinel-”.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon ECR di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Amazon ECR di akun AMS Anda.

Menggunakan AMS SSP untuk menyediakan EC2 Image Builder di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Image Builder EC2 secara langsung di akun terkelola AMS Anda. EC2 Image Builder adalah AWS layanan yang dikelola sepenuhnya yang membuatnya lebih mudah untuk mengotomatiskan pembuatan, pengelolaan, dan penyebaran gambar server yang disesuaikan, aman, dan up-to-date “emas” yang sudah diinstal sebelumnya dan dikonfigurasi sebelumnya dengan perangkat lunak dan pengaturan untuk memenuhi standar TI tertentu.

Anda dapat menggunakan Konsol Manajemen AWS, AWS CLI, atau APIs untuk membuat gambar khusus di akun Anda AWS . Saat Anda menggunakan Konsol Manajemen AWS, wizard Amazon EC2 Image Builder memandu Anda melalui langkah-langkah untuk:

- Berikan artefak awal

- Tambah dan hapus perangkat lunak
- Sesuaikan pengaturan dan skrip
- Jalankan tes yang dipilih
- Mendistribusikan gambar ke AWS Wilayah

Gambar yang Anda buat dibuat di akun Anda dan dapat dikonfigurasi untuk tambalan sistem operasi secara berkelanjutan. Untuk mempelajari lebih lanjut, lihat EC2 Image Builder.

EC2 FAQ Image Builder di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke EC2 Image Builder di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. Melalui RFC ini, peran IAM berikut akan disediakan di akun Anda:. `customer_ec2_imagebuilder_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk EC2 Image Builder?

AMS tidak mendukung penggunaan Default Layanan untuk konfigurasi infrastruktur. Anda dapat membuat konfigurasi infrastruktur baru atau menggunakan yang sudah ada.

AMS saat ini tidak mendukung pembuatan resep wadah.

T: Apa prasyarat atau dependensi untuk mengaktifkan Image Builder? EC2

- EC2 Peran terkait layanan Image Builder: Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat resource Image Builder pertama di Konsol Manajemen AWS, AWS CLI, atau AWS API, Image Builder membuat peran terkait layanan untuk Anda.
- Instans yang digunakan untuk membuat gambar dan menjalankan pengujian menggunakan Image Builder harus memiliki akses ke layanan Systems Manager. Agen SSM akan diinstal pada gambar sumber jika belum ada, dan akan dihapus sebelum gambar dibuat.
- AWS IAM: Peran IAM yang Anda kaitkan dengan profil instans harus memiliki izin untuk menjalankan komponen build dan test yang disertakan dalam image Anda. Kebijakan peran IAM berikut harus dilampirkan ke peran IAM yang terkait dengan profil instans: `EC2InstanceProfileForImageBuilder` dan. `AmazonSSMManagedInstanceCore` Nama peran IAM harus berisi `*imagebuilder*` kata kunci.

- Jika Anda mengonfigurasi logging, profil instance yang ditentukan dalam konfigurasi infrastruktur Anda harus memiliki `s3:PutObject` izin untuk bucket target (`arn:aws:s3:::{bucket-name}/*`). Misalnya:

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::{bucket-name}/*"
        }
    ]
}
```

- Buat topik SNS dengan nama 'imagebuilder' untuk menerima peringatan dan pemberitahuan dari Image Builder. EC2

Gunakan AMS SSP untuk menyediakan Amazon ECS AWS Fargate di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses Amazon ECS pada AWS Fargate kemampuan langsung di akun terkelola AMS Anda. AWS Fargate adalah teknologi yang dapat Anda gunakan dengan Amazon ECS untuk menjalankan kontainer (lihat Kontainer AWS aktif) tanpa harus mengelola server atau cluster instans Amazon EC2 . Dengan AWS Fargate, Anda tidak lagi harus menyediakan, mengonfigurasi, atau menskalakan, kelompok mesin virtual untuk menjalankan kontainer. Anda tidak perlu memilih jenis server, memutuskan kapan akan menskalakan klaster Anda, atau mengoptimalkan paket klaster.

Untuk mempelajari lebih lanjut, lihat Amazon ECS di AWS Fargate.

FAQ Amazon ECS di Fargate di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon ECS di Fargate di akun AMS saya?

Minta akses ke Amazon ECS di Fargate dengan mengirimkan RFC dengan Manajemen AWS | layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_ecs_fargate_console_role` (jika tidak ada peran IAM yang ada disediakan untuk mengaitkan kebijakan ECS),,,`customer_ecs_fargate_events_service_role`, `customer_ecs_task_execution_service_role` dan. `customer_ecs_codedeploy_service_role` `AWSServiceRoleForApplicationAutoScaling_ECSService` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon ECS di Fargate di akun AMS saya?

- Pemantauan dan pencatatan tugas Amazon ECS dianggap sebagai tanggung jawab Anda karena aktivitas tingkat kontainer terjadi di atas hypervisor, dan kemampuan logging dibatasi oleh Amazon ECS di Fargate. Sebagai pengguna Amazon ECS di Fargate, kami menyarankan Anda mengambil langkah-langkah yang diperlukan untuk mengaktifkan login pada tugas Amazon ECS Anda. Untuk informasi selengkapnya, lihat Mengaktifkan Driver Log awslogs untuk Kontainer Anda.
- Keamanan dan perlindungan malware di tingkat kontainer juga dianggap sebagai tanggung jawab Anda. Amazon ECS di Fargate tidak menyertakan Trend Micro atau komponen keamanan jaringan yang telah dikonfigurasi sebelumnya.
- Layanan ini tersedia untuk akun landing zone multi-akun dan single-account landing zone AMS.
- Amazon ECS Service Discovery dibatasi secara default dalam peran yang disediakan sendiri karena izin yang ditingkatkan diperlukan untuk membuat zona host pribadi Route 53. Untuk mengaktifkan Service Discovery pada layanan, kirimkan Manajemen | Lainnya | Lainnya | Perbarui jenis perubahan. Untuk memberikan informasi yang diperlukan untuk mengaktifkan Penemuan Layanan untuk Layanan Amazon ECS Anda, lihat manual Penemuan Layanan.
- AMS saat ini tidak mengelola atau membatasi gambar yang digunakan untuk menyebarkan ke kontainer ke Amazon ECS Fargate. Anda akan dapat menyebarkan gambar dari Amazon ECR, Docker Hub, atau repositori gambar pribadi lainnya. Oleh karena itu, kami menyarankan agar gambar publik atau gambar yang tidak aman tidak digunakan, karena dapat mengakibatkan aktivitas berbahaya di akun.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon ECS di Fargate di akun AMS saya?

- Berikut ini adalah dependensi Amazon ECS di Fargate; namun, tidak ada tindakan tambahan yang diperlukan untuk mengaktifkan layanan ini dengan peran yang Anda sediakan sendiri:

  - CloudWatch log
  - CloudWatch acara
  - CloudWatch alarm
  - CodeDeploy
  - App Mesh
  - Cloud Map
  - Route 53
- Bergantung pada kasus penggunaan Anda, berikut ini adalah sumber daya yang diandalkan Amazon ECS, dan mungkin diperlukan sebelum menggunakan Amazon ECS di Fargate di akun Anda:
  - Grup keamanan untuk digunakan dengan layanan Amazon ECS. Anda dapat menggunakan Deployment | Advanced stack components | Security Group | Create (auto) (ct-3pc215bnwb6p7), atau, jika grup keamanan Anda memerlukan aturan khusus, gunakan Deployment | Advanced stack components | Security Group | Create (review required) (ct-1oxx2g2d7hc90). Catatan: Grup keamanan yang Anda pilih dengan Amazon ECS harus dibuat khusus untuk Amazon ECS tempat layanan atau kluster Amazon ECS berada. Anda dapat mempelajari lebih lanjut di bagian Grup Keamanan di Menyiapkan dengan Amazon ECS dan Keamanan di Amazon Elastic Container Service.
  - Aplikasi load balancer (ALB), network load balancer (NLB), classic load balancer (ELB) untuk load balancing antar tugas.
  - Grup Sasaran untuk ALBs.
  - Sumber daya mesh aplikasi (misalnya, Router Virtual, Layanan Virtual, Node Virtual) untuk diintegrasikan dengan Amazon ECS Cluster Anda.
- Saat ini, tidak ada cara bagi AMS untuk secara otomatis mengurangi risiko yang terkait dengan izin grup keamanan pendukung saat dibuat di luar jenis perubahan AMS standar. Kami menyarankan Anda meminta grup keamanan tertentu untuk digunakan dengan klaster Fargate Anda untuk membatasi kemungkinan menggunakan grup keamanan yang tidak ditunjuk untuk digunakan dengan Amazon ECS.

Gunakan AMS SSP untuk menyediakan Amazon EKS AWS Fargate di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses Amazon EKS pada AWS Fargate kemampuan langsung di akun terkelola AMS Anda. AWS Fargate adalah teknologi yang menyediakan kapasitas komputasi sesuai permintaan dan berukuran tepat untuk kontainer (untuk memahami kontainer, lihat Apa itu Kontainer?). Dengan AWS Fargate, Anda tidak perlu lagi menyediakan, mengonfigurasi, atau menskalakan grup mesin virtual untuk menjalankan kontainer. Dengan begitu, Anda tidak perlu memilih jenis server, memutuskan kapan untuk skala simpul grup Anda, atau mengoptimalkan klaster packing.

Amazon Elastic Kubernetes Service (Amazon EKS) mengintegrasikan AWS Fargate Kubernetes dengan menggunakan kontroler yang AWS dibangun menggunakan model upstream yang dapat diperluas yang disediakan oleh Kubernetes. Pengontrol ini berjalan sebagai bagian dari bidang kontrol Kubernetes yang dikelola Amazon EKS dan bertanggung jawab untuk menjadwalkan pod Kubernetes asli ke Fargate. Pengendali Fargate termasuk penjadwal baru yang berjalan dengan penjadwal Kubernetes default selain beberapa pengendali masuk urusan mutasi dan validasi. Ketika Anda memulai pod yang memenuhi kriteria untuk berjalan di Fargate, pengendali Fargate yang berjalan di klaster akan mengenali, memperbarui, dan menjadwal pod ke Fargate.

Untuk mempelajari lebih lanjut, lihat Amazon EKS di AWS Fargate Sekarang Tersedia Secara Umum dan Panduan Praktik Terbaik Amazon EKS untuk Keamanan (termasuk “Rekomendasi” seperti “Tinjau dan cabut akses anonim yang tidak perlu” dan banyak lagi).

> **Tip**
>
> AMS memiliki tipe perubahan, Deployment | Komponen tumpukan lanjutan | Manajemen Identitas dan Akses (IAM) | Buat penyedia OpenID Connect (ct-30ecvfi3tq4k3), yang dapat Anda gunakan dengan Amazon EKS. Sebagai contoh, lihat Identity and Access Management (IAM) | Membuat Penyedia OpenID Connect.

FAQ Amazon EKS AWS Fargate aktif di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon EKS di Fargate di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda.

- `customer_eks_fargate_console_role`.

  Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.
- Peran layanan ini memberi Amazon EKS di Fargate izin untuk memanggil AWS layanan lain atas nama Anda:
  - `customer_eks_pod_execution_role`
  - `customer_eks_cluster_service_role`

T: Apa batasan untuk menggunakan Amazon EKS di Fargate di akun AMS saya?

- Membuat EC2 nodegroup yang dikelola atau dikelola sendiri tidak didukung di AMS. Jika Anda memiliki persyaratan untuk menggunakan node EC2 pekerja, hubungi AMS Cloud Service Delivery Manager (CSDM) atau Cloud Architect (CA).
- AMS tidak menyertakan Trend Micro atau komponen keamanan jaringan yang telah dikonfigurasi sebelumnya untuk gambar kontainer. Anda diharapkan untuk mengelola layanan pemindaian gambar Anda sendiri untuk mendeteksi gambar kontainer berbahaya sebelum penerapan.
- EKSCTL tidak didukung karena saling ketergantungan. CloudFormation
- Selama pembuatan klaster, Anda memiliki izin untuk menonaktifkan pencatatan bidang kontrol cluster. Untuk informasi selengkapnya, lihat Amazon EKS mengontrol pencatatan pesawat. Kami menyarankan agar Anda mengaktifkan semua pencatatan API, Otentikasi, dan Audit penting pada pembuatan klaster.
- Selama pembuatan klaster, akses titik akhir klaster untuk kluster Amazon EKS secara default menjadi publik; untuk informasi selengkapnya, lihat kontrol akses titik akhir klaster Amazon EKS. Kami menyarankan agar titik akhir Amazon EKS disetel ke pribadi. Jika titik akhir diperlukan untuk akses publik, maka itu adalah praktik terbaik untuk mengaturnya ke publik hanya untuk rentang CIDR tertentu.
- AMS tidak memiliki metode untuk memaksa dan membatasi gambar yang digunakan untuk menyebarkan ke wadah di Amazon EKS Fargate. Anda dapat menerapkan gambar dari Amazon ECR, Docker Hub, atau repositori gambar pribadi lainnya. Oleh karena itu, ada risiko menyebarkan citra publik yang mungkin melakukan aktivitas berbahaya di akun.
- Menerapkan kluster EKS melalui cloud development kit (CDK) atau CloudFormation Ingest tidak didukung di AMS.
- Anda harus membuat grup keamanan yang diperlukan menggunakan ct-3pc215bnwb6p7 Deployment | Komponen tumpukan lanjutan | Grup keamanan | Buat dan referensi dalam file

manifes untuk pembuatan ingress. Ini karena peran tersebut `customer-eks-alb-ingress-controller-role` tidak diizinkan untuk membuat grup keamanan.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon EKS di Fargate di akun AMS saya?

Untuk menggunakan layanan ini, dependensi berikut harus dikonfigurasi:

- Untuk autentikasi terhadap layanan, baik KUBECTL maupun aws-iam-authenticator harus diinstal; untuk informasi selengkapnya, lihat Mengelola otentikasi klaster.
- Kubernetes mengandalkan konsep yang disebut “akun layanan.” Untuk memanfaatkan fungsionalitas akun layanan di dalam klaster kubernetes di EKS, Manajemen | Lainnya | Lainnya | Pembaruan RFC diperlukan dengan masukan berikut:
  - [Diperlukan] Nama Cluster Amazon EKS
  - [Diperlukan] Namespace Amazon EKS Cluster tempat akun layanan (SA) akan digunakan.
  - [Diperlukan] Nama Amazon EKS Cluster SA.
  - [Wajib] Nama Kebijakan IAM dan permissions/document untuk dikaitkan.
  - [Diperlukan] Nama Peran IAM diminta.
  - [Opsional] URL penyedia OpenID Connect. Untuk informasi selengkapnya, lihat
    - Mengaktifkan peran IAM untuk akun layanan di klaster Anda
    - Memperkenalkan peran IAM berbutir halus untuk akun layanan
- Kami menyarankan agar aturan Config dikonfigurasi dan dipantau
  - Titik akhir klaster publik
  - Pencatatan API yang dinonaktifkan

  Anda bertanggung jawab untuk memantau dan memulihkan aturan Config ini.

Jika Anda ingin menerapkan pengontrol ALB Ingress, kirimkan Management | Other | Other Update RFC untuk menyediakan peran IAM yang diperlukan untuk digunakan dengan pod ALB Ingress Controller. Input berikut diperlukan untuk membuat sumber daya IAM untuk dikaitkan dengan ALB Ingress Controller (sertakan ini dengan RFC Anda):

- [Diperlukan] Nama Cluster Amazon EKS
- [Opsional] URL penyedia OpenID Connect

- [Opsional] Namespace Amazon EKS Cluster tempat layanan pengontrol masuk penyeimbang beban aplikasi (ALB) akan diterapkan. [default: kube-sistem]
- [Opsional] Nama akun layanan Amazon EKS Cluster (SA). [default: aws-load-balancer-controller]

Jika Anda ingin mengaktifkan enkripsi rahasia amplop di cluster Anda (yang kami sarankan), berikan kunci KMS yang ingin IDs Anda gunakan, di bidang deskripsi RFC untuk menambahkan layanan (Manajemen | layanan | Layanan yang disediakan sendiri | Tambahkan (AWS ct-1w8z66n899dct). Untuk mempelajari lebih lanjut tentang enkripsi amplop, lihat Amazon EKS menambahkan enkripsi amplop untuk rahasia dengan AWS KMS.

Gunakan AMS SSP untuk menyediakan Amazon EMR di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon EMR secara langsung di akun terkelola AMS Anda. Amazon EMR adalah platform cloud big data terkemuka di industri untuk memproses sejumlah besar data menggunakan alat open source seperti Apache Spark, Apache Hive, Apache, Apache Flink, Apache Hudi, dan Presto HBase. Dengan Amazon EMR, Anda dapat menjalankan analisis skala Petabyte dengan biaya kurang dari setengah biaya solusi lokal tradisional dan lebih dari 3x lebih cepat daripada Apache Spark standar. Untuk pekerjaan jangka pendek, Anda dapat memutar dan memutar cluster dan membayar per detik untuk instance yang digunakan. Untuk beban kerja yang berjalan lama, Anda dapat membuat klaster yang sangat tersedia yang secara otomatis menskalakan untuk memenuhi permintaan.

Anda dapat membuat satu atau beberapa instance klaster EMR Amazon di akun landing zone multi-akun AMS atau akun landing zone akun tunggal untuk mendukung klaster EMR Amazon sementara dan persisten. Anda juga dapat mengaktifkan otentikasi Kerberos untuk mengaktifkan autentikasi pengguna dari domain Active Directory lokal.

Anda dapat memanfaatkan beberapa penyimpanan data dengan kluster EMR Amazon untuk mendukung alat dan pustaka Hadoop khusus kasus penggunaan. Cluster EMR Amazon dapat dibuat menggunakan instans OnDemand atau Spot dan mengonfigurasi penskalaan otomatis untuk mengelola kapasitas dan mengurangi biaya.

File log cluster dapat diarsipkan ke bucket Amazon S3 untuk logging dan debugging. Anda juga dapat mengakses antarmuka web yang dihosting di klaster EMR Amazon untuk mendukung persyaratan administrasi hadoop atau pengalaman buku catatan bagi pelanggan.

Untuk mempelajari lebih lanjut, lihat Amazon EMR.

FAQ Amazon EMR di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon EMR di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:

- `customer_emr_cluster_instance_profile`
- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

Setelah disediakan di akun Anda, Anda harus memasukkan customer_emr_console_role di solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon EMR di akun AMS saya?

Saat membuat Amazon EMR di EC2 cluster dari konsol AWS, kami menyarankan Anda untuk menggunakan opsi Create Cluster — Advanced. Cluster EMR Amazon harus dibuat dengan menambahkan tag dengan Kunci "for-use-with-amazon-emr-managed-policies" dengan Nilai “benar”. Pilih konfigurasi berikut di opsi Keamanan:

- Pilih peran khusus untuk klaster Anda:
  - Peran EMR: customer_emr_cluster_service_role
  - EC2 Profil Contoh: customer_emr_cluster_instance_profile
  - Peran Auto Scaling: customer_emr_cluster_autoscaling_role
- EC2 Grup keamanan:
  - Master: ams-emr-master-security -grup
  - Inti & Tugas: ams-emr-worker-security -grup
  - Akses Layanan: ams-emr-serviceaccess-security -group

T: Apa prasyarat atau dependensi untuk menggunakan Amazon EMR di akun AMS saya?

AMS membuat grup keamanan default untuk master, pekerja, dan node layanan EMR Amazon.

Template peluncuran dan grup keamanan yang akan digunakan dengan cluster EMR Amazon harus memiliki kunci tag "for-use-with-amazon-emr-managed-policies" dengan nilai “true”.

Profil instans cluster Amazon EMR default memungkinkan akses ke sumber daya seperti bucket s3 dan tabel dynamodb dengan namanya yang berisi “emr”. Anda dapat meminta kebijakan IAM tambahan untuk menggunakan sumber daya tambahan apa pun yang akan digunakan dengan Amazon EMR. Sumber daya ARN berikut dapat digunakan dengan pekerjaan EMR Amazon menggunakan customer_emr_cluster_instance_profile:

- arn:aws:dynamodb: *:*:tabel/*emr*
- arn:aws:kinesis: *:*:stream/*emr*
- arn:aws:sns: *:*: *emr*arn:aws:sqs: *:*: *emr*
- arn:aws:sqs: *:*: *emr*
- arn:aws:sqs: *:*:AWS- -* ElasticMapReduce
- arn:aws:sdb: *:*:domain: *emr*
- arn:aws:s3: ::*emr*

Jika otentikasi kerberos diperlukan untuk cluster EMR Amazon:

- Berikan nama ranah yang akan digunakan untuk setiap kluster EMR Amazon kerberisasi dan alamat IP Direktori Aktif di lokasi.
- Persyaratan infrastruktur:

  Multi-Account Landing Zone (MALZ): Kirim RFC untuk membuat akun aplikasi Terkelola baru atau VPC baru di akun aplikasi yang ada.

  Single-Account Landing Zone (SALZ): Kirim RFC untuk membuat subnet baru di VPC Anda.
- Konfigurasikan kepercayaan yang masuk untuk ranah klaster di Active Directory di lokasi.
- Kirim RFC untuk mengonfigurasi zona DNS untuk ranah di AD Terkelola.
- Konfigurasi Realm:

  MALZ: Kirim Manajemen | Lainnya | Lainnya | Perbarui (ct-0xdawir96cy7k) RFC untuk memperbarui opsi VPC DHCP yang disetel untuk menggunakan nama ranah untuk akhiran nama domain.

SALZ: Kirim Manajemen | Lainnya | Lainnya | Perbarui (ct-0xdawir96cy7k) RFC untuk menghasilkan AMI EMR Amazon baru untuk menggunakan ranah khusus untuk akhiran nama domain.

Untuk menyebarkan Amazon EMR studio, `customer_emr_cluster_service_role` peran tersebut memiliki prasyarat untuk bucket Amazon Simple Storage Service. Untuk membuat bucket, gunakan CT otomatis `ct-1a68ck03fn98r` (Deployment | Advanced stack components | S3 storage | Create). Saat Anda menggunakan CT otomatis ini untuk membuat bucket Amazon S3 untuk Amazon EMR, nama bucket harus dimulai dengan awalan. `customer-emr-*` Dan, Anda harus membuat bucket di AWS Wilayah yang sama dengan cluster EMR Amazon.

Gunakan AMS SSP untuk menyediakan Amazon EventBridge di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses EventBridge kapabilitas Amazon secara langsung di akun terkelola AMS Anda. Amazon EventBridge adalah layanan bus acara tanpa server yang memudahkan untuk menghubungkan aplikasi Anda dengan data dari berbagai sumber. EventBridge memberikan aliran data real-time dari aplikasi Anda sendiri, aplikasi Software-as-a-Service (SaaS), AWS dan layanan dan rute data tersebut ke target seperti. AWS Lambda Anda dapat mengatur aturan perutean untuk menentukan ke mana harus mengirim data Anda untuk membangun arsitektur aplikasi yang bereaksi secara real time ke semua sumber data Anda. EventBridge memungkinkan Anda membangun arsitektur berbasis peristiwa, yang digabungkan dan didistribusikan secara longgar.

Untuk mempelajari lebih lanjut, lihat Amazon EventBridge.

EventBridge di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke EventBridge akun AMS saya?

Meminta akses EventBridge dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_eventbridge_role` dan. `customer_eventbridge_scheduler_execution_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

Peran eksekusi, `customer_eventbridge_scheduler_execution_role` adalah peran IAM yang diasumsikan oleh EventBridge Scheduler untuk berinteraksi dengan orang lain Layanan AWS

atas nama Anda. Kebijakan izin yang dilampirkan pada peran ini memberikan akses EventBridge Scheduler untuk memanggil target.

> **Note**
>
> Secara default, EventBridge Scheduler menggunakan kunci yang AWS dimiliki EventBridge untuk mengenkripsi data. Untuk menggunakan kunci yang dikelola pelanggan EventBridge untuk mengenkripsi data, kirimkan RFC menggunakan Layanan Manajemen | AWS | Layanan yang disediakan sendiri | Tambahkan (perlu ditinjau) jenis perubahan (ct-3qe6io8t6jtny) untuk penyediaan layanan.

T: Apa batasan penggunaan EventBridge di akun AMS saya?

Anda harus mengirimkan AMS RFCs dan membuat sumber daya berikut: Peran layanan untuk memicu pekerjaan batch, antrean SQS,, CodeBuild CodePipeline, dan perintah SSM.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? EventBridge

Anda harus meminta peran EventBridge layanan dengan RFC menggunakan Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat entitas atau kebijakan (perlu ditinjau) mengubah jenis (ct-3dpd8mdd9jn1r) sebelum menggunakan untuk memicu EventBridge sumber daya lain, seperti, Lambda, Amazon SNS, Amazon SQS, atau Amazon Sumber daya AWS log. AWS Batch CloudWatch Tentukan layanan yang akan dipanggil saat meminta peran layanan Anda. Untuk mempelajari tentang izin yang diperlukan untuk memanggil target, lihat Menggunakan Kebijakan Berbasis Sumber Daya untuk. EventBridge

EventBridge terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS dalam EventBridge. CloudTrail harus diaktifkan dan diizinkan untuk menyimpan file log ke ember S3. Catatan: Semua akun AMS telah CloudTrail diaktifkan, jadi tidak diperlukan tindakan.

T: Peran customer_eventbridge_scheduler_execution_role memiliki prasyarat untuk Key (opsional, jika digunakan untuk enkripsi). AWS Key Management Service Bagaimana cara mengadopsi AWS KMS CMKs enkripsi data saat istirahat/transit?

Secara default, EventBridge Scheduler mengenkripsi metadata peristiwa dan data pesan yang disimpan di bawah kunci yang AWS dimiliki (enkripsi saat istirahat). EventBridge Scheduler juga

mengenkripsi data yang melewati antara EventBridge Scheduler dan layanan lainnya menggunakan Transport Layer Security (TLS) (enkripsi dalam perjalanan).

Jika kasus penggunaan khusus Anda mengharuskan Anda mengontrol dan mengaudit kunci enkripsi yang melindungi data Anda di EventBridge Scheduler, Anda dapat menggunakan kunci yang dikelola pelanggan.

Anda harus meminta RFC menggunakan Management | Layanan AWS | Self-provisioned service | Tambahkan (perlu ditinjau) jenis perubahan sebelum menggunakan Amazon EventBridge untuk memasukkan izin. AWS KMS

Gunakan AMS SSP untuk menyediakan Amazon Forecast di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Forecast (Forecast) secara langsung di akun terkelola AMS Anda. Amazon Forecast adalah layanan yang dikelola sepenuhnya yang menggunakan pembelajaran mesin untuk memberikan perkiraan yang sangat akurat.

> **Note**
>
> AWS telah menutup akses pelanggan baru ke Amazon Forecast, efektif 29 Juli 2024. Amazon Forecast pelanggan lama dapat terus menggunakan layanan seperti biasa. AWS terus berinvestasi dalam peningkatan keamanan, ketersediaan, dan kinerja untuk Amazon Forecast, tetapi AWS tidak berencana untuk memperkenalkan fitur baru.
> Jika Anda ingin menggunakan Amazon Forecast, hubungi CSDM Anda sehingga mereka dapat memandu Anda lebih lanjut mengenai cara Transisi penggunaan Amazon Forecast Anda ke Amazon Canvas. SageMaker

Berdasarkan teknologi yang sama yang digunakan di Amazon.com, Forecast menggunakan pembelajaran mesin untuk menggabungkan data deret waktu dengan variabel tambahan untuk membangun prakiraan. Forecast tidak memerlukan pengalaman pembelajaran mesin untuk memulai. Anda hanya perlu memberikan data historis, ditambah data tambahan apa pun yang Anda yakini dapat memengaruhi perkiraan Anda. Misalnya, permintaan untuk warna kemeja tertentu dapat berubah dengan musim dan lokasi toko. Hubungan yang kompleks ini sulit ditentukan sendiri, tetapi pembelajaran mesin sangat cocok untuk mengenalinya. Setelah Anda memberikan data

Anda, Forecast akan secara otomatis memeriksanya, mengidentifikasi apa yang bermakna, dan menghasilkan model peramalan yang mampu membuat prediksi yang hingga 50% lebih akurat daripada melihat data deret waktu saja.

Untuk mempelajari lebih lanjut, lihat Amazon Forecast.

FAQ Amazon Forecast di AWS Managed Services

T: Bagaimana cara meminta akses ke Forecast di akun AMS saya?

Minta akses ke AWS Firewall Manager dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_forecast_admin_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan Forecast di akun AMS saya?

Akses bucket S3 default hanya memungkinkan Anda mengakses bucket dengan pola penamaan 'customer-forecast-*'. Jika Anda memiliki konvensi penamaan sendiri untuk bucket data, diskusikan penamaan bucket dan penyiapan akses terkait dengan Cloud Architect (CA) Anda. Misalnya:

- Anda dapat menentukan peran layanan Amazon Forecast spesifik Anda dengan penamaan seperti 'AmazonForecast- ExecutionRole -*' dan terkait akses bucket S3 yang tepat.
  Lihat peran Layanan - AmazonForecast-ExecutionRole-Admin dan kebijakan IAM - customer_forecast_default_s3_access_policy, di konsol IAM.
- Anda mungkin perlu mengaitkan akses bucket S3 terkait ke peran federasi IAM. Lihat kebijakan IAM - customer_forecast_default_s3_access_policy, di konsol IAM.

T: Apa prasyarat atau dependensi untuk menggunakan Forecast di akun AMS saya?

- Bucket Amazon S3 yang tepat harus dibuat sebelum menggunakan Forecast. Terutama, akses bucket S3 default adalah dengan pola penamaan 'customer-forecast-*'
- Jika Anda ingin menggunakan pola penamaan pada bucket S3 selain 'customer-forecast-* ', Anda harus membuat peran layanan baru dengan izin akses S3 di bucket:
  1. Peran layanan baru yang akan dibuat dengan penamaan 'AmazonForecast- ExecutionRole - {suffix}'.
  2. Kebijakan IAM baru yang akan dibuat yang mirip dengan customer_forecast_default_s3_access_policy dan dikaitkan dengan peran layanan baru dan peran admin federasi terkait (misalnya 'customer_forecast_admin_role')

T: Bagaimana cara meningkatkan keamanan data saat menggunakan Amazon Forecast?

- Untuk enkripsi data saat istirahat, Anda dapat menggunakan AWS KMS untuk menyediakan CMK yang dikelola pelanggan untuk melindungi penyimpanan data di layanan Amazon S3:
  - Aktifkan enkripsi default pada bucket dengan kunci penyediaan dan siapkan kebijakan bucket untuk menerima enkripsi AWS KMS data sambil meletakkan data.
  - Aktifkan peran layanan Amazon Forecast 'AmazonForecast- ExecutionRole -*' dan peran admin federasi (misalnya' customer_forecast_admin_role ') sebagai pengguna kunci. AWS KMS
- Untuk enkripsi data dalam perjalanan, Anda dapat mengatur protokol HTTPS, yang diperlukan saat mentransfer objek pada kebijakan bucket Amazon S3.
- Pembatasan lebih lanjut pada kontrol akses, aktifkan kebijakan bucket untuk akses yang disetujui untuk peran layanan Amazon Forecast 'AmazonForecast- ExecutionRole -*' dan peran admin (misalnya' customer_forecast_admin_role ').

T: Apa praktik terbaik saat menggunakan Amazon Forecast?

- Anda harus memiliki pemahaman yang baik tentang praktik klasifikasi data Anda dan memetakan kebutuhan keamanan data terkait saat menggunakan bucket S3 dengan Amazon Forecast.
- Untuk konfigurasi bucket Amazon S3, kami sangat menyarankan Anda untuk mengaktifkan penegakan HTTPS dalam kebijakan bucket S3 Anda.
- Anda harus mengetahui peran admin 'customer_forecast_admin_role' mendukung akses permisif (Get/Delete/Putobjek S3) di bucket Amazon S3 dengan penamaan 'customer-forecast-*'. CATATAN: Jika Anda memerlukan kontrol akses berbutir halus untuk beberapa tim, ikuti praktik berikut:
  - Tentukan identitas IAM akses berbasis tim Anda (peran/pengguna) dengan akses hak istimewa paling sedikit ke bucket Amazon S3 terkait.
  - Buat AWS KMS CMKs hibah team/project berbasis akses yang tepat ke identitas IAM yang sesuai. (akses pengguna dan 'AmazonForecast- ExecutionRole - {team/project}'.
  - Siapkan enkripsi default bucket S3 dengan yang dibuat AWS KMS CMKs.
  - Terapkan lalu lintas API S3 dengan protokol HTTPS pada kebijakan bucket S3.
  - Menerapkan konfigurasi bucket S3 untuk akses yang disetujui untuk identitas IAM terkait (akses pengguna dan 'AmazonForecast- ExecutionRole - {team/project}' ke bucket.
- Jika Anda ingin menggunakan 'customer_forecast_admin_role' untuk tujuan umum, pertimbangkan poin yang tercantum sebelumnya untuk melindungi bucket S3.

T: Di mana informasi kepatuhan tentang Amazon Forecast?

Lihat AWS layanan Program Kepatuhan.

Gunakan AMS SSP untuk menyediakan Amazon FSx di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses FSx kapabilitas Amazon secara langsung di akun terkelola AMS Anda. Amazon FSx menyediakan sistem file pihak ketiga yang dikelola sepenuhnya. Amazon FSx memberi Anda kompatibilitas asli sistem file pihak ketiga dengan set fitur untuk beban kerja seperti penyimpanan berbasis Windows, komputasi kinerja tinggi (HPC), pembelajaran mesin, dan otomatisasi desain elektronik (EDA). Amazon FSx mengotomatiskan tugas administrasi yang memakan waktu seperti penyediaan perangkat keras, konfigurasi perangkat lunak, penambalan, dan pencadangan. Amazon FSx mengintegrasikan sistem file dengan AWS layanan cloud-native, membuatnya lebih berguna untuk serangkaian beban kerja yang lebih luas.

Amazon FSx memberi Anda dua sistem file untuk dipilih: Amazon untuk Windows File Server FSx untuk aplikasi berbasis Windows dan Amazon untuk Lustre FSx untuk beban kerja intensif komputasi. Untuk mempelajari lebih lanjut, lihat Amazon FSx.

FAQ Amazon FSx di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon FSx di akun AMS saya?

Meminta akses ke Amazon FSx dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_fsx_admin_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon FSx di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh dari layanan ini tersedia.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon FSx di akun AMS saya?

Tidak ada prasyarat. Namun, untuk konfigurasi lanjutan seperti Multi-AZ, Anda harus menginstal dan mengelola layanan Replikasi DFS dan DFS Namespaces. Untuk informasi selengkapnya, lihat Menerapkan Sistem File Multi-AZ.

T: Bagaimana cara mengintegrasikan sistem FSx file Amazon saya dengan iklan terkelola landing zone multi-akun saya?

Saat membuat sistem FSx file Amazon, Anda dapat menentukan MALZ Managed AD sebagai 'Direktori Aktif Microsoft AWS Terkelola' untuk Otentikasi Windows. Untuk informasi selengkapnya lihat, Menggunakan Amazon FSx dengan AWS Directory Service Microsoft Active Directory

Anda juga harus membagikan iklan Terkelola ke akun aplikasi terlebih dahulu. Lakukan ini dengan mengirimkan RFC dengan Management | Directory Service | Directory | Share directory change type (ct-369odosk0pd9w).

T: Pengguna mana yang termasuk dalam grup AWS Delegated FSx Administrators?

Hanya administrator server file TI. Grup ini memiliki hak akses penuh di semua berbagi file.

T: Haruskah saya menggunakan file share default, share, yang dibuat saat FSx sistem disediakan?

Tidak, kami tidak menyarankan menggunakan berbagi file default, bagikan, seperti yang disediakan. Ini memberikan Akses Penuh ke Semua Orang, yang melanggar prinsip hak istimewa paling sedikit. Sebagai gantinya, buat berbagi file khusus yang lebih kecil yang sesuai dengan kebutuhan bisnis Anda.

T: Bagaimana cara membuat pembagian file khusus untuk organisasi tertentu dalam bisnis saya?

Lihat Berbagi File untuk petunjuk cara membuat berbagi file kustom. Batasi akses pada setiap berbagi file menggunakan prinsip hak istimewa paling sedikit.

Gunakan AMS SSP untuk menyediakan Amazon FSx untuk OpenZFS di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses Amazon FSx untuk kemampuan OpenZFS secara langsung di akun terkelola AMS Anda. FSx untuk OpenZFS adalah layanan penyimpanan file yang dikelola sepenuhnya yang memudahkan pemindahan data yang berada di ZFS lokal atau server file berbasis Linux lainnya ke AWS tanpa mengubah kode aplikasi atau cara Anda mengelola data. Ini menawarkan penyimpanan file yang sangat andal, terukur, berkinerja, dan kaya fitur yang dibangun di atas sistem file OpenZFS open-source, menyediakan fitur dan kemampuan sistem file OpenZFS yang sudah dikenal dengan kelincahan, skalabilitas, dan kesederhanaan layanan yang dikelola sepenuhnya. AWS Untuk pengembang yang membangun aplikasi cloud-native, ia menawarkan penyimpanan sederhana dan berkinerja tinggi dengan kemampuan yang kaya untuk bekerja dengan data.

FSx untuk sistem file OpenZFS dapat diakses secara luas dari Linux, Windows, dan instance komputasi macOS dan kontainer menggunakan protokol NFS standar industri (v3, v4.0, v4.1, v4.2).

Didukung oleh prosesor AWS Graviton dan teknologi AWS disk dan jaringan terbaru (termasuk jaringan Datagram AWS Scalable Reliable dan sistem AWS Nitro), FSx untuk OpenZFS memberikan hingga 1 juta IOPS dengan latensi ratusan mikrodetik. Dengan dukungan lengkap untuk fitur OpenZFS seperti point-in-time snapshot instan dan kloning data, FSx untuk OpenZFS memudahkan Anda mengganti server file lokal Anda dengan AWS penyimpanan yang menyediakan kemampuan sistem file yang sudah dikenal dan menghilangkan kebutuhan untuk melakukan kualifikasi panjang dan mengubah atau merancang ulang aplikasi atau alat yang ada. Dan, dengan menggabungkan kekuatan kemampuan manajemen data OpenZFS dengan kinerja tinggi dan efisiensi biaya dari teknologi AWS terbaru, FSx untuk OpenZFS memungkinkan Anda membangun dan menjalankan aplikasi intensif data berkinerja tinggi.

Sebagai layanan yang dikelola sepenuhnya, FSx untuk OpenZFS memudahkan peluncuran, menjalankan, dan menskalakan sistem file yang dikelola sepenuhnya AWS yang menggantikan server file yang Anda jalankan di tempat sambil membantu memberikan kelincahan yang lebih baik dan biaya yang lebih rendah. Dengan FSx untuk OpenZFS, Anda tidak perlu lagi khawatir tentang pengaturan dan penyediaan server file dan volume penyimpanan, mereplikasi data, menginstal dan menambal perangkat lunak server file, mendeteksi dan mengatasi kegagalan perangkat keras, dan melakukan backup secara manual. Ini juga menyediakan integrasi yang kaya dengan AWS layanan lain, seperti AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS), Amazon CloudWatch, dan AWS CloudTrail.

Amazon FSx memberi Anda dua sistem file untuk dipilih: Amazon untuk Windows File Server FSx untuk aplikasi berbasis Windows dan Amazon untuk Lustre FSx untuk beban kerja intensif komputasi. Untuk mempelajari lebih lanjut, lihat Amazon FSx.

FAQ Amazon FSx untuk OpenZFS di AWS Managed Services

T: Bagaimana cara meminta akses untuk digunakan FSx untuk OpenZFS di akun AMS saya?

Minta akses ke Amazon FSx OpenZFS dengan mengirimkan RFC dengan Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_fsx_ontap_admin_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan FSx OpenZFS di akun AMS saya?

Mengganti grup keamanan pada antarmuka jaringan FSx elastis Amazon (ENIs) mengharuskan Anda mengirimkan Manajemen | Lainnya | Lainnya | Pembaruan RFCs karena grup keamanan merupakan perimeter penting untuk lingkungan AMS. Itu satu-satunya batasan.

T: Apa prasyarat atau dependensi yang digunakan untuk OpenZFS di akun AMS saya FSx ?

Tidak ada prasyarat. Namun, Anda harus Gunakan AMS SSP untuk menyediakan Amazon FSx di akun AMS Anda menginstal.

Gunakan AMS SSP untuk menyediakan Amazon FSx untuk NetApp ONTAP di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses Amazon FSx untuk kemampuan NetApp ONTAP secara langsung di akun terkelola AMS Anda. Amazon FSx untuk NetApp ONTAP adalah layanan yang dikelola sepenuhnya yang menyediakan penyimpanan file yang sangat andal, terukur, berkinerja, dan kaya fitur yang dibangun di atas NetApp sistem file ONTAP yang populer. Ini menyediakan fitur, kinerja, kemampuan, dan sistem NetApp file APIs yang sudah dikenal dengan kelincahan, skalabilitas, dan kesederhanaan yang dikelola sepenuhnya. Layanan AWS

Amazon FSx untuk NetApp ONTAP menyediakan penyimpanan file bersama yang kaya fitur, cepat, dan fleksibel yang dapat diakses secara luas dari instans komputasi Linux, Windows, dan macOS yang berjalan di dalam atau di tempat. AWS FSx untuk ONTAP menawarkan penyimpanan SSD berkinerja tinggi dengan latensi sub-milidetik, dan membuatnya cepat dan mudah untuk mengelola data Anda dengan memungkinkan Anda memotret, mengkloning, dan mereplikasi file Anda dengan mengklik tombol. Ini juga secara otomatis meningkatkan data Anda ke penyimpanan elastis berbiaya lebih rendah, menghilangkan kebutuhan untuk menyediakan atau mengelola kapasitas dan memungkinkan Anda mencapai tingkat kinerja SSD untuk beban kerja Anda sambil hanya membayar penyimpanan SSD untuk sebagian kecil data Anda. Ini menyediakan penyimpanan yang sangat tersedia dan tahan lama dengan cadangan yang dikelola sepenuhnya dan dukungan untuk pemulihan bencana lintas wilayah, dan mendukung keamanan data populer dan aplikasi anti-virus yang membuatnya lebih mudah untuk melindungi dan mengamankan data Anda. Bagi pelanggan yang menggunakan NetApp ONTAP lokal, FSx ONTAP adalah solusi ideal untuk memigrasi, mencadangkan, atau mem-burst aplikasi berbasis file Anda dari lokal ke lokasi AWS tanpa perlu mengubah kode aplikasi atau cara Anda mengelola data.

Sebagai layanan yang dikelola sepenuhnya, Amazon FSx untuk NetApp ONTAP memudahkan peluncuran dan skala penyimpanan file bersama yang andal, berkinerja, dan aman di cloud. Dengan Amazon FSx untuk NetApp ONTAP, Anda tidak perlu lagi khawatir tentang pengaturan dan penyediaan server file dan volume penyimpanan, mereplikasi data, menginstal dan menambal perangkat lunak server file, mendeteksi dan mengatasi kegagalan perangkat keras, mengelola failover dan failback, dan melakukan backup secara manual. Ini juga menyediakan integrasi yang

kaya dengan yang lain Layanan AWS, seperti AWS Identity and Access Management, Amazon WorkSpaces, AWS Key Management Service, dan AWS CloudTrail.

Amazon FSx memberi Anda dua sistem file untuk dipilih: Amazon untuk Windows File Server FSx untuk aplikasi berbasis Windows dan Amazon untuk Lustre FSx untuk beban kerja intensif komputasi. Untuk mempelajari lebih lanjut, lihat Amazon FSx.

FAQ Amazon FSx untuk NetApp ONTAP di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon FSx untuk NetApp ONTAP di akun AMS saya?

Minta akses ke Amazon FSx untuk NetApp ONTAP dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_fsx_ontap_admin_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan Amazon FSx untuk NetApp ONTAP di akun AMS saya?

Mengganti grup keamanan di Amazon FSx untuk antarmuka jaringan elastis NetApp ONTAP (ENIs) mengharuskan Anda mengirimkan Manajemen | Lainnya | Lainnya | Pembaruan RFCs karena grup keamanan merupakan perimeter penting untuk lingkungan AMS. Itu satu-satunya batasan.

T: Apa prasyarat atau dependensi untuk menggunakan FSx Amazon NetApp untuk ONTAP di akun AMS saya?

Tidak ada prasyarat. Namun, Anda harus Gunakan AMS SSP untuk menyediakan Amazon FSx di akun AMS Anda menginstal.

Gunakan AMS SSP untuk menyediakan Amazon Inspector Classic di akun AMS Anda

> **Note**
>
> Pemberitahuan akhir dukungan: Pada 20 Mei 2026, AWS akan mengakhiri dukungan untuk Amazon Inspector Classic. Setelah 20 Mei 2026, Anda tidak akan lagi dapat mengakses konsol Amazon Inspector Classic atau sumber daya Amazon Inspector Classic. Amazon Inspector Classic tidak akan lagi tersedia untuk akun baru, dan akun yang belum menyelesaikan penilaian dalam enam bulan terakhir. Untuk semua akun lain, akses akan tetap berlaku hingga 20 Mei 2026, setelah itu Anda tidak lagi dapat mengakses konsol

Amazon Inspector Classic atau sumber daya Amazon Inspector Classic. Untuk informasi selengkapnya, lihat bagian akhir dukungan Amazon Inspector Classic.

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Inspector Classic secara langsung di akun terkelola AMS Anda. Amazon Inspector Classic adalah layanan penilaian keamanan otomatis yang membantu meningkatkan keamanan dan kepatuhan aplikasi yang digunakan. AWS Amazon Inspector Classic secara otomatis menilai aplikasi untuk eksposur, kerentanan, dan penyimpangan dari praktik terbaik. Setelah melakukan penilaian, Amazon Inspector Classic menghasilkan daftar rinci temuan keamanan yang diprioritaskan berdasarkan tingkat keparahan. Temuan ini dapat ditinjau secara langsung atau sebagai bagian dari laporan penilaian terperinci, yang tersedia melalui konsol Amazon Inspector Classic atau API. Untuk mempelajari lebih lanjut, lihat Amazon Inspector Classic.

FAQ Amazon Inspector di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon Inspector Classic di akun AMS saya?

Minta akses ke Amazon Inspector Classic dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran `customer_inspector_admin_role` IAM ke akun Anda. Peran tersebut mencakup AmazonInspectorFullAccess kebijakan AWS yang dikelola. Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Inspector Classic di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Inspector Classic tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Inspector Classic di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Amazon Inspector Classic di akun AMS Anda.

Gunakan Amazon Inspector baru di AMS

Anda sekarang dapat menggunakan Amazon Inspector baru di akun AMS Anda.

Untuk Amazon Inspector Classic, `customer-inspector-admin-role-ssm-inspector-agent-policy` dan diperlukan`AmazonInspectorFullAccess`. Namun, telah ada pembaruan untuk peran SSP`customer-inspector-admin-role`, yang sekarang mencakup tambahan.

`policyAmazonInspector2FullAccess` Kebijakan baru ini memungkinkan izin API untuk Amazon Inspector versi baru.

Gunakan AMS SSP untuk menyediakan Amazon Kendra di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Kendra secara langsung di akun terkelola AMS Anda. Amazon Kendra adalah layanan pencarian cerdas yang menggunakan pemrosesan bahasa alami dan algoritme pembelajaran mesin canggih untuk mengembalikan jawaban spesifik atas pertanyaan pencarian dari data Anda. Tidak seperti pencarian berbasis kata kunci tradisional, Amazon Kendra menggunakan kemampuan pemahaman semantik dan kontekstualnya untuk menentukan apakah dokumen relevan dengan kueri penelusuran. Amazon Kendra mengembalikan jawaban spesifik untuk pertanyaan, sehingga pengalaman Anda hampir berinteraksi dengan ahli manusia. Amazon Kendra sangat skalabel, mampu memenuhi tuntutan kinerja, terintegrasi erat dengan AWS layanan lain seperti Amazon S3 dan Amazon Lex, dan menawarkan keamanan tingkat perusahaan. Untuk mempelajari lebih lanjut, lihat Amazon Kendra;.

FAQ Amazon Kendra di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon Kendra di akun AMS saya?

Untuk meminta akses ke Amazon Inspector Classic, kirimkan RFC dengan Management | AWS service | Self-provisioned service | Tambahkan (ct-3qe6io8t6jtny) jenis perubahan. RFC ini menyediakan peran `customer_kendra_console_role` IAM ke akun Anda. Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Kendra di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Kendra tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Kendra di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk memulai dengan Amazon Kendra. Namun, tergantung pada kasus penggunaan spesifik Anda, Anda mungkin memerlukan akses ke AWS layanan lain.

Gunakan SSP AMS untuk menyediakan Amazon Kinesis Data Streams di akun AMS

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Kinesis Data Streams (KDS) secara langsung di akun terkelola AMS Anda. Amazon Kinesis Data Streams adalah layanan streaming data real-time yang sangat skalabel, dan tahan lama. KDS dapat terus

menangkap gigabyte data per detik dari ratusan ribu sumber seperti clickstream situs web, aliran peristiwa database, transaksi keuangan, umpan media sosial, log TI, dan peristiwa pelacakan lokasi. Data yang dikumpulkan tersedia dalam milidetik untuk memungkinkan kasus penggunaan analitik real-time seperti dasbor waktu nyata, deteksi anomali waktu nyata, harga dinamis, dan banyak lagi. Untuk mempelajari selengkapnya, lihat Amazon Kinesis Data Streams.

FAQ Kinesis Data Streams di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Kinesis Data Streams di akun AMS saya?

Meminta akses ke Amazon Kinesis Data Streams dengan mengirimkan RFC dengan Manajemen | Layanan AWS | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_kinesis_data_streaming_user_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Kinesis Data Streams di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Kinesis Data Streams tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Kinesis Data Streams di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Amazon Kinesis Data Streams di akun AMS Anda.

Gunakan AMS SSP untuk menyediakan Amazon Kinesis Video Streams di akun AMS

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Kinesis Video Streams (KVS) secara langsung di akun terkelola AMS Anda. Amazon Kinesis Video Streams membantu Anda mengalirkan video dengan aman dari AWS perangkat yang terhubung ke analitik, pembelajaran mesin (ML), pemutaran, dan pemrosesan lainnya. Kinesis Video Streams secara otomatis menyediakan, dan menskalakan secara elastis, semua infrastruktur yang diperlukan untuk menyerap data video streaming dari jutaan perangkat. Ini juga tahan lama menyimpan, mengenkripsi, dan mengindeks data video di aliran Anda, dan memungkinkan Anda untuk mengakses data Anda melalui. easy-to-use APIs Kinesis Video Streams memungkinkan Anda memutar video untuk dilihat langsung dan sesuai permintaan, dan dengan cepat membangun aplikasi yang memanfaatkan

visi komputer dan analitik video melalui integrasi dengan Amazon Rekognition Video, dan pustaka untuk kerangka kerja HTML seperti Apache,, dan OpenCV. MxNet TensorFlow Untuk mempelajari selengkapnya, lihat Amazon Kinesis Video Streams.

FAQ Amazon Kinesis Video Streams di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Kinesis Video Streams di akun AMS saya?

Minta akses ke Amazon Kinesis Video Streams dengan mengirimkan RFC dengan AWS Manajemen | layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_kinesis_video_streaming_user_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Kinesis Video Streams di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Amazon Kinesis Video Streams tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Kinesis Video Streams di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Amazon Kinesis Video Streams di akun AMS Anda.

Gunakan AMS SSP untuk menyediakan Amazon Lex di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Lex secara langsung di akun terkelola AMS Anda. Amazon Lex adalah layanan untuk membangun antarmuka percakapan ke dalam aplikasi apa pun menggunakan suara dan teks. Amazon Lex menyediakan fungsionalitas pembelajaran mendalam lanjutan dari pengenalan suara otomatis (ASR) untuk mengonversi ucapan menjadi teks, dan pemahaman bahasa alami (NLU) untuk mengenali maksud teks, untuk memungkinkan Anda membangun aplikasi dengan pengalaman pengguna yang sangat menarik dan interaksi percakapan yang hidup. Dengan Amazon Lex, teknologi pembelajaran mendalam yang sama yang mendukung Amazon Alexa sekarang tersedia untuk pengembang mana pun, memungkinkan Anda untuk dengan cepat dan mudah membangun bahasa alami, bot percakapan, atau chatbot percakapan yang canggih dan mudah. Untuk mempelajari lebih lanjut, lihat Amazon Lex.

FAQ Amazon Lex di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Lex di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_lex_author_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Lex di akun AMS saya?

Integrasi Amazon Lex dengan Lambda terbatas pada fungsi Lambda tanpa awalan “AMS-”, untuk mencegah modifikasi apa pun pada infrastruktur AMS.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Lex di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Amazon Lex di akun AMS Anda.

Gunakan AMS SSP untuk menyediakan Amazon MQ di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon MQ secara langsung di akun terkelola AMS Anda. Amazon MQ adalah layanan broker pesan terkelola untuk Apache ActiveMQ yang membantu Anda mengatur dan mengoperasikan broker pesan di cloud. Broker pesan memungkinkan sistem perangkat lunak yang berbeda, sering menggunakan bahasa pemrograman yang berbeda dan pada platform yang berbeda, untuk berkomunikasi dan bertukar informasi. Amazon MQ mengurangi beban operasional Anda dengan mengelola penyediaan, penyiapan, dan pemeliharaan ActiveMQ, broker pesan sumber terbuka yang populer. Menghubungkan aplikasi Anda saat ini ke Amazon MQ menggunakan standar industri APIs dan protokol untuk pengiriman pesan, termasuk JMS, NMS, AMQP, STOMP, MQTT, dan. WebSocket Menggunakan standar berarti, dalam banyak kasus, tidak perlu menulis ulang kode pesan apa pun saat Anda bermigrasi. AWS Untuk mempelajari lebih lanjut, lihat Apa itu Amazon MQ?

FAQ Amazon MQ di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon MQ di akun AMS saya?

Pemanfaatan Amazon MQ di akun AMS Anda adalah proses dua langkah:

1. Menyediakan Broker Amazon MQ. Untuk melakukan ini, kirimkan Template CFN, dengan Broker MQ Amazon disertakan, melalui RFC dengan Deployment | Ingestion | Stack CloudFormation from Template | Buat jenis perubahan (ct-36cn2avfrrj9v), atau kirimkan RFC dengan Manajemen | Lainnya | Lainnya | Buat jenis perubahan (ct-1e1xtak34nx76) mengubah jenis yang meminta Amazon MQ Broker disediakan di akun Anda.
2. Akses konsol Amazon MQ. Setelah Amazon MQ Broker disediakan, dapatkan akses ke konsol Amazon MQ dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_mq_console_role`

Setelah peran disediakan di akun Anda, Anda harus memasukkannya ke dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon MQ di akun AMS saya?

Fungsionalitas penuh Amazon MQ tersedia di akun AMS Anda; namun, penyediaan Broker MQ Amazon tidak tersedia melalui kebijakan karena izin tinggi yang diperlukan. Lihat di atas untuk detail tentang cara menyediakan broker Amazon MQ di akun Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon MQ di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Amazon MQ di akun AMS Anda.

Menggunakan AMS SSP untuk menyediakan Amazon Managed Service untuk Apache Flink di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses Amazon Managed Service untuk kemampuan Apache Flink secara langsung di akun terkelola AMS Anda. Layanan Terkelola untuk Apache Flink adalah cara termudah untuk menganalisis data streaming, mendapatkan wawasan yang dapat ditindaklanjuti, dan menanggapi kebutuhan bisnis dan pelanggan Anda secara real time. Amazon Managed Service untuk Apache Flink mengurangi kompleksitas membangun, mengelola, dan mengintegrasikan aplikasi streaming dengan layanan lain. AWS Pengguna SQL dapat dengan mudah menanyakan data streaming atau membangun seluruh aplikasi streaming menggunakan templat dan editor SQL interaktif. Pengembang Java dapat dengan cepat membangun aplikasi streaming canggih menggunakan pustaka dan AWS integrasi Java open source untuk mengubah dan menganalisis data secara real time. Amazon Managed Service untuk Apache Flink menangani semua yang diperlukan untuk menjalankan aplikasi real-time Anda secara terus menerus dan menskalakan secara otomatis agar sesuai dengan volume dan throughput data masuk Anda. Dengan Amazon Managed Service untuk Apache Flink, Anda hanya membayar sumber daya

yang digunakan aplikasi streaming Anda. Tidak ada biaya minimum atau biaya pengaturan. Untuk mempelajari selengkapnya, lihat Amazon Managed Service untuk Apache Flink.

Layanan Terkelola untuk Apache Flink di AWS Managed Services FAQ

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Managed Service untuk Apache Flink di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_kinesis_analytics_application_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Managed Service untuk Apache Flink di akun AMS saya?

- Konfigurasi terbatas pada sumber daya tanpa awalan 'AMS-' atau 'MC-' untuk mencegah modifikasi apa pun pada infrastruktur AMS.
- Izin untuk menghapus atau membuat Kinesis Data Streams atau Firehose baru telah dihapus dari kebijakan. Kami memiliki kebijakan lain yang memungkinkan itu.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Kinesis Data Streams di akun AMS saya?

Ada beberapa dependensi:

- Amazon Managed Service untuk Apache Flink mengharuskan Kinesis Data Streams atau Firehose harus dibuat sebelum mengonfigurasi aplikasi dengan Managed Service for Apache Flink.
- Izin kebijakan berbasis sumber daya harus menunjukkan sumber data input tertentu.

Gunakan AMS SSP untuk menyediakan Amazon Managed Streaming for Apache Kafka di akun AMS

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon Managed Streaming for Apache Kafka (Amazon MSK) secara langsung di akun terkelola AMS Anda. Amazon Managed Streaming for Apache Kafka adalah layanan data streaming yang AWS

dikelola sepenuhnya sehingga memudahkan Anda untuk membangun dan menjalankan aplikasi yang menggunakan Apache Kafka untuk memproses data streaming tanpa perlu menjadi ahli dalam mengoperasikan cluster Apache Kafka. Amazon MSK mengelola penyediaan, konfigurasi, dan pemeliharaan cluster Apache Kafka dan node Apache untuk Anda. ZooKeeper Amazon MSK juga menunjukkan metrik kinerja utama Apache Kafka di Konsol. AWS

Amazon MSK menyediakan beberapa tingkat keamanan untuk kluster Apache Kafka Anda, termasuk isolasi jaringan VPC, AWS IAM untuk otorisasi API bidang kontrol, enkripsi saat istirahat, enkripsi TLS dalam perjalanan, otentikasi sertifikat berbasis TLS, otentikasi diamankan oleh. SASL/SCRAM AWS Secrets Manager Untuk mempelajari lebih lanjut, lihat Amazon MSK.

FAQ Amazon MSK di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon MSK di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini memberikan kebijakan dan peran IAM berikut ke akun Anda:

- `customer-msk-admin-policy.json`
- `AmazonMSKFullAccess`
- `customer-msk-admin-role.json`

Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon MSK?

Agar Amazon MSK dapat mengirimkan log broker ke tujuan yang Anda konfigurasikan, pastikan bahwa `AmazonMSKFullAccess` kebijakan tersebut dilampirkan ke peran IAM Anda. Jadi izin akses penuh sudah ada.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon MSK?

Sebelum membuat cluster MSK Anda, Anda harus memiliki VPC dan subnet di dalam VPC itu. Secara default, AMS memiliki ini sebagai bagian dari pembuatan VPC AMS default.

Untuk mempelajari tentang batasan MSK Amazon, lihat Batas MSK Amazon.

Gunakan SSP AMS untuk menyediakan Layanan Terkelola Amazon untuk Prometheus di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon Managed Service for Prometheus (AMP) secara langsung di akun terkelola AMS Anda. Amazon Managed Service for Prometheus adalah layanan pemantauan tanpa server yang kompatibel dengan Prometheus untuk metrik kontainer yang memudahkan pemantauan lingkungan kontainer dengan aman dalam skala besar. Dengan Amazon Managed Service for Prometheus, Anda dapat menggunakan model data Prometheus sumber terbuka dan bahasa kueri yang sama yang Anda gunakan saat ini untuk memantau kinerja beban kerja kontainer Anda, dan juga menikmati peningkatan skalabilitas, ketersediaan, dan keamanan tanpa harus mengelola infrastruktur yang mendasarinya.

Amazon Managed Service for Prometheus secara otomatis menskalakan konsumsi, penyimpanan, dan kueri metrik operasional saat beban kerja meningkat dan turun. Ini terintegrasi dengan layanan AWS keamanan untuk memungkinkan akses cepat dan aman ke data. Untuk informasi selengkapnya, lihat Apa itu Layanan Terkelola Amazon untuk Prometheus?

Layanan Terkelola Amazon untuk Prometheus di AWS Managed Services FAQ

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Managed Service untuk Prometheus di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer-prometheus-console-role` Setelah disediakan di akun Anda, Anda harus memasukkan `customer-prometheus-console-role` peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Layanan Terkelola Amazon untuk Prometheus di akun AMS saya?

Semua fitur didukung.

T: Apa prasyarat atau dependensi untuk menggunakan Layanan Terkelola Amazon untuk Prometheus di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk memulai Layanan Terkelola Amazon untuk Prometheus. Namun, tergantung pada kasus penggunaan spesifik Anda, Anda mungkin memerlukan akses ke AWS layanan lain.

Menggunakan AMS SSP untuk menyediakan Amazon Personalize di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon Personalisasi secara langsung di akun terkelola AMS Anda. Amazon Personalize adalah layanan pembelajaran mesin yang memudahkan pengembang untuk membuat rekomendasi individual bagi pelanggan yang menggunakan aplikasi mereka.

Pembelajaran mesin semakin banyak digunakan untuk meningkatkan keterlibatan pelanggan dengan mendukung rekomendasi produk dan konten yang dipersonalisasi, hasil pencarian yang disesuaikan, dan promosi pemasaran yang ditargetkan. Namun, mengembangkan kemampuan pembelajaran mesin yang diperlukan untuk menghasilkan sistem rekomendasi canggih ini telah berada di luar jangkauan sebagian besar organisasi saat ini karena kompleksitasnya. Amazon Personalize memungkinkan pengembang tanpa pengalaman pembelajaran mesin sebelumnya untuk dengan mudah membangun kemampuan personalisasi canggih ke dalam aplikasi mereka, menggunakan teknologi pembelajaran mesin yang disempurnakan dari penggunaan bertahun-tahun di Amazon.com.

Dengan Amazon Personalize, Anda menyediakan aliran aktivitas dari aplikasi Anda — klik, tampilan halaman, pendaftaran, pembelian, dan sebagainya — serta inventaris item yang ingin Anda rekomendasikan, seperti artikel, produk, video, atau musik. Anda juga dapat memilih untuk memberikan Amazon Personalize dengan informasi demografis tambahan dari pengguna Anda seperti usia, atau lokasi geografis. Amazon Personalize akan memproses dan memeriksa data, mengidentifikasi apa yang berarti, memilih algoritme yang tepat, serta melatih serta mengoptimalkan model personalisasi yang disesuaikan untuk data Anda. Semua data yang dianalisis oleh Amazon Personalize dijaga kerahasiaan dan aman, dan hanya digunakan untuk rekomendasi khusus Anda. Anda dapat mulai menyajikan rekomendasi yang dipersonalisasi melalui panggilan API sederhana. Anda hanya membayar untuk apa yang Anda gunakan, dan tidak ada biaya minimum dan tidak ada komitmen di muka.

Untuk mempelajari selengkapnya, lihat Amazon Personalize.

FAQ Personalisasi Amazon di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon Personalize di akun AMS saya?

Minta akses dengan mengirimkan tipe perubahan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny), dan Anda perlu menentukan bucket S3 mana yang berisi data yang akan digunakan oleh personalisasi untuk menghasilkan rekomendasi. AWS RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_personalize_console_role` dan. `customer_personalize_service_role`

- Setelah `customer_personalize_console_role` disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda. Anda juga dapat melampirkan `customer_personalize_console_policy` ke peran lain yang ada selain`Customer_ReadOnly_Role`.
- Setelah `customer_personalize_service_role` diberikan ke akun Anda, maka Anda dapat merujuk ARN-nya saat membuat grup dataset baru.

Pada saat ini, Operasi AMS juga akan menerapkan peran layanan ini di akun Anda:`aws_code_pipeline_service_role_policy`.

T: Apa batasan untuk menggunakan Amazon Personalize di akun AMS saya?

Konfigurasi Amazon Personalize terbatas pada sumber daya tanpa awalan 'ams-' atau 'mc-', untuk mencegah modifikasi apa pun pada infrastruktur AMS.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Personalize di akun AMS saya?

- Jika bucket S3 tempat data disimpan dienkripsi, ID kunci KMS harus disediakan, sehingga kami dapat mengizinkan peran yang digunakan oleh Amazon Personalize untuk mendekripsi bucket.

  Amazon Personalize tidak mendukung kunci KMS S3 default. Jika diperlukan untuk menggunakan KMS, buat kunci kustom dan tambahkan kebijakan berikut dengan membuka RFC dengan jenis perubahan Kunci KMS | Buat (Review Required):

  JSON

```
{
    "Version":"2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": "personalize.amazonaws.com"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

- Bucket S3 harus dibuat dengan kebijakan bucket berikut. Lakukan ini dengan mengirimkan RFC dengan jenis perubahan S3 Storage | Create Policy. Kebijakan ini memungkinkan Amazon Personalize untuk mengakses data; bucket tersebut akan berisi data yang akan digunakan oleh Amazon Personalize.

