Informações avançadas de integração da conta do AMS

Guia de integração avançada do AMS

Versão September 25, 2025

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

Guia de integração avançada do AMS: Informações avançadas de integração da conta do AMS

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

As marcas comerciais e o visual comercial da Amazon não podem ser usados em conexão com nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa causar confusão entre os clientes ou que deprecie ou desacredite a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

Table of Contents

Introdução ao AWS Managed Services Onboarding 1
Aprendendo sobre o AMS 1
Principais termos 2
Modos AMS 9
Modos e aplicativos ou cargas de trabalho do AMS 9
Orientação prescritiva pós-conta do AMS 18
O que fazemos, o que não fazemos 18
Gerenciamento de tráfego de saída do AMS 19
Funções usuário do IAM 20
MALZ: funções de usuário padrão do IAM 21
SALZ: Função de usuário padrão do IAM 34
Regras de firewall de acesso padrão 42
Portas de instância do Linux Stack 42
Portas de instância do Windows Stack 43
Gerenciamento de serviços 44
Governança de contas 44
Início do serviço 45
Gestão do relacionamento com o cliente (CRM) 45
Processo de CRM 46
Reuniões de CRM 47
Organizações de reuniões de CRM 48
Relatórios mensais de CRM 49
Otimização de custo 50
Estrutura de otimização de custos 50
Matriz de responsabilidade de otimização de custos 53
Horário de atendimento 55
Como obter ajuda 56
Modos de gerenciamento de alterações 57
Visão geral dos modos 58
Tipos de modos e contas no AMS 59
Modos e aplicativos ou cargas de trabalho do AMS 62
Casos de uso do mundo real para modos AMS 71
Modo RFC 74
Saiba mais sobre RFCs 75

Quais são os tipos de mudança? ... 115
Solução de problemas de erros de RFC ... 128
Modo de mudança direta ... 139
Introdução ao modo Direct Change ... 140
Segurança e conformidade ... 142
Gerenciamento de alterações no modo Direct Change ... 148
Criação de pilhas usando o modo Direct Change ... 150
Casos de uso do Modo de Mudança Direta ... 153
Modo de desenvolvedor ... 154
Começando com o modo Desenvolvedor ... 155
Segurança e conformidade ... 157
Gerenciamento de alterações ... 159
Provisionar infraestrutura ... 164
Controles de detecção ... 165
Registro, monitoramento e gerenciamento de eventos ... 165
Gerenciamento de incidentes ... 165
Gerenciamento de patches ... 166
Gerenciamento de continuidade ... 166
Gerenciamento de segurança e acesso ... 167
Modo de provisionamento de autoatendimento no AMS ... 167
Introdução ao modo SSP no AMS ... 168
Amazon API Gateway ... 168
Alexa for Business ... 170
Amazon AppStream 2.0 ... 171
Amazon Athena ... 174
Amazon Bedrock ... 175
Amazon CloudSearch ... 176
Amazon CloudWatch Synthetics ... 177
Amazon Cognito ... 179
Amazon Comprehend ... 181
Amazon Connect ... 182
Amazon Data Firehose ... 184
DevOpsGuru da Amazon ... 185
Amazon DocumentDB (compatível com MongoDB) ... 186
Amazon DynamoDB ... 187
Amazon Elastic Container Registry ... 188

EC2 Image Builder 189
Amazon ECS em AWS Fargate 191
Amazon EKS em AWS Fargate 194
Amazon EMR 197
Amazon EventBridge 200
Amazon Forecast 202
Amazon FSx 205
Amazon FSx para OpenZFS 207
Amazon FSx para NetApp ONTAP 208
Amazon Inspector Classic 210
Amazon Kendra 211
Amazon Kinesis Data Streams 212
Amazon Kinesis Video Streams 213
Amazon Lex 214
Amazon MQ 215
Amazon Managed Service for Apache Flink 216
Amazon Managed Streaming for Apache Kafka 217
Amazon Managed Service para Prometheus 219
Amazon Personalize 220
Amazon QuickSight 222
Amazon Rekognition 224
SageMaker IA da Amazon 225
Amazon Simple Email Service 229
Amazon Simple Workflow Service 230
Amazon Textract 231
Amazon Transcribe 232
Amazon WorkSpaces 233
Serviços de código AMS 235
AWS Amplify 238
AWS AppSync 239
AWS App Mesh 240
AWS Audit Manager 241
AWS Batch 242
AWS Certificate Manager 244
Autoridade de Certificação Privada da AWS 245
AWS CloudEndure 248

AWS CloudHSM 249
AWS CodeBuild 251
AWS CodeCommit 252
AWS CodeDeploy 254
AWS CodePipeline 255
AWS Compute Optimizer 257
AWS DataSync 258
AWS Device Farm 259
AWS Elastic Disaster Recovery 260
AWS Elemental MediaConvert 262
AWS Elemental MediaLive 262
AWS Elemental MediaPackage 264
AWS Elemental MediaStore 265
AWS Elemental MediaTailor 266
AWS Global Accelerator 267
AWS Glue 267
AWS Lake Formation 269
AWS Lambda 270
AWS License Manager 272
AWS Migration Hub 273
AWS Outposts 273
AWS Resilience Hub 274
AWS Secrets Manager 275
AWS Security Hub CSPM 278
AWS Service Catalog AppRegistry 279
AWS Shield 280
AWS Snowball Edge 281
AWS Step Functions 283
AWS Systems Manager Armazenamento de parâmetros 284
AWS Systems Manager Automation 285
AWS Transfer Family 289
AWS Transit Gateway 290
AWS WAF 291
AWS Well-Architected Tool 292
AWS X-Ray 293
VM Import/Export 294

Modo gerenciado pelo cliente ... 295
Introdução ao modo Gerenciado pelo Cliente ... 296
AMS e AWS Service Catalog ... 296
Introdução ao Service Catalog ... 297
Service Catalog no AMS antes de você começar ... 297
Integração do AMS Multi-Account Landing Zone (MALZ) ... 302
Arquitetura de rede MALZ ... 302
Sobre a arquitetura de rede de landing zone com várias contas ... 302
Escolhendo um único MALZ ou vários MALZs ... 304
Contas de várias contas da Landing Zone ... 310
MALZ: Integração da conta principal ... 344
Crie uma AWS conta principal de landing zone com várias contas ... 345
Crie uma função do IAM para que o AMS acesse sua conta ... 346
Proteja a nova conta com autenticação multifator (MFA) para o usuário root ... 348
Inscreva-se AWS Marketplace para EPS ... 348
Configurar redes ... 349
Configurar o gerenciamento de acesso ... 352
MALZ: Integração de conta de aplicativo ... 358
Solicitando uma nova conta de aplicativo ... 358
Configurando o Active Directory para federar o acesso às funções do AMS IAM ... 360
Configurando a rede com a nova conta do aplicativo ... 363
Configurando adicionais VPCs na conta do aplicativo ... 365
Apêndice: lista de consideração de integração da multi-account landing zone (MALZ) ... 365
Configuração da conta ... 366
Alertas de monitoramento de landing zone com várias contas do AMS ... 367
Network configuration ... 367
Configuração do Active Directory ... 368
Proteção de terminais da Trend Micro (EPS) ... 368
Acesso: Bastions, SSH e RDP ... 369
Federação ... 370
Integração do AMS Single-Account Landing Zone (SALZ) ... 371
Processo de integração do AMS SALZ ... 371
Arquitetura de rede SALZ ... 372
Serviços compartilhados de landing zone com conta única do AMS ... 373
SALZ: Crie uma nova AWS conta para AMS ... 374
Crie um Conta da AWS ... 374

Configurar o faturamento consolidado — vincular a nova conta à conta do pagador 377
Configure seu Conta da AWS para acesso ao AMS 378
Inscreva-se AWS Marketplace para EPS 380
Inscreva-se AWS Marketplace para CentOS 7.6 381
Proteja a nova conta com autenticação multifator (MFA) para o usuário root 381
SALZ: Configure a rede 382
Aloque espaço IP para seu ambiente AMS 382
Estabeleça conectividade de rede privada com a AWS 383
Configure seu Firewall 385
Opções do AMS Bastion durante a migração/integração de aplicativos 385
SALZ: Configurar o gerenciamento de acesso 386
Estabeleça uma relação de confiança do Active Directory (AD) 387
Federe seu Active Directory com as funções do AMS AWS Identity and Access Management 393
SALZ: Configurações padrão 399
Segurança de terminais (EPS) 399
Grupos de segurança 404
EC2 Perfil de instância do IAM 409
Padrões de métricas monitoradas 417
Padrões de retenção e rotação de registros 434
Padrões de gerenciamento de continuidade 435
Padrões de correção 436
Validar o serviço AMS (SALZ) 438
Encontre as configurações da conta 438
Como encontrar um ID de instância ou endereço IP 442
Nomes de bastiões compatíveis com DNS 445
Encontrando endereços IP do Bastion 446
EC2 instâncias: Criação 447
Acesso, solicitação 456
Outros | Outro RFC, criação (CLI) 463
Qualquer pilha: excluindo, reiniciando, iniciando, parando 465
Exemplos de acesso 477
Relatar um incidente 487
Criando uma solicitação de serviço 490
Etapas de pós-integração 493
Tutoriais 493

Apêndice: questionário de integração da SALZ 521
Resumo da implantação 521
Considerações sobre a arquitetura do ambiente 521
Alertas de monitoramento da zona de pouso com uma única conta 522
Janela de manutenção 523
Próximas etapas 523
Apêndice: Regra de declaração dos Serviços de ActiveDirectory Federação (ADFS) e configurações de SAML 524
Configurações de regras de declaração do ADFS 524
Console web 525
Acesso à API e à CLI com SAML 525
Configuração do script 525
Configuração do Windows 525
Configuração do Linux 528
Histórico do documentos 529
..... dxxxii

Introdução ao AWS Managed Services Onboarding

Bem-vindo ao AWS Managed Services (AMS). O AMS é um serviço corporativo que fornece gerenciamento contínuo da sua infraestrutura da AWS. Este guia foi desenvolvido para ajudar você a começar a usar o AMS, incluindo como configurar uma nova conta para o AMS, configurar a rede e o acesso ao AMS e validar sua configuração de integração.

Ele é destinado a administradores de TI encarregados de preparar e executar as tarefas necessárias para integrar o serviço AMS a uma nova conta da AWS. A integração do serviço AMS exige privilégios especiais para configurar relações de confiança do Active Directory e concluir outras tarefas em nível de rede. Para obter ajuda na decisão de usar contas de zona de destino com várias contas ou contas de zona de destino com uma única conta, acesse Como escolher um MALZ único ou múltiplo. MALZs

> **Important**
>
> Este guia está dividido em duas partes após esta introdução: uma para contas de zona de pouso com várias contas e outra para contas de zona de destino com uma única conta. A integração é bem diferente para os dois. Acesse a seção do guia que se aplica à sua situação.

Tópicos

- Aprendendo sobre o AMS
- Termos-chave do AMS
- Modos AMS
- Orientação prescritiva pós-conta do AMS
- O que fazemos, o que não fazemos
- Gerenciamento de tráfego de saída do AMS
- Função de usuário do IAM no AMS
- Regras de firewall de acesso padrão

Aprendendo sobre o AMS

Para entender melhor o AMS, consulte estas seções do Guia do Usuário do AMS:

- What Is AWS Managed Services apresenta o serviço AMS e descreve os principais recursos, operações e interfaces, bem como uma arquitetura típica de rede gerenciada pela AMS. Este capítulo também fornece informações sobre gerenciamento de acesso, incluindo como acessar seus recursos gerenciados pelo AMS e usar bastiões.
- Key Terms fornece definições e explicações para a terminologia do AMS.
- A compreensão dos padrões do AMS fornece os valores padrão que o AMS usa, incluindo os padrões para componentes básicos do ambiente, IAM e proxies EC2, métricas monitoradas, registros, segurança de endpoints (EPS), backups e patches.
- O Gerenciamento de Mudanças fornece detalhes sobre como as solicitações de mudança (RFCs) e tipos de alteração (CTs) funcionam e inclui exemplos do uso do AMS RFCs.
- Vários capítulos adicionais abordam o acesso ao console da AWS, o AMS CLI, o uso do sistema de gerenciamento de alterações do AMS, o AMS SKMS, segurança, solicitações de serviço, incidentes, monitoramento, registros, EPS, backups e gerenciamento de patches.

Para saber mais sobre a arquitetura de zonas de aterrissagem multicontas do AMS, consulte Arquitetura de rede de zonas de aterrissagem de várias contas

Para saber mais sobre a arquitetura de zona de pouso de conta única do AMS, consulte Arquitetura de rede de zona de pouso de conta única

Termos-chave do AMS

- AMS Advanced: Os serviços descritos na seção “Descrição do serviço” da documentação do AMS Advanced. Consulte a descrição do serviço.
- Contas avançadas do AMS: AWS contas que sempre atendem a todos os requisitos dos requisitos avançados de integração do AMS. Para obter informações sobre os benefícios do AMS Advanced, estudos de caso e para entrar em contato com um vendedor, consulte AWS Managed Services.
- Contas do AMS Accelerate: AWS contas que sempre atendem a todos os requisitos dos requisitos de integração do AMS Accelerate. Consulte Introdução ao AMS Accelerate.
- AWS Managed Services: AMS e/ou AMS Accelerate.
- Contas do AWS Managed Services: as contas do AMS e/ou contas do AMS Accelerate.
- Recomendação crítica: Uma recomendação emitida por AWS meio de uma solicitação de serviço informando que sua ação é necessária para se proteger contra possíveis riscos ou interrupções em seus recursos ou no. Serviços da AWS Se você decidir não seguir uma recomendação crítica até a data especificada, você é o único responsável por qualquer dano resultante de sua decisão.

- Configuração solicitada pelo cliente: qualquer software, serviço ou outras configurações que não estejam identificadas em:
  - Acelerar: configurações suportadas ou AMS Accelerate; Descrição do serviço.
  - AMS Advanced: configurações suportadas ou AMS Advanced; Descrição do serviço.
- Comunicação de incidentes: o AMS comunica um incidente a você ou você solicita um incidente ao AMS por meio de um incidente criado no Support Center for AMS Accelerate e no AMS Console for AMS. O console do AMS Accelerate fornece um resumo dos incidentes e solicitações de serviço no painel e links para o Support Center para obter detalhes.
- Ambiente gerenciado: as contas do AMS Advanced e/ou as contas do AMS Accelerate operadas pela AMS.

  Para o AMS Advanced, elas incluem contas de landing zone com várias contas (MALZ) e de landing zone com uma única conta (SALZ).
- Data de início do faturamento: No dia útil seguinte ao AWS recebimento das informações solicitadas no e-mail de integração do AWS Managed Services. O e-mail de integração do AWS Managed Services se refere ao e-mail enviado por AWS você para coletar as informações necessárias para ativar o AWS Managed Services em suas contas.

  Para contas inscritas posteriormente por você, a data de início do faturamento é o dia seguinte após o envio da Notificação de ativação do AWS Managed Services para a conta inscrita. Uma notificação de ativação do AWS Managed Services ocorre quando:

  1. Você concede acesso a uma AWS conta compatível e a entrega ao AWS Managed Services.
  2. O AWS Managed Services projeta e cria a conta do AWS Managed Services.
- Encerramento do serviço: você pode encerrar o AWS Managed Services para todas as contas do AWS Managed Services ou para uma conta específica do AWS Managed Services por qualquer motivo, fornecendo um aviso prévio de pelo AWS menos 30 dias por meio de uma solicitação de serviço. Na Data de Rescisão do Serviço, você pode:

  1. AWS entrega os controles de todas as contas do AWS Managed Services ou das contas especificadas do AWS Managed Services, conforme aplicável, para você, ou
  2. As partes removem as AWS Identity and Access Management funções que dão AWS acesso de todas as contas do AWS Managed Services ou das contas especificadas do AWS Managed Services, conforme aplicável.
- Data de rescisão do serviço: A data de rescisão do serviço é o último dia do mês civil após o final do período de notificação de rescisão obrigatório de 30 dias. Se o final do período de notificação

de rescisão exigido cair após o vigésimo dia do mês civil, a data de rescisão do serviço será o último dia do mês civil seguinte. A seguir estão exemplos de cenários para datas de rescisão.

  - Se o aviso de rescisão for fornecido em 12 de abril, o aviso de 30 dias terminará em 12 de maio. A data de término do serviço é 31 de maio.
  - Se um aviso de rescisão for fornecido em 29 de abril, o aviso de 30 dias terminará em 29 de maio. A data de término do serviço é 30 de junho.
- Provisão do AWS Managed Services: AWS disponibiliza para você e você pode acessar e usar o AWS Managed Services para cada conta do AWS Managed Services a partir da data de início do serviço.
- Encerramento de contas específicas do AWS Managed Services: você pode encerrar o AWS Managed Services de uma conta específica do AWS Managed Services por qualquer motivo, enviando um AWS aviso por meio de uma solicitação de serviço (“Solicitação de encerramento da conta AMS”).

Termos de gerenciamento de incidentes:

- Evento: Uma mudança em seu ambiente AMS.
- Alerta: sempre que um evento de um suporte AWS service (Serviço da AWS) excede um limite e dispara um alarme, um alerta é criado e um aviso é enviado para sua lista de contatos. Além disso, um incidente é criado na sua lista de incidentes.
- Incidente: uma interrupção não planejada ou degradação do desempenho do seu ambiente de AMS ou do AWS Managed Services que resulta em um impacto conforme relatado pelo AWS Managed Services ou por você.
- Problema: Uma causa raiz subjacente compartilhada de um ou mais incidentes.
- Resolução de incidentes ou Resolver um incidente:
  - O AMS restaurou todos os serviços ou recursos indisponíveis do AMS relacionados a esse incidente para um estado disponível, ou
  - O AMS determinou que pilhas ou recursos indisponíveis não podem ser restaurados para um estado disponível, ou
  - O AMS iniciou uma restauração de infraestrutura autorizada por você.
- Tempo de resposta do incidente: a diferença de tempo entre o momento em que você cria um incidente e o momento em que o AMS fornece uma resposta inicial por meio do console, e-mail, centro de serviços ou telefone.

- Tempo de resolução do incidente: a diferença de tempo entre o momento em que você ou o AMS criam um incidente e o momento em que o incidente é resolvido.
- Prioridade do incidente: como os incidentes são priorizados pelo AMS ou por você como Baixa, Média ou Alta.
  - Baixo: um problema não crítico com seu serviço AMS.
  - Médio: um serviço da AWS em seu ambiente gerenciado está disponível, mas não está funcionando conforme o esperado (de acordo com a descrição do serviço aplicável).
  - Alto: (1) o console AMS ou um ou mais AMS APIs em seu ambiente gerenciado estão indisponíveis; ou (2) uma ou mais pilhas ou recursos do AMS em seu ambiente gerenciado estão indisponíveis e a indisponibilidade impede que seu aplicativo execute sua função.

  O AMS pode reclassificar os incidentes de acordo com as diretrizes acima.
- Restauração da infraestrutura: reimplantar pilhas existentes, com base em modelos de pilhas afetadas, e iniciar uma restauração de dados com base no último ponto de restauração conhecido, a menos que você especifique o contrário, quando a resolução de incidentes não for possível.

Termos de infraestrutura:

- Ambiente de produção gerenciado: uma conta de cliente na qual residem os aplicativos de produção do cliente.
- Ambiente gerenciado de não produção: uma conta de cliente que contém somente aplicativos que não são de produção, como aplicativos para desenvolvimento e teste.
- Pilha AMS: um grupo de um ou mais AWS recursos que são gerenciados pelo AMS como uma única unidade.
- Infraestrutura imutável: um modelo de manutenção de infraestrutura típico para grupos do Amazon EC2 Auto Scaling ASGs () em que componentes de infraestrutura atualizados (AWS na AMI) são substituídos em cada implantação, em vez de serem atualizados localmente. As vantagens da infraestrutura imutável são que todos os componentes permanecem em um estado síncrono, pois são sempre gerados a partir da mesma base. A imutabilidade é independente de qualquer ferramenta ou fluxo de trabalho para criar a AMI.
- Infraestrutura mutável: um modelo de manutenção de infraestrutura típico para pilhas que não são grupos do Amazon EC2 Auto Scaling e contêm uma única instância ou apenas algumas instâncias. Esse modelo representa mais de perto a implantação tradicional do sistema, baseada em hardware, em que um sistema é implantado no início de seu ciclo de vida e, em seguida, as atualizações são colocadas em camadas nesse sistema ao longo do tempo. Todas as atualizações

do sistema são aplicadas às instâncias individualmente e podem causar tempo de inatividade do sistema (dependendo da configuração da pilha) devido à reinicialização do aplicativo ou do sistema.

- Grupos de segurança: firewalls virtuais para sua instância para controlar o tráfego de entrada e saída. Os grupos de segurança atuam no nível da instância e não no nível da sub-rede. Portanto, cada instância em uma sub-rede em sua VPC pode ter um conjunto diferente de grupos de segurança atribuídos a ela.
- Acordos de nível de serviço (SLAs): parte dos contratos do AMS com você que definem o nível de serviço esperado.
- SLA indisponível e indisponível:
  - Uma solicitação de API enviada por você que resulta em um erro.
  - Uma solicitação de console enviada por você que resulta em uma resposta HTTP 5xx (o servidor é incapaz de realizar a solicitação).
  - Qualquer uma das AWS service (Serviço da AWS) ofertas que constituem pilhas ou recursos em sua infraestrutura gerenciada pela AMS está em um estado de “interrupção do serviço”, conforme mostrado no Service Health Dashboard.
  - A indisponibilidade resultante direta ou indiretamente de uma exclusão do AMS não é considerada na determinação da elegibilidade para créditos de serviço. Os serviços são considerados disponíveis, a menos que atendam aos critérios de indisponibilidade.
- Objetivos de nível de serviço (SLOs): parte dos contratos do AMS com você que definem metas de serviço específicas para os serviços do AMS.