  JSON

```
{
"Version":"2012-10-17",
"Id": "PersonalizeS3BucketAccessPolicy",
"Statement": [
{
"Sid": "PersonalizeS3BucketAccessPolicy",
"Effect": "Allow",
"Principal": {
"Service": "personalize.amazonaws.com"
},
"Action": [
"s3:GetObject",
"s3:ListBucket"
],
"Resource": [
"arn:aws:s3:::bucket-name",
"arn:aws:s3:::bucket-name/*"
]
}
]
}
```

Gunakan AMS SSP untuk menyediakan Amazon QuickSight di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses QuickSight kapabilitas secara langsung di akun terkelola AMS Anda. QuickSight adalah layanan intelijen bisnis yang cepat dan bertenaga cloud yang memberikan wawasan kepada semua orang di organisasi Anda. Sebagai layanan yang dikelola sepenuhnya, Anda QuickSight dapat dengan mudah membuat dan menerbitkan dasbor interaktif yang menyertakan wawasan pembelajaran mesin (ML). Untuk mempelajari lebih lanjut, lihat Amazon QuickSight.

QuickSight di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke QuickSight akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_quicksight_console_admin_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan QuickSight di akun AMS saya?

- AWS pengaturan sumber daya QuickSight tidak akan dapat diakses oleh Anda karena ketergantungan kebijakan IAM. Namun, tim AMS mengaktifkan setiap sumber daya untuk Anda sebagai tanggapan atas permintaan Anda untuk mengaktifkan layanan.
- Akses sumber daya untuk pengguna individu dan grup tidak didukung dalam model ini karena fitur ini memungkinkan pengguna untuk mengubah izin IAM yang dapat membahayakan infrastruktur AMS.
- Kemampuan untuk mengundang identitas IAM dari dalam tidak QuickSight didukung karena risiko yang terlibat mengubah objek IAM.
- QuickSight layanan menawarkan dua edisi: Enterprise dan Standard. Keduanya menyediakan opsi masuk tunggal (SSO) yang didukung di AMS. Namun, Enterprise Edition memiliki opsi untuk berintegrasi QuickSight dengan Active Directory (AD). QuickSight pada AMS tidak mendukung integrasi dengan AD karena ketidakcocokan antara struktur akun AMS dan persyaratan kepercayaan. QuickSight

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? QuickSight

- Ketika AMS menerima RFC ini untuk ditambahkan QuickSight, Anda akan dikirimi permintaan layanan untuk informasi tambahan; berikan mereka yang berikut:
  - QuickSight nama akun (misalnya, *CustomerName*-quicksight
  - QuickSight Edisi (Standar versus Perusahaan)
  - AWS Wilayah tempat mengaktifkan QuickSight layanan (default ke Wilayah AMS AWS Anda).
  - Alamat email notifikasi untuk QuickSight akun.
  - (Opsional) Bucket S3 tempat file data yang akan dianalisis berada.
  - VPC dan subnet IDs yang terhubung untuk QuickSight mendukung fitur untuk menambahkan koneksi VPC, yang memungkinkan konektivitas pribadi antara QuickSight dan sumber daya di dalam akun.

Operator AMS melakukan proses pendaftaran atas nama Anda dan mengonfigurasi dua QuickSight fungsi:

- Penemuan otomatis ke sumber data.
- Koneksi VPC.

> **Note**
>
> Tindakan ini perlu dilakukan oleh operator AMS karena izin IAM dan VPC yang ditinggikan diperlukan selama proses masuk.

Gunakan AMS SSP untuk menyediakan Amazon Rekognition di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Rekognition secara langsung di akun terkelola AMS Anda. Amazon Rekognition memudahkan untuk menambahkan analisis gambar dan video ke aplikasi Anda menggunakan teknologi pembelajaran mendalam yang terbukti, sangat skalabel, dan tidak memerlukan keahlian pembelajaran mesin untuk digunakan. Dengan Amazon Rekognition, Anda dapat mengidentifikasi objek, orang, teks, adegan, dan aktivitas dalam gambar dan video, serta mendeteksi konten yang tidak pantas. Amazon Rekognition juga menyediakan analisis wajah dan kemampuan pencarian wajah yang sangat akurat yang dapat Anda gunakan untuk mendeteksi, menganalisis, dan membandingkan wajah untuk

berbagai macam verifikasi pengguna, penghitungan orang, dan kasus penggunaan keselamatan publik.

Dengan Label Kustom Amazon Rekognition, Anda dapat mengidentifikasi objek dan adegan dalam gambar yang spesifik untuk kebutuhan bisnis Anda. Misalnya, Anda dapat membuat model untuk mengklasifikasikan suku cadang mesin tertentu di jalur perakitan Anda atau untuk mendeteksi tanaman yang tidak sehat. Amazon Rekognition Custom Labels menangani pengembangan model angkat berat untuk Anda, jadi tidak diperlukan pengalaman pembelajaran mesin. Anda hanya perlu menyediakan gambar objek atau adegan yang ingin Anda identifikasi, dan layanan menangani sisanya.

Untuk mempelajari lebih lanjut, lihat Amazon Rekognition.

FAQ Rekognition Amazon di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon Rekognition di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_rekognition_console_role & customer_rekognition_service_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Rekognition di akun AMS saya?

Fungsionalitas penuh Amazon Rekognition tersedia dengan peran layanan Amazon Rekognition yang disediakan sendiri.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Rekognition di akun AMS saya?

Jika Anda menggunakan Kinesis Video Streams yang menyediakan video streaming sumber untuk pemroses aliran Video Rekognition Amazon atau aliran data sebagai tujuan untuk menulis data ke Kinesis Data Streams, silakan berikan AMS saat membuat RFC. `kinesisStreamName`

Gunakan AMS SSP untuk menyediakan Amazon SageMaker AI di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon SageMaker AI secara langsung di akun terkelola AMS Anda. SageMaker AI memberi setiap

pengembang dan ilmuwan data kemampuan untuk membangun, melatih, dan menerapkan model pembelajaran mesin dengan cepat. Amazon SageMaker AI adalah layanan yang dikelola sepenuhnya yang mencakup seluruh alur kerja pembelajaran mesin untuk memberi label dan menyiapkan data Anda, memilih algoritme, melatih model, menyetel dan mengoptimalkannya untuk penerapan, membuat prediksi, dan mengambil tindakan. Model Anda dapat berproduksi lebih cepat dengan usaha yang jauh lebih sedikit dan biaya lebih rendah. Untuk mempelajari lebih lanjut, lihat Amazon SageMaker AI.

SageMaker FAQ AI di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke SageMaker AI di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_sagemaker_admin_role` dan peran layanan. `AmazonSageMaker-ExecutionRole-Admin` Setelah SageMaker AI disediakan di akun Anda, Anda harus memasukkan `customer_sagemaker_admin_role` peran tersebut dalam solusi federasi Anda. Peran layanan tidak dapat diakses oleh Anda secara langsung; layanan SageMaker AI menggunakannya saat melakukan berbagai tindakan seperti yang dijelaskan di sini: Melewati Peran.

T: Apa batasan untuk menggunakan SageMaker AI di akun AMS saya?

- Kasus penggunaan berikut tidak didukung oleh peran AMS Amazon SageMaker AI IAM:
  - SageMaker AI Studio tidak didukung saat ini.
  - SageMaker AI Ground Truth untuk mengelola tenaga kerja pribadi tidak didukung karena fitur ini memerlukan akses yang terlalu permisif ke sumber daya Amazon Cognito. Jika mengelola tenaga kerja pribadi diperlukan, Anda dapat meminta peran IAM khusus dengan izin gabungan SageMaker AI dan Amazon Cognito. Jika tidak, sebaiknya gunakan tenaga kerja publik (didukung oleh Amazon Mechanical Turk), AWS Marketplace atau penyedia layanan, untuk pelabelan data.
- Membuat Titik Akhir VPC untuk mendukung panggilan API ke layanan SageMaker AI (aws.sagemaker. {region} .notebook, com.amazonaws. {region} .sagemaker.api & com.amazonaws. {region} .sagemaker.runtime) tidak didukung karena izin tidak dapat dicakup ke layanan terkait AI saja. SageMaker Untuk mendukung kasus penggunaan ini, kirimkan Manajemen | Lainnya | RFC lainnya untuk membuat titik akhir VPC terkait.

- SageMaker Penskalaan otomatis titik akhir AI tidak didukung karena SageMaker AI memerlukan `DeleteAlarm` izin pada sumber daya (“*”) apa pun. Untuk mendukung penskalaan otomatis titik akhir, kirimkan Manajemen | Lainnya | RFC lainnya untuk mengatur penskalaan otomatis untuk titik akhir AI. SageMaker

T: Apa prasyarat atau dependensi untuk menggunakan SageMaker AI di akun AMS saya?

- Kasus penggunaan berikut memerlukan konfigurasi khusus sebelum digunakan:
  - Jika bucket S3 akan digunakan untuk menyimpan artefak dan data model, maka Anda harus meminta bucket S3 yang diberi nama dengan kata kunci yang diperlukan (“”, “Sagemaker”, SageMaker “sagemaker” atau “aws-glue”) dengan Deployment | Komponen tumpukan lanjutan | Penyimpanan S3 | Buat RFC.
  - Jika Elastic File Store (EFS) akan digunakan, maka penyimpanan EFS harus dikonfigurasi dalam subnet yang sama, dan diizinkan oleh grup keamanan.
  - Jika sumber daya lain memerlukan akses langsung ke layanan SageMaker AI (notebook, API, runtime, dan sebagainya), maka konfigurasi harus diminta oleh:
    - Mengirimkan RFC untuk membuat grup keamanan untuk titik akhir (Deployment | Advanced stack components | Security group | Create (auto)).
    - Mengirimkan Manajemen | Lainnya | Lainnya | Buat RFC untuk menyiapkan titik akhir VPC terkait.

T: Apa konvensi penamaan yang didukung untuk sumber daya yang **`customer_sagemaker_admin_role`** dapat diakses secara langsung? (Berikut ini adalah untuk memperbarui dan menghapus izin; jika Anda memerlukan konvensi penamaan tambahan yang didukung untuk sumber daya Anda, hubungi AMS Cloud Architect untuk konsultasi.)

- Sumber daya: Melewati `AmazonSageMaker-ExecutionRole-*` peran
  - Izin: Peran layanan yang disediakan sendiri SageMaker AI mendukung penggunaan peran layanan SageMaker AI (`AmazonSageMaker-ExecutionRole-*`) Anda dengan AWS Glue,, dan. AWS RoboMaker AWS Step Functions
- Sumber Daya: Rahasia tentang AWS Secrets Manager
  - Izin: Jelaskan, Buat, Dapatkan, Perbarui rahasia dengan `AmazonSageMaker-*` awalan.
  - Izin: Jelaskan, Dapatkan rahasia saat tag `SageMaker` sumber daya disetel ke`true`.
- Sumber Daya: Repositori di AWS CodeCommit

    - Izin: Buat/hapus repositori dengan awalan. `AmazonSageMaker-*`
    - Izin: Git Pull/Push pada repositori dengan awalan berikut,,, dan. `*sagemaker*` `*SageMaker*` `*Sagemaker*`
- Sumber Daya: Repositori Amazon ECR (Amazon Elastic Container Registry)
    - Izin: Izin: Setel, hapus kebijakan repositori, dan unggah gambar kontainer, saat konvensi penamaan sumber daya berikut digunakan,. `*sagemaker*`
- Sumber daya: ember Amazon S3
    - Izin: Dapatkan, Letakkan, Hapus objek, batalkan objek S3 unggahan multibagian saat sumber daya memiliki awalan berikut:,, dan. `*SageMaker*` `*Sagemaker*` `*sagemaker*` `aws-glue`
    - Izin: Dapatkan objek S3 saat `SageMaker` tag disetel ke. `true`
- Sumber Daya: Grup CloudWatch Log Amazon
    - Izin: Buat Grup Log atau Streaming, Letakkan Acara Log, Daftar, Perbarui, Buat, Hapus pengiriman log dengan awalan berikut:. `/aws/sagemaker/*`
- Sumber daya: Amazon CloudWatch Metric
    - Izin: Masukkan data metrik saat awalan berikut digunakan:`AWS/SageMaker`,,,,`AWS/SageMaker/`, `aws/SageMaker` `aws/SageMaker/aws/sagemaker`, `aws/sagemaker/` dan. `/aws/sagemaker/.`
- Sumber Daya: CloudWatch Dasbor Amazon
    - Izin: Create/Delete dasbor saat awalan berikut digunakan:. `customer_*`
- Sumber daya: Topik Amazon SNS (Layanan Pemberitahuan Sederhana)
    - Izin: Subscribe/Create topik saat awalan berikut digunakan:`*sagemaker*`,, `*SageMaker*` dan. `*Sagemaker*`

Q: Apa perbedaan antara **`AmazonSageMakerFullAccess`** dan**`customer_sagemaker_admin_role`**?

The `customer_sagemaker_admin_role` with the `customer_sagemaker_admin_policy` memberikan izin yang hampir sama dengan AmazonSageMakerFullAccess kecuali:

- Izin untuk terhubung dengan AWS RoboMaker, Amazon Cognito, dan AWS Glue sumber daya.
- SageMaker Penskalaan otomatis titik akhir AI. Anda harus mengirimkan RFC dengan Manajemen | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Perbarui entitas atau kebijakan (diperlukan tinjauan) jenis perubahan (ct-27tuth19k52b4) untuk meningkatkan izin

penskalaan otomatis sementara, atau secara permanen, karena penskalaan otomatis memerlukan akses permisif pada layanan. CloudWatch

T: Bagaimana cara mengadopsi kunci terkelola AWS KMS pelanggan dalam enkripsi data saat istirahat?

Anda harus memastikan bahwa kebijakan kunci telah diatur dengan benar pada kunci yang dikelola pelanggan sehingga pengguna atau peran IAM terkait dapat menggunakan kunci. Untuk informasi selengkapnya, lihat dokumen Kebijakan AWS KMS Utama.

Gunakan AMS SSP untuk menyediakan Amazon Simple Email Service di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Amazon Simple Email Service (Amazon SES) langsung di akun terkelola AMS Anda. Amazon Simple Email Service adalah layanan pengiriman email berbasis cloud yang dirancang untuk membantu pemasar digital dan pengembang aplikasi, mengirim email pemasaran, pemberitahuan, dan transaksional.

Anda dapat menggunakan antarmuka SMTP atau salah satu AWS SDKs untuk mengintegrasikan Amazon SES langsung ke aplikasi yang ada. Anda juga dapat mengintegrasikan kemampuan pengiriman email Amazon SES ke dalam perangkat lunak yang sudah Anda gunakan, seperti sistem tiket dan klien email.

Untuk mempelajari selengkapnya, lihat Amazon Simple Email Service.

FAQ Amazon SES di AWS Managed Services

T: Bagaimana cara meminta akses ke Amazon SES di akun AMS saya?

Meminta akses ke Amazon SES dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_ses_admin_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon SES di akun AMS saya?

- Anda harus mengonfigurasi kebijakan bucket S3 agar Amazon SES dapat memublikasikan peristiwa ke bucket.

- Anda harus menggunakan default (AWS SES), atau mengonfigurasi, kunci CMK untuk mengizinkan Amazon SES mengenkripsi email dan mendorong peristiwa ke sumber daya layanan lain seperti Amazon S3, Amazon SNS, Lambda, dan Firehose, milik akun.

T: Apa batasan untuk menggunakan Amazon SES di akun AMS saya?

Anda harus meningkatkan RFCs untuk membuat sumber daya berikut:

- Pengguna SMTP dan peran layanan IAM dengan PutEvents izin, ke aliran Kinesis Firehose.
- Anda harus membuat AWS sumber daya baru seperti bucket S3, aliran Firehose, topik SNS dengan menggunakan jenis perubahan AMS agar aturan Amazon SES dan tujuan set konfigurasi dapat berfungsi dengan sumber daya tersebut.
- Kredensi SMTP. Untuk meminta kredensi SMTP baru, gunakan Ubah Jenis (Manajemen | Lainnya | Lainnya | Buat). AMS membuat kredensil dan menambahkannya ke Secrets Manager untuk Anda.

Gunakan AMS SSP untuk menyediakan Amazon Simple Workflow Service di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Simple Workflow Service (Amazon SWF) secara langsung di akun terkelola AMS Anda. Amazon Simple Workflow Service membantu pengembang membangun, menjalankan, dan menskalakan pekerjaan latar belakang yang memiliki langkah paralel atau berurutan. Anda dapat menganggap Amazon SWF sebagai pelacak status dan koordinator tugas yang dikelola sepenuhnya di Cloud. Jika langkah aplikasi Anda membutuhkan waktu lebih dari 500 milidetik untuk diselesaikan, Anda perlu melacak status pemrosesan, atau Anda perlu memulihkan atau mencoba lagi jika tugas gagal, Amazon SWF dapat membantu Anda. Untuk mempelajari selengkapnya, lihat Amazon Simple Workflow Service.

FAQ Amazon SWF di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Amazon SWF di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_swf_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon SWF di akun AMS saya?

`InvokeFunction`Izin Lambda telah disertakan dalam layanan ini, namun AMS `customer_deny_policy` yang ditambahkan ke semua peran pelanggan AMS secara eksplisit menolak akses ke fungsi AMS Lambda dan sumber daya milik AMS. Untuk menandai atau menghapus tag sumber daya dalam Amazon SWF, kirimkan Manajemen | Lainnya | Jenis Perubahan Lainnya.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon SWF di akun AMS saya?

Amazon SWF bergantung pada AWS Lambda layanan, oleh karena itu, izin untuk memanggil Lambda telah diberikan sebagai bagian dari peran ini dan tidak ada izin tambahan yang diperlukan untuk memanggil Lambda dari Amazon SWF. Jika tidak, tidak ada prasyarat untuk menggunakan Amazon SWF.

Gunakan AMS SSP untuk menyediakan Amazon Ttract di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Textract secara langsung di akun terkelola AMS Anda. Amazon Textract adalah layanan pembelajaran mesin yang dikelola sepenuhnya yang secara otomatis mengekstrak teks cetak, tulisan tangan, dan data lain dari dokumen yang dipindai yang melampaui pengenalan karakter optik sederhana (OCR) untuk mengidentifikasi, memahami, dan mengekstrak data dari formulir dan tabel. Untuk mempelajari lebih lanjut, lihat Amazon Texttract.

FAQ Amazon Texttract di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta Amazon Texttract untuk disiapkan di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:`customer_textract_console_role`,`customer_textract_human_review_execution_role`, dan. `customer_ec2_textract_instance_profile` Setelah disediakan di akun Anda, Anda harus memasukkan peran `customer_textract_console_role` dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Amazon Ttract di akun AMS saya?

Tidak ada batasan untuk penggunaan Amazon Ttract di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Ttract di akun AMS saya?

Anda harus meminta pembuatan bucket S3 dengan mengirimkan Deployment RFC | Komponen tumpukan lanjutan |S3 storage | Create (ct-1a68ck03fn98r).

Gunakan SSP AMS untuk menyediakan Amazon Transcribe di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Amazon Transcribe secara langsung di akun terkelola AMS Anda. Amazon Transcribe adalah layanan pengenalan suara otomatis yang dikelola sepenuhnya dan dilatih terus menerus yang secara otomatis menghasilkan transkrip teks berstempel waktu dari file audio. Amazon Transcribe memudahkan pengembang untuk menambahkan speech-to-text kemampuan ke aplikasi mereka. Data audio hampir tidak mungkin bagi komputer untuk mencari dan menganalisis. Oleh karena itu, pidato yang direkam perlu dikonversi menjadi teks sebelum dapat digunakan dalam aplikasi. Secara historis, pelanggan harus bekerja dengan penyedia transkripsi yang mengharuskan mereka menandatangani kontrak mahal dan sulit untuk diintegrasikan ke dalam tumpukan teknologi mereka untuk menyelesaikan tugas ini. Banyak dari penyedia ini menggunakan teknologi usang yang tidak beradaptasi dengan baik untuk skenario yang berbeda, seperti audio telepon dengan kesetiaan rendah yang umum di pusat kontak, yang menghasilkan akurasi yang buruk.

Amazon Transcribe menggunakan proses pembelajaran mendalam yang disebut Automatic Speech Recognition (ASR) untuk mengubah ucapan menjadi teks, dengan cepat dan akurat. Amazon Transcribe dapat digunakan untuk mentranskripsikan panggilan layanan pelanggan, mengotomatiskan teks dan subtitling tertutup, dan menghasilkan metadata untuk aset media guna membuat arsip yang dapat dicari sepenuhnya. Anda dapat menggunakan Amazon Transcribe Medical untuk menambahkan speech-to-text kemampuan medis ke aplikasi dokumentasi klinis. Untuk mempelajari lebih lanjut, lihat Amazon Transcribe.

FAQ Amazon Transcribe di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta Amazon Transcribe disiapkan di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_transcribe_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan Amazon Transcribe di akun AMS saya?

Anda harus menggunakan 'customer-transcribe*' sebagai awalan untuk bucket Anda saat bekerja dengan transcribe, kecuali RA dan ditentukan lain.

Anda tidak dapat membuat peran IAM dalam transkrip Amazon.

Anda tidak dapat menggunakan bucket S3 yang dikelola layanan untuk data keluaran di SSPS default (jika diperlukan, hubungi CA akun Anda).

Anda harus mengirimkan Penerimaan Risiko jika ingin menggunakan Kunci KMS yang dikelola pelanggan yang tidak termasuk dalam namespace AMS.

T: Apa prasyarat atau dependensi untuk menggunakan Amazon Transcribe di akun AMS saya?

S3 harus memiliki akses ke bucket dengan nama 'customer-transcribe*'. KMS diperlukan untuk menggunakan Amazon Transcribe jika bucket S3 Anda dienkripsi dengan kunci KMS. Jika ember tidak perlu dienkripsi "KMStranscribeIzinkan” dapat dihapus.

Gunakan AMS SSP untuk menyediakan Amazon WorkSpaces di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses WorkSpaces kapabilitas secara langsung di akun terkelola AMS Anda. WorkSpaces memungkinkan Anda menyediakan desktop Microsoft Windows atau Amazon Linux virtual berbasis cloud untuk pengguna Anda, yang dikenal sebagai. WorkSpaces WorkSpaces menghilangkan kebutuhan untuk mendapatkan dan menyebarkan perangkat keras atau menginstal perangkat lunak yang kompleks. Anda dapat dengan cepat menambahkan atau menghapus pengguna saat kebutuhan Anda berubah. Pengguna mengaksesnya WorkSpaces dengan menggunakan aplikasi klien dari perangkat yang didukung atau, untuk Windows WorkSpaces, browser web, dan mereka masuk dengan menggunakan kredenal Active Directory (AD) lokal yang ada.

Untuk mempelajari lebih lanjut, lihat Amazon WorkSpaces.

WorkSpaces di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke WorkSpaces akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM

berikut ke akun Anda:. `customer_workspaces_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan WorkSpaces di akun AMS saya?

Fungsionalitas penuh Workspaces tersedia dengan peran layanan Amazon yang WorkSpaces disediakan sendiri.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? WorkSpaces

- WorkSpaces dibatasi oleh AWS Wilayah; oleh karena itu, AD Connector harus dikonfigurasi di AWS Wilayah yang sama tempat WorkSpaces instans di-host.

  Pelanggan dapat terhubung WorkSpaces ke AD pelanggan menggunakan salah satu dari dua metode berikut:

  1. Menggunakan konektor AD untuk otentikasi proxy ke layanan Active Directory lokal (lebih disukai):

     Konfigurasikan Konektor Direktori Aktif (AD) di akun AMS Anda sebelum mengintegrasikan WorkSpaces instans Anda dengan layanan direktori lokal. Konektor AD bertindak sebagai proxy bagi pengguna AD yang ada (dari domain Anda) untuk terhubung WorkSpaces menggunakan kredensil AD lokal yang ada. Ini lebih disukai karena WorkSpaces secara langsung bergabung dengan domain on-prem pelanggan, yang bertindak sebagai Resource dan User forest, yang mengarah ke kontrol yang lebih besar di sisi pelanggan.

     Untuk informasi selengkapnya, lihat Praktik Terbaik untuk Menerapkan Amazon WorkSpaces (Skenario 1).
  2. Menggunakan Konektor AD dengan AWS Microsoft AD, VPC Layanan Bersama, dan kepercayaan satu arah ke lokal:

     Anda juga dapat mengautentikasi pengguna dengan direktori lokal dengan terlebih dahulu membuat kepercayaan keluar satu arah dari AD yang dikelola AMS ke AD lokal. WorkSpaces akan bergabung dengan AMS-managed AD menggunakan AD Connector. WorkSpaces Izin akses kemudian akan didelegasikan ke WorkSpaces instans melalui AD yang dikelola AMS, tanpa perlu membangun kepercayaan dua arah dengan lingkungan lokal Anda. Dalam skenario ini, hutan Pengguna akan berada di AD pelanggan dan hutan Sumber Daya akan berada di AD yang dikelola AMS (perubahan pada AD yang dikelola AMS dapat diminta melalui RFC). Perhatikan bahwa konektivitas antara WorkSpaces VPC dan VPC Layanan Bersama MALZ yang menjalankan AD yang dikelola AMS dibuat melalui Transit Gateway.

Untuk informasi selengkapnya, lihat Praktik Terbaik untuk Menerapkan Amazon WorkSpaces (Skenario 6).

> **Note**
>
> AD Connector dapat dikonfigurasi dengan mengirimkan Management | Other | Other | Other | Create change type RFC dengan detail konfigurasi AD prasyarat; untuk informasi selengkapnya, lihat Membuat AD Connector. Jika metode 2 digunakan untuk membuat hutan Sumber Daya di AD yang dikelola AMS, kirimkan Manajemen lain | Lainnya | Lainnya | Lainnya | Buat jenis perubahan RFC di akun layanan bersama AMS dengan menjalankan AD yang dikelola AMS.

Gunakan SSP AMS untuk menyediakan layanan Kode AMS di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas layanan Kode AMS secara langsung di akun terkelola AMS Anda. Layanan AMS Code adalah bundling eksklusif dari layanan manajemen kode AWS sebagaimana dirinci selanjutnya. Anda dapat memilih untuk menerapkan semua layanan di AMS dengan layanan Kode AMS, atau Anda dapat menerapkannya di AMS satu per satu.

Layanan Kode AMS mencakup layanan berikut:

- AWS CodeCommit: Layanan kontrol sumber yang dikelola sepenuhnya yang menampung repositori berbasis Git yang aman. Itu membuatnya sehingga tim dapat berkolaborasi dalam kode dalam ekosistem yang aman dan sangat skalabel. CodeCommit menghilangkan kebutuhan untuk mengoperasikan sistem kontrol sumber Anda sendiri atau khawatir tentang penskalaan infrastrukturnya. Anda dapat menggunakan CodeCommit untuk menyimpan apa pun dengan aman dari kode sumber ke biner dan bekerja dengan mulus dengan alat Git Anda yang ada. Untuk mempelajari selengkapnya, lihat AWS CodeCommit

  Untuk menerapkan ini di akun AMS Anda secara independen dari layanan Kode AMS, lihatGunakan SSP AMS untuk menyediakan AWS CodeCommit di akun AMS Anda.
- AWS CodeBuild: Layanan integrasi berkelanjutan yang dikelola sepenuhnya yang mengkompilasi kode sumber, menjalankan pengujian, dan menghasilkan paket perangkat lunak yang siap digunakan. Dengan CodeBuild, Anda tidak perlu menyediakan, mengelola, dan menskalakan

server build Anda sendiri. CodeBuild menskalakan terus menerus dan memproses beberapa build secara bersamaan, sehingga build Anda tidak dibiarkan menunggu dalam antrian. Anda dapat memulai dengan cepat menggunakan lingkungan build yang dikemas sebelumnya, atau Anda dapat membuat lingkungan build khusus yang menggunakan alat build Anda sendiri. Dengan CodeBuild, Anda dikenakan biaya per menit untuk sumber daya komputasi yang Anda gunakan. Untuk mempelajari selengkapnya, lihat AWS CodeBuild

Untuk menerapkan ini di akun AMS Anda secara independen dari layanan Kode AMS, lihatGunakan SSP AMS untuk menyediakan AWS CodeBuild di akun AMS Anda.

- AWS CodeDeploy: Layanan penyebaran terkelola penuh yang mengotomatiskan penerapan perangkat lunak ke berbagai layanan komputasi seperti Amazon EC2 dan server lokal Anda. AWS CodeDeploy membantu Anda merilis fitur baru dengan cepat, membantu Anda menghindari downtime selama penerapan aplikasi, dan menangani kompleksitas memperbarui aplikasi Anda. Anda dapat menggunakan AWS CodeDeploy untuk mengotomatiskan penerapan perangkat lunak, menghilangkan kebutuhan akan operasi manual yang rawan kesalahan. Skala layanan agar sesuai dengan kebutuhan penerapan Anda. Untuk mempelajari selengkapnya, lihat AWS CodeDeploy

  Untuk menerapkan ini di akun AMS Anda secara independen dari layanan Kode AMS, lihatGunakan SSP AMS untuk menyediakan AWS CodeDeploy di akun AMS Anda.
- AWS CodePipeline: Layanan pengiriman berkelanjutan yang dikelola sepenuhnya yang membantu Anda mengotomatiskan saluran pipa rilis untuk pembaruan aplikasi dan infrastruktur yang cepat dan andal. CodePipeline mengotomatiskan fase build, test, dan deploy dari proses rilis Anda setiap kali ada perubahan kode, berdasarkan model rilis yang Anda tentukan. Ini memungkinkan Anda untuk dengan cepat dan andal memberikan fitur dan pembaruan. Anda dapat dengan mudah mengintegrasikan AWS CodePipeline dengan layanan pihak ketiga seperti GitHub atau dengan plugin kustom Anda sendiri. Dengan AWS CodePipeline, Anda hanya membayar untuk apa yang Anda gunakan. Tidak ada biaya di muka atau komitmen jangka panjang. Untuk mempelajari selengkapnya, lihat AWS CodePipeline

  Untuk menerapkan ini di akun AMS Anda secara independen dari layanan Kode AMS, lihatGunakan SSP AMS untuk menyediakan AWS CodePipeline di akun AMS Anda.

Layanan Kode AMS di AWS Managed Services FAQ

T: Bagaimana cara meminta akses ke layanan Kode AMS di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM

berikut ke akun Anda:. `customer_code_suite_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda. Pada saat ini Operasi AMS juga akan menerapkan`customer_codebuild_service_role`,`customer_codedeploy_service_role`, peran `aws_code_pipeline_service_role` layanan di akun Anda untuk CodeBuild, CodeDeploy dan CodePipeline layanan. Jika izin IAM tambahan untuk diperlukan untuk diperlukan, kirimkan permintaan layanan AMS. `customer_codebuild_service_role`

> **Note**
>
> Anda juga dapat menambahkan layanan ini secara terpisah; untuk informasi, lihatGunakan SSP AMS untuk menyediakan AWS CodeBuild di akun AMS Anda,Gunakan SSP AMS untuk menyediakan AWS CodeDeploy di akun AMS Anda, danGunakan SSP AMS untuk menyediakan AWS CodePipeline di akun AMS Anda, masing-masing.

T: Apa batasan untuk menggunakan layanan Kode AMS di akun AMS saya?

- AWS CodeCommit: Fitur pemicu CodeCommit dinonaktifkan mengingat hak terkait untuk membuat topik SNS. Autentikasi langsung terhadap CodeCommit dibatasi; pengguna harus mengautentikasi dengan Credential Helper. Beberapa perintah KMS juga dibatasi: kms: Enkripsi, kms: Dekripsi,,, kms:ReEncrypt, kms: GenereteDataKey dan. kms: GenerateDataKeyWithoutPlaintext kms: DescribeKey
- CodeBuild: Untuk akses admin AWS CodeBuild konsol, izin dibatasi pada tingkat sumber daya; misalnya, CloudWatch tindakan dibatasi pada sumber daya tertentu dan `iam:PassRole` izin dikontrol.
- CodeDeploy: Saat ini CodeDeploy mendukung penerapan hanya di EC2 Amazon/On-premise. Penerapan di ECS dan Lambda melalui tidak didukung. CodeDeploy
- CodePipeline: CodePipeline fitur, tahapan, dan penyedia terbatas pada hal-hal berikut:
  - Tahap Penerapan: Amazon S3 dan AWS CodeDeploy
  - Tahap Sumber: Amazon S3,, Bit Bucket AWS CodeCommit, dan GitHub
  - Build Stage: AWS CodeBuild dan Jenkins
  - Tahap Persetujuan: Amazon SNS
  - Tahap Uji: AWS CodeBuild, Jenkins,, Pengujian UI Ghost Inspector BlazeMeter, Beban StormRunner Fokus Mikro, Pemantauan API Runscope
  - Panggilan Panggilan: Step Functions dan Lambda

> **Note**
>
> Operasi AMS menyebarkan `customer_code_pipeline_lambda_policy` di akun Anda; itu harus dilampirkan dengan peran eksekusi Lambda untuk tahap pemanggilan Lambda. Berikan nama service/execution peran Lambda yang Anda inginkan agar kebijakan ini ditambahkan. Jika tidak ada service/execution peran Lambda khusus, maka AMS membuat peran baru bernama`customer_code_pipeline_lambda_execution_role`, yaitu salinan dari peran Lambda `customer_lambda_basic_execution_role`. `customer_code_pipeline_lambda_policy`

T: Apa prasyarat atau dependensi untuk menggunakan layanan Kode AMS di akun AMS saya?

- CodeCommit: Jika bucket S3 dienkripsi dengan AWS KMS kunci, S3 dan AWS KMS harus digunakan. AWS CodeCommit
- CodeBuild: Jika izin IAM tambahan diperlukan untuk peran AWS CodeBuild layanan yang ditentukan, minta izin tersebut melalui permintaan layanan AMS.
- CodeDeploy: Tidak ada.
- CodePipeline: Tidak ada. AWS layanan yang didukung—AWS CodeCommit AWS CodeBuild,, AWS CodeDeploy—harus diluncurkan sebelum, atau bersamaan dengan, peluncuran. CodePipeline Namun ini dilakukan oleh insinyur AMS.

Gunakan SSP AMS untuk menyediakan AWS Amplify di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Amplify kapabilitas secara langsung di akun terkelola AMS Anda. AWS Amplify Ini adalah solusi lengkap yang memungkinkan pengembang web dan seluler frontend untuk dengan mudah membangun, menghubungkan, dan meng-host aplikasi fullstack. Amplify memberikan fleksibilitas untuk memanfaatkan luasnya AWS layanan saat kasus penggunaan Anda berkembang. Amplify menyediakan produk untuk membangun aplikasi iOS, Android, Flutter, Web, dan React Native fullstack. Untuk mempelajari selengkapnya, lihat AWS Amplify.

AWS Amplify di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara saya meminta AWS Amplify untuk disiapkan di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_amplify_console_role` Setelah disediakan ke akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

Selain itu, Anda harus memberikan Penerimaan Risiko karena AWS Amplify memiliki izin mutasi infrastruktur. Untuk melakukan ini, bekerja dengan Cloud Service Delivery Manager (CSDM) Anda.

T: Apa batasan penggunaan AWS Amplify di akun AMS saya?

Anda harus menggunakan `'amplify*'` sebagai awalan untuk bucket Anda saat bekerja dengan Amplify, kecuali RA dan ditentukan lain.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Amplify

Tidak ada prasyarat untuk penggunaan di akun AMS Anda. AWS Amplify

Hanya lingkungan Malz: Peran bawaan bawaan untuk Amplify adalah “customer_amplify_console_role”. Untuk menggunakan peran kustom, pertama-tama gunakan entitas IAM. Kemudian, buat RFC tambahan untuk menambahkan peran kustom Anda ke daftar izin Kebijakan Kontrol Layanan untuk Akun Aplikasi.

Gunakan AMS SSP untuk menyediakan AWS AppSync

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS AppSync kapabilitas secara langsung di akun terkelola AMS Anda. AWS AppSync menyederhanakan pengembangan aplikasi dengan memungkinkan Anda membuat API fleksibel untuk mengakses, memanipulasi, dan menggabungkan data dengan aman dari satu atau beberapa sumber data. AWS AppSync adalah layanan terkelola yang menggunakan GraphQL untuk memudahkan aplikasi mendapatkan data yang tepat yang mereka butuhkan.

Dengan AWS AppSync, Anda dapat membangun aplikasi yang dapat diskalakan, termasuk yang memerlukan pembaruan waktu nyata, pada berbagai sumber data seperti penyimpanan data NoSQL, database relasional, APIs HTTP, dan sumber data kustom Anda. AWS Lambda Untuk aplikasi seluler dan web, AWS AppSync juga menyediakan akses data lokal saat perangkat offline, dan sinkronisasi data dengan resolusi konflik yang dapat disesuaikan, saat kembali online. Untuk mempelajari selengkapnya, lihat AWS AppSync.

AWS AppSync di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses AWS AppSync di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_appsync_service_role` dan. `customer_appsync_author_role` Setelah disediakan di akun Anda, Anda harus memasukkan solusi `customer_appsync_author_role` dalam federasi Anda.

T: Apa batasan untuk menggunakan AWS AppSync?

- Saat membuat Sumber Data AppSync pada pelanggan perlu menentukan peran layanan yang dibuat sebelumnya, pembuatan peran baru tidak diperbolehkan dan oleh karena itu akan mengembalikan akses yang ditolak
- AppSync peran dikonfigurasi untuk membatasi izin ke sumber daya yang berisi awalan 'AMS-' atau 'MC-' untuk mencegah modifikasi apa pun pada infrastruktur AMS.

T: Apa prasyarat atau dependensi yang digunakan? AWS AppSync

Layanan ini memungkinkan beberapa layanan lain untuk digunakan sebagai sumber data, Izin dasar untuk menggunakannya seperti itu termasuk dalam peran layanan (`customer_appsync_service_role`), tetapi Anda harus secara manual memilih peran layanan saat menggunakan layanan.

Gunakan SSP AMS untuk menyediakan AWS App Mesh di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS App Mesh kapabilitas secara langsung di akun terkelola AMS Anda. AWS App Mesh menyediakan jaringan tingkat aplikasi untuk memudahkan layanan Anda berkomunikasi satu sama lain di berbagai jenis infrastruktur komputasi. App Mesh menstandarisasi cara layanan Anda berkomunikasi, memberi Anda end-to-end visibilitas dan memastikan ketersediaan tinggi untuk aplikasi Anda.

AWS App Mesh memudahkan menjalankan layanan dengan menyediakan visibilitas yang konsisten dan kontrol lalu lintas jaringan untuk layanan yang dibangun di berbagai jenis infrastruktur komputasi. App Mesh menghilangkan kebutuhan untuk memperbarui kode aplikasi untuk mengubah cara data pemantauan dikumpulkan atau lalu lintas dirutekan antar layanan. App Mesh mengonfigurasi setiap

layanan untuk mengekspor data pemantauan dan mengimplementasikan logika kontrol komunikasi yang konsisten di seluruh aplikasi Anda. Ini memudahkan untuk dengan cepat menentukan lokasi kesalahan yang tepat dan secara otomatis merutekan ulang lalu lintas jaringan ketika ada kegagalan atau ketika perubahan kode perlu digunakan. Untuk mempelajari selengkapnya, lihat AWS App Mesh.

AWS App Mesh di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses AWS App Mesh di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_app_mesh_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS App Mesh?

Fungsionalitas penuh AWS App Mesh tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan? AWS App Mesh

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS App Mesh

Gunakan SSP AMS untuk menyediakan AWS Audit Manager di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Audit Manager secara langsung di akun terkelola AMS Anda. Audit Manager membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda menilai risiko dan kepatuhan terhadap peraturan dan standar industri. Audit Manager mengotomatisasi pengumpulan bukti untuk membuatnya lebih mudah untuk menilai apakah kebijakan, prosedur, dan aktivitas Anda beroperasi secara efektif. Ketika tiba waktunya untuk audit, Audit Manager membantu Anda mengelola tinjauan pemangku kepentingan atas kontrol Anda dan membantu Anda membuat laporan siap audit dengan upaya manual yang jauh lebih sedikit. Untuk mempelajari lebih lanjut, lihat Audit Manager.

AWS Audit Manager di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Audit Manager akun AMS saya?

Anda dapat meminta akses melalui pengajuan Manajemen RFC Layanan | Layanan AWS | AWS Layanan yang disediakan sendiri | Tambah (diperlukan peninjauan) (ct-3qe6io8t6jtny). RFC ini menyediakan peran IAM berikut di akun Anda:. `customer-audit-manager-admin-Role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS Audit Manager?

Tidak ada batasan untuk penggunaan AWS Audit Manager di akun AMS Anda. Fungsionalitas AWS Audit Manager penuh untuk disediakan.

T: Apa prasyarat atau dependensi yang digunakan? AWS Audit Manager

1. Anda perlu menyediakan AMS dengan ember s3 tempat Anda reports/assessments ingin tinggal.
2. Jika Anda ingin memiliki enkripsi dengan layanan ini, Anda perlu menyediakan AMS dengan KMS CMK ARN untuk digunakan.
3. Jika Anda ingin mengirim pemberitahuan SNS ke Topik, Anda harus memberikan nama topik atau arn.
4. (Opsional) Ada prasyarat tambahan jika Anda ingin mengaktifkan Organizations sebagai bagian dari landing zone multi-akun Anda di Audit Manager dan Anda menginginkan akun administrator yang didelegasikan: Di kolom deskripsi untuk RFC (Manajemen AWS | layanan | Layanan yang Kompatibel | Tambah), sebutkan bahwa Anda ingin menggunakan akun administrator yang didelegasikan sebagai bagian dari Pengaturan Audit Manager dan berikan rincian di bawah ini:
   - KMS CMK ARN (digunakan untuk mengatur Audit Manager, awalnya)
   - ID akun administrator yang didelegasikan untuk Audit Manager untuk digunakan sebagai bagian dari landing zone multi-akun ini (dapat berupa akun aplikasi MALZ)

Gunakan SSP AMS untuk menyediakan AWS Batch di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Batch kapabilitas secara langsung di akun terkelola AMS Anda. AWS Batch memungkinkan pengembang, ilmuwan, dan insinyur untuk dengan mudah dan efisien menjalankan ratusan ribu pekerjaan komputasi batch AWS. AWS Batch secara dinamis menyediakan kuantitas dan jenis sumber daya komputasi yang optimal (seperti CPU atau instance yang dioptimalkan memori) berdasarkan volume dan persyaratan sumber daya spesifik dari pekerjaan batch yang dikirimkan. Dengan AWS Batch, tidak perlu menginstal dan mengelola perangkat lunak komputasi batch atau cluster server yang Anda

gunakan untuk menjalankan pekerjaan Anda, memungkinkan Anda untuk fokus pada menganalisis hasil dan memecahkan masalah. Untuk mempelajari selengkapnya, lihat AWS Batch.

AWS Batch di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Batch akun AMS saya?

1. Untuk meminta akses ke AWS Batch, kirimkan Manajemen RFC | Layanan AWS | Layanan yang disediakan sendiri | Tambah (ct-1w8z66n899dct). RFC ini menyediakan peran dan kebijakan IAM berikut di akun Anda:

Peran IAM:

- `customer_batch_console_role`
- `customer_batch_ecs_instance_role`
- `customer_batch_events_service_role`
- `customer_batch_service_role`
- `customer_batch_ecs_task_role`

Kebijakan:

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`
- `customer_batch_events_service_role_policy`

2. Setelah disediakan di akun Anda, Anda harus memasukkan peran `customer_batch_console_role` dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS Batch?

Saat membuat Lingkungan Komputasi, Anda harus menandai EC2 instance sebagai “customer_batch” atau “customer-batch”. Jika instance tidak diberi tag, instance tidak akan dihentikan berdasarkan batch saat pekerjaan selesai.

T: Apa prasyarat atau dependensi yang digunakan? AWS Batch

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS Batch

Gunakan SSP AMS untuk menyediakan AWS Certificate Manager di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas AWS Certificate Manager (ACM) secara langsung di akun terkelola AMS Anda. AWS Certificate Manager adalah layanan yang memungkinkan Anda menyediakan, mengelola, dan menyebarkan sertifikat Secure Sockets Layer/Transport Layer Security (SSL/TLS) publik dan pribadi untuk digunakan dengan AWS layanan dan sumber daya internal Anda yang terhubung. SSL/TLS sertifikat digunakan untuk mengamankan komunikasi jaringan dan menetapkan identitas situs web melalui internet serta sumber daya di jaringan pribadi. AWS Certificate Manager menghapus proses manual yang memakan waktu untuk membeli, mengunggah, dan memperbarui SSL/TLS sertifikat.

Dengan AWS Certificate Manager, Anda dapat meminta sertifikat, menerapkannya pada AWS sumber daya yang terintegrasi dengan ACM, seperti Elastic Load Balancers, distribusi CloudFront Amazon, dan pada APIs API Gateway, dan biarkan menangani perpanjangan sertifikat. AWS Certificate Manager Ini juga memungkinkan Anda untuk membuat sertifikat pribadi untuk sumber daya internal Anda dan mengelola siklus hidup sertifikat secara terpusat. Sertifikat publik dan swasta yang disediakan AWS Certificate Manager untuk digunakan dengan layanan terintegrasi ACM gratis. Anda hanya membayar untuk AWS sumber daya yang Anda buat untuk menjalankan aplikasi Anda. Dengan AWS Private Certificate Authority, Anda membayar bulanan untuk pengoperasian AWS Private CA dan untuk sertifikat pribadi yang Anda terbitkan. Untuk mempelajari lebih lanjut, lihat AWS Certificate Manager - AWS Dokumentasi.

FAQ ACM di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Certificate Manager akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_acm_create_role` Anda dapat menggunakan peran ini untuk membuat dan mengelola sertifikat ACM. Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

Sertifikat ACM dapat dibuat menggunakan jenis perubahan berikut, meskipun Anda belum menambahkan peran `customer_acm_create_role` IAM:

- ACM | Buat Sertifikat Publik
- ACM | Buat Sertifikat Pribadi
- Sertifikat ACM dengan tambahan SANs | Buat

T: Apa batasan untuk menggunakan AWS Certificate Manager?

Anda harus mengirimkan Permintaan Perubahan (RFC) ke AMS untuk menghapus atau memodifikasi sertifikat yang ada, karena tindakan tersebut memerlukan akses admin penuh (gunakan Manajemen | Lainnya | Lainnya | Jenis perubahan pembaruan (ct-0xdawir96cy7k). Perhatikan bahwa kebijakan IAM tidak dapat mengecualikan hak berdasarkan nama tag (mc*, ams*, dll). Sertifikat tidak dikenakan biaya, jadi menghapus sertifikat yang tidak digunakan tidak sensitif terhadap waktu.

T: Apa prasyarat atau dependensi untuk menggunakan Certificate Manager?

Nama DNS publik yang ada, dan akses untuk membuat catatan DNS CNAME, tetapi itu tidak perlu di-host di akun terkelola.

Gunakan SSP AMS untuk menyediakan AWS Private Certificate Authority di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Private Certificate Authority kapabilitas secara langsung di akun terkelola AMS Anda. Sertifikat privat digunakan untuk mengidentifikasi dan mengamankan komunikasi antara sumber daya yang terhubung di jaringan pribadi, seperti server, seluler, dan perangkat dan aplikasi IoT. AWS Private CA adalah layanan CA pribadi terkelola yang membantu Anda mengelola siklus hidup sertifikat pribadi Anda dengan mudah dan aman. AWS Private CA memberi Anda layanan CA pribadi yang sangat tersedia tanpa investasi di muka dan biaya pemeliharaan berkelanjutan untuk mengoperasikan CA pribadi Anda sendiri. AWS Private CA memperluas kemampuan manajemen sertifikat ACM ke sertifikat pribadi, memungkinkan Anda untuk membuat dan mengelola sertifikat publik dan swasta secara terpusat. Anda dapat dengan mudah membuat dan menerapkan sertifikat pribadi untuk AWS sumber daya menggunakan AWS Management Console atau ACM API. Untuk EC2 instance, container, perangkat IoT, dan sumber daya lokal, Anda dapat dengan mudah membuat dan melacak sertifikat pribadi dan menggunakan kode otomatisasi sisi klien Anda sendiri untuk menerapkannya. Anda juga memiliki fleksibilitas untuk membuat sertifikat pribadi dan mengelolanya sendiri untuk aplikasi yang memerlukan masa pakai sertifikat khusus, algoritme kunci, atau nama sumber daya Untuk mempelajari lebih lanjut, lihat. AWS Private CA

AWS Private CA di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses AWS Private CA di akun AMS saya?

Meminta akses melalui pengajuan AWS Layanan RFC (Manajemen | layanan | AWS Layanan yang Kompatibel). Melalui RFC ini peran IAM berikut akan disediakan di akun Anda:. `customer_acm_pca_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS Private CA?

Saat ini, AWS Resource Access Manager (AWS RAM) tidak dapat digunakan untuk berbagi AWS Private CA lintas akun Anda.

T: Apa prasyarat atau dependensi yang digunakan? AWS Private CA

1. Jika Anda berencana untuk membuat CRL, Anda memerlukan ember S3 untuk menyimpannya. AWS Private CA secara otomatis menyetor CRL di bucket Amazon S3 yang Anda tunjuk dan memperbaruinya secara berkala. Merupakan syarat awal bahwa bucket S3 memiliki kebijakan bucket di bawah ini sebelum Anda dapat menyiapkan CRL. Untuk melanjutkan permintaan ini; buat RFC dengan ct-0fpjlxa808sh2 (Manajemen | Komponen tumpukan lanjutan | Penyimpanan S3 | Kebijakan pembaruan) sebagai berikut:

- Berikan nama bucket S3 atau ARN.
- Salin kebijakan di bawah ini ke RFC dan ganti `bucket-name` dengan nama bucket S3 yang Anda inginkan.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"acm-pca.amazonaws.com"
         },
         "Action":[
```

```
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetBucketAcl",
            "s3:GetBucketLocation"
         ],
         "Resource":[
            "arn:aws:s3:::bucket-name/*",
            "arn:aws:s3:::bucket-name"
         ]
      }
   ]
}
```

2. Jika bucket S3 di atas dienkripsi, maka Service Principal acm-pca.amazonaws.com memerlukan izin untuk mendekripsi. Untuk melanjutkan permintaan ini; buat RFC dengan ct-3ovo7px2vsa6n (Manajemen | Komponen tumpukan lanjutan | Kunci KMS | Pembaruan) sebagai berikut:

- Berikan ARN Kunci KMS di mana kebijakan harus diperbarui.
- Salin kebijakan di bawah ini ke RFC dan ganti `bucket-name` dengan nama bucket S3 yang Anda inginkan.

```
{
   "Sid":"Allow ACM-PCA use of the key",
   "Effect":"Allow",
   "Principal":{
      "Service":"acm-pca.amazonaws.com"
   },
   "Action":[
      "kms:GenerateDataKey",
      "kms:Decrypt"
   ],
   "Resource":"*",
   "Condition":{
      "StringLike":{
         "kms:EncryptionContext:aws:s3:arn":[
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
            "arn:aws:s3:::bucket_name/audit-report/*",
            "arn:aws:s3:::bucket_name/crl/*"
         ]
```