Termos de aplicação de patches:

- Patches obrigatórios: atualizações de segurança críticas para resolver problemas que podem comprometer o estado de segurança do seu ambiente ou conta. Uma “atualização crítica de segurança” é uma atualização de segurança classificada como “crítica” pelo fornecedor de um sistema operacional compatível com a AMS.
- Patches anunciados versus lançados: Os patches geralmente são anunciados e lançados de acordo com um cronograma. Os patches emergentes são anunciados quando a necessidade do patch é descoberta e, geralmente, logo depois, o patch é lançado.
- Complemento de patch: correção baseada em tags para instâncias do AMS que aproveita a funcionalidade AWS Systems Manager (SSM) para que você possa marcar instâncias e fazer com que essas instâncias sejam corrigidas usando uma linha de base e uma janela que você configura.

- Métodos de patch:
  - Aplicação de patches no local: correção que é feita alterando as instâncias existentes.
  - Patching de substituição de AMI: patch que é feito alterando o parâmetro de referência da AMI de uma configuração existente EC2 de lançamento de grupo do Auto Scaling.
- Provedor de patches (fornecedores de sistemas operacionais, terceiros): os patches são fornecidos pelo fornecedor ou pelo órgão regulador do aplicativo.
- Tipos de patch:
  - Atualização crítica de segurança (CSU): uma atualização de segurança classificada como “Crítica” pelo fornecedor de um sistema operacional compatível.
  - Atualização importante (IU): uma atualização de segurança classificada como “Importante” ou uma atualização não relacionada à segurança classificada como “Crítica” pelo fornecedor de um sistema operacional compatível.
  - Outra atualização (OU): uma atualização do fornecedor de um sistema operacional compatível que não é uma CSU ou uma IU.
- Patches suportados: O AMS oferece suporte a patches em nível de sistema operacional. As atualizações são lançadas pelo fornecedor para corrigir vulnerabilidades de segurança ou outros bugs ou para melhorar o desempenho. Para obter uma lista das opções atualmente suportadas OSs, consulte Support Configurations.

Termos de segurança:

- Detective Controls: uma biblioteca de monitores criados ou habilitados pela AMS que fornecem supervisão contínua dos ambientes e cargas de trabalho gerenciados pelo cliente para configurações que não se alinham aos controles de segurança, operacionais ou do cliente e agem notificando os proprietários, modificando ou encerrando recursos de forma proativa.

Termos da solicitação de serviço:

- Solicitação de serviço: uma solicitação feita por você para uma ação que você deseja que o AMS execute em seu nome.
- Notificação de alerta: um aviso publicado pelo AMS em sua página de lista de solicitações de serviço quando um alerta do AMS é acionado. O contato configurado para sua conta também é notificado pelo método configurado (por exemplo, e-mail). Se você tiver tags de contato em suas instâncias/recursos e tiver fornecido consentimento ao seu gerente de prestação de serviços em

nuvem (CSDM) para notificações baseadas em tags, as informações de contato (valor-chave) na tag também serão notificadas para alertas automatizados do AMS.

- Notificação de serviço: um aviso do AMS publicado na sua página de lista de solicitações de serviço.

Termos diversos:

- Interface de serviços gerenciados da AWS: Para AMS: o console avançado do AWS Managed Services, a API do AMS CM e a Suporte API. Para o AMS Accelerate: o Suporte console e a Suporte API.
- Satisfação do cliente (CSAT): O AMS CSAT é informado por meio de análises profundas, incluindo classificações de correspondência de casos em cada caso ou correspondência quando fornecida, pesquisas trimestrais e assim por diante.
- DevOps: DevOps é uma metodologia de desenvolvimento que defende fortemente a automação e o monitoramento em todas as etapas. DevOps visa ciclos de desenvolvimento mais curtos, maior frequência de implantação e lançamentos mais confiáveis, reunindo as funções tradicionalmente separadas de desenvolvimento e operações em uma base de automação. Quando os desenvolvedores podem gerenciar as operações e as operações informam o desenvolvimento, questões e problemas são descobertos e resolvidos mais rapidamente, e os objetivos de negócios são alcançados com mais facilidade.
- ITIL: A Biblioteca de Infraestrutura de Tecnologia da Informação (chamada ITIL) é uma estrutura de ITSM projetada para padronizar o ciclo de vida dos serviços de TI. O ITIL é organizado em cinco estágios que abrangem o ciclo de vida do serviço de TI: estratégia do serviço, design do serviço, transição do serviço, operação do serviço e melhoria do serviço.
- Gerenciamento de serviços de TI (ITSM): um conjunto de práticas que alinha os serviços de TI às necessidades da sua empresa.
- Serviços de monitoramento gerenciados (MMS): O AMS opera seu próprio sistema de monitoramento, o Managed Monitoring Service (MMS), que consome eventos de AWS saúde e agrega dados da CloudWatch Amazon e dados de Serviços da AWS outros, notificando operadores do AMS (on-line 24 horas por dia, 7 dias por semana) sobre quaisquer alarmes criados por meio de um tópico do Amazon Simple Notification Service (Amazon SNS).
- Namespace: ao criar políticas do IAM ou trabalhar com Amazon Resource Names (ARNs), você identifica uma AWS service (Serviço da AWS) usando um namespace. Os namespaces são usados ao identificar ações e recursos.

Modos AMS

Use isso para ajudá-lo a selecionar o modo apropriado do AWS Managed Services (AMS) para hospedar seus aplicativos, com base na combinação desejada de flexibilidade e governança prescritiva para alcançar seus resultados comerciais.

O público-alvo dessas informações é:

- Equipes de clientes responsáveis pela estratégia e governança de sua landing zone. Essas informações ajudarão a equipe a estabelecer a base de uma landing zone gerenciada pela AMS, com os modos de AMS que eles gostariam de oferecer a seus clientes internos e externos.
- Proprietários de empresas e aplicativos encarregados de migrar seus aplicativos para o AMS. Essas informações ajudarão no planejamento da migração do aplicativo, com o modo AMS apropriado para migrate/host o aplicativo. Observe que o mesmo aplicativo pode ser hospedado em mais de um modo AMS durante diferentes fases do ciclo de vida do ciclo de vida do desenvolvimento de software (SDLC).
- Parceiros do AMS encarregados de orientar os clientes sobre as diferentes opções de criação e migração para o AMS.

Essas informações pressupõem que você já tenha tomado a decisão de utilizar o AMS para acelerar sua jornada para a nuvem. Consulte este paper em dois pontos de sua jornada de migração para a nuvem: primeiro, durante a fase inicial da configuração da plataforma gerenciada pela AMS. Segundo, quando você está fazendo a transição da fase básica para a fase de migração de sua jornada de adoção da nuvem, logo após a conclusão da integração ao AMS e você está se concentrando na governança e nas operações de aplicativos.

Modos e aplicativos ou cargas de trabalho do AMS

Considere os requisitos operacionais e de governança para seus aplicativos ao selecionar o modo certo, seja solicitando uma nova conta de aplicativo ou hospedando o aplicativo em uma conta de aplicativo existente. A seleção do modo AMS apropriado para cada aplicativo ou carga de trabalho depende dos seguintes fatores:

- O tipo de função do ciclo de vida do SDLC que o ambiente fornecerá (por exemplo, sandbox com mudanças não moderadas, UAT com algumas mudanças frequentes, produção com alterações mínimas e altamente regulamentada)
- As políticas de governança necessárias (aplicadas SCPs no nível da OU)

- Modelo operacional (se você quiser assumir a responsabilidade operacional ou terceirizá-la para a AMS)
- Os resultados comerciais desejados, como tempo para operar na nuvem e custo das operações.

> **Note**
>
> Para obter uma descrição dos tipos de modo por serviço do AMS, consulte Tipos de modos e contas no AMS.
> Para casos de uso reais dos diferentes modos, consulte Casos de uso do mundo real para modos AMS

A tabela a seguir descreve as principais considerações para os proprietários de aplicativos ajudarem a decidir sobre o modo AMS mais adequado. Os proprietários do aplicativo devem incluir uma fase de avaliação antes da migração do aplicativo para entender completamente qual modo se aplica ao aplicativo específico. Exemplo: Para aplicativos baseados em serviços nativos da nuvem ou arquitetura sem servidor, a melhor opção pode ser começar a criar e iterar no modo Desenvolvedor e implantar a infraestrutura final como código usando o modo AMS Managed — SSP. Nesse caso, a refatoração leve pode ser necessária para garantir que todos os CloudFormation modelos criados para implantação automatizada atendam às diretrizes de ingestão estabelecidas pela AMS. Além disso, todas as permissões do IAM precisam ser aprovadas pela AMS Security para garantir que sigam o modelo de menor privilégio.

O modo AMS selecionado para hospedar o aplicativo pode ajudar a permitir que você desenvolva o modelo operacional de nuvem desejado.

> **Note**
>
> Mais de um modelo operacional em nuvem pode existir em uma única zona de aterrissagem gerenciada pelo AMS com base nos diferentes modos do AMS selecionados para hospedar os aplicativos.

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
Prontidão operacional						
Registro, monitoramento e gerenciamento de eventos	AMS responsável por toda a infraestrutura gerenciada			Cliente responsável pelos serviços provisionados de autoatendimento (SSP)	Cliente responsável pelos recursos provisionados usando a função IAM de desenvolvedor fora do sistema AMS CM	Cliente responsável
Gerenciamento de continuidade	Responsabilidade do AMS de executar o plano de backup selecionado pelo cliente			Cliente responsável pelos serviços provisionados de autoatendimento (SSP)	Cliente responsável pelos recursos provisionados usando a função IAM de desenvolvedor fora do sistema AMS CM	
Gerenciamento de	Gerenciado pelo AMS por meio de confiança unidirecional do AD com			Não aplicável	Cliente responsáv	

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
acesso em nível de instância	domínio local. Requer infraestrutura gerenciada para ingressar no domínio AMS				el pelos recursos provisionados usando a função IAM de desenvolvedor fora do sistema AMS CM	
Gerenciamento de segurança e gerenciamento de acesso em nível de conta	Responsabilidade do AMS por todas as contas gerenciadas			AMS responsável por todas as contas gerenciadas	Cliente responsável pelos recursos provisionados usando a função IAM de desenvolvedor fora do sistema AMS CM	

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
Gerenciamento de patches	Responsabilidade do AMS por todas as contas gerenciadas			Cliente responsável pelos serviços provisionados de autoatendimento (SSP)	Cliente responsável pelos recursos provisionados usando a função IAM de desenvolvedor fora do sistema AMS CM	
Gerenciamento de alterações	Responsabilidade do AMS por todas as contas gerenciadas			Cliente responsável pelos serviços provisionados de autoatendimento (SSP)	Cliente responsável pelos recursos provisionados usando a função IAM de desenvolvedor fora do sistema AMS CM	

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
Gerenciamento de provisionamento	Prescritivo e padronizado para as opções de provisionamento oferecidas no AMS	Flexibilidade para usar diretamente a API de serviços da AWS para o AWS Service Catalog seguindo os padrões prescritivos da AMS	Flexibilidade para usar diretamente a API de serviços da AWS seguindo os padrões prescritivos da AMS	Flexibilidade para usar diretamente o serviço da AWS APIs para serviços SSP	Flexibilidade para usar diretamente a API de serviços da AWS para provisionamento	

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
Gerenciamento e auditoria de incidentes	AMS responsável por todas as contas gerenciadas				Cliente responsável pelos recursos provisionados usando a função de desenvolvedor IAM fora do AMS Change Management System	
GuardRails e infraestrutura compartilhada (rede) e estrutura de segurança	Prescritivo e padronizado, aproveitando as contas principais do AMS					Aproveitando as contas principais do AMS de forma flexível e personalizada
Prontidão de aplicação						

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
Refatoração de aplicativos	A refatoração da luz é necessária				A refatoração de luz é necessária (se provisionada usando o AMS Standard CM)	Não há necessidade de refatoração
Support para serviços da AWS	Limitado ao que é suportado pelo AMS					Não limitado
Considerações de negócios						
Tempo até a prontidão operacional	Três a seis meses			Mais de 6 meses, dependendo das competências operacionais de aplicativos do cliente		6 a 18 meses, dependendo da infraestrutura do cliente e das competências em operações de aplicativos
Custos	$$$$			$$$	$$	$

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
Exemplos de aplicação	Servidor web com pilha de 3 níveis, aplicativos com requisitos regulatórios e de conformidade			Servidor web usando API Gateway, aplicativo em contêiner que utiliza ECS/EKS	Iterando/ otimizando no aplicativo Data Lake que usa Lambda, Glue, Athena etc.	Descentralizado, accounts/ applications como sandbox, aplicativos gerenciados por terceiros

* Operations On Demand (OOD) tem uma oferta para clientes que usam o modo CM padrão para gerenciar suas alterações por meio de recursos dedicados. Para obter mais detalhes, consulte o catálogo de ofertas do Operations on Demand e fale com seu gerente de prestação de serviços em nuvem (CSDM).

> **Note**
>
> A comparação de preços entre o modo SSP e o modo Desenvolvedor pressupõe que os mesmos serviços da AWS sejam provisionados.

Comparando os modos AMS com os objetivos de negócios e de TI

Conforme mostrado, se você estiver procurando por um modelo de governança altamente controlado e padronizado para seus aplicativos, os modos Standard Change, AWS Service Catalog ou Direct Change gerenciados pela AMS são os mais adequados. Se você precisar de um modelo de governança personalizado com foco na inovação de aplicativos sem a necessidade de prontidão operacional, selecione o modo Gerenciado pelo Cliente. Com o modo Gerenciado pelo Cliente, pode levar mais tempo para operacionalizar seus aplicativos, pois você assume a responsabilidade de estabelecer pessoas, processos e ferramentas para dar suporte a recursos operacionais, como

gerenciamento de incidentes, gerenciamento de configuração, gerenciamento de provisionamento, gerenciamento de segurança, gerenciamento de patches etc.

Orientação prescritiva pós-conta do AMS

À medida que as organizações adotam operações e DevOps práticas distribuídas, há um conjunto básico de recursos operacionais que devem ser aplicados a todas as contas antes da implantação das cargas de trabalho para atender aos pilares da Well Architected.

Esse link baixa um arquivo ZIP contendo um documento do Word e um arquivo ZIP com scripts e exemplos. A Configuração Automatizada de Conta é um conjunto de scripts para automatizar, ou inicializar, a configuração de uma nova conta de aplicativo.

Depois que uma nova conta é vendida e antes da implantação de qualquer carga de trabalho, para prepará-la do ponto de vista operacional, de segurança e gerenciamento, você configura planos de backup padrão, janelas de patch e criptografia (e muito mais). Para ajudar a melhorar a agilidade, a consistência e a capacidade de resposta da configuração da conta do aplicativo, o exemplo de “Como fazer” a seguir é fornecido para sua referência.

Configuração automatizada da conta.

O que fazemos, o que não fazemos

O AMS oferece uma abordagem padronizada para a implantação da infraestrutura da AWS e fornece o gerenciamento operacional contínuo necessário. Para obter uma descrição completa das funções, responsabilidades e serviços suportados, consulte Descrição do serviço.

> **Note**
>
> Para solicitar que o AMS forneça um serviço adicional da AWS, registre uma solicitação de serviço. Para obter mais informações, consulte Fazer solicitações de serviço.

- O que fazemos:

  Depois de concluir a integração, o ambiente AMS estará disponível para receber solicitações de mudança (RFCs), incidentes e solicitações de serviço. Sua interação com o serviço AMS gira em torno do ciclo de vida de uma pilha de aplicativos. As novas pilhas são ordenadas a partir de uma lista pré-configurada de modelos, lançadas em sub-redes específicas de nuvem privada virtual

(VPC), modificadas durante sua vida operacional por meio de solicitações de mudança (RFCs) e monitoradas para eventos e incidentes 24 horas por dia, 7 dias por semana.

As pilhas de aplicativos ativas são monitoradas e mantidas pelo AMS, incluindo a aplicação de patches, e não exigem nenhuma ação adicional durante a vida útil da pilha, a menos que seja necessária uma alteração ou que a pilha seja desativada. Os incidentes detectados pelo AMS que afetam a integridade e o funcionamento da pilha geram uma notificação e podem ou não precisar de sua ação para serem resolvidos ou verificados. Perguntas práticas e outras perguntas podem ser feitas enviando uma solicitação de serviço.

Além disso, o AMS permite que você habilite serviços compatíveis da AWS que não são gerenciados pelo AMS. Para obter informações sobre serviços compatíveis com AWS-AMS, consulte Modo de provisionamento de autoatendimento.

- O que NÃO fazemos:

  Embora o AMS simplifique a implantação de aplicativos fornecendo várias opções manuais e automatizadas, você é responsável pelo desenvolvimento, teste, atualização e gerenciamento de seu aplicativo. O AMS fornece assistência para solução de problemas de infraestrutura que afetam os aplicativos, mas o AMS não pode acessar ou validar suas configurações de aplicativos.

Gerenciamento de tráfego de saída do AMS

Por padrão, a rota com um CIDR de destino de 0.0.0.0/0 para sub-redes privadas e de aplicativos de clientes do AMS tem um gateway de tradução de endereços de rede (NAT) como destino. Os serviços TrendMicro e patches do AMS são componentes que devem ter acesso de saída à Internet para que o AMS possa fornecer seus serviços TrendMicro e que os sistemas operacionais possam obter atualizações.

O AMS suporta o desvio do tráfego de saída para a Internet por meio de um dispositivo de saída gerenciado pelo cliente, desde que:

- Ele atua como um proxy implícito (por exemplo, transparente).

  and

- Ele permite dependências HTTP e HTTPS do AMS (listadas nesta seção) para permitir a aplicação contínua de patches e a manutenção da infraestrutura gerenciada pelo AMS.

Alguns exemplos são:

- O gateway de trânsito (TGW) tem uma rota padrão apontando para o firewall local gerenciado pelo cliente pela conexão do AWS Direct Connect na conta de rede de zona de destino de várias contas.
- O TGW tem uma rota padrão apontando para um endpoint da AWS na VPC de saída da zona de destino de várias contas utilizando a AWS, apontando para um proxy gerenciado pelo cliente em outra conta PrivateLink da AWS.
- O TGW tem uma rota padrão apontando para um firewall gerenciado pelo cliente em outra conta da AWS, com conexão site-to-site VPN como anexo ao Multi-Account Landing Zone TGW.

O AMS identificou as dependências HTTP e HTTPS correspondentes do AMS e desenvolve e refina essas dependências continuamente. Consulte egressMgmt.zip. Junto com o arquivo JSON, o ZIP contém um README.

> **Note**
>
> - Essas informações não são abrangentes. Alguns sites externos obrigatórios não estão listados aqui.
> - Não use essa lista em uma lista de negação ou estratégia de bloqueio.
> - Essa lista serve como ponto de partida para um conjunto de regras de filtragem de saída, com a expectativa de que as ferramentas de geração de relatórios sejam usadas para determinar com precisão onde o tráfego real diverge da lista.

Para solicitar informações sobre como filtrar o tráfego de saída, envie um e-mail para seu CSDM: ams-csdm@amazon.com.

Função de usuário do IAM no AMS

Uma função do IAM é semelhante à de um usuário do IAM, pois é uma AWS identidade com políticas de permissão que determinam o que a identidade pode ou não fazer AWS. No entanto, em vez de ser exclusivamente associada a uma pessoa, o propósito do perfil é ser assumido por qualquer pessoa que precisar dele.

Atualmente, há uma função de usuário padrão do AMS`Customer_ReadOnly_Role`, para contas padrão do AMS e uma função adicional, `customer_managed_ad_user_role` para contas do AMS com o Active Directory gerenciado.

As políticas de função definem permissões CloudWatch e ações de log do Amazon S3, acesso ao console AMS, restrições de somente leitura para a maioria Serviços da AWS, acesso restrito ao console S3 da conta e acesso por tipo de alteração do AMS.

Além disso, `Customer_ReadOnly_Role` tem permissões mutativas de instâncias reservadas que permitem reservar instâncias. Ele tem alguns valores de economia de custos, então, se você sabe que precisará de um certo número de EC2 instâncias da Amazon por um longo período de tempo, pode ligar para elas APIs. Para saber mais, consulte Instâncias EC2 reservadas da Amazon.

> **Note**
>
> O objetivo de nível de serviço (SLO) do AMS para criar políticas personalizadas do IAM para usuários do IAM é de quatro dias úteis, a menos que uma política existente seja reutilizada. Se você quiser modificar a função de usuário do IAM existente ou adicionar uma nova, envie uma RFC IAM: Update Entity ou IAM: Create Entity, respectivamente.

Se você não estiver familiarizado com as funções do Amazon IAM, consulte Funções do IAM para obter informações importantes.

Zona de aterrissagem com várias contas (MALZ): Para ver as políticas de função de usuário padrão e não personalizadas da zona de pouso multiconta do AMS, consulte a seguir. MALZ: funções de usuário padrão do IAM

MALZ: funções de usuário padrão do IAM

Declarações de política JSON para as funções padrão de usuário multicontas do AMS na landing zone.

> **Note**
>
> As funções do usuário são personalizáveis e podem diferir de acordo com a conta. São fornecidas instruções sobre como encontrar sua função.

Esses são exemplos das funções de usuário padrão do MALZ. Para garantir que você tenha as políticas definidas de que precisa, execute o comando da AWS `get-role`ou faça login no console AWS Management -> IAM e escolha Roles no painel de navegação.