```
        }
    }
}
```

3. AWS Private CA CRLs tidak mendukung pengaturan S3 “Blokir akses publik ke ember dan objek yang diberikan melalui daftar kontrol akses baru (ACLs)”. Anda harus menonaktifkan pengaturan ini dengan akun S3 dan bucket untuk memungkinkan penulisan CRLs seperti yang disebutkan di Cara membuat dan menyimpan CRL Anda dengan aman untuk ACM Private CA Jika Anda ingin menonaktifkan, buat RFC baru dengan ct-0xdawir96cy7k (Manajemen | Lainnya | Lainnya | Pembaruan) dan lampirkan Penerimaan Risiko. AWS Private CA Jika Anda memiliki pertanyaan tentang penerimaan risiko, hubungi Cloud Architect Anda.

Gunakan SSP AMS untuk menyediakan AWS CloudEndure di akun AMS Anda

> **Note**
>
> Setelah peluncuran yang sukses AWS Application Migration Service, layanan CloudEndure Migrasi sekarang berakhir di semua AWS Wilayah. Kami merekomendasikan penggunaan pelanggan AWS Application Migration Service untuk migrasi lift dan shift ke GovCloud Wilayah dan ke Wilayah Komersil. Untuk informasi, lihat Apa itu AWS Application Migration Service? .
> Jika Anda ingin menggunakan AWS Application Migration Service, hubungi CA Anda sehingga mereka dapat memandu Anda.

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS CloudEndure kapabilitas secara langsung di akun terkelola AMS Anda. AWS CloudEndure migrasi menyederhanakan, mempercepat, dan mengotomatiskan migrasi skala besar dari infrastruktur fisik, virtual, dan berbasis cloud ke infrastruktur. AWS CloudEndure Disaster Recovery (DR) melindungi terhadap downtime dan kehilangan data dari ancaman apa pun, termasuk ransomware dan korupsi server.

AWS CloudEndure di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke CloudEndure akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan Pengguna

IAM berikut ke akun Anda:. `customer_cloud_endure_user` Setelah disediakan di akun Anda, kunci akses dan kunci rahasia untuk pengguna dibagikan di AWS Secrets Manager.

Kebijakan ini juga disediakan untuk akun: `customer_cloud_endure_policy` dan. `customer_cloud_endure_deny_policy`

Selain itu, Anda harus memberikan Penerimaan Risiko karena solusi CloudEndure DR untuk integrasi aplikasi memiliki izin mutasi infrastruktur. Untuk melakukan ini, bekerja dengan manajer pengiriman layanan cloud (CSDM) Anda.

T: Apa batasan penggunaan CloudEndure di akun AMS saya?

Instans replikasi dan konversi cloud endure hanya dapat diluncurkan di subnet yang Anda tunjukkan.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? CloudEndure Bagikan hal berikut melalui korespondensi dua arah RFC:

- Detail Subnet VPC untuk instans Replikasi dan Konversi yang akan diluncurkan.
- Nama Sumber Daya Amazon Kunci KMS (ARN) jika volume EBS dienkripsi.

Gunakan SSP AMS untuk menyediakan AWS CloudHSM di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS CloudHSM kapabilitas secara langsung di akun terkelola AMS Anda. AWS CloudHSM membantu Anda memenuhi persyaratan kepatuhan perusahaan, kontraktual, dan peraturan untuk keamanan data dengan menggunakan instans Modul Keamanan Perangkat Keras (HSM) khusus di cloud. AWS AWS, dan mitra AWS Marketplace, menawarkan berbagai solusi untuk melindungi data sensitif dalam AWS platform, tetapi untuk beberapa aplikasi dan data yang tunduk pada mandat kontrak atau peraturan untuk mengelola kunci kriptografi, perlindungan tambahan mungkin diperlukan. AWS CloudHSM melengkapi solusi perlindungan data yang ada dan memungkinkan Anda untuk melindungi kunci enkripsi Anda di dalamnya HSMs yang dirancang dan divalidasi dengan standar pemerintah untuk manajemen kunci yang aman. AWS CloudHSM memungkinkan Anda untuk membuat, menyimpan, dan mengelola kunci kriptografi dengan aman yang digunakan untuk enkripsi data dengan cara yang kunci hanya dapat diakses oleh Anda. Untuk mempelajari selengkapnya, lihat AWS CloudHSM.

AWS CloudHSM di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS CloudHSM akun AMS saya?

Pemanfaatan di akun AMS Anda adalah proses dua langkah:

1. Minta AWS CloudHSM cluster. Lakukan ini dengan mengirimkan RFC dengan Manajemen | Lainnya | Lainnya | Buat (ct-1e1xtak34nx76) jenis perubahan. Sertakan detail berikut:
   - AWS Wilayah.
   - VPC ID/ARN. Provide a VPC ID/VPC ARN yang berada di akun yang sama dengan RFC yang Anda kirimkan.
   - Tentukan setidaknya dua Availability Zone untuk cluster.
   - ID EC2 instans Amazon yang akan terhubung ke cluster HSM.
2. Akses AWS CloudHSM konsol. Lakukan ini dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_cloudhsm_console_role`

Setelah peran disediakan di akun Anda, Anda harus memasukkannya ke dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS CloudHSM di akun AMS saya?

Akses ke AWS CloudHSM konsol tidak memberi Anda kemampuan untuk membuat, menghentikan, atau memulihkan klaster Anda. Untuk melakukan hal-hal itu, kirimkan Manajemen | Lainnya | Lainnya | Buat jenis perubahan (ct-1e1xtak34nx76) jenis perubahan.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS CloudHSM

Anda harus mengizinkan lalu lintas TCP menggunakan port 2225 melalui EC2 instans Amazon klien dalam VPC, atau menggunakan Direct Connect VPN untuk server on-premise yang menginginkan akses ke cluster HSM. AWS CloudHSM tergantung pada Amazon EC2 untuk grup keamanan dan antarmuka jaringan. Untuk pemantauan atau audit log, HSM mengandalkan CloudTrail (operasi AWS API) dan CloudWatch Log untuk semua aktivitas perangkat HSM lokal.

T: Siapa yang akan menerapkan pembaruan ke AWS CloudHSM klien dan pustaka perangkat lunak terkait?

Anda bertanggung jawab untuk menerapkan pembaruan perpustakaan dan klien. Anda akan ingin memantau halaman riwayat versi CloudHSM untuk rilis, dan kemudian menerapkan pembaruan menggunakan peningkatan klien CloudHSM.

> **Note**
>
> Tambalan perangkat lunak untuk alat HSM selalu diterapkan secara otomatis oleh layanan. AWS CloudHSM

Gunakan SSP AMS untuk menyediakan AWS CodeBuild di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS CodeBuild kapabilitas secara langsung di akun terkelola AMS Anda. AWS CodeBuild adalah layanan integrasi berkelanjutan yang dikelola sepenuhnya yang mengkompilasi kode sumber, menjalankan pengujian, dan menghasilkan paket perangkat lunak yang siap digunakan. Dengan CodeBuild, Anda tidak perlu menyediakan, mengelola, dan menskalakan server build Anda sendiri. CodeBuild menskalakan terus menerus dan memproses beberapa build secara bersamaan, sehingga build Anda tidak dibiarkan menunggu dalam antrian. Anda dapat memulai dengan cepat menggunakan lingkungan build yang dikemas sebelumnya, atau Anda dapat membuat lingkungan build khusus yang menggunakan alat build Anda sendiri. Dengan CodeBuild, Anda dikenakan biaya per menit untuk sumber daya komputasi yang Anda gunakan. Untuk mempelajari selengkapnya, lihat AWS CodeBuild.

> **Note**
>
> Untuk onboard CodeCommit,, CodeBuild CodeDeploy, dan CodePipeline dengan satu RFC, kirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) ubah jenis dan minta tiga layanan:, dan. CodeBuild CodeDeploy CodePipeline Kemudian, ketiga peran,`customer_codebuild_service_role`,`customer_codedeploy_service_role`, dan `aws_code_pipeline_service_role` disediakan di akun Anda. Setelah penyediaan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

CodeBuild di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS CodeBuild akun AMS saya?

Pemanfaatan AWS CodeBuild di akun AMS Anda adalah proses dua langkah:

1. Menyediakan proses build `CodeBuild Service Role` untuk berkoordinasi dengan bucket AWS S3, Amazon, CloudWatch dan grup Log
2. Minta akses ke CodeBuild konsol

Anda dapat meminta agar keduanya disiapkan di akun AMS Anda dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS CodeBuild di akun AMS saya?

Untuk akses administrator AWS CodeBuild konsol, izin dibatasi pada tingkat sumber daya; misalnya, CloudWatch tindakan dibatasi pada sumber daya tertentu dan `iam:PassRole` izin dikontrol.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? CodeBuild

Jika izin IAM tambahan diperlukan untuk peran AWS CodeBuild layanan yang ditentukan, minta izin tersebut melalui permintaan layanan AMS.

Gunakan SSP AMS untuk menyediakan AWS CodeCommit di akun AMS Anda

> **Note**
>
> AWS telah menutup akses pelanggan baru AWS CodeCommit, efektif 25 Juli 2024. AWS CodeCommit Pelanggan yang sudah ada dapat terus menggunakan layanan seperti biasa. AWS terus berinvestasi dalam keamanan, ketersediaan, dan peningkatan kinerja untuk AWS CodeCommit, tetapi kami tidak berencana untuk memperkenalkan fitur baru.
> Untuk memigrasikan CodeCommit repositori AWS Git ke penyedia Git lainnya, hubungi arsitek cloud (CA) Anda untuk mendapatkan panduan. Untuk informasi selengkapnya tentang memigrasi repositori Git Anda, lihat Cara memigrasikan repositori CodeCommit AWS Anda ke penyedia Git lain.

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS CodeCommit kapabilitas secara langsung di akun terkelola AMS Anda. AWS CodeCommit adalah layanan kontrol sumber yang dikelola sepenuhnya yang menampung repositori berbasis Git yang aman. Ini membantu tim untuk berkolaborasi dalam kode dalam ekosistem yang aman dan sangat skalabel.

CodeCommit menghilangkan kebutuhan untuk mengoperasikan sistem kontrol sumber Anda sendiri atau khawatir tentang penskalaan infrastrukturnya. Anda dapat menggunakan CodeCommit untuk menyimpan apa pun dengan aman mulai dari kode sumber hingga binari, dan ini bekerja dengan mulus dengan alat Git Anda yang ada. Untuk mempelajari selengkapnya, lihat AWS CodeCommit.

> **Note**
>
> Untuk onboard CodeCommit,, CodeBuild CodeDeploy, dan CodePipeline dengan satu RFC, kirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) ubah jenis dan minta tiga layanan:, dan. CodeBuild CodeDeploy CodePipeline Kemudian, ketiga peran,`customer_codebuild_service_role`,`customer_codedeploy_service_role`, dan `aws_code_pipeline_service_role` disediakan di akun Anda. Setelah penyediaan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

CodeCommit di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke CodeCommit akun AMS saya?

AWS CodeCommit peran konsol dan akses data dapat diminta melalui pengajuan dua AWS Layanan RFCs, akses konsol, dan akses data:

- Minta akses ke AWS CodeCommit dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_codecommit_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

  Akses data (seperti Pelatihan dan Daftar Entitas) memerlukan terpisah CTs untuk setiap sumber data yang menentukan sumber data S3 (wajib), bucket keluaran (wajib) dan KMS (opsional). Tidak ada batasan untuk penciptaan lapangan AWS CodeCommit kerja selama semua sumber data telah diberikan peran akses. Untuk meminta akses data, kirimkan RFC dengan Manajemen | Lainnya | Lainnya | Buat (ct-1e1xtak34nx76).

T: Apa batasan penggunaan AWS CodeCommit di akun AMS saya?

Fitur pemicu CodeCommit dinonaktifkan mengingat hak terkait untuk membuat topik SNS. Autentikasi langsung terhadap CodeCommit dibatasi, pengguna harus mengautentikasi dengan Credential

Helper. Beberapa perintah KMS juga dibatasi:`kms:Encrypt`,,`kms:Decrypt`,`kms:ReEncrypt`, `kms:GenereteDataKeykms:GenerateDataKeyWithoutPlaintext`, dan`kms:DescribeKey`.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS CodeCommit

Jika bucket S3 dienkripsi dengan kunci KMS, S3 dan KMS harus digunakan. AWS CodeCommit

Gunakan SSP AMS untuk menyediakan AWS CodeDeploy di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS CodeDeploy kapabilitas secara langsung di akun terkelola AMS Anda. AWS CodeDeploy adalah layanan penyebaran terkelola penuh yang mengotomatiskan penerapan perangkat lunak ke berbagai layanan komputasi seperti Amazon EC2, AWS Fargate AWS Lambda, dan server lokal Anda. AWS CodeDeploy membantu Anda merilis fitur baru dengan cepat, membantu Anda menghindari downtime selama penerapan aplikasi, dan menangani kompleksitas memperbarui aplikasi Anda. Anda dapat menggunakan AWS CodeDeploy untuk mengotomatiskan penerapan perangkat lunak, menghilangkan kebutuhan akan operasi manual yang rawan kesalahan. Skala layanan agar sesuai dengan kebutuhan penerapan Anda. Untuk mempelajari selengkapnya, lihat AWS CodeDeploy.

> **Note**
>
> Untuk onboard CodeCommit,, CodeBuild CodeDeploy, dan CodePipeline dengan satu RFC, kirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) ubah jenis dan minta tiga layanan:, dan. CodeBuild CodeDeploy CodePipeline Kemudian, ketiga peran,`customer_codebuild_service_role`,`customer_codedeploy_service_role`, dan `aws_code_pipeline_service_role` disediakan di akun Anda. Setelah menyediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

CodeDeploy di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke CodeDeploy akun AMS saya?

Meminta akses CodeDeploy dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_codedeploy_console_role`

dan. `customer_codedeploy_service_role` Setelah disediakan di akun Anda, Anda harus memasukkan `customer_codedeploy_console_role` peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan CodeDeploy di akun AMS saya?

Saat ini kami hanya mendukung Platform Komputasi sebagai — EC2 Amazon/On-Premises. Blue/Green Penerapan tidak didukung.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? CodeDeploy

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. CodeDeploy

Gunakan SSP AMS untuk menyediakan AWS CodePipeline di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS CodePipeline kapabilitas secara langsung di akun terkelola AMS Anda. AWS CodePipeline adalah layanan pengiriman berkelanjutan yang dikelola sepenuhnya yang membantu Anda mengotomatiskan saluran pipa rilis Anda untuk pembaruan aplikasi dan infrastruktur yang cepat dan andal. CodePipeline mengotomatiskan fase build, test, dan deploy dari proses rilis Anda setiap kali ada perubahan kode, berdasarkan model rilis yang Anda tentukan. Ini memungkinkan Anda untuk dengan cepat dan andal memberikan fitur dan pembaruan. Anda dapat dengan mudah mengintegrasikan AWS CodePipeline dengan layanan pihak ketiga seperti GitHub atau dengan plugin kustom Anda sendiri. Dengan AWS CodePipeline, Anda hanya membayar untuk apa yang Anda gunakan. Tidak ada biaya di muka atau komitmen jangka panjang. Untuk mempelajari selengkapnya, lihat AWS CodePipeline.

> **Note**
>
> Untuk onboard CodeCommit,, CodeBuild CodeDeploy, dan CodePipeline dengan satu RFC, kirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) ubah jenis dan minta tiga layanan:, dan. CodeBuild CodeDeploy CodePipeline Kemudian, ketiga peran,`customer_codebuild_service_role`,`customer_codedeploy_service_role`, dan `aws_code_pipeline_service_role` disediakan di akun Anda. Setelah menyediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda. CodePipeline di AMS tidak mendukung " CloudWatch Acara Amazon" untuk Tahap Sumber karena memerlukan izin yang lebih tinggi untuk membuat peran dan kebijakan layanan, yang melewati model hak istimewa paling sedikit dan proses manajemen perubahan AMS.

CodePipeline di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke CodePipeline akun AMS saya?

Minta akses ke CodePipeline dengan mengirimkan permintaan layanan untuk `customer_code_pipeline_console_role` di akun yang relevan. Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

Pada saat ini, Operasi AMS juga akan menerapkan peran layanan ini di akun Anda: `aws_code_pipeline_service_role_policy`

T: Apa batasan penggunaan CodePipeline di akun AMS saya?

Ya. CodePipeline fitur, tahapan, dan penyedia terbatas pada hal-hal berikut:

1. Tahap Penerapan: Terbatas untuk Amazon S3, dan AWS CodeDeploy
2. Tahap Sumber: Terbatas untuk Amazon S3,, AWS CodeCommit, dan BitBucket GitHub
3. Build Stage: Terbatas untuk AWS CodeBuild, dan Jenkins
4. Tahap Persetujuan: Terbatas untuk Amazon SNS
5. Tahap Uji: Terbatas pada AWS CodeBuild, Jenkins,, Ghost Inspector UI Testing BlazeMeter, Micro StormRunner Focus Load, dan Runscope API Monitoring
6. Panggilan Panggilan: Terbatas untuk Step Functions, dan Lambda

> **Note**
>
> Operasi AMS akan diterapkan `customer_code_pipeline_lambda_policy` di akun Anda; itu harus dilampirkan dengan peran eksekusi Lambda untuk tahap pemanggilan Lambda. Harap berikan nama service/execution peran Lambda yang Anda inginkan agar kebijakan ini ditambahkan. Jika tidak ada service/execution peran Lambda khusus, AMS akan membuat peran baru bernama`customer_code_pipeline_lambda_execution_role`, yang akan menjadi salinan dari peran Lambda`customer_lambda_basic_execution_role`. `customer_code_pipeline_lambda_policy`

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? CodePipeline

AWS layanan yang didukung AWS CodeCommit AWS CodeBuild,, AWS CodeDeploy harus diluncurkan sebelum, atau bersamaan dengan, peluncuran CodePipeline.

Gunakan SSP AMS untuk menyediakan AWS Compute Optimizer di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Compute Optimizer kapabilitas secara langsung di akun terkelola AMS Anda. AWS Compute Optimizer merekomendasikan sumber daya AWS Komputasi yang optimal untuk beban kerja Anda untuk mengurangi biaya dan meningkatkan kinerja dengan menggunakan pembelajaran mesin untuk menganalisis metrik pemanfaatan historis. Komputasi penyediaan berlebih (EC2 Amazon ASGs dan) dapat menyebabkan biaya infrastruktur yang tidak perlu dan komputasi yang kurang penyediaan dapat menyebabkan kinerja aplikasi yang buruk. Compute Optimizer membantu Anda memilih jenis instans EC2 Amazon yang optimal, termasuk yang merupakan bagian dari grup Auto EC2 Scaling Amazon, berdasarkan data pemanfaatan Anda. Untuk mempelajari selengkapnya, lihat AWS Compute Optimizer.

FAQ Compute Optimizer di AWS Managed Services

T: Bagaimana cara meminta akses ke Compute Optimizer di akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_compute_optimizer_readonly_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Compute Optimizer di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh AWS Compute Optimizer tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi untuk menggunakan Compute Optimizer di akun AMS saya?

- Anda harus mengirimkan RFC (Manajemen | Lainnya | Lainnya | Pembaruan) yang mengizinkan AMS Ops untuk mengaktifkan layanan di akun. Selama penerapan, peran terkait layanan (SLR) dibuat untuk memungkinkan pengumpulan metrik dan pembuatan laporan. SLR diberi label "" AWSServiceRoleForComputeOptimizer. Untuk informasi selengkapnya, lihat Menggunakan Peran Tertaut Layanan untuk AWS Compute Optimizer
- CloudWatch metrik harus diaktifkan untuk metrik berikut:
  - Pemanfaatan CPU: Persentase unit EC2 komputasi Amazon yang dialokasikan yang digunakan pada instance. Metrik ini mengidentifikasi daya pemrosesan yang diperlukan untuk menjalankan aplikasi pada instance yang dipilih.

- Pemanfaatan memori: Jumlah memori yang telah digunakan dalam beberapa cara selama periode sampel. Metrik ini mengidentifikasi memori yang diperlukan untuk menjalankan aplikasi pada instance yang dipilih. Pemanfaatan memori dianalisis hanya untuk sumber daya yang memiliki CloudWatch agen terpadu diinstal pada mereka. Untuk informasi lebih lanjut, lihat Mengaktifkan Pemanfaatan Memori dengan CloudWatch Agen (hal. 10).
- Jaringan di: Jumlah byte yang diterima pada semua antarmuka jaringan oleh instance. Metrik ini mengidentifikasi volume trafik jaringan yang masuk ke satu instance.
- Jaringan keluar: Jumlah byte yang dikirim pada semua antarmuka jaringan oleh instance. Metrik ini mengidentifikasi volume trafik jaringan keluar dari satu instance.
- Disk lokal input/output (I/O): Jumlah input/output operasi untuk disk lokal. Metrik ini mengidentifikasi kinerja volume root dari sebuah instance

Gunakan SSP AMS untuk menyediakan AWS DataSync di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS DataSync kapabilitas secara langsung di akun terkelola AMS Anda. AWS DataSync memindahkan sejumlah besar data secara online antara penyimpanan lokal dan Amazon S3, Amazon Elastic File System (Amazon Elastic File System) atau Amazon. FSx Tugas manual yang terkait dengan transfer data dapat memperlambat migrasi dan membebani operasi TI. DataSync menghilangkan atau secara otomatis menangani banyak tugas ini, termasuk pekerjaan penyalinan skrip, penjadwalan dan pemantauan transfer, memvalidasi data, dan mengoptimalkan pemanfaatan jaringan. Agen DataSync perangkat lunak terhubung ke penyimpanan Network File System (NFS) dan Server Message Block (SMB) Anda, sehingga Anda tidak perlu memodifikasi aplikasi Anda. DataSync Dapat mentransfer ratusan terabyte dan jutaan file dengan kecepatan hingga 10 kali lebih cepat daripada alat sumber terbuka, melalui internet atau tautan. AWS Direct Connect Anda dapat menggunakan DataSync untuk memigrasikan kumpulan data aktif atau arsip ke AWS, mentransfer data ke cloud untuk analisis dan pemrosesan tepat waktu, atau mereplikasi data AWS untuk kelangsungan bisnis.

Untuk mempelajari selengkapnya, lihat AWS DataSync.

DataSync di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke DataSync akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_datasync_console_role`

Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

Grup CloudWatch log yang digunakan untuk melakukan streaming log tugas adalah “/aws/datasync”.

T: Apa batasan penggunaan DataSync di akun AMS saya?

Fungsionalitas penuh AWS DataSync tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? DataSync

- Amazon S3 (Nama Sumber Daya ARNs Amazon) diperlukan untuk semua bucket S3 yang terkait dengan DataSync tugas yang akan dilakukan menggunakan peran layanan. DataSync `customer_datasync_service_role`
- Endpoint VPC dan grup keamanan untuk DataSync agen harus diminta dengan RFC dengan Manajemen | Lainnya | Lainnya | Buat (ct-1e1xtak34nx76) mengubah jenis sebelum menggunakan VPC Endpoints.
- AWS DataSync agen berjalan di AMS sebagai alat. AWS DataSync Agen ditambal dan diperbarui oleh layanan; untuk detailnya, lihat AWS DataSync FAQ.
- Untuk meluncurkan AWS DataSync agen, kirimkan RFC dengan Manajemen | Lainnya | Lainnya | Buat (ct-1e1xtak34nx76) jenis perubahan, meminta agen disebarkan. Berikan ID AWS DataSync Amazon EC2 AMI, jenis instans, subnet, grup keamanan; dan referensi EC2 keypair Amazon yang ada atau minta pembuatan keypair baru.

> **Note**
>
> AMS menyediakan AWS DataSync agen secara manual atas nama pelanggan, dan tidak memerlukan proses konsumsi WIGS di Amazon AWS DataSync AMI. EC2

Gunakan SSP AMS untuk menyediakan AWS Device Farm di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Device Farm kapabilitas secara langsung di akun terkelola AMS Anda. AWS Device Farm adalah layanan pengujian aplikasi yang memungkinkan Anda meningkatkan kualitas web dan aplikasi seluler Anda dengan mengujinya di berbagai browser desktop dan perangkat seluler nyata; tanpa harus menyediakan dan mengelola infrastruktur pengujian apa pun. Layanan ini memungkinkan Anda menjalankan pengujian secara bersamaan di beberapa browser desktop atau perangkat nyata untuk

mempercepat eksekusi rangkaian pengujian, serta menghasilkan video dan log untuk membantu Anda mengidentifikasi masalah dengan aplikasi dengan cepat.

Untuk mempelajari selengkapnya, lihat AWS Device Farm.

AWS Device Farm di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke AWS Device Farm akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_devicefarm_role`

Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Device Farm di akun AMS saya?

Akses penuh ke AWS Device Farm layanan disediakan dengan pengecualian menggunakan namespace AMS di tag 'Nama'.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Device Farm

Tidak ada.

Gunakan SSP AMS untuk menyediakan AWS Elastic Disaster Recovery di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Elastic Disaster Recovery kapabilitas secara langsung di akun terkelola AMS Anda. AWS Elastic Disaster Recovery meminimalkan waktu henti dan kehilangan data dengan pemulihan aplikasi berbasis cloud dan lokal yang cepat dan andal menggunakan penyimpanan yang terjangkau, komputasi minimal, dan pemulihan. point-in-time Anda dapat meningkatkan ketahanan TI saat digunakan AWS Elastic Disaster Recovery untuk mereplikasi aplikasi lokal atau berbasis cloud yang berjalan pada sistem operasi yang didukung. Gunakan Konsol Manajemen AWS untuk mengonfigurasi pengaturan replikasi dan peluncuran, memantau replikasi data, dan meluncurkan instance untuk latihan atau pemulihan.

Untuk mempelajari selengkapnya, lihat AWS Elastic Disaster Recovery.

AWS Elastic Disaster Recovery di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke AWS Elastic Disaster Recovery akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_drs_console_role`

Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Elastic Disaster Recovery di akun AMS saya?

Tidak ada batasan untuk digunakan AWS Elastic Disaster Recovery di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Elastic Disaster Recovery

- Setelah Anda memiliki akses ke peran konsol, Anda harus menginisialisasi layanan Elastic Disaster Recovery untuk membuat peran IAM yang diperlukan dalam akun.
  - Anda harus mengirimkan tipe perubahan Manajemen | Aplikasi | Profil instans IAM | Buat (ulasan diperlukan) ubah jenis ct-0ixp4ch2tiu04 RFC untuk membuat tiruan dari profil instans dan melampirkan kebijakan. `customer-mc-ec2-instance-profile` `AWSElasticDisasterRecoveryEc2InstancePolicy` Anda harus menentukan mesin mana yang akan dilampirkan kebijakan baru.
  - Jika instance tidak menggunakan profil instance default, AMS dapat melampirkan `AWSElasticDisasterRecoveryEc2InstancePolicy` melalui otomatisasi.
- Anda harus menggunakan kunci KMS milik pelanggan untuk pemulihan lintas akun. Kunci KMS akun sumber harus diperbarui mengikuti kebijakan untuk mengizinkan akses akun target. Untuk informasi selengkapnya, lihat Berbagi kunci enkripsi EBS dengan akun target.
- Kebijakan kunci KMS harus diperbarui untuk memungkinkan izin `customer_drs_console_role` melihat kebijakan jika Anda tidak ingin beralih peran ke tampilan.
- Untuk pemulihan bencana lintas akun dan lintas wilayah, AMS harus menyiapkan akun sumber dan target sebagai Akun Tepercaya dan menerapkan Failback dan peran dalam ukuran yang tepat.AWS CloudFormation

Gunakan SSP AMS untuk menyediakan AWS Elemental MediaConvert di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Elemental MediaConvert kapabilitas secara langsung di akun terkelola AMS Anda. AWS Elemental MediaConvert adalah layanan transcoding video berbasis file dengan fitur tingkat siaran. Ini

memungkinkan Anda untuk membuat konten video-on-demand (VOD) untuk siaran dan pengiriman multilayar dalam skala besar. Layanan ini menggabungkan kemampuan video dan audio canggih dengan antarmuka dan pay-as-you-go harga layanan web yang sederhana. Dengan AWS Elemental MediaConvert, Anda dapat fokus pada memberikan pengalaman media yang menarik tanpa harus khawatir tentang kompleksitas membangun dan mengoperasikan infrastruktur pemrosesan video Anda sendiri.

Untuk mempelajari selengkapnya, lihat AWS Elemental MediaConvert.

MediaConvert di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke MediaConvert akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_mediaconvert_author_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

Peran kedua akan disediakan,`customer_MediaConvert_Default_Role`, yang digunakan oleh MediaConvert untuk membaca dari bucket S3 sumber dan menulis output ke bucket S3 tujuan, dan juga untuk memanggil gateway API jika Anda memerlukan manajemen hak digital (DRM).

T: Apa batasan penggunaan MediaConvert di akun AMS saya?

Tidak ada batasan untuk penggunaan MediaConvert di AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? MediaConvert

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. MediaConvert

Gunakan SSP AMS untuk menyediakan AWS Elemental MediaLive di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Elemental MediaLive kapabilitas secara langsung di akun terkelola AMS Anda. AWS Elemental MediaLive adalah layanan pemrosesan video langsung tingkat siaran. Ini memungkinkan Anda untuk membuat aliran video berkualitas tinggi untuk pengiriman ke televisi siaran dan perangkat multilayar yang terhubung ke internet, seperti terhubung, tablet, smartphone, dan TVs set-top box. Layanan ini bekerja dengan menyandikan streaming video langsung Anda secara real-time, mengambil sumber video langsung berukuran lebih besar dan mengompresnya menjadi versi yang lebih kecil untuk didistribusikan ke pemirsa Anda. Dengan AWS Elemental MediaLive, Anda dapat dengan mudah mengatur streaming

untuk acara langsung dan saluran 24x7 dengan fitur penyiaran lanjutan, ketersediaan tinggi, dan harga. pay-as-you-go AWS Elemental MediaLive memungkinkan Anda fokus untuk menciptakan pengalaman video langsung yang menarik bagi pemirsa Anda tanpa kerumitan membangun dan mengoperasikan infrastruktur pemrosesan video tingkat siaran.

Untuk mempelajari selengkapnya, lihat AWS Elemental MediaLive.

MediaLive di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke MediaLive akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_medialive_author_role`

Sebagai bagian dari RFC ini, peran kedua diterapkan ke akun Anda; `customer_medialive_service_role` peran, peran ini dapat ditetapkan ke saluran dan input Media Live Anda untuk berinteraksi dengan layanan lain seperti Amazon S3,, dan Log. MediaStore CloudWatch

Setelah peran disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan MediaLive di akun AMS saya?

Tidak ada batasan untuk penggunaan MediaLive di AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? MediaLive

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. MediaLive

Gunakan SSP AMS untuk menyediakan AWS Elemental MediaPackage di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Elemental MediaPackage kapabilitas secara langsung di akun terkelola AMS Anda. AWS Elemental MediaPackage andal mempersiapkan dan melindungi video Anda untuk pengiriman melalui internet. Dari satu input video, AWS Elemental MediaPackage buat aliran video yang diformat untuk diputar di ponsel TVs, komputer, tablet, dan konsol game yang terhubung. Ini membuatnya mudah untuk menerapkan fitur video populer untuk pemirsa (start-over, pause, rewind, dan sebagainya.), Seperti yang biasa ditemukan di. DVRs AWS Elemental MediaPackage juga dapat melindungi konten Anda menggunakan Digital Rights Management (DRM). AWS Elemental MediaPackage skala secara

otomatis sebagai respons terhadap pemuatan, sehingga pemirsa Anda akan selalu mendapatkan pengalaman hebat tanpa Anda harus memprediksi secara akurat terlebih dahulu kapasitas yang Anda perlukan.

Untuk mempelajari selengkapnya, lihat AWS Elemental MediaPackage.

MediaPackage di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke AWS Elemental MediaPackage akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_mediapackage_author_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

Peran kedua akan diberikan,`customer_mediapackage_service_role`, yang dapat ditetapkan ke saluran Media Live Anda dan input untuk berinteraksi dengan layanan lain seperti S3 dan Secrets Manager.

T: Apa batasan penggunaan MediaPackage di akun AMS saya?

Tidak ada batasan untuk penggunaan MediaPackage di AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? MediaPackage

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. MediaPackage

Gunakan SSP AMS untuk menyediakan AWS Elemental MediaStore di akun AMS Anda

> **Note**
>
> Setelah pertimbangan cermat, AWS telah membuat keputusan untuk berhenti MediaStore, efektif 13 November 2025. Jika Anda adalah pelanggan aktif MediaStore, Anda dapat menggunakan MediaStore seperti biasa hingga 13 November 2025, ketika dukungan untuk layanan akan berakhir. Setelah tanggal ini, Anda tidak akan lagi dapat menggunakan MediaStore atau kemampuan apa pun yang disediakan oleh layanan ini.

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Elemental MediaStore kapabilitas secara langsung di akun terkelola AMS Anda. AWS Elemental MediaStore adalah layanan

AWS penyimpanan yang dioptimalkan untuk media. Ini memberi Anda kinerja, konsistensi, dan latensi rendah yang diperlukan untuk mengirimkan konten video streaming langsung. AWS Elemental MediaStore bertindak sebagai toko asal dalam alur kerja video Anda. Kemampuan kinerjanya yang tinggi memenuhi kebutuhan beban kerja pengiriman media yang paling menuntut, dikombinasikan dengan penyimpanan jangka panjang yang hemat biaya. Untuk mempelajari selengkapnya, lihat AWS Elemental MediaStore.

MediaStore di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke MediaStore akun AMS saya?

Meminta akses MediaStore dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_mediastore_author_role` Sebagai bagian dari RFC ini, peran kedua diterapkan ke akun Anda; `MediaStoreAccessLogs` peran, yang digunakan oleh MediaStore layanan untuk log aktivitas CloudWatch, jika Anda memilih untuk mengaktifkan fitur tersebut. Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

Pada saat ini, Operasi AMS juga akan menerapkan peran layanan ini di akun Anda: `aws_code_pipeline_service_role_policy`

T: Apa batasan penggunaan MediaStore di akun AMS saya?

Tidak ada batasan untuk penggunaan MediaStore di AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? MediaStore

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. MediaStore

Gunakan SSP AMS untuk menyediakan AWS Elemental MediaTailor di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Elemental MediaTailor kapabilitas secara langsung di akun terkelola AMS Anda. AWS Elemental MediaTailor memungkinkan penyedia video memasukkan iklan yang ditargetkan secara individual ke dalam aliran video mereka tanpa mengorbankan tingkat siaran. quality-of-service Dengan AWS Elemental MediaTailor, pemirsa video langsung atau sesuai permintaan Anda masing-masing menerima streaming yang menggabungkan konten Anda dengan iklan yang dipersonalisasi untuk mereka. Tetapi tidak seperti solusi iklan yang dipersonalisasi lainnya, dengan seluruh streaming AWS

Elemental MediaTailor Anda — video dan iklan — disampaikan dengan kualitas video tingkat siaran untuk meningkatkan pengalaman bagi pemirsa Anda. AWS Elemental MediaTailor memberikan pelaporan otomatis berdasarkan metrik pengiriman iklan sisi klien dan server, untuk mengukur tayangan iklan dan perilaku pemirsa secara akurat. Anda dapat dengan mudah memonetisasi acara menonton permintaan tinggi yang tidak terduga tanpa menggunakan biaya di muka. AWS Elemental MediaTailor Ini juga meningkatkan tingkat pengiriman iklan, membantu Anda menghasilkan lebih banyak uang dari setiap video, dan bekerja dengan berbagai jaringan pengiriman konten, server keputusan iklan, dan perangkat klien yang lebih luas.

Untuk mempelajari selengkapnya, lihat AWS Elemental MediaTailor.

MediaTailor di FAQ AWS Managed Services

T: Bagaimana cara meminta akses ke MediaTailor akun AMS saya?

Meminta akses MediaTailor dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer-mediatailor-role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan MediaTailor di akun AMS saya?

Tidak ada batasan untuk penggunaan MediaTailor di AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? MediaTailor

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. MediaTailor

Gunakan SSP AMS untuk menyediakan AWS Global Accelerator di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas Global Accelerator secara langsung di akun terkelola AMS Anda. Global Accelerator adalah layanan lapisan jaringan di mana Anda membuat akselerator untuk meningkatkan ketersediaan dan kinerja untuk aplikasi internet yang digunakan oleh khalayak global. Untuk mempelajari lebih lanjut, lihat Akselerator Global.

FAQ Akselerator Global di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta Global Accelerator untuk disiapkan di akun AMS saya?

Meminta akses melalui pengajuan AWS Layanan RFC (Manajemen | layanan | AWS Layanan Penyediaan Mandiri). Melalui RFC ini, peran IAM berikut akan disediakan di akun Anda:. `customer_global_accelerator_console_role` Setelah disediakan di akun Anda, Anda harus mengaktifkan peran konsol dalam solusi federasi Anda.

T: Apa batasan penggunaan Global Accelerator di akun AMS saya?

Global Accelerator adalah layanan global yang mendukung titik akhir di beberapa AWS Wilayah, yang tercantum dalam Tabel AWS Wilayah.

T: Apa prasyarat atau dependensi untuk menggunakan Global Accelerator di akun AMS saya?

Saat Anda mengatur akselerator dengan Global Accelerator, Anda mengaitkan alamat IP statis ke titik akhir regional di satu atau beberapa Wilayah. AWS Untuk akselerator standar, titik akhir adalah Network Load Balancer, Application Load Balancer, EC2 instans Amazon, atau alamat IP Elastis. Untuk akselerator perutean khusus, titik akhir adalah subnet virtual private cloud (VPC) dengan satu atau beberapa instance. EC2

Gunakan SSP AMS untuk menyediakan AWS Glue di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Glue kapabilitas secara langsung di akun terkelola AMS Anda. AWS Glue adalah layanan ekstrak, transformasi, dan pemuatan (ETL) yang dikelola sepenuhnya yang membantu Anda mempersiapkan dan memuat data Anda untuk analitik. Anda dapat membuat dan menjalankan pekerjaan ETL dengan beberapa klik di file. Konsol Manajemen AWS Anda menunjuk AWS Glue ke data yang disimpan AWS, dan AWS Glue menemukan data Anda serta menyimpan metadata terkait (misalnya definisi tabel dan skema) di. AWS Glue Data Catalog Setelah dikatalogkan, data Anda segera dapat dicari, dapat ditanyakan, dan tersedia untuk tindakan ETL. Untuk mempelajari selengkapnya, lihat AWS Glue.

AWS Glue di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara saya meminta AWS Glue untuk disiapkan di akun AMS saya?

Meminta akses AWS Glue dengan mengirimkan RFC dengan Manajemen | Layanan AWS | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:

- `customer_glue_console_role`
- `customer_glue_service_role`

Peran sebelumnya mencakup kebijakan terlampir berikut:

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

Setelah peran disediakan di akun Anda, Anda harus memasukkannya ke dalam solusi federasi Anda.

Untuk akses ke titik akhir Crawler, Jobs, dan Development (peran yang diperlukan untuk kasus penggunaan tertentu), kirimkan RFC dengan Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat entitas atau kebijakan (ct-3dpd8mdd9jn1r).

T: Apa batasan penggunaan AWS Glue di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh AWS Glue tersedia di akun AMS Anda. Untuk lingkungan interaktif tempat Anda dapat membuat dan menguji skrip ETL, gunakan Notebook di Studio. AWS Glue AWS Glue Sesi Interaktif dan Notebook Job adalah fitur tanpa server AWS Glue yang dapat Anda gunakan AWS Glue dan yang memanfaatkan peran layanan. AWS Glue

AWS Glue sebelum 2.0: AWS Glue Notebook adalah sumber daya yang tidak dikelola yang meluncurkan instans EC2 Amazon di akun. Ini adalah praktik terbaik untuk meluncurkan EC2 instans Amazon Anda sendiri dan menginstal perangkat lunak yang diperlukan untuk mendukung lingkungan dan pengembangan notebook. Untuk informasi lebih lanjut, lihat Tutorial: Mengatur Notebook Apache Zeppelin Lokal untuk Menguji dan Mendebug Skrip ETL dan Menggunakan Titik Akhir Pengembangan untuk Mengembangkan Skrip.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Glue

AWS Glue memiliki ketergantungan pada Amazon S3 CloudWatch,, CloudWatch dan Log. Dependensi transitif bervariasi berdasarkan sumber data, dan fitur AWS Glue layanan lainnya mungkin berinteraksi dengannya (contoh: Amazon Redshift, Amazon RDS, Athena).

Gunakan SSP AMS untuk menyediakan AWS Lake Formation di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Lake Formation kapabilitas secara langsung di akun terkelola AMS Anda. AWS Lake Formation adalah layanan

yang membuatnya mudah untuk mengatur danau data yang aman dalam beberapa hari. Sebuah danau data adalah repositori terpusat, dikurasi, dan aman yang menyimpan semua data Anda, baik dalam bentuk aslinya dan yang disiapkan untuk analisis. Danau data memungkinkan Anda untuk menguraikan silo data dan menggabungkan berbagai jenis analitik untuk mendapatkan wawasan dan memandu keputusan bisnis yang lebih baik.

Membuat danau data dengan Lake Formation sesederhana mendefinisikan sumber data serta kebijakan akses dan keamanan data apa yang ingin Anda terapkan. Lake Formation kemudian membantu Anda mengumpulkan dan membuat katalog data dari database dan penyimpanan objek, memindahkan data ke danau data Amazon S3 baru Anda, membersihkan dan mengklasifikasikan data Anda menggunakan algoritma machine learning, dan mengamankan akses ke data sensitif Anda. Pengguna Anda dapat mengakses katalog data terpusat (untuk detailnya, lihat AWS Glue FAQ) yang menjelaskan kumpulan data yang tersedia dan penggunaannya yang sesuai. Pengguna Anda kemudian memanfaatkan kumpulan data ini dengan pilihan layanan analisis dan pembelajaran mesin mereka, seperti Amazon Redshift, Amazon Athena, dan (dalam versi beta) Amazon EMR untuk Apache Spark. Lake Formation dibangun di atas kemampuan yang tersedia di AWS Glue.

Untuk mempelajari selengkapnya, lihat AWS Lake Formation.

FAQ Lake Formation di AWS Managed Services

T: Bagaimana cara meminta akses ke AWS Lake Formation akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_lakeformation_data_analyst_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

Selain itu, dua peran berikut adalah opsional:

- `customer_lakeformation_admin_role`
- `customer_lakeformation_workflow_role`

Untuk izin admin, Anda dapat memilih untuk onboard peran `customer_lakeformation_admin_role` sebagai bagian dari jenis perubahan SSPS yang sama (ct-3qe6io8t6jtny).

Jika Anda ingin membuat Cetak Biru di AWS Lake Formation Konsol, Anda harus mengirimkan Manajemen | Lainnya | RFC lainnya (ct-1e1xtak34nx76) untuk menyebarkan.

`customer_lakeformation_workflow_role` Di RFC, Anda harus memberikan nama bucket S3 jika bucket adalah sumber saat Blueprints dibuat. Bucket S3 berlaku jika tipe Blueprint adalah, Classic Load Balancer Load AWS CloudTrail Balancer atau Application Load Balancer Load Balancer.

T: Apa batasan penggunaan AWS Lake Formation di akun AMS saya?

Fungsionalitas penuh dari Lake Formation tersedia di AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Lake Formation

Lake Formation terintegrasi dengan AWS Glue layanan, oleh karena itu AWS Glue pengguna hanya dapat mengakses database dan tabel di mana mereka memiliki izin Lake Formation. Selain itu, pengguna AWS Athena dan Amazon Redshift hanya dapat menanyakan database dan tabel AWS Glue tempat mereka memiliki izin Lake Formation.

Gunakan SSP AMS untuk menyediakan AWS Lambda di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Lambda kapabilitas secara langsung di akun terkelola AMS Anda. AWS Lambda memungkinkan Anda menjalankan kode tanpa menyediakan atau mengelola server. Anda hanya membayar untuk waktu komputasi yang Anda konsumsi, tidak ada biaya ketika kode Anda tidak berjalan. Dengan Lambda, Anda dapat menjalankan kode untuk hampir semua jenis aplikasi atau layanan back-end, semuanya tanpa administrasi. Unggah kode Anda dan Lambda menangani semua yang diperlukan untuk menjalankan dan menskalakan kode Anda dengan ketersediaan tinggi. Anda dapat mengatur kode Anda untuk secara otomatis memicu dari AWS layanan lain, atau memanggilnya langsung dari Web atau aplikasi seluler apa pun. Untuk mempelajari selengkapnya, lihat AWS Lambda.

Lambda di AWS Managed Services FAQ

T: Bagaimana cara meminta akses ke AWS Lambda akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_lambda_admin_role` dan. `customer_lambda_basic_execution_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Lambda di akun AMS saya?

- Fungsi Lambda dirancang untuk dipanggil oleh sumber peristiwa. Untuk daftar layanan yang dapat digunakan sebagai sumber peristiwa Lambda, lihat Menggunakan AWS Lambda dengan Layanan Lain. Tidak semua layanan ini saat ini tersedia di akun AMS. Jika Anda memerlukan layanan yang tidak tersedia, kerjakan dengan AMS CSDM Anda untuk mengajukan pengecualian.
- Secara default AMS memberi Anda peran inisiasi Lambda dasar yang berisi izin `AWSLambdaBasicExecutionRole` dan `AWSXrayWriteOnlyAccess` izin; untuk selengkapnya, lihat Peran Inisiasi.AWS Lambda Jika Anda memerlukan izin tambahan, seperti kemampuan untuk menyediakan fungsi Lambda dalam VPC AMS Anda, kirimkan RFC ke Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) tipe perubahan.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Lambda

Tidak ada prasyarat atau dependensi untuk memulai AWS Lambda; Namun, tergantung pada kasus penggunaan spesifik Anda, Anda mungkin memerlukan akses ke AWS layanan lain untuk membuat sumber peristiwa, atau izin tambahan untuk fungsi Anda untuk melakukan berbagai tindakan. Jika izin tambahan diperlukan, kirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (perlu ditinjau) jenis perubahan (ct-3qe6io8t6jtny).

T: Apa yang harus saya lakukan untuk menjalankan fungsi Lambda di salah satu akun saya?

Untuk menerapkan fungsi Lambda di akun inti, gunakan pedoman berikut:

- Pastikan SSPS untuk AWS Lambda onboard.
- Tidak ada batasan khusus yang melarang penerapan ini di bawah tanggung jawab AMS, selama sumber daya AMS Anda dilindungi dan sesuai.
- Jika Anda ingin AMS membuat fungsi Lambda, maka Anda harus terlebih dahulu menggunakan peran SSPS yang disediakan. AWS Lambda Kemudian, jika Anda masih menginginkan bantuan AMS untuk menyebarkan atau mendukung fungsi tersebut, hubungi CA Anda dan mulai proses di luar cakupan (OOS).

Gunakan SSP AMS untuk menyediakan AWS License Manager di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS License Manager kapabilitas secara langsung di akun terkelola AMS Anda. AWS License Manager terintegrasi dengan AWS layanan untuk menyederhanakan pengelolaan lisensi di beberapa AWS akun, katalog TI, dan lokal, melalui satu akun. AWS AWS License Manager memungkinkan administrator membuat aturan

lisensi khusus yang meniru persyaratan perjanjian lisensi mereka, dan kemudian memberlakukan aturan ini ketika instance Amazon diluncurkan. EC2 Aturan AWS License Manager memungkinkan Anda membatasi pelanggaran lisensi dengan menghentikan peluncuran instans secara fisik atau dengan memberi tahu administrator tentang pelanggaran tersebut. Untuk mempelajari selengkapnya, lihat AWS License Manager.

License Manager di AWS Managed Services FAQ

Pertanyaan dan jawaban umum:

T: Bagaimana cara saya meminta AWS License Manager untuk disiapkan di akun AMS saya?

Minta akses ke AWS License Manager dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_license_manager_role` Setelah peran IAM License Manager disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS License Manager di akun AMS saya?

Anda dapat mengaitkan AWS License Manager aturan dengan aturan yang AMIs Anda miliki (difilter di bawah “Dimiliki oleh saya”). Jika Anda memilih untuk menerapkan asosiasi batas ke AMI (contoh: hanya dapat mendukung 100 vCPU dari AMI ini) dan menghabiskan batasnya, peluncuran future dengan AMI tersebut diblokir dan mengembalikan kesalahan yang menyatakan “Tidak ada lisensi yang tersedia.” Ini adalah perilaku yang dimaksudkan dari layanan ini (tidak mengizinkan kelelahan lisensi). Jika Anda kehabisan batas tetapi perlu meluncurkan AMI lagi, Anda harus mengubah aturan yang dikonfigurasi AWS License Manager.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS License Manager

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS License Manager

Gunakan SSP AMS untuk menyediakan AWS Migration Hub di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Migration Hub kapabilitas secara langsung di akun terkelola AMS Anda. AWS Migration Hub menyediakan satu lokasi di mana Anda dapat melacak kemajuan migrasi aplikasi di beberapa solusi AWS dan mitra. Menggunakan Migration Hub memungkinkan Anda memilih alat migrasi AWS dan mitra yang paling sesuai dengan kebutuhan Anda, sekaligus memberikan visibilitas ke status migrasi di seluruh

portofolio aplikasi Anda. Migration Hub juga menyediakan metrik dan kemajuan utama untuk aplikasi individual, terlepas dari alat mana yang digunakan untuk memigrasikannya. Ini memungkinkan Anda untuk dengan cepat mendapatkan pembaruan kemajuan di semua migrasi Anda, dengan mudah mengidentifikasi dan memecahkan masalah apa pun, dan mengurangi keseluruhan waktu dan upaya yang dihabiskan untuk proyek migrasi Anda. Untuk mempelajari selengkapnya, lihat AWS Migration Hub.

FAQ Migration Hub di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Migration Hub di akun AMS saya?

Minta akses ke Migration Hub dengan mengirimkan RFC dengan Management | AWS service | Self-provisioned service | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_migrationhub_author_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk Migration Hub?

Tidak ada.

T: Apa prasyarat untuk mengaktifkan Migration Hub?

Tidak ada prasyarat untuk mulai menggunakan Migration Hub di akun AMS Anda. Namun, izin di luar Migration Hub mungkin diperlukan selama pengelolaan layanan, seperti menulis izin ke Amazon S3 untuk mengunggah informasi server.

Gunakan SSP AMS untuk menyediakan AWS Outposts di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Outposts kapabilitas secara langsung di akun terkelola AMS Anda. AWS Outposts adalah layanan yang dikelola sepenuhnya yang memperluas AWS infrastruktur, AWS layanan APIs, dan alat ke hampir semua pusat data, ruang co-lokasi, atau fasilitas lokal untuk pengalaman hybrid yang konsisten. AWS Outposts baik untuk beban kerja yang memerlukan akses latensi rendah ke sistem lokal, pemrosesan data lokal, atau penyimpanan data lokal. Untuk mempelajari selengkapnya, lihat AWS Outposts.

AWS Outposts di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara saya meminta AWS Outposts untuk disiapkan di akun AMS saya?

Minta akses ke AWS Outposts dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_outposts_role` Setelah peran disediakan di akun Anda, Anda harus memasukkannya ke dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Outposts di akun AMS saya?

Tidak ada batasan untuk penggunaan AWS Outposts di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Outposts

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS Outposts

Gunakan SSP AMS untuk menyediakan AWS Resilience Hub di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Resilience Hub kapabilitas secara langsung di akun terkelola AMS Anda. AWS Resilience Hub membantu Anda secara proaktif mempersiapkan dan melindungi AWS aplikasi Anda dari gangguan. Resilience Hub menawarkan penilaian dan validasi ketahanan yang terintegrasi ke dalam siklus hidup pengembangan perangkat lunak Anda untuk mengungkap kelemahan ketahanan. Resilience Hub membantu Anda memperkirakan apakah aplikasi Anda dapat memenuhi target tujuan waktu pemulihan (RTO) dan tujuan titik pemulihan (RPO) atau tidak, dan membantu menyelesaikan masalah sebelum dirilis ke produksi. Setelah menerapkan AWS aplikasi ke dalam produksi, Anda dapat menggunakan Resilience Hub untuk terus melacak postur ketahanan aplikasi Anda. Jika terjadi pemadaman, Resilience Hub mengirimkan pemberitahuan ke operator untuk meluncurkan proses pemulihan terkait.

AWS Resilience Hub di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Resilience Hub akun AMS saya?

Minta akses ke Resilience Hub dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran dan kebijakan IAM berikut ke akun Anda:

IAM role

- `customer_resiliencehub_console_role`
- `customer_resiliencehub_service_role`

Kebijakan

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

Setelah peran disediakan di akun Anda, Anda harus memasukkan peran tersebut `customer_resiliencehub_console_role` dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Resilience Hub di akun AMS saya?

Tidak ada batasan. Fungsionalitas penuh Resilience Hub tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Resilience Hub

Tidak ada prasyarat atau dependensi untuk menggunakan Resilience Hub di akun AMS Anda.

Gunakan SSP AMS untuk menyediakan AWS Secrets Manager di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Secrets Manager kapabilitas secara langsung di akun terkelola AMS Anda. AWS Secrets Manager membantu Anda melindungi rahasia yang diperlukan untuk mengakses aplikasi, layanan, dan sumber daya TI Anda. Layanan ini memungkinkan Anda untuk dengan mudah memutar, mengelola, dan mengambil kredenal database, kunci API, dan rahasia lainnya sepanjang siklus hidupnya. Pengguna dan aplikasi mengambil rahasia dengan panggilan ke Secrets Manager APIs, menghilangkan kebutuhan untuk hardcode informasi sensitif dalam teks biasa. Secrets Manager menawarkan rotasi rahasia dengan integrasi bawaan untuk Amazon RDS, Amazon Redshift, dan Amazon DocumentDB. Selain itu, layanan ini dapat diperluas ke jenis rahasia lainnya, termasuk kunci API dan OAuth token. Untuk mempelajari selengkapnya, lihat AWS Secrets Manager.

> **Note**
>
> Secara default, operator AMS dapat mengakses rahasia AWS Secrets Manager yang dienkripsi menggunakan AWS KMS kunci default akun (CMK). Jika Anda ingin rahasia Anda

tidak dapat diakses oleh Operasi AMS, gunakan CMK kustom, dengan kebijakan kunci AWS Key Management Service (AWS KMS) yang menentukan izin yang sesuai dengan data yang disimpan dalam rahasia.

FAQ Secrets Manager di AWS Managed Services

T: Bagaimana cara meminta akses ke AWS Secrets Manager akun AMS saya?

Minta akses ke Secrets Manager dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-3qe6io8t6jtny) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_secrets_manager_console_role` dan. `customer-rotate-secrets-lambda-role` `customer_secrets_manager_console_role`Ini digunakan sebagai peran Admin untuk menyediakan dan mengelola rahasia, dan `customer-rotate-secrets-lambda-role` digunakan sebagai peran eksekusi Lambda untuk fungsi Lambda yang memutar rahasia. Setelah disediakan di akun Anda, Anda harus memasukkan `customer_secrets_manager_console_role` peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Secrets Manager di akun AMS saya?

Fungsionalitas penuh AWS Secrets Manager tersedia di akun AMS Anda, bersama dengan fungsi rotasi otomatis rahasia. Namun, perhatikan bahwa mengatur rotasi Anda menggunakan 'Buat fungsi Lambda baru untuk melakukan rotasi 'tidak didukung karena memerlukan izin yang lebih tinggi untuk membuat CloudFormation tumpukan (Peran IAM dan pembuatan fungsi Lambda), yang melewati proses Manajemen Perubahan. AMS Advanced hanya mendukung 'Gunakan fungsi Lambda yang ada untuk melakukan rotasi 'di mana Anda mengelola fungsi Lambda untuk memutar rahasia menggunakan peran Admin Lambda SSPS. AWS AMS Advanced tidak membuat atau mengelola Lambda untuk memutar rahasia.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Secrets Manager

Ruang nama berikut dicadangkan untuk digunakan oleh AMS dan tidak tersedia sebagai bagian dari akses langsung ke: AWS Secrets Manager

- arn:aws:secretsmanager: *:*:rahasia:ams-shared/*
- arn:aws:secretsmanager: *:*:rahasia:dibagikan pelanggan/*
- arn:aws:secretsmanager: *:*:rahasia:ams/*

Berbagi kunci menggunakan Secrets Manager (AMS SSPS)

Berbagi rahasia dengan AMS dalam teks biasa RFC, permintaan layanan, atau laporan insiden, menghasilkan insiden pengungkapan informasi dan AMS menyunting informasi tersebut dari kasus dan meminta Anda membuat ulang kunci.

Anda dapat menggunakan AWS Secrets Manager(Secrets Manager) di bawah namespace ini,. `customer-shared`

Berbagi Kunci menggunakan Secrets Manager FAQ

T: Jenis rahasia apa yang harus dibagikan menggunakan Secrets Manager?

Beberapa contoh adalah kunci yang telah dibagikan sebelumnya untuk pembuatan VPN, kunci rahasia seperti kunci Otentikasi (IAM, SSH), kunci Lisensi, dan Kata Sandi.

T: Bagaimana cara berbagi kunci dengan AMS menggunakan Secrets Manager?

1. Masuk ke konsol AWS Manajemen menggunakan akses federasi Anda dan peran yang sesuai:

   untuk SALZ, `Customer_ReadOnly_Role`

   untuk MALZ,`AWSManagedServicesChangeManagementRole`.
2. Arahkan ke AWS Secrets Manager konsol dan klik Simpan rahasia baru.
3. Pilih Tipe rahasia lainnya.
4. Masukkan nilai rahasia sebagai teks biasa dan gunakan enkripsi KMS default. Klik Berikutnya.
5. Masukkan nama rahasia dan deskripsi, nama selalu dimulai dengan customer-shared/. Misalnya yang dibagikan pelanggan/mykey2022. Klik Berikutnya.
6. Biarkan rotasi otomatis dinonaktifkan, Klik Berikutnya.
7. Tinjau dan klik Store untuk menyimpan rahasia.
8. Balas kepada kami dengan nama rahasia melalui permintaan Layanan, RFC, atau laporan insiden, sehingga kami dapat mengidentifikasi dan mengambil rahasia tersebut.

T: Izin apa yang diperlukan untuk berbagi kunci menggunakan Secrets Manager?

SALZ: Cari kebijakan IAM `customer_secrets_manager_shared_policy` terkelola dan verifikasi bahwa dokumen kebijakan sama dengan yang dilampirkan dalam langkah-langkah

pembuatan di bawah ini. Konfirmasikan bahwa kebijakan tersebut dilampirkan pada Peran IAM berikut:`Customer_ReadOnly_Role`.

MALZ: Validasi bahwa`AMSSecretsManagerSharedPolicy`, dilampirkan ke `AWSManagedServicesChangeManagementRole` peran yang memungkinkan Anda `GetSecretValue` melakukan tindakan di namespace. `ams-shared`

Contoh:

```
{
 "Action": "secretsmanager:*",
 "Resource": [
 "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
 "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
 ],
 "Effect": "Allow",
 "Sid": "AllowAccessToSharedNameSpaces"
 }
```

> **Note**
>
> Izin yang diperlukan diberikan saat Anda menambahkan AWS Secrets Manager sebagai layanan yang disediakan layanan mandiri.

Gunakan SSP AMS untuk menyediakan AWS Security Hub CSPM di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Security Hub CSPM kapabilitas secara langsung di akun terkelola AMS Anda. AWS Security Hub CSPM memberi Anda pandangan komprehensif tentang keadaan keamanan Anda di dalam AWS dan kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub memusatkan dan memprioritaskan temuan keamanan dan kepatuhan dari seluruh AWS akun, layanan, dan mitra pihak ketiga yang didukung untuk membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi. Untuk mempelajari selengkapnya, lihat AWS Security Hub CSPM.

FAQ Security Hub di AWS Managed Services

T: Bagaimana cara meminta akses ke AWS Security Hub CSPM akun AMS saya?

Meminta akses ke Security Hub dengan mengirimkan RFC dengan Management | AWS service | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_securityhub_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan Security Hub di akun AMS saya?

Fungsionalitas pengarsipan telah dicatat sebagai potensi keamanan dan risiko operasional dan telah dibatasi sebagai bagian dari peran Keamanan layanan yang disediakan sendiri.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Security Hub CSPM

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS Security Hub CSPM

Gunakan SSP AMS untuk menyediakan AWS Service Catalog AppRegistry di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AppRegistry kapabilitas secara langsung di akun terkelola AMS Anda. AppRegistry memungkinkan pencarian aplikasi, pelaporan, dan tindakan manajemen dari lokasi pusat. Pembangun jarang membuat aplikasi dalam satu AWS akun. Mereka biasanya memisahkan sumber daya aplikasi berdasarkan fase siklus hidup, seperti pengembangan, pengujian, dan produksi. AppRegistry memungkinkan Anda untuk mengelompokkan dan melihat semua koleksi sumber daya Anda di seluruh AWS akun yang Anda tentukan.

Dengan AppRegistry, Anda dapat menyimpan AWS aplikasi Anda, kumpulan sumber daya yang terkait dengan aplikasi Anda, dan grup atribut aplikasi. Untuk mempelajari lebih lanjut, lihat Apa itu AppRegistry.

FAQ: AWS Service Catalog AppRegistry di AMS

T: Bagaimana cara meminta akses ke AWS Service Catalog AppRegistry akun AMS saya?

Minta akses ke AppRegistry dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (diperlukan ulasan) (ct-3qe6io8t6jtny) mengubah jenis. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer-appregistry-console-role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Service Catalog AppRegistry di akun AMS saya?

Akses penuh ke AppRegistry layanan disediakan dengan pengecualian menggunakan namespace AMS di `'Name'` tag.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Service Catalog AppRegistry

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AppRegistry

Gunakan SSP AMS untuk menyediakan AWS Shield Advanced di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Shield Advanced kapabilitas secara langsung di akun terkelola AMS Anda. AWS Shield Advanced adalah layanan perlindungan Distributed Denial of Service (DDoS) terkelola yang melindungi aplikasi yang berjalan. AWS Shield Advanced menyediakan deteksi selalu aktif dan mitigasi inline otomatis yang meminimalkan waktu henti dan latensi aplikasi, sehingga tidak perlu menggunakan Support untuk mendapatkan manfaat dari perlindungan S. AWS DDo Ada dua tingkatan AWS Shield - Standard dan Advanced; AMS menawarkan Shield Advanced. Untuk mempelajari selengkapnya, lihat Shield Advanced.

Semua AWS pelanggan mendapat manfaat dari perlindungan otomatis AWS Shield Standard, tanpa biaya tambahan. AWS Shield Standard bertahan terhadap serangan lapisan DDo S jaringan dan transportasi yang paling umum, sering terjadi, yang menargetkan situs web atau aplikasi Anda. Saat Anda menggunakan AWS Shield Standard Amazon CloudFront dan Amazon Route 53, Anda menerima perlindungan ketersediaan komprehensif terhadap semua serangan infrastruktur yang diketahui (Layer 3 dan 4).

Untuk tingkat perlindungan yang lebih tinggi terhadap serangan yang menargetkan aplikasi Anda yang berjalan di Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), CloudFront Amazon, dan AWS Global Accelerator Amazon Route 53 resource, Anda dapat berlangganan. AWS Shield Advanced

Selain perlindungan lapisan jaringan dan transport yang disertakan AWS Shield Standard, AWS Shield Advanced menyediakan deteksi dan mitigasi tambahan terhadap serangan DDo S yang besar dan canggih, visibilitas mendekati real-time ke dalam serangan, dan integrasi dengan AWS WAF, firewall aplikasi web. AWS Shield Advanced juga memberi Anda akses 24x7 ke Tim AWS Shield Response (SRT) dan perlindungan terhadap lonjakan terkait DDo S di Amazon Elastic Compute Cloud (Amazon), EC2 Elastic Load Balancing (Elastic Load Balancing), Amazon, CloudFront dan Amazon Route 53. AWS Global Accelerator

Pertanyaan Umum tentang Shield Advanced di AWS Managed Services

T: Bagaimana cara meminta akses ke Shield Advanced di akun AMS saya?

Minta akses ke Shield Advanced dengan mengirimkan RFC dengan Management | AWS service | Self-provisioned service | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda: `customer_shield_role` dan. `aws_drt_shield_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

Setelah peran diterapkan ke akun Anda, Anda dapat menggunakan `customer_shield_role` untuk mengonfirmasi langganan Anda AWS Shield Advanced di akun Anda.

> **Note**
>
> Perhatikan bahwa ada biaya bulanan dan komitmen satu tahun yang terkait dengan penggunaan. AWS Shield Advanced Selain itu, menggunakan AWS Shield Advanced AMS memberi wewenang kepada AMS untuk meningkatkan ke AWS Shield (SRT), yang dapat membuat perubahan pada aturan firewall (AWS WAF) aplikasi web Anda selama insiden penolakan layanan terdistribusi yang meningkat. DDo Perubahan ini akan dilakukan dalam koordinasi dengan AMS.

T: Apa batasan penggunaan Shield Advanced di akun AMS saya?

Meskipun bukan pembatasan, Anda harus memahami bahwa menggunakan Shield Advanced menyebarkan`aws_drt_shield_role`, yang memungkinkan AWS Shield tim (SRT) untuk membuat perubahan darurat pada AWS WAF aturan di dalam akun AMS selama insiden S meningkat DDo. Ini direkomendasikan oleh AMS untuk remediasi tercepat serangan DDo S, dan akan terjadi setelah eskalasi AMS ke SRT.

T: Apa prasyarat atau dependensi untuk menggunakan Shield Advanced di akun AMS saya?

Tidak ada prasyarat atau dependensi untuk menggunakan Shield Advanced di akun AMS Anda.

Gunakan SSP AMS untuk menyediakan AWS Snowball Edge di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan Snowball Edge secara langsung di akun terkelola AMS Anda. Snowball Edge adalah solusi transportasi

data skala petabyte yang menggunakan perangkat yang dirancang agar aman, untuk mentransfer sejumlah besar data ke dalam dan keluar dari Cloud. AWS Snowball Edge mengatasi tantangan umum dengan transfer data skala besar termasuk biaya jaringan yang tinggi, waktu transfer yang lama, dan masalah keamanan. Anda dapat menggunakan Snowball Edge untuk memigrasikan data analitik, data genomik, pustaka video, repositori gambar, cadangan, dan untuk mengarsipkan bagian dari shutdown pusat data, penggantian tape, atau proyek migrasi aplikasi. Mentransfer data dengan Snowball Edge sederhana, cepat, lebih aman, dan hanya seperlima biaya transfer data melalui Internet berkecepatan tinggi.

Dengan Snowball Edge, Anda tidak perlu menulis kode apa pun atau membeli perangkat keras apa pun untuk mentransfer data Anda. Mulailah dengan menggunakan Konsol AWS Manajemen untuk Membuat Pekerjaan Impor untuk Snowball, dan perangkat Snowball akan dikirimkan secara otomatis kepada Anda. Setelah tiba, pasang perangkat ke jaringan lokal Anda, unduh dan jalankan Klien Snowball ("Klien") untuk membuat koneksi, dan kemudian gunakan Klien untuk memilih direktori file yang ingin Anda transfer ke perangkat. Klien kemudian mengenkripsi dan mentransfer file ke perangkat dengan kecepatan tinggi. Setelah transfer selesai dan perangkat siap dikembalikan, label pengiriman E Ink secara otomatis diperbarui dan Anda dapat melacak status pekerjaan dengan Amazon Simple Notification Service (Amazon SNS), pesan teks, atau langsung di Konsol. Untuk mempelajari selengkapnya, lihat AWS Snowball Edge.

FAQ Snowball Edge di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Snowball Edge akun AMS saya?

Implementasi Snowball Edge di AMS adalah proses dua langkah:

1. Kirim Manajemen | Lainnya | Lainnya | Buat (ct-1e1xtak34nx76) ubah jenis dan minta peran layanan untuk Snowball Edge untuk Akun AMS Anda.
2. Minta akses pengguna dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:`customer_snowball_console_role`,`customer_snowball_export_role`, dan. `customer_snowball_import_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Snowball Edge di akun AMS saya?

Fungsionalitas penuh AWS Snowball Edge tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Snowball Edge

Anda harus memiliki akun peran layanan seperti yang disebutkan di atas.

Gunakan SSP AMS untuk menyediakan AWS Step Functions di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Step Functions kapabilitas secara langsung di akun terkelola AMS Anda. AWS Step Functions adalah layanan Web yang memungkinkan Anda untuk mengoordinasikan komponen aplikasi terdistribusi dan layanan mikro dengan menggunakan alur kerja visual. Anda membangun aplikasi dari komponen individu yang masing-masing menjalankan fungsi diskrit, atau tugas, memungkinkan Anda untuk menskalakan dan mengubah aplikasi dengan cepat. Step Functions menyediakan cara yang dapat diandalkan untuk mengkoordinasikan komponen dan langkah melalui fungsi aplikasi Anda. Step Functions menawarkan konsol grafis untuk memvisualisasikan komponen aplikasi Anda sebagai serangkaian langkah. Ini secara otomatis memicu dan melacak setiap langkah, dan mencoba lagi ketika ada kesalahan, sehingga aplikasi Anda berjalan secara berurutan dan seperti yang diharapkan, setiap saat. Step Functions mencatat status setiap langkah, jadi ketika terjadi kesalahan, Anda dapat mendiagnosis dan melakukan debug masalah dengan cepat. Untuk mempelajari selengkapnya, lihat AWS Step Functions.

FAQ Step Functions di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Step Functions akun AMS saya?

Minta akses ke AWS Step Functions dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_step_functions_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Step Functions di akun AMS saya?

Fungsionalitas penuh AWS Step Functions tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Step Functions

Saat runtime, peran yang digunakan oleh Step Functions harus memiliki akses ke layanan yang digunakan oleh fungsi step. Misalnya, fungsi langkah dapat bergantung pada fungsi Lambda. Seseorang yang membuat fungsi langkah kemungkinan akan membuat fungsi Lambda pada saat yang sama dan harus meminta akses ke layanan itu juga.

Gunakan AMS SSP untuk menyediakan AWS Systems Manager Parameter Store di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan AWS Systems Manager Parameter Store secara langsung di akun terkelola AMS Anda. AWS Systems Manager Parameter Store menyediakan penyimpanan hierarkis yang aman untuk manajemen data konfigurasi dan manajemen rahasia. Anda dapat menyimpan data seperti kata sandi, string database, dan kode lisensi sebagai nilai parameter. Anda dapat menyimpan nilai sebagai teks biasa atau data terenkripsi. Anda kemudian dapat mereferensikan nilai dengan menggunakan nama unik yang Anda tentukan saat Anda membuat parameter. Sangat skalabel, tersedia, dan tahan lama, Parameter Store didukung oleh AWS Cloud. Untuk mempelajari lebih lanjut, lihat Menyimpan AWS Systems Manager Parameter.

> **Note**
>
> Jika Anda ingin menyimpan rahasia khusus dengan manajemen siklus hidup, gunakan Gunakan SSP AMS untuk menyediakan AWS Secrets Manager di akun AMS Anda alih-alih Parameter Store. Secrets Manager membantu Anda memenuhi persyaratan keamanan dan kepatuhan dengan memungkinkan Anda memutar rahasia secara otomatis. Secrets Manager menawarkan integrasi bawaan untuk MySQL, PostgreSQL, dan Amazon Aurora di Amazon RDS, yang dapat diperluas ke jenis rahasia lain dengan menyesuaikan fungsi Lambda.

AWS Systems Manager FAQ Parameter Store di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Systems Manager Parameter Store di akun AMS saya?

Minta akses ke AWS Systems Manager Parameter Store dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_systemsmanager_parameterstore_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS Systems Manager Parameter Store di akun AMS saya?

Anda diminta untuk menggunakan kunci AWS Terkelola; akses dibatasi dari membuat kunci KMS kustom. Namun, jika kunci khusus diperlukan, kirimkan RFC untuk membuat kunci yang dikelola pelanggan (CMK) menggunakan Deployment | Komponen Tumpukan Tingkat Lanjut | Kunci KMS | Buat jenis perubahan (ct-1d84keiri1jhg) dengan peran IAM ini, sebagai nilai untuk parameter dan. `customer_systemsmanager_parameterstore_console_role` `IAMPrincipalsRequiringDecryptPermissions` `IAMPrincipalsRequiringEncryptPermissionsPrincipal` Setelah Kunci KMS dibuat, Anda dapat membuat String Aman menggunakannya.

T: Apa prasyarat atau dependensi untuk menggunakan AWS Systems Manager Parameter Store di akun AMS saya?

Tidak ada prasyarat; Namun, SSM Parameter Store bergantung pada KMS untuk membuat String Aman sehingga Anda dapat mengenkripsi dan mendekripsi Nilai mereka yang disimpan di Parameter Store.

Gunakan SSP AMS untuk menyediakan AWS Systems Manager Otomasi di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kemampuan AWS Systems Manager Otomasi secara langsung di akun terkelola AMS Anda. AWS Systems Manager Otomatisasi menyederhanakan tugas pemeliharaan dan penerapan umum instans Amazon Elastic Compute Cloud dan AWS sumber daya lainnya menggunakan runbook, tindakan, dan kuota layanan. Ini memungkinkan Anda untuk membangun, mengeksekusi, dan memantau otomatisasi dalam skala besar. Automasi Systems Manager adalah jenis dokumen Systems Manager yang mendefinisikan tindakan yang dilakukan Systems Manager pada instans terkelola Anda. Runbook yang Anda gunakan untuk melakukan tugas pemeliharaan dan penerapan umum seperti menjalankan perintah atau skrip otomatisasi dalam instance terkelola Anda. Systems Manager menyertakan fitur yang membantu Anda menargetkan grup instans besar dengan menggunakan tag Amazon Elastic Compute Cloud, dan kontrol kecepatan yang membantu Anda meluncurkan perubahan sesuai dengan batas yang Anda tentukan. Runbook ditulis menggunakan JavaScript Object Notation (JSON) atau YAMM. Menggunakan Pembuat Dokumen di konsol Otomatisasi Systems Manager, namun, Anda dapat membuat runbook tanpa harus menulis dalama JSON atau YAML. Atau Anda dapat menggunakan runbook yang disediakan Manajer Sistem dengan langkah-langkah yang telah ditentukan sebelumnya yang sesuai dengan kebutuhan Anda. Untuk mempelajari lebih lanjut, lihat Bekerja dengan runbook dalam AWS Systems Manager dokumentasi.

> **Note**
>
> Meskipun Systems Manager Automation mendukung 20 jenis tindakan yang dapat digunakan di runbook, sejumlah tindakan terbatas yang dapat Anda gunakan saat membuat runbook untuk digunakan di akun AMS Advanced Anda. Demikian pula, sejumlah runbook yang disediakan Manajer Sistem dapat digunakan baik secara langsung atau dari dalam runbook Anda sendiri. Untuk detailnya, lihat batasan di FAQ berikut.

AWS Systems Manager FAQ Otomasi di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke Systems Manager Automation di akun AMS saya?

Minta akses ke AWS Systems Manager Otomasi dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_systemsmanager_automation_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS Systems Manager Otomasi di akun AMS saya?

Anda diminta untuk membuat runbook Anda, dengan serangkaian tindakan yang didukung Systems Manager terbatas untuk otomatisasi, hanya untuk menjalankan and/or skrip perintah dalam instance terkelola Anda. Tindakan yang tersedia untuk Anda bersama dengan batasan apa pun diuraikan seperti di bawah ini.

AWS Systems Manager Batasan Otomasi

Tindakan	Deskripsi	Batasan
aws: assertAwsResource Properti —	Menegaskan status AWS sumber daya atau status acara	Hanya EC2 contoh
aws:aws:cabang —	Jalankan langkah-langkah otomatisasi bersyarat	Tidak ada batasan

Tindakan	Deskripsi	Batasan
AWS: createTags -	Buat tag untuk AWS sumber daya	Hanya untuk runbook otomatisasi SSM yang Anda buat
AWS: ExecuteAutomation -	Jalankan otomatisasi lain	Hanya runbook otomatisasi yang Anda buat
AWS: ExecuteScript -	Jalankan skrip	Hanya skrip yang tidak melakukan panggilan API apa pun ke layanan apa pun
aws:jeda —	Jeda otomatisasi	Tidak ada batasan
AWS: runcommand —	Jalankan perintah pada instance terkelola	Hanya menggunakan dokumen yang disediaka n Manajer Sistem - AWS-RunShellScript dan AWS-RunPowerShellScript
aws:tidur —	Tunda otomatisasi	Tidak ada batasan
aws: waitForAws ResourceP roperty —	Tunggu properti AWS sumber daya	Hanya EC2 contoh

Anda juga dapat memilih untuk menjalankan perintah atau skrip secara langsung dengan Systems Manager yang disediakan runbook AWS- RunShellScript dan AWS- RunPowerShellScript menggunakan fitur 'Run Command' dari dalam konsol Systems Manager. Anda juga dapat membuat sarang runbook ini di dalam runbook Anda yang melayani validasi pra and/or posting tambahan atau logika otomatisasi kompleks apa pun.

Peran tersebut mematuhi prinsip hak istimewa terkecil dan hanya memberikan izin yang diperlukan untuk membuat, mengeksekusi, dan mengambil detail eksekusi runbook yang bertujuan untuk mengeksekusi and/or skrip perintah dalam instance terkelola Anda. Itu tidak memberikan izin untuk kemampuan lain yang disediakan AWS Systems Manager layanan. Meskipun fitur ini memungkinkan Anda untuk membuat runbook otomatisasi, eksekusi runbook tidak dapat ditargetkan untuk sumber daya yang dimiliki AMS.

T: Apa prasyarat atau dependensi untuk menggunakan AWS Systems Manager Otomasi di akun AMS saya?

Tidak ada prasyarat; Namun, Anda harus memastikan kontrol and/or kepatuhan proses internal Anda dipatuhi saat membuat runbook. Kami juga merekomendasikan untuk menguji runbook secara menyeluruh sebelum menjalankannya terhadap sumber daya produksi.

T: Dapatkah kebijakan Systems Manager **`customer_systemsmanager_automation_policy`** dilampirkan ke peran IAM lainnya?

Tidak, tidak seperti layanan berkemampuan penyediaan mandiri lainnya, kebijakan ini hanya dapat ditetapkan ke peran default yang disediakan. `customer_systemsmanager_automation_console_role`

Tidak seperti kebijakan peran SSPS lainnya, kebijakan SSM SSM ini tidak dapat dibagikan dengan peran IAM kustom lainnya, karena layanan AMS ini hanya untuk menjalankan perintah atau skrip otomatisasi dalam instans terkelola Anda. Jika izin ini diizinkan untuk dilampirkan ke peran IAM kustom lainnya, berpotensi dengan izin pada layanan lain, cakupan tindakan yang diizinkan dapat diperluas ke layanan terkelola, dan berpotensi menurunkan postur keamanan akun Anda.

Untuk mengevaluasi setiap permintaan perubahan (RFCs) terhadap standar teknis AMS kami, bekerja sama dengan Arsitek Cloud atau Manajer Pengiriman Layanan Anda masing-masing, lihat ulasan keamanan RFC.

> **Note**
>
> AWS Systems Manager memungkinkan Anda menggunakan runbook yang dibagikan dengan akun Anda. Kami menyarankan Anda berhati-hati dan melakukan pemeriksaan uji tuntas saat menggunakan runbook bersama dan pastikan untuk meninjau konten untuk memahami yang dijalankan command/scripts sebelum menjalankan runbook. Untuk detailnya, lihat Praktik terbaik untuk dokumen SSM bersama.

Gunakan SSP AMS untuk menyediakan AWS Transfer Family di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas (Transfer AWS Transfer Family Family) secara langsung di akun terkelola AMS Anda. AWS Transfer Family adalah AWS layanan yang dikelola sepenuhnya yang memungkinkan Anda mentransfer file melalui

Secure File Transfer Protocol (SFTP), masuk dan keluar dari penyimpanan Amazon Simple Storage Service (Amazon S3). SFTP juga dikenal sebagai Secure Shell (SSH) File Transfer Protocol. SFTP digunakan dalam alur kerja pertukaran data di berbagai industri seperti layanan keuangan, perawatan kesehatan, periklanan, dan ritel, antara lain.

Dengan AWS SFTP, Anda mendapatkan akses ke server SFTP AWS tanpa perlu menjalankan infrastruktur server apa pun. Anda dapat menggunakan layanan ini untuk memigrasikan alur kerja berbasis SFTP AWS sambil mempertahankan klien dan konfigurasi pengguna akhir Anda apa adanya. Pertama-tama Anda mengaitkan nama host Anda dengan titik akhir server SFTP, lalu tambahkan pengguna Anda dan berikan mereka tingkat akses yang tepat. Setelah Anda melakukannya, permintaan transfer pengguna Anda dilayani langsung dari titik akhir server AWS SFTP Anda. Untuk mempelajari selengkapnya AWS Transfer for SFTP, lihat juga Membuat server berkemampuan SFTP.

AWS Transfer for SFTP di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Transfer for SFTP akun AMS saya?

Minta akses ke AWS Transfer for SFTP dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). Melalui RFC ini, peran IAM berikut, dan kebijakan, disediakan di akun Anda:

- `customer_transfer_author_role`. Peran ini dirancang bagi Anda untuk mengelola layanan SFTP melalui konsol.
- `customer_transfer_sftp_server_logging_role`. Peran ini dirancang untuk dilampirkan pada Server SFTP. Hal ini memungkinkan server SFTP untuk menarik log ke dalam. CloudWatch
- `customer_transfer_sftp_user_role`. Peran ini dirancang untuk dilampirkan pada pengguna SFTP. Ini memungkinkan pengguna SFTP untuk berinteraksi dengan bucket S3.
- `policy customer_transfer_scope_down_policy`. Kebijakan ini adalah kebijakan cakupan bawah yang dapat diterapkan pada Pengguna SFTP untuk membatasi akses mereka pada bucket S3 ke folder rumah mereka.
- `customer_transfer_sftp_efs_user_role`. Peran ini dirancang untuk dilampirkan pada pengguna SFTP. Hal ini memungkinkan pengguna SFTP untuk berinteraksi dengan sistem file EFS.

Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Transfer for SFTP di akun AMS saya?

AWS Transfer untuk konfigurasi SFTP terbatas pada sumber daya tanpa awalan “AMS-” atau “MC-” untuk mencegah modifikasi apa pun pada infrastruktur AMS.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Transfer for SFTP

- Anda harus memiliki bucket Amazon S3 dengan nama yang berisi kata kunci “transfer” sebelum membuat AWS Transfer for SFTP server dan pengguna.
- Untuk menggunakan “Penyedia Identifikasi Pelanggan”, Anda harus menerapkan API Gateway, fungsi Lambda, dan repositori pengguna Anda (AD, Secrets Manager, dan sebagainya). Untuk informasi selengkapnya, lihat Mengaktifkan otentikasi kata sandi untuk AWS Transfer for SFTP menggunakan AWS Secrets Manager dan Bekerja dengan Penyedia Identitas.

Gunakan SSP AMS untuk menyediakan AWS Transit Gateway di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Transit Gateway kapabilitas secara langsung di akun terkelola AMS Anda. AWS Transit Gateway adalah layanan yang memungkinkan Anda menghubungkan Amazon Virtual Private Cloud (VPCs) dan jaringan lokal Anda ke satu gateway. Saat Anda meningkatkan jumlah beban kerja yang berjalan AWS, Anda harus dapat menskalakan jaringan Anda di beberapa akun dan Amazon VPCs untuk mengikuti pertumbuhannya. Hari ini, Anda dapat menghubungkan pasangan Amazon VPCs menggunakan peering. Namun, mengelola point-to-point konektivitas di banyak Amazon VPCs, tanpa kemampuan untuk mengelola kebijakan konektivitas secara terpusat, dapat menjadi mahal dan rumit secara operasional. Untuk konektivitas lokal, Anda perlu melampirkan AWS VPN ke setiap VPC Amazon individual. Solusi ini dapat memakan waktu untuk membangun dan sulit untuk mengelola ketika jumlah VPCs tumbuh menjadi ratusan. Untuk mempelajari selengkapnya, lihat AWS Transit Gateway.

AWS Transit Gateway di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Transit Gateway akun AMS saya?

Minta akses ke AWS Transit Gateway dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_tgw_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Transit Gateway di akun AMS saya?

Fungsionalitas lengkap AWS Transit Gateway tersedia di akun landing zone akun tunggal AMS Anda kecuali modifikasi tabel rute untuk perutean Transit Gateway. Minta perubahan tabel rute dengan mengirimkan Manajemen | Lainnya | Lainnya | Buat jenis perubahan (ct-1e1xtak34nx76).

> **Note**
>
> Layanan ini hanya didukung untuk single-account landing zone (SALZ), bukan multi-account landing zone (MALZ).

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Transit Gateway

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS Transit Gateway

Gunakan AMS SSP untuk menyediakan AWS WAF - Firewall Aplikasi Web di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS WAF kapabilitas secara langsung di akun terkelola AMS Anda. AWS WAF adalah firewall aplikasi web (AWS WAF) yang membantu melindungi aplikasi web Anda dari eksploitasi web umum yang dapat memengaruhi ketersediaan aplikasi, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan. AWS WAF memberi Anda kontrol atas lalu lintas mana yang diizinkan, atau diblokir, ke aplikasi web Anda dengan mendefinisikan aturan keamanan web yang dapat disesuaikan. Anda dapat menggunakan AWS WAF untuk membuat aturan kustom yang memblokir pola serangan umum, seperti injeksi SQL atau cross-site scripting; dan aturan yang dirancang untuk aplikasi spesifik Anda.

Untuk mempelajari lebih lanjut, lihat AWS WAF - Firewall Aplikasi Web.

AMS tidak mendukung pemantauan (CloudWatch alarm/acara/peringatan MMS) untuk. AWS WAF Karena sifatnya AWS WAF, Anda harus membuat aturan khusus untuk aplikasi Anda; AMS tidak dapat mengukur dan membuat alarm untuk Anda, tanpa konteks aplikasi Anda. Untuk mempelajari lebih lanjut, lihat AWS WAF - Firewall Aplikasi Web.

AWS WAF di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara saya meminta AWS WAF untuk disiapkan di akun AMS saya?

Meminta akses AWS WAF dengan mengirimkan RFC dengan Manajemen | Layanan AWS | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_waf_role` Setelah peran AWS WAF IAM disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan untuk menggunakan AWS WAF?

Setelah izin disediakan, Anda memiliki fungsionalitas penuh. AWS WAF

T: Apa prasyarat atau dependensi yang digunakan? AWS WAF

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS WAF

Gunakan SSP AMS untuk menyediakan AWS Well-Architected Tool di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses AWS Well-Architected Tool kapabilitas secara langsung di akun terkelola AMS Anda. AWS Well-Architected Tool Ini membantu Anda meninjau keadaan beban kerja Anda dan membandingkannya dengan praktik terbaik AWS arsitektur terbaru. Alat ini didasarkan pada AWS Well-Architected Framework, yang dikembangkan untuk membantu arsitek cloud membangun infrastruktur aplikasi yang aman, berkinerja tinggi, tangguh, dan efisien. Kerangka kerja ini memberikan pendekatan yang konsisten bagi Anda untuk mengevaluasi arsitektur, telah digunakan dalam puluhan ribu tinjauan beban kerja yang dilakukan oleh tim arsitektur AWS solusi, dan memberikan panduan untuk membantu mengimplementasikan desain yang sesuai dengan kebutuhan aplikasi dari waktu ke waktu. Untuk mempelajari selengkapnya, lihat AWS Well-Architected Tool.

AWS WA Tool di FAQ AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS Well-Architected Tool akun AMS saya?

Meminta akses AWS Well-Architected Tool dengan mengirimkan RFC dengan Manajemen | Layanan AWS | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_well_architected_tool_console_admin_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

T: Apa batasan penggunaan AWS Well-Architected Tool di akun AMS saya?

Fungsionalitas penuh AWS Well-Architected Tool tersedia di akun AMS Anda.

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS Well-Architected Tool

Tidak ada prasyarat atau dependensi untuk digunakan di akun AMS Anda. AWS Well-Architected Tool

Gunakan SSP AMS untuk menyediakan AWS X-Ray di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses kapabilitas (AWS X-Ray X-Ray) secara langsung di akun terkelola AMS Anda. AWS X-Ray membantu pengembang menganalisis dan men-debug produksi, aplikasi terdistribusi, seperti yang dibangun menggunakan arsitektur microservices. Dengan X-Ray, Anda dapat memahami kinerja aplikasi dan layanan yang mendasarinya, untuk mengidentifikasi dan memecahkan masalah akar penyebab masalah kinerja dan kesalahan. X-Ray memberikan end-to-end tampilan permintaan saat mereka melakukan perjalanan melalui aplikasi Anda, dan menunjukkan peta komponen dasar aplikasi Anda. Anda dapat menggunakan X-Ray untuk menganalisis kedua aplikasi dalam pengembangan dan produksi, dari aplikasi tiga tingkat sederhana, hingga aplikasi layanan mikro kompleks yang terdiri dari ribuan layanan. Untuk mempelajari selengkapnya, lihat AWS X-Ray.

FAQ X-Ray di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke AWS X-Ray akun AMS saya?

Minta akses dengan mengirimkan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan (ct-1w8z66n899dct) jenis perubahan. RFC ini menyediakan peran IAM berikut ke akun Anda:. `customer_xray_console_role` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda. Selain itu, Anda harus memiliki kemampuan `customer_xray_daemon_write_instance_profile` untuk mendorong data dari EC2 instans Amazon Anda ke X-Ray. Profil instance ini dibuat saat Anda menerima file`customer_xray_console_role`.

Anda dapat mengirimkan permintaan layanan ke Operasi AMS untuk menetapkan profil instans yang ada, atau Anda dapat menggunakan profil instans yang dibuat saat Operasi AMS mengaktifkan X-Ray untuk Anda. `customer_xray_daemon_write_policy`

T: Apa batasan penggunaan AWS X-Ray di akun AMS saya?

Fungsionalitas penuh AWS X-Ray tersedia di akun AMS Anda kecuali untuk enkripsi dengan kunci AWS KMS (kunci KMS). AWS X-Ray mengenkripsi semua data jejak secara default. Secara default, X-Ray mengenkripsi jejak dan data terkait saat istirahat. Jika Anda perlu mengenkripsi data saat istirahat dengan kunci, Anda dapat memilih kunci KMS AWS-managed (aws/xray) atau kunci KMS Customer-Managed. Untuk kunci KMS yang Dikelola Pelanggan untuk enkripsi X-Ray, kirimkan Manajemen | Lainnya | Lainnya | Buat jenis perubahan (ct-1e1xtak34nx76).

T: Apa prasyarat atau dependensi yang digunakan di akun AMS saya? AWS X-Ray

AWS X-Ray memiliki ketergantungan pada Amazon S3 CloudWatch,, CloudWatch dan Log, yang sudah diterapkan di akun AMS. Dependensi transitif bervariasi berdasarkan sumber data dan AWS layanan lain AWS X-Ray yang mungkin berinteraksi dengan fitur (misalnya, Amazon Redshift, Amazon RDS, Athena).

Gunakan AMS SSP untuk menyediakan VM Import/Export di akun AMS Anda

Gunakan mode AMS Self-Service Provisioning (SSP) untuk mengakses VM Import/Exportcapabilities secara langsung di akun terkelola AMS Anda. VM Import/Export memungkinkan Anda untuk dengan mudah mengimpor gambar mesin virtual dari lingkungan yang ada ke EC2 instans Amazon dan mengekspornya kembali ke lingkungan lokal Anda. Penawaran ini memungkinkan Anda untuk memanfaatkan investasi yang ada di mesin virtual yang telah Anda buat untuk memenuhi persyaratan keamanan, manajemen konfigurasi, dan kepatuhan TI Anda dengan membawa mesin virtual tersebut ke Amazon EC2 sebagai ready-to-use contoh. Anda juga dapat mengekspor instans yang diimpor kembali ke infrastruktur virtualisasi lokal Anda, memungkinkan Anda untuk menyebarkan beban kerja di seluruh infrastruktur TI Anda. Untuk mempelajari lebih lanjut, lihat Impor/Ekspor VM.

FAQ VM Import/Export di AWS Managed Services

Pertanyaan dan jawaban umum:

T: Bagaimana cara meminta akses ke VM Import/Export di akun AMS saya?

Minta akses ke VM Import/Export dengan mengirimkan RFC dengan Manajemen | AWS layanan | Layanan yang disediakan sendiri | Tambahkan jenis perubahan (ct-1w8z66n899dct). RFC ini

memberikan kebijakan IAM berikut ke akun Anda:. `customer_vmimport_policy` Setelah disediakan di akun Anda, Anda harus memasukkan peran tersebut dalam solusi federasi Anda.

Peran tambahan, peran Import/Export Layanan VM, diperlukan agar layanan dapat melakukan tindakan di akun Anda.

T: Apa batasan untuk menggunakan VM Import/Export di akun AMS saya?

- Fungsionalitas untuk mengimpor gambar mesin khusus dan volume data keduanya tersedia di AMS VM Impor/Ekspor. Namun, izin ke S3 telah dicakup untuk membatasi tindakan ke bucket yang cocok dengan nama untuk membatasi akses ke informasi `customer-vmimport-*` dalam akun.
- Impor gambar dan snapshot didukung di AMS VM Impor/Ekspor. Namun, fungsi impor instance dan ekspor instance tidak tersedia karena langkah-langkah keamanan.
- Selain itu, fungsionalitas ekspor telah dinonaktifkan untuk mengurangi risiko mengekspor data yang dibatasi dan sensitif.

T: Apa prasyarat atau dependensi untuk menggunakan VM di akun AMS saya? Import/Export

- Anda harus memberikan image disk yang didukung untuk mengimpor ke AWS lingkungan. Untuk selengkapnya, lihat Import/Export Persyaratan VM.
- VM Import/Export tidak dapat diakses melalui AWS konsol. Anda harus mengakses layanan ini melalui AWS CLI AWS Tools for PowerShell,, atau AWS SDKs. Atau, Anda dapat meminta profil instance dengan mengirimkan jenis perubahan ct-117rmp64d5mvb: Deployment | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Buat profil instance. EC2 Profil instance ini memungkinkan alat untuk melakukan perintah dari sebuah instance.

Modus Dikelola Pelanggan

Mode AWS Managed Services (AMS) Customer Managed menyediakan model tata kelola yang fleksibel dan dapat disesuaikan dengan kebutuhan Anda. Ini dapat dianggap sebagai opsi fallback untuk layanan dan aplikasi yang AMS tidak dapat beroperasi untuk Anda. AMS tidak mengoperasikan infrastruktur yang dihosting di akun yang dibuat dalam mode ini. Namun, Anda dapat memanfaatkan manajemen multi-akun terpusat dalam mode ini. Fitur Zona Pendaratan Multi-Akun berikut dapat dimanfaatkan dalam mode ini:

- Penyebaran Akun Otomatis
- Konektivitas melalui Transit Gateway di akun jaringan

- Pustaka Aturan Konfigurasi AMS
- Simpan salinan log di akun logging
- Agregasi peringatan Guard Duty yang dikelola pelanggan ke akun Keamanan
- Tagihan Terkonsolidasi
- Pengaktifan Kebijakan Kontrol Layanan kustom.

Misalnya: Jika Anda ingin menjalankan beban kerja di Ubuntu Pro, yang bukan Sistem Operasi yang dikelola oleh AMS, Anda dapat menggunakan akun yang dikelola pelanggan untuk hosting itu. Anda juga dapat mengkonsolidasikan beban kerja melalui akun yang dikelola pelanggan, untuk memanfaatkan diskon massal pada Instances/Sharing Paket Cadangan yang tersedia melalui berbagi di seluruh organisasi AWS.

Memulai mode Customer Managed

Mode Terkelola Pelanggan AMS tersedia melalui akun Aplikasi landing zone multi-akun khusus.

Untuk detailnya, termasuk cara membuat akun Aplikasi Terkelola Pelanggan, lihat Akun aplikasi yang Dikelola Pelanggan.

AMS dan AWS Service Catalog

Service Catalog di AWS Managed Services (AMS) memungkinkan organisasi untuk membuat dan mengelola katalog layanan teknologi informasi AWS (TI) dan memungkinkan administrator TI untuk membuat, mengelola, dan mendistribusikan katalog produk yang disetujui kepada pengguna akhir di akun mereka, yang kemudian dapat mengakses produk yang mereka butuhkan di portal layanan yang dipersonalisasi. Administrator dapat mengontrol pengguna mana yang memiliki akses ke setiap produk untuk menegakkan kepatuhan terhadap kebijakan bisnis organisasi. Administrator juga dapat mengatur peran sehingga pengguna akhir hanya memerlukan akses IAM ke Service Catalog untuk menyebarkan sumber daya yang disetujui. Service Catalog memungkinkan organisasi Anda mendapatkan keuntungan dari peningkatan kelincahan dan pengurangan biaya karena pengguna akhir hanya dapat menemukan dan meluncurkan produk yang mereka butuhkan dari katalog yang Anda kontrol.

Service Catalog memberi Anda alternatif untuk proses permintaan perubahan (RFC) AMS untuk menyediakan dan memperbarui sumber daya di akun terkelola AMS Anda. AMS mengelola semua tugas operasi infrastruktur yang diperlukan untuk menjalankan AWS dalam skala besar untuk semua sumber daya infrastruktur yang disediakan melalui Service Catalog termasuk keamanan, kepatuhan,

penyediaan, ketersediaan, tambalan, pemantauan, peringatan, pelaporan, respons insiden, dan pengoptimalan biaya. Memanfaatkan Service Catalog di akun terkelola AMS Anda memberi Anda mekanisme untuk mengelola layanan TI yang umum digunakan secara terpusat dan membantu Anda mencapai tata kelola yang konsisten sekaligus memungkinkan pengguna untuk dengan cepat menerapkan hanya layanan TI yang disetujui yang mereka butuhkan ke lingkungan terkelola mereka.

Memulai Service Catalog

Untuk memulai Service Catalog di AMS, kirimkan permintaan layanan melalui konsol AMS untuk meminta akses ke Service Catalog. Setelah mengajukan permintaan, tiga peran IAM akan diterapkan ke akun Anda bersama dengan tumpukan terkelola AMS yang berisi CloudFormation makro yang memanggil AMS `Transform` (dijelaskan sebelumnya) sehingga kami dapat mendaftarkan produk di sistem kami, dan untuk melakukan operasi terhadap infrastruktur yang disediakan melalui Service Catalog. Tiga peran IAM yang digunakan termasuk peran bagi admin TI untuk mengelola produk sebagai admin Service Catalog; peran bagi pemilik aplikasi dan pengguna akhir untuk mengonfigurasi, meluncurkan, dan mengelola produk; dan peran yang akan digunakan sebagai kendala peluncuran, yang menentukan izin yang akan digunakan oleh Service Catalog saat meluncurkan atau memperbarui produk Anda.

Service Catalog di AMS sebelum Anda mulai

Apakah Service Catalog menggantikan proses AMS request for change (RFC) yang ada?

> Di akun di mana Service Catalog diaktifkan, itu akan bertindak sebagai sistem manajemen perubahan tempat Anda menyediakan dan memperbarui layanan TI di akun AMS Anda melalui katalog produk yang telah ditentukan sebelumnya; AMS akan menyediakan portfolio/product katalog default, dan admin TI Anda dapat membuat dan mengonfigurasi milik Anda sendiri. Service Catalog hanya akan mengakui tumpukan yang disediakan melalui Service Catalog. Demikian juga, layanan yang disediakan melalui Service Catalog tidak akan dapat dimodifikasi melalui proses AMS RFC karena modifikasi di luar Service Catalog akan mengalihkan tumpukan dari konfigurasi produk yang disetujui.

Dapatkah saya melihat tumpukan yang disediakan melalui katalog layanan di Konsol AMS?

> Ya. Anda dapat melihat semua tumpukan yang disediakan melalui katalog layanan di konsol AMS. Tumpukan yang disediakan melalui katalog layanan mudah diidentifikasi oleh ID tumpukan “SC-”. Meskipun tumpukan dapat dilihat di konsol AMS, Anda tidak akan dapat memperbarui melalui proses AMS RFC. Akses ke sistem manajemen perubahan AMS (RFCs) terbatas pada permintaan akses, orkestrasi patch, dan cadangan saja. RFCs

Jika saya menyediakan and/or pembaruan tumpukan melalui Service Catalog, apakah akan ada RFC yang sesuai di Konsol AMS?

Satu-satunya RFC yang akan ditampilkan di konsol AMS adalah RFC untuk mendaftarkan tumpukan dengan AMS saat tumpukan awalnya disediakan. RFC ini diajukan secara otomatis oleh proses validasi AMS yang dipicu saat tumpukan diluncurkan melalui Service Catalog. Semua penyediaan dan perubahan lainnya dilacak secara langsung di Service Catalog dan dapat dilihat di konsol Service Catalog. Selanjutnya, Anda dapat menggunakan fitur Provisioned Product Plan di Service Catalog untuk melihat daftar perubahan yang akan dilakukan pada sumber daya sebelum penyediaan atau pembaruan produk.

Apakah saya harus melakukan sesuatu yang spesifik untuk menyediakan produk di akun terkelola AMS saya?

Ya. Semua produk Service Catalog yang disediakan di akun AMS harus berisi baris JSON ini dalam template CFN yang mendefinisikan produk tersebut:

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

Cuplikan CloudFormation kode ini memicu validasi AMS yang diperlukan sebelum sumber daya dapat disediakan di akun terkelola AMS Anda. Adalah tanggung jawab Anda untuk memasukkan baris kode ini sebagai bagian dari definisi produk. Jika tidak disertakan, penyediaan akan gagal dan pesan kesalahan berikut akan ditampilkan: “Gagal membuat produk. Akun ini dikelola oleh AMS. Semua produk di akun AMS harus memiliki `Transform` kode AMS di template.

Apakah ada fungsionalitas Service Catalog yang tidak tersedia and/or terbatas untuk pelanggan AMS saat diluncurkan?

Ya, fitur SC berikut tidak tersedia untuk pelanggan AMS pada peluncuran awal:

- Pembuatan Akun melalui Service Catalog
- Kemampuan untuk meluncurkan semua AWS Services melalui Service Catalog ke dalam akun yang dikelola AMS. Ketersediaan AWS Service terbatas pada layanan yang didukung AMS (dikelola dan disediakan sendiri). Untuk informasi selengkapnya tentang layanan yang didukung AMS, lihat deskripsi layanan AMS.
- Konektor Service Catalog IT service manager (ITSM) tidak akan berkomunikasi dengan laporan insiden AMS, dan permintaan layanan.

- Kemampuan untuk memanfaatkan Service Catalog mulai cepat dan arsitektur referensi tanpa modifikasi. Ingat bahwa produk Service Catalog untuk akun AMS harus berisi baris kode JSON ini:

  ```
  "Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
  {"Ref":"AWS::StackId"}}}
  ```

  dalam template CNF. Perhatikan bahwa baris ini bukan bagian dari CloudFormation template AWS biasa dan harus ditambahkan secara eksplisit.
- Terraform saat ini tidak didukung oleh AMS untuk menyediakan produk Service Catalog.
- Stackset AWS CFN tidak didukung di AMS.
- Anda tidak dapat membuat peran IAM kustom.
- Tindakan Layanan terbatas pada:
  - AWS- RebootRdsInstance
  - Instans AWS-Restart EC2
  - Instans AWS-Mulai EC2
  - AWS- StartRdsInstance
  - Instans AWS-Stop EC2
  - AWS- StopRdsInstance
  - AWS- CreateImage
  - AWS- CreateRdsSnapshot
  - AWS- CreateSnapshot

  > **Note**
  >
  > Saat membuat tindakan layanan, Anda dapat mengonfigurasi peran eksekusi menjadi izin pengguna akhir, peran peluncuran, atau peran IAM khusus yang Anda pilih. Peran eksekusi yang dipilih harus memiliki izin yang cukup untuk melakukan tindakan layanan, dan memiliki peran TrustPolicy yang memungkinkannya diasumsikan oleh Service Catalog, jika tidak, tindakan layanan akan gagal pada saat eksekusi. Sebaiknya gunakan AWSManagedServicesServiceCatalogLaunchRole, yang memiliki izin dan kebijakan kepercayaan yang benar untuk digunakan sebagai tindakan layanan.

Untuk apa saya masih perlu menggunakan sistem AMS RFC?

Pada ketersediaan umum (GA) Anda masih perlu menggunakan RFCS untuk menjalankan tindakan berikut:

- Mengkonfigurasi Patch Orchestrator
- Mengkonfigurasi kebijakan Cadangkan
- Meminta akses instans
- Membuat dan menetapkan grup keamanan yang berada di luar pedoman AMS.
- Melakukan konsumsi beban kerja (WIGS)
- Membuat Peran IAM

Dapatkah saya menggunakan Service Catalog CLI untuk mengakses Service Catalog di akun terkelola AMS saya?

Ya, Service Catalog APIs tersedia dan diaktifkan melalui CLI. Tindakan dari pengelolaan artefak Service Catalog melalui penyediaan dan penghentian artefak tersebut, tersedia. Untuk informasi selengkapnya, lihat Sumber Daya AWS Service Catalog, atau unduh AWS SDK atau CLI terbaru.

Siapa yang membuat, mengelola, dan mendistribusikan katalog produk yang disetujui pelanggan?

Administrator and/or TI administrator katalog pelanggan, atau sumber daya yang ditetapkan, bertanggung jawab atas pengelolaan katalog Service Catalog dan produk yang disetujui.

Bisakah saya menggunakan AMS AMIs?

AMIs AMS yang dijual setelah Maret 2020 dapat digunakan melalui AWS Service Catalog.

Bagaimana cara bermigrasi ke AMS menggunakan Service Catalog?

Untuk memigrasikan beban kerja Anda ke AMS menggunakan Service Catalog, Anda mulai dengan mengikuti proses Workload Ingest (WIGs) untuk membuat AMI di AMS. Anda menggunakan AMI yang diproduksi oleh WIGS untuk membuat produk di Service Catalog. Cara melakukannya dirinci di AWS Service Catalog - Memulai.

Orientasi AMS Multi-akun landing zone (MALZ)

Arsitektur jaringan MALZ

Tentang arsitektur jaringan landing zone multi-akun

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

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

> **Note**
>
> Untuk perkiraan biaya, lihat komponen dasar lingkungan landing zone multi-akun AMS.

Topik

- Wilayah layanan
- Unit organisasi
- Kebijakan kontrol layanan dan AWS Organization

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

Wilayah layanan

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

Unit organisasi

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

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

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

- mempercepat OU:

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

- aplikasi> OU terkelola:

  Dalam unit sub organisasi Aplikasi OU ini, akun dikelola sepenuhnya oleh AMS termasuk semua tugas operasional. Tugas operasional meliputi manajemen permintaan layanan, manajemen insiden, manajemen keamanan, manajemen kontinuitas, manajemen patch, optimalisasi biaya, pemantauan dan manajemen acara. Tugas-tugas ini dilakukan untuk manajemen infrastruktur Anda. Beberapa anak OUs dapat dibuat sesuai kebutuhan, hingga batas maksimum nested OUs tercapai untuk organisasi AWS. Untuk detailnya, lihat Kuota untuk AWS Organizations.

- aplikasi> pengembangan OU:

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

- OU yang dikelola pelanggan:

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

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

Kebijakan kontrol layanan dan AWS Organization

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

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

Memilih MALZ tunggal atau ganda MALZs

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

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

Entitas	Zona pendaratan AMS tunggal	Beberapa (dua atau lebih) zona pendaratan
Biaya dasar	Lebih rendah, dioptimalkan sekitar $3.000 per bulan.	Lebih tinggi, biaya tambahan sekitar $3.000 per lingkungan.
Penagihan	Tagihan tunggal, karena akun Penagihan/Manajemen tunggal.	Pisahkan tagihan untuk setiap landing zone multi-akun. Saat ini AWS Org

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Selain itu:

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

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

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

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

Akun Zona Pendaratan Multi-Akun

Topik

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

Akun manajemen

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

Untuk informasi selengkapnya tentang penggunaan akun manajemen, lihat Praktik terbaik untuk akun manajemen.

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

Sumber daya di akun manajemen

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

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

Akun jaringan

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

Arsitektur akun jaringan

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

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

> **Note**
>
> Untuk informasi tentang batasan dan batasan layanan default untuk semua layanan aktif, lihat dokumentasi AWS Service Limits.

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

Konektivitas jaringan pribadi ke lingkungan landing zone multi-akun AMS

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

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

Konektivitas tepi terpusat menggunakan gateway transit

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

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

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

Konfigurasi ini menawarkan manfaat sebagai berikut. Anda dapat:

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

> **Note**
>
> Untuk informasi tentang penggunaan DX dengan layanan AWS, lihat bagian Ketahanan Toolkit Klasik. Untuk informasi selengkapnya, lihat asosiasi Transit Gateway.

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

Menghubungkan DX atau VPN ke akun VPCs

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

Sumber daya di akun jaringan

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

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

Manajer Jaringan AWS

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

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

Gunakan salah satu peran berikut untuk mengakses sumber daya ini:

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

Keluar VPC

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

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

> **Note**
>
> Rentang CIDR VPC Jaringan: Saat Anda membuat VPC, Anda harus menentukan rentang alamat IPv4 untuk VPC dalam bentuk blok Classless Inter-Domain Routing (CIDR); misalnya, 10.0.16.0/24. Ini akan menjadi blok CIDR utama VPC Anda.
> Tim landing zone multi-akun AMS merekomendasikan rentang 24 (dengan lebih banyak alamat IP) untuk menyediakan beberapa buffer jika sumber daya/peralatan lain, digunakan di masa mendatang.

Firewall jalan keluar Palo Alto yang dikelola

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

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

Kontrol lalu lintas

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

Arsitektur

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

Aliran jaringan

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

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

Firewall itu sendiri berisi tiga antarmuka:

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

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

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

Modifikasi daftar izinkan

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

Kebijakan keamanan khusus

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

> **Note**
>
> Kebijakan keamanan default `ams-allowlist` tidak dapat diubah

CloudWatch Dasbor jalan keluar PA

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