Funções principais da conta OU

Uma conta principal é uma conta de infraestrutura gerenciada pela MALZ. As contas principais da landing zone com várias contas do AMS incluem uma conta de gerenciamento e uma conta de rede.

Conta principal da OU: funções e políticas comuns

Role (Função)	Política ou políticas
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Política pública gerenciada pela AWS).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAcesso (política pública gerenciada pela AWS).
AWSManagedServicesChangeManagementRole (Versão da conta principal)	ReadOnlyAccess
	AWSSupportAcesso
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

Conta principal da OU: funções e políticas da conta de gerenciamento

Role (Função)	Política ou políticas
AWSManagedServicesBillingRole	AMSBillingPolítica (AMSBillingPolítica).
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Política pública gerenciada pela AWS).
AWSManagedServicesCaseRole	ReadOnlyAccess

Role (Função)	Política ou políticas
	AWSSupportAcesso (política pública gerenciada pela AWS).
AWSManagedServicesChangeManagementRole (Versão da conta de gerenciamento)	ReadOnlyAccess
	AWSSupportAcesso
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

Conta principal da OU: funções e políticas da conta de rede

Role (Função)	Política ou políticas
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Política pública gerenciada pela AWS).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAcesso (política pública gerenciada pela AWS).
AWSManagedServicesChangeManagementRole (Versão da conta de rede)	ReadOnlyAccess
	AWSSupportAcesso
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

Funções da conta do aplicativo

As funções da conta do aplicativo são aplicadas às contas específicas do seu aplicativo.

Conta de aplicativo: funções e políticas

Role (Função)	Política ou políticas
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Política pública gerenciada pela AWS).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAcesso (política pública gerenciada pela AWS). Essa política fornece acesso a todas as operações e recursos de suporte. Para obter informações, consulte Getting Started with AWS Support.
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess
	AWSSupportExemplo de acesso Essa política fornece acesso a todas as operações e recursos de suporte.
	AWSCertificateManagerFullAccess informações, (política pública gerenciada pela AWS)
	AWSWAFFullAccess informações, (política pública gerenciada pela AWS). Essa política concede acesso total aos recursos do AWS WAF.
	AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole (Versão da conta do aplicativo)	ReadOnlyAccess

Role (Função)	Política ou políticas
AWSManagedServicesAdminRole	AWSSupportAcesso (política pública gerenciada pela AWS). Essa política fornece acesso a todas as operações e recursos de suporte. Para obter informações, consulte Getting Started with AWS Support.
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AMSReservedInstancesPolicy
	AMSS3Política
	ReadOnlyAccess
	AWSSupportAcesso
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFullAcesso
	AMSS3Política
	AMSReservedInstancesPolicy

Exemplos de políticas

Exemplos são fornecidos para a maioria das políticas usadas. Para ver a ReadOnlyAccess política (que tem páginas longas, pois fornece acesso somente para leitura a todos os AWS serviços), você pode usar este link, se você tiver uma conta ativa da AWS:. ReadOnlyAccess Além disso, uma versão condensada está incluída aqui.

AMSBillingPolítica

`AMSBillingPolicy`

A nova função de cobrança pode ser usada pelo departamento de contabilidade para visualizar e alterar as informações de cobrança ou as configurações da conta na conta de gerenciamento. Para acessar informações como contatos alternativos, visualizar o uso dos recursos da conta, acompanhar seu faturamento ou até mesmo modificar suas formas de pagamento, você usa essa função. Essa nova função inclui todas as permissões listadas na página de ações do 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

Permissões para ver todos os tipos de alteração do AMS e o histórico dos tipos de alteração solicitados.

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

`AMSMasterAccountSpecificChangeManagementInfrastructurePolicy`

Permissões para solicitar o tipo de alteração Deployment | Managed landing zone | Management account | Create application account (com VPC).

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

`AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy`

Permissões para solicitar o tipo de alteração de Deployment | Managed landing zone | Networking account | Criar tabela de rotas de aplicativos.

AMSChangeManagementInfrastructurePolicy

`AMSChangeManagementInfrastructurePolicy`(para Gestão | Outros | Outros CTs)

Permissões para solicitar os tipos de alteração Gerenciamento | Outros | Outros | Criar e Gerenciamento | Outros | Outros | Atualizar.

AMSSecretsManagerSharedPolicy

`AMSSecretsManagerSharedPolicy`

Permissões para visualizar o segredo passwords/hashes compartilhado pelo AMS por meio de AWS Secrets Manager (por exemplo, senhas de infraestrutura para auditoria).

Permissões para criar um segredo password/hashes para compartilhar com o AMS. (por exemplo, chaves de licença para produtos que precisam ser implantados).

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`

Permissões para solicitar e visualizar todos os tipos de alteração do AMS e o histórico dos tipos de alteração solicitados.

AMSReservedInstancesPolicy

`AMSReservedInstancesPolicy`

Permissões para gerenciar instâncias EC2 reservadas da Amazon; para obter informações sobre preços, consulte Instâncias EC2 reservadas da Amazon.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
```

```
  "Sid": "AllowReservedInstancesManagement",
  "Effect": "Allow",
  "Action": [
   "ec2:ModifyReservedInstances",
   "ec2:PurchaseReservedInstancesOffering"
  ],
  "Resource": [
   "*"
  ]
 }]
}
```

AMSS3Política

`AMSS3Policy`

Permissões para criar e excluir arquivos de buckets Amazon S3 existentes.

> **Note**
>
> Essas permissões não concedem a capacidade de criar buckets do S3; isso deve ser feito com o tipo Deployment | Advanced stack components | S3 storage | Create change type.

JSON

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

AWSSupportAcesso

`AWSSupportAccess`

Acesso total Suporte a. Para obter informações, consulte Introdução ao Suporte. Para obter informações sobre o Premium Support, consulte Suporte.

JSON

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

AWSMarketplaceManageSubscriptions

`AWSMarketplaceManageSubscriptions`(Política pública AWS gerenciada)

Permissões para assinar, cancelar e visualizar AWS Marketplace assinaturas.

JSON

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

AWSCertificateManagerFullAccess

`AWSCertificateManagerFullAccess`

Acesso total AWS Certificate Manager a. Para obter mais informações, consulte AWS Certificate Manager.

`AWSCertificateManagerFullAccess`informações, (Política pública gerenciada pela AWS).

JSON

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

AWSWAFFullAcesso

`AWSWAFFullAccess`

Acesso total AWS WAF a. Para obter mais informações, consulte AWS WAF - Web Application Firewall.

`AWSWAFFullAccess`informação, (política pública AWS gerenciada). Essa política concede acesso total aos AWS WAF recursos.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "waf:*",
   "waf-regional:*",
   "elasticloadbalancing:SetWebACL"
```

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

ReadOnlyAccess

`ReadOnlyAccess`

Acesso somente de leitura a todos os AWS serviços e recursos no AWS console. Quando AWS inicia um novo serviço, o AMS atualiza a ReadOnlyAccess política para adicionar permissões somente de leitura para o novo serviço. As permissões atualizadas são aplicadas a todas as entidades principais às quais política estiver anexada.

Isso não concede a capacidade de fazer login em EC2 hosts ou hosts de banco de dados.

Se você tiver uma política ativa Conta da AWS, poderá usar esse link ReadOnlyAccesspara ver toda a ReadOnlyAccess política. Toda a ReadOnlyAccess política é muito longa, pois fornece acesso somente de leitura a todos. Serviços da AWS A seguir está um trecho parcial da ReadOnlyAccess política.

Zona de aterrissagem de conta única (SALZ): para ver as políticas de função de usuário padrão e não personalizadas da zona de destino de conta única do AMS, consulte a seguir. SALZ: Função de usuário padrão do IAM

SALZ: Função de usuário padrão do IAM

Declarações de política JSON para a função de usuário padrão da landing zone de conta única do AMS.

> **Note**
>
> A função de usuário padrão do SALZ é personalizável e pode variar de acordo com a conta. São fornecidas instruções sobre como encontrar sua função.

Veja a seguir um exemplo da função de usuário padrão do SALZ. Para garantir que você tenha as políticas definidas para você, execute o `get-role`comando. Ou, entre no AWS Identity and Access Management console em https://console.aws.amazon.com/iam/e escolha Funções.

A função de cliente somente para leitura é uma combinação de várias políticas. Segue abaixo um detalhamento da função (JSON).

Política de auditoria do Managed Services:

ReadOnly Política de IAM do Managed Services

Política de usuário do 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": [
        "*"
      ]
    }
  ]
}
```

Política compartilhada do Customer Secrets Manager

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/*"
    }
  ]
}
```

Política de assinatura do Customer Marketplace

JSON

```
{
  "Version":"2012-10-17",
```

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

Regras de firewall de acesso padrão

Essas são as regras de firewall padrão necessárias para acessar suas instâncias.

> **Note**
>
> Para obter informações sobre as regras de firewall e as portas necessárias para estabelecer uma confiança unidirecional do AD, consulte o Guia de segurança do AMS acessando o console do AWS Artifact -> a guia Relatórios e pesquise por AWS Managed Services.

Portas de instância do Linux Stack

Essas regras são necessárias para sua autenticação em pilhas AMS Linux.

Regras de portas de instâncias Linux DE: Instância Linux Stack ATÉ: Controlador de domínio CORP

Porta	Protocolo	Serviço	Direction
389	TCP	LDAP	Ingress
389	UDP	LDAP	Ingress
88	TCP	Kerberos	Ingress

Porta	Protocolo	Serviço	Direction
88	UDP	Kerberos	Ingress

Portas de instância do Windows Stack

Essas regras são necessárias para sua autenticação nas pilhas do AMS Windows.

DE: Instância do Windows Stack PARA: Controlador de domínio CORP

Porta	Protocolo	Serviço	Direction
88	TCP | UDP	Kerberos	Entrada e saída
135	TCP | UDP	Serviço de localização DCE/RPC	Entrada e saída
389	TCP | UDP	LDAP	Entrada e saída
3268	TCP | UDP	msft-gc, Microsoft Global Catalog (serviço LDAP que contém dados das florestas do Active Directory)	Entrada e saída
445	TCP	Microsoft-DS Active Directory, compartilhamentos do Windows	Entrada e saída
49152 – 65535	TCP	Portas dinâmicas ou privadas que não podem ser registradas na IANA. Esse intervalo é usado para serviços privados ou personalizados ou para fins temporários e para alocação automática de portas efêmeras.	Entrada e saída

Gerenciamento de serviços no AWS Managed Services

Tópicos

- Governança de contas no AWS Managed Services
- Início do serviço no AWS Managed Services
- Gestão do relacionamento com o cliente (CRM)
- Otimização de custos no AWS Managed Services
- Horas de serviço no AWS Managed Services
- Obter ajuda no AWS Managed Services

Como o serviço AMS funciona para você.

Governança de contas no AWS Managed Services

Esta seção aborda a governança de contas do AMS.

Você é designado como gerente de prestação de serviços em nuvem (CSDM) que fornece assistência consultiva em todo o AMS e tem uma compreensão detalhada do seu caso de uso e da arquitetura de tecnologia para o ambiente gerenciado. CSDMs trabalhe com gerentes de contas, gerentes técnicos de contas, arquitetos de nuvem do AWS Managed Services (CAs) e arquitetos de soluções da AWS (SAs), conforme aplicável, para ajudar a lançar novos projetos e oferecer recomendações de melhores práticas em todos os processos operacionais e de desenvolvimento de software. O CSDM é o principal ponto de contato do AMS. As principais responsabilidades do seu CSDM são:

- Organize e conduza reuniões mensais de análise de serviços com os clientes.
- Forneça detalhes sobre segurança, atualizações de software para o ambiente e oportunidades de otimização.
- Defenda seus requisitos, incluindo solicitações de recursos para o AMS.
- Responda e resolva solicitações de faturamento e relatórios de serviços.
- Forneça insights para recomendações financeiras e de otimização de capacidade.

Início do serviço no AWS Managed Services

Início do serviço: A data de início do serviço para uma conta do AWS Managed Services é o primeiro dia do primeiro mês civil após o qual a AWS notifica você de que as atividades definidas nos requisitos de integração dessa conta do AWS Managed Services foram concluídas; desde que, se a AWS fizer essa notificação após o vigésimo dia de um mês civil, a data de início do serviço será o primeiro dia do segundo mês civil após a data de tal notificação.

Início do serviço

- R significa parte responsável que faz o trabalho para realizar a tarefa.
- I significa informado; uma parte que é informada sobre o progresso, geralmente apenas após a conclusão da tarefa ou do resultado final.

Início do serviço

N.º da etapa	Título da etapa	Descrição	Cliente	AMS
1.	Entrega da conta AWS do cliente	O cliente cria uma nova conta da AWS e a entrega ao AWS Managed Services	R	eu
2.	Conta do AWS Managed Services — design	Finalize o design da conta do AWS Managed Services	eu	R
3.	Conta do AWS Managed Services — criar	Uma conta do AWS Managed Services é criada de acordo com o design na Etapa 2	eu	R

Gestão do relacionamento com o cliente (CRM)

O AWS Managed Services (AMS) fornece um processo de gerenciamento de relacionamento com o cliente (CRM) para garantir que um relacionamento bem definido seja estabelecido e mantido com você. A base desse relacionamento é baseada na visão da AMS sobre seus requisitos de negócios. O processo de CRM facilita a compreensão precisa e abrangente de:

- Suas necessidades de negócios e como atender a essas necessidades
- Suas capacidades e restrições
- AMS e suas diferentes responsabilidades e obrigações

O processo de CRM permite que a AMS use métodos consistentes para fornecer serviços a você e fornecer governança para seu relacionamento com a AMS. O processo de CRM inclui:

- Identificando suas principais partes interessadas
- Estabelecendo uma equipe de governança
- Conduzindo e documentando reuniões de revisão de serviços com você
- Fornecer um procedimento formal de reclamação de serviço com um procedimento de escalonamento
- Implementando e monitorando seu processo de satisfação e feedback
- Gerenciando seu contrato

Processo de CRM

O processo de CRM inclui as seguintes atividades:

- Identificar e entender seus processos e necessidades de negócios. Seu contrato com a AMS identifica suas partes interessadas.
- Definindo os serviços a serem fornecidos para atender às suas necessidades e exigências.
- Reunir-se com você nas reuniões de revisão de serviços para discutir quaisquer alterações no escopo do serviço AMS, no SLA, no contrato e nas necessidades de seus negócios. Reuniões provisórias podem ser realizadas com você para discutir desempenho, conquistas, problemas e planos de ação.
- Monitorando sua satisfação usando nossa pesquisa de satisfação do cliente e o feedback fornecido nas reuniões.
- Relatórios de desempenho em relatórios mensais de desempenho medidos internamente.
- Analisar o serviço com você para determinar oportunidades de melhorias. Isso inclui comunicação frequente com você sobre o nível e a qualidade do serviço de AMS fornecido.

Reuniões de CRM

Os gerentes de prestação de serviços em nuvem (CSDMs) da AMS realizam reuniões com você regularmente para discutir faixas de serviços (operações, segurança e inovações de produtos) e executivas (relatórios de SLA, medidas de satisfação e mudanças nas necessidades de seus negócios).

Reunião	Finalidade	Modo	Participantes
Revisão semanal do status (opcional)	Problemas ou incidentes pendentes , correções, eventos de segurança, registros de problemas Tendência operacional de 12 semanas (+/- 6) Preocupações do operador do aplicativo Programação de fim de	Cliente no local location/ Telecom/Chime	AMS: CSDM e arquiteto de nuvem (CA) Membros da equipe designados pelo cliente (ex: Cloud/Inf rastructure, Application Support, equipes de arquitetura etc.)
Análise mensal de negócios	Analise o desempenho do nível de serviço (relatórios, análises e tendências) Análise financeira Roteiro do produto GATO	Cliente no local location/ Telecom/Chime	AMS: CSDM, arquiteto de nuvem (CA), equipe de contas do AMS, gerente técnico de produto do AMS (TPM) (opcional), gerente do AMS OPS (opcional)

Reunião	Finalidade	Modo	Participantes
			Você: representante do operador do aplicativo
Análise trimestral de negócios	Desempenho e tendências do scorecard e do acordo de nível de serviço (SLA) (6 meses) Próximos planos/migrações de 3/6/9/12 meses Risco e mitigação de riscos Principais iniciativas de melhoria Itens do roteiro do produto Oportunidades alinhadas à direção futura Finanças Iniciativas de redução de custos Otimização de negócios	Localização do cliente no local	AMS: CSDM, arquiteto de nuvem, equipe de contas do AMS, diretor de serviços do AMS, gerente de operações do AMS Você: representante do operador do aplicativo, representante do serviço, diretor de serviços

Organizações de reuniões de CRM

O CSDM do AMS é responsável por documentar a reunião, incluindo:

- Criação da agenda, incluindo itens de ação, problemas e lista de participantes.
- Criar a lista de itens de ação revisados em cada reunião para garantir que os itens sejam concluídos e resolvidos dentro do cronograma.
- Distribuir as atas da reunião e a lista de itens de ação aos participantes da reunião por e-mail dentro de um dia útil após a reunião.
- Armazenar as atas da reunião no repositório de documentos apropriado.

Na ausência do CSDM, o representante da AMS que lidera a reunião cria e distribui atas.

> **Note**
>
> Seu CSDM trabalha com você para estabelecer a governança da sua conta.

Relatórios mensais de CRM

Seu CSDM do AMS prepara e envia apresentações mensais sobre o desempenho do serviço. As apresentações incluem informações sobre o seguinte:

- Data do relatório
- Resumo e insights:
  - Principais chamadas: contagem total e ativa de pilhas, status de patches de pilha, status de integração da conta (somente durante a integração), resumos de problemas específicos do cliente
  - Desempenho: estatísticas sobre resolução de incidentes, alertas, correções, solicitações de mudança (RFCs), solicitações de serviço e disponibilidade do console e da API
  - Problemas, desafios, preocupações e riscos: status de problemas específicos do cliente
  - Itens futuros: planos de integração ou resolução de incidentes específicos para o cliente
- Recursos gerenciados: gráficos e diagramas circulares de pilhas
- Métricas do AMS: métricas de monitoramento e eventos, métricas de incidentes, métricas de adesão ao AMS SLA, métricas de solicitação de serviço, métricas de gerenciamento de mudanças, métricas de armazenamento, métricas de continuidade, métricas do Trusted Advisor e resumos de custos (apresentados de várias maneiras). Solicitações de recursos. Informações de contato.

> **Note**
>
> Além das informações descritas, seu CSDM também o informa sobre qualquer alteração material no escopo ou nos termos, incluindo o uso de subcontratados pela AMS para atividades operacionais.
> O AMS gera relatórios sobre patches e backup que seu CSDM inclui em seu relatório mensal. Como parte do sistema de geração de relatórios, o AMS adiciona alguma infraestrutura à sua conta que não está acessível para você:

- Um bucket S3, com os dados brutos relatados
- Uma instância do Athena, com definições de consulta para consultar os dados
- Um Glue Crawler para ler os dados brutos do bucket S3

Otimização de custos no AWS Managed Services

O AWS Managed Services fornece relatórios detalhados de utilização de custos e economia todos os meses para você durante suas análises mensais de negócios (MBRs).

O AMS segue um conjunto padrão de processos e mecanismos para identificar formas de redução de custos em suas contas gerenciadas e ajudá-lo a planejar e implementar as mudanças para otimizar seus gastos com a AWS.

> **Note**
>
> A AMS está desenvolvendo um vídeo para ajudar na otimização de custos. A primeira etapa é fornecer a você um PDF e uma planilha do Excel com as melhores práticas de otimização de custos. Para acessar esses recursos, abra o arquivo ZIP do Guia rápido para otimização de custos.

Estrutura de otimização de custos

O AMS segue uma abordagem de três estágios com você para otimizar seus custos da AWS:

1. Identifique caminhos de otimização de custos em seu ambiente gerenciado
2. Apresente um plano de otimização de custos para você
3. Auxiliar na otimização de custos de forma mensurável

Identifique caminhos de otimização de custos no ambiente gerenciado

O AMS utiliza ferramentas AWS nativas, como o Cost Explorer e o Trusted Advisor, enquanto aproveita mais de 20 padrões de economia de custos em otimização de arquitetura, otimizações AWS focadas em EC2 instâncias e contas para criar recomendações personalizadas de economia de custos para você.

Algumas das recomendações de otimização incluem o seguinte.

Recomendações de otimização arquitetônica:

- Uso ideal da classe de armazenamento S3: O Amazon S3 oferece uma variedade de classes de armazenamento para atender a vários requisitos de carga de trabalho com base no acesso, resiliência e custo dos dados. O S3 Intelligent-Tiering e a análise da classe de armazenamento S3 com base nas necessidades da carga de trabalho permitem que você gerencie os custos do S3 com eficiência.
- Usando arquiteturas de cache: o uso de instâncias de cache, quando aplicável, pode ajudá-lo a substituir algumas instâncias de banco de dados e, ao mesmo tempo, atender aos requisitos de IOPS.
- Economia de upgrade do EBS: migrar seus volumes do EBS de gp2 para gp3 proporciona uma economia de até 20% e você pode aproveitar o desempenho previsível da linha de base de 3.000 IOPS e 125 MiB/s, independentemente do tamanho do volume.
- Usando elasticidade: os recursos de auto-scaling fornecidos permitem a utilização eficaz dos recursos AWS e caminhos para a otimização de custos. Revisar e atualizar as políticas de escalabilidade de instâncias regularmente com base na necessidade proporciona ainda mais economia de custos.

EC2 recomendações focadas na instância

- Dimensionamento correto da instância: recomendações focadas no dimensionamento das instâncias e nas configurações ideais com base no uso. As recomendações também incluem a utilização do recurso Amazon EC2 Auto Scaling e a EC2 substituição de instâncias, quando aplicável AWS Lambda , por conteúdo web estático no Amazon S3, etc.
- Agendamento de instâncias: usar o AMS Resource Scheduler para iniciar e interromper automaticamente instâncias com base em um cronograma ajuda a conter custos, especialmente para instâncias que não são de produção e que não são utilizadas fora do horário comercial.
- Assinando planos de poupança: O plano de economia é a maneira mais fácil de economizar no AWS uso. Os EC2 Instance Savings Plans oferecem até 72% de economia em comparação com os preços sob demanda no uso de suas EC2 instâncias da Amazon. Os Amazon SageMaker AI Savings Plans oferecem até 64% de economia no uso dos serviços de SageMaker IA da Amazon. O AMS fornece recomendações apropriadas sobre planos de economia com base no uso AWS de seus recursos.

- Orientação de uso e consumo de instâncias reservadas (RI): as Instâncias EC2 Reservadas (RI) da Amazon oferecem um desconto significativo (até 75%) em comparação com os preços sob demanda e fornecem uma reserva de capacidade quando usadas em uma zona de disponibilidade específica.
- Uso de instâncias spot: cargas de trabalho tolerantes a falhas podem utilizar instâncias spot e reduzir os preços em até 90%.
- Encerramento de instância ociosa: identificar e relatar instâncias que estão ociosas ou com baixa utilização que podem ser encerradas.

Recomendações focadas na conta

- Limpeza da conta: no nível da conta, o AMS também identifica volumes do EBS não utilizados, CloudTrail trilhas duplicadas, contas vazias com recursos não utilizados e assim por diante, além de fornecer recomendações para limpeza.
- Recomendações de SLA: Além disso, o AMS revisa regularmente suas contas Plus e Premium e recomenda escolher o nível de SLA certo para as contas.
- Otimização da automação do AMS: O AMS otimiza continuamente a automação e a infraestrutura do AMS usada para fornecer serviços do AMS.

Apresente aos clientes e auxilie no planejamento

A AMS conduz análises comerciais mensais (MBRs) com as principais partes interessadas do cliente e apresenta as vias, mecanismos e recomendações de redução de custos identificados, juntamente com possíveis economias de custos. Além disso, trabalhamos com você para planejar as mudanças necessárias.

Auxiliar na implementação de recomendações e medir o impacto nos custos

O AMS auxilia na obtenção e medição dos impactos nos custos e nas mudanças de otimização.

Você avalia o impacto do aplicativo, o risco e os critérios de sucesso das alterações recomendadas e gera as solicitações apropriadas de mudança (RFCs) por meio do console do AMS. O AMS colabora com você e implementa as mudanças relacionadas à otimização de custos em suas contas gerenciadas. O AMS mede o impacto nos custos e inclui as economias realizadas nas análises mensais de negócios (MBRs).

Matriz de responsabilidade de otimização de custos

Responsabilidades na otimização de custos do AMS.

Otimização de custos RACI

Atividades	Cliente	AMS
Compilando recomendações de redução de custos e preparando o relatório	eu	R
Apresentando relatório de economia de custos	C	R
Planejando mudanças associadas à economia de custos	R	C
Avaliando o impacto e o	R	C

Atividades	Cliente	AMS
risco da mudança		
Levantando RFCs para implementar as mudanças	R	C
Analisando RFCs e implementando as mudanças	C	R
Testando o aplicativo e validando a implementação da mudança	R	C

Atividades	Cliente	AMS
Medir o impacto nos custos após a mudança e apresentá-lo ao cliente	eu	R

Horas de serviço no AWS Managed Services

Recurso	AMS Avançado
	Nível Premium
Solicitação de serviço	24/7
Gerenciamento de incidentes (P2-P3)	24/7
Backup e recuperação	24/7
Gerenciamento de patches	24/7
Monitoramento e alertas	24/7
Solicitação automática de alteração (RFC)	24/7
Solicitação de alteração não automatizada (RFC)	24/7
Gerente de entrega de serviços em nuvem (CSDM)	Segunda a sexta-feira: das 08:00 às 17:00, horário comercial local

Obter ajuda no AWS Managed Services

O AMS oferece suporte com gerenciamento de incidentes, gerenciamento de solicitações de serviço e gerenciamento de alterações 24 horas por dia, 7 dias por semana, 365 dias por ano (de acordo com o Acordo de Nível de Serviço do AMS aplicado à conta).

Para relatar um problema de desempenho do serviço da AWS ou do AMS que afeta seu ambiente gerenciado, use o console do AMS e envie um relatório de incidentes. Para obter detalhes, consulte Relatar um incidente. Para obter informações gerais sobre o gerenciamento de incidentes do AMS, consulte Resposta a incidentes.

Para solicitar informações ou conselhos, ou para solicitar serviços adicionais do AMS, use o console do AMS e envie uma solicitação de serviço. Para obter detalhes, consulte Criando uma solicitação de serviço. Para obter informações gerais sobre solicitações de serviço do AMS, consulte Gerenciamento de solicitações de serviço.

Modos de gerenciamento de alterações

O AWS Managed Services (AMS) usa o modo de gerenciamento de alterações para proteger as alterações no AMS Advanced. Os modos de gerenciamento de mudanças ajudam você a manter altos padrões operacionais para o meio ambiente, controlar riscos e evitar impactos adversos. O AMS Advanced tem modos diferentes que fornecem diferentes níveis de controle e risco. Todos os modos, exceto o modo gerenciado pelo cliente, são gerenciados pelo AMS. A seguir estão os modos de gerenciamento de alterações disponíveis:

- Modo RFC (antigo modo CM padrão): fornece um sistema de “solicitação de alteração” (RFC) e tipos de alteração personalizados pelo AMS () CTs
- Modo Direct Change: igual ao modo RFC, além do uso da AWS APIs e dos consoles para criar recursos gerenciados pelo AMS
- AWS Service Catalog no AMS: semelhante ao modo Direct Change, mas em vez de usar o sistema de gerenciamento de alterações do AMS (RFCs), você usa o AWS Service Catalog para criar recursos que o AMS então gerencia.
- Modo de desenvolvedor: igual ao modo Direct Change, somente os recursos que você cria com a AWS APIs e os consoles não são gerenciados pela AMS — você é responsável pelo gerenciamento deles
- Modo de provisionamento de autoatendimento (SSP): igual ao modo Desenvolvedor, exceto que não há acesso ao sistema de gerenciamento de alterações do AMS (não) RFCs
- Modo gerenciado pelo cliente: o AMS fornece uma zona de pouso com várias contas, mas todo o gerenciamento de recursos é de sua responsabilidade.

O sistema de gerenciamento de mudanças do AWS Managed Services (AMS), usando a API de gerenciamento de mudanças (CM), fornece operações para criar e gerenciar solicitações de mudança (RFCs) para contas de várias contas de landing zone (MALZ) e de landing zone de conta única (SALZ).

Uma solicitação de mudança (RFC) é uma solicitação criada por você ou pelo AMS por meio da interface do AMS para fazer uma alteração em seu ambiente gerenciado e inclui uma ID de tipo de alteração (CT) para uma operação específica.

A API de gerenciamento de alterações (CM) do AMS fornece operações para criar e gerenciar solicitações de mudança (RFCs). Você pode criar, atualizar, enviar, aprovar, rejeitar e cancelar

RFCs. Os operadores do AMS podem criar, atualizar, enviar, aprovar, rejeitar, cancelar e marcar RFCs como fechado.

Para obter uma lista de prefixos reservados do AMS que não devem ser usados em tags ou outros nomes, consulte Prefixos reservados.

Para obter informações sobre cada tipo de alteração, incluindo esquemas e exemplos, consulte a Referência de tipo de alteração do AMS.

> **Note**
>
> Todas as chamadas da API de gerenciamento de mudanças são registradas na AWS CloudTrail. Para obter mais informações, consulte Como acessar seus registros.

Visão geral dos modos

Use essas informações para ajudá-lo a selecionar o modo apropriado do AWS Managed Services (AMS) para hospedar seus aplicativos, com base na combinação desejada de flexibilidade e governança prescritiva para alcançar seus resultados comerciais.

O público-alvo dessas informações é:

- Equipes de clientes responsáveis pela estratégia e governança de sua landing zone. Essas informações ajudarão a equipe a estabelecer a base de uma landing zone gerenciada pela AMS, com os modos de AMS que eles gostariam de oferecer a seus clientes internos e externos.
- Proprietários de empresas e aplicativos encarregados de migrar seus aplicativos para o AMS. Essas informações ajudarão no planejamento da migração do aplicativo, com o modo AMS apropriado para migrate/host o aplicativo. Observe que o mesmo aplicativo pode ser hospedado em mais de um modo AMS durante diferentes fases do ciclo de vida do ciclo de vida do desenvolvimento de software (SDLC).
- Parceiros do AMS encarregados de orientar os clientes sobre as diferentes opções de criação e migração para o AMS.

Essas informações são mais úteis durante a fase básica da configuração de sua plataforma gerenciada pelo AMS e, quando você está fazendo a transição da fase básica para a fase de migração de sua jornada de adoção da nuvem, logo após a conclusão da integração ao AMS e você está se concentrando na governança e nas operações de aplicativos.

Tipos de modos e contas no AMS

Os modos do AWS Managed Services (AMS) podem ser definidos como as formas de interagir com o serviço AMS de acordo com a estrutura de governança específica para cada modo. As diferenças da zona de pouso, a zona de pouso com várias contas ou MALZ e a zona de pouso com conta única ou SALZ são anotadas.

> **Note**
>
> Para obter detalhes sobre a implantação de aplicativos e a escolha do modo AMS correto, consulte Modos e aplicativos ou cargas de trabalho do AMS.
> Para casos de uso reais dos diferentes modos, consulte Casos de uso do mundo real para modos AMS

A tabela a seguir fornece descrições dos modos por serviço AMS.

Recurso AMS	Modo RFC (anteriormente modo CM padrão) / OOD *	Modo de mudança direta	AWS Service Catalog	Provisionamento de autoatendimento/Modo de desenvolvedor	Gerenciado pelo cliente
Configuração da zona de pouso	MALZ e SALZ	MALZ e SALZ	MALZ e SALZ		
Gerenciamento de alterações	Programação de alterações, revisão de alterações manuais e registro de alterações	O mesmo que o modo RFC para alterações de alto risco, como IAM ou grupos de segurança	Nenhum		
Registro, monitoram	Sim (recursos suportados)			Não	

Recurso AMS	Modo RFC (anteriormente modo CM padrão) / OOD *	Modo de mudança direta	AWS Service Catalog	Provisionamento de autoatendimento/Modo de desenvolvedor	Gerenciado pelo cliente
ento, grades de proteção e gerenciamento de eventos					
Gerenciamento de continuidade	Sim (recursos suportados)			Não aplicável/ Não	Não
Gerenciamento de segurança	Controles de segurança em nível de instância e controles em nível de conta			Controles no nível da conta	Controles em nível organizacional da AWS
Gerenciamento de patches	Sim			Não aplicável/ Não	Não
Gerenciamento de incidentes e problemas	SLA de resposta e resolução para recursos suportados pelo AMS			SLA de resposta para os recursos resultantes	Não
Relatórios	Sim			Não	
Gerenciamento de solicitações de serviço	Sim			Somente solicitações de suporte	Não

* Operations On Demand (OOD) tem uma oferta para clientes que usam o modo RFC para gerenciar suas alterações por meio de recursos dedicados. Para obter mais detalhes, consulte o catálogo de ofertas do Operations on Demand e fale com seu gerente de prestação de serviços em nuvem (CSDM).

> **Note**
>
> Modo de provisionamento de autoatendimento no AMSe ambos Modo AMS Advanced Developer podem parecer adequados para um aplicativo que tem uma arquitetura complexa baseada em serviços nativos da AWS. Ao arquitetar cargas de trabalho, você faz concessões entre excelência operacional e agilidade, com base em seu contexto de negócios. Essa é uma boa maneira de pensar em selecionar o modo SSP ou o modo Desenvolvedor para seu aplicativo. A seleção também pode mudar com base na fase SDLC da inscrição. Por exemplo: quando o aplicativo está pronto para produção, o modo SSP talvez seja uma opção mais apropriada devido às grades de proteção mais rígidas do AMS nesse modo. As grades de proteção são aplicadas na forma de controles preventivos, como controle de alterações baseado em RFC para atualizações do IAM e no nível de UO do aplicativo. SCPs Essas decisões comerciais podem determinar suas prioridades de engenharia. Você pode otimizar para aumentar a flexibilidade dos proprietários de aplicativos na fase de “pré-produção” em detrimento da governança e do suporte operacional.

Arquitetura MALZ e modos AMS associados

O AMS multi-account landing zone (MALZ) oferece a opção de provisionar automaticamente contas de aplicativos (ou contas de recursos) sob as Unidades Organizacionais (OU) padrão: OU gerenciada pelo cliente, OU gerenciada ou OU de desenvolvimento. A infraestrutura provisionada nas contas de aplicativos criadas em cada uma delas OUs está sujeita ao modo AMS específico oferecido por essas contas básicas. OUs É comum encontrar uma combinação de dois ou mais modos na mesma conta do aplicativo. Por exemplo: o modo RFC e o modo SSP podem coexistir em uma conta gerenciada pelo AMS que hospeda uma arquitetura de pipeline que consiste em API Gateway e Lambda para funções de acionamento e S3 e SQS para EC2 ingestão e orquestração. Nesse caso, o modo SSP se aplicaria ao Lambda e ao API Gateway.

A Figura 1 apresenta como os diferentes modos são oferecidos por meio do básico OUs no AMS. Ao solicitar uma nova conta de aplicativo no AMS, você deve selecionar a OU para a conta.

Arquitetura MALZ e modos AMS associados

O AMS aproveita a base com OUs base nas melhores práticas da AWS como uma forma de gerenciar contas de forma lógica usando políticas de controle de serviços (). SCPs Isso serve como uma forma de aplicar a estrutura de governança em cada modo AMS. Quaisquer barreiras de governança e segurança (na forma de SCPs) aplicadas à fundação OUs também são aplicadas automaticamente. custom/child OUs SCPs Podem ser solicitados adicionais para a criança OUs. É importante entender que contas de aplicativos não são o mesmo que modos. Os modos são aplicados à infraestrutura provisionada nas contas e definem as responsabilidades operacionais entre a AMS e os clientes.

Figura 1: Arquitetura MALZ e modos AMS associados

> **Note**
>
> "Restritivo" implica que você pode solicitar políticas personalizadas para elas. Elas são aprovadas pela AMS case-by-case com base em garantir que não interfiram nas capacidades da AMS de fornecer excelência operacional. OUs Para obter uma lista detalhada das grades de proteção do AMS, consulte as grades de proteção do AMS no guia do usuário.

Modos e aplicativos ou cargas de trabalho do AMS

Considere os requisitos operacionais e de governança para seus aplicativos ao selecionar o modo certo, seja solicitando uma nova conta de aplicativo ou hospedando o aplicativo em uma conta de aplicativo existente. A seleção do modo AMS apropriado para cada aplicativo ou carga de trabalho depende dos seguintes fatores:

- O tipo de função do ciclo de vida do SDLC que o ambiente fornecerá (por exemplo, sandbox com mudanças não moderadas, UAT com algumas mudanças frequentes, produção com alterações mínimas e altamente regulamentada)
- As políticas de governança necessárias (aplicadas SCPs no nível da OU)
- Modelo operacional (se você quiser assumir a responsabilidade operacional ou terceirizá-la para a AMS)
- Os resultados comerciais desejados, como tempo para operar na nuvem e custo das operações.

> **Note**
>
> Para obter uma descrição dos tipos de modo por serviço do AMS, consulte Tipos de modos e contas no AMS.
> Para casos de uso reais dos diferentes modos, consulte Casos de uso do mundo real para modos AMS

A tabela a seguir descreve as principais considerações para os proprietários de aplicativos ajudarem a decidir sobre o modo AMS mais adequado. Os proprietários do aplicativo devem incluir uma fase de avaliação antes da migração do aplicativo para entender completamente qual modo se aplica ao aplicativo específico. Exemplo: Para aplicativos baseados em serviços nativos da nuvem ou arquitetura sem servidor, a melhor opção pode ser começar a criar e iterar no modo Desenvolvedor e implantar a infraestrutura final como código usando o modo AMS Managed — SSP. Nesse caso, a refatoração leve pode ser necessária para garantir que todos os CloudFormation modelos criados para implantação automatizada atendam às diretrizes de ingestão estabelecidas pela AMS. Além disso, todas as permissões do IAM precisam ser aprovadas pela AMS Security para garantir que sigam o modelo de menor privilégio.

O modo AMS selecionado para hospedar o aplicativo pode ajudar a permitir que você desenvolva o modelo operacional de nuvem desejado.

> **Note**
>
> Mais de um modelo operacional em nuvem pode existir em uma única zona de aterrissagem gerenciada pelo AMS com base nos diferentes modos do AMS selecionados para hospedar os aplicativos.

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
Prontidão operacional						
Registro, monitoram	AMS responsável por toda a infraestrutura gerenciada			Cliente responsáv	Cliente responsáv	Cliente responsável

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
ento e gerenciamento de eventos				el pelos serviços provisionados de autoatendimento (SSP)	el pelos recursos provisionados usando a função IAM de desenvolvedor fora do sistema AMS CM	
Gerenciamento de continuidade	Responsabilidade do AMS de executar o plano de backup selecionado pelo cliente			Cliente responsável pelos serviços provisionados de autoatendimento (SSP)	Cliente responsável pelos recursos provisionados usando a função IAM de desenvolvedor fora do sistema AMS CM	

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
Gerenciamento de acesso em nível de instância	Gerenciado pelo AMS por meio de confiança unidirecional do AD com domínio local. Requer infraestrutura gerenciada para ingressar no domínio AMS			Não aplicável	Cliente responsável pelos recursos provisionados usando a função IAM de desenvolvedor fora do sistema AMS CM	
Gerenciamento de segurança e gerenciamento de acesso em nível de conta	Responsabilidade do AMS por todas as contas gerenciadas			AMS responsável por todas as contas gerenciadas	Cliente responsável pelos recursos provisionados usando a função IAM de desenvolvedor fora do sistema AMS CM	

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
Gerenciamento de patches	Responsabilidade do AMS por todas as contas gerenciadas			Cliente responsável pelos serviços provisionados de autoatendimento (SSP)	Cliente responsável pelos recursos provisionados usando a função IAM de desenvolvedor fora do sistema AMS CM	
Gerenciamento de alterações	Responsabilidade do AMS por todas as contas gerenciadas			Cliente responsável pelos serviços provisionados de autoatendimento (SSP)	Cliente responsável pelos recursos provisionados usando a função IAM de desenvolvedor fora do sistema AMS CM	

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
Gerenciamento de provisionamento	Prescritivo e padronizado para as opções de provisionamento oferecidas no AMS	Flexibilidade para usar diretamente a API de serviços da AWS para o AWS Service Catalog seguindo os padrões prescritivos da AMS	Flexibilidade para usar diretamente a API de serviços da AWS seguindo os padrões prescritivos da AMS	Flexibilidade para usar diretamente o serviço da AWS APIs para serviços SSP	Flexibilidade para usar diretamente a API de serviços da AWS para provisionamento	

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
Gerenciamento e auditoria de incidentes	AMS responsável por todas as contas gerenciadas				Cliente responsável pelos recursos provisionados usando a função de desenvolvedor IAM fora do AMS Change Management System	
GuardRails e infraestrutura compartilhada (rede) e estrutura de segurança	Prescritivo e padronizado, aproveitando as contas principais do AMS					Aproveitando as contas principais do AMS de forma flexível e personalizada
Prontidão de aplicação						

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
Refatoração de aplicativos	A refatoração da luz é necessária				A refatoração de luz é necessária (se provisionada usando o AMS Standard CM)	Não há necessidade de refatoração
Support para serviços da AWS	Limitado ao que é suportado pelo AMS					Não limitado
Considerações de negócios						
Tempo até a prontidão operacional	Três a seis meses			Mais de 6 meses, dependendo das competências operacionais de aplicativos do cliente		6 a 18 meses, dependendo da infraestrutura do cliente e das competências em operações de aplicativos
Custos	$$$$			$$$	$$	$

Problemas de decisão	Modo CM padrão/ OOD *	AWS Service Catalog	Modo de mudança direta	Provisionamento por autoatendimento	Modo de desenvolvedor	Gerenciado pelo cliente
Exemplos de aplicação	Servidor web com pilha de 3 níveis, aplicativos com requisitos regulatórios e de conformidade			Servidor web usando API Gateway, aplicativo em contêiner que utiliza ECS/EKS	Iterando/ otimizando no aplicativo Data Lake que usa Lambda, Glue, Athena etc.	Descentralizado, accounts/ applications como sandbox, aplicativos gerenciados por terceiros

* Operations On Demand (OOD) tem uma oferta para clientes que usam o modo CM padrão para gerenciar suas alterações por meio de recursos dedicados. Para obter mais detalhes, consulte o catálogo de ofertas do Operations on Demand e fale com seu gerente de prestação de serviços em nuvem (CSDM).

> **Note**
>
> A comparação de preços entre o modo SSP e o modo Desenvolvedor pressupõe que os mesmos serviços da AWS sejam provisionados.

Comparando os modos AMS com os objetivos de negócios e de TI

Conforme mostrado, se você estiver procurando por um modelo de governança altamente controlado e padronizado para seus aplicativos, os modos Standard Change, AWS Service Catalog ou Direct Change gerenciados pela AMS são os mais adequados. Se você precisar de um modelo de governança personalizado com foco na inovação de aplicativos sem a necessidade de prontidão operacional, selecione o modo Gerenciado pelo Cliente. Com o modo Gerenciado pelo Cliente, pode levar mais tempo para operacionalizar seus aplicativos, pois você assume a responsabilidade de estabelecer pessoas, processos e ferramentas para dar suporte a recursos operacionais, como

gerenciamento de incidentes, gerenciamento de configuração, gerenciamento de provisionamento, gerenciamento de segurança, gerenciamento de patches etc.