```
fields @timestamp, @message
| filter @logStream like /pa-traffic-logs/
| filter @message like /<Security Policy Name>/
| parse @message
 "*,*,*,
```

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

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

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

Pembaruan

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

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

Akses operator

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

Log default

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

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

Log yang dikumpulkan oleh solusi adalah sebagai berikut:

Kode Status RFC

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

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

Manajemen acara

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

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

Alarm Acara:

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

Alarm Manajemen:

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

Metrik

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

Metrik Kustom:

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

CloudWatch Integrasi log

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

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

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

CloudWatch Langganan. Pelajari lebih lanjut tentang Panorama di bagian berikut. Untuk mempelajari lebih lanjut tentang Splunk, lihat Mengintegrasikan dengan Splunk.

Integrasi Panorama

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

Lisensi

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

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

Batasan

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

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

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

Persyaratan orientasi

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

Harga

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

Harga berikut didasarkan pada firewall seri VM-300.

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

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

Perimeter (DMZ) VPC

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

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

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

AWS Transit Gateway

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

Berikan masukan berikut untuk membuat sumber daya ini:

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

Akun Layanan Bersama

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

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

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

  > **Note**
  >
  > Tim AMS merekomendasikan kisaran /23.

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

- Trend Micro — endpoint protection security (EPS): Trend Micro endpoint protection (EPS) adalah komponen utama dalam AMS untuk keamanan sistem operasi. Sistem ini terdiri dari Deep Security

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

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

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

- Jenis Instance Relay: Nilai Default - m5.large
- Jenis Instans DSM: Nilai Default - m5.xlarge
- Ukuran Instans DB: Nilai Default - 200 GB
- Jenis Instans RDS: Nilai Default - db.m5.large

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

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

Pembaruan untuk layanan bersama: Zona Pendaratan Multi-Akun

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

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

- Akun yang merupakan bagian dari inti OU.

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

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

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

Akun Arsip Log

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

Akun keamanan

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

Jenis akun aplikasi

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

- Akun aplikasi yang dikelola AMS
- AMS Mempercepat akun
- Akun aplikasi yang Dikelola Pelanggan

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

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

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

Akun aplikasi disediakan melalui RFC yang dikirimkan dari akun Manajemen:

- Buat Akun Aplikasi Dengan VPC ct-1zdasmc2ewzrs
- Buat Accelerate Account ct-2p93tyd5angmi
- Buat Akun Aplikasi yang Dikelola Pelanggan ct-3pwbixz27n3tn

Akun aplikasi yang dikelola AMS

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

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

- Modus RFC
- Mode Perubahan Langsung di AMS
- AMS dan AWS Service Catalog
- Mode Pengembang AMS Lanjutan
- Mode Penyediaan Layanan Mandiri di AMS

Untuk informasi selengkapnya tentang manajemen perubahan dan mode yang berbeda, lihatUbah mode manajemen.

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

AMS Mempercepat akun

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

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

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

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

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

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

Untuk detail selengkapnya tentang Accelerate, lihat Apa itu Mempercepat.

Membuat akun Accelerate Anda

Untuk membuat akun Accelerate, ikuti langkah-langkah yang diuraikan di sini Buat akun Accelerate.

Mengakses akun Accelerate Anda

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

Untuk mengakses akun Accelerate baru:

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

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

Menghubungkan akun Accelerate Anda dengan Transit Gateway

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

> **Note**
>
> Anda hanya dapat memiliki VPC yang dilampirkan ke TGW jika akun Accelerate berada di Wilayah AWS yang sama. Untuk informasi lebih lanjut, lihat Transit gateway.

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

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

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

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

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

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

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

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

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

Mengaitkan lampiran TGW ke tabel rute:

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

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

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

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

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

Akun aplikasi yang Dikelola Pelanggan

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

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

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

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

Untuk membuat akun aplikasi yang Dikelola Pelanggan, lihat Akun manajemen | Membuat Akun Aplikasi yang Dikelola Pelanggan.

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

Mengakses akun yang Dikelola Pelanggan

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

Untuk mengakses CMA:

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

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

Menghubungkan CMA Anda dengan Transit Gateway

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

> **Note**
>
> Anda hanya dapat memiliki VPC yang dilampirkan ke TGW jika CMA berada di Wilayah AWS yang sama. Untuk informasi lebih lanjut, lihat Transit gateway.

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

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

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

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

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

Mengaitkan lampiran TGW ke tabel rute:

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

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

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

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

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

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

Mendapatkan bantuan operasional dengan akun yang Dikelola Pelanggan

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

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

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

Akun AMS Tools (memigrasikan beban kerja)

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

Akun alat menyediakan yang berikut:

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

Diagram arsitektur tingkat tinggi:

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

> **Note**
>
> Kami merekomendasikan memiliki dua zona ketersediaan (AZs), karena ini adalah hub migrasi.
> Secara default, AMS membuat dua grup keamanan berikut (SGs) di setiap akun.
> Konfirmasikan bahwa SGs keduanya hadir. Jika mereka tidak hadir, silakan buka permintaan layanan baru dengan tim AMS untuk memintanya.
>
> - SentinelDefaultSecurityGroupPrivateOnlyEgressAll
> - InitialGarden-SentinelDefaultSecurityGroupPrivateOnly

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

Prasyarat:

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

AWS Layanan Migrasi Aplikasi (AWS MGN)

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

Untuk up-to-date informasi paling banyak tentang AWS Region dukungan, lihat Daftar Layanan AWS Regional.

Jika pilihan Anda saat AWS Region ini tidak didukung oleh AWS MGN, atau sistem operasi tempat aplikasi Anda berjalan saat ini tidak didukung oleh AWS MGN, pertimbangkan untuk menggunakan akun CloudEndure Migrasi di Alat Anda.

Meminta Inisialisasi AWS MGN

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

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

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

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

Aktifkan akses ke akun AMS Tools baru

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

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

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

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

   - IAM role: `AWSManagedServicesMigrationRole`
   - Pengguna IAM: `customer_cloud_endure_user`
2. Minta kebijakan dan peran untuk memungkinkan anggota tim integrasi layanan menyiapkan alat tingkat berikutnya.

   Arahkan ke konsol AMS dan ajukan yang berikut ini RFCs:

   a. Buat kunci KMS. Gunakan Create KMS Key (auto) atau Create KMS Key (review required).

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

   b. Bagikan kunci KMS.

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

Contoh grafik pengaturan akun akhir:

Contoh kebijakan IAM yang telah disetujui AMS CloudEndure

Untuk melihat CloudEndure kebijakan IAM AMS yang telah disetujui sebelumnya:
Buka paket file Contoh Zona Pendaratan Cloud Endure WIGS dan buka file.
`customer_cloud_endure_policy.json`

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

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

Proses konsumsi AMS:

Kebersihan akun AMS Tools

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

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

Migrasi dalam skala - Pabrik Migrasi

Lihat Memperkenalkan Solusi Pabrik CloudEndure Migrasi AWS.

MALZ: Orientasi akun inti

Tugas utama yang harus Anda selesaikan saat melakukan orientasi ke akun inti landing AWS zone multi-akun adalah sebagai berikut:

Topik

- Buat AWS akun inti landing zone multi-akun di AMS
- Buat peran IAM untuk AMS untuk mengakses akun Anda

- Amankan akun baru dengan otentikasi multi-faktor (MFA) untuk pengguna root di AMS
- Berlangganan AWS Marketplace untuk Trend Micro Endpoint Protection (EPS)
- Mengatur jaringan
- Mengatur manajemen akses

Untuk pertanyaan orientasi, hubungi Cloud Architect Anda.

Buat AWS akun inti landing zone multi-akun di AMS

AMS multi-account landing zone memerlukan penyediaan akun Amazon Web Services (AWS) baru untuk bertindak sebagai akun manajemen di lingkungan landing zone multi-akun AMS. Untuk membuat Akun AWS, ikuti step-by-step petunjuk berikut: Bagaimana cara membuat dan mengaktifkan akun Amazon Web Services baru?

Langkah sederhananya adalah: Buka Buat Akun, dan klik Daftar Sekarang dan, pada halaman yang terbuka, klik Buat yang baru Akun AWS. Ikuti petunjuk di layar, termasuk menerima panggilan telepon dan memasukkan PIN menggunakan keypad ponsel Anda. Anda juga harus memasukkan kartu kredit. AMS menggunakan akun ini sebagai akun manajemen, atau akun pembayar, untuk landing zone multi-akun baru Anda.

> **Note**
>
> Setelah Anda onboard, bicarakan dengan manajer pengiriman layanan cloud (CSDM) Anda tentang memindahkan tagihan dari kartu kredit Anda dan ke sistem faktur. Informasi berikut akan diperlukan:
>
> - Nama Perusahaan Penagihan
> - Nama Kontak Penagihan
> - Nomor Telepon Kontak Penagihan
> - Email Kontak Penagihan
> - Alamat Penagihan
>
> CSDM Anda akan membantu Anda dengan pembaruan ini. Setelah selesai, dan untuk mengubah metode pembayaran, lihat Mengelola metode AWS pembayaran Anda.

> **Note**
>
> Jangan menautkan akun baru Anda ke akun manajemen yang ada, atau akun pembayar. Pastikan akun Anda bukan bagian dari akun yang sudah ada AWS Organizations; untuk informasi, lihat Apa itu AWS Organizations?

> **Important**
>
> Sangat penting bagi Anda untuk memastikan bahwa alamat email (daftar distribusi, bukan alamat email individu) dan nomor telepon dikaitkan dengan akun sehingga Anda menerima tanggapan terhadap potensi insiden keamanan. Nomor telepon dan alamat email untuk akun tidak dapat diubah tanpa mengatur ulang kata sandi akun, yang merupakan upaya signifikan untuk akun root AMS. Untuk memastikan bahwa nilai-nilai ini stabil, sangat penting untuk memilih informasi kontak yang tidak terkait dengan individu, yang dapat berubah. Pilih alias email yang dapat menunjuk ke grup. Ikuti praktik yang sama dalam memilih nomor telepon: pilih nomor yang dapat menunjuk ke grup atau ke nomor yang dimiliki oleh perusahaan dan bukan individu.

Untuk detail tentang pertanyaan yang akan diminta untuk memasukkan akun Core ke landing zone multi-akun AMS, lihat. Lampiran: daftar pertimbangan orientasi multi-akun landing zone (MALZ)

Buat peran IAM untuk AMS untuk mengakses akun Anda

Sekarang setelah Anda berhasil membuat yang baru Akun AWS, langkah selanjutnya dalam proses ini adalah mengizinkan akses AMS ke akun baru untuk membuat dan mengonfigurasi lingkungan AMS Anda, dan agar permintaan perubahan dan penyediaan yang sedang berlangsung dipenuhi. Untuk detailnya, lihat Mendelegasikan Akses di Seluruh AWS Akun Menggunakan Peran IAM.

AWS Identity and Access Management (IAM) adalah layanan web yang membantu Anda mengontrol akses ke AWS sumber daya dengan aman bagi pengguna Anda. Anda menggunakan IAM untuk mengontrol siapa yang dapat menggunakan AWS sumber daya Anda (otentikasi) dan sumber daya apa yang dapat mereka gunakan dan dengan cara apa (otorisasi).

Aktifkan akses IAM ke konsol AWS

1. Masuk ke konsol AWS Manajemen dengan kredensi akun root Anda (email dan kata sandi yang Anda gunakan untuk membuat). Akun AWS Jangan masuk dengan kredensi IAM lainnya. Halaman beranda konsol AWS Manajemen terbuka.
2. Di bilah navigasi atas, buka menu tarik-turun untuk nama akun Anda, lalu pilih Akun. Halaman beranda Penagihan terbuka.
3. Gulir ke bawah ke pengguna IAM dan akses peran ke informasi Penagihan, lalu pilih Edit. Area akses Activate IAM terbuka.
4. Pilih kotak centang dan kemudian pilih Perbarui. Anda sekarang dapat menggunakan kebijakan IAM untuk mengontrol halaman mana yang dapat diakses pengguna.

Membuat Peran IAM untuk AMS untuk digunakan

1. Dapatkan file JSON atau YAMB yang mendefinisikan peran IAM untuk digunakan AMS untuk membuat infrastruktur Anda. Entah:
   - Arsitek cloud AMS (CA) Anda memberi Anda file JSON atau YAMG.
   - Anda dapat mengunduh onboarding_iam_roles.zip dan memilih salah satu dari yang berikut:
     - onboarding_role_admin.json (lebih pendek, memberikan akses admin penuh)
     - onboarding_role_minimal.json (lebih lama, memberikan hak istimewa paling sedikit)
2. Masuk ke Konsol Manajemen AWS dan buka CloudFormation konsol di https://console.aws.amazon.com/cloudformation.
3. Pilih Buat tumpukan. Anda melihat halaman berikut.
4. Pilih Unggah file templat, unggah file JSON atau YAMB dari peran IAM, lalu pilih Berikutnya. Anda melihat halaman berikut.
5. Masuk **`ams-onboarding-role`** ke bagian Stack name dan lanjutkan gulir ke bawah dan pilih berikutnya sampai Anda mencapai halaman ini.

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

Amankan akun baru dengan otentikasi multi-faktor (MFA) untuk pengguna root di AMS

Bagian ini telah disunting karena berisi informasi sensitif terkait keamanan AMS. Informasi ini tersedia melalui Dokumentasi konsol AMS. Untuk mengakses Artifact AWS, Anda dapat menghubungi CSDM untuk mendapatkan petunjuk atau membuka Memulai dengan Artifact AWS.

Berlangganan AWS Marketplace untuk Trend Micro Endpoint Protection (EPS)

Trend Micro Endpoint Protection (EPS) adalah komponen utama dalam AMS untuk keamanan sistem operasi. Untuk menyiapkan EPS setelah pembuatan landing zone AMS dimulai, Anda harus masuk ke akun inti layanan bersama dan berlangganan AMI Trend Micro Deep Security aktif AWS Marketplace. CSDM atau CA Anda akan memberi tahu Anda.

1. Masuk ke AWS konsol menggunakan peran atau pengguna yang Anda tentukan dalam Kuesioner Orientasi untuk `CustomerEPSSubscriptionIAMRoleOrUser`
2. Arahkan ke layar Beralih Peran.

   - Akun: Disediakan oleh AMS
   - Peran: `EPSMarketplaceSubscriptionRole`
   - Nama Tampilan: Sesi Berlangganan EPS

   Untuk berlangganan Trend Micro Deep Security di AWS Marketplace, ikuti langkah-langkah berikut setelah Anda beralih peran di konsol:

   1. Arahkan ke AWS Marketplace.
   2. Di bawah Temukan AWS Marketplace produk yang memenuhi kebutuhan Anda, pilih opsi berikut:

      a. Penjual: Trend Micro

   b. Paket Harga: Bawa Lisensi Anda Sendiri jika Anda memiliki lisensi atau Penagihan Oleh Tuan Rumah
   c. Metode Pengiriman: Gambar Mesin Amazon
3. Klik Lanjutkan untuk Berlangganan di panel kanan.
4. Tinjau Syarat dan Ketentuan, dan klik Terima Syarat di sudut kanan atas.
5. Keluar dari akun dan konfirmasikan dengan Cloud Architect Anda bahwa prosedur telah selesai.

Pada titik ini AMS menyebarkan infrastruktur ke lingkungan AMS Anda dan lingkungan siap untuk Anda gunakan setelah Anda menghubungkan jaringan Anda dan mengatur akses Anda.

Mengatur jaringan

Jaringan di lingkungan AMS terutama ditangani di akun inti jaringan.

Ada beberapa proses yang perlu diselesaikan untuk menyiapkan jaringan untuk AWS Managed Services (AMS):

- Mengalokasikan ruang IP untuk lingkungan AMS Anda
- Membangun konektivitas jaringan pribadi ke AWS
- Menyiapkan firewall Anda untuk mengizinkan operasi AMS

Mengalokasikan ruang IP untuk lingkungan AMS Anda

Anda seharusnya sudah bekerja dengan Cloud Architect Anda dalam menentukan ruang IP untuk lingkungan AMS Anda sambil mengisi kuesioner orientasi.

Membangun konektivitas jaringan pribadi ke AWS AMS

AWS menawarkan konektivitas pribadi dengan menggunakan konektivitas VPN dan jalur khusus melalui AWS Direct Connect. Konektivitas Pribadi dapat diatur dengan dua cara:

- Konektivitas Edge terpusat menggunakan Transit Gateway
- Menghubungkan Direct Connect and/or VPN ke akun VPCs

Konektivitas tepi terpusat menggunakan Transit Gateway

AWS Transit Gateway adalah layanan yang memungkinkan Anda menghubungkan Amazon Virtual Private Clouds (VPCs) dan jaringan lokal Anda ke satu gateway. Transit Gateway dapat digunakan untuk mengkonsolidasikan konektivitas edge yang ada dan mengarahkannya melalui satu ingress/egress titik. Untuk detail selengkapnya, lihat AWS Transit Gateway.

Menghubungkan Direct Connect ke Transit Gateway

Anda dapat menggunakan koneksi Direct Connect yang sudah ada atau membuat koneksi Direct Connect baru di salah satu AWS akun yang sudah ada. Koneksi Direct Connect harus berupa koneksi khusus atau host yang berjalan pada 1 Gbps atau lebih.

> **Note**
>
> Untuk informasi tentang penggunaan Direct Connect dengan AWS layanan, lihat Memulai di Lokasi AWS Direct Connect.

Untuk menggunakan koneksi khusus Direct Connect yang ada, koneksi tidak boleh memiliki lebih dari 3 antarmuka virtual transit yang dibuat di dalamnya. Ini karena koneksi Direct Connect khusus memiliki batas 4 antarmuka virtual transit per koneksi.

Untuk informasi tambahan tentang Batas Direct Connect, lihat Batas AWS Direct Connect.

Setelah koneksi Direct Connect tersedia, berikut ini terjadi:

1. AMS membuat Direct Connect Gateway di akun jaringan. Anda harus memberikan nomor Autonomous System Number (ASN) untuk Direct Connect Gateway dan awalan yang harus diiklankan dari Direct Connect Gateway. ASN ini digunakan sebagai Amazon ASN.
2. Anda membuat VIF Transit baru dan mengatur pemilik antarmuka virtual sebagai akun jaringan.
3. AMS masuk ke akun jaringan dan menerima proposal koneksi.
4. AMS mengaitkan gateway transit dengan gateway Direct Connect.
5. AMS mengaitkan lampiran dengan tabel perutean Transit Gateway on-prem.

> **Note**
>
> ASN yang disediakan untuk gateway Direct Connect dan Transit Gateway harus berbeda.

Untuk meningkatkan ketahanan konektivitas Anda, sebaiknya pasang setidaknya 2 antarmuka virtual transit, dari lokasi Direct AWS Connect yang berbeda, ke gateway Direct Connect. Untuk informasi lebih lanjut, lihat Direct Connect rekomendasi ketahanan.

Menghubungkan VPN ke Transit Gateway

Untuk melampirkan koneksi VPN ke gateway transit Anda, Anda harus menentukan gateway pelanggan. Untuk informasi selengkapnya tentang persyaratan gateway pelanggan, lihat Persyaratan untuk Gateway Pelanggan Anda di Panduan Administrator Jaringan VPC Amazon.

Anda perlu memberikan nomor BGP ASN, alamat IP publik statis dan Opsi perutean (Statis atau Dinamis). Setelah detail ini diberikan, AMS akan membuat lampiran VPN dan mengaitkan lampiran dengan tabel perutean Transit Gateway on-prem.

Untuk detail selengkapnya tentang lampiran Transit Gateway, lihat Lampiran VPN Transit Gateway.

Menghubungkan Direct Connect and/or VPN ke akun VPCs

Anda juga dapat langsung menghubungkan Anda VPCs ke Direct Connect atau VPN. Lalu lintas mengalir langsung dari VPCs ke Direct Connect atau VPN tanpa melintasi gateway transit.

> **Note**
>
> VPC layanan bersama dan akun aplikasi VPCs harus terhubung ke koneksi Direct Connect atau VPN untuk membangun konektivitas pribadi.

Direct Connect penyiapan di AMS

Siapkan a Direct Connect untuk berkomunikasi antara VPC yang dikelola AMS dan jaringan internal Anda.

> **Note**
>
> Untuk informasi tentang penggunaan Direct Connect dengan AWS layanan, lihat Memulai di Direct Connect Lokasi.

Untuk mengatur koneksi Direct Connect, selesaikan langkah-langkah berikut:

1. Daftar untuk Amazon Web Services (AWS)
2. Kirim permintaan Direct Connect koneksi.
3. Selesaikan Cross Connect.
4. (Opsional) Konfigurasikan koneksi redundan dengan. Direct Connect
5. Dilakukan oleh AMS: Buat antarmuka virtual.
6. Dilakukan oleh AMS: Unduh konfigurasi router.
7. Verifikasi antarmuka virtual Anda.

Penyiapan VPN

Langkah-langkah dasar yang diikuti AMS untuk menyiapkan VPN untuk berkomunikasi antara VPC yang dikelola AMS dan jaringan internal Anda.

> **Note**
>
> Untuk mendapatkan pemahaman menyeluruh tentang penggunaan VPN dengan AWS layanan, lihat Apa itu AWS Site-to-Site VPN dan Gateway Pelanggan Anda (alat VPN Anda).

Kami mengikuti Panduan Pengguna AWS VPN Memulai dan Menguji bagian Koneksi Site-to-Site VPN untuk menyelesaikan langkah-langkah berikut:

1. Di AWS VPC Anda, Buat Gateway Pelanggan.
2. Di AWS VPC Anda, Buat Gateway Pribadi Virtual.
3. Di AWS VPC Anda, Aktifkan Propagasi Rute di Tabel Rute Anda.
4. Di AWS VPC Anda, Perbarui Grup Keamanan Anda untuk Mengaktifkan Akses SSH, RDP, dan ICMP Masuk.

5. Di Jaringan internal Anda, Buat Koneksi VPN dan Konfigurasikan Gateway Pelanggan.
6. Uji konektivitas VPN antara VPC dan jaringan internal Anda.

Mengatur manajemen akses

Menggunakan jaringan yang dikelola oleh AWS Managed Services (AMS) berarti memberikan AMS akses untuk mengelola infrastruktur cloud Anda. Anda harus mengonfigurasi sarana untuk menghubungkan dengan aman antara jaringan pribadi Anda dan AMS. Ini dimulai dengan beberapa keputusan:

- Akses AMS API/CLI dan Konsol: Anda akan ingin menginstal AMS CLI (instruksi disediakan dalam dokumen ini). Anda menggunakan API manajemen perubahan AMS untuk membuat permintaan perubahan ke AMS dan AMS SKMS API untuk mempelajari sumber daya yang dikelola AMS. Menggunakan Active Directory Federation Services (AD FS), Anda dapat mengakses Konsol AMS.
- Akses pengguna: Konektivitas harus dibuat antara AD di sisi AMS (melalui Layanan Direktori) dan direktori yang Anda gunakan untuk mengelola pengguna.
- Akses instans: Akses tingkat instans dilakukan melalui konfigurasi kepercayaan satu arah. Directory Services mempercayai kredensi di CORP AD Anda, memungkinkan tumpukan di sisi AMS untuk mengizinkan login dengan kredenal CORP.

> **Note**
>
> Direktori Aktif (AD) Anda yang AMS mengatur kepercayaan, harus merupakan direktori yang memiliki akun pengguna yang diotorisasi oleh Anda untuk mendapatkan akses ke sumber daya AWS Anda.

Membangun Kepercayaan Direktori Aktif

Untuk mengatur kepercayaan, AMS memerlukan pengontrol domain Anda Kebijakan Lokal -> Opsi Keamanan -> Akses Jaringan: Pipa Bernama yang dapat diakses secara anonim, daftar pipa Netlogon dan lsarpc. Pipa ini terdaftar secara default, tetapi kadang-kadang dihapus untuk masalah keamanan. Setelah kepercayaan ditetapkan, mereka dapat dihapus dari daftar lagi.

Konfigurasikan Conditional Forwarder

1. Di Manajer DNS AD -> Buat Forwarder Bersyarat Baru, di bawah Domain DNS: Gunakan nama domain AMS yang diberikan kepada Anda; misalnya, A523434123.amazonaws.com (ubah ini menjadi nama domain yang dipilih dalam kuesioner orientasi.
2. Di bawah alamat IP server master: Tambahkan alamat IP yang disediakan AMS. Pastikan tidak ada masalah koneksi dengan memvalidasi kedua alamat.
3. Pilih Simpan forwarder bersyarat ini di Active Directory dan replikasi sebagai berikut: Semua server DNS di domain ini dan tekan OK.

Konfigurasikan kepercayaan AD

Ikuti artikel Microsoft AD ini Buat kepercayaan hutan satu arah, masuk, untuk satu sisi kepercayaan, menggunakan pengaturan dan pilihan yang dijelaskan di bagian ini.

1. Buka dialog Start -> Administrative Tools -> Active Directory Domains and Trusts. Klik kanan node domain untuk domain yang ingin Anda percayai, lalu klik Properties -> Trusts -> New Trust untuk membuka New Trust Wizard. Masukkan nama domain yang diberikan kepada Anda oleh AMS untuk Nama Kepercayaan dan tekan Berikutnya.
2. Di bawah Jenis Kepercayaan, pilih tingkat kepercayaan yang sesuai (misalnya Forest Trust). Tekan Berikutnya.
3. Di bawah Direction of Trust, pilih Satu arah: masuk. Tekan Berikutnya.
4. Di bawah Sisi Kepercayaan, pilih Domain ini saja. Tekan Berikutnya.
5. Di bawah Trust Password, ketikkan kata sandi pilihan Anda. Tekan Berikutnya.
6. Untuk Seleksi Kepercayaan Selesai dan Pembuatan Kepercayaan Selesai, cukup tekan Berikutnya.
7. Di bawah Konfirmasi Kepercayaan Masuk, pilih Tidak, jangan konfirmasi kepercayaan yang masuk. Tekan Berikutnya.
8. Di bawah Selesai New Trust Wizard, pilih Selesai, lalu OK untuk menutup.
9. Berikan kata sandi kepercayaan (hubungi kami melalui nomor telepon CSDM Anda untuk alasan keamanan). AMS akan menyelesaikan konfigurasi kepercayaan.

Situs dan layanan Active Directory

Untuk mengurangi latensi login, tambahkan rentang CIDR VPC ke situs dan layanan Direktori Aktif Anda (Mulai -> Alat Administratif -> Situs dan Layanan Direktori Aktif). Tambahkan rentang CIDR VPC ke Situs Direktori Aktif yang berisi Pengontrol Domain yang paling dekat dengan AWS.

Berikan nama situs AD dari situs yang Anda dedikasikan untuk AMS ke CSDM Anda. AMS akan mengganti nama situs default di sisi AMS AD agar sesuai dengan nama yang diberikan.

Perutean akhiran nama Direktori Aktif

Setelah kepercayaan hutan satu arah ditetapkan, selesaikan langkah-langkah berikut untuk memvalidasi perutean sufiks:

1. Di bawah Mulai > Semua Program > Alat Administratif, klik Active Directory Domains and Trusts.

   Konsol Active Directory Domains and Trusts terbuka.
2. Klik kanan domain perusahaan Anda dan klik Properties

   Dialog Properties untuk domain itu terbuka.
3. Klik tab Trusts.

   Halaman Trust terbuka.
4. Klik nama domain Amazon dan klik Properties.

   Halaman Properti untuk kepercayaan domain Amazon terbuka.
5. Klik Name Suffix Routing dan klik Refresh.

   Pastikan tidak ada konflik untuk memastikan bahwa Nama Prinsipal Layanan (SPNs) dapat menyelesaikan kepercayaan.

Federasi Direktori Aktif Anda dengan peran AMS IAM

Tujuan menggabungkan direktori Anda dengan peran AMS IAM adalah untuk memungkinkan pengguna korporat menggunakan kredensi perusahaan mereka untuk berinteraksi dengan AWS Console dan AWS, dan, oleh karena itu APIs, konsol AMS dan. APIs

Contoh proses federasi

Contoh ini menggunakan Layanan Federasi Direktori Aktif (AD FS); namun, teknologi apa pun yang mendukung AWS IAM Federation didukung. Untuk informasi lebih lanjut tentang federasi IAM yang didukung AWS, lihat Mitra IAM dan Penyedia Identitas dan Federasi. CSDM Anda akan membantu Anda melalui proses ini, yang melibatkan upaya bersama dengan tim AD dan AMS Anda.

Untuk informasi terperinci tentang mengintegrasikan SAFL untuk akses API, lihat blog AWS ini, Cara Menerapkan API Federasi dan Akses CLI Menggunakan SAFL 2.0 dan AD FS.

Untuk contoh yang menginstal AMS CLI dan SALL, lihat Lampiran: Aturan klaim AD FS dan setelan SAFL.

Mengkonfigurasi federasi ke konsol AMS (MALZ)

Peran IAM dan penyedia identitas SAM (Entitas Tepercaya) yang dirinci dalam tabel berikut telah disediakan sebagai bagian dari infrastruktur AMS. Peran ini memungkinkan Anda untuk mengaudit dan melihat akun inti AMS.

Peran	Izin
AWSManagedServicesReadOnlyRole	Memungkinkan Anda melihat infrastruktur AMS di akun inti.
AWSManagedServicesCaseRole	Memungkinkan Anda melihat sumber daya di akun aplikasi baru Anda dan mengajukan insiden AMS dan permintaan layanan.
AWSManagedServicesChangeManagementRole	Memungkinkan Anda melihat infrastruktur AMS di akun inti, mengajukan tiket AWS Support, dan meminta beberapa RFCs.

Untuk daftar lengkap peran yang tersedia di berbagai akun, lihatPeran pengguna IAM di AMS.

Verifikasi akses konsol

Setelah Anda diatur dengan ADFS, dan memiliki URL AMS untuk digunakan untuk otentikasi, ikuti langkah-langkah ini.

Dengan konfigurasi Active Directory Federated Service (ADFS), Anda dapat mengikuti langkah-langkah berikut:

1. Buka jendela browser dan buka halaman masuk yang disediakan untuk Anda untuk akun Anda. IdpInitiatedSignOnHalaman ADFS untuk akun Anda terbuka.
2. Pilih tombol radio di sebelah Masuk ke salah satu situs berikut. Daftar pilih situs Masuk menjadi aktif.
3. Pilih situs signin.aws.amazon.com dan klik Masuk. Opsi untuk memasukkan kredensyal Anda terbuka.
4. Masukkan kredensyal CORP Anda dan klik Masuk. Konsol Manajemen AWS Terbuka.
5. Tempel ke bilah lokasi URL konsol AMS dan tekan Enter. Konsol AMS terbuka.

Verifikasi akses API

AMS menggunakan AWS API, dengan beberapa operasi khusus AMS yang dapat Anda baca di Referensi API AMS.

AWS menyediakan beberapa SDKs yang dapat Anda akses di Tools for Amazon Web Services. Jika Anda tidak ingin menggunakan SDK, Anda dapat melakukan panggilan API langsung. Untuk informasi tentang autentikasi, lihat Menandatangani Permintaan AWS API. Jika Anda tidak menggunakan SDK, atau membuat permintaan HTTP API langsung, Anda dapat menggunakan AMS CLIs for Change Management (CM) dan SKMS.

Instal AMS CLIs

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

1. Untuk menginstal AWS CLI, lihat Menginstal AWS Command Line Interface, dan ikuti petunjuk yang sesuai. Perhatikan bahwa di bagian bawah halaman itu ada instruksi untuk menggunakan installer yang berbeda, Linux, MS Windows, macOS, Virtual Environment, Bundled Installer (Linux, macOS, atau Unix).
2. Setelah instalasi, jalankan aws help untuk memverifikasi instalasi.
3. Setelah AWS CLI diinstal, untuk menginstal atau memutakhirkan AMS CLI, unduh file zip yang dapat didistribusikan AMS dan unzip. Anda dapat mengakses distribusi AMS CLI melalui tautan Dokumentasi di navigasi kiri konsol AMS, atau meminta manajer pengiriman layanan cloud (CSDM) Anda untuk mengirimkan file zip kepada Anda.

4. Buka Managed Cloud Distributables -> CLI -> Windows atau Managed Cloud Distributables -> CLI -> Linux/macOS direktori, tergantung pada sistem operasi Anda, dan:
5. Untuk Windows, jalankan penginstal yang sesuai (metode ini hanya berfungsi pada sistem Windows 32 atau 64 bit):
   - 32 Bit: ManagedCloud API_x86.msi
   - 64 Bit: ManagedCloud API_x64.msi
6. Untuk Mac/Linux, jalankan file bernama: MC_CLI.sh dengan menjalankan perintah ini: sh MC_CLI.sh. Perhatikan bahwa direktori amscm dan amsskms dan isinya harus berada di direktori yang sama dengan file MC_CLI.sh.
7. Jika kredensi perusahaan Anda digunakan melalui federasi dengan AWS (konfigurasi default AMS), Anda harus menginstal alat manajemen kredensi yang dapat mengakses layanan federasi Anda. Misalnya, Anda dapat menggunakan AWS Security Blog Cara Menerapkan API Federasi dan Akses CLI Menggunakan SAFL 2.0 dan AD FS untuk bantuan mengonfigurasi alat manajemen kredensi Anda.
8. Setelah instalasi, jalankan `aws amscm help` dan `aws amsskms help` untuk melihat perintah dan opsi.

MALZ: Orientasi akun aplikasi

Anda harus menyiapkan lingkungan AWS Managed Services (AMS) multi-akun dengan akun inti, sebelum meminta akun aplikasi baru. Berikut adalah langkah-langkah yang perlu Anda ambil setelah menyiapkan lingkungan Anda.

Topik

- Meminta akun aplikasi baru
- Menyiapkan Active Directory untuk mengfederasi akses ke peran AMS IAM
- Menyiapkan jaringan dengan akun Aplikasi baru
- Menyiapkan tambahan VPCs di akun Aplikasi

Untuk pertanyaan orientasi, hubungi manajer pengiriman layanan cloud (CSDM) Anda. Lihat juga Akun aplikasi: Dikelola AMS, Mode Dev, Dikelola pelanggan. Untuk informasi umum tentang mode, lihat mode AMSManajemen layanan di AWS Managed Services.

Untuk informasi tentang berbagai mode akun aplikasi, lihat Akun aplikasi: Dikelola AMS, Mode Dev, Dikelola Pelanggan. Untuk informasi umum tentang mode, lihat mode AMS.

Meminta akun aplikasi baru

Anda harus menyiapkan lingkungan AWS Managed Services (AMS) multi-akun dengan akun inti, sebelum meminta akun aplikasi baru. Untuk informasi tentang menyiapkan lingkungan multi-akun dengan akun inti, lihatMALZ: Orientasi akun inti.

Anda dapat memilih salah satu jenis VPC Amazon berikut untuk VPC awal di akun aplikasi:

- Pribadi: VPC ini tidak memiliki gateway Internet yang terpasang. Ini cocok untuk aplikasi pribadi yang tidak memerlukan akses to/from Internet.
- Publik: VPC ini memiliki gateway Internet yang terpasang dan memiliki subnet publik dan pribadi. Ini cocok untuk aplikasi publik yang membutuhkan akses to/from Internet.

Anda dapat meminta akun aplikasi baru dengan mengirimkan Deployment | Managed landing zone | Akun manajemen | Buat akun aplikasi (dengan VPC) (ct-1zdasmc2ewzrs) RFC dan memberikan nilai-nilai berikut di RFC:

- Nama Akun: Nama khusus untuk akun. Perhatikan bahwa Nama Akun memiliki panjang maksimum 50 karakter.
- Email Akun: Email daftar distribusi untuk akun. ID email ini digunakan untuk membuat akun AWS.
- Level Support: Tingkat AWS Support, Premium atau Plus.
- Nama VPC: Nama untuk VPC.
- Jumlah Availability Zone (AZs): 2 atau 3.
- VPC CIDR: Blok CIDR untuk VPC.
- Jenis Rute: Ini bisa berupa `routable` atau`isolated`. `Routable`berarti bahwa aplikasi yang VPCs terkait dengan tabel rute aplikasi Transit Gateway (TGW) dapat terhubung ke VPC ini. `Isolated`berarti bahwa aplikasi yang VPCs terkait dengan tabel rute aplikasi TGW tidak dapat terhubung ke VPC ini. Nilai default-nya `routable`.
- Tabel Rute Aplikasi Transit Gateway: Tabel rute Transit Gateway yang harus dikaitkan dengan akun aplikasi VPC. Jika tidak ada nilai yang diberikan, default `defaultAppRouteDomain` digunakan, yang berarti bahwa akun ini akan dapat berkomunikasi dengan semua akun lain di bawah tabel rute yang sama.

- PublicSubnetAZ *<1-3>* CIDRCIDR untuk subnet publik di AZ 1: CIDR untuk subnet publik di Availability Zone 1.
- PrivateSubnet*<1-10>*AZ *<I-3>* CIDRCIDR untuk subnet publik di AZ 1: CIDR untuk subnet publik di Availability Zone 1.

Pada titik ini, AMS menyebarkan akun aplikasi baru ke akun manajemen AMS Anda, dengan konfigurasi VPC yang ditentukan.

Menyiapkan Active Directory untuk mengfederasi akses ke peran AMS IAM

Federasi direktori Anda dengan peran AMS IAM untuk memungkinkan pengguna korporat menggunakan kredensi perusahaan mereka untuk berinteraksi dengan AWS Console dan AWS APIs, serta konsol AMS dan AMS. APIs

Contoh proses federasi

Contoh ini menggunakan Active Directory Federation Services (ADFS). Namun, teknologi apa pun yang mendukung AWS IAM Federation didukung. Untuk informasi selengkapnya tentang federasi IAM yang didukung AWS, lihat Mitra IAM dan Penyedia Identitas dan Federasi. CSDM Anda akan membantu Anda melalui proses ini, yang melibatkan upaya bersama dengan tim AD dan AMS Anda.

Untuk informasi terperinci tentang mengintegrasikan SALL untuk akses API, lihat blog AWS ini, Cara Menerapkan API Federasi dan Akses CLI Menggunakan SAFL 2.0 dan AD FS.

Untuk contoh yang menginstal AMS CLI dan SALL, lihat Lampiran: Aturan klaim AD FS dan setelan SAFL di Panduan Pengguna AMS.

Mengkonfigurasi federasi ke konsol AMS

Peran IAM dan penyedia identitas SAM (Entitas Tepercaya) yang dirinci dalam tabel berikut disediakan di akun aplikasi baru Anda. Peran ini memungkinkan Anda untuk mendapatkan akses ke akun dan file aplikasi baru RFCs, menulis ke bucket S3, dan melakukan tindakan lainnya.

Peran	Izin
AWSManagedServicesReadOnlyRole	Memungkinkan Anda melihat sumber daya di akun aplikasi baru Anda.

Peran	Izin
AWSManagedServicesCaseRole	Memungkinkan Anda melihat sumber daya di akun aplikasi baru Anda dan mengajukan tiket AWS Support.
AWSManagedServicesChangeManagementRole	Memungkinkan Anda melihat infrastruktur AMS di akun aplikasi, file, file tiket AWS Support RFCs, menulis ke bucket S3, mengelola rahasia Secrets Manager, dan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) yang dicadangkan.
AWSManagedServicesSecurityOpsRole	Memungkinkan Anda melihat infrastruktur AMS di akun aplikasi, mengelola rahasia Secrets Manager, mengelola aturan Firewall Aplikasi Web, mengelola sertifikat, dan mengajukan tiket AWS Support.
AWSManagedServicesAdminRole	Memungkinkan Anda melihat infrastruktur AMS di akun aplikasi, mengelola langganan Marketplace, mengelola rahasia Secrets Manager, mengelola aturan Firewall Aplikasi Web, mengelola sertifikat, membuat, mengelola EC2 instans Amazon Cadangan RFCs, menulis ke bucket S3, mengajukan tiket AWS Support, dan mengelola perjanjian AWS Artifacts.

Mengirimkan permintaan federasi ke AMS

Jika ini adalah akun pertama Anda, bekerjalah dengan Arsitek and/or Cloud CSDM Anda untuk menyediakan file XMLmetadata untuk penyedia identitas Anda.

Jika Anda memasukkan akun tambahan atau Penyedia Identitas dan memiliki akses ke akun manajemen atau akun aplikasi yang diinginkan, ikuti langkah-langkah ini.

1. Buat permintaan layanan dari konsol AMS.

> **Note**
>
> - Jika membuat penyedia identitas untuk akun aplikasi, kirimkan permintaan ini dari akun aplikasi itu sendiri atau akun manajemen.
> - Jika membuat penyedia identitas untuk akun inti AMS, kirimkan permintaan ini dari akun manajemen.
> - Jika membuat penyedia identitas untuk akun manajemen, kirimkan permintaan ini dari akun manajemen, atau hubungi CSDM Anda untuk bantuan.

Dalam permintaan layanan, berikan detail yang diperlukan untuk menambahkan penyedia identitas:

- AccountId dari akun tempat penyedia identitas baru akan dibuat.
- Nama penyedia identitas yang diinginkan, jika tidak disediakan, defaultnya adalah saml pelanggan; biasanya, ini harus sesuai dengan pengaturan yang dikonfigurasi di penyedia federasi Anda.
- Untuk akun yang ada, sertakan apakah penyedia identitas baru harus disebarkan ke semua peran konsol yang ada atau berikan daftar peran yang harus mempercayai penyedia identitas baru.
- Lampirkan file XHTML metadata yang diekspor dari agen federasi Anda ke permintaan layanan sebagai lampiran file.

2. Dari akun yang sama tempat Anda membuat permintaan layanan, buat RFC baru menggunakan CT-ID ct-1e1xtak34nx76 (Manajemen | Lainnya | Lainnya | Buat) dengan informasi berikut.

   - Judul: “IDP SAMP onboard <Name>untuk Akun < >”AccountId.
   - AccountId dari akun tempat penyedia identitas akan dibuat.
   - Nama penyedia identitas.
   - Untuk Akun yang Ada: Apakah penyedia identitas harus disebarkan ke semua peran konsol yang ada, atau daftar peran yang harus mempercayai penyedia identitas baru.
   - ID kasus permintaan layanan dibuat pada Langkah 1, di mana file XMLmetadata dilampirkan.

Verifikasi Akses Konsol

Setelah Anda diatur dengan AD FS, dan memiliki URL AMS untuk digunakan untuk otentikasi, Anda dapat melakukan prosedur berikut.

Dengan konfigurasi Active Directory Federated Service (AD FS), Anda dapat mengikuti langkah-langkah berikut:

1. Buka jendela browser dan buka halaman masuk yang disediakan untuk Anda untuk akun Anda. IdpInitiatedSignOnHalaman AD FS untuk akun Anda terbuka.
2. Pilih tombol radio di sebelah Masuk ke salah satu situs berikut. Daftar situs masuk menjadi aktif.
3. Pilih situs signin.aws.amazon.com dan pilih Masuk. Opsi untuk memasukkan kredensyal Anda terbuka.
4. Masukkan kredensyal CORP Anda dan pilih Masuk. AWS Management Console terbuka.
5. Tempel ke bilah lokasi URL konsol AMS dan tekan Enter. Konsol AMS terbuka.

Verifikasi Akses API

AMS menggunakan AWS API, dengan beberapa operasi khusus AMS yang dapat Anda baca di Referensi API AMS.

AWS menyediakan beberapa SDKs yang dapat Anda akses di Tools for Amazon Web Services. Jika Anda tidak ingin menggunakan SDK, Anda dapat melakukan panggilan API langsung. Untuk informasi tentang autentikasi, lihat Menandatangani Permintaan AWS API. . Jika Anda tidak menggunakan SDK, atau membuat permintaan HTTP API langsung, Anda dapat menggunakan AMS CLIs for Change Management (CM) dan SKMS.

Menyiapkan jaringan dengan akun Aplikasi baru

Menyiapkan jaringan untuk akun aplikasi termasuk mengonfigurasi aturan firewall dan berpotensi menyiapkan tabel rute Transit Gateway (TGW) tambahan.

Menyiapkan firewall Anda

Untuk menggunakan aplikasi yang digunakan di lingkungan AMS Anda, Anda harus membuat beberapa aturan firewall. Anda tidak memerlukan aturan ini untuk mengakses instance Anda, Anda dapat melompat melalui benteng ke instance Anda.

Aturan Firewall untuk Akses Aplikasi

Anda harus membuka port berikut untuk lalu lintas melalui firewall Anda:

- Dari jaringan on-premise Anda ke VPC aplikasi baru Anda CIDRs di kedua arah masuk dan keluar.
- Dari VPC aplikasi baru Anda CIDRs ke jaringan on-premise Anda di kedua arah masuk dan keluar (jika aplikasi cloud Anda perlu menjangkau aplikasi on-premise Anda).

Port	Protokol	Layanan	Dari/Ke	Ke/Dari
80	TCP	Akses Web HTTP	Pada Jaringan Premis	Aplikasi AMS VPC
443	TCP	Akses Web HTTPS	Pada Jaringan Premis	Aplikasi AMS VPC

Menyiapkan tabel rute aplikasi gateway transit tambahan

Jaringan AWS Managed Services (AMS) fleksibel dan mendukung berbagai kasus penggunaan jaringan.

- Komunikasi antar aplikasi VPCs di akun yang sama.
- Komunikasi antar aplikasi VPCs di akun yang berbeda.
- Isolasi antar aplikasi VPCs di akun yang berbeda.
- Isolasi antara aplikasi VPCs dalam akun yang sama.

Jika Anda memiliki unique/special persyaratan untuk jaringan, hubungi AMS Cloud Architect Anda dan mereka akan mengembangkan rencana agar persyaratan Anda dipenuhi oleh arsitektur jaringan AMS.

Berdasarkan keputusan jaringan yang diambil untuk akun aplikasi VPCs, Anda dapat membuat beberapa tabel rute aplikasi Transit Gateway (TGW) dengan mengirimkan Deployment | Managed landing zone | Akun jaringan | Buat tabel rute gateway transit (ct-3dscwaeyi6cup) RFC.

Jenis perubahan mengharuskan Anda untuk menentukan `TransitGatewayRouteTableName` (nama yang berarti untuk tabel rute TGW),`TransitGatewayId`, dan. `TGWRouteTableType`

> **Note**
>
> Jika createCustomRoute Domain dipilih TGWRouteTableType, tabel rute yang dibuat kosong. Anda harus mengajukan RFC dengan jenis perubahan Deployment | Managed landing zone | Networking account | Add static route (ct-3r2ckznmt0a59).

Menyiapkan tambahan VPCs di akun Aplikasi

Anda dapat meminta akun aplikasi tambahan VPC dengan mengirimkan Deployment | Managed landing zone | Akun aplikasi | Buat VPC (ct-1j3503fres5a5) RFC.

Ini bekerja dengan cara yang sama seperti mengonfigurasi VPC untuk akun aplikasi baru. Lihat perinciannya di Meminta akun aplikasi baru.

Lampiran: daftar pertimbangan orientasi multi-akun landing zone (MALZ)

Ada sejumlah pertimbangan utama yang perlu Anda pikirkan dalam merencanakan penerapan landing zone multi-akun AMS Anda. Pilihan Anda akan memberi AMS informasi yang diperlukan untuk menentukan komponen infrastruktur yang Anda perlukan. Cloud Architect (CA) Anda akan memberi Anda kuesioner untuk membantu pekerjaan ini.

Topik

- Konfigurasi akun landing zone multi-akun AMS
- Peringatan pemantauan landing zone multi-akun AMS
- Konfigurasi jaringan
- Konfigurasi Direktori Aktif
- Perlindungan Titik Akhir Trend Micro (EPS)
- Akses: Bastion, SSH dan RDP
- Federation

> **Note**
>
> Untuk informasi selengkapnya tentang jenis instans, lihat Jenis EC2 Instance Amazon.

Untuk informasi selengkapnya tentang jenis instans database, lihat Jenis Instans Amazon RDS.
Jika Anda memerlukan Direct connect, lihat Panduan Onboarding landing zone akun tunggal AMS untuk membuat koneksi Direct Connect.

Anda akan menerima kuesioner orientasi dari Cloud Service Delivery Manager (CSDM) yang berisi pertanyaan tentang pengaturan konfigurasi yang Anda inginkan untuk akun Anda. Bekerja dengan CSDM Anda untuk mengisi kuesioner sebelum melanjutkan.

Konfigurasi akun landing zone multi-akun AMS

- ID Akun Baru

  Akun AWS ID yang Anda buat untuk landing zone multi-akun AMS. Seharusnya tidak menjadi bagian dari AWS organisasi.
- Wilayah Layanan

  Wilayah utama di mana lingkungan landing zone multi-akun AMS akan digunakan.
- Email akun inti untuk notifikasi. (ini semua harus berada dalam domain yang sama). Berikan alamat email untuk masing-masing:
  - Akun Layanan Bersama
  - Akun jaringan
  - Logging akun
  - Akun keamanan
- Jenis layanan Anda, Premium atau Plus

  Ini menentukan perjanjian tingkat layanan (SLAs) untuk menyelesaikan masalah di lingkungan Anda

Peringatan pemantauan landing zone multi-akun AMS

AMS menyediakan cara bagi Anda untuk diperingatkan secara langsung (versus mendapatkan pemberitahuan layanan AMS) untuk peringatan pemantauan tertentu. Untuk mendaftar, pastikan Cloud Architect (CA) atau Cloud Service Delivery Manager (CSDM) Anda menerima informasi ini:

Direct Alerts Email: Ini adalah alamat email yang Anda ingin AMS untuk mengirim peringatan berbasis sumber daya tertentu. Untuk detail peringatan mana yang dikirim langsung ke email, lihat Peringatan dari pemantauan dasar di AMS di Panduan Pengguna Lanjutan AMS. Untuk informasi selengkapnya tentang pemantauan AMS, lihat Manajemen Pemantauan di Panduan Pengguna AMS untuk Zona Pendaratan Akun Tunggal.

Konfigurasi jaringan

- Nomor ASN Transit Gateway

  Ini adalah Autonomous System Number (ASN) untuk sisi AWS dari sesi Border Gateway Protocol (BGP), harus unik dan tidak boleh sama dengan yang digunakan untuk Direct Connect atau VPN Anda. Kisarannya adalah 64512 hingga 65534 (inklusif) untuk 16-bit. ASNs

- Infrastruktur landing zone multi-akun AMS Anda, rentang VPC CIDR.

  Rentang CIDR ini tidak dapat tumpang tindih dengan jaringan lokal Anda

  Anda dapat menyertakan rentang CIDR /22, atau menyediakan setiap CIDR VPC satu per satu. Perhatikan bahwa hanya rentang CIDR ini yang diizinkan:

  - 10.0.0.0 - 10.255.255.255 (prefiks 10/8)
  - 172.16.0.0 - 172.31.255.255 (prefiks 172.16/12)
  - 192.168.0.0 - 192.168.255.255 (prefiks 192.168/16)

  Perhatikan bahwa rentang IP 198.18.0.0/15 tidak dapat digunakan (ini dicadangkan oleh AWS Directory Service).

  - Rentang CIDR VPC Infrastruktur Inti (/rentang 22 direkomendasikan)
  - Jaringan VPC CIDR rentang (/24 rentang direkomendasikan)
  - Jangkauan CIDR VPC Layanan Bersama (/23 rentang direkomendasikan)
  - Rentang CIDR VPC DMZ (/rentang 25 direkomendasikan)

- VPN ECMP (mengaktifkan atau menonaktifkan)

  Untuk dukungan VPN ECMP, pilih aktifkan jika Anda memerlukan dukungan perutean Equal Cost Multipath (ECMP) antara koneksi VPN. Jika koneksi mengiklankan hal yang sama CIDRs, lalu lintas didistribusikan secara merata di antara mereka.

Daftar kontrol akses jaringan (NACL)

Network Access Control List (NACL) adalah lapisan keamanan opsional untuk VPC Anda yang bertindak sebagai firewall untuk mengontrol lalu lintas masuk dan keluar dari satu atau lebih subnet. Anda dapat mengatur jaringan ACLs dengan aturan yang mirip dengan grup keamanan Anda untuk menambahkan lapisan keamanan tambahan ke VPC Anda. Untuk informasi selengkapnya tentang perbedaan antara grup keamanan dan jaringan ACLs, lihat Perbandingan grup keamanan dan jaringan ACLs.

Namun, di AMS multi-account landing zone, agar AMS dapat mengelola dan memantau Infrastruktur secara efektif, penggunaan NACLs terbatas pada cakupan berikut:

- NACLs tidak didukung di akun inti landing zone multi-akun: Manajemen, Jaringan, Layanan Bersama, Logging, dan Keamanan.
- NACLs didukung di akun aplikasi landing zone multi-akun selama hanya digunakan sebagai daftar “Tolak”. Selain itu, mereka harus memiliki “Izinkan Semua” yang dikonfigurasi untuk memastikan pemantauan AMS dan operasi manajemen.

Di lingkungan multi-akun berskala besar, Anda juga dapat memanfaatkan fitur seperti firewall jalan keluar terpusat untuk mengontrol lalu lintas keluar dan/atau tabel perutean Transit AWS Gateway di landing zone multi-akun AMS untuk memisahkan lalu lintas jaringan. VPCs

Konfigurasi Direktori Aktif

Domain FQDN untuk Direktori Aktif yang dikelola AMS

Perlindungan Titik Akhir Trend Micro (EPS)

- Ukuran instans untuk EC2 instans dan grup Auto Scaling

  Trend Micro Endpoint Protection (EPS) adalah komponen utama dalam AMS untuk keamanan sistem operasi. Sistem ini terdiri dari instans Deep Security Manager (DSM), EC2 instans relay, dan agen yang ada di semua bidang data AMS dan EC2 instans Anda. EC2

  - Jenis instans relai (minimum yang didukung oleh AMS adalah m5.large)
  - Ukuran instans DB (disarankan 200 GB)
  - Jenis instance RDS (hanya db.m5.large atau db.m5.xlarge yang diizinkan)
- Jenis Lisensi DSM (Marketplace atau BYOL)

Jika Anda sudah memiliki lisensi, pilih BYOL (bawa lisensi Anda sendiri). AMS akan menghubungi Anda untuk mendapatkan informasi yang diperlukan tentang lisensi.

- AWS Pengguna IAM atau nama sumber daya Amazon peran (ARN) untuk Langganan Trend Micro Deep Security (Peran ARN: arn:aws:iam: ::role/) *ACCOUNT_ID ROLE_NAME*

  Berikan kami peran IAM; ARN, atau ARN pengguna IAM dari salah satu ARN Anda yang ada yang dapat Akun AWS Anda akses. AMS membuat peran IAM; di akun Layanan Bersama landing zone multi-akun AMS Anda dan menambahkan peran atau pengguna yang diberikan dalam kepercayaan peran IAM dalam Layanan Bersama sehingga peran tersebut dapat diasumsikan oleh Anda untuk berlangganan Trend Micro Deep Security di. AWS Marketplace

Akses: Bastion, SSH dan RDP

- Pengaturan SSH Bastion

  AMS menyediakan benteng SSH di akun Layanan Bersama Anda untuk mengakses host di lingkungan AMS. Untuk mengakses jaringan AMS sebagai pengguna SSH, Anda harus menggunakan SSH Bastions sebagai titik masuk. Jalur jaringan berasal dari jaringan On-Prem, melewati DX/VPN gateway transit (TGW), dan kemudian dirutekan ke VPC Layanan Bersama. Setelah Anda dapat mengakses benteng, Anda dapat melompat ke host lain di lingkungan AMS Anda, asalkan permintaan akses yang tepat telah diberikan.

  - Jumlah instans yang diinginkan (disarankan 2)
  - Contoh maksimum (4 disarankan)
  - Contoh minimum (disarankan 2)
  - Jenis instans (disarankan m5.large)
  - Ingress CIDRs: Rentang alamat IP dari mana pengguna di jaringan Anda akan mengakses SSH Bastions (rentang ip 1, rentang ip 2, rentang ip 3,... dll)
- Pengaturan RDP Bastion

  AMS secara opsional menyediakan benteng RDP di akun Layanan Bersama Anda untuk mengakses host di lingkungan AMS. Untuk mengakses jaringan AMS sebagai pengguna RDP, Anda harus menggunakan RDP Bastions sebagai titik masuk. Jalur jaringan berasal dari jaringan On-Prem, melewati DX/VPN ke TGW, dan kemudian dirutekan ke VPC Layanan Bersama. Setelah Anda dapat mengakses benteng, Anda dapat melompat ke host lain di lingkungan AMS, asalkan permintaan akses yang tepat telah diberikan.

  - Jenis instans (disarankan t3.medium)
  - Sesi minimum yang diinginkan (disarankan 2)
  - Sesi maksimum yang diinginkan (disarankan 10)
- Jenis Konfigurasi Bastion RDP, Standar Bersama atau HA Bersama (default adalah Standar Bersama)

  SecureStandard = Seorang pengguna menerima satu benteng dan hanya satu pengguna yang dapat terhubung ke benteng.

  SecureHa = Seorang pengguna menerima dua benteng dalam dua AZ yang berbeda untuk terhubung dan hanya satu pengguna yang dapat terhubung ke benteng.

  SharedStandard = Seorang pengguna menerima satu benteng untuk terhubung dan dua pengguna dapat terhubung ke benteng yang sama sekaligus.

  SharedHa = Seorang pengguna menerima dua benteng dalam dua AZ yang berbeda untuk terhubung dan dua pengguna dapat terhubung ke benteng yang sama sekaligus.

Federation

Nama Penyedia Identitas (IDP)

Default ke `customer-saml`

Orientasi AMS Single-account landing zone (SALZ)

Proses orientasi AMS SALZ

Untuk melakukan onboard akun landing zone (SALZ) akun AMS single-account, Anda harus mengambil langkah-langkah berikut:

1. Buat akun AWS baru yang dikonfigurasi AMS sebagai akun jaringan untuk meng-host firewall. Buat akun baru dalam organisasi AWS Anda, jika Anda memilikinya. AMS akan mengikuti prosedur pembuatan akun AMS normal, sehingga semua informasi yang diperlukan harus dikumpulkan (misalnya CIDR, lisensi EPS, dan pengguna). Catatan: Alokasi CIDR /24 bagus.
2. Tentukan apakah Anda ingin menghapus gateway Internet (IGWs) dari akun lalu lintas jalan keluar atau tidak.
3. Tentukan domain Anda yang disetujui. AMS memungkinkan pemfilteran tujuan dengan mempertahankan daftar domain yang disetujui; daftar dapat dimodifikasi nanti.
4. Konfirmasikan ukuran instans yang ingin Anda gunakan berdasarkan throughput yang Anda harapkan. Secara default, instance dibuat dalam instance m4.xlarge di mana kami telah menemukan bahwa throughput firewall adalah 350Mbps. AMS dapat meningkatkan ukuran menjadi instance C4.8xLarge dengan throughput yang diharapkan adalah 1,25 Gbps.
5. Siapkan jaringan antara AMS dan jaringan pribadi Anda. Ini melibatkan beberapa tugas:
    a. Alokasikan ruang IP
    b. Membangun konektivitas jaringan pribadi ke AWS
    c. Siapkan firewall Anda
    d. Siapkan manajemen akses
    e. Jadwalkan pencadangan
6. Berikan akses ke akun yang dibuat ke AMS.
7. Validasi bahwa layanan AMS beroperasi dengan benar.

AMS akan dapat melakukan pembuatan akun (orientasi) akun Anda dalam waktu 2 minggu (10 hari kerja) sejak tanggal permintaan awal. Setiap kegiatan tindak lanjut dapat dilakukan dengan menggunakan AMS Planned Event Management (PEM).

Note

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

Daerah baru sering ditambahkan. Untuk daftar terbaru, lihat Wilayah AWS dan zona ketersediaan.

Arsitektur jaringan SALZ

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

AMS mengonfigurasi semua aspek jaringan untuk Anda berdasarkan templat standar kami dan opsi pilihan Anda yang disediakan selama orientasi. Desain jaringan AWS standar diterapkan ke akun AWS Anda, dan virtual private cloud (VPC) dibuat untuk Anda dan terhubung ke AMS oleh VPN.

atau Direct Connect. Pelajari selengkapnya tentang Direct Connect di AWS Direct Connect. Standar VPCs termasuk DMZ, layanan bersama, dan subnet aplikasi. Selama proses orientasi, tambahan VPCs mungkin diminta dan dibuat agar sesuai dengan kebutuhan Anda (misalnya, divisi pelanggan, mitra). Setelah onboarding, Anda diberikan diagram jaringan. dokumen lingkungan yang menjelaskan bagaimana jaringan Anda telah diatur.

> **Note**
>
> Untuk mempelajari batasan dan batasan layanan default untuk semua layanan aktif, lihat dokumentasi AWS Service Limits.

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

Layanan bersama landing zone akun tunggal AMS

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

- Layanan Direktori AMS = Pengontrol Domain AD

  Membuat Direktori Aktif di akun AMS, membuat domain AMS, menggabungkan tumpukan terkelola ke domain saat diluncurkan.
- Host manajemen = Host Manajemen AMS (mengotomatiskan penyediaan dan tugas umum)

  Bertindak sebagai endpoint API untuk memodifikasi Directory Service, berinteraksi dengan pengontrol Directory Service domain.
- Layanan keamanan: Server manajemen Antivirus (TrendMicro) = EPS DSM+EPS Relay

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

- Host benteng internal = Benteng pelanggan

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

SALZ: Buat AWS akun baru untuk AMS

Lima langkah untuk membuat AWS akun baru untuk AWS Managed Services (AMS) adalah:

1. Buat sebuah Akun AWS
2. Siapkan tagihan konsolidasan—tautkan akun baru ke akun Pembayar
3. Konfigurasikan Akun AWS akses AMS Anda
4. Amankan akun baru dengan otentikasi multi-faktor (MFA) untuk pengguna root di AMS
5. Berlangganan AWS Marketplace untuk EPS

Silakan hubungi manajer pengiriman layanan pelanggan (CSDM) Anda jika Anda memiliki pertanyaan.

Buat sebuah Akun AWS

Program AMS memerlukan penyediaan akun Amazon Web Services (AWS) baru. Petunjuk langkah demi langkah tersedia di video berikut: Bagaimana cara membuat dan mengaktifkan akun Amazon Web Services baru? Langkah-langkah sederhananya adalah:

Mendaftar untuk Akun AWS

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

Untuk mendaftar untuk Akun AWS

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

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

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

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

Buat pengguna dengan akses administratif

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

Amankan Anda Pengguna root akun AWS

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

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

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

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

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

Masuk sebagai pengguna dengan akses administratif

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

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

Tetapkan akses ke pengguna tambahan

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

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

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

> **Note**
>
> Jika Anda sudah memiliki akun, Anda dapat membuka halaman AWS Harga dan klik Buat Akun Gratis. Pastikan untuk mendaftar ke EC2 Layanan, setidaknya. Mendaftar untuk satu layanan memungkinkan Anda mengakses semua layanan di AWS. Anda hanya membayar biaya layanan yang Anda gunakan.
> Jika Anda berencana untuk menautkan akun baru Anda ke akun pembayar untuk tujuan penagihan konsolidasi, Anda tidak perlu memasukkan informasi metode pembayaran saat diminta. Sebagai gantinya, setelah Anda mencapai layar untuk memasukkan informasi kartu kredit, cukup navigasikan. Anda akan memerlukan alamat email yang terkait dengan akun pembayar untuk mengirim permintaan billing/linked akun konsolidasi yang dirinci di bagian berikutnya.

> **Important**
>
> Sangat penting bahwa Anda memastikan bahwa alamat email dan nomor telepon dikaitkan dengan akun sehingga Anda menerima tanggapan terhadap insiden keamanan potensial. Nomor telepon dan alamat email untuk akun tidak dapat diubah tanpa mengatur ulang kata

sandi akun, yang merupakan upaya signifikan untuk akun root AMS. Untuk memastikan bahwa nilai-nilai ini stabil, sangat penting untuk memilih informasi kontak yang tidak terkait dengan individu, yang dapat berubah. Pilih alias email yang dapat menunjuk ke grup. Ikuti praktik terbaik yang sama dalam memilih nomor telepon: pilih nomor yang dapat menunjuk ke grup atau nomor yang dimiliki oleh perusahaan dan bukan individu.

Siapkan tagihan konsolidasan—tautkan akun baru ke akun Pembayar

Jika Anda ingin Akun AWS tagihan yang dikelola AMS baru Anda dimasukkan ke dalam pembayaran untuk akun AWS Organizations manajemen yang ada, Anda perlu menyiapkan penagihan konsolidasi dan menautkan akun. Untuk detail tentang melakukan ini, lihat

- Penagihan konsolidasi untuk AWS Organizations dan Strategi Penagihan AWS Multi-Akun.
- Mengundang Akun AWS untuk bergabung dengan organisasi Anda

> **Note**
>
> Anda dapat melakukan langkah-langkah ini sebelum melakukan serah terima akun ke AMS. Setelah serah terima, langkah-langkah untuk bergabung dengan organisasi Anda (disediakan di atas) dapat dilakukan melalui proses manajemen perubahan. Konsultasikan dengan manajer pengiriman layanan cloud (CSDM) atau arsitek cloud (CA) Anda jika Anda memerlukan bantuan.

Untuk informasi penagihan umum termasuk mengelola penagihan konsolidasi, lihat Apa itu Penagihan. AWS Untuk AWS Organizations informasi umum tentang bagaimana akun dapat bekerja sama, lihat Apa itu AWS Organizations. Untuk panduan preskriptif tentang akun AWS Organizations manajemen, lihat Akun manajemen, akses tepercaya, dan administrator yang didelegasikan

Konfigurasikan Akun AWS akses AMS Anda

Dengan langkah-langkah di atas selesai, Anda telah berhasil mengamankan biaya terkait baru Akun AWS dan memastikan ditagih dengan tepat. Langkah terakhir dalam proses ini adalah mengizinkan akses AMS ke akun baru untuk konfigurasi tumpukan awal dan agar permintaan perubahan dan penyediaan yang sedang berlangsung dipenuhi. Untuk detailnya, baca Mendelegasikan Akses Lintas AWS Akun Menggunakan Peran IAM. Langkah-langkah dasar dijelaskan di bagian ini.

Aktifkan akses ke AWS situs web

Untuk memberikan pengguna IAM Anda akses ke informasi dan alat penagihan akun Anda, Anda harus mengaktifkan fungsionalitas tersebut.

Ikuti langkah-langkah ini:

1. Masuk ke Konsol Manajemen AWS dengan kredensi akun root Anda (email dan kata sandi yang Anda gunakan untuk membuat). Akun AWS Jangan masuk dengan kredensi pengguna IAM Anda.

   Konsol Manajemen AWS Halaman beranda terbuka.
2. Di bilah navigasi atas, buka menu tarik-turun untuk nama akun Anda, lalu pilih Akun Saya.

   Halaman beranda Penagihan terbuka.
3. Gulir ke bawah ke area Akses Pengguna IAM ke Informasi Penagihan, dan klik Edit di sisi kanan. *`The area does not appear unless you are logged in with root credentials`*.

   Area akses Activate IAM terbuka.
4. Pilih kotak centang dan klik Perbarui.

   Anda sekarang dapat menggunakan kebijakan IAM untuk mengontrol halaman mana yang dapat diakses pengguna.

Untuk detail selengkapnya tentang proses ini AWS, lihat Ikhtisar mengelola izin akses.

Buat peran IAM dengan akses ke situs web AWS

AWS Identity and Access Management (IAM) adalah layanan web yang membantu Anda mengontrol akses ke AWS sumber daya dengan aman bagi pengguna Anda. Anda menggunakan IAM untuk mengontrol siapa yang dapat menggunakan AWS sumber daya Anda (otentikasi) dan sumber daya apa yang dapat mereka gunakan dan dengan cara apa (otorisasi).

1. Buka Konsol Manajemen IAM, klik Peran di panel navigasi kiri.

   Halaman manajemen peran terbuka dengan informasi tentang peran IAM, opsi Buat peran, dan daftar peran yang ada.

2. Klik Buat peran.

Buat peran Pilih jenis halaman entitas tepercaya terbuka. Klik Lainnya Akun AWS dan area pengaturan terbuka di bawah ini.

Masukkan ID Akun AMS tepercaya yang diberikan kepada Anda oleh AMS. Biarkan opsi Memerlukan ID eksternal dan Memerlukan MFA tidak dipilih.

3. Klik Berikutnya: Izin.

   Halaman Buat peran Lampirkan kebijakan izin terbuka dengan opsi untuk membuat kebijakan baru, menyegarkan halaman, dan mencari kebijakan yang ada. Daftar kebijakan yang ada disediakan.

4. Pilih AdministratorAccesskebijakan dan kemudian klik Berikutnya: Tinjau.

   Halaman Create role Review akan terbuka.

5. Beri nama peran baru aws_managedservices_onboarding_role dan ketik “AMS Onboarding Role” untuk deskripsi Peran. Tinjau pengaturan untuk peran baru dan, jika puas, klik Buat peran.

   Halaman manajemen peran terbuka dengan daftar peran baru Anda.

Berlangganan AWS Marketplace untuk EPS

Perubahan terbaru pada keamanan titik akhir AMS (EPS) mengharuskan Anda untuk berlangganan TrendMicro Deep Security melalui AWS Marketplace dan menerima persyaratan perangkat lunak.

TrendMicro menawarkan dua model lisensi: Per Jam Instans yang Dilindungi dan Bawa Lisensi Anda sendiri (BYOL).

- BYOL:
  1. Anda menggunakan lisensi Anda sendiri yang telah Anda beli melalui saluran eksternal.
  2. Anda harus memberikan semua kunci lisensi ke AMS untuk membangun infrastruktur EPS. Anda dapat memberikan kode aktivasi yang melisensikan semua modul, atau kode aktivasi individu yang melisensikan satu set modul tertentu. AMS hanya membuat file lisensi yang sesuai

dengan kode aktivasi yang Anda berikan. Karena aktivasi lisensi terjadi selama orientasi, di hadapan insinyur utama AMS dan CSDM, Anda dapat membagikan informasi itu kemudian.

3. Selain itu, Anda harus berlangganan Langganan AMI BYOL TrendMicro Market Place. Lihat Trend Micro Deep Security (BYOL).

- Per Jam Instans yang Dilindungi:
  1. Dalam langganan ini, Anda tidak diharuskan memiliki lisensi Trend yang diperoleh sebelumnya.
  2. Namun, Anda harus berlangganan langganan Marketplace.
  3. Tidak diperlukan pembagian kunci lisensi dengan AMS dalam model ini, karena penggunaan Trend diukur secara otomatis termasuk penggunaan EC2 infrastruktur lisensi perangkat lunak+. Lihat Trend Micro Deep Security.

Untuk berlangganan Trend Micro, ikuti langkah-langkah berikut:

1. Login ke Anda Akun AWS.
2. Arahkan ke halaman produk Trend Micro Deep Security (BYOL atau Per Protected Instance Hour).
3. Klik Lanjutkan untuk Berlangganan di panel kanan.
4. Klik Terima Ketentuan di sudut kanan atas.

Aktifkan IDS dan IPS di Trend Micro Deep Security

Anda dapat meminta agar AMS mengaktifkan Trend Micro Intrusion Detection System (IDS) dan Intrusion Protection Systems (IPS), fitur non-default, untuk akun Anda.

Untuk melakukan ini, kirimkan permintaan pembaruan (Manajemen | Lainnya | Lainnya | Pembaruan) dan sertakan daftar alamat email untuk menerima pemberitahuan ID dan IPS. Alamat ini ditambahkan ke topik SNS di akun Anda, yang dibuat AMS untuk Anda.

> **Note**
>
> AMS tidak dapat menambahkan layanan Trend Micro yang mungkin mengganggu kemampuan kami untuk menyediakan layanan AMS lainnya.

Langkah selanjutnya: Amankan akun baru dengan otentikasi multi-faktor (MFA) untuk pengguna root di AMS

Berlangganan AWS Marketplace untuk CentOS 7.6

AMS sekarang menyediakan CentOS 7 (x86_64) - dengan Pembaruan HVM yang dijual oleh CentOs.org, sebagai AMS AMI. Untuk memanfaatkan AMI ini, Anda harus ikut serta dalam lisensi OS Cent GRATIS, dan menerima lisensi di semua akun AMS Anda.

Untuk berlangganan, buka AWS Marketplacedan ikuti instruksi untuk ikut serta.

Anda tidak akan dikenakan biaya perangkat lunak untuk menggunakan produk ini, tetapi Anda masih bertanggung jawab atas AWS biaya lain, termasuk EC2 penggunaan. Jika ini adalah produk “Bawa Lisensi Anda Sendiri”, Anda harus memiliki lisensi perangkat lunak yang valid untuk menggunakannya.

Anda dapat meninjau informasi untuk perangkat lunak ini di CentOS 7 (x86_64) - with Updates HVM.

Amankan akun baru dengan otentikasi multi-faktor (MFA) untuk pengguna root di AMS

Bagian ini telah disunting karena berisi informasi sensitif terkait keamanan AMS. Informasi ini tersedia melalui Dokumentasi konsol AMS. Untuk mengakses Artifact AWS, Anda dapat menghubungi CSDM Anda untuk mendapatkan petunjuk atau membuka Memulai dengan Artifact AWS.

SALZ: Mengatur jaringan

Ada beberapa proses yang perlu diselesaikan untuk menyiapkan jaringan untuk AWS Managed Services (AMS):

1. Mengalokasikan ruang IP untuk lingkungan AMS Anda
2. Membangun konektivitas jaringan pribadi ke AWS
3. Menyiapkan firewall Anda untuk mengizinkan operasi AMS

Alokasikan Ruang IP untuk Lingkungan AMS Anda

AMS dirancang dan diuji menggunakan blok CIDR /16 sebagai alokasi jaringan yang direkomendasikan. Penting bahwa jaringan tepercaya yang terhubung ke AMS menggunakan blok CIDR yang tidak tumpang tindih dengan blok CIDR yang ditetapkan ke AMS. Alamat ini diperlukan

untuk mengatur virtual private cloud (VPC) dan subnet Anda. Untuk informasi selengkapnya tentang AWS VPCs, lihat Batas VPC Amazon dan Amazon VPC. FAQs

Sementara blok CIDR /16 mungkin tampak seperti banyak alamat IP, VPC, setelah dibuat, tidak dapat diperluas. Jadi alokasi ini memastikan bahwa VPC yang dikelola AMS Anda dapat berfungsi untuk jangka waktu yang cukup lama. Dalam blok CIDR, Anda harus mengalokasikan rentang alamat IP untuk, setidaknya, dua subnet pribadi dan dua subnet publik.

AWS menerima konektivitas ke lingkungan AMS melalui fungsionalitas AWS virtual private network (VPN) asli. Di pihak Anda, ini dapat dicapai melalui AWS Direct Connect (DX), VPN perangkat keras, atau VPN perangkat lunak. Di sisi AMS, kami menggunakan fungsionalitas Virtual Gateway dari VPCs.

Komponen Lingkungan Dasar

Opsi Network-to-Amazon	Konektivitas VPC Pengguna
Perangkat Keras VPN	Membuat koneksi VPN perangkat keras dari peralatan jaringan Anda di jaringan jarak jauh ke peralatan jaringan yang dikelola AMS yang terpasang ke VPC Anda.
AWS Direct Connect (DX)	Menetapkan koneksi pribadi, logis (atau terenkripsi jika digunakan dengan VPN) dari jaringan jarak jauh Anda ke Amazon VPC, memanfaatkan AWS Direct Connect.
Perangkat Lunak VPN	Membuat koneksi VPN dari peralatan Anda di jaringan jarak jauh ke perangkat lunak VPN yang dikelola pengguna yang berjalan di dalam VPC Amazon.

> **Note**
>
> AMS merekomendasikan koneksi VPN pribadi ke DX yang berlebihan. Manajer pengiriman layanan pelanggan (CSDM) Anda akan membantu dalam mengatur ini pada saat orientasi akun Anda.

Membangun Konektivitas Jaringan Pribadi ke AWS

Tambahkan AMS ke Active Directory perusahaan Anda untuk membangun konektivitas. Anda mungkin ingin melakukan tindakan administratif atau akses pengguna melalui koneksi jaringan pribadi. AWS menawarkan konektivitas VPN dan jalur khusus melalui Direct Connect. Langkah-langkah berikut menjelaskan cara bekerja dengan AMS untuk menetapkan salah satu (atau keduanya) sarana konektivitas.

Pengaturan VPN

Bagian ini menjelaskan langkah-langkah dasar untuk menyiapkan VPN untuk berkomunikasi antara VPC yang dikelola AMS dan jaringan internal Anda.

> **Note**
>
> Untuk mendapatkan pemahaman menyeluruh tentang penggunaan VPN dengan layanan AWS, lihat Apa itu AWS Site-to-Site VPN dan semua tentang Gateway Pelanggan Anda (perangkat VPN Anda).

Ikuti Panduan Pengguna AWS VPN Memulai dan Menguji bagian Koneksi Site-to-Site VPN untuk menyelesaikan langkah-langkah berikut.

- Langkah 1: Di AWS VPC Anda, Buat Gateway Pelanggan
- Langkah 2: Di AWS VPC Anda, Buat Gateway Pribadi Virtual
- Langkah 3: Di AWS VPC Anda, Aktifkan Propagasi Rute di Tabel Rute Anda
- Langkah 4: Di AWS VPC Anda, Perbarui Grup Keamanan Anda untuk Mengaktifkan Akses SSH, RDP, dan ICMP Masuk
- Langkah 5: Di Jaringan internal Anda, Buat Koneksi VPN dan Konfigurasikan Gateway Pelanggan
- Langkah 6: Uji konektivitas VPN antara VPC dan jaringan internal Anda

Direct Connect Pengaturan

Bagian ini menjelaskan langkah-langkah dasar untuk menyiapkan Direct Connect (DX) untuk berkomunikasi antara VPC yang dikelola AMS dan jaringan internal Anda.

> **Note**
>
> Untuk informasi tentang penggunaan DX dengan layanan AWS, lihat Memulai di Direct Connect Lokasi.

Untuk mengatur koneksi DX, Anda harus menyelesaikan langkah-langkah berikut:

1. Mendaftar untuk Amazon Web Services
2. Kirim Permintaan Koneksi AWS Direct Connect
3. Selesaikan Cross Connect
4. (Opsional) Konfigurasikan Koneksi Redundan dengan AWS Direct Connect
5. Dilakukan oleh AMS: Buat Antarmuka Virtual
6. Dilakukan oleh AMS: Unduh Konfigurasi Router
7. Verifikasi Antarmuka Virtual Anda

Siapkan Firewall Anda

Bagian ini telah disunting karena berisi informasi sensitif terkait keamanan AMS. Informasi ini tersedia melalui Dokumentasi konsol AMS. Untuk mengakses Artifact AWS, Anda dapat menghubungi CSDM Anda untuk mendapatkan petunjuk atau membuka Memulai dengan Artifact AWS.

Opsi AMS Bastion selama Migrasi/Orientasi Aplikasi

Untuk memberi Anda pengalaman terbaik selama upaya migrasi, di bawah ini adalah opsi potensial yang saat ini dapat dimanfaatkan AMS:

- Opsi 1: Bypass Bastion hanya untuk upaya migrasi (Anda harus menandatangani ini untuk tujuan keamanan sebagai tindakan sementara).

  Catatan: Kemampuan audit akan tetap ada untuk memastikan AMS memiliki visibilitas ke setiap permintaan.
- Opsi 2: SSH Tunneling dengan alat pilihan; misalnya, PuTTy, seperti yang diilustrasikan.

  Komponen lingkungan yang dijelaskan sudah perlu ada untuk opsi ini.

  AMS akan memberikan catatan dan instruksi tambahan.

Langkah-langkah tunneling SSH dengan Pu: TTy

Dalam PuTTY, Anda akan membuat sesi SSH, dengan IP publik dari host bastion, menyediakan kunci PEM di bagian AUTH, dan kemudian membuat Tunnel. Port sumber terowongan harus berupa port lokal yang tidak digunakan (misalnya 5000) dan IP akan menjadi IP dari host tujuan (kotak Windows yang Anda coba jangkau) dengan port RDP ditambahkan (3389). Pastikan untuk menyimpan konfigurasi Anda, karena Anda tidak ingin harus melakukannya setiap kali Anda masuk ke kotak. Connect ke host bastion, dan masuk. Kemudian, mulai sesi RDP untuk localhost: 5000 (atau port mana pun yang Anda pilih).

1. Tetapkan Nama Host atau IP publik dari host bastion

2. Di SSH -> Auth, atur file kunci pribadi dalam format.ppk

3. Di SSH -> Tunnels, tambahkan port baru yang diteruskan. Port Sumber harus berupa port yang tidak digunakan sewenang-wenang, dan Tujuan harus menjadi IP server tujuan di belakang host bastion, dengan port RDP ditambahkan.

4. Connect ke host bastion melalui PuTTY dan masuk.

5. Mulai sesi RDP ke localhost:5000 untuk mencapai server tujuan.

SALZ: Mengatur manajemen akses

Menggunakan jaringan yang dikelola oleh AWS Managed Services (AMS) berarti memberikan AMS akses untuk mengelola infrastruktur cloud Anda. Anda harus mengonfigurasi sarana untuk menghubungkan dengan aman antara jaringan pribadi Anda dan AMS. Ini dimulai dengan beberapa keputusan tentang jenis akses yang ingin Anda berikan:

- Untuk akses AMS API/CLI dan Konsol: Anda akan ingin menginstal AMS CLI (instruksi disediakan dalam dokumen ini). Anda menggunakan API manajemen perubahan AMS untuk membuat permintaan perubahan ke AMS dan AMS SKMS API untuk mempelajari sumber daya yang dikelola

AMS. Menggunakan Active Directory Federation Services (AD FS), Anda dapat mengakses Konsol AMS.

> **Note**
>
> Jika Anda menyiapkan ITSM Anda sendiri, Anda harus menggunakan AWS Support API (SAPI) untuk permintaan layanan dan laporan insiden. SAPI didokumentasikan dalam AWS Support API Reference.

- Untuk akses pengguna: Apakah Anda mengelola pengguna dengan Windows Active Directory (AD), atau Linux/LDAP solusi, konektivitas harus dibuat antara AD di sisi AMS (melalui Layanan Direktori) dan direktori Anda.
- Misalnya akses: Akses tingkat instans dicapai melalui konfigurasi kepercayaan Forest satu arah. Directory Services mempercayai kredensi di CORP AD mereka, memungkinkan tumpukan di sisi AMS untuk mengizinkan login dengan kredenal CORP.

  Perhatikan bahwa Active Directory (AD) yang AMS mengatur kepercayaan harus berupa direktori yang memiliki akun pengguna yang diotorisasi oleh Anda untuk mendapatkan akses ke sumber daya AWS Anda.

> **Important**
>
> Untuk menyiapkan kepercayaan Hutan, AMS memerlukan pengontrol domain Anda Kebijakan Lokal -> Opsi Keamanan -> Akses Jaringan: Pipa Bernama yang dapat diakses secara anonim, daftar pipa Netlogon dan lsarpc. Pipa ini terdaftar secara default, tetapi kadang-kadang dihapus untuk masalah keamanan. Setelah kepercayaan ditetapkan, mereka dapat dihapus dari daftar lagi.

Membangun kepercayaan Active Directory (AD)

Sebelum Anda mulai membuat kepercayaan Active Directory (AD) untuk akun AWS Managed Services (AMS) Anda, pastikan port firewall yang sesuai terbuka.

Kepercayaan dari Direktori Aktif yang dikelola AMS dan layanan direktori perusahaan memungkinkan Anda menggunakan kredenal yang dikelola perusahaan untuk mengakses instans yang dikelola AMS untuk melakukan pengembangan, pengujian, atau fungsi administratif.

Membuat koneksi kepercayaan adalah latihan dua bagian:

Pertama, konfigurasikan forward bersyarat, konfigurasi DNS sehingga kueri DNS tahu server DNS mana yang akan dituju.

Kedua, konfigurasikan kepercayaan, konstruksi Active Directory (AD) untuk memungkinkan akses dari pengguna di satu domain untuk menggunakan sumber daya di domain lain.

Konfigurasikan forwarder bersyarat

Ikuti artikel Microsoft AD ini Menetapkan Forwarder Bersyarat untuk Nama Domain, dan gunakan pengaturan dan pilihan ini:

1. Di Manajer DNS AD -> Buat Forwarder Bersyarat Baru, di bawah Domain DNS: Gunakan nama domain AMS yang diberikan kepada Anda; misalnya,. *A523434123.amazonaws.com*
2. Di bawah alamat IP server master: Tambahkan alamat IP yang disediakan AMS. Pastikan tidak ada masalah koneksi dengan memvalidasi kedua alamat.
3. Pilih Simpan forwarder bersyarat ini di Active Directory dan replikasi sebagai berikut: Semua server DNS di domain ini dan tekan OK.

Konfigurasikan kepercayaan

Untuk mengonfigurasi kepercayaan untuk akun AWS Managed Services (AMS) Anda, ikuti artikel MicroSoft AD ini Buat kepercayaan hutan satu arah, masuk, untuk satu sisi kepercayaan, menggunakan pengaturan dan pilihan yang dijelaskan di bagian ini.

1. Buka dialog Start -> Administrative Tools -> Active Directory Domains and Trusts. Klik kanan node domain untuk domain yang ingin Anda percayai, lalu klik Properties -> Trusts -> New Trust untuk membuka New Trust Wizard. Masukkan nama domain yang diberikan kepada Anda oleh AMS untuk Nama Kepercayaan dan tekan Berikutnya.
2. Di bawah Jenis Kepercayaan, pilih Forest Trust. Tekan Berikutnya.
3. Di bawah Direction of Trust, pilih Satu arah: masuk. Tekan Berikutnya.
4. Di bawah Sisi Kepercayaan, pilih Domain ini saja. Tekan Berikutnya.
5. Di bawah Trust Password, ketikkan kata sandi pilihan Anda. Tekan Berikutnya.
6. Untuk Seleksi Kepercayaan Selesai dan Pembuatan Kepercayaan Selesai, cukup tekan Berikutnya.

7. Di bawah Konfirmasi Kepercayaan Masuk, pilih Tidak, jangan konfirmasi kepercayaan yang masuk. Tekan Berikutnya.
8. Di bawah Selesai New Trust Wizard, pilih Selesai, lalu OK untuk menutup.
9. Berikan kata sandi kepercayaan (hubungi kami melalui nomor telepon CSDM Anda untuk alasan keamanan). AMS akan menyelesaikan konfigurasi kepercayaan.

Situs dan layanan Active Directory

Untuk mengurangi latensi login, tambahkan rentang CIDR VPC ke Situs dan Layanan Direktori Aktif Anda (Mulai -> Alat Administratif -> Situs dan Layanan Direktori Aktif). Tambahkan rentang CIDR VPC ke Situs Direktori Aktif yang berisi Pengontrol Domain yang paling dekat dengan AWS.

Perutean akhiran nama Direktori Aktif

Setelah kepercayaan hutan satu arah ditetapkan, harap selesaikan langkah-langkah tambahan.

1. Di bawah Mulai > Semua Program > Alat Administratif, klik Active Directory Domains and Trusts.

   Konsol Active Directory Domains and Trusts terbuka.
2. Klik kanan domain perusahaan Anda dan klik Properties

   Dialog Properties untuk domain itu terbuka.
3. Klik tab Trusts.

   Halaman Trust terbuka.
4. Klik nama domain Amazon dan klik Properties.

   Halaman Properti untuk kepercayaan domain Amazon terbuka.
5. Klik Name Suffix Routing dan klik Refresh.

   Langkah-langkah ini memastikan bahwa Nama Prinsipal Layanan (SPNs) dapat mengatasi kepercayaan.

Pemecahan Masalah

Beberapa hal yang harus dicoba jika Anda mengalami masalah:

- Grup keamanan keluar Direktori Aktif yang dikelola AMS harus diizinkan koneksi melalui blok CIDR Anda (misalnya 10.27.0.0/16) ke pengontrol domain Anda.
- Lacak rute di AWS Console dari pengontrol domain ke pengontrol domain yang memeriksa semua grup keamanan di sepanjang jalan.
- Pastikan Anda dapat melakukan ping ke Pengontrol Domain Direktori Aktif yang dikelola AMS jika Internet Control Message Protocol (ICMP) diizinkan.
- Pastikan Pengontrol Domain Anda dapat berkomunikasi dengan AWS Directory Services.
- Pastikan forwarder bersyarat menyelesaikan dan divalidasi.
- Jika Anda tidak melihat Forest Trust di wizard New Trust, maka forwarder bersyarat Anda mungkin tidak berfungsi dengan benar:
  - Gunakan nslookup untuk menguji resolusi
  - Coba reboot Pengontrol Domain

Direktori Aktif Terkelola AMS

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

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

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

Catatan:

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

Access berfungsi seperti ini:

- AWS Tim Directory Service: Memiliki akses ke pengontrol domain.
- AMS: Memiliki akses ke Directory Service APIs untuk melakukan tindakan tertentu pada domain. Tindakan ini termasuk mengambil snapshot AD, mengubah skema AD, dan tindakan lainnya.
- Anda: Memiliki akses ke domain (AD) untuk membuat pengguna, grup, dan sebagainya.

- Kami menyarankan Anda melakukan bukti konsep pada AD Terkelola sebelum memigrasikan iklan perusahaan Anda, karena tidak semua fungsionalitas dari lingkungan AD tradisional tersedia di lingkungan AD Terkelola.
- AMS tidak akan mengelola atau memberikan panduan tentang manajemen AD Anda. Misalnya, AMS tidak akan memberikan panduan tentang struktur Unit Organisasi, struktur kebijakan grup, konvensi penamaan pengguna AD, dan sebagainya.

Ini bekerja seperti ini:

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

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

   - Informasi akun
     - ID akun Akun AWS yang dibuat untuk AD yang dikelola AMS: nomor Akun AWS
     - Wilayah untuk memasukkan iklan Terkelola Anda ke: AWS Region
   - Informasi Direktori Aktif Terkelola:
     - Microsoft AD Edition: Standar/Perusahaan. AWS Microsoft AD (Edisi Standar) mencakup 1 GB penyimpanan objek direktori. Kapasitas ini dapat mendukung hingga 5.000 pengguna atau 30.000 objek direktori, termasuk pengguna, grup, dan komputer. AWS Microsoft AD (Enterprise Edition) mencakup penyimpanan objek direktori 17 GB, yang dapat mendukung hingga 100.000 pengguna atau 500.000 objek.

       Untuk informasi selengkapnya, lihat AWS Directory Service FAQs.
     - Domain FQDN: FQDN untuk domain AMS Managed AD Anda.
     - Nama Domain NetBIOS: Nama NetBIOS untuk domain AMS Managed AD Anda.

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

      Misalnya:

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

      Untuk menghindari konflik alamat IP, pastikan CIDR VPC AD Terkelola yang Anda tentukan tidak bertentangan dengan CIDR subnet pribadi lainnya yang Anda gunakan di jaringan perusahaan Anda.
    - Teknologi VPN (opsional): [Direct Connect/Direct Connect dan VPN]
        - Nomor Sistem Otonomi BGP (ASN) gateway Anda: [ASN yang disediakan pelanggan]
        - Alamat IP yang dapat dirutekan Internet untuk antarmuka luar gateway Anda, alamatnya harus statis: [Alamat IP yang Diberikan Pelanggan]
        - Apakah koneksi VPN Anda memerlukan rute statis atau tidak: [ya/tidak]
2. AMS memberi Anda kata sandi akun Admin untuk lingkungan AD dan meminta Anda untuk mengatur ulang kata sandi sehingga teknisi AMS tidak dapat lagi mengakses lingkungan AD Anda.
3. Untuk mengatur ulang kata sandi akun Admin, sambungkan ke lingkungan Active Directory menggunakan Active Directory Users and Computers (ADUC). ADUC dan Remote Server Administration Tools (RSAT) lainnya harus diinstal dan dijalankan pada host Administratif yang disediakan oleh Anda pada infrastruktur non-AMS. Microsoft memiliki praktik terbaik untuk mengamankan host administratif tersebut. Untuk selengkapnya, lihat Menerapkan

Host Administratif Aman. Anda mengelola lingkungan Direktori Aktif Anda menggunakan host Administratif ini.

4. Dalam operasi harian, AMS mengelola Akun AWS hingga ke sisi AWS Directory Service; misalnya, konfigurasi VPC, pencadangan AD, pembuatan dan penghapusan kepercayaan AD, dan sebagainya. Anda menggunakan, dan mengelola, lingkungan iklan Anda; misalnya, pembuatan pengguna, pembuatan grup, pembuatan kebijakan grup, dan sebagainya.

Untuk tabel RACI terbaru, lihat bagian “Peran dan Tanggung Jawab” di Lihat deskripsi Layanan.

Federasi Direktori Aktif Anda dengan peran AMS AWS Identity and Access Management

Tujuan menggabungkan direktori Anda dengan peran AMS IAM adalah untuk memungkinkan pengguna perusahaan menggunakan kredensi perusahaan mereka untuk berinteraksi dengan dan AWS APIs, Konsol Manajemen AWS dan oleh karena itu konsol AMS dan. APIs

Contoh proses federasi

Contoh ini menggunakan Layanan Federasi Direktori Aktif (AD FS); Namun, teknologi apa pun yang mendukung AWS Identity and Access Management Federasi didukung. Untuk informasi selengkapnya tentang federasi IAM yang AWS didukung, lihat Mitra IAM dan Penyedia Identitas dan Federasi. CSDM Anda akan membantu Anda melalui proses ini, yang melibatkan upaya bersama dengan tim AD dan AMS Anda.

Untuk informasi rinci tentang mengintegrasikan SAFL untuk akses API, lihat AWS blog ini, Cara Menerapkan API Federasi dan Akses CLI Menggunakan SAFL 2.0 dan AD FS.

> **Note**
>
> Untuk contoh yang menginstal AMS CLI dan SALL, lihat. Lampiran: Aturan klaim ActiveDirectory Federation Services (ADFS) dan pengaturan SAMP

Mengkonfigurasi federasi ke konsol AMS (SALZ)

Peran IAM dan penyedia identitas SAMP (Entitas Tepercaya) yang dirinci dalam tabel berikut telah disediakan sebagai bagian dari orientasi akun Anda. Peran ini memungkinkan Anda untuk

mengirimkan dan memantau RFCs, permintaan layanan, dan laporan insiden, serta mendapatkan informasi tentang Anda VPCs dan tumpukan.

Peran	Penyedia Identitas	Izin
Pelanggan_ ReadOnly _Peran	SAML	Untuk akun AMS standar. Memungkinkan Anda mengirimkan RFCs untuk membuat perubahan pada infrastruktur yang dikelola AMS, serta membuat permintaan dan insiden layanan.
customer_managed_ad_user_role	SAML	Untuk akun Direktori Aktif Terkelola AMS. Memungkinkan Anda masuk ke Konsol AMS untuk membuat permintaan layanan dan insiden (tidak ada RFCs).

Untuk daftar lengkap peran yang tersedia di berbagai akun, lihatPeran pengguna IAM di AMS.

Anggota tim orientasi mengunggah file metadata dari solusi federasi Anda ke penyedia identitas yang telah dikonfigurasi sebelumnya. Anda menggunakan penyedia identitas SAMP saat ingin membangun kepercayaan antara IDP (penyedia identitas) yang kompatibel dengan SAMP seperti Shibboleth atau Layanan Federasi Direktori Aktif, sehingga pengguna di organisasi Anda dapat mengakses sumber daya AWS. Penyedia identitas SAMP di IAM digunakan sebagai prinsip dalam kebijakan kepercayaan IAM dengan peran di atas.

Sementara solusi federasi lainnya memberikan instruksi integrasi untuk AWS, AMS memiliki instruksi terpisah. Menggunakan posting blog berikut, Mengaktifkan Federasi ke AWS Menggunakan Windows Active Directory, AD FS, dan SAMP 2.0, bersama dengan amandemen yang diberikan di bawah ini, akan memungkinkan pengguna perusahaan Anda mengakses beberapa akun AWS dari satu browser.

Setelah membuat kepercayaan pihak yang mengandalkan sesuai posting blog, konfigurasikan aturan klaim dengan cara berikut:

- NameId: Ikuti posting blog.
- RoleSessionName: Gunakan nilai-nilai berikut:
  - Nama aturan klaim: RoleSessionName

  - Toko atribut: Direktori Aktif
  - Atribut LDAP: SAM-Account-Name
  - Jenis Klaim Keluar: https://aws.amazon.com/SAML/ Atribut/ RoleSessionName
- Dapatkan Grup Iklan: Ikuti posting blog.
- Klaim peran: Ikuti posting blog, tetapi untuk aturan Kustom, gunakan ini:

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
 => issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-",
 "arn:aws:iam::$1:saml-provider/customer-readonly-saml,arn:aws:iam::$1:role/"));
```

Saat menggunakan AD FS, Anda harus membuat grup keamanan Direktori Aktif untuk setiap peran dalam format yang ditampilkan dalam tabel berikut (customer_managed_ad_user_role hanya untuk akun AMS Managed AD):

Grup	Peran
AWS- [AccountNo] ReadOnly -Pelanggan_ _Peran	Pelanggan_ ReadOnly _Peran
AWS- [AccountNo] -customer_managed_ ad_user_role	customer_managed_ad_user_role

Untuk informasi lebih lanjut, lihat Mengonfigurasi Pernyataan SAMP untuk Respons Otentikasi.