Casos de uso do mundo real para modos AMS

Examine-os para ajudar a determinar como usar os modos AMS.

- Caso de uso 1, imperativo comercial de reduzir custos com uma saída urgente do data center: uma empresa com um evento comercial atraente, como a saída de um data center, está interessada em rehospedar seus aplicativos locais na nuvem. A maior parte do inventário local consiste em servidores Windows e Linux com uma combinação de versões do sistema operacional. Ao fazer isso, o cliente também quer aproveitar a economia de custos que a mudança para a nuvem oferece e melhorar a postura técnica e de segurança de seus aplicativos. O cliente quer agir rapidamente, mas ainda não tem a experiência interna em operações de nuvem desenvolvida. O cliente precisa encontrar um equilíbrio entre a refatoração. Refatorar demais pode ser arriscado em um cronograma apertado. No entanto, com algumas refatorações, como atualizar as versões do sistema operacional e otimizar bancos de dados, os aplicativos podem alcançar o próximo nível de desempenho. Neste exemplo, o cliente pode selecionar o modo RFC gerenciado pelo AMS para rehospedar a maioria de seus aplicativos. O AMS fornece operações de infraestrutura, além de orientar as equipes de operações do cliente sobre as melhores práticas para operar com segurança na nuvem.

  O AWS Service Catalog gerenciado pela AMS e o modo Direct Change gerenciado pela AMS oferecem ao cliente uma flexibilidade extra, ao mesmo tempo em que alcança os mesmos resultados e objetivos comerciais. Além disso, o cliente pode usar a oferta do AMS Operations On Demand (OOD) para ter engenheiros de operações dedicados do AMS para priorizar a execução de solicitações de mudança (). RFCs

  Ao transferir as tarefas operacionais indiferenciadas da infraestrutura (aplicação de patches, backups, gerenciamento de contas etc.) para o AMS, o cliente pode continuar se concentrando na otimização de seus aplicativos e na capacitação de suas equipes internas nas operações em nuvem. O AMS fornece relatórios mensais ao cliente sobre economia de custos e faz recomendações sobre otimizações de recursos. Nesse caso de uso, se houvesse end-of-life aplicativos hospedados em versões antigas do sistema operacional, como Windows 2003 e 2008, que o cliente decidisse não refatorar, eles também podem ser migrados para o AMS e hospedados em uma conta que utiliza o modo Gerenciado pelo Cliente.
- Caso de uso 2, criando um data lake com Lambda, Glue e Athena dentro do limite seguro do AMS: uma empresa está procurando configurar um data lake para atender às necessidades

de geração de relatórios de vários aplicativos no AMS. O cliente quer usar buckets S3 para o armazenamento de conjuntos de dados e o AWS Athena para consultar o conjunto de dados para cada relatório. O S3 e o AWS Athena serão implantados em contas gerenciadas separadas pelo AMS. A conta com o S3 também tem outros serviços, como Glue, Lambda e Step Functions, para criar um pipeline de ingestão de dados. Glue, Lambda, Athena e Step Functions são considerados serviços de provisionamento de autoatendimento (SSP) nesse caso. O cliente também implantou uma EC2 instância na conta que atua como um servidor ad hoc tooling/scripting . O cliente começa solicitando que o AMS habilite os serviços SSP em sua conta gerenciada pelo AMS. O AMS provisiona uma função do IAM para cada serviço que o cliente pode assumir, uma vez que a função é integrada à solução de federação do cliente. Para facilitar o gerenciamento, o cliente também pode combinar as políticas para as funções separadas do IAM em uma função personalizada, aliviando a necessidade de alternar funções ao trabalhar entre os serviços da AWS. Depois que a função é ativada na conta, o cliente pode configurar os serviços de acordo com seus requisitos. No entanto, o cliente deve trabalhar com o sistema de gerenciamento de alterações do AMS para solicitar permissões adicionais, dependendo do caso de uso.

Por exemplo, para acessar o Glue Crawlers, o Glue precisa de permissões adicionais. Também serão necessárias permissões adicionais para criar fontes de eventos para o Lambda. O cliente trabalhará com o AMS para atualizar as funções do IAM para permitir o acesso entre contas para que o Athena consulte buckets do S3. Atualizações nas funções de serviço ou funções vinculadas a serviços também serão necessárias por meio do gerenciamento de alterações do AMS para que o Lambda chame o serviço Step Functions e o Glue para ler e gravar em todos os buckets do S3. O AMS trabalha com os clientes para garantir que o modelo de acesso com privilégios mínimos seja seguido e que as alterações solicitadas no IAM não sejam excessivamente permissivas e exponham o ambiente a riscos desnecessários. A equipe de data lake do cliente gasta tempo planejando todas as permissões do IAM necessárias para os serviços específicos da arquitetura do cliente e solicita que o AMS as habilite. Isso ocorre porque todas as alterações do IAM são processadas manualmente e submetidas à análise da equipe de segurança do AMS. O tempo para processar essas solicitações deve ser contabilizado no cronograma de implantação do aplicativo.

Como os serviços SSP estão operacionais na conta, o cliente pode solicitar suporte e relatar problemas por meio do gerenciamento de incidentes e solicitações de serviço do AMS. No entanto, o AMS não monitorará ativamente as métricas de desempenho e simultaneidade do Lambda ou as métricas de trabalho do Glue. É responsabilidade do cliente garantir que o registro e o monitoramento adequados estejam habilitados para os serviços SSP. A EC2 instância e o bucket S3 na conta são totalmente gerenciados pelo AMS.

- Caso de uso 3, configuração rápida e flexível de um pipeline de implantação de CICD no AMS: um cliente está procurando configurar um pipeline de CICD baseado em Jenkins para implantar um pipeline de código em todas as contas de aplicativos no AMS. O cliente pode achar mais adequado hospedar esse pipeline do CICD no modo Direct Change (DCM) gerenciado pelo AMS ou no modo Desenvolvedor gerenciado pelo AMS, pois isso oferece flexibilidade para configurar o servidor Jenkins com a configuração personalizada necessária ativada EC2, com as permissões de acesso do IAM desejadas CloudFormation e os buckets do S3 que hospedam o repositório de artefatos. Embora isso também possa ser feito no modo RFC gerenciado pelo AMS, a equipe do cliente precisaria criar vários manuais para funções do IAM RFCs para iterar o conjunto menos permissivo de permissões aprovadas, que são revisadas manualmente pelo AMS. O DCM permite que os clientes atinjam suas metas operacionais na AWS, evitando a necessidade de criar vários manuais RFCs para funções do IAM, ao usar o modo RFC gerenciado pela AMS, para iterar no conjunto menos permissivo de permissões aprovadas, que são revisadas manualmente pelo AMS. Isso levaria tempo, além de educação por parte do cliente, para aprimorar os processos e ferramentas do AMS. Trabalhando com o modo Desenvolvedor, o cliente pode começar com uma “função de desenvolvedor” para provisionar a infraestrutura usando a AWS nativa APIs. A maneira mais rápida e flexível de configurar esse pipeline seria usar o modo AMS Managed-Developer. O modo de desenvolvedor oferece a maneira mais rápida e fácil, ao mesmo tempo que compromete a integração operacional, enquanto o DCM é menos flexível, mas fornece o mesmo nível de suporte operacional do modo RFC.
- Caso de uso 4, modelo operacional personalizado dentro da base da AMS: um cliente está considerando a saída do data center com prazos determinados e um de seus aplicativos corporativos é totalmente gerenciado por um MSP terceirizado, incluindo operações de aplicativos e operações de infraestrutura. Supondo que o cliente não tenha tempo no cronograma para refatorar esse aplicativo para que ele possa ser operado pelo AMS, o modo Customer Managed é uma opção adequada. O cliente pode aproveitar a configuração rápida e automatizada da Zona de Aterrissagem gerenciada pela AMS. Eles podem aproveitar o gerenciamento centralizado de contas que controla a venda e a conectividade da conta por meio da conta de rede centralizada. Também simplifica o faturamento ao consolidar as cobranças de todas as contas gerenciadas pelo cliente por meio da conta AMS Payer. O cliente tem flexibilidade para configurar seu modelo de gerenciamento de acesso personalizado com o MSP, separado do gerenciamento de acesso padrão usado para contas gerenciadas pelo AMS. Dessa forma, usando o modo Customer Managed, eles podem configurar um ambiente gerenciado pelo AMS e, ao mesmo tempo, atender aos requisitos comerciais de desocupar seu ambiente local. Nesse caso, se o cliente também tiver aplicativos baseados no Windows que está migrando para a nuvem e optar por movê-los para uma conta gerenciada pelo cliente, o cliente será responsável por criar um modelo operacional

em nuvem. Isso pode ser complexo, caro e demorado, dependendo da capacidade do cliente de transformar os processos tradicionais de TI e treinar pessoas. O cliente pode economizar tempo e custos “transferindo e transferindo” essas cargas de trabalho para uma conta gerenciada pelo AMS e transferindo as operações de infraestrutura para o AMS.

> **Note**
>
> Às vezes, os clientes podem sentir a necessidade de mover as contas de aplicativos entre a estrutura de governança do modo RFC ou SSP e o modo Desenvolvedor. Por exemplo, os clientes podem hospedar um aplicativo no modo gerenciado pelo AMS como parte da migração inicial do tipo lift and shift, mas, com o tempo, desejam reescrever o aplicativo para otimizá-lo para serviços da AWS nativos da nuvem. Eles poderiam mudar o modo da conta de pré-produção do RFC gerenciado pelo AMS para o modo Desenvolvedor gerenciado pelo AMS, oferecendo a flexibilidade e a agilidade para provisionar a infraestrutura. No entanto, depois que as alterações no provisionamento da infraestrutura forem feitas usando a “função de desenvolvedor”, a mesma infraestrutura não poderá ser movida de volta para o modo RFC gerenciado pelo AMS. Isso ocorre porque o AMS não pode garantir as operações da infraestrutura que foi provisionada fora do sistema de gerenciamento de alterações do AMS. Talvez os clientes precisem criar uma nova conta de aplicativo que ofereça o modo RFC gerenciado pelo AMS e, em seguida, reimplantar a configuração “otimizada” da infraestrutura por meio de CloudFormation modelos ou AMIs ingeridos de forma personalizada em uma conta gerenciada pelo AMS. Essa é uma maneira limpa de implantar uma configuração pronta para produção. Depois de implantado, o aplicativo estará sob a governança e as operações prescritivas do AMS. O mesmo se aplica à alternância de modos entre o modo gerenciado pelo cliente e o gerenciado pelo AMS.

Modo RFC

O modo RFC é o modo padrão para clientes do plano de operações do AMS Advanced. Ele inclui um sistema de gerenciamento de mudanças com solicitações de alteração ou RFCs um catálogo de tipos de alterações a serem usados para solicitar a adição ou alteração de que você precisa em suas contas. Esse sistema de gerenciamento de alterações fornece um nível de segurança ao limitar quem pode fazer alterações em suas contas.

Para obter detalhes sobre os tipos de alteração do AMS Advanced, consulte O que são os tipos de alteração do AMS? .

Para obter detalhes sobre a integração ao AMS Advanced, consulte Introdução ao AWS Managed Services Onboarding.

Para ver exemplos de exemplos de tipo de alteração, consulte a seção “Informações adicionais” para o tipo de alteração relevante na seção Tipos de alteração de referência do tipo de alteração do AMS Advanced por classificação.

> **Note**
>
> O modo RFC era anteriormente chamado de “modo de gerenciamento de alterações” ou “modo CM padrão”.

Tópicos

- Saiba mais sobre RFCs
- Quais são os tipos de mudança?
- Solução de problemas de erros de RFC no AMS

Saiba mais sobre RFCs

Solicitações de mudança ou RFCs trabalho de maneira dupla. Primeiro, existem parâmetros necessários para o próprio RFC. Essas são as opções na `CreateRfc` API. E segundo, existem parâmetros necessários para a ação do RFC (os parâmetros de execução). Para saber mais sobre as `CreateRfc` opções, consulte a CreateRfcseção da Referência da API do AMS. Essas opções geralmente aparecem na área Configurações adicionais das páginas Criar RFC.

Você pode criar e enviar uma RFC com a `CreateRfc` API, a `aws amscm create-rfc` CLI ou usando o console AMS. Crie páginas RFC. Para obter um tutorial sobre como criar um RFC, consulteCrie um RFC.

Tópicos

- O que são RFCs?
- Autentique ao usar a API/CLI do AMS
- Entenda as análises de segurança da RFC

- Entenda as classificações de tipo de alteração de RFC
- Entenda os estados de ação e atividade do RFC
- Entenda os códigos de status do RFC
- Entenda a atualização de RFC CTs e a detecção CloudFormation de desvios de modelos
- Cronograma RFCs
- Aprovar ou rejeitar RFCs
- Solicitar períodos de execução restritos do RFC
- Crie, clone, atualize, encontre e cancele RFCs
- Use o console AMS com RFCs
- Saiba mais sobre os parâmetros comuns de RFC
- Inscreva-se para receber o e-mail diário da RFC

O que são RFCs?

Uma solicitação de mudança, ou RFC, é como você faz uma alteração em seu ambiente gerenciado pelo AMS ou pede que o AMS faça uma alteração em seu nome. Para criar um RFC, você escolhe entre os tipos de alteração do AMS, escolhe os parâmetros do RFC (como agendamento) e, em seguida, envia a solicitação usando o console do AMS ou os comandos da API e. CreateRfcSubmitRfc

Uma RFC contém duas especificações, uma para a própria RFC e outra para os parâmetros do tipo de alteração (CT). Na linha de comando, você pode usar um comando RFC embutido ou um CreateRfc modelo padrão no formato JSON, que você preenche e envia junto com o arquivo de esquema CT JSON que você cria (com base nos parâmetros do CT). O nome do CT é uma descrição informal do CT. Um CSIO (categoria, subcategoria, item, operação) é uma descrição mais formal de um CT. Somente o CT ID deve ser especificado ao criar um RFC.

O AMS notifica você quando a alteração foi concluída com êxito (Êxito) ou sem sucesso (Falha).

> **Note**
>
> Para obter informações sobre a solução de problemas de falhas de RFC, consulteSolução de problemas de erros de RFC no AMS.

O gráfico a seguir mostra o fluxo de trabalho de uma RFC enviada por você.

Autentique ao usar a API/CLI do AMS

Ao usar a API/CLI do AMS, você deve se autenticar com credenciais temporárias.
Para solicitar credenciais de segurança temporárias para usuários federados, cal GetFederationTokenAssumeRole, AssumeRoleWithSAML ou AssumeRoleWithWebIdentityAWS security token service (STS). APIs

Uma opção comum é o SAML. Após a configuração, você adiciona um argumento a cada operação que você chama. Por exemplo: `aws --profile saml amscm list-change-type-categories`.

Um atalho para perfis SAML 2.0 é definir a variável de perfil no início de cada um API/CLI com `set AWS_DEFAULT_PROFILE=saml` (para Windows; para Linux, seria`export AWS_DEFAULT_PROFILE=saml`). Para obter informações sobre a configuração de variáveis de ambiente da CLI, consulte Configuração da interface de linha de comando da AWS, Variáveis de ambiente.

Entenda as análises de segurança da RFC

O processo de aprovação do gerenciamento de mudanças do AWS Managed Services (AMS) garante que realizemos uma análise de segurança das alterações que fazemos em suas contas.

O AMS avalia todas as solicitações de mudança (RFCs) de acordo com os padrões técnicos do AMS. Qualquer alteração que possa diminuir a postura de segurança da sua conta ao se desviar dos padrões técnicos passa por uma análise de segurança. Durante a análise de segurança, o AMS destaca o risco relevante e, em casos de risco de segurança alto ou muito alto, sua equipe de segurança autorizada aceita ou rejeita a RFC. Todas as mudanças também são avaliadas para avaliar o impacto adverso na capacidade de operação da AMS. Se possíveis impactos adversos forem encontrados, revisões e aprovações adicionais serão necessárias no AMS.

Normas técnicas da AMS

Os Padrões Técnicos do AMS definem os critérios, configurações e processos mínimos de segurança para estabelecer a segurança básica de suas contas. Esses padrões devem ser seguidos pela AMS e por você.

Qualquer alteração que possa potencialmente reduzir a postura de segurança de sua conta, desviando-se dos padrões técnicos, passa por um processo de aceitação de riscos, em que o risco

relevante é destacado pela AMS e aceito ou rejeitado pela equipe de segurança autorizada de sua parte. Todas essas mudanças também são avaliadas para avaliar se haveria algum impacto adverso na capacidade da AMS de operar a conta e, em caso afirmativo, revisões e aprovações adicionais são necessárias dentro da AMS.

Processo de gerenciamento de risco de segurança do cliente (CSRM) RFC

Quando alguém da sua organização solicita uma alteração em seu ambiente gerenciado, o AMS analisa a alteração para determinar se a solicitação pode deteriorar a postura de segurança da sua conta ao não cumprir os padrões técnicos. Se a solicitação diminuir a postura de segurança da conta, a AMS notifica o contato da sua equipe de segurança sobre o risco relevante e executa a alteração; ou, se a alteração introduzir um risco de segurança alto ou muito alto no ambiente, a AMS busca a aprovação explícita do contato da equipe de segurança na forma de aceitação do risco (explicado a seguir). O processo de aceitação de riscos do cliente da AMS foi projetado para:

- Garanta que os riscos sejam claramente identificados e comunicados aos proprietários certos
- Minimize os riscos identificados em seu ambiente
- Obtenha e documente a aprovação dos contatos de segurança designados que entendem o perfil de risco da sua organização
- Reduza a sobrecarga operacional contínua para riscos identificados

Como acessar padrões técnicos e riscos altos ou muito altos

Disponibilizamos a documentação das Normas Técnicas da https://console.aws.amazon.com/artifact/AMS para sua referência no relatório. Use a documentação das Normas Técnicas da AMS para entender se uma alteração exigiria a aceitação do risco de seu contato de segurança autorizado antes de enviar uma solicitação de alteração (RFC).

Encontre o relatório de Normas Técnicas pesquisando “Normas técnicas do AWS Managed Services (AMS)” na barra de pesquisa da guia AWS Artifact Relatórios após fazer login com o padrão AWSManagedServicesChangeManagementRole.

> **Note**
>
> O documento padrão técnico do AMS está acessível para o Cliente_ ReadOnly _Role na landing zone de conta única. Na landing zone de várias contas, a AWSManaged ServicesAdminRole usada pelos administradores de segurança e AWSManaged ServicesChangeManagementRole usada pelas equipes de aplicativos pode ser usada para

acessar o documento. Se sua equipe usa um papel personalizado, crie um Outro | Outro RFC para solicitar acesso e atualizaremos o papel personalizado especificado.

Entenda as classificações de tipo de alteração de RFC

Os tipos de alteração que você usa ao enviar uma RFC são divididos em duas grandes categorias:

- Implantação: essa classificação serve para criar recursos.
- Gerenciamento: Essa classificação serve para atualizar ou excluir recursos. A categoria Gerenciamento também contém tipos de alteração para acessar instâncias, criptografar ou compartilhar e iniciar AMIs, interromper, reinicializar ou excluir pilhas.

Entenda os estados de ação e atividade do RFC

`RfcActionState`(API) /Activity State (console) ajudam você a entender o status da intervenção ou ação humana em um RFC. Usado principalmente para fins manuais RFCs, `RfcActionState` ajuda você a entender quando há necessidade de ação por você ou pelas operações do AMS e ajuda a ver quando as operações do AMS estão trabalhando ativamente em sua RFC. Isso proporciona maior transparência às ações que estão sendo tomadas em um RFC durante seu ciclo de vida.

`RfcActionState`Definições (API) /Estado da atividade (console):

- AwsOperatorAssigned: Um operador da AWS está trabalhando ativamente em sua RFC.
- AwsActionPending: Espera-se uma resposta ou ação da AWS.
- CustomerActionPending: Espera-se uma resposta ou ação do cliente.
- NoActionPending: Nenhuma ação é exigida da AWS ou do cliente.
- NotApplicable: Esse estado não pode ser definido por operadores ou clientes da AWS e é usado somente para RFCs aqueles que foram criados antes do lançamento dessa funcionalidade.

Os estados de ação da RFC diferem dependendo se o tipo de alteração enviado requer revisão manual e tem agendamento definido como ASAP ou não.

- O RFC ActionStatemuda durante a revisão, aprovação e início de um tipo de alteração manual com agendamento adiado:
  - Depois de enviar uma RFC manual e programada, ela muda ActionStateautomaticamente AwsActionPendingpara indicar que um operador precisa revisar e aprovar a RFC.

- Quando um operador começa a revisar ativamente sua RFC, ela ActionStatemuda para. AwsOperatorAssigned
- Quando o operador aprova sua RFC, o status da RFC muda para Programado e o muda ActionStateautomaticamente para. NoActionPending
- Quando a hora de início programada da RFC é atingida, o status da RFC muda para InProgress, e o status da RFC muda ActionStateautomaticamente AwsActionPendingpara indicar que um operador precisa ser designado para a revisão da RFC.
- Quando um operador começa a executar ativamente o RFC, ele muda ActionStatepara AwsOperatorAssigned.
- Depois de concluído, o Operador fecha o RFC. Isso muda automaticamente o ActionStatepara NoActionPending.

⚠ Important

- Os estados de ação não podem ser definidos por você. Eles são definidos automaticamente com base nas alterações na RFC ou definidos manualmente pelos operadores do AMS.
- Se você adicionar correspondência a um RFC, o será automaticamente ActionStatedefinido como. AwsActionPending
- Quando um RFC é criado, o ActionStateé automaticamente definido como. NoActionPending
- Quando um RFC é enviado, o ActionStateé automaticamente definido como. AwsActionPending
- Quando uma RFC é rejeitada, cancelada ou concluída com o status de Êxito ou Falha, ela ActionStateé automaticamente redefinida para. NoActionPending
- Os estados de ação estão habilitados tanto para o automático quanto para o manual RFCs, mas a maioria é importante para o manual, RFCs pois esses tipos RFCs geralmente exigem comunicação.

Analise os exemplos de casos de uso dos estados de ação da RFC

Caso de uso: visibilidade no processo manual de RFC

- Depois de enviar uma RFC manual, o estado da ação da RFC muda automaticamente `AwsActionPending` para indicar que um operador precisa revisar e aprovar a RFC. Quando um operador começa a revisar ativamente sua RFC, o estado de ação da RFC muda para. `AwsOperatorAssigned`
- Considere uma RFC manual que tenha sido aprovada e programada e esteja pronta para começar a ser executada. Quando o status da RFC muda para`InProgress`, o estado da ação da RFC muda automaticamente para. `AwsActionPending` Ele muda novamente para `AwsOperatorAssigned` quando um operador começa a executar ativamente o RFC.
- Quando uma RFC manual é concluída (fechada como “Sucesso” ou “Falha”), o estado da Ação da RFC muda `NoActionPending` para indicar que nenhuma ação adicional é necessária do cliente ou do operador.

Caso de uso: correspondência RFC

- Quando um RFC manual é`Pending Approval`, um operador de AMS pode precisar de mais informações de você. Os operadores publicarão uma correspondência na RFC e alterarão o estado da ação da RFC para. `CustomerActionPending` Quando você responde adicionando uma nova correspondência de RFC, o estado da ação de RFC muda automaticamente para. `AwsActionPending`
- Quando uma RFC automática ou manual falha, você pode adicionar uma correspondência aos detalhes da RFC, perguntando ao operador do AMS por que a RFC falhou. Quando sua correspondência é adicionada, o estado de ação do RFC é automaticamente definido como. `AwsActionPending` Quando o operador do AMS pega o RFC para ver sua correspondência, o estado da ação do RFC muda para. `AwsOperatorAssigned` Quando o operador responde adicionando uma nova correspondência de RFC, o estado de ação da RFC pode ser definido como`CustomerActionPending`, indicando que há outra resposta do cliente esperada, ou para`NoActionPending`, indicando que nenhuma resposta do cliente é necessária ou esperada.

Entenda os códigos de status do RFC

Os códigos de status RFC ajudam você a rastrear suas solicitações. Você pode observar esses códigos de status durante uma execução de RFC na saída da CLI ou atualizando a página da lista de RFC no console.

Você também pode ver os códigos de um RFC na página de detalhes desse RFC, que pode ter a seguinte aparência:

Talvez você veja um RFC em sua lista que você não enviou. Quando os operadores do AMS usam uma CT somente interna, eles a enviam em uma RFC e ela é exibida na sua lista de RFC. Para obter mais informações, consulte Tipos de alteração somente internos.

> **Important**
>
> Você pode solicitar notificações de alterações no estado do RFC. Para obter detalhes, consulte Notificações de alteração de estado da RFC.

Códigos de status RFC

Bem-sucedida	Falha
Edição: o RFC foi criado, mas não foi enviado	Rejeitados: RFCs são rejeitados normalmente porque falham na validação; por exemplo, um recurso inutilizável, ou seja, uma sub-rede, é especificado
PendingApproval /Enviado: o RFC foi enviado e o sistema está determinando se ele requer aprovação e obtendo essa aprovação, se necessário	Cancelados: RFCs são cancelados normalmen te porque não passam pela validação antes que a hora de início configurada tenha passado
Aprovado pela AWS/Aprovado pelo cliente: o RFC foi aprovado. RFCs Os automatizados são aprovados pela AWS, RFCs os manuais são aprovados pelos operadores e, às vezes, pelos clientes	Falha: o RFC falhou; veja os motivos da falha StatusReason na saída, e as operações do AMS criam automaticamente um tíquete de problema e se comunicam com você conforme necessário
Programado: o RFC passou pelas verificações de sintaxe e requisitos e está programado para execução	
InProgress: o RFC está sendo executado , observe RFCs que esse provisionamento de vários recursos ou, de longa duração UserData, leva mais tempo para ser executado	
Executado: O RFC foi executado	

Bem-sucedida	Falha
Sucesso/Sucesso: O RFC foi concluído com sucesso	

> **Note**
>
> Cancelado ou rejeitado RFCs pode ser reenviado usando UpdateRfc; veja também. Atualizar RFCs

Se a RFC passar por todas as condições necessárias (por exemplo, todos os parâmetros necessários forem especificados), o status mudará para `PendingApproval` (até mesmo a CTs aprovação automática, o que acontece automaticamente se as verificações de sintaxe e parâmetros forem aprovadas). Se não for aprovado, o status mudará para`Rejected`. O `StatusReason` fornece informações sobre rejeições; os `ExecutionOutput` campos fornecem informações sobre aprovação e conclusão. Os códigos de erro incluem:

- InvalidRfcStateException: o RFC está em um status que não permite a operação que foi chamada. Por exemplo, se o RFC foi movido para o estado Enviado, ele não poderá mais ser modificado.
- InvalidRfcScheduleException: Os TimeoutInMinutes parâmetros StartTime EndTime, ou foram violados.
- InternalServerError: Foi encontrada uma dificuldade com o sistema.
- InvalidArgumentException: um parâmetro está especificado incorretamente; por exemplo, um valor inaceitável é usado.
- ResourceNotFoundException: um valor, como o ID da pilha, não pode ser encontrado.

Se os horários de início e término solicitados programados (também conhecidos como janela de execução de alterações) ocorrerem antes da aprovação da alteração, o status da RFC mudará para`Canceled`. Se a alteração for aprovada, o status da RFC mudará para`Scheduled`. A janela de execução da alteração para o ASAP RFCs é a hora de envio mais o `ExpectedExecutionDuration` valor do CT.

A qualquer momento antes da chegada da janela de execução da alteração, uma alteração programada (enviada com um `RequestedStartTime` na CLI) pode ser modificada ou cancelada. Se a alteração programada for modificada, ela deverá ser reenviada.

Quando a hora de início da alteração chega (agendada ou o mais rápido possível) e após a conclusão das aprovações, o status muda `InProgress` e nenhuma modificação pode ser feita. Se a alteração for concluída dentro da janela de execução da alteração especificada, o status mudará para`Success`. Se alguma parte da alteração falhar ou se a alteração ainda estiver em andamento quando a janela de execução da alteração terminar, o status mudará para`Failure`.

> **Note**
>
> Durante os estados`InProgress`,`Success`, ou `Failure` alterados, o RFC não pode ser modificado ou cancelado.

O diagrama a seguir ilustra os status do RFC desde a chamada CreateRFC até a resolução.

Entenda a atualização de RFC CTs e a detecção CloudFormation de desvios de modelos

Os recursos provisionados no AMS usam um modelo modificado CloudFormation . Se um recurso tiver um parâmetro alterado diretamente por meio do console de AWS gerenciamento de um serviço, o registro de CloudFormation criação desse recurso ficará fora de sincronia. Se isso acontecer e você tentar usar um tipo de alteração de atualização do AMS para atualizar o recurso no AMS, o AMS referenciará a configuração original do recurso e potencialmente redefinirá os parâmetros alterados. Essa redefinição pode ser prejudicial, portanto, o AMS não permite RFCs os tipos de alteração de atualização se alguma alteração extra na configuração do AMS for detectada.

Para obter uma lista dos tipos de alteração de atualização, use o filtro do console.

Remediação de deriva FAQs

Perguntas e respostas sobre a remediação do desvio do AMS. Há dois tipos de alteração que você pode usar para iniciar a correção do desvio: um é o modo de execução = manual ou “revisão necessária”, o outro é o modo de execução = automatizado.

Recursos suportados para remediação de deriva (ct-3kinq0u4l33zf)

Esses são os recursos suportados pelo tipo de alteração de remediação de deriva (ct-3kinq0u4l33zf). Para remediar qualquer recurso, use o tipo de alteração “revisão necessária” (ct-34sxfo53yuzah) em vez disso.

```
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
```

Tipos de alteração de remediação de deriva

Perguntas e respostas sobre o uso dos tipos de alteração de remediação de deriva do AMS.

Para obter uma lista dos recursos compatíveis com o recurso de remediação de deriva, consulte. Recursos suportados para remediação de deriva (ct-3kinq0u4l33zf)

Important

A remediação de deriva modifica os and/or parâmetros do modelo de pilha e é obrigatório atualizar seus repositórios de modelos locais ou qualquer automação que esteja atualizando essas pilhas para usar o modelo e os parâmetros de pilha mais recentes. Usar and/or parâmetros de modelos antigos sem sincronização pode causar alterações prejudiciais aos recursos subjacentes.

O CT automatizado e sem revisão (ct-3kinq0u4l33zf) suporta a correção de apenas 10 recursos por RFC. Para remediar os recursos restantes em lotes de 10, crie novos RFCs até que todos os recursos sejam corrigidos.

Qual tipo de alteração de remediação de deriva devo usar?

Recomendamos usar a tomografia computadorizada automatizada, sem necessidade de revisão (ct-3kinq0u4l33zf) quando:

- Você tenta realizar uma atualização em um recurso de pilha existente usando uma tomografia computadorizada e a RFC é rejeitada da mesma forma que a pilha. `DRIFTED`
- Você usou um Update CT no passado e ele falhou porque a pilha foi DERIVADA. Você não precisa tentar uma atualização novamente e, em vez disso, pode usar a revisão necessária, o manual ou a tomografia computadorizada.

Recomendamos usar a revisão obrigatória, manual, CT (ct-34sxfo53yuzah) somente quando os tipos de recursos desviados não forem suportados pela remediação de deriva (nenhuma revisão é necessária), automatizada, CT (ct-3kinq0u4l33zf), ou quando a remediação de desvio (sem necessidade de revisão), automatizada, falha.

Quais alterações são realizadas na pilha durante a remediação?

A remediação requer atualizações nos and/or parâmetros do modelo de pilha, dependendo das propriedades que são alteradas. A remediação também atualiza a política de pilha da pilha durante a remediação e restaura o valor anterior da política de pilha quando a remediação é concluída.

Como podemos ver as alterações realizadas nos and/or parâmetros do modelo de pilha?

Na resposta à RFC, um resumo das alterações é fornecido com as seguintes informações:

- `ChangeSummaryJson`: contém o resumo das alterações dos and/or parâmetros do Stack Template como parte da correção do desvio. A remediação é realizada em várias fases. Esse resumo de alterações consiste em alterações para fases individuais. Se a remediação for bem-sucedida, verifique as alterações da última fase. Veja ExecutionPlan no JSON as fases executadas em ordem. Por exemplo, a RestoreReferences seção when present é sempre executada no final e contém JSON para alterações pós-remediação. Se a remediação fosse executada no DryRun modo, nenhuma dessas alterações teria sido aplicada à pilha.
- `PreRemediationStackTemplateAndConfigurationJson`: contém um instantâneo da configuração da CloudFormation pilha, incluindo modelo, parâmetros e saídas, StackPolicyBody antes que a correção fosse acionada na pilha.

O que eu preciso fazer depois que a remediação for realizada?

> **Important**
>
> Você precisa atualizar seus repositórios de modelos locais, ou qualquer automação, que estaria atualizando a pilha corrigida, com o modelo e os parâmetros mais recentes fornecidos no resumo do RFC. É muito importante fazer isso porque usar os and/or parâmetros do modelo antigo pode causar mais alterações destrutivas nos recursos da pilha.

Minha solicitação será efetivada durante essa remediação?

A remediação é um processo off-line executado somente na configuração da CloudFormation pilha. Nenhuma atualização é executada no recurso subjacente.

Posso continuar usando Gerenciamento | Outros | Outros RFCs para realizar atualizações nos recursos após a correção?

Recomendamos que você sempre realize atualizações para empilhar recursos usando a atualização CTs automatizada disponível. Quando a atualização disponível CTs não suportar seu caso de uso, use Gerenciamento | Outros | Outras solicitações.

A remediação cria novos recursos na pilha?

A remediação não cria novos recursos na pilha. No entanto, a remediação cria novas saídas e atualiza a seção de metadados do modelo de pilha para armazenar o resumo da remediação para sua referência.

A remediação sempre será bem-sucedida?

A remediação requer análise e validação cuidadosas da configuração do modelo para determinar se ela pode ser executada. Em cenários em que essas validações falham, o processo de remediação é interrompido e nenhuma alteração é realizada no modelo ou nos parâmetros da pilha. Além disso, a remediação só pode ser realizada em tipos de recursos compatíveis.

Como posso realizar atualizações para acumular recursos se a remediação não for bem-sucedida?

Você pode usar o Gerenciamento | Outros | Outros | Atualizar CT (ct-0xdawir96cy7k) para solicitar alterações. O AMS monitora esses cenários e trabalha para melhorar a solução de remediação.

Posso corrigir pilhas que têm tipos de recursos compatíveis e não compatíveis?

Sim. No entanto, a remediação é realizada somente se os tipos de recursos suportados forem encontrados DRIFTED na pilha. Se algum tipo de recurso não suportado for DERIVADO, a remediação não continuará.

Posso solicitar remediação para pilhas criadas por meio do Non-CFN Ingest? CTs

Sim. A remediação pode ser realizada em pilhas, independentemente do tipo de alteração usado para criar a pilha.

Posso saber as alterações que seriam realizadas na pilha antes da remediação?

Sim. Os dois tipos de alteração fornecem uma DryRunopção que você pode usar para solicitar alterações que seriam realizadas se a pilha fosse corrigida. No entanto, as alterações finais da remediação podem diferir dependendo do desvio presente na pilha no momento da remediação.

Cronograma RFCs

O recurso de agendamento permite que você escolha um horário de início para RFCs. As seguintes opções estão disponíveis no recurso de agendamento:

- Execute essa alteração o mais rápido possível: O AMS executa o RFC assim que ele for aprovado. A CTs maioria é aprovada automaticamente. Use essa opção se não quiser que o RFC comece em um horário específico.
- Agende essa alteração: defina um dia, hora e fuso horário para a execução do RFC. Para tipos de alteração automatizados, é uma prática recomendada solicitar um horário de início de pelo menos 10 minutos após o planejamento do envio da RFC. Para revisar os tipos de alteração necessários, é necessário que você solicite um horário de início de pelo menos 24 horas após o plano de enviar a RFC. Se a RFC não for aprovada na hora de início configurada, a RFC será rejeitada.

Defina uma programação de RFC

Para agendar um RFC, use um dos seguintes métodos:

Execute esta alteração o mais rápido possível:

- Console: Não faça nada. Isso usa a programação de RFC padrão.
- API ou CLI: remova as `RequestedEndTime` opções `RequestedStartTime` e na operação Criar RFC.

As “revisões obrigatórias” o mais rápido possível RFCs são rejeitadas automaticamente se não forem aprovadas dentro de trinta dias após o envio.

Agende essa alteração:

- Console: Selecione o botão de rádio Agendar esta alteração. Uma área de horário de início é aberta. Digite manualmente um dia ou use o widget de calendário para escolher um dia. Insira uma hora, em UTC, expressa no formato ISO 8601 e use a lista suspensa para escolher um local. Por padrão, o AMS usa o formato ISO 8601 YYYYMMDDThhmmss Z YYYY-MM-DDThh ou:MM:SSZ, qualquer um dos formatos é aceito.

  > **Note**
  >
  > O horário de término padrão é de 4 horas a partir do horário de início inserido. Para definir a hora de término da alteração programada além de 4 horas, use a API ou a CLI para executar a alteração.

- API ou CLI: envie valores para os `RequestedEndTime` parâmetros `RequestedStartTime` e na operação Criar RFC. Passar uma configuração `RequestedEndTime` não interrompe a execução de um tipo de alteração automatizada que já foi iniciado. Para um tipo de alteração de “revisão obrigatória”, se ela `RequestedEndTime` for alcançada enquanto a pesquisa operacional do AMS ainda estiver em andamento e você estiver em comunicação com a AMS, poderá solicitar uma extensão ou talvez seja solicitado que você reenvie a RFC.

  > **Tip**
  >
  > Para ver um exemplo de leitura da hora UTC, consulte UTC no site Time-is. Exemplo de formato ISO 8601 para um date/time valor de 2016-12-05 às 14h20:2016-12-05T 14:20:00 Z ou 20161205T142000Z.

Se você fornecer...

- somente a`RequestedStartTime`, a RFC é considerada programada e `RequestedEndTime` é preenchida usando o `ExecutionDurationInMinutes` valor.
- apenas um`RequestedEndTime`, nós jogamos um InvalidArgumentException.
- ambos `RequestedStartTime` e`RequestedEndTime`, substituímos o pela hora `RequestedEndTime` de início especificada mais o `ExecutionDurationInMinutes` valor.

- `RequestedStartTime`nem tampouco`RequestedEndTime`, mantemos esses valores como nulos e o RFC é tratado como um ASAP RFC.

> **Note**
>
> Para todos os agendados RFCs, um horário de término não especificado é escrito como o horário especificado `RequestedStartTime` mais o `ExpectedExecutionDurationInMinutes` atributo do tipo de alteração enviado. Por exemplo, se `ExpectedExecutionDurationInMinutes` for “60" (minutos) e o especificado `RequestedStartTime` for `2016-12-05T14:20:00Z` (5 de dezembro de 2016 às 4h20), o horário real de término seria definido como 5 de dezembro de 2016 às 5h20. Para encontrar o `ExpectedExecutionDurationInMinutes` para um tipo de alteração específico, execute este comando:
>
> ```
> aws amscm --profile saml get-change-type-version --
> change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.
> {ExpectedDuration:ExpectedExecutionDurationInMinutes}"
> ```

Use a opção RFC Priority

Use a opção Prioridade nos tipos de `execution mode = manual` alteração para alertar as operações do AMS sobre a urgência da solicitação.

Opção prioritária em`execution mode = manual`:

Especifique a prioridade de um RFC manual como Alta, Média ou Baixa. RFCs classificados como Alto são revisados e aprovados antes de serem RFCs classificados como Médios, sujeitos aos objetivos de nível de serviço da RFC (SLOs) e seus prazos de envio. RFCs com baixa prioridade ou nenhuma prioridade especificada são processados na ordem em que são enviados.

Aprovar ou rejeitar RFCs

RFCs enviado com aprovação obrigatória (manual) CTs deve ser aprovado por você ou pela AMS. Os pré-aprovados CTs são processados automaticamente. Para obter mais informações, consulte Requisitos de aprovação do CT.

> **Note**
>
> Ao usar “revisão obrigatória” CTs, o AMS recomenda que você use a opção ASAP Scheduling (escolha ASAP no console, deixe a hora de início e término em branco na API/CLI), pois isso CTs exige que um operador do AMS examine a RFC e, possivelmente, se comunique com você antes que ela possa ser aprovada e executada. Se você agendá-los RFCs, aguarde pelo menos 24 horas. Se a aprovação não ocorrer antes do horário de início programado, a RFC será rejeitada automaticamente.

Se um RFC exigido para aprovação for enviado com sucesso pelo AMS, ele deverá ser aprovado explicitamente por você. Ou, se você enviar uma RFC exigida para aprovação, ela deverá ser aprovada pelo AMS. Se você precisar aprovar uma RFC enviada pelo AMS, um e-mail ou outra comunicação predeterminada será enviada para você solicitando a aprovação. A comunicação inclui o ID do RFC. Depois que a comunicação for enviada, faça o seguinte:

- Aprovar ou rejeitar o console: use a página de detalhes do RFC para o RFC relevante:

- Aprovação de API/CLI: ApproveRfcmarca uma alteração como aprovada. A ação deve ser tomada pelo proprietário e pelo operador, se ambos forem necessários. Veja a seguir um exemplo de comando CLI approve. No exemplo a seguir, substitua RFC_ID pela ID de RFC apropriada.

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

- Rejeição de API/CLI: RejectRfcmarca uma alteração como rejeitada. Veja a seguir um exemplo de comando de rejeição da CLI. No exemplo a seguir, substitua RFC_ID pela ID de RFC apropriada.

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

Solicitar períodos de execução restritos do RFC

Anteriormente conhecidos como dias de blackout, você pode solicitar a restrição de determinados períodos de tempo. Nenhuma alteração pode ser executada durante esses períodos.

Para definir um período de execução restrito, use a operação da UpdateRestrictedExecutionTimesAPI e defina um período específico, em UTC. O período que você especifica substitui todos os períodos anteriores que foram especificados. Se você enviar uma RFC

durante o tempo de execução restrito especificado, o envio falhará com o erro Invalid RFC Schedule. Você pode especificar até 200 períodos restritos. Por padrão, nenhum período restrito é definido. Veja a seguir um exemplo de comando de solicitação (com a autenticação SAML configurada):

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

Você também pode ver sua RestrictedExecutionTimes configuração atual executando a operação ListRestrictedExecutionTimesda API. Exemplo:

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

Se você quiser enviar um RFC durante um tempo de execução restrito especificado, adicione o RestrictedExecutionTimesOverrideIdcom o valor de e OverrideRestrictedTimeRanges, em seguida, envie o RFC como faria normalmente. É uma prática recomendada usar esse método somente para uma RFC crítica ou de emergência. Para obter mais informações, consulte a referência da API para SubmitRfc.

Crie, clone, atualize, encontre e cancele RFCs

Os exemplos a seguir orientam você em várias operações de RFC.