> **Tip**
>
> Untuk membantu pemecahan masalah, unduh plugin pelacak SAMP untuk browser Anda.

Mengirimkan permintaan federasi ke AMS

Jika ini adalah akun pertama Anda, bekerjalah dengan Arsitek and/or Cloud CSDM Anda untuk menyediakan file XMLmetadata untuk penyedia identitas Anda.

Jika Anda memasukkan akun tambahan atau Penyedia Identitas dan memiliki akses ke akun manajemen atau akun aplikasi yang diinginkan, ikuti langkah-langkah ini.

1. Buat permintaan layanan dari konsol AMS, berikan detail yang diperlukan untuk menambahkan penyedia identitas:

   - AccountId dari akun tempat penyedia identitas baru akan dibuat.
   - Nama penyedia identitas yang diinginkan, jika tidak disediakan, defaultnya adalah saml pelanggan; biasanya, ini harus sesuai dengan pengaturan yang dikonfigurasi di penyedia federasi Anda.
   - Untuk akun yang ada, sertakan apakah penyedia identitas baru harus disebarkan ke semua peran konsol yang ada atau berikan daftar peran yang harus mempercayai penyedia identitas baru.
   - Lampirkan file XHTML metadata yang diekspor dari agen federasi Anda ke permintaan layanan sebagai lampiran file.
2. Dari akun yang sama tempat Anda membuat permintaan layanan, buat RFC baru menggunakan CT-ID ct-1e1xtak34nx76 (Manajemen | Lainnya | Lainnya | Buat) dengan informasi berikut.

   - Judul: “IDP SAMP onboard <Name>untuk Akun < >”AccountId.
   - AccountId dari akun tempat penyedia identitas akan dibuat.
   - Nama penyedia identitas.
   - Untuk Akun yang Ada: Apakah penyedia identitas harus disebarkan ke semua peran konsol yang ada, atau daftar peran yang harus mempercayai penyedia identitas baru.
   - ID kasus permintaan layanan dibuat pada Langkah 1, di mana file XMLmetadata dilampirkan.

Verifikasi akses konsol

Setelah Anda diatur dengan ADFS, dan memiliki URL AMS untuk digunakan untuk otentikasi, ikuti langkah-langkah ini.

Dengan konfigurasi Active Directory Federated Service (ADFS), Anda dapat mengikuti langkah-langkah berikut:

1. Buka jendela browser dan buka halaman masuk yang disediakan untuk Anda untuk akun Anda. IdpInitiatedSignOnHalaman ADFS untuk akun Anda terbuka.
2. Pilih tombol radio di sebelah Masuk ke salah satu situs berikut. Daftar pilih situs Masuk menjadi aktif.
3. Pilih situs signin.aws.amazon.com dan klik Masuk. Opsi untuk memasukkan kredensyal Anda terbuka.

4. Masukkan kredensyal CORP Anda dan klik Masuk. Konsol Manajemen AWS Terbuka.
5. Tempel ke bilah lokasi URL konsol AMS dan tekan Enter. Konsol AMS terbuka.

Verifikasi akses API

AMS menggunakan AWS API, dengan beberapa operasi khusus AMS yang dapat Anda baca di Referensi API AMS.

AWS menyediakan beberapa SDKs yang dapat Anda akses di Tools for Amazon Web Services. Jika Anda tidak ingin menggunakan SDK, Anda dapat melakukan panggilan API langsung. Untuk informasi tentang autentikasi, lihat Menandatangani Permintaan AWS API. Jika Anda tidak menggunakan SDK, atau membuat permintaan HTTP API langsung, Anda dapat menggunakan AMS CLIs for Change Management (CM) dan SKMS.

Instal AMS CLIs

Untuk contoh menginstal AWS Managed Services (AMS) CLI untuk digunakan dengan SALL, lihat. Lampiran: Aturan klaim ActiveDirectory Federation Services (ADFS) dan pengaturan SAMP

Jika Anda memerlukan akses sementara, untuk mendapatkan dan menginstal AWS Managed Services (AMS) SDKs, lihat Akses konsol AMS Sementara.

> **Note**
>
> Anda harus memiliki kredensi administrator untuk prosedur ini.

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

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

   Setelah instalasi, jalankan `aws help` untuk memverifikasi instalasi.
2. Setelah AWS CLI diinstal, untuk menginstal atau memutakhirkan AMS CLI, unduh file zip yang dapat didistribusikan AMS AMS CLI atau AMS SDK dan unzip. Anda dapat mengakses distribusi AMS CLI melalui tautan Sumber Daya Pengembang di navigasi kiri konsol AMS.

3. File README memberikan instruksi untuk instalasi apa pun.

   Buka:

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

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

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

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

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

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

Menjadwalkan backup AMS di tingkat VPC

Penjadwalan cadangan AWS Managed Services (AMS) di VPC, tempat instans target dialokasikan, dibuat selama orientasi akun dengan tag default dalam skema pembuatan VPC. Sistem cadangan menjadwalkan eksekusi snapshot tergantung pada Tag VPC itu. Modifikasi jadwal dapat dilakukan dengan membuat permintaan layanan. Untuk informasi selengkapnya, lihat Tag VPC dan Default.

Untuk default cadangan, lihat Memahami Default AMS

SALZ: Pengaturan default

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

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

Untuk contoh biaya infrastruktur, lihat Komponen dasar.

Aturan firewall disediakan di Siapkan Firewall Anda

Keamanan Titik Akhir (EPS)

Sumber daya yang Anda sediakan di lingkungan AMS Advanced secara otomatis menyertakan penginstalan klien pemantauan keamanan titik akhir (EPS). Proses ini memastikan bahwa sumber daya AMS Advanced-managed dipantau dan didukung 24x7. Selain itu, AMS Advanced memantau semua aktivitas agen, dan insiden dibuat jika ada peristiwa keamanan yang terdeteksi.

> **Note**
>
> Insiden keamanan ditangani sebagai insiden; untuk informasi lebih lanjut, lihat Respons insiden.

Keamanan endpoint memberikan perlindungan anti-malware, khususnya, tindakan berikut didukung:

- EC2 instans mendaftar dengan EPS
- EC2 instance deregister dari EPS
- EC2 contoh perlindungan anti-malware real-time
- Detak jantung yang diprakarsai agen EPS

- EPS mengembalikan file yang dikarantina
- Pemberitahuan acara EPS
- Pelaporan EPS

AMS Advanced menggunakan Trend Micro untuk keamanan endpoint (EPS). Ini adalah pengaturan EPS default. Untuk mempelajari lebih lanjut tentang Trend Micro, lihat Pusat Bantuan Trend Micro Deep Security; perhatikan bahwa tautan non-Amazon dapat berubah tanpa pemberitahuan kepada kami.

Pengaturan default AMS Advanced Multi-Account Landing Zone (MALZ) dijelaskan di bagian berikut; untuk pengaturan EPS landing zone multi-akun AMS non-default, lihat pengaturan non-default AMS Advanced Multi-Account Landing Zone EPS.

> **Note**
>
> Anda dapat membawa EPS Anda sendiri, lihat AMS membawa EPS Anda sendiri.

Pengaturan EPS umum

Pengaturan jaringan umum keamanan titik akhir.

Default EPS

Pengaturan	Default
Port Firewall (Grup Keamanan Instans)	Agen EPS Deep Security Manager (DSMs) harus memiliki port 4120 terbuka untuk komunikasi Agent/Relay to Manager, dan port 4119 untuk Konsol Manajer. Relay EPS harus memiliki port 4122 terbuka untuk komunikasi Manager/Agent to Relay. Tidak ada port khusus yang harus terbuka untuk komunikasi inbound instance pelanggan karena agen memulai semua permintaan.
Arah Komunikasi	Agen/Alat Dimulai
Interval Detak Jantung	Sepuluh menit

Pengaturan	Default
Jumlah detak jantung yang terlewat sebelum peringatan	Dua
Drift maksimum yang diizinkan (perbedaan) antara waktu server	Tidak terbatas.
Meningkatkan kesalahan offline untuk mesin virtual yang tidak aktif (terdaftar, tetapi tidak online)	Tidak
Kebijakan default	Kebijakan dasar (dijelaskan selanjutnya)
Aktivasi beberapa komputer dengan nama host yang sama	Diijinkan
Peringatan untuk pembaruan yang tertunda dinaikkan	Setelah tujuh hari
Perbarui jadwal	AMS menargetkan siklus rilis bulanan untuk pembaruan perangkat lunak Trend Micro Deep Security Manager (DSM) /Deep Security Agent (DSA). Namun, AMS tidak mempertahankan SLA untuk pembaruan. Pembaruan dilakukan secara armada oleh tim pengembang AMS selama penerapan. Pembaruan DSA/DSA dicatat dalam peristiwa sistem Trend Micro DSM yang disimpan AMS secara lokal secara default selama 13 minggu. Untuk dokumentasi vendor, lihat Acara sistem di Pusat Bantuan Trend Micro Deep Security. Log juga diekspor ke grup log/aws/ams/eps/var/log/DSM.log di Amazon. CloudWatch
Perbarui sumber	Server Pembaruan Trend Micro (https://ipv6-iaus.trendmicro.com/iau_server.dll/)

Pengaturan	Default
Penghapusan data peristiwa atau log	Peristiwa dan log dihapus dari database DSM setelah tujuh hari.
Versi perangkat lunak agen diadakan	Hingga lima
Pembaruan aturan terbaru diadakan	Hingga sepuluh
Penyimpanan log	Secara default, file log disimpan dengan aman di Amazon S3, tetapi Anda juga dapat mengarsipkannya ke Amazon Glacier untuk membantu memenuhi persyaratan audit dan kepatuhan.

Kebijakan dasar

Pengaturan default kebijakan basis keamanan titik akhir.

Kebijakan dasar EPS

Pengaturan	Default
Modul yang Diaktifkan	Anti-Malware
Modul Dinonaktifkan	Reputasi Web
	Firewall
	Perlindungan Intrusi
	Pemantauan Integritas
	Inspeksi Log
	Kontrol Aplikasi

Anti-malware

Pengaturan anti-malware keamanan titik akhir.

Default anti-malware EPS

Pengaturan	Default	Catatan
Pemindaian Waktu Nyata	Pindai semuanya Setiap Day/All hari (24 jam)	Karantina semua virus yang dicurigai . Aktifkan IntelliTr ap dan spyware/g rayware perlindungan. Spyware dan Grayware memicu Anti-Malware dan mengakibatkan karantina item tersebut.
Pemindaian Manual	Pindai semuanya	Harus diminta, kemudian mengikuti konfigurasi pemindaia n real-time default.
Pemindaian Terjadwal	Pindai semuanya	Ditetapkan untuk hari Minggu terakhir setiap bulan, 6 pagi.
Perlindungan Cerdas	Nonaktif	N/A
File yang Dikarantina	Manajer Keamanan Trend Micro Deep (DSM)	Appx 1GB disk dicadangkan untuk karantina.
Batasan Pindai	Tren Mikro DSM	Pindai file dari semua ukuran.
Spyware atau Grayware yang Diizinkan	Tidak ada	N/A
Pemberitahuan Acara Lokal	Ya	N/A

Grup keamanan

Di AWS VPCs, AWS Security Groups bertindak sebagai firewall virtual, mengontrol lalu lintas untuk satu atau beberapa tumpukan (instance atau satu set instance). Ketika tumpukan diluncurkan, itu terkait dengan satu atau beberapa grup keamanan, yang menentukan lalu lintas apa yang diizinkan untuk mencapainya:

- Untuk tumpukan di subnet publik Anda, grup keamanan default menerima lalu lintas dari HTTP (80) dan HTTPS (443) dari semua lokasi (internet). Tumpukan juga menerima lalu lintas SSH dan RDP internal dari jaringan perusahaan Anda, dan benteng AWS. Tumpukan tersebut kemudian dapat keluar melalui port apa pun ke Internet. Mereka juga dapat keluar ke subnet pribadi Anda dan tumpukan lain di subnet publik Anda.
- Tumpukan di subnet pribadi Anda dapat keluar ke tumpukan lain di subnet pribadi Anda, dan instance dalam tumpukan dapat sepenuhnya berkomunikasi melalui protokol apa pun satu sama lain.

> **Important**
>
> Grup keamanan default untuk tumpukan pada subnet pribadi memungkinkan semua tumpukan di subnet pribadi Anda untuk berkomunikasi dengan tumpukan lain di subnet pribadi tersebut. Jika Anda ingin membatasi komunikasi antar tumpukan dalam subnet pribadi, Anda harus membuat grup keamanan baru yang menjelaskan pembatasan tersebut. Misalnya, jika Anda ingin membatasi komunikasi ke server database sehingga tumpukan di subnet pribadi itu hanya dapat berkomunikasi dari server aplikasi tertentu melalui port tertentu, mintalah grup keamanan khusus. Cara melakukannya dijelaskan di bagian ini.

Grup Keamanan Default

MALZ

Tabel berikut menjelaskan pengaturan grup keamanan masuk (SG) default untuk tumpukan Anda. SG diberi nama "SentinelDefaultSecurityGroupPrivateOnly-VPC-ID” yang merupakan ID VPC di *ID* akun landing zone multi-akun AMS Anda. Semua lalu lintas diizinkan keluar ke "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly" melalui grup keamanan ini (semua lalu lintas lokal dalam subnet tumpukan diizinkan).

Semua lalu lintas diizinkan keluar ke 0.0.0.0/0 oleh grup keamanan kedua "". SentinelDefaultSecurityGroupPrivateOnly

> **Tip**
>
> Jika Anda memilih grup keamanan untuk jenis perubahan AMS, seperti EC2 membuat, atau OpenSearch membuat domain, Anda akan menggunakan salah satu grup keamanan default yang dijelaskan di sini, atau grup keamanan yang Anda buat. Anda dapat menemukan daftar grup keamanan, per VPC, di EC2 konsol AWS atau konsol VPC.

Ada grup keamanan default tambahan yang digunakan untuk keperluan AMS internal.

Grup keamanan default AMS (lalu lintas masuk)

Jenis	Protokol	Rentang port	Sumber
Semua Lalu lintas	Semua	Semua	SentinelDefaultSecurityGroupPrivateOnly (membatasi lalu lintas keluar ke anggota grup keamanan yang sama)
Semua Lalu lintas	Semua	Semua	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (tidak membatasi lalu lintas keluar)
HTTP, HTTPS, SSH, RDP	TCP	80/443 (Sumber 0.0.0.0/0) Akses SSH dan RDP diizinkan dari benteng	SentinelDefaultSecurityGroupPublic (tidak membatasi lalu lintas keluar)
Benteng MALZ:			
SSH	TCP	22	SharedServices VPC CIDR dan DMZ VPC CIDR, ditambah pelanggan yang disediakan secara on-prem CIDRs
SSH	TCP	22	
RDP	TCP	3389	

Jenis	Protokol	Rentang port	Sumber
RDP	TCP	3389	
Benteng SALZ:			
SSH	TCP	22	mc-initial-garden- LinuxBastion SG
SSH	TCP	22	mc-initial-garden- LinuxBastion DMZSG
RDP	TCP	3389	mc-initial-garden- WindowsBastion SG
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMZSG

SALZ

Tabel berikut menjelaskan pengaturan grup keamanan masuk (SG) default untuk tumpukan Anda. SG diberi nama "mc-initial-garden- SentinelDefaultSecurityGroupPrivateOnly -*ID*" di mana *ID* adalah pengenal unik. Semua lalu lintas diizinkan keluar ke "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly" melalui grup keamanan ini (semua lalu lintas lokal dalam subnet tumpukan diizinkan).

Semua lalu lintas diizinkan keluar ke 0.0.0.0/0 oleh grup keamanan kedua "- -". mc-initial-garden SentinelDefaultSecurityGroupPrivateOnlyEgressAll *ID*

> **Tip**
>
> Jika Anda memilih grup keamanan untuk jenis perubahan AMS, seperti EC2 membuat, atau OpenSearch membuat domain, Anda akan menggunakan salah satu grup keamanan default yang dijelaskan di sini, atau grup keamanan yang Anda buat. Anda dapat menemukan daftar grup keamanan, per VPC, di EC2 konsol AWS atau konsol VPC.

Ada grup keamanan default tambahan yang digunakan untuk keperluan AMS internal.

Grup keamanan default AMS (lalu lintas masuk)

Jenis	Protokol	Rentang port	Sumber
Semua Lalu lintas	Semua	Semua	SentinelDefaultSecurityGroupPrivateOnly (membatasi lalu lintas keluar ke anggota grup keamanan yang sama)
Semua Lalu lintas	Semua	Semua	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (tidak membatasi lalu lintas keluar)
HTTP, HTTPS, SSH, RDP	TCP	80/443 (Sumber 0.0.0.0/0) Akses SSH dan RDP diizinkan dari benteng	SentinelDefaultSecurityGroupPublic (tidak membatasi lalu lintas keluar)
Benteng MALZ:			
SSH	TCP	22	SharedServices VPC CIDR dan DMZ VPC CIDR, ditambah pelanggan yang disediakan secara on-prem CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
Benteng SALZ:			
SSH	TCP	22	mc-initial-garden- LinuxBastion SG
SSH	TCP	22	mc-initial-garden- LinuxBastion DMZSG
RDP	TCP	3389	mc-initial-garden- WindowsBastion SG
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMZSG

Membuat, Mengubah, atau Menghapus Grup Keamanan

Anda dapat meminta grup keamanan khusus. Jika grup keamanan default tidak memenuhi kebutuhan aplikasi atau organisasi Anda, Anda dapat memodifikasi atau membuat grup keamanan baru. Permintaan semacam itu akan dianggap memerlukan persetujuan dan akan ditinjau oleh tim operasi AMS.

Untuk membuat grup keamanan di luar tumpukan dan VPCs, kirimkan RFC menggunakan jenis `Deployment | Advanced stack components | Security group | Create (review required)` perubahan (ct-1oxx2g2d7hc90).

Untuk modifikasi grup keamanan Active Directory (AD), gunakan jenis perubahan berikut:

- Untuk menambahkan pengguna: Kirim RFC menggunakan Manajemen | Directory Service | Pengguna dan grup | Tambahkan pengguna ke grup [ct-24pi85mjtza8k]
- Untuk menghapus pengguna: Kirim RFC menggunakan Manajemen | Directory Service | Pengguna dan grup | Hapus pengguna dari grup [ct-2019s9y3nfml4]

> **Note**
>
> Saat menggunakan “review required” CTs, AMS merekomendasikan agar Anda menggunakan opsi Penjadwalan ASAP (pilih ASAP di konsol, biarkan waktu mulai dan berakhir kosong di API/CLI) karena ini CTs memerlukan operator AMS untuk memeriksa RFC, dan mungkin berkomunikasi dengan Anda sebelum dapat disetujui dan dijalankan. Jika Anda menjadwalkan ini RFCs, pastikan untuk mengizinkan setidaknya 24 jam. Jika persetujuan tidak terjadi sebelum waktu mulai yang dijadwalkan, RFC ditolak secara otomatis.

Temukan Grup Keamanan

Untuk menemukan grup keamanan yang dilampirkan ke tumpukan atau instance, gunakan EC2 konsol. Setelah menemukan tumpukan atau instance, Anda dapat melihat semua grup keamanan yang melekat padanya.

Untuk cara menemukan grup keamanan di baris perintah dan memfilter output, lihat `describe-security-groups`.

EC2 Profil instans IAM

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

MALZ

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

Deskripsi kebijakan

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

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

SALZ

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

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

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

EC2 izin profil instans IAM default

CW = CloudWatch. ARN = Nama Sumber Daya Amazon. * = wildcard (apa saja).			
Pernyataan kebijakan	Efek	Tindakan	Deskripsi dan sumber daya (ARN)
Amazon Elastic Compute Cloud (Amazon EC2)			
EC2 Tindakan Pesan	Izinkan	AcknowledgeMessage, DeleteMessage,	Mengizinkan tindakan perpesanan EC2 Systems Manager di akun Anda.

CW = CloudWatch. ARN = Nama Sumber Daya Amazon. * = wildcard (apa saja).			
Pernyataan kebijakan	Efek	Tindakan	Deskripsi dan sumber daya (ARN)
		FailMessage, GetEndpoint, GetMessages, SendReply	
Ec2 Jelaskan	Izinkan	* (Semua)	Memungkinkan konsol menampilkan detail konfigurasi EC2 di akun Anda.
Saya Dapatkan ID Peran	Izinkan	GetRole	Memungkinkan EC2 untuk mendapatkan ID IAM Anda dari `aws:iam::*:role/customer-*` dan `aws:iam::*:role/customer_*` .
Instance Untuk Mengunggah Peristiwa Log	Izinkan	Buat Grup Log	Mengizinkan log dibuat di: `aws:logs:*:*:log-group:i-*`
		Buat Aliran Log	Memungkinkan log dialirkan ke: `aws:logs:*:*:log-group:i-*`

CW = CloudWatch. ARN = Nama Sumber Daya Amazon. * = wildcard (apa saja).			
Pernyataan kebijakan	Efek	Tindakan	Deskripsi dan sumber daya (ARN)
CW Untuk MMS	Izinkan	DescribeAlarms, PutMetricAlarm, PutMetricData	Memungkinkan CloudWatch untuk mengambil alarm di akun Anda. Memungkinkan CW membuat atau memperbarui alarm dan mengaitkannya dengan metrik yang ditentukan. Memungkinkan CW mempublikasikan titik data metrik ke akun Anda.
Tag Ec2	Izinkan	CreateTags, DescribeTags,	Memungkinkan tag ditambahkan, ditimpa, dan dijelaskan pada instance yang ditentukan di akun Anda.
Secara Eksplisit Menolak Log CW	Menyangkal	DescribeLogStreams, FilterLogEvents, GetLogEvents	Tidak mengizinkan daftar, memfilter, atau mendapatkan aliran log untuk: `aws:logs:*:*:log-group:/mc/*`
Amazon EC2 Simple Systems Manager (SSM)			

CW = CloudWatch. ARN = Nama Sumber Daya Amazon. * = wildcard (apa saja).			
Pernyataan kebijakan	Efek	Tindakan	Deskripsi dan sumber daya (ARN)
Tindakan SSM	Izinkan	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	Memungkinkan berbagai fungsi SSM di akun Anda.
Akses SSM Di S3	Izinkan	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadPorts, ListBucketMultipartUploads	Memungkinkan SSM EC2 untuk mendapatkan dan memperbarui objek, dan membatalkan unggahan objek multi-bagian ke, dan daftar port dan ember yang tersedia untuk, unggahan multi-bagian di. `aws:s3:::mc-*-internal-*/aws/ssm*`
Amazon EC2 Simple Storage Service (S3)			
Dapatkan Objek Di S3	Izinkan	Dapatkan Daftar	Memungkinkan EC2 aplikasi untuk mengambil dan mencantumkan objek dalam bucket S3 di akun Anda.
Akses Log S3 Terenkripsi Pelanggan	Izinkan	PutObject	Memungkinkan EC2 aplikasi untuk memperbarui objek di `aws:s3:::mc-*-logs-*/encrypted/app/*`

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

Pernyataan kebijakan	Efek	Tindakan	Deskripsi dan sumber daya (ARN)
Patch Data Letakkan Objek S3	Izinkan	PutObject	Memungkinkan EC2 aplikasi untuk mengunggah data patching ke bucket S3 Anda di `aws:s3:::awsms-a*-patch-data-*`
Mengunggah Log Sendiri Ke S3	Izinkan	PutObject	Memungkinkan EC2 aplikasi untuk mengunggah log kustom ke: `aws:s3:::mc-a*-logs-*/aws/instances/*/${aws:userid}/*`
Secara Eksplisit Menolak Log MC Namespace S3	Menyang l	GetObject* Meletakkan*	Melarangkan EC2 aplikasi mendapatkan atau meletakkan objek apa pun dari atau ke: `aws:s3:::mc-*-logs-*/encrypted/mc*` , `aws:s3:::mc-*-logs-*/mc/*`, `aws:s3:::mc-a*-logs-*-audit/*`
Secara Eksplisit Tolak Hapus S3	Menyang l	* (semua)	Melarangkan EC2 aplikasi mengambil tindakan apa pun pada objek di: `aws:s3:::mc-a*-logs-*/*` , `aws:s3:::mc-a*-internal-*/*` ,

CW = CloudWatch. ARN = Nama Sumber Daya Amazon. * = wildcard (apa saja).			
Pernyataan kebijakan	Efek	Tindakan	Deskripsi dan sumber daya (ARN)
Secara Eksplisit Menolak Bucket CFN S3	Menyang l	Hapus*	MelRANG EC2 aplikasi menghapus objek apa pun dari: `aws:s3:::cf-templates-*`
Secara Eksplisit Menolak Daftar Bucket S3	Menyang l	ListBucket	Melarang Anda mencantumkan objek terenkripsi, log audit, atau cadangan (mc) dari: `aws:s3::: mc-*-logs-*`
AWS Secrets Manager di Amazon EC2			

CW = CloudWatch. ARN = Nama Sumber Daya Amazon. * = wildcard (apa saja).			
Pernyataan kebijakan	Efek	Tindakan	Deskripsi dan sumber daya (ARN)
Akses Rahasia Trend Cloud One	Izinkan	GetSecretValue	Memungkinkan Amazon EC2 mengakses rahasia untuk migrasi Trend Cloud One: `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` , `arn:aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-activation-token*` , `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` , `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-guid*`
AWS Key Management Service di Amazon EC2			
Kunci Dekripsi Trend Cloud One	Izinkan	Dekripsi	Izinkan Amazon EC2 mendekripsi AWS KMS kunci dengan nama alias/-migrasi ams/eps/cloudone `arn:aws:kms:*:*:alias/ams/eps/cloudone-migration`

Jika Anda tidak terbiasa dengan kebijakan Amazon IAM, lihat Ikhtisar Kebijakan IAM untuk informasi penting.

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

Metrik yang dipantau secara default

Tabel berikut menunjukkan apa yang dipantau dan ambang batas peringatan default. Anda dapat mengubah default dengan permintaan manajemen perubahan untuk perubahan (RFC).

> **Note**
>
> CloudWatch meluncurkan retensi metrik yang diperpanjang pada 1 November 2016. Untuk informasi selengkapnya, lihat CloudWatch Batasan-batasan.

Peringatan dari pemantauan dasar

Layanan	Peringatan keaman	Nama peringatan dan kondisi pemicu	Catatan
Untuk peringatan berbintang (*), AMS secara proaktif menilai dampak dan memulihkan bila memungkinkan; jika remediasi tidak memungkinkan, AMS menciptakan insiden. Jika otomatisasi gagal memperbaiki masalah, AMS memberi tahu Anda tentang kasus insiden dan seorang insinyur AMS terlibat. Selain itu, peringatan ini dapat dikirim langsung ke email Anda (jika Anda telah memilih topik Direct-Customer-Alerts SNS).			
Contoh Application Load Balancer (ALB)	Tidak	RejectedConnectionCount jumlah> 0 selama 1 menit, 5 kali berturut-turut.	CloudWatch alarm jika jumlah koneksi yang ditolak karena load balancer mencapai maksimum.

Layanan	Peringatan keaman	Nama peringatan dan kondisi pemicu	Catatan
Target Application Load Balancer (ALB)	Tidak	TargetConnectionErrorCount jumlah> 0 selama 1 menit, 5 kali berturut-turut.	CloudWatch alarm jika jumlah koneksi tidak berhasil dibuat antara penyeimbang beban dan instans terdaftar.
EC2 Contoh Amazon - Windows	Tidak	SecureChannelFailure > 0,0 untuk 10 dari 15 titik data terakhir.	CloudWatch alarm pada instance Windows untuk mengingatkan ketika koneksi Secure a Channel gagal.
Contoh Aurora	Tidak	CPUUtilization > 85% selama 5 menit, 2 kali berturut-turut.	CloudWatch alarm.
AWS Backup	Ya	DeleteRecoveryPoint Prinsipal peran IAM yang tidak terduga atau prinsipal pengguna IAM telah menghapus titik AWS Backup pemulihan.	CloudWatch acara. Dipancarkan saat titik pemulihan cadangan dihapus.
AWS Outposts	Ya	AMSOutpostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 80% selama 5 menit, 12 kali berturut-turut.	CloudWatch alarm pada ketersediaan kapasitas keluarga misalnya AWS Outposts sumber daya.

Layanan	Peringatan keaman	Nama peringatan dan kondisi pemicu	Catatan
		AMSOutpostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80% selama 5 menit, 12 kali berturut-turut.	CloudWatch alarm pada ketersediaan kapasitas tipe instans AWS Outposts sumber daya.
		AMSOutpostsConnectedStatusConnectedStatus < 1 selama 5 menit, 1 kali berturut-turut.	CloudWatch alarm pada koneksi tautan AWS Outposts layanan, kurang dari 1 hitungan terganggu.
		AMSOutpostsCapacityExceptionCapacityExceptions 0 selama 5 menit, 1 kali berturut-turut.	CloudWatch alarm pada kesalahan kapasitas yang tidak mencukupi misalnya peluncuran untuk sumber daya AWS Outposts s .
EC2 contoh - semua OSs	Tidak	CPUUtilization* >= 95% selama 5 menit, 6 kali berturut-turut.	CloudWatch alarm. Pemanfaatan CPU yang tinggi adalah indikator perubahan status aplikasi seperti kunci mati, loop tak terbatas, serangan berbahaya, dan anomali lainnya.
		StatusCheckFailed > 0 selama 5 menit, 3 kali berturut-turut.	CloudWatch alarm.

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

Layanan	Peringatan keaman	Nama peringatan dan kondisi pemicu	Catatan
		Bebas Swap * Memory Swap < 5% selama 5 menit, 6 kali berturut-turut.	
ElastiCache Cluster	Tidak	CurrConnections = 65000	Alarm ini memberi tahu AMS tentang batas koneksi maksimum ElastiCache Host. CloudWatch Alarm. Jika Anda ingin memperbarui ambang batas ini, hubungi dukungan AMS.

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

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

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

Layanan	Peringatan keaman	Nama peringatan dan kondisi pemicu	Catatan
		CPUUtilization Rata-rata adalah >= 80% selama 15 menit, 3 kali berturut-turut AMS mengambil tindakan proaktif untuk mengurangi dampak operasional, saat peringatan ini dipicu.	Pemanfaatan CPU 100% adalah umum, tetapi rata-rata tinggi yang berkelanjutan bermasalah. Pertimbangkan untuk menggunakan jenis instans yang lebih besar atau menambahkan instans.
		JVMMemoryTekanan maksimum adalah> = 80% selama 5 menit, 3 kali berturut-turut AMS mengambil tindakan proaktif untuk mengurangi dampak operasional, saat peringatan ini dipicu.	Klaster bisa mengalami kesalahan kehabisan memori jika penggunaan meningkat . Pertimbangkan penskalaan vertikal. Amazon ES menggunakan separuh dari RAM instans untuk Java heap, hingga ukuran tumpukan 32 GiB. Anda dapat menskalakan instans secara vertikal hingga 64 GiB RAM, di mana Anda dapat menskalakan secara horizontal dengan menambahkan instans.

Layanan	Peringatan keaman	Nama peringatan dan kondisi pemicu	Catatan
		Guru CPUUtilization Rata-rata adalah >= 50% selama 15 menit, 3 kali berturut-turut AMS mengambil tindakan proaktif untuk mengurangi dampak operasional, saat peringatan ini dipicu.	Pertimbangkan untuk menggunakan jenis instance yang lebih besar untuk node master khusus Anda. Karena perannya dalam stabilitas dan blue/green penerapan cluster, node master khusus harus memiliki penggunaan CPU rata-rata yang lebih rendah daripada node data.
		JVMMemoryTekanan Master maksimum adalah> = 80% selama 15 menit, 1 kali berturut-turut AMS mengambil tindakan proaktif untuk mengurangi dampak operasional, saat peringatan ini dipicu.	Pertimbangkan untuk menggunakan jenis instance yang lebih besar untuk node master khusus Anda. Karena perannya dalam stabilitas dan blue/green penerapan cluster, node master khusus harus memiliki penggunaan CPU rata-rata yang lebih rendah daripada node data.
OpenSearch contoh	Tidak	AutomatedSnapshotFailure maksimum adalah >= 1 selama 1 menit, 1 kali berturut-turut.	CloudWatch alarm. Sebuah snapshot otomatis gagal. Kegagalan ini sering merupakan hasil dari status kesehatan klaster merah. Lihat Status Cluster Merah.
Contoh Elastic Load Balancing	Tidak	SurgeQueueLength > 100 selama 1 menit, 15 kali berturut-turut.	CloudWatch alarm jika kelebihan jumlah permintaan sedang menunggu perutean.

Layanan	Peringatan keaman	Nama peringatan dan kondisi pemicu	Catatan
		HTTPCode_ELB_5xx_Hitung jumlah> 0 selama 5 menit, 3 kali berturut-turut.	CloudWatch alarm pada kelebihan jumlah kode respons HTTP 5XX yang berasal dari penyeimbang beban.
		SpilloverCount > 1 selama 1 menit, 15 kali berturut-turut.	CloudWatch alarm jika kelebihan jumlah permintaan yang ditolak karena antrian lonjakan penuh.
GuardDuty layanan	Ya	Tidak berlaku; semua temuan (tujuan ancaman) dipantau. Setiap temuan sesuai dengan peringatan. Perubahan dalam GuardDuty temuan. Perubahan ini termasuk temuan yang baru dihasilkan atau kejadian selanjutnya dari temuan yang ada.	Daftar jenis GuardDuty temuan yang didukung ada di Jenis Pencarian GuardDuty Aktif.
Kondisi	Bervariasi	Dasbor AWS Health	Pemberitahuan dikirim ketika ada perubahan status Dasbor AWS Health (AWS Health) peristiwa sehubungan dengan layanan dasar yang didukung oleh AMS. Untuk informasi selengkapnya, lihat Layanan yang didukung.
AWS Managed Microsoft AD	Tidak	Status Direktori Aktif AWS Managed Microsoft AD instance mengirimkan acara status aktif.	Acara layanan. Dipancarkan ketika direktori beroperasi secara normal setelah suatu peristiwa.

Layanan	Peringatan keaman	Nama peringatan dan kondisi pemicu	Catatan
		Status Direktori Terganggu AWS Managed Microsoft AD instance mengirimkan peristiwa status direktori terganggu.	Acara layanan. Dipancarkan saat direktori berjalan dalam keadaan terdegradasi. Satu atau lebih masalah telah terdeteksi, dan tidak semua operasi direktori dapat bekerja pada kapasitas operasional penuh.
		Status Direktori Tidak Dapat Dioperasikan AWS Managed Microsoft AD instance mengirimkan peristiwa status yang tidak dapat dioperasikan.	Acara layanan. Dipancarkan ketika direktori tidak berfungsi. Semua titik akhir direktori telah melaporkan masalah.
		Menghapus Status Direktori AWS Managed Microsoft AD misalnya mengirimkan acara status direktori penghapusan.	Acara layanan. Dipancarkan saat direktori sedang dihapus.
		Status Direktori Gagal AWS Managed Microsoft AD instance mengirimkan peristiwa status gagal.	Acara layanan. Dipancarkan ketika direktori tidak dapat dibuat.
		RestoreFailed Status Direktori AWS Managed Microsoft AD instance mengirimkan peristiwa status direktori yang gagal dipulihkan.	Acara layanan. Dipancarkan saat memulihkan direktori dari snapshot gagal.

Layanan	Peringatan keaman	Nama peringatan dan kondisi pemicu	Catatan
Contoh Amazon RDS	Tidak	Peringatan Penyimpanan Rendah dipicu ketika penyimpanan yang dialokasikan untuk instans DB telah habis.	RDS-EVENT-0007, lihat detail di Menggunakan pemberitahuan acara Amazon RDS.
		Instans DB gagal Instans DB gagal karena konfigurasi tidak kompatibel atau masalah penyimpanan yang mendasarinya. Mulailah a point-in-time-restore untuk instance DB.	Acara layanan. RDS-EVENT-0031, Kategori Acara Amazon RDS dan Pesan Acara.
		Failover tidak dicoba Amazon RDS tidak mencoba failover yang diminta karena failover baru-baru ini terjadi pada instans DB.	Acara layanan. RDS-EVENT-0034, Kategori Acara Amazon RDS dan Pesan Acara.
		Parameter instans DB tidak valid Misalnya, MySQL tidak dapat memulai karena parameter terkait memori disetel terlalu tinggi untuk kelas instance ini, sehingga tindakan pelanggan adalah memodifikasi parameter memori dan me-reboot instance DB.	Acara layanan. RDS-EVENT-0035, Kategori Acara Amazon RDS dan Pesan Acara.
		Instans IDs subnet DB tidak valid Instans DB ada di jaringan yang tidak kompatibel. Beberapa subnet yang ditentukan IDs tidak valid atau tidak ada.	Acara layanan. RDS-EVENT-0036, Kategori Acara Amazon RDS dan Pesan Acara.

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

Layanan	Peringatan keaman	Nama peringatan dan kondisi pemicu	Catatan
		Pemulihan instans DB dimulai Instans DB SQL Server membangun ulang cerminnya. Performa akan diturunkan hingga cermin dibangun kembali. Basis data ditemukan dengan model pemulihan non-FULL. Model pemulihan diubah kembali ke FULL dan pemulihan mirroring dimulai. (<dbname>: <recovery model found>[,...]).	Acara layanan. RDS-EVENT-0066, Kategori Acara Amazon RDS dan Pesan Acara.
		Failover untuk klaster DB telah gagal.	RDS-EVENT-0069, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.
		Bucket S3 pemulihan izin tidak valid Peran IAM yang Anda gunakan untuk mengakses bucket Amazon S3 untuk pencadangan dan pemulihan native SQL Server tidak dikonfigurasi dengan benar. Untuk informasi selengkapnya, lihat Menyiapkan Pencadangan dan Pemulihan Asli.	Acara layanan. RDS-EVENT-0081, Kategori Acara Amazon RDS dan Pesan Acara.
		Aurora tidak dapat menyalin data cadangan dari bucket Amazon S3.	RDS-EVENT-0082, lihat detail di Kategori Acara Amazon RDS dan Pesan Acara.

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

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

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

Retensi log dan default rotasi

Bagian ini menjelaskan default manajemen log AMS; untuk informasi selengkapnya, lihat Manajemen Log.

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

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

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

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

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

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

Default manajemen kontinuitas

Bagian ini menjelaskan default manajemen kontinuitas AMS; untuk informasi selengkapnya tentang cadangan AMS, lihat bagian Manajemen Kontinuitas Panduan Pengguna AMS.

Konfigurasi Backup dilakukan pada saat onboarding. Ini adalah pengaturan cadangan default (disarankan).

Tag VPC dan default

Untuk informasi terbaru tentang cadangan AMS, lihat Manajemen kontinuitas.

> **Important**
>
> Secara default, cadangan EC2 tumpukan dinonaktifkan (Backup = False). Anda dapat mengaktifkan cadangan EC2 instance pada saat pembuatan dengan menambahkan tag `Key: Backup, Value: True` saat meminta EC2 tumpukan melalui RFC (CT ct-14027q0sjyt1h). Jika Anda ingin menambahkan tag setelah instance dibuat, kirimkan RFC dengan Management | Advanced stack components | EC2 instance stack | Update CT (ct-38s4s4tm4ic4u).

EC2 tag instance dan default

Tag cadangan EC2 stack menentukan apakah tumpukan memerlukan snapshot dari volume EBS terlampir atau tidak.

`Tag Key: Backup`

`Tag Value: True, False`

Secara default, nilainya adalah `False` tag cadangan tidak ada, dan tumpukan tidak memiliki cadangan terjadwal.

Ubah tag `Key: Backup` `Value: True` untuk mengaktifkan cadangan, yang kemudian dilakukan pada jadwal yang ditetapkan dengan tag cadangan VPC.

> **Note**
>
> Casing untuk nilai tag (hanya Nilai) tidak sensitif, jadi True/true atau False/false semuanya dapat diterima.

Pencadangan dan default instans RDS

Nilai default Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) didefinisikan dalam template tumpukan:

```
Backup: Yes

Backup Window: 22:00-23:00 (RDS local time zone)

Retention Period: 7 (7 snapshots stored)
```

Menambal default

Bagian ini menjelaskan default penambalan AMS; untuk informasi selengkapnya tentang penambalan AMS, lihat bagian Manajemen Patch Panduan Pengguna AMS.

Rilis AMS ditambal AMIs setiap bulan; semua permintaan tumpukan baru harus dikonfigurasi dengan AMS AMI terbaru.

> **Important**
>
> AMS Patch Orchestrator, penambalan berbasis tag, menggunakan fungsionalitas AWS Systems Manager (SSM) untuk memungkinkan Anda menandai, atau memiliki tag AMS untuk Anda, instance, dan menambal instance tersebut menggunakan baseline dan jendela yang Anda konfigurasikan. Untuk mempelajari lebih lanjut, lihat Patch Orchestrator: model patching berbasis tag.

Standar AMS, berbasis akun, patching: Untuk setiap akun dengan tumpukan yang menerima penambalan di tempat, pemberitahuan tambalan yang berlaku yang akan datang dikirim segera setelah “patch Tuesday”. Pemberitahuan berisi daftar semua tumpukan dan tambalan yang berlaku serta jendela tambalan yang disarankan. Untuk tambalan kritis, jendela diatur tidak lebih dari 10 hari

sebelumnya, dan untuk penambalan standar tidak lebih dari 14 hari sebelumnya. Jika Anda tidak membalas notifikasi, penambalan tidak terjadi. Jika Anda ingin mengecualikan tambalan tertentu, balas pemberitahuan, atau kirimkan permintaan layanan. Jika Anda membalas dengan persetujuan untuk menambal, tetapi tidak secara khusus meminta jadwal yang berbeda, tambalan diterapkan seperti yang dijelaskan dalam pemberitahuan yang Anda terima.

> **Note**
>
> Pemberitahuan layanan tambalan adalah email yang dikirim ke kontak akun dan berisi tautan ke konsol AWS Support. Anda dapat membalas melalui AWS Support console atau melalui halaman permintaan layanan AMS, di mana notifikasi muncul sebagai pemberitahuan layanan.

Pada saat proses penambalan standar AMS, AMS melakukan hal berikut:

1. Anda dikirimi pemberitahuan layanan patching empat belas hari sebelum jendela patch yang diusulkan. Pemberitahuan layanan patching dikirim melalui email ke alamat email kontak yang Anda miliki di file untuk akun Anda.
2. Mengidentifikasi semua EC2 instance yang dapat dijangkau dalam tumpukan berdasarkan daftar tumpukan yang disediakan dalam pemberitahuan penambalan. Dalam hal ini, “Dapat Dijangkau” berarti instance yang berada dalam EC2 status “Running”, dan agen EC2 Run Command beroperasi penuh.
3. AMS melakukan penambalan dengan cara yang memastikan bahwa jumlah EC2 instance yang cukup berjalan secara bersamaan (dikonfigurasi melalui `healthy-host-threshold` pengaturan) sehingga tumpukan tetap sehat.
4. Setelah operasi patching selesai untuk semua EC2 instance, AMS memperbarui RFC dengan status patching: Success, Partial Success atau Failure. Dalam hal status apa pun selain Sukses, tiket dibuat untuk operator untuk menindaklanjuti hasil penambalan dan mengambil tindakan korektif apa pun.

Validasi layanan AMS (SALZ)

Untuk memvalidasi bahwa layanan AWS Managed Services (AMS) berfungsi seperti yang diharapkan, beberapa latihan yang dapat Anda lakukan dijelaskan dalam Bab ini.

Temukan pengaturan akun AMS

Pengaturan akun yang digunakan untuk membuat AMS RFCs, mengatur jadwal, dan menentukan siapa yang menerima notifikasi.

Beberapa pengaturan dibuat selama orientasi dan memerlukan permintaan layanan untuk diubah. Anda harus mencatat detail akun ini karena Anda akan menggunakannya saat berkomunikasi dengan AMS:

- Kredensil: Jika Anda perlu mengambil nama pengguna atau kata sandi AMS Anda, hubungi Administrator TI lokal Anda - AMS menggunakan Direktori Aktif perusahaan Anda.
- Cloud Service Delivery Manager (CSDM): Orang ini adalah penghubung Anda dengan AMS dan tersedia untuk menjawab pertanyaan layanan. Anda diberikan informasi kontak orang ini saat orientasi dan harus tetap tersedia untuk semua orang di organisasi Anda yang berinteraksi dengan AMS. Anda dapat mengharapkan untuk menerima laporan bulanan tentang layanan AMS Anda dari orang ini.
- Akses konsol: Anda mengakses konsol AMS di URL yang disiapkan khusus untuk akun Anda. Anda bisa mendapatkan URL dari CSDM Anda.
- AMS CLI: Anda dapat memperoleh AMS CLI melalui halaman sumber daya Pengembang konsol AMS, atau paket yang dapat didistribusikan yang Anda dapatkan dari CSDM Anda. Setelah Anda memiliki paket yang dapat didistribusikan, ikuti langkah-langkah yang diuraikan dalam Menginstal atau meningkatkan CLI AMS.
- Jendela pemeliharaan: Jendela pemeliharaan Anda menentukan kapan penambalan terjadi untuk EC2 instance Anda. AWS Managed Services Maintenance Window (atau Maintenance Window) melakukan aktivitas pemeliharaan untuk AWS Managed Services (AMS) dan berulang pada hari Kamis kedua setiap bulan mulai pukul 15:00 hingga 16:00 Waktu Pasifik. AMS dapat mengubah jendela pemeliharaan dengan pemberitahuan 48 jam. Anda mungkin telah memilih jendela yang berbeda saat onboarding--menyimpan catatan jendela pemeliharaan yang Anda pilih.
- Pemantauan: AMS menyediakan satu set CloudWatch metrik secara default, tetapi Anda juga dapat meminta metrik tambahan. Jika Anda melakukannya, catat itu.
- Log: Secara default, log Anda disimpan di ams-a- *ACCOUNT_ID* -log-management- *REGION* di mana *REGION* adalah wilayah tempat log dibuat.
- Mitigasi: Saat orientasi, AMS mencatat tindakan mitigasi pilihan Anda jika serangan malware terhadap sumber daya Anda diidentifikasi. Misalnya, hubungi orang-orang tertentu. Pastikan informasi ini tersedia untuk semua orang di organisasi Anda yang berinteraksi dengan AMS.

- Wilayah: Anda dapat melihat halaman detail VPC di konsol AMS. Anda juga dapat menjalankan perintah ini setelah Anda menginstal AMS SKMS CLI (perintah ini menggunakan profil SAFL, hapus jika metode otentikasi Anda berbeda):

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

Important

Note

Titik akhir AMS API/CLI (amscm dan amsskms) berada di Wilayah AWS N. Virginia,. `us-east-1` Bergantung pada bagaimana autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan`--profile saml`, jika itu adalah metode otentikasi Anda.

Temukan FQDNs di AMS

Jenis perubahan akses AWS Managed Services (AMSCTs) () memerlukan nama domain yang sepenuhnya memenuhi syarat, atau FQDN, dari domain tepercaya AMS Anda, dalam bentuk. `C844273800838.amazonaws.com` Untuk menemukan AWS FQDN Anda, lakukan salah satu hal berikut:

- AWS Console: Lihat di konsol AWS Directory Service di kolom nama Direktori.
- CLI: Gunakan perintah ini saat masuk ke domain Anda:

  Windows (mengembalikan pengguna dan FQDN):

```
whoami /upn
```

  atau (DC+DC+DC = FQDN)

```
whoami /fqdn
```

  Linux:

```
hostname --fqdn
```

> **Note**
>
> Titik akhir AMS API/CLI (amscm dan amsskms) berada di Wilayah AWS N. Virginia,. `us-east-1` Bergantung pada cara autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan`--profile saml`, jika itu adalah metode otentikasi Anda.

Temukan zona ketersediaan (AZs) di AMS

Availability Zone: Semua akun memiliki setidaknya dua zona ketersediaan. Untuk menemukan nama zona ketersediaan Anda secara akurat, Anda harus terlebih dahulu mengetahui ID subnet terkait.

- Konsol AMS: Di panel navigasi klik VPCs, lalu klik VPC yang relevan, jika perlu. Pada halaman VPCs detail, pilih subnet yang relevan dalam tabel subnet untuk membuka halaman detail subnet dengan nama zona ketersediaan terkait.
- AMS SKMS API/CLI:

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

> **Note**
>
> Titik akhir AMS API/CLI (amscm dan amsskms) berada di Wilayah AWS N. Virginia,. `us-east-1` Bergantung pada cara autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan`--profile saml`, jika itu adalah metode otentikasi Anda.

Temukan topik SNS di AMS

Topik SNS Anda menentukan siapa yang diberi tahu dalam berbagai keadaan. AMS menyediakan topik SNS untuk notifikasi AMI (lihat notifikasi AMS AMI dengan SNS), CloudWatch alarm, dan EC2 sumber daya (lihat Menerima peringatan yang dihasilkan oleh AMS) dan banyak lagi. Untuk menemukan topik SNS Anda yang ada:

- AWS Console: Gunakan konsol SNS untuk melihat semua topik, aplikasi, dan langganan, serta grafik pesan. Juga buat, hapus, berlangganan, dan publikasikan ke topik.
- API/CLI (saat masuk ke akun AMS Anda, memerlukan AWS CLI):

  Daftar topik SNS Anda:

  ```
  aws sns list-topics
  ```

  Daftar langganan SNS Anda:

  ```
  aws sns list-subscriptions
  ```

> **Note**
>
> Titik akhir AMS API/CLI (amscm dan amsskms) berada di Wilayah AWS N. Virginia,. `us-east-1` Bergantung pada cara autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan`--profile saml`, jika itu adalah metode otentikasi Anda.

Temukan pengaturan cadangan di AMS

Cadangan dan snapshot dikelola oleh AMS melalui layanan asli. AWS Backup

Konfigurasi dikelola melalui AWS Backup rencana. Anda dapat memiliki beberapa AWS Backup paket yang mengaitkan sumber daya yang ditandai dengan jadwal cadangan dan kebijakan penyimpanan. Untuk menemukan AWS Backup pengaturan akun AMS Anda, gunakan konsol https://console.aws.amazon.com/backup, atau AWS CLI Command Reference untuk perintah cadangan.

Untuk informasi selengkapnya tentang AMS dan AWS Backup, lihat Manajemen Kontinuitas.

Menemukan ID instans atau alamat IP

Anda memerlukan alamat IP instance untuk masuk ke instance.

- Untuk meminta akses ke instance, masuk ke instance, atau membuat AMI, Anda harus memiliki ID instans. Untuk sebuah EC2 instance (baik instance mandiri atau bagian dari tumpukan), atau instance database, Anda dapat menemukan ID dalam beberapa cara berbeda:
  - Konsol AMS untuk instance dalam tumpukan ASG: Lihat di halaman detail RFC untuk RFC yang membuat tumpukan. Di bagian Output Eksekusi, Anda akan menemukan ID tumpukan untuk tumpukan ASG dan Anda kemudian dapat pergi ke halaman EC2 Console Auto Scaling Groups dan mencari ID tumpukan itu dan menemukan instance untuk itu. Ketika Anda menemukan instance, pilih dan area terbuka di bagian bawah halaman dengan detail, termasuk alamat IP.
  - Konsol AMS untuk instance mandiri EC2 atau database (DB): Lihat di halaman detail RFC untuk RFC yang membuat instans EC2 stack atau DB. Di bagian Output Eksekusi, Anda akan menemukan ID Instans dan alamat IP.
  - EC2 Konsol AWS:
    1. Di panel navigasi, pilih Instans. Halaman Instances terbuka.
    2. Klik contoh yang Anda inginkan ID untuk. Halaman detail instance membuka dan menampilkan ID dan alamat IP.
  - Konsol Database AWS:
    1. Pada halaman Beranda, pilih Instans DB. Halaman Instances terbuka.
    2. Filter untuk instance DB yang Anda inginkan ID untuk. Halaman detail instance membuka dan menampilkan ID.
  - AMS CLI/API.

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

kehabisan us-east-1; misalnya. `aws amscm ams-cli-command --region=us-east-1`

> **Note**
>
> Titik akhir AMS API/CLI (amscm dan amsskms) berada di Wilayah AWS N. Virginia,. `us-east-1` Bergantung pada bagaimana autentikasi Anda disetel, dan di Wilayah AWS akun dan sumber daya Anda, Anda mungkin perlu menambahkan `--region us-east-1` saat mengeluarkan perintah. Anda mungkin juga perlu menambahkan`--profile saml`, jika itu adalah metode otentikasi Anda.

Jalankan perintah berikut untuk mendapatkan detail output eksekusi stack:

```
aws amsskms get-stack --stack-id STACK_ID
```

Outputnya terlihat mirip dengan ini dengan InstanceId muncul di dekat bagian bawah, di bawah `Outputs` (nilai yang ditampilkan adalah contoh):

```
{
    "Stack": {
        "StackId": "stack-7fa52bd5eb8240123",
        "Status": {
            "Id": "CreateCompleted",
            "Name": "CreateCompleted"
        },
        "VpcId": "vpc-01234567890abcdef",
        "Description": "Amazon",
        "Parameters": [
            {
                "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
                "Key": "SecurityGroups"
            },
            {
                "Value": "subnet-01234567890abcdef",
                "Key": "InstanceSubnetId"
            },
            {
                "Value": "t2.large",
```

```
                "Key": "InstanceType"
            },
            {
                "Value": "ami-01234567890abcdef",
                "Key": "InstanceAmiId"
            }
        ],
        "Tags": [],
        "Outputs": [
            {
                "Value": "i-0b22a22eec53b9321",
                "Key": "InstanceId"
            },
            {
                "Value": "10.0.5.000",
                "Key": "InstancePrivateIP"
            }
        ],
        "StackTemplateId": "stm-s6xvs000000000000",
        "CreatedTime": "1486584508416",
        "Name": "Amazon"
    }
}
```


Nama benteng ramah DNS

MALZ

Untuk multi-account landing zone (MALZ), catatan DNS dibuat untuk bastion di FQDN dari Direktori Aktif yang dikelola AMS. AMS menggantikan benteng Linux dan Windows sesuai kebutuhan. Misalnya, jika ada benteng AMI baru yang harus digunakan, catatan DNS bastion diperbarui secara dinamis untuk menunjuk ke bastion baru yang valid.

1. Untuk mengakses bastion SSH (Linux), gunakan catatan DNS seperti ini: `sshbastion`*`(1-4)`*`.`*`Your_Domain`*`.com`

   Misalnya, di mana domain adalah`Your_Domain`:

   - `sshbastion1.`*`Your_Domain`*`.com`
   - `sshbastion2.`*`Your_Domain`*`.com`

- sshbastion3.*Your_Domain*.com
- sshbastion4.*Your_Domain*.com

2. Untuk mengakses benteng RDP (Windows), gunakan catatan DNS seperti ini:. rdp-*Username*.*Your_Domain*.com

   Misalnya, di mana nama pengguna adalahalex,test,demo, ataubob, dan domain adalah*Your_Domain*.com:

   - rdp-alex.*Your_Domain*.com
   - rdp-test.*Your_Domain*.com
   - rdp-demo.*Your_Domain*.com
   - rdp-bob.*Your_Domain*.com

SALZ

Single-account landing zone (SALZ) menggantikan benteng Linux dan Windows sesuai kebutuhan. Misalnya, jika ada benteng AMI baru yang harus digunakan, catatan DNS bastion diperbarui secara dinamis untuk menunjuk ke bastion baru yang valid.

1. Untuk mengakses bastion SSH (Linux), gunakan catatan DNS seperti ini: sshbastion*(1-4)*.A*AccountNumber*.amazonaws.com.

   Misalnya, di 123456789012 mana nomor akun:

   - sshbastion1.A123456789012.amazonaws.com
   - sshbastion2.A123456789012.amazonaws.com
   - sshbastion3.A123456789012.amazonaws.com
   - sshbastion4.A123456789012.amazonaws.com

2. Untuk mengakses benteng RDP (Windows), gunakan catatan DNS seperti ini:. rdpbastion*(1-4)*.A*ACCOUNT_NUMBER*.amazonaws.com

   Misalnya, di 123456789012 mana nomor akun:

   - rdpbastion1.A123456789012.amazonaws.com
   - rdpbastion2.A123456789012.amazonaws.com
   - rdpbastion3.A123456789012.amazonaws.com

- `rdpbastion4.A123456789012.amazonaws.com`

Menemukan alamat IP benteng

Pelanggan AMS dapat menggunakan bastion SSH dan RDP, baik yang Nama benteng ramah DNS dijelaskan sebelumnya, atau alamat IP bastion.

Untuk menemukan alamat IP bastion, SSH dan RDP, untuk akun Anda:

1. Hanya untuk landing zone multi-akun: Masuk ke akun Layanan Bersama.
2. Buka EC2 Console dan pilih Running Instances.

   Halaman Instances terbuka.
3. Di kotak filter di bagian atas, masukkan ssh-bastion atau rdp-bastion.

   Di kotak filter di bagian atas, masukkan customer-ssh atau customer-rdp.

   Benteng SSH and/or RDP untuk tampilan akun Anda.

   Perhatikan bahwa selain bastion SSH Anda, Anda mungkin melihat benteng jaringan perimeter AMS dalam daftar, yang tidak tersedia untuk ini.
4. Pilih benteng SSH atau RDP. Jika Anda menggunakan komputer Windows dan ingin masuk ke instance Linux, Anda menggunakan bastion SSH. Jika Anda ingin masuk ke instance Windows, Anda menggunakan benteng RDP. Jika Anda menggunakan OS Linux dan ingin masuk ke instance Windows, Anda menggunakan benteng SSH melalui terowongan RDP (ini agar Anda dapat mengakses desktop Windows). Untuk mengakses instance Linux dari OS Linux, Anda menggunakan bastion SSH.

EC2 contoh: Membuat

Anda dapat menggunakan konsol AMS atau API/CLI untuk membuat Amazon EC2 dan Amazon EC2 dengan volume tambahan.

Buat tumpukan

Membuat EC2 instance dengan konsol

Berikut ini menunjukkan jenis perubahan ini di konsol AMS.

Cara kerjanya:

1. Arahkan ke halaman Buat RFC: Di panel navigasi kiri konsol AMS klik RFCsuntuk membuka halaman RFCs daftar, lalu klik Buat RFC.
2. Pilih jenis perubahan populer (CT) di tampilan default Jelajahi jenis perubahan, atau pilih CT dalam tampilan Pilih menurut kategori.
   - Jelajahi berdasarkan jenis perubahan: Anda dapat mengklik CT populer di area Buat cepat untuk segera membuka halaman Jalankan RFC. Perhatikan bahwa Anda tidak dapat memilih versi CT yang lebih lama dengan pembuatan cepat.

     Untuk mengurutkan CTs, gunakan area Semua jenis perubahan dalam tampilan Kartu atau Tabel. Di kedua tampilan, pilih CT dan kemudian klik Buat RFC untuk membuka halaman Jalankan RFC. Jika berlaku, opsi Buat dengan versi yang lebih lama muncul di sebelah tombol Buat RFC.
   - Pilih berdasarkan kategori: Pilih kategori, subkategori, item, dan operasi dan kotak detail CT terbuka dengan opsi untuk Membuat dengan versi yang lebih lama jika berlaku. Klik Buat RFC untuk membuka halaman Jalankan RFC.
3. Pada halaman Run RFC, buka area nama CT untuk melihat kotak detail CT. Subjek diperlukan (ini diisi untuk Anda jika Anda memilih CT Anda di tampilan jenis perubahan Jelajahi). Buka area konfigurasi tambahan untuk menambahkan informasi tentang RFC.

   Di area konfigurasi Eksekusi, gunakan daftar drop-down yang tersedia atau masukkan nilai untuk parameter yang diperlukan. Untuk mengkonfigurasi parameter eksekusi opsional, buka area konfigurasi tambahan.
4. Setelah selesai, klik Jalankan. Jika tidak ada kesalahan, halaman RFC berhasil dibuat ditampilkan dengan detail RFC yang dikirimkan, dan output Run awal.
5. Buka area parameter Jalankan untuk melihat konfigurasi yang Anda kirimkan. Segarkan halaman untuk memperbarui status eksekusi RFC. Secara opsional, batalkan RFC atau buat salinannya dengan opsi di bagian atas halaman.

Membuat EC2 instance dengan CLI

Cara kerjanya:

1. Gunakan Inline Create (Anda mengeluarkan `create-rfc` perintah dengan semua RFC dan parameter eksekusi disertakan), atau Template Create (Anda membuat dua file JSON, satu untuk parameter RFC dan satu untuk parameter eksekusi) dan mengeluarkan `create-rfc` perintah dengan dua file sebagai input. Kedua metode tersebut dijelaskan di sini.
2. Kirim `aws amscm submit-rfc --rfc-id` *`ID`* perintah RFC: dengan ID RFC yang dikembalikan.

   Pantau `aws amscm get-rfc --rfc-id` *`ID`* perintah RFC:.

Untuk memeriksa versi jenis perubahan, gunakan perintah ini:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Anda dapat menggunakan `CreateRfc` parameter apa pun dengan RFC apa pun apakah itu bagian dari skema untuk jenis perubahan atau tidak. Misalnya, untuk mendapatkan pemberitahuan ketika status RFC berubah, tambahkan baris ini, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` ke bagian parameter RFC dari permintaan (bukan parameter eksekusi). Untuk daftar semua CreateRfc parameter, lihat Referensi AMS Change Management API.

BUAT SEBARIS:

Keluarkan perintah create RFC dengan parameter eksekusi yang disediakan sebaris (tanda kutip escape saat memberikan parameter eksekusi sebaris), lalu kirimkan ID RFC yang dikembalikan. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```
aws amscm create-rfc --change-type-id "ct-14027q0sjyt1h" --change-type-version "4.0"
 --title "EC2-Create-RFC" --execution-parameters "{\"Description\": \"Create a new
 EC2 Instance stack\",\"VpcId\": \"vpc-0a60eb65b4EXAMPLE\",\"Name\": \"My-EC2\",
\"TimeoutInMinutes\": 60,\"Parameters\": {\"InstanceAmiId\": \"ami-1234567890EXAMPLE\",
\"InstanceDetailedMonitoring\": false,\"InstanceEBSOptimized\": false,\"InstanceProfile
\": \"customer-mc-ec2-instance-profile\",\"InstanceRootVolumeIops\": 3000,
\"InstanceRootVolumeType\": \"gp3\",\"InstanceType\": \"t2.large\",\"InstanceUserData
```

```
\": \"\",\"InstanceSubnetId\": \"subnet-0bb1c79de3EXAMPLE\",\"EnforceIMDSV2\":
 \"false\"}}"
```

TEMPLATE MEMBUAT:

1. Output parameter eksekusi untuk jenis perubahan ini ke file JSON; contoh ini menamainya Create EC2 Params.json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-14027q0sjyt1h" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2Params.json
   ```

2. Ubah dan simpan file Create EC2 Params. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

   ```
   {
     "Description": "Create a new EC2 Instance stack",
     "VpcId": "vpc-0a60eb65b4EXAMPLE",
     "Name": "My-EC2",
     "TimeoutInMinutes": 60,
     "Parameters": {
       "InstanceAmiId": "ami-1234567890EXAMPLE",
       "InstanceDetailedMonitoring": false,
       "InstanceEBSOptimized": false,
       "InstanceProfile": "customer-mc-ec2-instance-profile",
       "InstanceRootVolumeIops": 3000,
       "InstanceRootVolumeType": "gp3",
       "InstanceType": "t2.large",
       "InstanceUserData": "",
       "InstanceSubnetId": "subnet-0bb1c79de3EXAMPLE",
       "EnforceIMDSV2": "false"
     }
   }
   ```

3. Keluarkan template RFC ke file di folder Anda saat ini; contoh ini menamainya Create EC2 RFC.json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > CreateEC2Rfc.json
   ```

4. Ubah dan simpan file Create EC2 RFC.json. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:.

   ```
   {
   ```

```
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-14027q0sjyt1h",
"Title":                "EC2-Create-RFC"
}
```

5. Buat RFC, tentukan file Create EC2 Rfc dan file Create EC2 Params:

```
aws amscm create-rfc --cli-input-json file://CreateEC2Rfc.json  --execution-
parameters file://CreateEC2Params.json
```

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

Kiat

Grup Keamanan

Dimulai dengan versi 3.0 dari jenis perubahan ini, AMS tidak melampirkan grup keamanan AMS default jika Anda menentukan grup keamanan Anda sendiri. Jika Anda tidak menentukan grup keamanan Anda sendiri dalam permintaan, AMS melampirkan grup keamanan default AMS. Di versi sebelumnya, AMS melampirkan grup keamanan default apakah Anda menyediakan grup keamanan Anda sendiri atau tidak.
Saat ini, jika Anda menentukan grup keamanan khusus, Anda juga harus menentukan grup keamanan AMS default untuk akun Anda, `mc-initial-garden-SG-name` dan`mc-initial-garden-SG-name`. IDs

Jenis Instance

AMS tidak merekomendasikan tipe t2.micro/t3.micro dan t2.nano/t3.nano. Ini adalah jenis instans yang lebih kecil, dan dapat menurunkan kinerja aplikasi dan alat AMS Anda. EC2 Instans membutuhkan kapasitas yang cukup untuk mendukung alat AMS seperti EPS, SSM, dan Cloudwatch selain beban kerja aplikasi. Untuk informasi selengkapnya, lihat Memilih Jenis EC2 Instans yang Tepat untuk Aplikasi Anda.

Untuk membuat EC2 tumpukan dengan volume tambahan, lihat EC2 Stack | Create (with Additional Volume).

Anda dapat menambahkan hingga 50 tag, tetapi untuk melakukannya Anda harus mengaktifkan tampilan konfigurasi tambahan.

Jika diperlukan, lihat EC2 instance stack create gagal.

Buat tumpukan (dengan volume tambahan)

Membuat EC2 instance dan volume tambahan dengan konsol

Berikut ini menunjukkan jenis perubahan ini di konsol AMS.

Cara kerjanya:

1. Arahkan ke halaman Buat RFC: Di panel navigasi kiri konsol AMS klik RFCsuntuk membuka halaman RFCs daftar, lalu klik Buat RFC.
2. Pilih jenis perubahan populer (CT) di tampilan default Jelajahi jenis perubahan, atau pilih CT dalam tampilan Pilih menurut kategori.
   - Jelajahi berdasarkan jenis perubahan: Anda dapat mengklik CT populer di area Buat cepat untuk segera membuka halaman Jalankan RFC. Perhatikan bahwa Anda tidak dapat memilih versi CT yang lebih lama dengan pembuatan cepat.

     Untuk mengurutkan CTs, gunakan area Semua jenis perubahan dalam tampilan Kartu atau Tabel. Di kedua tampilan, pilih CT dan kemudian klik Buat RFC untuk membuka halaman Jalankan RFC. Jika berlaku, opsi Buat dengan versi yang lebih lama muncul di sebelah tombol Buat RFC.
   - Pilih berdasarkan kategori: Pilih kategori, subkategori, item, dan operasi dan kotak detail CT terbuka dengan opsi untuk Membuat dengan versi yang lebih lama jika berlaku. Klik Buat RFC untuk membuka halaman Jalankan RFC.
3. Pada halaman Run RFC, buka area nama CT untuk melihat kotak detail CT. Subjek diperlukan (ini diisi untuk Anda jika Anda memilih CT Anda di tampilan jenis perubahan Jelajahi). Buka area konfigurasi tambahan untuk menambahkan informasi tentang RFC.

   Di area konfigurasi Eksekusi, gunakan daftar drop-down yang tersedia atau masukkan nilai untuk parameter yang diperlukan. Untuk mengkonfigurasi parameter eksekusi opsional, buka area konfigurasi tambahan.

4. Setelah selesai, klik Jalankan. Jika tidak ada kesalahan, halaman RFC berhasil dibuat ditampilkan dengan detail RFC yang dikirimkan, dan output Run awal.
5. Buka area parameter Jalankan untuk melihat konfigurasi yang Anda kirimkan. Segarkan halaman untuk memperbarui status eksekusi RFC. Secara opsional, batalkan RFC atau buat salinannya dengan opsi di bagian atas halaman.

Membuat EC2 instance dan volume tambahan dengan CLI

Cara kerjanya:

1. Gunakan Inline Create (Anda mengeluarkan `create-rfc` perintah dengan semua RFC dan parameter eksekusi disertakan), atau Template Create (Anda membuat dua file JSON, satu untuk parameter RFC dan satu untuk parameter eksekusi) dan mengeluarkan `create-rfc` perintah dengan dua file sebagai input. Kedua metode tersebut dijelaskan di sini.
2. Kirim `aws amscm submit-rfc --rfc-id` *`ID`* perintah RFC: dengan ID RFC yang dikembalikan.

   Pantau `aws amscm get-rfc --rfc-id` *`ID`* perintah RFC:.

Untuk memeriksa versi jenis perubahan, gunakan perintah ini:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Anda dapat menggunakan `CreateRfc` parameter apa pun dengan RFC apa pun apakah itu bagian dari skema untuk jenis perubahan atau tidak. Misalnya, untuk mendapatkan pemberitahuan ketika status RFC berubah, tambahkan baris ini, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` ke bagian parameter RFC dari permintaan (bukan parameter eksekusi). Untuk daftar semua CreateRfc parameter, lihat Referensi AMS Change Management API.

BUAT SEBARIS:

Keluarkan perintah create RFC dengan parameter eksekusi yang disediakan sebaris (tanda kutip escape saat memberikan parameter eksekusi sebaris), lalu kirimkan ID RFC yang dikembalikan

(contoh hanya menunjukkan parameter yang diperlukan). Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```
aws amscm create-rfc --change-type-id "ct-1aqsjf86w6vxg" --change-type-version "4.0"
 --title "EC2-Create-A-V-QC" --execution-parameters "{\"Description\":\"My EC2 stack
 with addl vol\",\"VpcId\":\"VPC_ID\",\"Name\":\"My Stack\",\"StackTemplateId\":
\"stm-nn8v8ffhcal611bmo\",\"TimeoutInMinutes\":60,\"Parameters\":{\"InstanceAmiId\":
\"AMI_ID\",\"InstanceSubnetId\":\"SUBNET_ID\"}}
```

TEMPLATE MEMBUAT:

1. Output parameter eksekusi untuk jenis perubahan ini ke file JSON bernama Create EC2 AVParams .json.

   ```
   aws amscm get-change-type-version --change-type-id "ct-1aqsjf86w6vxg" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2AVParams.json
   ```

2. Ubah dan simpan EC2 AVParams file Buat (contoh menunjukkan sebagian besar parameter). Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

   ```
   {
   "Description":      "EC2-Create-1-Addl-Volumes",
   "VpcId":            "VPC_ID",
   "StackTemplateId":  "stm-nn8v8ffhcal611bmo",
   "Name":             "My-EC2-1-Addl-Volume",
   "TimeoutInMinutes": 60,
   "Parameters":   {
       "InstanceAmiId":    "AMI_ID",
       "InstanceSecurityGroupIds": "SECURITY_GROUP_ID",
       "InstanceCoreCount": 1,
       "InstanceThreadsPerCore": 2,
       "InstanceDetailedMonitoring": "true",
       "InstanceEBSOptimized": "false",
       "InstanceProfile": "customer-mc-ec2-instance-profile",
       "InstanceRootVolumeIops": 100,
       "InstanceRootVolumeName": "/dev/xvda",
       "InstanceRootVolumeSize": 50,
       "InstanceRootVolumeType": "io1",
       "RootVolumeKmsKeyId": "default",
       "InstancePrivateStaticIp": "10.27.0.100",
       "InstanceSecondaryPrivateIpAddressCount": 0,
       "InstanceTerminationProtection": "false",
   ```

```
    "InstanceType": "t3.large",
    "CreditSpecification": "unlimited",
    "InstanceUserData": "echo $",
    "Volume1Encrypted": "true",
    "Volume1Iops":      "IOPS"
    "Volume1KmsKeyId":  "KMS_MASTER_KEY_ID",
    "Volume1Name":      "xvdh"
    "Volume1Size":      "2 GiB",
    "Volume1Snapshot":  "SNAPSHOT_ID",
    "Volume1Type":      "iol",
    "InstanceSubnetId": "SUBNET_ID"
    }
}
```

3. Keluarkan template RFC ke file di folder Anda saat ini; contoh ini menamainya Create EC2 AVRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2AVRfc.json
```

4. Ubah dan simpan file Create EC2 AVRfc .json. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-1aqsjf86w6vxg",
"Title":                "EC2-Create-1-Addl-Volume-RFC"
}
```

5. Buat RFC, tentukan file Create dan Create EC2 AVRfc file: EC2 AVParams

```
aws amscm create-rfc --cli-input-json file://CreateEC2AVRfc.json  --execution-
parameters file://CreateEC2AVParams.json
```

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

Kiat

Important

Ada versi baru dari jenis perubahan ini, v 4.0, yang menggunakan yang berbeda StackTemplateId (stm-nn8v8ffhcal611bmo). Ini penting jika Anda mengirimkan RFC dengan jenis perubahan ini di baris perintah. Versi baru memperkenalkan dua parameter baru (RootVolumeKmsKeyIddan CreditSpecification) dan mengubah default untuk satu parameter yang ada (InstanceType).

Jenis Instance

- Jika Anda memilih untuk menentukan jumlah inti atau utas, Anda harus menentukan nilai untuk keduanya. Gunakan parameter `InstanceCoreCount` dan`InstanceThreadsPerCore`. Untuk menemukan kombinasi inti/utas yang valid, lihat inti CPU dan utas per inti CPU per jenis instans.
- AMS tidak merekomendasikan jenis instans t2.micro/t3.micro atau t2.nano/t3.nano. Ini terlalu kecil untuk mendukung alat AMS seperti EPS, SSM, dan Cloudwatch selain beban kerja bisnis Anda. Untuk informasi selengkapnya, lihat Memilih Jenis EC2 Instans yang Tepat untuk Aplikasi Anda.
- Di versi 4.0, tipe default dinaikkan dari t2.large ke t3.large. Instans T3 diluncurkan dengan 'kredit tidak terbatas' secara default. Anda tidak akan mengalami pelambatan CPU meskipun instans mengkonsumsi semua kredit CPU. Anda dapat, sebagai gantinya, memilih instans T2 dan menggunakan opsi CreditSpecification tak terbatas.
- Untuk informasi selengkapnya tentang Amazon EC2, termasuk rekomendasi ukuran, lihat Amazon Elastic Compute Cloud Documentation.

Untuk memperbarui EC2 tumpukan Anda dengan volume tambahan setelah dibuat, lihat Tumpukan EC2 instans: Memperbarui (Dengan Volume Tambahan)

Akses, meminta

Minta akses administratif

Meminta akses administrator dengan konsol

Berikut ini menunjukkan jenis perubahan ini di konsol AMS.

Cara kerjanya:

1. Arahkan ke halaman Buat RFC: Di panel navigasi kiri konsol AMS klik RFCsuntuk membuka halaman RFCs daftar, lalu klik Buat RFC.
2. Pilih jenis perubahan populer (CT) di tampilan default Jelajahi jenis perubahan, atau pilih CT dalam tampilan Pilih menurut kategori.
   - Jelajahi berdasarkan jenis perubahan: Anda dapat mengklik CT populer di area Buat cepat untuk segera membuka halaman Jalankan RFC. Perhatikan bahwa Anda tidak dapat memilih versi CT yang lebih lama dengan pembuatan cepat.

     Untuk mengurutkan CTs, gunakan area Semua jenis perubahan dalam tampilan Kartu atau Tabel. Di kedua tampilan, pilih CT dan kemudian klik Buat RFC untuk membuka halaman Jalankan RFC. Jika berlaku, opsi Buat dengan versi yang lebih lama muncul di sebelah tombol Buat RFC.
   - Pilih berdasarkan kategori: Pilih kategori, subkategori, item, dan operasi dan kotak detail CT terbuka dengan opsi untuk Membuat dengan versi yang lebih lama jika berlaku. Klik Buat RFC untuk membuka halaman Jalankan RFC.
3. Pada halaman Run RFC, buka area nama CT untuk melihat kotak detail CT. Subjek diperlukan (ini diisi untuk Anda jika Anda memilih CT Anda di tampilan jenis perubahan Jelajahi). Buka area konfigurasi tambahan untuk menambahkan informasi tentang RFC.

   Di area konfigurasi Eksekusi, gunakan daftar drop-down yang tersedia atau masukkan nilai untuk parameter yang diperlukan. Untuk mengkonfigurasi parameter eksekusi opsional, buka area konfigurasi tambahan.
4. Setelah selesai, klik Jalankan. Jika tidak ada kesalahan, halaman RFC berhasil dibuat ditampilkan dengan detail RFC yang dikirimkan, dan output Run awal.
5. Buka area parameter Jalankan untuk melihat konfigurasi yang Anda kirimkan. Segarkan halaman untuk memperbarui status eksekusi RFC. Secara opsional, batalkan RFC atau buat salinannya dengan opsi di bagian atas halaman.

Meminta akses administrator dengan CLI

Cara kerjanya:

1. Gunakan Inline Create (Anda mengeluarkan `create-rfc` perintah dengan semua RFC dan parameter eksekusi disertakan), atau Template Create (Anda membuat dua file JSON, satu untuk parameter RFC dan satu untuk parameter eksekusi) dan mengeluarkan `create-rfc` perintah dengan dua file sebagai input. Kedua metode tersebut dijelaskan di sini.
2. Kirim `aws amscm submit-rfc --rfc-id` *`ID`* perintah RFC: dengan ID RFC yang dikembalikan.

   Pantau `aws amscm get-rfc --rfc-id` *`ID`* perintah RFC:.

Untuk memeriksa versi jenis perubahan, gunakan perintah ini:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Anda dapat menggunakan `CreateRfc` parameter apa pun dengan RFC apa pun apakah itu bagian dari skema untuk jenis perubahan atau tidak. Misalnya, untuk mendapatkan pemberitahuan ketika status RFC berubah, tambahkan baris ini, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` ke bagian parameter RFC dari permintaan (bukan parameter eksekusi). Untuk daftar semua CreateRfc parameter, lihat Referensi AMS Change Management API.

BUAT SEBARIS:

Keluarkan perintah create RFC dengan parameter eksekusi yang disediakan sebaris (tanda kutip escape saat memberikan parameter eksekusi sebaris), lalu kirimkan ID RFC yang dikembalikan. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```
aws --profile saml amscm create-rfc --change-type-id "ct-1dmlg9g1l91h6" --change-type-
version "3.0" --title "Stack-Admin-Access-QC" --execution-parameters "{\"DomainFQDN
\":\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

TEMPLATE MEMBUAT:

1. Output parameter eksekusi skema JSON untuk jenis perubahan ini ke file; contoh ini menamainya GrantAdminAccessParams .json:

```
aws amscm get-change-type-version --change-type-id "ct-1dmlg9g1l91h6"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 GrantAdminAccessParams.json
```

   Ubah dan simpan GrantAdminAccessParams file. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```
{
"DomainFQDN":           "mycorpdomain.acme.com",
"StackIds":             [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Username":             ["USERNAME", "USERNAME"],
"VpcId":                "VPC_ID"
}
```

   Perhatikan bahwa `TimeRequestedInHours` opsi default menjadi satu jam. Anda dapat meminta hingga dua belas jam.

2. Keluarkan template RFC ke file di folder Anda saat ini; contoh ini menamainya GrantAdminAccessRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > GrantAdminAccessRfc.json
```

3. Ubah dan simpan GrantAdminAccessRfc file.json. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```
{
"ChangeTypeId":         "ct-1dmlg9g1l91h6",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-Admin-Access-to-EC2-RFC"
}
```

4. Buat RFC, tentukan GrantAdminAccessRfc file dan file: GrantAdminAcessParams

```
aws amscm create-rfc --cli-input-json file://GrantAdminAccessRfc.json --execution-
parameters file://GrantAdminAccessParams.json
```

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

Untuk masuk ke instance melalui benteng, ikuti prosedur berikutnya, contoh akses Instance.

Kiat

> **Note**
>
> Anda dapat mengirimkan pembaruan ke permintaan akses Anda sebelum kedaluwarsa. Untuk selengkapnya, lihat Stack Admin Access | Update.
> Untuk masuk ke instance yang merupakan bagian dari ASG, Anda meminta akses ke tumpukan ASG, yang memberi Anda akses ke semua instance terkait.

Untuk contoh tentang meminta ReadOnly akses, lihat ReadOnly akses: meminta.

Minta ReadOnly akses

Meminta ReadOnly akses dengan konsol

Berikut ini menunjukkan jenis perubahan ini di konsol AMS.

Cara kerjanya:

1. Arahkan ke halaman Buat RFC: Di panel navigasi kiri konsol AMS klik RFCsuntuk membuka halaman RFCs daftar, lalu klik Buat RFC.
2. Pilih jenis perubahan populer (CT) di tampilan default Jelajahi jenis perubahan, atau pilih CT dalam tampilan Pilih menurut kategori.
   - Jelajahi berdasarkan jenis perubahan: Anda dapat mengklik CT populer di area Buat cepat untuk segera membuka halaman Jalankan RFC. Perhatikan bahwa Anda tidak dapat memilih versi CT yang lebih lama dengan pembuatan cepat.

Untuk mengurutkan CTs, gunakan area Semua jenis perubahan dalam tampilan Kartu atau Tabel. Di kedua tampilan, pilih CT dan kemudian klik Buat RFC untuk membuka halaman Jalankan RFC. Jika berlaku, opsi Buat dengan versi yang lebih lama muncul di sebelah tombol Buat RFC.

- Pilih berdasarkan kategori: Pilih kategori, subkategori, item, dan operasi dan kotak detail CT terbuka dengan opsi untuk Membuat dengan versi yang lebih lama jika berlaku. Klik Buat RFC untuk membuka halaman Jalankan RFC.

3. Pada halaman Run RFC, buka area nama CT untuk melihat kotak detail CT. Subjek diperlukan (ini diisi untuk Anda jika Anda memilih CT Anda di tampilan jenis perubahan Jelajahi). Buka area konfigurasi tambahan untuk menambahkan informasi tentang RFC.

   Di area konfigurasi Eksekusi, gunakan daftar drop-down yang tersedia atau masukkan nilai untuk parameter yang diperlukan. Untuk mengkonfigurasi parameter eksekusi opsional, buka area konfigurasi tambahan.

4. Setelah selesai, klik Jalankan. Jika tidak ada kesalahan, halaman RFC berhasil dibuat ditampilkan dengan detail RFC yang dikirimkan, dan output Run awal.

5. Buka area parameter Jalankan untuk melihat konfigurasi yang Anda kirimkan. Segarkan halaman untuk memperbarui status eksekusi RFC. Secara opsional, batalkan RFC atau buat salinannya dengan opsi di bagian atas halaman.

Meminta ReadOnly akses dengan CLI

Cara kerjanya:

1. Gunakan Inline Create (Anda mengeluarkan `create-rfc` perintah dengan semua RFC dan parameter eksekusi disertakan), atau Template Create (Anda membuat dua file JSON, satu untuk parameter RFC dan satu untuk parameter eksekusi) dan mengeluarkan `create-rfc` perintah dengan dua file sebagai input. Kedua metode tersebut dijelaskan di sini.

2. Kirim `aws amscm submit-rfc --rfc-id` *`ID`* perintah RFC: dengan ID RFC yang dikembalikan.

   Pantau `aws amscm get-rfc --rfc-id` *`ID`* perintah RFC:.

Untuk memeriksa versi jenis perubahan, gunakan perintah ini:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Anda dapat menggunakan `CreateRfc` parameter apa pun dengan RFC apa pun apakah itu bagian dari skema untuk jenis perubahan atau tidak. Misalnya, untuk mendapatkan pemberitahuan ketika status RFC berubah, tambahkan baris ini, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` ke bagian parameter RFC dari permintaan (bukan parameter eksekusi). Untuk daftar semua CreateRfc parameter, lihat Referensi AMS Change Management API.

BUAT SEBARIS:

Keluarkan perintah create RFC dengan parameter eksekusi yang disediakan sebaris (tanda kutip saat memberikan parameter eksekusi sebaris), lalu kirimkan ID RFC yang dikembalikan. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```
aws --profile saml amscm create-rfc --change-type-id "ct-199h35t7uz6jl" --change-type-
version "3.0" --title "Stack-RO-Access-QC" --execution-parameters "{\"DomainFQDN\":
\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

TEMPLATE MEMBUAT:

1. Output parameter eksekusi skema JSON untuk jenis perubahan ini ke file; contoh ini menamainya GrantReadOnlyAccessParams .json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-199h35t7uz6jl"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantReadOnlyAccessParams.json
   ```

   Ubah dan simpan GrantReadOnlyAccessParams file. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

   ```
   {
   "DomainFQDN":           "mycorpdomain.acme.com",
   ```

```
"StackIds":              [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Usernames":              ["USERNAME", "USERNAME"],
"VpcId":                 "VPC_ID"
}
```

Perhatikan bahwa `TimeRequestedInHours` opsi default menjadi satu jam. Anda dapat meminta hingga dua belas jam.

2. Keluarkan template RFC ke file di folder Anda saat ini; contoh ini menamainya GrantReadOnlyAccessRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > GrantReadOnlyAccessRfc.json
```

3. Ubah dan simpan GrantReadOnlyAccessRfc file.json. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```
{
"ChangeTypeId":          "ct-199h35t7uz6jl",
"ChangeTypeVersion":     "3.0",
"Title":                 "Request-ReadOnly-Access-to-EC2-RFC"
}
```

4. Buat RFC, tentukan GrantReadOnlyAccessRfc file dan file: GrantReadOnlyAcessParams

```
aws amscm create-rfc --cli-input-json file://GrantReadOnlyAccessRfc.json --
execution-parameters file://GrantReadOnlyAccessParams.json
```

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

Untuk masuk ke instance melalui benteng, ikuti prosedur berikutnya, contoh akses Instance.

Kiat

> **Note**
>
> Anda dapat mengirimkan pembaruan ke permintaan akses Anda sebelum kedaluwarsa. Untuk detailnya, lihat Stack Read-Only Access | Update.

Untuk masuk ke instance yang merupakan bagian dari grup EC2 Auto Scaling (ASG), Anda meminta akses ke tumpukan ASG, yang memberi Anda akses ke semua instance terkait.

Untuk panduan tentang meminta akses Admin, lihat Akses Admin: meminta.

Lainnya | RFC lainnya, membuat (CLI)

Contoh ini menunjukkan cara meminta perubahan yang tidak ada CTs alamat yang tersedia, dengan menggunakan Manajemen | Lainnya | Lainnya | Buat CT (ct-1e1xtak34nx76).

Gunakan CT ini ketika Anda tidak dapat menemukan jenis perubahan untuk apa yang Anda inginkan; Namun, jika Anda tidak yakin tentang menentukan parameter dalam CT yang ada, lebih baik untuk mengirimkan permintaan layanan untuk bantuan. Untuk informasi tentang mengirimkan permintaan layanan, lihat Contoh Permintaan Layanan.

Jenis RFC ini diperlukan Persetujuan, artinya memerlukan persetujuan AMS sebelum dapat diimplementasikan. Setelah mengirimkan RFC, operator AMS akan menghubungi Anda untuk mendiskusikan tumpukan yang ingin Anda terapkan.

> **Note**
>
> Saat menggunakan “review required” CTs, AMS merekomendasikan agar Anda menggunakan opsi Penjadwalan ASAP (pilih ASAP di konsol, biarkan waktu mulai dan berakhir kosong di API/CLI) karena ini CTs memerlukan operator AMS untuk memeriksa RFC, dan mungkin berkomunikasi dengan Anda sebelum dapat disetujui dan dijalankan. Jika Anda menjadwalkan ini RFCs, pastikan untuk mengizinkan setidaknya 24 jam. Jika persetujuan tidak terjadi sebelum waktu mulai yang dijadwalkan, RFC ditolak secara otomatis.

DATA YANG DIBUTUHKAN:

- `Comment`: Untuk apa RFC itu.
- `ChangeTypeIddanChangeTypeVersion`: Gunakan Other | Create (`ct-1e1xtak34nx76`) untuk meminta sumber daya baru, gunakan Other | Update (`ct-0xdawir96cy7k`) untuk mengubah sumber daya yang ada; keduanya`v1`.

DATA OPSIONAL:`Priority`: Nilai yang dapat diterima adalah `High`Medium,, atau`Low`.

BUAT SEBARIS:

- Keluarkan perintah buat RFC dengan parameter eksekusi yang disediakan sebaris (tanda kutip saat memberikan parameter eksekusi sebaris). Contoh menggunakan Lainnya | Buat.

```
aws amscm create-rfc --change-type-id "ct-1e1xtak34nx76" --change-type-version "1.0"
 --title "TITLE" --execution-parameters "{\"Comment\": \"What you want created\"}"
```

- Kirim RFC menggunakan ID RFC yang dikembalikan dalam operasi create RFC. Sampai diserahkan, RFC tetap di `Editing` negara bagian dan tidak ditindaklanjuti.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- Pantau status RFC dan lihat output eksekusi:

```
aws amscm get-rfc --rfc-id RFC_ID
```

TEMPLATE MEMBUAT:

1. Buat dan simpan file JSON untuk parameter eksekusi; contoh menamainya OtherParams .json dan menyertakan parameter opsional: `Priority`

```
{
"Comment":          "What you want created",
"Priority":         "Medium"
}
```

2. Buat dan simpan file JSON untuk parameter RFC; contoh menamainya OtherRfc .json.

```
{
"ChangeTypeId":         "ct-1e1xtak34nx76",
"ChangeTypeVersion":    "1.0",
"Title":                "TITLE"
}
```

3. Buat RFC, tentukan OtherRfc file dan file: OtherParams

```
aws amscm create-rfc --cli-input-json file://OtherRfc.json  --execution-parameters
 file://OtherParams.json
```

Anda menerima RFC baru sebagai tanggapan. RfcId Misalnya:

```
{
"RfcId": "RFC-ID"
}
```

4. Kirim RFC:

```
aws amscm submit-rfc --rfc-id RFC-ID
```

Jika tidak ada kesalahan yang dilaporkan, operasi berhasil.

5. Untuk memantau status permintaan dan untuk melihat Output Eksekusi:

```
aws amscm get-rfc --rfc-id RFC-ID
```

Tumpukan apa pun: menghapus, me-reboot, memulai, menghentikan

Anda dapat menggunakan konsol AMS atau API/CLI untuk menghapus, reboot, memulai, atau menghentikan, tumpukan AMS.

Hapus tumpukan

Menghapus Stack dengan Konsol

Tangkapan layar dari jenis perubahan ini di konsol AMS:

Cara kerjanya:

1. Arahkan ke halaman Buat RFC: Di panel navigasi kiri konsol AMS klik RFCsuntuk membuka halaman RFCs daftar, lalu klik Buat RFC.
2. Pilih jenis perubahan populer (CT) dalam tampilan default Jelajahi jenis perubahan, atau pilih CT dalam tampilan Pilih menurut kategori.

- Jelajahi berdasarkan jenis perubahan: Anda dapat mengklik CT populer di area Buat cepat untuk segera membuka halaman Jalankan RFC. Perhatikan bahwa Anda tidak dapat memilih versi CT yang lebih lama dengan pembuatan cepat.

  Untuk mengurutkan CTs, gunakan area Semua jenis perubahan dalam tampilan Kartu atau Tabel. Di kedua tampilan, pilih CT dan kemudian klik Buat RFC untuk membuka halaman Jalankan RFC. Jika berlaku, opsi Buat dengan versi yang lebih lama muncul di sebelah tombol Buat RFC.
- Pilih berdasarkan kategori: Pilih kategori, subkategori, item, dan operasi dan kotak detail CT terbuka dengan opsi untuk Membuat dengan versi yang lebih lama jika berlaku. Klik Buat RFC untuk membuka halaman Jalankan RFC.

3. Pada halaman Run RFC, buka area nama CT untuk melihat kotak detail CT. Subjek diperlukan (ini diisi untuk Anda jika Anda memilih CT Anda di tampilan jenis perubahan Jelajahi). Buka area konfigurasi tambahan untuk menambahkan informasi tentang RFC.

   Di area konfigurasi Eksekusi, gunakan daftar drop-down yang tersedia atau masukkan nilai untuk parameter yang diperlukan. Untuk mengkonfigurasi parameter eksekusi opsional, buka area konfigurasi tambahan.
4. Setelah selesai, klik Jalankan. Jika tidak ada kesalahan, halaman RFC berhasil dibuat ditampilkan dengan detail RFC yang dikirimkan, dan output Run awal.
5. Buka area parameter Jalankan untuk melihat konfigurasi yang Anda kirimkan. Segarkan halaman untuk memperbarui status eksekusi RFC. Secara opsional, batalkan RFC atau buat salinannya dengan opsi di bagian atas halaman.

Menghapus Stack dengan CLI

Cara kerjanya:

1. Gunakan Inline Create (Anda mengeluarkan `create-rfc` perintah dengan semua RFC dan parameter eksekusi disertakan), atau Template Create (Anda membuat dua file JSON, satu untuk parameter RFC dan satu untuk parameter eksekusi) dan mengeluarkan `create-rfc` perintah dengan dua file sebagai input. Kedua metode dijelaskan di sini.
2. Kirim `aws amscm submit-rfc --rfc-id` *`ID`* perintah RFC: dengan ID RFC yang dikembalikan.

   Pantau `aws amscm get-rfc --rfc-id` *`ID`* perintah RFC:.

Untuk memeriksa versi jenis perubahan, gunakan perintah ini:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Anda dapat menggunakan `CreateRfc` parameter apa pun dengan RFC apa pun apakah itu bagian dari skema untuk jenis perubahan atau tidak. Misalnya, untuk mendapatkan pemberitahuan ketika status RFC berubah, tambahkan baris ini, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` ke bagian parameter RFC dari permintaan (bukan parameter eksekusi). Untuk daftar semua CreateRfc parameter, lihat Referensi AMS Change Management API.

BUAT SEBARIS:

Keluarkan perintah create RFC dengan parameter eksekusi yang disediakan sebaris (tanda kutip escape saat memberikan parameter eksekusi sebaris), lalu kirimkan ID RFC yang dikembalikan. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0" --
title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

TEMPLATE MEMBUAT:

1. Keluarkan template RFC ke file di folder Anda saat ini; contoh ini menamainya DeleteStackRfc .json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. Ubah dan simpan DeleteStackRfc file.json.

   Tanda kutip internal dalam ekstensi ExecutionParameters JSON harus diloloskan dengan garis miring terbalik (\). Contoh tanpa waktu mulai dan berakhir:

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   ```

```
"ExecutionParameters":  "{
        \"StackId\":\"STACK_ID\"}"
}
```

3. Buat RFC:

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
```

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

Kiat

> **Note**
>
> Jika menghapus ember S3, itu harus dikosongkan dari objek terlebih dahulu.

> **Important**
>
> Menghapus tumpukan dapat memiliki konsekuensi yang tidak diinginkan dan tidak terduga. Untuk peringatan penting, lihat bagian RFCs Pemecahan Masalah RFC untuk Hapus Tumpukan.

Reboot tumpukan

Mem-boot ulang Stack dengan Konsol

Tangkapan layar dari jenis perubahan ini di konsol AMS:

Cara kerjanya:

1. Arahkan ke halaman Buat RFC: Di panel navigasi kiri konsol AMS klik RFCsuntuk membuka halaman RFCs daftar, lalu klik Buat RFC.
2. Pilih jenis perubahan populer (CT) dalam tampilan default Jelajahi jenis perubahan, atau pilih CT dalam tampilan Pilih menurut kategori.

- Jelajahi berdasarkan jenis perubahan: Anda dapat mengklik CT populer di area Buat cepat untuk segera membuka halaman Jalankan RFC. Perhatikan bahwa Anda tidak dapat memilih versi CT yang lebih lama dengan pembuatan cepat.

  Untuk mengurutkan CTs, gunakan area Semua jenis perubahan dalam tampilan Kartu atau Tabel. Di kedua tampilan, pilih CT dan kemudian klik Buat RFC untuk membuka halaman Jalankan RFC. Jika berlaku, opsi Buat dengan versi yang lebih lama muncul di sebelah tombol Buat RFC.
- Pilih berdasarkan kategori: Pilih kategori, subkategori, item, dan operasi dan kotak detail CT terbuka dengan opsi untuk Membuat dengan versi yang lebih lama jika berlaku. Klik Buat RFC untuk membuka halaman Jalankan RFC.

3. Pada halaman Run RFC, buka area nama CT untuk melihat kotak detail CT. Subjek diperlukan (ini diisi untuk Anda jika Anda memilih CT Anda di tampilan jenis perubahan Jelajahi). Buka area konfigurasi tambahan untuk menambahkan informasi tentang RFC.

   Di area konfigurasi Eksekusi, gunakan daftar drop-down yang tersedia atau masukkan nilai untuk parameter yang diperlukan. Untuk mengkonfigurasi parameter eksekusi opsional, buka area konfigurasi tambahan.
4. Setelah selesai, klik Jalankan. Jika tidak ada kesalahan, halaman RFC berhasil dibuat ditampilkan dengan detail RFC yang dikirimkan, dan output Run awal.
5. Buka area parameter Jalankan untuk melihat konfigurasi yang Anda kirimkan. Segarkan halaman untuk memperbarui status eksekusi RFC. Secara opsional, batalkan RFC atau buat salinannya dengan opsi di bagian atas halaman.

Mem-boot ulang Stack dengan CLI

Cara kerjanya:

1. Gunakan Inline Create (Anda mengeluarkan `create-rfc` perintah dengan semua RFC dan parameter eksekusi disertakan), atau Template Create (Anda membuat dua file JSON, satu untuk parameter RFC dan satu untuk parameter eksekusi) dan mengeluarkan `create-rfc` perintah dengan dua file sebagai input. Kedua metode dijelaskan di sini.
2. Kirim `aws amscm submit-rfc --rfc-id` *`ID`* perintah RFC: dengan ID RFC yang dikembalikan.

   Pantau `aws amscm get-rfc --rfc-id` *`ID`* perintah RFC:.

Untuk memeriksa versi jenis perubahan, gunakan perintah ini:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Anda dapat menggunakan `CreateRfc` parameter apa pun dengan RFC apa pun apakah itu bagian dari skema untuk jenis perubahan atau tidak. Misalnya, untuk mendapatkan pemberitahuan ketika status RFC berubah, tambahkan baris ini, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` ke bagian parameter RFC dari permintaan (bukan parameter eksekusi). Untuk daftar semua CreateRfc parameter, lihat Referensi AMS Change Management API.

BUAT SEBARIS:

Keluarkan perintah create RFC dengan parameter eksekusi yang disediakan sebaris (tanda kutip escape saat memberikan parameter eksekusi sebaris), lalu kirimkan ID RFC yang dikembalikan. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```
aws amscm create-rfc --change-type-id "ct-02u0hoaa9grat" --change-type-version "1.0" --
title "Reboot My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

TEMPLATE MEMBUAT:

1. Keluarkan template RFC ke file di folder Anda saat ini. Contoh ini menamainya RebootStackRfc .json. Perhatikan bahwa karena hanya ada satu parameter eksekusi untuk menghentikan (me-reboot, atau memulai) sebuah instance, parameter eksekusi dapat berada dalam file JSON skema itu sendiri dan tidak perlu membuat parameter eksekusi terpisah file JSON.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopInstanceRfc.json
   ```

2. Ubah dan simpan RebootStackRfc file.json.

   Tanda kutip internal dalam ekstensi `ExecutionParameters` JSON harus diloloskan dengan garis miring terbalik (\). Contoh:

```
{
"ChangeTypeId":         "ct-02u0hoaa9grat",
"Title":                "Reboot-My-EC2-RFC",
"TimeoutInMinutes":     60,
"ExecutionParameters":  "{
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. Buat RFC:

```
aws amscm create-rfc --cli-input-json file://RebootStackRfc.json
```

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

Kiat

Untuk informasi tentang Application Load Balancer, lihat Application Load Balancers.

Mulai tumpukan

Memulai Stack dengan Konsol

Tangkapan layar dari jenis perubahan ini di konsol AMS:

Cara kerjanya:

1. Arahkan ke halaman Buat RFC: Di panel navigasi kiri konsol AMS klik RFCsuntuk membuka halaman RFCs daftar, lalu klik Buat RFC.
2. Pilih jenis perubahan populer (CT) dalam tampilan default Jelajahi jenis perubahan, atau pilih CT dalam tampilan Pilih menurut kategori.
   - Jelajahi berdasarkan jenis perubahan: Anda dapat mengklik CT populer di area Buat cepat untuk segera membuka halaman Jalankan RFC. Perhatikan bahwa Anda tidak dapat memilih versi CT yang lebih lama dengan pembuatan cepat.

Untuk mengurutkan CTs, gunakan area Semua jenis perubahan dalam tampilan Kartu atau Tabel. Di kedua tampilan, pilih CT dan kemudian klik Buat RFC untuk membuka halaman Jalankan RFC. Jika berlaku, opsi Buat dengan versi yang lebih lama muncul di sebelah tombol Buat RFC.

- Pilih berdasarkan kategori: Pilih kategori, subkategori, item, dan operasi dan kotak detail CT terbuka dengan opsi untuk Membuat dengan versi yang lebih lama jika berlaku. Klik Buat RFC untuk membuka halaman Jalankan RFC.

3. Pada halaman Run RFC, buka area nama CT untuk melihat kotak detail CT. Subjek diperlukan (ini diisi untuk Anda jika Anda memilih CT Anda di tampilan jenis perubahan Jelajahi). Buka area konfigurasi tambahan untuk menambahkan informasi tentang RFC.

   Di area konfigurasi Eksekusi, gunakan daftar drop-down yang tersedia atau masukkan nilai untuk parameter yang diperlukan. Untuk mengkonfigurasi parameter eksekusi opsional, buka area konfigurasi tambahan.

4. Setelah selesai, klik Jalankan. Jika tidak ada kesalahan, halaman RFC berhasil dibuat ditampilkan dengan detail RFC yang dikirimkan, dan output Run awal.
5. Buka area parameter Jalankan untuk melihat konfigurasi yang Anda kirimkan. Segarkan halaman untuk memperbarui status eksekusi RFC. Secara opsional, batalkan RFC atau buat salinannya dengan opsi di bagian atas halaman.

Memulai Stack dengan CLI

Cara kerjanya:

1. Gunakan Inline Create (Anda mengeluarkan `create-rfc` perintah dengan semua RFC dan parameter eksekusi disertakan), atau Template Create (Anda membuat dua file JSON, satu untuk parameter RFC dan satu untuk parameter eksekusi) dan mengeluarkan `create-rfc` perintah dengan dua file sebagai input. Kedua metode dijelaskan di sini.
2. Kirim `aws amscm submit-rfc --rfc-id` *`ID`* perintah RFC: dengan ID RFC yang dikembalikan.

   Pantau `aws amscm get-rfc --rfc-id` *`ID`* perintah RFC:.

Untuk memeriksa versi jenis perubahan, gunakan perintah ini:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Anda dapat menggunakan `CreateRfc` parameter apa pun dengan RFC apa pun apakah itu bagian dari skema untuk jenis perubahan atau tidak. Misalnya, untuk mendapatkan pemberitahuan ketika status RFC berubah, tambahkan baris ini, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` ke bagian parameter RFC dari permintaan (bukan parameter eksekusi). Untuk daftar semua CreateRfc parameter, lihat Referensi AMS Change Management API.

BUAT SEBARIS:

Keluarkan perintah create RFC dengan parameter eksekusi yang disediakan sebaris (tanda kutip escape saat memberikan parameter eksekusi sebaris), lalu kirimkan ID RFC yang dikembalikan. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```
aws amscm create-rfc --change-type-id "ct-1h5xgl9cr4bzy" --change-type-version "1.0" --
title "Start My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

TEMPLATE MEMBUAT:

1. Keluarkan template RFC ke file di folder Anda saat ini. Contoh ini menamainya StartInstanceRfc .json. Perhatikan bahwa karena hanya ada satu parameter eksekusi untuk memulai tumpukan, parameter eksekusi dapat berada dalam file JSON skema itu sendiri dan tidak perlu membuat file JSON parameter eksekusi terpisah.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StartStackRfc.json
   ```

2. Ubah dan simpan StartStackRfc file.json. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

   ```
   {
   "ChangeTypeId":         "ct-1h5xgl9cr4bzy",
   "Title":                "Start-My-EC2-RFC",
   "TimeoutInMinutes":     60,
   ```

```
"ExecutionParameters":  "{
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. Buat RFC:

```
aws amscm create-rfc --cli-input-json file://StartStackRfc.json
```

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

Kiat

Untuk informasi tentang Application Load Balancer, lihat Application Load Balancers.

Hentikan tumpukan

Menghentikan Stack dengan Konsol

Tangkapan layar dari jenis perubahan ini di konsol AMS:

Cara kerjanya:

1. Arahkan ke halaman Buat RFC: Di panel navigasi kiri konsol AMS klik RFCsuntuk membuka halaman RFCs daftar, lalu klik Buat RFC.
2. Pilih jenis perubahan populer (CT) dalam tampilan default Jelajahi jenis perubahan, atau pilih CT dalam tampilan Pilih menurut kategori.
   - Jelajahi berdasarkan jenis perubahan: Anda dapat mengklik CT populer di area Buat cepat untuk segera membuka halaman Jalankan RFC. Perhatikan bahwa Anda tidak dapat memilih versi CT yang lebih lama dengan pembuatan cepat.

     Untuk mengurutkan CTs, gunakan area Semua jenis perubahan dalam tampilan Kartu atau Tabel. Di kedua tampilan, pilih CT dan kemudian klik Buat RFC untuk membuka halaman Jalankan RFC. Jika berlaku, opsi Buat dengan versi yang lebih lama muncul di sebelah tombol Buat RFC.

- Pilih berdasarkan kategori: Pilih kategori, subkategori, item, dan operasi dan kotak detail CT terbuka dengan opsi untuk Membuat dengan versi yang lebih lama jika berlaku. Klik Buat RFC untuk membuka halaman Jalankan RFC.

3. Pada halaman Run RFC, buka area nama CT untuk melihat kotak detail CT. Subjek diperlukan (ini diisi untuk Anda jika Anda memilih CT Anda di tampilan jenis perubahan Jelajahi). Buka area konfigurasi tambahan untuk menambahkan informasi tentang RFC.

   Di area konfigurasi Eksekusi, gunakan daftar drop-down yang tersedia atau masukkan nilai untuk parameter yang diperlukan. Untuk mengkonfigurasi parameter eksekusi opsional, buka area konfigurasi tambahan.

4. Setelah selesai, klik Jalankan. Jika tidak ada kesalahan, halaman RFC berhasil dibuat ditampilkan dengan detail RFC yang dikirimkan, dan output Run awal.

5. Buka area parameter Jalankan untuk melihat konfigurasi yang Anda kirimkan. Segarkan halaman untuk memperbarui status eksekusi RFC. Secara opsional, batalkan RFC atau buat salinannya dengan opsi di bagian atas halaman.

Menghentikan Stack dengan CLI

Cara kerjanya:

1. Gunakan Inline Create (Anda mengeluarkan `create-rfc` perintah dengan semua RFC dan parameter eksekusi disertakan), atau Template Create (Anda membuat dua file JSON, satu untuk parameter RFC dan satu untuk parameter eksekusi) dan mengeluarkan `create-rfc` perintah dengan dua file sebagai input. Kedua metode dijelaskan di sini.

2. Kirim `aws amscm submit-rfc --rfc-id` *`ID`* perintah RFC: dengan ID RFC yang dikembalikan.

   Pantau `aws amscm get-rfc --rfc-id` *`ID`* perintah RFC:.

Untuk memeriksa versi jenis perubahan, gunakan perintah ini:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Anda dapat menggunakan `CreateRfc` parameter apa pun dengan RFC apa pun apakah itu bagian dari skema untuk jenis perubahan atau tidak. Misalnya, untuk mendapatkan pemberitahuan ketika status RFC berubah, tambahkan baris ini, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` ke bagian parameter RFC dari permintaan (bukan parameter eksekusi). Untuk daftar semua CreateRfc parameter, lihat Referensi AMS Change Management API.

BUAT SEBARIS:

Keluarkan perintah create RFC dengan parameter eksekusi yang disediakan sebaris (tanda kutip escape saat memberikan parameter eksekusi sebaris), lalu kirimkan ID RFC yang dikembalikan. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

```
aws amscm create-rfc --change-type-id "ct-3dgbnh6gpst4d" --change-type-version "1.0" --
title "Stop My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

TEMPLATE MEMBUAT:

1. Keluarkan template RFC ke file di folder Anda saat ini. Contoh ini menamainya StopStackRfc .json. Perhatikan bahwa karena hanya ada satu parameter eksekusi untuk menghentikan (me-reboot, atau memulai) sebuah instance, parameter eksekusi dapat berada dalam file JSON skema itu sendiri dan tidak perlu membuat parameter eksekusi terpisah file JSON.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopStackRfc.json
   ```

2. Ubah dan simpan StopStackRfc file.json. Misalnya, Anda dapat mengganti konten dengan sesuatu seperti ini:

   ```
   {
   "ChangeTypeId":          "ct-3dgbnh6gpst4d",
   "Title":                 "Stop-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
       }"
   ```

```
}
```

3. Buat RFC:

```
aws amscm create-rfc --cli-input-json file://StopInstanceRfc.json
```

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

Kiat

Instans yang dihentikan tetap dihentikan kecuali Anda telah menjadwalkan restart menggunakan Penjadwal Sumber Daya AMS.

Jika diperlukan, lihat EC2 instance stack stop gagal.

Contoh akses

Contoh-contoh ini menunjukkan cara masuk ke instance melalui benteng setelah Anda diberikan akses melalui RFC. Untuk detail tentang mendapatkan akses yang diberikan, lihat Permintaan akses.

> **Note**
>
> Sebuah EC2 instance yang dibuat melalui grup Auto Scaling akan memiliki alamat IP yang berputar masuk dan keluar dan Anda harus menggunakan EC2 konsol Anda untuk menemukan alamat IP tersebut.

Data yang dibutuhkan:

- Nama atau alamat IP ramah DNS Bastion: Gunakan nama ramah DNS seperti yang dijelaskan dalam Nama benteng ramah DNS atau temukan alamat IP benteng seperti yang dijelaskan dalam. Menemukan alamat IP benteng
- Nama pengguna (misalnya username@customerdomain.com) dan Kata Sandi: Kredensial untuk akun.
- Alamat IP Stack: Dapatkan ini dengan melihat halaman AMS console Stacks untuk tumpukan yang ingin Anda masuki dan kemudian memfilter ID tumpukan itu di EC2 konsol untuk akun Anda.

Untuk satu EC2 instance, Anda juga dapat menggunakan perintah AMS SKMS Untuk referensi AMS SKMS API, lihat tab Laporan di AWS Artifact Console. untuk menemukan ID tumpukan dan kemudian Untuk referensi AMS SKMS API, lihat tab Laporan di AWS Artifact Console. untuk menemukan alamat IP stack.

Akses alamat IP bastion, baik SSH atau RDP, yang sesuai, dan masuk menggunakan salah satu prosedur berikut.

Komputer Linux ke Linux misalnya

Gunakan SSH untuk terhubung ke bastion SSH dan kemudian ke instance Linux.

MALZ

Untuk informasi selengkapnya tentang nama benteng ramah, lihat Benteng DNS.

Untuk terhubung ke instance Linux, Anda harus terlebih dahulu terhubung ke bastion SSH.

1. Buka jendela shell dan masukkan:

```
ssh Domain_FQDN\\Username@SSH_bastion_name
    or SSH_bastion_IP
```

Yang akan terlihat seperti ini jika domain_FQDN Anda adalah “corp.domain.com”, nomor akun Anda adalah “123456789123", Your_Domain adalah “amazonaws.com”, Anda memilih benteng “4", dan nama pengguna Anda adalah" “: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. Masuk dengan kredensyal Active Directory perusahaan Anda.
3. Ketika disajikan dengan prompt Bash, SSH masuk ke instance, dan kemudian masukkan:

```
ssh Domain_FQDN\\Username@Instance_IP
```

Atau, Anda dapat menggunakan bendera Login (-l):

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

Untuk informasi selengkapnya tentang nama benteng ramah, lihat Benteng DNS.

Untuk terhubung ke instance Linux, Anda harus terlebih dahulu terhubung ke bastion SSH.

1. Buka jendela shell dan masukkan:

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name
    or SSH_BASTION_IP
```

Yang akan terlihat seperti ini jika nomor akun Anda adalah 123456789123, Anda memilih bastion 4, dan nama pengguna Anda adalah: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. Masuk dengan kredensyal Active Directory perusahaan Anda.
3. Ketika disajikan dengan prompt Bash, SSH masuk ke instance, dan kemudian masukkan:

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Atau, Anda dapat menggunakan bendera Login (-l):

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Komputer Linux ke instans Windows

Gunakan terowongan SSH dan klien RDP untuk terhubung ke instance Windows dari komputer Linux Anda.

MALZ

Prosedur ini memerlukan klien Remote Desktop Connection untuk Linux; contohnya menggunakan Microsoft Remote Desktop (klien UNIX open source untuk menghubungkan ke Windows Remote Desktop Services). Rdesktop adalah alternatif.

> **Note**
>
> Cara Anda masuk ke instance Windows mungkin berubah berdasarkan klien desktop jarak jauh yang digunakan.

Pertama Anda membuat terowongan SSH, dan kemudian masuk.

Untuk informasi lebih lanjut tentang nama benteng ramah, lihatNama benteng ramah DNS.

Sebelum Anda memulai:

- Meminta akses ke instans yang ingin Anda sambungkan; untuk informasi, lihat Permintaan akses.
- Pilih nama bastion SSH DNS yang ramah untuk dihubungkan; misalnya:

  ```
  sshbastion(1-4).Your_Domain
  ```

  Yang akan terlihat seperti ini jika domain_fqdn Anda adalah “corp.domain.com”, Your_Domain yang dikelola AMS Anda adalah “amazonaws.com”, Anda memilih benteng “4", dan nama pengguna Anda adalah" “: JoeSmith

  ```
  ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
  ```
- Temukan alamat IP dari instans yang ingin Anda sambungkan; untuk informasi, lihat Menemukan ID instans atau alamat IP.

1. Siapkan RDP melalui terowongan SSH dari desktop Linux ke instance Windows. Untuk mengeluarkan `ssh` perintah dengan nilai yang tepat, ada beberapa cara untuk melanjutkan:

   - Di shell Linux, atur variabel, lalu masukkan perintah koneksi SSH:

     ```
     BASTION="sshbastion(1-4).Your_Domain""
     WINDOWS="Windows_Instance_Private_IP"
     AD="AD_Account_Number"
     USER="AD_Username"
     ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
     ```

     Contoh, jika nilai berikut digunakan:

```
BASTION="sshbastion4.A123456789123.amazonaws.com"

WINDOWS="172.16.3.254"

AD="ACORP_example"

USER="john.doe"
```

- Tambahkan nilai variabel langsung ke `ssh` perintah.

Dalam kedua kasus, inilah permintaan yang dirender (dengan asumsi kumpulan nilai variabel yang sama):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
```

2. Entah: Buka Klien Desktop Jarak Jauh Anda, masukkan alamat dan port loopback, 127.0.0.1:3389, lalu buka koneksi.

   Atau, masuk ke instance Windows dari shell desktop Linux baru. Jika Anda menggunakan RDesktop, perintahnya terlihat seperti ini:

   ```
   rdesktop 127.0.0.1:3389
   ```

   Jendela desktop jarak jauh untuk instance Windows muncul di desktop Linux Anda.

   Tip

   Jika sesi desktop jarak jauh gagal dimulai, verifikasi bahwa konektivitas jaringan ke instance Windows dari bastion SSH diizinkan pada port 3389 dari shell pada langkah 1 (ganti dengan tepat): `private_ip_address_of_windows_instance`

   ```
   nc private_ip_address_of_windows_instance 3389 -v -z
   ```

   Sukses:

   ```
   nc 172.16.0.83 3389 -v -z
           Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
           netstat -anvp | grep 3389
   ```

```
tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

SALZ

Prosedur untuk landing zone akun tunggal ini memerlukan klien Remote Desktop Connection untuk Linux; contohnya menggunakan Microsoft Remote Desktop (klien UNIX open source untuk menghubungkan ke Windows Remote Desktop Services). Rdesktop adalah alternatif.

> **Note**
>
> Cara Anda masuk ke instance Windows mungkin berubah berdasarkan klien desktop jarak jauh yang digunakan.

Pertama Anda membuat terowongan SSH, dan kemudian masuk.

Untuk informasi lebih lanjut tentang nama benteng ramah, lihatNama benteng ramah DNS.

Sebelum Anda memulai:

- Meminta akses ke instans yang ingin Anda sambungkan; untuk informasi, lihat Permintaan akses.
- Pilih nama bastion SSH DNS yang ramah untuk dihubungkan; misalnya:

  ```
  sshbastion(1-4).AAMSAccountNumber.amazonaws.com
  ```

  Yang akan terlihat seperti ini jika nomor akun Anda 123456789123 dan Anda memilih benteng 4:

  ```
  sshbastion4.A123456789123.amazonaws.com
  ```

- Temukan alamat IP dari instans yang ingin Anda sambungkan; untuk informasi, lihat Menemukan ID instans atau alamat IP.

1. Siapkan RDP melalui terowongan SSH dari desktop Linux ke instance Windows. Untuk mengeluarkan `ssh` perintah dengan nilai yang tepat, ada beberapa cara untuk melanjutkan:

   - Di shell Linux, atur variabel, lalu masukkan perintah koneksi SSH:

```
BASTION="sshbastion(1-4).AAMSAccountNumber.amazonaws.com"
WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"
AD="AD_ACCOUNT_NUMBER"
USER="AD_USERNAME"
ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
```

Contoh, jika nilai berikut digunakan:

```
BASTION="sshbastion4.A123456789123.amazonaws.com"

WINDOWS="172.16.3.254"

AD="ACORP_example"

USER="john.doe"
```

- Tambahkan nilai variabel langsung ke `ssh` perintah.

Dalam kedua kasus, inilah permintaan yang dirender (dengan asumsi kumpulan nilai variabel yang sama):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. Entah: Buka Klien Desktop Jarak Jauh Anda, masukkan alamat dan port loopback, 127.0.0.1:3389, lalu buka koneksi.

   Atau, masuk ke instance Windows dari shell desktop Linux baru. Jika Anda menggunakan RDesktop, perintahnya terlihat seperti ini:

   ```
   rdesktop 127.0.0.1:3389
   ```

   Jendela desktop jarak jauh untuk instance Windows muncul di desktop Linux Anda.