Tópicos

- Crie um RFC
- Clonar RFCs (recriar) com o console AMS
- Atualizar RFCs
- Encontre RFCs
- Cancelar RFCs

Crie um RFC

Criando um RFC com o console

A seguir está a primeira página do processo de criação de RFC no console AMS, com os cartões rápidos abertos e os tipos de alteração de navegação ativos:

A seguir está a primeira página do processo de criação de RFC no console AMS, com a opção Selecionar por categoria ativa:

Como funciona:

1. Navegue até a página Criar RFC: No painel de navegação esquerdo do console AMS, clique RFCspara abrir a página da RFCs lista e, em seguida, clique em Criar RFC.
2. Escolha um tipo de alteração popular (CT) na visualização padrão Procurar tipos de alteração ou selecione uma CT na visualização Escolher por categoria.
   - Navegar por tipo de alteração: você pode clicar em um CT popular na área de criação rápida para abrir imediatamente a página Executar RFC. Observe que você não pode escolher uma versão mais antiga do CT com a criação rápida.

     Para classificar CTs, use a área Todos os tipos de alteração na exibição Cartão ou Tabela. Em qualquer exibição, selecione uma CT e clique em Criar RFC para abrir a página Executar RFC. Se aplicável, a opção Criar com uma versão mais antiga aparece ao lado do botão Criar RFC.
   - Escolha por categoria: selecione uma categoria, subcategoria, item e operação e a caixa de detalhes do CT será aberta com a opção Criar com uma versão mais antiga, se aplicável. Clique em Criar RFC para abrir a página Executar RFC.
3. Na página Executar RFC, abra a área do nome do CT para ver a caixa de detalhes do CT. É necessário um Assunto (preenchido se você escolher seu CT na visualização Procurar tipos de alteração). Abra a área Configuração adicional para adicionar informações sobre o RFC.

   Na área Configuração de execução, use as listas suspensas disponíveis ou insira valores para os parâmetros necessários. Para configurar parâmetros de execução opcionais, abra a área Configuração adicional.
4. Ao terminar, clique em Executar. Se não houver erros, a página RFC criada com sucesso será exibida com os detalhes da RFC enviada e a saída inicial de execução.
5. Abra a área Parâmetros de execução para ver as configurações que você enviou. Atualize a página para atualizar o status de execução do RFC. Opcionalmente, cancele a RFC ou crie uma cópia dela com as opções na parte superior da página.

Criando um RFC com a CLI

Como funciona:

1. Use o Inline Create (você emite um `create-rfc` comando com todos os parâmetros de RFC e execução incluídos) ou o Template Create (você cria dois arquivos JSON, um para os parâmetros RFC e outro para os parâmetros de execução) e emita o `create-rfc` comando com os dois arquivos como entrada. Ambos os métodos são descritos aqui.
2. Envie o `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: com o ID RFC retornado.

   Monitore o `aws amscm get-rfc --rfc-id` *`ID`* comando RFC:.

Para verificar a versão do tipo de alteração, use este comando:

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

> **Note**
>
> Você pode usar qualquer `CreateRfc` parâmetro com qualquer RFC, independentemente de eles fazerem parte do esquema para o tipo de alteração. Por exemplo, para receber notificações quando o status da RFC mudar, adicione essa linha `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` à parte dos parâmetros da RFC da solicitação (não aos parâmetros de execução). Para obter uma lista de todos os CreateRfc parâmetros, consulte a Referência da API de gerenciamento de alterações do AMS.

CRIAÇÃO EM LINHA:

Execute o comando create RFC com os parâmetros de execução fornecidos em linha (aspas de escape ao fornecer parâmetros de execução em linha) e, em seguida, envie a ID de RFC retornada. Por exemplo, você pode substituir o conteúdo por algo assim:

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

CRIAÇÃO DE MODELO:

> **Note**
>
> Este exemplo de criação de um RFC usa o tipo de alteração de pilha do Load Balancer (ELB).

1. Encontre a tomografia computadorizada relevante. O comando a seguir pesquisa resumos de classificação de CT para aqueles que contêm “ELB” no nome do item e cria a saída da categoria, item, operação e ChangeType ID em forma de tabela (a subcategoria de ambos é). `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. Encontre a versão mais atual do CT:

   `ChangeTypeIdeChangeTypeVersion`: O ID do tipo de alteração para este passo a passo é `ct-123h45t6uz7jl` (criar ELB). Para descobrir a versão mais recente, execute este comando:

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

3. Conheça as opções e os requisitos. O comando a seguir gera o esquema em um arquivo JSON chamado .json. CreateElbParams

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

4. Modifique e salve o arquivo JSON dos parâmetros de execução. Este exemplo chama o arquivo de CreateElbParams .json.

Para uma CT de provisionamento, o StackTemplateId é incluído no esquema e deve ser enviado nos parâmetros de execução.

Por TimeoutInMinutes quantos minutos são permitidos para a criação da pilha antes que a RFC falhe, essa configuração não atrasará a execução da RFC, mas você deverá dedicar tempo suficiente (por exemplo, não especifique “5"). Os valores válidos são de “60" a “360", pois, CTs com longa duração UserData: Crie EC2 e crie ASG. Recomendamos o máximo permitido de “60" para todos os outros CTs provisionamentos.

Forneça a ID da VPC em que você deseja que a pilha seja criada; você pode obter a ID da VPC com o comando da 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. Envie o modelo RFC JSON para um arquivo em sua pasta atual chamado CreateElbRfc .json:

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

6. Modifique e salve o CreateElbRfc arquivo.json. Como você criou os parâmetros de execução em um arquivo separado, remova a `ExecutionParameters` linha. Por exemplo, você pode substituir o conteúdo por algo assim:

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

```
}
```

7. Crie o RFC. O comando a seguir especifica o arquivo de parâmetros de execução e o arquivo de modelo RFC:

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

Você recebe a ID da nova RFC na resposta e pode usá-la para enviar e monitorar a RFC. Até que você o envie, o RFC permanece no estado de edição e não inicia.

Dicas

> **Note**
>
> Você pode usar o AMS API/CLI para criar um RFC sem criar um arquivo RFC JSON ou um arquivo JSON de parâmetros de execução de CT. Para fazer isso, você usa o `create-rfc` comando e adiciona o RFC e os parâmetros de execução necessários ao comando, isso é chamado de “Inline Create”. Observe que todo o provisionamento CTs continha no `execution-parameters` bloco uma `Parameters` matriz com os parâmetros do recurso. Os parâmetros devem ter aspas escapadas com uma barra invertida (\).
> O outro método documentado de criar um RFC é chamado de “Criação de modelo”. É aqui que você cria um arquivo JSON para os parâmetros RFC e outro arquivo JSON para os parâmetros de execução e envia os dois arquivos com o comando. `create-rfc` Esses arquivos podem servir como modelos e ser reutilizados para o futuro. RFCs
> Ao criar RFCs com modelos, você pode usar um comando para criar o arquivo JSON com o conteúdo desejado emitindo um comando conforme mostrado. Os comandos criam um arquivo chamado “parameters.json” com o conteúdo mostrado; você também pode usar esses comandos para criar o arquivo RFC JSON.

Clonar RFCs (recriar) com o console AMS

Você pode usar o console AMS para clonar um RFC existente.

Para clonar ou recriar um RFC usando o console AMS, siga estas etapas:

1. Encontre o RFC relevante. Na navegação à esquerda, clique em RFCs.

O RFCs painel é aberto.

2. Percorra as páginas até encontrar o RFC que você deseja clonar. Use a opção Filtro para restringir a lista. Escolha o RFC que você deseja clonar.

   A página de detalhes do RFC é aberta.

3. Clique em Criar uma cópia.

   A página Criar uma solicitação de alteração é aberta com todas as opções definidas como na RFC original.

4. Faça as alterações desejadas. Para definir opções adicionais, altere a opção Básico para Avançado. Depois de definir todas as opções, escolha Enviar.

   A página de detalhes da RFC ativa é aberta com uma nova ID de RFC para a RFC clonada e a RFC clonada aparece no painel da RFC.

Atualizar RFCs

Você pode reenviar uma RFC que tenha sido rejeitada ou que ainda não tenha sido enviada, atualizando a RFC e, em seguida, enviando-a ou reenviando-a. Observe que a RFCs maioria é rejeitada porque o especificado `RequestedStartTime` foi aprovado antes do envio ou porque o especificado TimeoutInMinutes é inadequado para executar o RFC (como TimeoutInMinutes não prolonga um RFC bem-sucedido, recomendamos sempre definir isso para pelo menos “60" e até “360" para um grupo da Amazon ou do EC2 Amazon Auto Scaling EC2 com longa duração). UserData Esta seção descreve como usar a versão CLI do `UpdateRfc` comando para atualizar uma RFC com um novo parâmetro RFC ou novos parâmetros usando JSON em sequência de caracteres ou um arquivo de parâmetros atualizado.

Este exemplo descreve o uso da versão CLI da UpdateRfc API AMS (consulte Atualizar RFC). Embora existam tipos de alteração para atualizar alguns recursos (DNS privado e público, pilhas de balanceadores de carga e configuração de patches de pilha), não há CT para atualizar uma RFC.

Recomendamos que você envie uma UpdateRfc operação por vez. Se você enviar várias atualizações, por exemplo, em uma pilha de DNS, as atualizações podem falhar ao tentar atualizar o DNS ao mesmo tempo.

DADOS NECESSÁRIOS`RfcId`: O RFC que você está atualizando.

DADOS OPCIONAIS`ExecutionParameters`: A menos que você esteja atualizando um campo não obrigatório, por exemplo`Description`, você enviaria parâmetros de execução modificados para resolver os problemas que fizeram com que a RFC fosse rejeitada ou cancelada. Todos os valores não nulos enviados sobrescrevem esses valores no RFC original.

1. Encontre o RFC relevante rejeitado ou cancelado, você pode usar este comando (você pode substituir o valor por): `Canceled`

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

2. Você pode modificar qualquer um dos seguintes parâmetros de RFC:

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

Exemplo de comando atualizando o campo Descrição:

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

Exemplo de comando atualizando o ExecutionParameters VpcId campo:

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

Exemplo de comando atualizando o RFC com um arquivo de parâmetros de execução que contém as atualizações; veja exemplo de arquivo de parâmetros de execução na etapa 2 de: EC2 stack | Create:

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

3. Reenvie a RFC usando `submit-rfc` a mesma ID de RFC que você tem de quando a RFC foi criada pela primeira vez:

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

   Se o RFC for bem-sucedido, você não receberá nenhuma mensagem de confirmação ou erro na linha de comando.
4. Para monitorar o status da solicitação e visualizar a Saída de Execução, execute o comando a seguir.

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

Encontre RFCs

Encontre uma solicitação de alteração (RFC) com o console

Para encontrar um RFC usando o console AMS, siga estas etapas.

> **Note**
>
> Esse procedimento se aplica somente aos agendados RFCs, ou seja, RFCs que não utilizaram a opção ASAP.

1. Na navegação à esquerda, clique em RFCs.

   O RFCs painel é aberto.
2. Percorra a lista ou use a opção Filtro para refinar a lista.

   A lista de RFC muda de acordo com os critérios do filtro.
3. Escolha o link Assunto para o RFC que você deseja.

   A página de detalhes da RFC é aberta para essa RFC com informações, incluindo a ID da RFC.
4. Se houver muitos RFCs no painel, você pode usar a opção Filtro para pesquisar por RFC:

- Assunto: A linha de assunto ou título (na API/CLI) fornecida à RFC quando ela foi criada.
- ID do RFC: O identificador do RFC.
- Estado da atividade: se você conhece o estado da RFC, pode escolher entre AwsOperatorAssignedsignificar que um operador está examinando a RFC no momento, o que AwsActionPendingsignifica que um operador de AMS deve realizar algo antes que a execução da RFC possa continuar ou CustomerActionPendingque você precisa realizar alguma ação antes que a execução da RFC possa continuar.
- Status: Se você souber o status do RFC, poderá escolher entre:
  - Programado: RFCs que foram programados.
  - Cancelado: RFCs que foram cancelados.
  - Em andamento: RFCs em andamento.
  - Sucesso: RFCs executado com sucesso.
  - Rejeitado: RFCs que foram rejeitados.
  - Edição: RFCs que estão sendo editadas.
  - Fracasso: RFCs isso falhou.
  - Aprovação pendente: RFCs isso não pode continuar até que o AMS ou você aprove. Normalmente, isso indica que você precisa aprovar o RFC. Você receberá uma notificação de serviço sobre isso na sua lista de solicitações de serviço.
- Tipo de alteração: escolha a categoria, a subcategoria, o item e a operação, e a ID do tipo de alteração será recuperada para você.
- Hora de início solicitada ou Hora de término solicitada: essa opção de filtro permite escolher Antes ou Depois e, em seguida, inserir uma Data e, opcionalmente, uma Hora (hh:mm e fuso horário). Esse filtro opera com sucesso somente quando programado RFCs (não o mais rápido possível RFCs).
- Status: Programado, Cancelado, Em andamento, Sucesso, Rejeitado, Edição ou Falha.
- Assunto: O assunto (ou título, se o RFC foi criado com a API/CLI) que você deu ao RFC.
- ID do tipo de alteração: use o identificador do tipo de alteração enviado com o RFC.

A pesquisa permite que você adicione os filtros, conforme mostrado na captura de tela a seguir.

5. Clique no link Assunto do RFC que você deseja.

A página de detalhes da RFC é aberta para essa RFC com informações, incluindo a ID da RFC.

Encontrando uma solicitação de mudança (RFC) com a CLI

Você pode usar vários filtros para encontrar um RFC.

Para verificar a versão do tipo de alteração, use este comando:

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

> **Note**
>
> Você pode usar qualquer `CreateRfc` parâmetro com qualquer RFC, independentemente de eles fazerem parte do esquema para o tipo de alteração. Por exemplo, para receber notificações quando o status da RFC mudar, adicione essa linha `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` à parte dos parâmetros da RFC da solicitação (não aos parâmetros de execução). Para obter uma lista de todos os CreateRfc parâmetros, consulte a Referência da API de gerenciamento de alterações do AMS.

Se você não anotar o ID do RFC e precisar encontrá-lo posteriormente, poderá usar o sistema de gerenciamento de alterações (CM) do AMS para pesquisá-lo e restringir os resultados com um filtro ou consulta.

1. A ListRfcSummariesoperação da API CM tem filtros. Você pode filtrar os resultados com base em um `Attribute` e `Value` combinados em uma operação AND lógica ou com base em um `AttributeCondition`, a `Values` e.

   Filtragem RFC

Atributo	Valores válidos	Condições válidas	Condição padrão	Observações
ActualEndTime	Qualquer string representando uma data e hora	Antes, depois, entre	Nenhum	A condição Antes ou Depois aceita somente um valor

Atributo	Valores válidos	Condições válidas	Condição padrão	Observações
	ISO86 01 (por exemplo, “20170101 T000000Z”)			no campo Valores. A condição Between deve ter exatament e dois valores no campo Valores, onde o primeiro valor deve representar uma data que ocorre antes do segundo valor
ActualStartTime	Qualquer string representando uma data e hora ISO86 01 (por exemplo, “20170101 T000000Z”)	Antes, depois, entre	Nenhum	A condição Antes ou Depois aceita somente um valor no campo Valores. A condição Between deve ter exatament e dois valores no campo Valores, onde o primeiro valor deve representar uma data que ocorre antes do segundo valor
AutomationStatusId	Manual, automatiz ado	Igual	Igual	Existem apenas dois status de automação
ChangeTypeId	Qualquer ID de tipo de alteração válida; por exemplo, ct-123h45t6uz7jl	Igual	Igual	Encontrando um tipo de alteração ou CSIO

Atributo	Valores válidos	Condições válidas	Condição padrão	Observações
ChangeTypeVersion	Qualquer ID de tipo de alteração válida; por exemplo, 1.0	Igual	Igual	Encontrando um tipo de alteração ou CSIO
CreatedBy	Qualquer sequência de caracteres (o tamanho máximo permitido é de 2048 caracteres)	Contém	Contém	O CreatedBy campo do RFC contém o ARN do usuário que o criou
CreatedTime	Qualquer string representando uma data e hora ISO86 01 (por exemplo, “20170101 T000000Z”)	Antes, depois, entre	Nenhum	A condição Antes ou Depois aceita somente um valor no campo Valores. A condição Between deve ter exatament e dois valores no campo Valores, onde o primeiro valor deve representar uma data que ocorre antes do segundo valor

Atributo	Valores válidos	Condições válidas	Condição padrão	Observações
LastModifiedTime	Qualquer string representando uma data e hora ISO86 01 (por exemplo, “20170101 T000000Z”)	Antes, depois, entre	Nenhum	A condição Antes ou Depois aceita somente um valor no campo Valores. A condição Between deve ter exatament e dois valores no campo Valores, onde o primeiro valor deve representar uma data que ocorre antes do segundo valor
LastSubmittedTime	Qualquer string representando uma data e hora ISO86 01 (por exemplo, “20170101 T000000Z”)	Antes, depois, entre	Nenhum	A condição Antes ou Depois aceita somente um valor no campo Valores. A condição Between deve ter exatament e dois valores no campo Valores, onde o primeiro valor deve representar uma data que ocorre antes do segundo valor

Atributo	Valores válidos	Condições válidas	Condição padrão	Observações
RequestedEndTime	Qualquer string representando uma data e hora ISO86 01 (por exemplo, “20170101 T000000Z”)	Antes, depois, entre	Nenhum	A condição Antes ou Depois aceita somente um valor no campo Valores. A condição Between deve ter exatament e dois valores no campo Valores, onde o primeiro valor deve representar uma data que ocorre antes do segundo valor
RequestedStartTime	Qualquer string representando uma data e hora ISO86 01 (por exemplo, “20170101 T000000Z”)	Antes, depois, entre	Nenhum	A condição Antes ou Depois aceita somente um valor no campo Valores. A condição Between deve ter exatament e dois valores no campo Valores, onde o primeiro valor deve representar uma data que ocorre antes do segundo valor
RfcStatusId	Cancelado, edição, falha,, InProgress, rejeitado PendingAp proval, agendado, sucesso	Igual	Igual	Atualize a lista de RFC no console AMS ou execute GetRfc

Atributo	Valores válidos	Condições válidas	Condição padrão	Observações
Cargo	Qualquer título RFC válido	Contém	Contém	Expressões regulares em cada campo individual não são suportada s. Pesquisa sem distinção entre maiúsculas e min

Exemplos:

Para encontrar todos os RFCs relacionados ao SQS (onde o SQS está contido na parte Item do CT), você pode usar este comando: IDs

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

O que retorna algo assim:

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

Outro filtro disponível `list-rfc-summaries` é`AutomationStatusId`, para procurar RFCs que sejam automáticos ou manuais:

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

Outro filtro disponível para `list-rfc-summaries` é `Title` (Assunto no console):

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

Exemplo da nova estrutura de solicitação em JSON que retorna RFCs onde:

- (O título CONTÉM a frase “Windows 2012" OU “Amazon Linux”) E
- (RfcStatusId É IGUAL A “Sucesso” OU "InProgress“) E
- (20170101T000000Z <= <= 20170103T000000Z) E (<= RequestedStartTime 20170103T000000Z) 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

Com o Advanced`Filters`, o AMS pretende descontinuar os seguintes campos em uma próxima versão:

- Valor: O campo Valor faz parte do campo Filtros. Use o campo Valores que oferece suporte a funcionalidades mais avançadas.

- RequestedEndTimeRange: use o campo RequestedEndTime interno de Filtros que oferece suporte a funcionalidades mais avançadas
- RequestedStartTimeRange: use o campo RequestedStartTime interno de Filtros que oferece suporte a funcionalidades mais avançadas.

Para obter informações sobre o uso de consultas CLI, consulte Como filtrar a saída com a opção --query e a referência da linguagem de consulta, Especificação. JMESPath

2. Se você estiver usando o console AMS:

   Vá para a página da RFCslista. Se necessário, você pode filtrar o assunto da RFC, que é o que você inseriu como RFC `Title` ao criá-la.

Dicas

> **Note**
>
> Esse procedimento se aplica somente aos agendados RFCs, ou seja, RFCs que não utilizaram a opção ASAP.

Cancelar RFCs

Você pode cancelar um RFC usando o console ou a API/CLI do AMS.

Para cancelar uma RFC com o console, localize a RFC na sua lista de RFC, abra-a e clique em Cancelar.

Dados necessários:

- `Reason`: Por que você está cancelando o RFC.
- `RfcId`: O RFC que você está cancelando.

1. Normalmente, você cancelaria uma RFC logo após enviá-la (portanto, a ID da RFC deve ser útil); caso contrário, você não poderá cancelá-la, a menos que a tenha agendado e seja antes do horário de início especificado. Se precisar encontrar o ID do RFC, você pode usar

este comando (você pode substituir o `Value` com `PendingApproval` por um RFC aprovado manualmente):

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

2. Exemplo de comando para cancelar um RFC:

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

Use o console AMS com RFCs

O console AMS fornece recursos para ajudá-lo a ter sucesso na criação e no envio RFCs.

Use a página Lista de RFC (Console)

A página RFCsde lista do console AMS fornece as seguintes opções:

- Pesquisa avançada de RFC por meio de um filtro. Para mais informações, consulte Encontre RFCs.
- Descobrindo a última vez em que o RFC foi modificado. Esse valor representa a última vez em que o status da RFC foi alterado.
- Visualizando detalhes da RFC com o assunto da RFC. A escolha desse link abre a página de detalhes desse RFC.
- Visualizando o status do RFC. Para obter mais informações, consulte Entenda os códigos de status do RFC

Use a criação rápida de RFC (console)

Use os cartões de criação rápida do RFC ou a tabela de listas, ou escolha os tipos de alteração RFCs por classificação.