   > **Tip**
   >
   > Jika sesi desktop jarak jauh gagal dimulai, verifikasi bahwa konektivitas jaringan ke instance Windows dari bastion SSH diizinkan pada port 3389 dari shell pada langkah 1 (ganti dengan tepat): `private_ip_address_of_windows_instance`

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

Sukses:

```
nc 172.16.0.83 3389 -v -z
        Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
        netstat -anvp | grep 3389
        tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

Komputer Windows ke instans Windows

Gunakan klien Windows Remote Desktop Connection untuk terhubung ke instance Windows dari komputer Windows Anda.

MALZ

Untuk informasi lebih lanjut tentang nama benteng ramah, lihatNama benteng ramah DNS.

1. Buka program Remote Desktop Connection, program Windows standar, dan masukkan nama DNS ramah dari benteng Windows di bidang hostname.

2. Pilih Hubungkan. Remote Desktop Connection mencoba koneksi RDP ke benteng.

   Jika berhasil, kotak dialog kredensial terbuka. Untuk mendapatkan akses, gunakan kredenal Active Directory perusahaan Anda, seperti yang Anda lakukan dengan instance Windows.

3. Buka program Remote Desktop Connection di bastion dan masukkan alamat IP instance Windows yang ingin Anda sambungkan (misalnya, 10.0.0.100), lalu pilih Connect. Kredensi Active Directory perusahaan Anda diperlukan lagi sebelum Anda terhubung ke instans Windows.

SALZ

Untuk informasi lebih lanjut tentang nama benteng ramah, lihatNama benteng ramah DNS.

1. Buka program Remote Desktop Connection, program Windows standar, dan masukkan nama DNS ramah dari benteng Windows di bidang nama host; misalnya`rdpbastion(1-4).AAMSAccountNumber.amazonaws.com`, yang akan terlihat seperti ini jika nomor akun Anda 123456789123 dan Anda memilih bastion 4,. `rdpbastion4.A123456789123.amazonaws.com`

2. Pilih Hubungkan. Remote Desktop Connection mencoba koneksi RDP ke benteng.

   Jika berhasil, kotak dialog kredensial terbuka. Untuk mendapatkan akses, gunakan kredenal Active Directory perusahaan Anda, seperti yang Anda lakukan dengan instance Windows.

3. Buka program Remote Desktop Connection di bastion dan masukkan alamat IP instance Windows yang ingin Anda sambungkan (misalnya, 10.0.0.100), lalu pilih Connect. Kredensi Active Directory perusahaan Anda diperlukan lagi sebelum Anda terhubung ke instans Windows.

Komputer Windows ke Linux misalnya

Untuk RDP ke benteng SSH dari lingkungan Windows, ikuti langkah-langkah ini.

MALZ

Sebelum Anda memulai:

- Meminta akses ke instans yang ingin Anda sambungkan; untuk informasi, lihat Permintaan akses.
- Pilih nama bastion SSH DNS yang ramah untuk dihubungkan; misalnya:

  ```
  sshbastion(1-4).YOUR_DOMAIN
  ```

  Yang akan terlihat seperti ini jika YOUR_DOMAIN adalah myamsaddomain.com” dan Anda memilih benteng 4:

  ```
  sshbastion4.myamsaddomain.com
  ```

- Temukan alamat IP dari instans yang ingin Anda sambungkan; untuk informasi, lihat Menemukan ID instans atau alamat IP.

Untuk terhubung ke instance Linux dari mesin Windows Anda, Anda harus terlebih dahulu terhubung ke bastion SSH.

Gunakan klien OpenSSH Windows asli atau instal Putty di mesin lokal Anda. Untuk mempelajari lebih lanjut tentang OpenSSH, lihat OpenSSH di Windows.

1. Gunakan Windows asli atau buka PuTTY dan masukkan nama host bastion SSH atau alamat IP bastion SSH. Misalnya, 10.65.2.214 (22 adalah port yang digunakan untuk SSH; itu akan diatur secara default).
2. OpenSSH atau Putty mencoba koneksi SSH ke benteng dan membuka jendela shell.
3. Gunakan kredenal Active Directory perusahaan Anda seperti yang Anda lakukan dengan host RDP untuk mendapatkan akses.
4. Saat disajikan dengan prompt Bash, SSH ke dalam instance. Masukkan:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

Sebelum Anda memulai:

- Meminta akses ke instans yang ingin Anda sambungkan; untuk informasi, lihat Permintaan akses.
- Pilih nama bastion SSH DNS yang ramah untuk dihubungkan; misalnya:

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

Yang akan terlihat seperti ini jika nomor akun Anda 123456789123 dan Anda memilih benteng 4:

```
sshbastion4.A123456789123.amazonaws.com
```

- Temukan alamat IP dari instans yang ingin Anda sambungkan; untuk informasi, lihat Menemukan ID instans atau alamat IP.

Untuk terhubung ke instance Linux dari mesin Windows Anda, Anda harus terlebih dahulu terhubung ke bastion SSH.

Gunakan klien OpenSSH Windows asli atau instal Putty di mesin lokal Anda. Untuk mempelajari lebih lanjut tentang OpenSSH, lihat OpenSSH di Windows.

1. Gunakan Windows asli atau buka PuTTY dan masukkan nama host bastion SSH atau alamat IP bastion SSH. Misalnya, 10.65.2.214 (22 adalah port yang digunakan untuk SSH; itu akan diatur secara default).
2. OpenSSH atau Putty mencoba koneksi SSH ke benteng dan membuka jendela shell.
3. Gunakan kredenal Active Directory perusahaan Anda seperti yang Anda lakukan dengan host RDP untuk mendapatkan akses.
4. Saat disajikan dengan prompt Bash, SSH ke dalam instance. Masukkan:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

Melaporkan insiden

Gunakan konsol AMS untuk melaporkan insiden. Penting untuk membuat insiden baru untuk setiap masalah atau pertanyaan baru. Saat membuka kasus yang terkait dengan pertanyaan lama, akan sangat membantu untuk memasukkan nomor kasus terkait sehingga kami dapat merujuk ke korespondensi sebelumnya.

> **Note**
>
> Jika korespondensi kasus menyimpang dari masalah asli, operator AMS mungkin meminta Anda untuk melaporkan insiden baru.

Untuk melaporkan insiden menggunakan konsol AMS:

1. Dari navigasi kiri, pilih Insiden

   Daftar Insiden terbuka:

   Jika daftar insiden Anda kosong, opsi Hapus filter akan mengatur ulang filter ke Status apa pun.

Jika Anda tahu ingin menggunakan telepon atau obrolan, klik Buat insiden di Support Center untuk membuka halaman Create insiden di Support Center Console, yang diisi otomatis dengan jenis layanan AMS.

> **Important**
>
> - Panggilan telepon yang dimulai dengan Dukungan direkam, untuk meningkatkan respons dengan lebih baik. Jika panggilan turun, Anda harus menelepon kembali melalui kasus Support Center, tidak AWS memiliki mekanisme untuk menelepon Anda kembali.
> - Dukungan telepon dan obrolan dirancang untuk membantu kasus dukungan, insiden. dan permintaan layanan, bukan RFC atau masalah keamanan.
> - Untuk masalah RFC, gunakan opsi korespondensi pada halaman detail RFC yang relevan, untuk menghubungi insinyur AMS.
> - Untuk masalah keamanan, buat kasus dukungan prioritas tinggi (P1 atau P2). Fitur obrolan langsung bukan untuk acara keamanan.

2. Jika Anda ingin menemukan insiden yang ada, pilih filter status insiden di daftar drop-down.

	• Semua insiden yang belum terselesaikan. • Insiden baru yang belum ditetapkan. • Insiden yang telah ditetapkan. • Insiden yang Anda buka kembali. • Insiden yang ditugaskan dan rumit. • Insiden yang membutuhkan umpan balik Anda sebelum langkah berikutnya. • Insiden yang baru-baru ini Anda kirimkan informasi. • Sebuah insiden yang telah berakhir. • Semua insiden di akun.

3. Pilih Buat.

   Halaman Buat insiden terbuka:

4. Pilih Prioritas:

   - Rendah: Fungsi non-kritis dari layanan bisnis Anda atau aplikasi yang terkait dengan sumber AWS daya/AMS terpengaruh.
   - Medium: Layanan bisnis atau aplikasi yang terkait dengan sumber AWS daya/AMS cukup terpengaruh dan berfungsi dalam keadaan terdegradasi.
   - Tinggi: Bisnis Anda terpengaruh secara signifikan. Fungsi penting aplikasi Anda yang terkait dengan sumber daya AWS/AMS tidak tersedia. Dicadangkan untuk pemadaman paling kritis yang mempengaruhi sistem produksi.

5. Pilih Kategori.

   > **Note**
   >
   > Jika Anda akan menguji fungsionalitas insiden, tambahkan flag no-action (AMSTestNoOpsActionRequired) ke judul insiden Anda.

6. Masukkan informasi untuk:

   - Subjek: Judul deskriptif untuk laporan insiden.
   - Email CC: Daftar alamat email untuk orang yang ingin Anda informasikan tentang laporan dan resolusi insiden.
   - Detail: Deskripsi komprehensif tentang insiden tersebut, sistem yang terkena dampak, dan hasil yang diharapkan dari resolusi tersebut. Jawab pertanyaan yang telah ditetapkan sebelumnya, atau hapus dan masukkan informasi yang relevan.

   Untuk menambahkan lampiran, pilih Tambahkan Lampiran, telusuri lampiran yang Anda inginkan, dan klik Buka. Untuk menghapus lampiran, klik ikon Hapus:

7. Pilih Kirim.

   Halaman detail terbuka dengan informasi tentang insiden—seperti Jenis, Subjek, Dibuat, ID, dan Status—dan area Korespondensi yang menyertakan deskripsi permintaan yang Anda buat.

Klik Balas untuk membuka area korespondensi dan memberikan rincian tambahan atau pembaruan status.

Klik Tutup Kasus ketika insiden telah diselesaikan.

Klik Muat Lebih banyak jika ada lebih banyak korespondensi daripada yang akan muat pada satu halaman.

Jangan lupa untuk menilai komunikasi!

Insiden Anda ditampilkan di halaman daftar Insiden.

Membuat permintaan layanan

Untuk membuat permintaan layanan menggunakan konsol AWS Managed Services (AMS):

1. Dari navigasi kiri, pilih Permintaan layanan.

   Daftar permintaan Layanan terbuka.

   Jika daftar permintaan layanan Anda kosong, opsi Hapus filter akan mengatur ulang filter ke Status apa pun.

   Jika Anda tahu ingin menggunakan telepon atau obrolan, klik Buat permintaan layanan di Support Center untuk membuka halaman Buat permintaan layanan di Konsol Pusat Dukungan, yang diisi otomatis dengan jenis layanan AMS.

   > **Note**
   >
   > Panggilan telepon yang dimulai dengan Dukungan pusat direkam, untuk meningkatkan respons dengan lebih baik. Jika panggilan turun, Anda harus menelepon kembali melalui kasus Support Center, tidak AWS memiliki mekanisme untuk menelepon Anda kembali.

> **Important**
>
> Dukungan telepon dan obrolan dirancang untuk membantu kasus dukungan, insiden, dan permintaan layanan. Untuk masalah RFC, gunakan opsi korespondensi pada halaman detail RFC yang relevan, untuk menghubungi insinyur AMS.

2. Jika Anda ingin menemukan permintaan layanan yang ada, pilih filter status permintaan layanan di daftar drop-down.

	• Semua permintaan layanan yang belum diselesaikan. • Permintaan layanan baru yang belum ditetapkan. • Permintaan layanan yang telah ditetapkan. • Permintaan layanan yang Anda buka kembali. • Permintaan layanan yang ditugaskan, rumit,. • Permintaan layanan yang memerluka n umpan balik Anda sebelum langkah berikutnya. • Permintaan layanan yang baru-baru ini Anda kirimkan informasinya. • Permintaan layanan yang telah selesai. • Semua permintaan layanan di akun.

3. Pilih Buat.

   Halaman Buat permintaan layanan terbuka.

4. Pilih Kategori.

> **Note**
>
> Jika Anda akan menguji fungsionalitas permintaan layanan, tambahkan flag no-action,`AMSTestNoOpsActionRequired`. ke judul permintaan layanan Anda.

5. Masukkan informasi untuk:

   - Subjek: Ini membuat tautan ke detail permintaan layanan di halaman daftar.
   - Email CC: Email ini menerima korespondensi selain kontak email default Anda.
   - Detail: Berikan informasi sebanyak mungkin di sini.

   Untuk menambahkan lampiran, pilih Tambahkan Lampiran, telusuri lampiran yang Anda inginkan, dan klik Buka. Untuk menghapus lampiran, klik ikon Hapus:

6. Pilih Kirim.

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

   Selain itu, permintaan layanan Anda ditampilkan pada halaman daftar Permintaan Layanan. Gunakan ini ketika Anda memiliki peringatan tetapi belum mendengar dari AMS.

   Klik Balas untuk membuka area korespondensi dan memberikan detail tambahan atau pembaruan status.

   Klik Selesaikan Kasus ketika permintaan layanan telah diselesaikan.

   Klik Muat Lainnya untuk melihat korespondensi tambahan yang tidak sesuai di halaman awal.

   Jangan lupa untuk menilai komunikasi!

Untuk kueri terkait penagihan, gunakan Kategori Lain di konsol AMS; di AMS CM API, atau `ChangeTypeId ct-1e1xtak34nx76` di `IssueType=AMS` AWS Support API.

Langkah pasca-orientasi

Sekarang setelah Anda masuk ke akun AMS, Anda akan ingin membaca lebih banyak dokumentasi AMS. Lihat dokumen-dokumen ini:

- Tutorial untuk menggunakan CT stack HA Two-Tier untuk membuat WordPress tumpukan yang berfungsi penuh, selanjutnya, memberikan pengalaman AMS penuh.
- Panduan Pengguna AMS: Panduan Pengguna AMS menjelaskan fungsionalitas AMS, mencantumkan istilah utama, operasi, antarmuka, dan memberikan gambaran umum tentang arsitektur infrastruktur terkelola AMS yang khas. Selain itu, rincian manajemen akses dan default AMS diberikan. Juga disediakan deskripsi rinci tentang cara menggunakan sistem manajemen perubahan AMS dan beberapa penelusuran disediakan. Konsep manajemen tambahan juga dijelaskan.
- Referensi API AMS: Referensi API ini memberikan deskripsi semua panggilan API, termasuk permintaan, respons, dan contoh.
- Panduan Aplikasi AMS: Panduan Aplikasi AMS menjelaskan berbagai opsi dan metode untuk menerapkan dan memelihara aplikasi Anda di AMS.

Tutorial

Tutorial berikut merinci langkah-langkah untuk membuat tumpukan dua tingkat dengan CT Ketersediaan Tinggi (lanjutan) (ct-06mjngx5flwto), menggunakan CLI dan menggunakan Konsol. Tutorial diberikan untuk menyebarkan grup Auto Scaling Linux (ASG) dan untuk menyebarkan ASG Windows.

Deskripsi untuk semua opsi CT, termasuk ChangeTypeId dapat ditemukan di Referensi Jenis Perubahan AMS.

Tutorial CLI: Tumpukan Dua Tingkat Ketersediaan Tinggi (Linux/RHEL)

Bagian ini menjelaskan cara menerapkan tumpukan dua tingkat ketersediaan tinggi (HA) ke dalam lingkungan AMS menggunakan AMS CLI.

> **Note**
>
> Panduan penerapan ini telah diuji di lingkungan AMZN Linux dan RHEL.

Ringkasan tugas dan diperlukan RFCs:

1. Buat infrastruktur (tumpukan dua tingkat HA)
2. Buat bucket S3 untuk aplikasi CodeDeploy
3. Buat bundel WordPress aplikasi dan unggah ke bucket S3
4. Menyebarkan aplikasi dengan CodeDeploy
5. Akses WordPress situs dan masuk untuk memvalidasi penerapan

Sebelum Anda Memulai

Deployment | Advanced Stack Components | High Availability Two Tier Stack Advanced | Create CT membuat grup Auto Scaling, load balancer, database, dan CodeDeploy nama aplikasi serta grup deployment (dengan nama yang sama dengan yang Anda berikan pada aplikasi). Untuk informasi tentang CodeDeploy lihat Apa itu CodeDeploy?

Panduan ini menggunakan RFC High Availability Two-Tier Stack (Advanced) yang menyertakan UserData dan juga menjelaskan cara membuat WordPress bundel yang dapat diterapkan. CodeDeploy

Yang `UserData` ditunjukkan dalam contoh mendapatkan metadata instance seperti ID instance, wilayah, dll, dari dalam instance yang sedang berjalan dengan menanyakan layanan metadata EC2 instance yang tersedia di http://169.254.169.254/latest/meta-data/. Baris ini dalam skrip data pengguna:`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, mengambil nama zona ketersediaan dari layanan meta-data ke variabel $REGION untuk wilayah yang kami dukung, dan menggunakannya untuk melengkapi URL untuk bucket S3 tempat agen diunduh. CodeDeploy IP 169.254.169.254 hanya dapat dirutekan dalam VPC (semua dapat menanyakan layanan). VPCs Untuk informasi tentang layanan, lihat Metadata Instans dan Data Pengguna. Perhatikan juga bahwa skrip yang UserData dimasukkan sebagai dijalankan sebagai pengguna “root” dan tidak perlu menggunakan perintah “sudo”.

Panduan ini meninggalkan parameter berikut pada nilai default (ditampilkan):

- Grup Auto Scaling:. `Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium,`

`MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`

- Load Balancer:. `HealthCheckInterval=30, HealthCheckTimeout=5`
- Basis data:`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.
- Aplikasi:`DeploymentConfigName=CodeDeployDefault.OneAtATime`.
- Ember S3:`AccessControl=Private`.

PENGATURAN TAMBAHAN:

`RequestedStartTime`dan `RequestedEndTime` jika Anda ingin menjadwalkan RFC Anda: Anda dapat menggunakan time.Is untuk menentukan waktu UTC yang benar. Contoh yang diberikan harus disesuaikan dengan tepat. RFC tidak dapat melanjutkan jika waktu mulai telah berlalu. Atau, Anda dapat mengabaikan nilai-nilai tersebut untuk membuat ASAP RFC yang dijalankan segera setelah persetujuan dilewatkan.

> **Note**
>
> Ada banyak parameter yang mungkin Anda pilih untuk diatur secara berbeda dari seperti yang ditunjukkan. Nilai untuk parameter yang ditunjukkan dalam contoh telah diuji tetapi mungkin tidak tepat untuk Anda.

Buat Infrastruktur

Mengumpulkan data berikut sebelum Anda mulai akan membuat penyebaran berjalan lebih cepat.

DATA YANG DIBUTUHKAN HA STACK:

- AutoScalingGroup:

- `UserData`: Nilai ini disediakan dalam tutorial ini. Ini termasuk perintah untuk mengatur sumber daya untuk CodeDeploy dan memulai CodeDeploy agen.
- `AMI-ID`: Nilai ini menentukan jenis EC2 instance grup Auto Scaling (ASG) Anda yang akan berputar. Pastikan untuk memilih AMI di akun Anda yang dimulai dengan “pelanggan-” dan merupakan sistem operasi yang Anda inginkan. Temukan AMI IDs dengan referensi Untuk AMS SKMS API, lihat tab Laporan di AWS Artifact Console. operasi (CLI: list-amis) atau di halaman AMS Console -> detail. VPCs VPCs Panduan ini untuk ASGs dikonfigurasi untuk menggunakan AMI Linux.

- Database:
  - Parameter ini`DBEngine`,`EngineVersion`,, dan `LicenseModel` harus diatur sesuai dengan situasi Anda meskipun nilai yang ditunjukkan dalam contoh telah diuji.
  - Parameter ini`RDSSubnetIds`,`DBName`,`MasterUsername`,, dan `MasterUserPassword` diperlukan saat menerapkan bundel aplikasi. Untuk RDSSubnet Id, gunakan dua subnet Private.
- LoadBalancer:
  - Parameter ini`DBEngine`,`EngineVersion`,, dan `LicenseModel` harus diatur sesuai dengan situasi Anda meskipun nilai yang ditunjukkan dalam contoh telah diuji.
  - `ELBSubnetIds`: Gunakan dua subnet Publik.
- Aplikasi: `ApplicationName` Nilai menetapkan nama CodeDeploy aplikasi dan nama grup CodeDeploy penyebaran. Anda menggunakannya untuk menyebarkan aplikasi Anda. Itu harus unik di akun. Untuk memeriksa CodeDeploy nama akun Anda, lihat CodeDeploy Konsol. Contoh menggunakan "WordPress" tetapi, jika Anda akan menggunakan nilai itu, pastikan itu belum digunakan.

Prosedur ini menggunakan CT stack dua tingkat (lanjutan) ketersediaan tinggi (ct-06mjngx5flwto) dan CT penyimpanan Create S3 (ct-1a68ck03fn98r). Dari akun Anda yang diautentikasi, ikuti langkah-langkah ini di baris perintah.

1. Luncurkan tumpukan infrastruktur.

   a. Keluarkan parameter eksekusi skema JSON untuk CT stack dua tingkat HA ke file di folder Anda saat ini bernama CreateStackParams .json.

```
aws amscm get-change-type-version --change-type-id "ct-06mjngx5flwto"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateStackParams.json
```

b. Ubah skema. Ganti *variables* yang sesuai. Misalnya, gunakan OS yang Anda inginkan untuk EC2 instance yang akan dibuat ASG. Rekam `ApplicationName` karena Anda akan menggunakannya nanti untuk menyebarkan aplikasi. Perhatikan bahwa Anda dapat menambahkan hingga 50 tag.

```
{
"Description":      "HA two tier stack for WordPress",
"Name":             "WordPressStack",
"TimeoutInMinutes":  360,
"Tags": [
        {
            "Key": "ApplicationName",
            "Value": "WordPress"
        }
    ],
"AutoScalingGroup": {
            "AmiId":    "AMI-ID",
            "UserData": "#!/bin/bash \n
            REGION=$(curl 169.254.169.254/latest/meta-data/placement/
availability-zone/ | sed 's/[a-z]$//') \n
            yum -y install ruby httpd \n
            chkconfig httpd on \n
            service httpd start \n
            touch /var/www/html/status \n
            cd /tmp \n
            curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/
install \n
            chmod +x ./install \n
            ./install auto \n
            chkconfig codedeploy-agent on \n
            service codedeploy-agent start"
    },
    "LoadBalancer": {
        "Public":               true,
        "HealthCheckTarget":    "HTTP:80/status"
    },
    "Database":     {
        "DBEngine":             "MySQL",
        "DBName":               "wordpress",
        "EngineVersion":        "8.0.16 ",
        "LicenseModel":         "general-public-license",
        "MasterUsername":       "admin",
        "MasterUserPassword":   "p4ssw0rd"
```

```
    },
    "Application":  {
    "ApplicationName":  "WordPress"
        }
}
```

c. Keluarkan template CreateRfc JSON ke file di folder Anda saat ini bernama CreateStackRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateStackRfc.json
```

d. Ubah template RFC sebagai berikut dan simpan, Anda dapat menghapus dan mengganti isinya. Perhatikan bahwa `RequestedStartTime` dan `RequestedEndTime` sekarang opsional; mengecualikan mereka membuat ASAP RFC yang mengeksekusi segera setelah disetujui (yang biasanya terjadi secara otomatis). Untuk mengirimkan RFC terjadwal, tambahkan nilai-nilai tersebut.

```
{
"ChangeTypeVersion":    "3.0",
"ChangeTypeId":         "ct-06mjngx5flwto",
"Title":                "HA-Stack-For-WP-RFC"
}
```

e. Buat RFC, tentukan CreateStackRfc file.json dan file parameter eksekusi CreateStackParams .json:

```
aws amscm create-rfc --cli-input-json file://CreateStackRfc.json --execution-
parameters file://CreateStackParams.json
```

Anda menerima ID RFC dalam tanggapan. Simpan ID untuk langkah selanjutnya.

f. Kirim RFC:

```
aws amscm submit-rfc --rfc-id  RFC_ID
```

Jika RFC berhasil, Anda tidak menerima output.

g. Untuk memeriksa status RFC, jalankan

```
aws amscm get-rfc --rfc-id RFC_ID
```

Catat ID RFC.

2. Luncurkan ember S3

   Mengumpulkan data berikut sebelum Anda mulai akan membuat penyebaran berjalan lebih cepat.

   EMBER DATA S3 YANG DIBUTUHKAN:

   - `VPC-ID`: Nilai ini menentukan di mana Bucket S3 Anda akan berada. Gunakan ID VPC yang sama dengan yang Anda gunakan sebelumnya.
   - `BucketName`: Nilai ini menetapkan nama Bucket S3, Anda menggunakannya untuk mengunggah bundel aplikasi Anda. Itu harus unik di seluruh wilayah akun dan tidak dapat menyertakan huruf besar. Menyertakan ID akun Anda sebagai bagian dari BucketName bukan persyaratan tetapi membuatnya lebih mudah untuk mengidentifikasi bucket nanti. Untuk melihat nama bucket S3 yang ada di akun, buka Konsol Amazon S3 untuk akun Anda.

   a. Output parameter eksekusi skema JSON untuk penyimpanan S3 create CT ke file JSON bernama creates3 .json. StoreParams

   ```
   aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    CreateS3StoreParams.json
   ```

   b. Ubah skema sebagai berikut, Anda dapat menghapus dan mengganti isinya. Ganti *`VPC_ID`* dengan tepat. Nilai-nilai dalam contoh telah diuji, tetapi mungkin tidak tepat untuk Anda.

   > **Tip**
   >
   > `BucketName`Harus unik di seluruh wilayah akun dan tidak dapat menyertakan huruf besar. Menyertakan ID akun Anda sebagai bagian dari BucketName bukan persyaratan tetapi membuatnya lebih mudah untuk mengidentifikasi bucket nanti. Untuk melihat nama bucket S3 yang ada di akun, buka Konsol Amazon S3 untuk akun Anda.

   ```
   {
   ```

```
"Description":      "S3BucketForWordPressBundle",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-s2b72beb000000000",
"Name":             "S3BucketForWP",
"TimeoutInMinutes":  60,
"Parameters":   {
    "AccessControl":    "Private",
    "BucketName":       "ACCOUNT_ID-BUCKET_NAME"
    }
}
```

c. Keluarkan template JSON CreateRfc ke file, di folder Anda saat ini, bernama StoreRfc createS3 .json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateS3StoreRfc.json
```

d. Ubah dan simpan file creates3 StoreRfc .json, Anda dapat menghapus dan mengganti isinya. Perhatikan bahwa `RequestedStartTime` dan `RequestedEndTime` sekarang opsional; mengecualikan mereka membuat ASAP RFC yang mengeksekusi segera setelah disetujui (yang biasanya terjadi secara otomatis). Untuk mengirimkan RFC terjadwal, tambahkan nilai-nilai tersebut.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-1a68ck03fn98r",
"Title":                "S3-Stack-For-WP-RFC"
}
```

e. Buat RFC, tentukan file creates3 .json dan file parameter eksekusi creates3 StoreRfc .json: StoreParams

```
aws amscm create-rfc --cli-input-json file://CreateS3StoreRfc.json  --
execution-parameters file://CreateS3StoreParams.json
```

Anda menerima RFC baru sebagai tanggapan. RfcId Simpan ID untuk langkah selanjutnya.

f. Kirim RFC:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Jika RFC berhasil, Anda tidak menerima output.

g. Untuk memeriksa status RFC, jalankan

```
aws amscm get-rfc --rfc-id RFC_ID
```

Membuat, Mengunggah, dan Menyebarkan Aplikasi

Pertama, buat bundel WordPress aplikasi, lalu gunakan CodeDeploy CTs untuk membuat dan menyebarkan aplikasi.

1. Unduh WordPress, ekstrak file dan buat file. /scripts direktori.

   Perintah Linux:

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: Tempel `https://github.com/WordPress/WordPress/archive/master.zip` ke jendela browser dan unduh file zip.

   Buat direktori sementara untuk merakit paket.

   Linux:

   ```
   mkdir /tmp/WordPress
   ```

   Windows: Buat direktori WordPress "", Anda akan menggunakan jalur direktori nanti.

2. Ekstrak WordPress sumber ke direktori WordPress "" dan buat file. /scripts direktori.

   Linux:

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   mkdir scripts
   ```

   Windows: Buka direktori "WordPress" yang Anda buat dan buat direktori “skrip” di sana.

Jika Anda berada di lingkungan Windows, pastikan untuk mengatur jenis istirahat untuk file skrip ke Unix (LF). Di Notepad ++, ini adalah opsi di kanan bawah jendela.

3. Buat file CodeDeploy appspec.yl, di WordPress direktori (jika menyalin contoh, periksa lekukan, setiap spasi dihitung). PENTING: Pastikan jalur “sumber” benar untuk menyalin WordPress file (dalam hal ini, di WordPress direktori Anda) ke tujuan yang diharapkan (/var/www/html/WordPress). Dalam contoh, file appspec.ymlada di direktori dengan WordPress file, jadi hanya “/” yang diperlukan. Juga, bahkan jika Anda menggunakan RHEL AMI untuk grup Auto Scaling Anda, biarkan baris “os: linux” apa adanya. Contoh file appspec.yml:

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. Buat skrip file bash di file. WordPress /scripts direktori.

   Pertama, buat `config_wordpress.sh` dengan konten berikut (jika Anda mau, Anda dapat mengedit file wp-config.php secara langsung).

> **Note**
>
> Ganti *DBName* dengan nilai yang diberikan dalam HA Stack RFC (misalnya,`wordpress`).

Ganti *DB_MasterUsername* dengan `MasterUsername` nilai yang diberikan dalam HA Stack RFC (misalnya,`admin`).
Ganti *DB_MasterUserPassword* dengan `MasterUserPassword` nilai yang diberikan dalam HA Stack RFC (misalnya,`p4ssw0rd`).
Ganti *DB_ENDPOINT* dengan nama DNS endpoint dalam output eksekusi HA Stack RFC (misalnya,). `srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com` Anda dapat menemukannya dengan GetRfcoperasi (CLI: get-rfc --rfc-id RFC_ID) atau di halaman detail RFC Konsol AMS untuk HA Stack RFC yang sebelumnya Anda kirimkan.

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. Di direktori yang sama buat `install_dependencies.sh` dengan konten berikut:

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS diinstal sebagai bagian dari data pengguna saat peluncuran untuk memungkinkan pemeriksaan kesehatan berfungsi sejak awal.

6. Di direktori yang sama buat `start_server.sh` dengan konten berikut:

   - Untuk instance Amazon Linux, gunakan ini:

```
#!/bin/bash
service httpd start
```

- Untuk instance RHEL, gunakan ini (perintah tambahan adalah kebijakan yang memungkinkan SELINUX menerima): WordPress

```
#!/bin/bash
setsebool -P  httpd_can_network_connect_db 1
setsebool -P  httpd_can_network_connect 1
chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
restorecon -Rv /var/www/html
service httpd start
```

7. Di direktori yang sama buat `stop_server.sh` dengan konten berikut:

```
#!/bin/bash
service httpd stop
```

8. Buat bundel zip.

   Linux:

```
$ cd /tmp/WordPress
$ zip -r wordpress.zip .
```

   Windows: Buka direktori "WordPress" Anda dan pilih semua file dan buat file zip, pastikan untuk menamainya wordpress.zip.

1. Unggah bundel aplikasi ke bucket S3.

   Bundel harus ada untuk terus menerapkan tumpukan.

   Anda secara otomatis memiliki akses ke instans bucket S3 yang Anda buat. Anda dapat mengaksesnya melalui benteng Anda, atau melalui konsol S3, dan mengunggah WordPress bundel dengan drag-and-drop atau menjelajah ke dan memilih file zip.

   Anda juga dapat menggunakan perintah berikut di jendela shell; pastikan Anda memiliki jalur yang benar ke file zip:

```
aws s3 cp wordpress.zip s3://BUCKET_NAME/
```

2. Menyebarkan bundel WordPress aplikasi.

Mengumpulkan data berikut sebelum Anda mulai akan membuat penyebaran berjalan lebih cepat.

DATA YANG DIBUTUHKAN:

- `VPC-ID`: Nilai ini menentukan di mana Bucket S3 Anda akan berada. Gunakan ID VPC yang sama dengan yang Anda gunakan sebelumnya.
- `CodeDeployApplicationNamedanCodeDeployApplicationName`: `ApplicationName` Nilai yang Anda gunakan dalam HA 2-Tier Stack RFC mengatur CodeDeployApplicationName dan. CodeDeployDeploymentGroupName Contoh menggunakan "WordPress" tetapi Anda mungkin telah menggunakan nilai yang berbeda.
- `S3Location`: Untuk`S3Bucket`, gunakan `BucketName` yang Anda buat sebelumnya. Itu `S3BundleType` dan `S3Key` berasal dari bundel yang Anda letakkan di toko S3 Anda.

a. Output parameter eksekusi skema JSON untuk CodeDeploy aplikasi menyebarkan CT ke file JSON bernama Deploy Params.json. CDApp

```
aws amscm get-change-type-version --change-type-id "ct-2edc3sd1sqmrb"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 DeployCDAppParams.json
```

b. Ubah skema sebagai berikut dan simpan sebagai, Anda dapat menghapus dan mengganti isinya.

```
{
"Description":                          "DeployWPCDApp",
"VpcId":                                "VPC_ID",
"Name":                                 "WordPressCDAppDeploy",
"TimeoutInMinutes":                     60,
"Parameters":   {
    "CodeDeployApplicationName":                "WordPress",
    "CodeDeployDeploymentGroupName":            "WordPress",
    "CodeDeployIgnoreApplicationStopFailures":   false,
    "CodeDeployRevision": {
      "RevisionType": "S3",
      "S3Location": {
        "S3Bucket":     "BUCKET_NAME",
        "S3BundleType": "zip",
        "S3Key":        "wordpress.zip" }
```

```
        }
    }
}
```

c. Keluarkan template JSON CreateRfc ke file, di folder Anda saat ini, bernama Deploy CDApp RFC.json:

```
aws amscm create-rfc --generate-cli-skeleton > DeployCDAppRfc.json
```

d. Ubah dan simpan file Deploy CDApp RFC.json, Anda dapat menghapus dan mengganti isinya. Perhatikan bahwa `RequestedStartTime` dan `RequestedEndTime` sekarang opsional; mengecualikan mereka membuat ASAP RFC yang mengeksekusi segera setelah disetujui (yang biasanya terjadi secara otomatis). Untuk mengirimkan RFC terjadwal, tambahkan nilai-nilai tersebut.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-2edc3sd1sqmrb",
"Title":                "CD-Deploy-For-WP-RFC"
}
```

e. Buat RFC, tentukan file Deploy CDApp Rfc dan file parameter eksekusi Deploy CDApp Params:

```
aws amscm create-rfc --cli-input-json file://DeployCDAppRfc.json  --execution-
parameters file://DeployCDAppParams.json
```

Anda menerima RFC baru sebagai tanggapan. RfcId Simpan ID untuk langkah selanjutnya.

f. Kirim RFC:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Jika RFC berhasil, Anda tidak menerima output.

g. Untuk memeriksa status RFC, jalankan

```
aws amscm get-rfc --rfc-id RFC_ID
```

Validasi Penerapan Aplikasi

Arahkan ke titik akhir (ELB CName) penyeimbang beban yang dibuat sebelumnya, dengan jalur yang diterapkan:/. WordPress WordPress Misalnya:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

Meruntuhkan Penerapan Aplikasi

Setelah Anda selesai dengan tutorial, Anda akan ingin meruntuhkan penyebaran sehingga Anda tidak dikenakan biaya untuk sumber daya.

Berikut ini adalah operasi penghapusan tumpukan generik. Anda akan ingin mengirimkannya dua kali, sekali untuk tumpukan HA 2-Tier dan sekali untuk tumpukan bucket S3. Sebagai tindak lanjut terakhir, kirimkan permintaan layanan agar semua snapshot untuk bucket S3 (termasuk ID tumpukan bucket S3 dalam permintaan layanan) dihapus. Mereka secara otomatis dihapus setelah 10 hari, tetapi menghapusnya lebih awal menghemat sedikit biaya.

Panduan ini memberikan contoh penggunaan konsol AMS untuk menghapus tumpukan S3; prosedur ini berlaku untuk menghapus tumpukan apa pun menggunakan konsol AMS.

> **Note**
>
> Jika menghapus ember S3, itu harus dikosongkan dari objek terlebih dahulu.

DATA YANG DIBUTUHKAN:

- `StackId`: Tumpukan untuk digunakan. Anda dapat menemukannya dengan melihat halaman AMS Console Stacks, tersedia melalui tautan di navigasi kiri. Menggunakan AMS SKMS API/CLI, jalankan referensi Untuk AMS SKMS API, lihat tab Laporan di AWS Artifact Console. operasi (di CLI). `list-stack-summaries`
- ID tipe perubahan untuk panduan ini adalah`ct-0q0bic0ywqk6c`, versinya adalah “1.0", untuk mengetahui versi terbaru, jalankan perintah ini:

  ```
  aws amscm list-change-type-version-summaries --filter
   Attribute=ChangeTypeId,Value=ct-0q0bic0ywqk6c
  ```

BUAT SEBARIS:

- Keluarkan perintah buat RFC dengan parameter eksekusi yang disediakan sebaris (tanda kutip saat memberikan parameter eksekusi sebaris). E

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0"
 --title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

- Kirim RFC menggunakan ID RFC yang dikembalikan dalam operasi create RFC. Sampai diserahkan, RFC tetap di `Editing` negara bagian dan tidak ditindaklanjuti.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- Pantau status RFC dan lihat output eksekusi:

```
aws amscm get-rfc --rfc-id RFC_ID
```

TEMPLATE MEMBUAT:

1. Keluarkan template RFC ke file di folder Anda saat ini; contoh menamainya DeleteStackRfc .json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. Ubah dan simpan DeleteStackRfc file.json. Karena menghapus tumpukan hanya memiliki satu parameter eksekusi, parameter eksekusi dapat berada di DeleteStackRfc file.json itu sendiri (tidak perlu membuat file JSON terpisah dengan parameter eksekusi).

   Tanda kutip internal dalam ekstensi ExecutionParameters JSON harus diloloskan dengan garis miring terbalik (\). Contoh tanpa waktu mulai dan berakhir:

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   }
   ```

3. Buat RFC:

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
```

Anda menerima RFC baru sebagai tanggapan. RfcId Misalnya:

```
{
"RfcId": "daaa1867-ffc5-1473-192a-842f6b326102"
}
```

Simpan ID untuk langkah selanjutnya.

4. Kirim RFC:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Jika RFC berhasil, Anda tidak menerima konfirmasi di baris perintah.

5. Untuk memantau status permintaan dan untuk melihat Output Eksekusi:

```
aws amscm get-rfc --rfc-id RFC_ID --query "Rfc.
{Status:Status.Name,Exec:ExecutionOutput}" --output table
```

Tutorial Konsol: Ketersediaan Tinggi Dua Tingkat Stack (Linux/RHEL)

Bagian ini menjelaskan cara menerapkan WordPress situs ketersediaan tinggi (HA) ke lingkungan AMS menggunakan konsol AMS.

> **Note**
>
> Panduan penerapan ini telah diuji di lingkungan AMZN Linux dan RHEL.

Ringkasan tugas dan diperlukan RFCs:

1. Buat infrastruktur (tumpukan dua tingkat HA)
2. Buat bucket S3 untuk aplikasi CodeDeploy
3. Buat bundel WordPress aplikasi dan unggah ke bucket S3
4. Menyebarkan aplikasi dengan CodeDeploy

5. Akses WordPress situs dan masuk untuk memvalidasi penerapan
6. Meruntuhkan penyebaran

Deskripsi untuk semua opsi CT, termasuk ChangeTypeId, dapat ditemukan di Referensi Jenis Perubahan AMS.

Sebelum Anda Memulai

Deployment | Advanced Stack Components | High Availability Two Tier Stack | Create CT membuat grup Auto Scaling, load balancer, database, dan CodeDeploy nama aplikasi serta grup deployment (dengan nama yang sama dengan yang Anda berikan pada aplikasi). Untuk informasi tentang CodeDeploy lihat Apa itu CodeDeploy?

Panduan ini menggunakan RFC Stack Dua Tingkat Ketersediaan Tinggi yang menyertakan `UserData` dan juga menjelaskan cara membuat WordPress bundel yang dapat digunakan. CodeDeploy

Yang `UserData` ditunjukkan dalam contoh mendapatkan metadata instance seperti ID instance, wilayah, dll, dari dalam instance yang sedang berjalan dengan menanyakan layanan metadata EC2 instance yang tersedia di http://169.254.169.254/latest/meta-data/. Baris ini dalam skrip data pengguna:`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, mengambil nama zona ketersediaan dari layanan meta-data ke variabel $REGION untuk wilayah yang kami dukung, dan menggunakannya untuk melengkapi URL untuk bucket S3 tempat agen diunduh. CodeDeploy IP 169.254.169.254 hanya dapat dirutekan dalam VPC (semua dapat menanyakan layanan). VPCs Untuk informasi tentang layanan, lihat Metadata Instans dan Data Pengguna. Perhatikan juga bahwa skrip yang UserData dimasukkan sebagai dijalankan sebagai pengguna “root” dan tidak perlu menggunakan perintah “sudo”.

Panduan ini meninggalkan parameter berikut pada nilai default (ditampilkan):

- Grup Auto Scaling:. `Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average,`

`ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`

- Load Balancer:. `HealthCheckInterval=30, HealthCheckTimeout=5`
- Basis data:`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.
- Aplikasi:`DeploymentConfigName=CodeDeployDefault.OneAtATime`.

Parameter Variabel:

Konsol menyediakan opsi ASAP untuk waktu mulai dan panduan ini merekomendasikan untuk menggunakannya. ASAP menyebabkan RFC dieksekusi segera setelah persetujuan disahkan.

> **Note**
>
> Ada banyak parameter yang mungkin Anda pilih untuk diatur secara berbeda dari seperti yang ditunjukkan. Nilai untuk parameter yang ditunjukkan dalam contoh telah diuji tetapi mungkin tidak tepat untuk Anda. Hanya nilai yang diperlukan yang ditampilkan dalam contoh. Nilai dalam *`replaceable`* font harus diubah karena mereka khusus untuk akun Anda.

Buat Infrastruktur

Prosedur ini menggunakan CT stack dua tingkat ketersediaan tinggi diikuti oleh CT penyimpanan Create S3.

Mengumpulkan data berikut sebelum Anda mulai akan membuat penyebaran berjalan lebih cepat.

DATA YANG DIBUTUHKAN HA STACK:

- AutoScalingGroup:
  - UserData: Nilai ini disediakan dalam tutorial ini. Ini termasuk perintah untuk mengatur sumber daya untuk CodeDeploy dan memulai CodeDeploy agen.
  - AMI-ID: Nilai ini menentukan sistem operasi EC2 instance grup Auto Scaling (ASG) Anda akan berputar. Pilih AMI di akun Anda yang dimulai dengan “pelanggan-” dan merupakan sistem

operasi yang Anda inginkan. Temukan AMI IDs di AMS Console VPCs -> halaman VPCs detail. Panduan ini untuk ASGs dikonfigurasi untuk menggunakan Amazon Linux atau RHEL AMI.

- Database:
  - Parameter ini DBEngine, EngineVersion,, dan LicenseModelharus diatur sesuai dengan situasi Anda meskipun nilai yang ditunjukkan dalam contoh telah diuji. Tutorial menggunakan nilai-nilai ini, masing-masing:*MySQL*,*8.0.16*,*general-public-license*.
  - Parameter ini DBName, MasterUserPassword,, dan MasterUsernamediperlukan saat menerapkan bundel aplikasi. Tutorial menggunakan nilai-nilai ini, masing-masing:*wordpressDB*,*p4ssw0rd*,*admin*. Perhatikan bahwa hanya DBName dapat berisi karakter alfanumerik.
  - Ketika Anda memasukkan MasterUsernameuntuk RDS DB, itu akan muncul di cleartext, jadi masuk ke database sesegera mungkin dan ubah kata sandi untuk memastikan keamanan Anda.
  - Untuk RDSSubnetId, gunakan dua subnet Private. Masukkan mereka satu per satu menekan “Enter” setelah masing-masing. Temukan Subnet IDs dengan referensi Untuk AMS SKMS API, lihat tab Laporan di AWS Artifact Console. operasi (CLI list-subnet-summaries:) atau di halaman AMS Console -> VPC details. VPCs
- LoadBalancer:
  - Atur parameter ini, Public ke true karena tutorial menggunakan subnet ELB Public.
  - ELBSubnetIds: Gunakan dua subnet Publik. Masukkan mereka satu per satu menekan “Enter” setelah masing-masing. Temukan Subnet IDs dengan referensi Untuk AMS SKMS API, lihat tab Laporan di AWS Artifact Console. operasi (CLI list-subnet-summaries:) atau di halaman AMS Console -> VPC details. VPCs
- Aplikasi: ApplicationNameNilai menetapkan nama CodeDeploy aplikasi dan nama grup CodeDeploy penyebaran. Anda menggunakannya untuk menyebarkan aplikasi Anda. Itu harus unik di akun. Untuk memeriksa CodeDeploy nama akun Anda, lihat CodeDeploy Konsol. Contoh menggunakan *WordPress* tetapi, jika Anda akan menggunakan nilai itu, pastikan bahwa itu belum digunakan.

1. Luncurkan tumpukan ketersediaan tinggi.

   a. Pada halaman Buat RFC, pilih kategori Deployment, subkategori Stack Standar, item Ketersediaan tinggi tumpukan dua tingkat dan operasi Buat, dari daftar.

   b. PENTING: Pilih Advanced dan atur nilai seperti yang ditunjukkan.

Anda hanya perlu memasukkan nilai untuk opsi berbintang (*), nilai yang diuji ditampilkan dalam contoh; Anda dapat membiarkan opsi kosong yang tidak diperlukan kosong.

c. Untuk bagian Deskripsi RFC:

```
Subject: WP-HA-2-Tier-RFC
```

d. Untuk bagian Informasi sumber daya, tetapkan parameter untuk AutoScalingGroup, Database LoadBalancer,, Aplikasi, dan Tag.

Juga, tujuan dari kunci tag AppName "" adalah agar Anda dapat dengan mudah mencari instance ASG di EC2 konsol; Anda dapat memanggil kunci tag ini “Nama” atau nama kunci lain yang Anda inginkan. Perhatikan bahwa Anda dapat menambahkan hingga 50 tag.

```
UserData:
    #!/bin/bash
    REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/
 | sed 's/[a-z]$//')
    yum -y install ruby httpd
    chkconfig httpd on
    service httpd start
    touch /var/www/html/status
    cd /tmp
    curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/install
    chmod +x ./install
    ./install auto
    chkconfig codedeploy-agent on
    service codedeploy-agent start
AmiId:              AMI-ID
Description:        WP-HA-2-Tier-Stack

Database:
    LicenseModel:    general-public-license (USE RADIO BUTTON)
    EngineVersion:   8.0.16
    DBEngine:        MySQL
    RDSSubnetIds:    PRIVATE_AZ1 PRIVATE_AZ2 (ENTER ONE AT A TIME PRESSING
 "ENTER" AFTER EACH)
    MasterUserPassword:  p4ssw0rd
    MasterUsername:      admin
    DBName:              wordpressDB

LoadBalancer:
```

```
    Public:              true (USE RADIO BUTTON)
    ELBSubnetIds:        PUBLIC_AZ1 PUBLIC_AZ2

Application:
    ApplicationName:     WordPress

Tags:
    Name:                WP-Rhel-Stack
```

e. Klik Kirim setelah selesai.

2. Masuk ke database yang Anda buat dan ubah kata sandi.

3. Luncurkan S3 bucket Stack.

   Mengumpulkan data berikut sebelum Anda mulai akan membuat penyebaran berjalan lebih cepat.

   EMBER DATA S3 YANG DIBUTUHKAN:

   - VPC-ID: Nilai ini menentukan di mana Bucket S3 Anda akan berada. Temukan VPC IDs dengan referensi Untuk AMS SKMS API, lihat tab Laporan di AWS Artifact Console. operasi (CLI:) atau di halaman AMS Console. list-vpc-summaries VPCs
   - BucketName: Nilai ini menetapkan nama Bucket S3, Anda menggunakannya untuk mengunggah bundel aplikasi Anda. Itu harus unik di seluruh wilayah akun dan tidak dapat menyertakan huruf besar. Menyertakan ID akun Anda sebagai bagian dari BucketName bukan persyaratan tetapi membuatnya lebih mudah untuk mengidentifikasi bucket nanti. Untuk melihat nama bucket S3 yang ada di akun, buka Konsol Amazon S3 untuk akun Anda.

   a. Pada halaman Create RFC, pilih kategori Deployment, subkategori Advanced Stack Components, item S3 storage, dan operation Create dari RFC CT pick list.

   b. Pertahankan opsi Basic default dan atur nilai seperti yang ditunjukkan.

```
Subject:             S3-Bucket-WP-HA-RFC
Description:         S3BucketForWordPressBundles
BucketName:          ACCOUNT_ID-BUCKET_NAME
AccessControl:       Private
VpcId:               VPC_ID
Name:                S3-Bucket-WP-HA-Stack
TimeoutInMinutes:    60
```

c. Klik Kirim setelah selesai. Bucket yang digunakan dengan jenis perubahan ini memungkinkan read/write akses penuh ke seluruh akun.

Membuat, Mengunggah, dan Menyebarkan Aplikasi

Pertama, buat bundel WordPress aplikasi, lalu gunakan CodeDeploy CTs untuk membuat dan menyebarkan aplikasi.

1. Unduh WordPress, ekstrak file dan buat file. /scripts direktori.

   Perintah Linux:

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: Tempel `https://github.com/WordPress/WordPress/archive/master.zip` ke jendela browser dan unduh file zip.

   Buat direktori sementara untuk merakit paket.

   Linux:

   ```
   mkdir /tmp/WordPress
   ```

   Windows: Buat direktori WordPress "", Anda akan menggunakan jalur direktori nanti.

2. Ekstrak WordPress sumber ke direktori WordPress "" dan buat file. /scripts direktori.

   Linux:

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   mkdir scripts
   ```

   Windows: Buka direktori "WordPress" yang Anda buat dan buat direktori “skrip” di sana.

   Jika Anda berada di lingkungan Windows, pastikan untuk mengatur jenis istirahat untuk file skrip ke Unix (LF). Di Notepad ++, ini adalah opsi di kanan bawah jendela.

3. Buat file CodeDeploy appspec.yl, di WordPress direktori (jika menyalin contoh, periksa lekukan, setiap spasi dihitung). PENTING: Pastikan jalur “sumber” benar untuk menyalin WordPress file (dalam hal ini, di WordPress direktori Anda) ke tujuan yang diharapkan (/var/www/html/WordPress). Dalam contoh, file appspec.ymlada di direktori dengan WordPress file, jadi hanya “/” yang diperlukan. Juga, bahkan jika Anda menggunakan RHEL AMI untuk grup Auto Scaling Anda, biarkan baris “os: linux” apa adanya. Contoh file appspec.yml:

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. Buat skrip file bash di file. WordPress /scripts direktori.

   Pertama, buat `config_wordpress.sh` dengan konten berikut (jika Anda mau, Anda dapat mengedit file wp-config.php secara langsung).

   > **Note**
   >
   > Ganti *`DBName`* dengan nilai yang diberikan dalam HA Stack RFC (misalnya,`wordpress`). Ganti *`DB_MasterUsername`* dengan `MasterUsername` nilai yang diberikan dalam HA Stack RFC (misalnya,`admin`).

Ganti *DB_MasterUserPassword* dengan `MasterUserPassword` nilai yang diberikan dalam HA Stack RFC (misalnya,`p4ssw0rd`).
Ganti *DB_ENDPOINT* dengan nama DNS endpoint dalam output eksekusi HA Stack RFC (misalnya,). `srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com` Anda dapat menemukannya dengan GetRfcoperasi (CLI: get-rfc --rfc-id RFC_ID) atau di halaman detail RFC Konsol AMS untuk HA Stack RFC yang sebelumnya Anda kirimkan.

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. Di direktori yang sama buat `install_dependencies.sh` dengan konten berikut:

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS diinstal sebagai bagian dari data pengguna saat peluncuran untuk memungkinkan pemeriksaan kesehatan berfungsi sejak awal.

6. Di direktori yang sama buat `start_server.sh` dengan konten berikut:

   - Untuk instance Amazon Linux, gunakan ini:

     ```
     #!/bin/bash
     service httpd start
     ```

   - Untuk instance RHEL, gunakan ini (perintah tambahan adalah kebijakan yang memungkinkan SELINUX menerima): WordPress

```
#!/bin/bash
setsebool -P  httpd_can_network_connect_db 1
setsebool -P  httpd_can_network_connect 1
chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
restorecon -Rv /var/www/html
service httpd start
```

7. Di direktori yang sama buat `stop_server.sh` dengan konten berikut:

```
#!/bin/bash
service httpd stop
```

8. Buat bundel zip.

   Linux:

```
$ cd /tmp/WordPress
$ zip -r wordpress.zip .
```

   Windows: Buka direktori "WordPress" Anda dan pilih semua file dan buat file zip, pastikan untuk menamainya wordpress.zip.

1. Unggah bundel aplikasi ke bucket S3

   Paket harus ada untuk terus menerapkan tumpukan.

   Anda secara otomatis memiliki akses ke instans bucket S3 yang Anda buat. Anda dapat mengaksesnya melalui Bastions Anda (lihat Mengakses Instans), atau melalui konsol S3, dan mengunggah CodeDeploy paket dengan drag-and-drop, atau dengan menjelajah ke dan memilih file.

   Anda juga dapat menggunakan perintah berikut di jendela shell; pastikan Anda memiliki jalur yang benar ke file zip:

```
aws s3 cp wordpress/wordpress.zip s3://BUCKET_NAME/
```

2. Menyebarkan Bundel WordPress CodeDeploy Aplikasi

   PENYEBARAN APLIKASI PENYEBARAN KODE DATA YANG DIPERLUKAN:

- CodeDeployApplicationName: Nama yang Anda berikan pada CodeDeploy aplikasi.
- CodeDeployGroupName: Karena CodeDeploy aplikasi dan grup keduanya dibuat dari nama yang Anda berikan CodeDeploy aplikasi di tumpukan HA RFC, ini adalah nama yang sama dengan CodeDeployApplicationName.
- S3Bucket: Nama yang Anda berikan pada ember S3.
- S3 BundleType dan S3Key: Ini adalah bagian dari bundel WordPress aplikasi yang Anda gunakan.
- VpcId: VPC yang relevan.

a. Pada halaman Create RFC, pilih kategori Deployment, subcategory Applications, item CodeDeploy application, dan operation Deploy dari RFC CT pick list.

b. Pertahankan opsi Basic default, dan atur nilai seperti yang ditunjukkan.

> **Note**
>
> Referensi CodeDeploy aplikasi, grup CodeDeploy penyebaran, bucket S3, dan bundel yang sebelumnya dibuat.

```
Subject:                                    WP-CD-Deploy-RFC
Description:                                DeployWordPress
S3Bucket:                                   BUCKET_NAME
S3Key:                                      wordpress.zip
S3BundleType:                               zip
CodeDeployApplicationName:                  WordPress
CodeDeployDeploymentGroupName:              WordPress
CodeDeployIgnoreApplicationStopFailures:    false
RevisionType:                               S3



VpcId:                                      VPC_ID
Name:                                       WP-CD-Deploy-Op
TimeoutInMinutes:                           60
```

c. Klik Kirim setelah selesai.

Validasi Penerapan Aplikasi

Arahkan ke titik akhir (LoadBalancerCName) penyeimbang beban yang dibuat sebelumnya, dengan jalur yang diterapkan:/. WordPress WordPress Misalnya:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

Anda akan melihat halaman seperti ini:

Meruntuhkan Penerapan Ketersediaan Tinggi

Untuk meruntuhkan penerapan, Anda mengirimkan Delete Stack CT terhadap tumpukan HA Two-Tier, dan bucket S3, dan Anda dapat meminta agar snapshot RDS dihapus (mereka dihapus secara otomatis setelah sepuluh hari, tetapi biayanya sedikit sementara di sana). Kumpulkan tumpukan IDs untuk tumpukan HA dan ember S3 lalu ikuti langkah-langkah ini. Lihat Tumpukan | Hapus.

Lampiran: Kuesioner orientasi SALZ

Topik

- Ringkasan penyebaran
- Pertimbangan arsitektur lingkungan
- Peringatan Pemantauan Zona Pendaratan Akun Tunggal
- Jendela Pemeliharaan
- Langkah Berikutnya

Ini adalah beberapa informasi yang perlu Anda pikirkan sebelum melakukan onboarding akun.

Ringkasan penyebaran

Deskripsi deployment. Misalnya:

- Akun ini adalah untuk penyebaran Line-of-Business aplikasi (sebagai lawan dari penyebaran aplikasi Produk).
- Penyebaran melibatkan ARP berskala otomatis (proxy terbalik yang diautentikasi) dalam subnet publik atau DMZ akun.
- Server web dan aplikasi akan digunakan dalam subnet pribadi akun.

- Instans RDS (Amazon Relational Database Service) juga akan digunakan dalam Subnet pribadi akun.
- Server (ARP, web, aplikasi, database, load balancer, dll.) Dipisahkan ke dalam kelompok keamanan yang berbeda.
- Akun tersebut memerlukan desain HA (ketersediaan tinggi) yang tersebar di seluruh zona ketersediaan (AZs) yaitu “Multi-AZ”.

Pertimbangan arsitektur lingkungan

Pertimbangkan kriteria berikut dalam memutuskan cara mengkonfigurasi lingkungan dan arsitektur Anda.

- Apakah pusat data virtual Anda akan terhubung kembali ke jaringan perusahaan Anda?
  - Apakah Anda memiliki AWS DirectConnect layanan yang sudah ada atau Anda memerlukan DirectConnect layanan baru?
  - Apakah Anda memiliki koneksi VPN yang sudah ada atau Anda memerlukan layanan VPN baru?
- Berapa rentang blok CIDR yang tersedia dari alamat internal yang dapat Anda alokasikan? (/16 direkomendasikan, tidak boleh tumpang tindih rentang jaringan perusahaan)
- Apakah pusat data virtual Anda memerlukan akses internet?
- Wilayah mana yang ingin Anda gunakan? (Sydney/N. Virginia/Dublin)
- Apakah Anda memerlukan subnet Layanan Bersama untuk meng-host aplikasi yang memiliki konektivitas ke semua subnet lainnya?
- Apa divisi organisasi Anda yang ingin Anda hosting sebagai subnet terpisah. Untuk masing-masing:
  - Konektivitas apa ke subnet lain yang Anda butuhkan?
  - Apakah subnet memerlukan akses Internet?
  - Apakah ada batasan penerapan aplikasi untuk subnet itu?
  - Apakah ada persyaratan jaringan khusus untuk subnet itu?
- Apakah Anda ingin lingkungan and/or pengujian pengembangan yang terpisah? (Akan mencakup duplikat layanan bersama untuk akses kapan saja)
- Apa persyaratan cadangan snapshot Anda?
- Apakah Anda memiliki proses pemeliharaan atau jendela tambalan yang ingin Anda simpan?
- Apa persyaratan pendaftaran domain Anda?

- Apakah Anda memiliki persyaratan masuk tunggal? (misalnya, AD, LDAP)
- Apa sistem operasi yang Anda harapkan secara keseluruhan dan persyaratan kapasitas yang diantisipasi?

Peringatan Pemantauan Zona Pendaratan Akun Tunggal

AMS menyediakan cara bagi Anda untuk diperingatkan secara langsung (versus mendapatkan pemberitahuan layanan AMS) untuk peringatan pemantauan tertentu. Untuk mendaftar, pastikan Cloud Architect (CA atau Cloud Service Delivery Manager (CSDM) Anda menerima informasi ini:

Direct Alerts Email: Ini adalah alamat email yang Anda ingin AMS untuk mengirim peringatan berbasis sumber daya tertentu. Untuk detail peringatan yang dikirim langsung ke email, lihat Peringatan dari Pemantauan Dasar di AMS di Panduan Pengguna AMS untuk Zona Pendaratan Akun Tunggal. Untuk informasi selengkapnya tentang pemantauan AMS, lihat Manajemen Pemantauan di Panduan Pengguna AMS untuk Zona Pendaratan Akun Tunggal.

Jendela Pemeliharaan

Anda akan ingin membuat jendela pemeliharaan yang mempertimbangkan kebutuhan aplikasi yang berbeda, berbeda Wilayah AWS, dan periode stres yang berbeda. Jendela pemeliharaan Anda adalah saat AMS akan menerapkan patching. Berikut adalah beberapa pedoman:

- Untuk membatasi dampak pada pengguna, rencanakan jendela pemeliharaan Anda sesuai dengan AWS Region tempat lingkungan Anda digunakan.
- Jadwalkan jendela di luar jam kerja reguler dan kapan lalu lintas paling sedikit diharapkan di server produksi.
- Biasanya, tumpukan infrastruktur memerlukan pembaruan bulanan.
- Jadwalkan jendela pemeliharaan setidaknya selama 300 menit. Penambalan sistem operasi membutuhkan waktu 60-90 menit, penambalan tumpukan infrastruktur membutuhkan waktu 180-300 menit.

Langkah Berikutnya

Tim orientasi AMS akan membantu Anda dalam setiap langkah orientasi akun Anda ke AMS. Ini adalah persyaratan orientasi:

- Menyediakan yang baru Akun AWS untuk digunakan untuk AMS dan memberikan Akun AWS ID.

- Mendaftar untuk tingkat Support yang diinginkan.
- Buat peran IAM lintas akun untuk memberikan akses akun penyediaan AMS dan berikan nama peran ke AMS.
- Tambahkan akun 753102745277 sebagai Entitas Tepercaya.

Lampiran: Aturan klaim ActiveDirectory Federation Services (ADFS) dan pengaturan SAMP

Untuk step-by-step petunjuk terperinci tentang cara menginstal dan mengonfigurasi AD FS, lihat Mengaktifkan Federasi ke AWS Menggunakan Windows Active Directory, ADFS, dan SAMP 2.0.

Konfigurasi aturan klaim ADFS

Jika Anda sudah memiliki implementasi ADFS, konfigurasikan berikut:

- Mengandalkan kepercayaan partai
- Aturan klaim

Langkah-langkah aturan kepercayaan dan klaim pihak yang mengandalkan diambil dari Mengaktifkan Federasi ke AWS Menggunakan Windows Active Directory, AD FS, dan blog SAMP 2.0

- Aturan klaim:
  - Nameid: Konfigurasi per posting blog
  - RoleSessionName: Konfigurasikan sebagai berikut
    - Nama aturan klaim: **`RoleSessionName`**
    - Toko atribut: **`Active Directory`**
    - Atribut LDAP: **`SAM-Account-Name`**
    - Jenis Klaim Keluar: **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`**
    - Dapatkan Grup AD: Konfigurasi per posting blog
    - Klaim peran: Konfigurasikan sebagai berikut

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-", "arn:aws:iam::$1:saml-provider/
customer-readonly-saml,arn:aws:iam::$1:role/"));
```

Konsol web

Anda dapat mengakses konsol Web AWS dengan menggunakan tautan di bawah ini menggantikan *[ADFS-FQDN]* FQDN implementasi ADFS Anda.

https://*[ADFS-FQDN]*/.aspx adfs/ls/IdpInitiatedSignOn

Departemen TI Anda dapat menerapkan tautan di atas ke populasi pengguna melalui Kebijakan Grup.

Akses API dan CLI dengan SAMP

Cara mengkonfigurasi akses API dan CLI dengan SAMP.

Paket python bersumber dari posting blog di bawah ini:

- NTLM: Cara Menerapkan API Federasi dan Akses CLI Menggunakan SAMP 2.0 dan AD FS
- Formulir: Cara Menerapkan Solusi Umum untuk API/CLI Akses Federasi Menggunakan SAMP 2.0
- PowerShell: Cara Mengatur Akses API Federasi ke AWS dengan Menggunakan Windows PowerShell

Konfigurasi skrip

1. Menggunakan Notepad ++, ubah wilayah default ke wilayah yang benar
2. Menggunakan Notepad ++, nonaktifkan verifikasi SSL untuk lingkungan pengujian dan dev
3. Menggunakan Notepad ++, konfigurasikan idpentryurl

   ```
   https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?
   loginToRp=urn:amazon:webservices
   ```

Konfigurasi Windows

Petunjuk di bawah ini adalah untuk paket python. Kredensi yang dihasilkan akan berlaku selama 1 jam.

1. Unduh dan instal python (2.7.11)
2. Unduh dan instal alat AWS CLI

3. Instal AMS CLI:

   a. Unduh file zip yang dapat didistribusikan AMS yang disediakan oleh manajer pengiriman layanan cloud (CSDM) Anda dan unzip.

      Beberapa direktori dan file tersedia.

   b. Buka Managed Cloud Distributables -> CLI -> Windows atau Managed Cloud Distributables -> CLI -> Linux/macOS direktori, tergantung pada sistem operasi Anda, dan:

      Untuk Windows, jalankan penginstal yang sesuai (metode ini hanya berfungsi pada sistem Windows 32 atau 64 bit):

      - 32 Bit: ManagedCloud API_x86.msi
      - 64 Bit: ManagedCloud API_x64.msi

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

   c. Jika kredensi perusahaan Anda digunakan melalui federasi dengan AWS (konfigurasi default AMS), Anda harus menginstal alat manajemen kredensi yang dapat mengakses layanan federasi Anda. Misalnya, Anda dapat menggunakan AWS Security Blog Cara Menerapkan API Federasi dan Akses CLI Menggunakan SAMP 2.0 dan AD FS untuk bantuan mengonfigurasi alat manajemen kredensi Anda.

   d. Setelah instalasi, jalankan `aws amscm help` dan `aws amsskms help` untuk melihat perintah dan opsi.

4. Unduh skrip SAMP yang diperlukan

   Unduh ke c:\aws\scripts

5. Unduh PIP

   Unduh ke c:\aws\downloads

6. Menggunakan PowerShell, instal PIP

   <pythondir>. \ python.exe c:\aws\downloads\get -pip.py

7. Menggunakan PowerShell, instal modul boto

   <pythondir\ scripts>pip instal boto

8. Menggunakan PowerShell, menginstal modul permintaan

   permintaan<pythondir\ scripts> pemasangan pip

9. Menggunakan PowerShell, menginstal modul keamanan permintaan

   <pythondir\ scripts>permintaan pemasangan pip [keamanan]

10. Menggunakan PowerShell, instal modul beautifulsoup

    <pythondir\ scripts>pip install beautifulsoup4

11. Menggunakan PowerShell, buat folder bernama .aws di profil pengguna (%userprofile%\ .aws)

    mkdir .aws

12. Menggunakan PowerShell, buat file kredensi di folder.aws

    Kredensi Baru-Item -type file —force

    File kredensial tidak boleh memiliki ekstensi file

    Nama file harus semua huruf kecil dan memiliki kredenal nama

13. Buka file kredensil dengan notepad dan tempel di data berikut, tentukan wilayah yang benar

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

14. Menggunakan PowerShell, skrip SAMP dan logon

    <pythondir>. \ python.exe c:\aws\scripts\samlapi.py

    Nama Pengguna: [NAMA PENGGUNA] @upn

    Pilih peran yang ingin Anda asumsikan

Konfigurasi Linux

Kredensi yang dihasilkan akan berlaku selama 1 jam.

1. Menggunakan WinSCP, transfer skrip SAMP
2. Menggunakan WinSCP, transfer sertifikat Root CA (abaikan untuk pengujian dan dev)
3. Tambahkan ROOT CA ke sertifikat root tepercaya (abaikan untuk pengujian dan dev)

   $ openssl x509 -inform der -in [certname] .cer -out certificate.pem (abaikan untuk pengujian dan dev)

   Tambahkan konten certificate.pem ke akhir file/etc/ssl/certs/ca-bundle.crt ((abaikan untuk test dev)
4. Buat folder.aws di rumah/ec2-user 5

   ```
   [default]
   output = json
   region = us-east-1
   aws_access_key_id =
   aws_secret_access_key =
   ```
5. Menggunakan WinSCP, transfer file kredensial ke folder.aws
6. Instal modul boto

   $ sudo pip instal boto
7. Instal modul permintaan

   Permintaan instal $ sudo pip
8. Instal modul beautifulsoup

   $ sudo pip instal beautifulsoup4
9. Salin skrip ke rumah/ec2-user

   Tetapkan izin yang diperlukan

   Jalankan skrip: samlapi.py

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir AMS.

- Versi API: 2019-05-21
- Pembaruan dokumentasi terbaru: 23 September 2025

Ubah	Deskripsi	Tanggal
Jenis perubahan yang diperbarui untuk penskalaa n otomatis titik akhir di SageMaker AI di bagian FAQ AWS Managed Services	Gunakan AMS SSP untuk menyediakan Amazon SageMaker AI di akun AMS Anda. Kirim RFC dengan Manajemen | Komponen tumpukan lanjutan | Identity and Access Management (IAM) | Perbarui entitas atau kebijakan (diperlukan tinjauan) jenis perubahan (ct-27tuth19k52b4) untuk meningkatkan izin penskalaan otomatis sementara, atau secara permanen, karena penskalaan otomatis memerlukan akses permisif pada layanan. CloudWatch	September 25, 2025
Referensi tipe perubahan yang tepat	Buat, Ubah, atau Hapus Grup Keamanan. Untuk menambahkan pengguna: Kirim RFC menggunakan Manajemen | Directory Service | Pengguna dan grup | Tambahkan pengguna ke grup [ct-24pi85mjtza8k] dan Untuk menghapus pengguna: Kirim RFC menggunakan Manajemen | Directory Service | Pengguna dan grup | Hapus pengguna dari grup [ct-2019s9y3nfml4]	Agustus 08, 2025
Tautan TOC dihapus	Tautan AWS Glosarium TOC dihapus.	Agustus 08, 2025

Ubah	Deskripsi	Tanggal
Menambahkan tautan untuk panduan resep	Siapkan tagihan konsolidasan—tautkan akun baru ke akun Pembayar.	Mei 08, 2025
Instruksi yang diperbarui untuk mengaktifkan akses IAM ke Konsol Manajemen AWS	Mengklarifikasi instruksi untuk mengaktifkan akses IAM ke. Konsol Manajemen AWS	Aktifkan akses IAM ke konsol AWS
Jumlah antarmuka virtual transit yang diizinkan yang diperbarui pada koneksi khusus Direct Connect	Koneksi khusus Direct Connect sekarang memiliki batas 4 antarmuka virtual transit per koneksi	Menghubungkan Direct Connect ke Transit Gateway
Tingkatkan kata-kata.	Ditentukan bahwa “hanya digunakan sebagai daftar “Tolak” "harus menyertakan “Izinkan Semua” untuk memastikan pemantauan AMS dan operasi manajemen.	Konfigurasi jaringan
Informasi tambahan tentang penggunaan AMS CLI.	“Menambahkan catatan bahwa `--region` opsi mungkin diperlukan untuk beberapa perintah CLI”	Instal AMS CLIs
Diperbarui: Judul Bab untuk konsistensi dan pembacaan, memindahkan beberapa sub-bagian topik ke bagian yang lebih tepat	“Mode untuk manajemen perubahan” adalah judul baru untuk “Manajemen perubahan”	Ubah mode manajemen
Konten diperbarui	Mode AMS yang sebelumnya dikenal sebagai “Mode Manajemen Ubah” atau “Mode CM Standar” sekarang dikenal sebagai “mode RFC.” Bagian mode telah diperluas.	Modus RFC.

Ubah	Deskripsi	Tanggal
Konten diperbarui	Mode AMS yang sebelumnya dikenal sebagai “Mode Manajemen Ubah” atau “Mode CM Standar” sekarang dikenal sebagai “mode RFC.” Bagian mode telah dipersingkat dan ditautkan ke bagian Panduan Pengguna Lanjutan AMS tentang mode yang ditambahkan.	Mode AMS.
MALZ: Diagram arsitektur jaringan yang diperbarui	Arsitektur akun jaringanm	16 Juni 2022
Memindahkan daftar topik ke paragraf pembuka di bawah	AWS Managed Services Onboarding Pendahuluan	16 Juni 2022
Konten yang diperbarui, inisiatif bahasa inklusif	“Akun manajemen” bukan “Akun induk.	Peran pengguna IAM di AMS, Bagian “Contoh kebijakan”
Konten yang diperbarui, nama peran akun Alat	Nama peran yang diperbarui CustomerMigrationAccessRole ke AWSManagedServicesMigrationRole.	AWS Layanan Migrasi Aplikasi (AWS MGN)
SALZ: Default manajemen kontinuitas	Tautan yang diperbarui dan menghapus informasi usang dari Tag VPC dan default	28 Februari 2022

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.