Para saber mais, consulte Crie um RFC.

Adicionar correspondência e anexos RFC (console)

Você pode adicionar correspondência a uma RFC depois que ela for enviada e antes de ser aprovada; por exemplo, enquanto ela estiver no estado de ""PendingApproval. Depois que um RFC é aprovado (em um estado de “Programado” ou "InProgress“), a correspondência não pode ser adicionada, pois pode ser interpretada como uma alteração na solicitação. Depois que um RFC é concluído (em um estado de “Cancelado”, “Rejeitado”, “Sucesso” ou “Falha”), a correspondência é novamente ativada, embora a correspondência seja desativada quando um RFC é fechado por mais de 30 dias.

> **Note**
>
> Cada correspondência é limitada a 5.000 caracteres.

Limitações para anexos:

- Apenas três anexos por correspondência.
- Limite de cinquenta anexos por RFC.
- Cada anexo deve ter menos de 5 MB.
- Somente arquivos de texto são aceitos, como texto simples (`.txt`), valores separados por vírgula (`.csv`), JSON () ou YAML (`.json`). `.yaml` No caso do formato YAML, o arquivo deve ser anexado usando a extensão `.yaml` de arquivo.

  > **Note**
  >
  > Arquivos de texto com conteúdo XML são proibidos. Se você tiver conteúdo XML para compartilhar com o AMS, use uma solicitação de serviço.

- Os nomes dos arquivos são limitados a 255 caracteres, com apenas números, letras, espaços, traços (-), sublinhados (_) e pontos (.).
- Atualmente, não há suporte para atualizar e excluir anexos em um RFC.

Para adicionar correspondência e anexos a um RFC, siga estas etapas:

1. No console AMS, na página de detalhes da RFC de uma RFC, encontre a seção Correspondência na parte inferior da página.

Antes de qualquer correspondência:

Depois de alguma correspondência:

2. Para adicionar uma nova correspondência, digite sua mensagem na caixa de texto Responder. Para anexar arquivos relacionados à correspondência, escolha Adicionar anexo e escolha os arquivos desejados.

3. Ao terminar, escolha Enviar.

   A nova correspondência, junto com os links para os arquivos anexados, aparecem na lista de correspondência na página de detalhes da RFC.

Configurar notificações por e-mail RFC (console)

A página de criação de Solicitações de Mudança do console AMS oferece a opção de adicionar endereços de e-mail para receber notificações de alterações no estado da RFC:

Além disso, você pode adicionar endereços de e-mail para notificações de qualquer tipo de alteração, por exemplo:

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

Adicione uma linha semelhante (`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`) a qualquer solicitação embutida ou modelo de alteração de tipo na parte de parâmetros RFC da solicitação, não na parte de parâmetros.

Saiba mais sobre os parâmetros comuns de RFC

A seguir estão os parâmetros de RFC que você deve enviar e os parâmetros que são comumente usados em: RFCs

- Altere as informações do tipo: ChangeTypeId ChangeTypeVersion e. Para obter uma lista do tipo de alteração IDs e dos números de versão, consulte Referência do tipo de alteração.

  Execute `list-change-type-classification-summaries` na CLI com o `query` argumento para restringir os resultados. Por exemplo, restrinja os resultados para alterar os tipos que contêm "Acesso" no `Item` nome.

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

  Execute `get-change-type-version` e especifique o ID do tipo de alteração. O comando a seguir obtém a versão CT para ct-2tylseo8rxfsc.

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

- Título: Um nome para o RFC; isso se torna o assunto do RFC na lista de RFC do console AMS e você pode pesquisá-lo com o `GetRfc` comando e um filtro ativado `Title`
- Agendamento: Se você quiser um RFC agendado, deverá incluir os `RequestedEndTime` parâmetros `RequestedStartTime` e ou usar a opção Agendar esta alteração do console. Para um ASAP RFC (que é executado assim que aprovado), ao usar a CLI, deixe e anule. `RequestedStartTime` `RequestedEndTime` Ao usar o console, aceite a opção ASAP.

  Se o `RequestedStartTime` for perdido, o RFC será rejeitado.
- Provisionamento CTs: os parâmetros de execução ou `Parameters` são as configurações específicas necessárias para provisionar o recurso. Eles variam muito dependendo da tomografia computadorizada.
- Não provisionamento CTs: CTs que não provisionam um recurso, como acesso CTs ou Outro | Outro, ou excluem a pilha, têm parâmetros de execução mínimos e nenhum bloqueio. `Parameters`
- Alguns RFCs também exigem que você especifique um`TimeoutInMinutes`, ou quantos minutos são permitidos para a criação da pilha antes que o RFC falhe. Os valores válidos são de 60 (minutos) a 360, para longa duração UserData. Se a execução não puder ser concluída antes de ser `TimeoutInMinutes` excedida, o RFC falhará. No entanto, essa configuração não atrasa a execução do RFC.
- RFCs que criam instâncias, como um bucket do S3 ou um ELB, geralmente fornecem um esquema que permite adicionar até sete tags (pares de chave/valor). Você pode adicionar mais tags ao seu

bucket do S3 enviando uma RFC usando Deployment | Advanced stack components | Tag | Create change type (ct-3cx7we852p3af). EC2, EFS, RDS e os esquemas de várias camadas (HA de duas camadas e HA de uma camada) permitem até cinquenta tags. As tags são especificadas na `ExecutionParameters` parte do esquema. Fornecer etiquetas pode ser de grande valor. Para obter mais informações, consulte Como marcar seus EC2 recursos da Amazon.

Ao usar o console AMS, você deve abrir a área de configuração adicional para adicionar tags.

> **Tip**
>
> Muitos esquemas de CT têm um `Name` campo `Description` and próximo ao topo do esquema. Esses campos são usados para nomear a pilha ou o componente da pilha, eles não nomeiam o recurso que você está criando. Alguns esquemas oferecem um parâmetro para nomear o recurso que você está criando e outros não. Por exemplo, o esquema CT para Create EC2 stack não oferece um parâmetro para nomear a EC2 instância. Para fazer isso, você deve criar uma tag com a chave “Nome” e o valor do que você deseja que o nome seja. Se você não criar essa tag, sua EC2 instância será exibida no EC2 console sem um atributo name.

Use a opção AWS Região RFC

Os endpoints da API e da CLI (`amscmeamsskms`) do AMS estão ativados. `us-east-1` Se você se federar com a Security Assertion Markup Language (SAML), serão fornecidos scripts na integração que definem sua região como us-east-1. AWS Se você usa SAML, não precisa especificar a `--region` opção ao emitir um comando. Se o SAML estiver configurado para usar us-east-1, mas sua conta não estiver AWS nessa região, você deverá especificar a região integrada à conta ao emitir outros comandos (por exemplo,). AWS `aws s3`

> **Note**
>
> A maioria dos exemplos de comando fornecidos neste guia não inclui a `--region` opção.

Inscreva-se para receber o e-mail diário da RFC

Você pode se inscrever para receber um e-mail diário resumindo a atividade de RFC em sua conta nas últimas 24 horas usando o recurso de resumo de RFC. O recurso de resumo do RFC é um

processo simplificado que reduz o número de notificações por e-mail que você recebe em relação à sua conta. RFCs O resumo do RFC pode reduzir a probabilidade de você perder ações que estão pendentes de resposta.

Para ativar o recurso de resumo de RFC, entre em contato com seu AMS Cloud Service Delivery Manager (CSDM). O CSDM inscreve você. Você pode solicitar até 20 endereços de e-mail (ou aliases) para incluir na sua lista de e-mails do RFC Digest. A programação atual de e-mails é fixada às 09:00 UTC-8.

Para desativar o recurso de resumo de RFC, entre em contato com seu CSDM com sua solicitação.

Se você não configurar o resumo da RFC e quiser notificações sobre sua RFCs, ou se quiser informações mais detalhadas RFCs do que as fornecidas pelo resumo da RFC, use o Sistema de Gerenciamento de Mudanças para configurar notificações de CloudWatch eventos ou notificações por e-mail para cada RFC individual sobre a qual deseja informações. Para obter informações sobre como configurar notificações de RFC, consulte Notificações de alteração de estado de RFC.

Os tópicos contidos no resumo do RFC incluem o seguinte:

- Aprovação pendente do cliente: listas RFCs que estão em PendingApprovalstatus, aguardando sua aprovação
- Resposta pendente do cliente: listas RFCs que aguardam sua resposta na correspondência RFC
- Aprovação ou resposta pendente da AWS: listas RFCs que aguardam resposta ou aprovação do AMS
- Concluído: Listas RFCs com status de sucesso, falha, cancelado e rejeitado

Veja a seguir um exemplo de resumo de RFC:

Quais são os tipos de mudança?

O tipo de alteração se refere à ação que uma solicitação de mudança (RFC) do AWS Managed Services (AMS) executa e engloba a ação de mudança em si e o tipo de alteração — manual versus automatizada. O AMS tem uma grande coleção de tipos de alteração não usados por outros serviços web da Amazon. Você usa esses tipos de alteração ao enviar uma solicitação de alteração (RFC) para implantar, gerenciar ou obter acesso a recursos.

Tópicos

- Automatizado e manual CTs
- Requisitos de aprovação do CT
- Alterar versões do tipo
- Crie tipos de alteração
- Atualizar tipos de alteração
- Tipos de alteração somente internos
- Esquemas de tipo de alteração
- Gerenciando permissões para tipos de alteração
- Eliminação de informações confidenciais dos tipos de alteração
- Encontrando um tipo de alteração, usando a opção de consulta

Automatizado e manual CTs

Uma restrição nos tipos de alteração é se eles são automatizados ou manuais. Esse é o `AutomationStatusId` atributo do tipo de alteração, chamado de modo de execução no console do AMS.

Os tipos de mudança automatizados têm resultados e tempos de execução esperados e são executados no sistema automatizado do AMS, geralmente em uma hora ou menos (isso depende muito dos recursos que a CT está fornecendo). Os tipos de alteração manual são incomuns, mas são tratados de forma diferente porque exigem que um operador do AMS atue na RFC antes que ela possa ser executada. Às vezes, isso significa comunicar-se com o remetente do RFC, portanto, os tipos de alteração manual exigem vários períodos de tempo para serem concluídos.

Para todos os agendados RFCs, um horário de término não especificado é escrito como o horário especificado `RequestedStartTime` mais o `ExpectedExecutionDurationInMinutes` atributo do tipo de alteração enviado. Por exemplo, se `ExpectedExecutionDurationInMinutes` for “60" (minutos) e o especificado `RequestedStartTime` for `2016-12-05T14:20:00Z` (5 de dezembro de 2016 às 4h20), o horário real de término seria definido como 5 de dezembro de 2016 às 5h20. Para encontrar o `ExpectedExecutionDurationInMinutes` para um tipo de alteração específico, execute este comando:

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

> **Note**
>
> Programado RFCs com o modo de execução = Manual, no console, deve ser configurado para ser executado pelo menos 24 horas no futuro. Essa ressalva não se aplica à API/CLI do AMS, mas ainda é importante agendar o manual com RFCs pelo menos 8 horas de antecedência.

> **Note**
>
> Ao usar “revisão obrigatória” CTs, o AMS recomenda que você use a opção ASAP Scheduling (escolha ASAP no console, deixe a hora de início e término em branco na API/CLI), pois isso CTs exige que um operador do AMS examine a RFC e, possivelmente, se comunique com você antes que ela possa ser aprovada e executada. Se você agendá-los RFCs, aguarde pelo menos 24 horas. Se a aprovação não ocorrer antes do horário de início programado, a RFC será rejeitada automaticamente.

O AMS visa responder a uma tomografia computadorizada manual em quatro horas e corresponderá o mais rápido possível, mas pode levar muito mais tempo para que a RFC seja realmente executada.

Para obter uma lista dos CTs que são manuais e precisam ser revisados pelo AMS, consulte o arquivo CSV do tipo de alteração, disponível na página Recursos do desenvolvedor do console.

YouTube Vídeo: Como posso encontrar tipos de alteração automatizados para o AMS RFCs?

Para encontrar o modo de execução de um CT no console do AMS, você deve usar a opção de pesquisa Procurar tipos de alteração. Os resultados mostram o modo de execução do tipo de alteração correspondente ou dos tipos de alteração.

Para encontrar um tipo de alteração específico usando a CLI do AMS, execute este comando: `AutomationStatus`

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

Você também pode pesquisar os tipos de alteração na Referência de tipo de alteração do AMS, que fornece informações sobre todos os tipos de alteração do AMS.

> **Note**
>
> Atualmente, o AMS API/CLI não faz parte da AWSAPI/CLI. To access the AMS API/CLI. Você baixa o SDK do AMS por meio do console do AMS.

Requisitos de aprovação do CT

O AMS CTs sempre tem duas condições de aprovação, AwsApprovalIdCustomerApprovalIdque indicam se o RFC exige que o AMS ou você, ou qualquer pessoa, aprove a execução.

A condição de aprovação está um pouco relacionada ao modo de execução; para obter detalhes, consulteAutomatizado e manual CTs.

Para descobrir a condição de aprovação de um CT, você pode consultar a Referência de Tipo de Alteração do AMS ou executar GetChangeTypeVersion. Ambos também oferecem o modo CT **`AutomationStatusId`** ou Execução.

Você pode aprovar RFCs usando o console AMS ou com o seguinte comando:

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

Condição de aprovação do CT

Se a condição de aprovação do CT for	Requer aprovação de	E
`AwsApprovalId: Required`	O sistema de mudança de tipo do AMS,	Nenhuma ação é necessária. Essa condição é típica de automação CTs.
`AwsApprovalId: NotRequiredIfSubmitter`	O sistema de tipo de alteração do AMS e mais ninguém, se o RFC enviado for para a conta	Nenhuma ação é necessária. Essa condição é típica dos manuais CTs porque eles sempre serão revisados pelos operadores do AMS.

Se a condição de aprovação do CT for	Requer aprovação de	E
	contra a qual foi enviado,	
`CustomerApprovalId: NotRequired`	O sistema de mudança de tipo do AMS,	Se a RFC passar pelas verificações de sintaxe e parâmetros, ela será aprovada automaticamente.
`CustomerApprovalId: Required`	O sistema de mudança de tipo do AMS e você,	Uma notificação é enviada a você e você deve aprovar explicitamente a RFC, respondendo à notificação ou executando a operação. ApproveRfc
`CustomerApprovalId: NotRequiredIfSubmitter`	O sistema de mudança de tipo do AMS e mais ninguém, se você enviou o RFC.	Se a RFC passar pelas verificações de sintaxe e parâmetros, ela será aprovada automaticamente.
Incidente ou patch de segurança urgente	AMS	É aprovado e implementado automaticamente.

Alterar versões do tipo

Os tipos de alteração são versionados e a versão muda quando uma atualização importante é feita no tipo de alteração.

Depois de selecionar um tipo de alteração usando o console AMS, você tem a opção de abrir a área Configuração adicional e selecionar uma versão do tipo de alteração. Você também pode especificar uma versão do tipo de alteração na linha de API/CLI comando. Talvez você queira fazer isso por vários motivos, incluindo:

- Você sabe que a versão do tipo de alteração Atualizar que você deseja deve corresponder à versão do tipo Criar alteração que você usou para criar o recurso que agora deseja atualizar.

Por exemplo, você pode ter uma instância do Elastic Load Balancer (ELB) criada com o tipo de alteração do ELB Create versão 1. Para atualizá-lo, escolha ELB Update version 1.

- Você deseja usar uma versão do tipo de alteração que tenha opções diferentes do tipo de alteração mais recente. Não recomendamos isso porque as atualizações do AMS mudam de tipo principalmente por motivos de segurança e recomendamos que você sempre escolha a versão mais recente.

Crie tipos de alteração

Os tipos de alteração de criação são combinados version-to-version com os tipos de alteração de atualização. Ou seja, a versão do tipo de alteração que você usa para provisionar um recurso deve corresponder à versão do tipo de alteração de atualização que você usaria posteriormente para modificar esse recurso. Por exemplo, se você criar um bucket do S3 com o tipo de alteração Create S3 Bucket versão 2.0 e, posteriormente, quiser enviar um RFC para modificar esse bucket do S3, você também deverá usar o tipo de alteração do Update S3 Bucket versão 2.0, mesmo que haja um tipo de alteração do Update S3 Bucket com a versão 3.0.

Recomendamos manter um registro da ID do tipo de alteração e da versão que você usa ao provisionar um recurso com o tipo Criar alteração, caso queira usar posteriormente um tipo de alteração Atualizar para modificá-lo.

Atualizar tipos de alteração

O AMS fornece tipos de alteração de atualização para atualizar recursos que foram criados com Criar tipos de alteração. Os tipos de alteração Atualizar devem corresponder version-to-version ao tipo Criar alteração usado originalmente para provisionar o recurso.

Recomendamos manter um registro do ID do tipo de alteração e da versão que você usa ao provisionar um recurso para facilitar a atualização.

YouTube Vídeo: Como uso CTs a atualização para alterar recursos em uma conta do AWS Managed Services (AMS)?

Tipos de alteração somente internos

Você pode ver os tipos de alteração que são somente para uso interno. Isso é para que você saiba quais ações o AMS pode ou faz. Se houver um tipo de alteração somente interno que você gostaria de ter disponível para seu uso, envie uma solicitação de serviço.

Por exemplo, há um Gerenciamento | Monitoramento e notificação | supressão de CloudWatch alarme | Atualizar CT que é somente interno. O AMS o usa para implantar atualizações de infraestrutura (como patches) para desativar as notificações de alarme que as atualizações possam acionar erroneamente. Quando esta CT for enviada, você notará a RFC da CT na sua lista de RFC. Qualquer CT somente interna implantada em uma RFC aparece na sua lista de RFC.

Esquemas de tipo de alteração

Todos os tipos de alteração fornecem um esquema JSON para sua entrada na criação, modificação ou acesso de recursos. O esquema fornece os parâmetros e suas descrições para você criar uma solicitação de alteração (RFC).

A execução bem-sucedida de um RFC resulta na saída da execução. Para provisionamento RFCs, a saída da execução inclui um “stack_id” que representa a pilha CloudFormation e pode ser pesquisado no console. CloudFormation Às vezes, a saída da execução inclui a saída do ID da instância criada e esse ID pode ser usado para pesquisar a instância no console da AWS correspondente. Por exemplo, a saída de execução do Create ELB CT inclui um “stack_id” que pode ser pesquisado CloudFormation e gera um key=ELB value= <stack-xxxx>que pode ser pesquisado no console da Amazon para o Elastic Load Balancing. EC2

Vamos examinar um esquema de tomografia computadorizada. Esse é o esquema do CodeDeploy Application Create, um esquema relativamente pequeno. Alguns esquemas têm `Parameter` áreas muito grandes.

```
{
  "$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": {
```

A primeira parte do esquema fornece informações ao AMS sobre o tipo de alteração solicitado.

```
      "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.",
      "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
```

O TimeoutInMinutes parâmetro permite que você indique um tempo limite para executar o tipo de alteração. Os valores válidos são de 60 a 360, para longos períodos. UserData

A seção Parâmetros é onde você especifica

```
    },
    "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.",
          "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"
  ]
```

as configurações para o recurso que você está criando ou para a ação que você está solicitando.

As seções “propried ades adicionais” permitem que você saiba quais parâmetro s são obrigatórios e quais são opcionais.

```
}
```

> **Note**
>
> Esse esquema permite até sete tags; no entanto, EFS EC2, RDS e os esquemas de criação de várias camadas permitem até 50 tags.

Gerenciando permissões para tipos de alteração

Você pode usar uma política personalizada para restringir quais tipos de alteração (CTs) estão disponíveis para diferentes grupos ou usuários.

Para saber mais sobre como fazer isso, consulte a seção Configuração de permissões do Guia do Usuário do AMS.

Eliminação de informações confidenciais dos tipos de alteração

Os esquemas de tipo de alteração do AMS oferecem um atributo de parâmetro, `"metadata":"ams:sensitive":"true"` que é usado para parâmetros que conteriam informações confidenciais, como uma senha. Quando esse atributo é definido, a entrada fornecida é obscurecida. Observe que você não pode definir esse atributo de parâmetro; no entanto, se estiver trabalhando com o AMS para criar um tipo de alteração e tiver um parâmetro que gostaria de ocultar na entrada, você pode solicitar isso.

Encontrando um tipo de alteração, usando a opção de consulta

Este exemplo demonstra como usar o console AMS para encontrar o tipo de alteração apropriado para o RFC que você deseja enviar.

Você pode usar o console ou o API/CLI para encontrar uma ID de tipo de alteração (CT) ou versão. Existem dois métodos: pesquisar ou escolher a classificação. Para ambos os tipos de seleção, você pode classificar a pesquisa escolhendo Usado com mais frequência, Usado mais recentemente ou Alfabético.

YouTube Vídeo: Como faço para criar uma RFC usando a CLI do AWS Managed Services e onde posso encontrar o esquema de CT?

No console do AMS, na página RFCs-> Criar RFC:

- Com a opção Procurar por tipo de alteração selecionada (o padrão), você pode:
  - Use a área de criação rápida para selecionar entre as mais populares do AMS CTs. Clique em um rótulo e a página Executar RFC será aberta com a opção Assunto preenchida automaticamente para você. Preencha as opções restantes conforme necessário e clique em Executar para enviar a RFC.
  - Ou desça até a área Todos os tipos de alteração e comece a digitar um nome de CT na caixa de opções, você não precisa ter o nome exato ou completo do tipo de alteração. Você também pode pesquisar uma tomografia computadorizada por ID do tipo de alteração, classificação ou modo de execução (automático ou manual) inserindo as palavras relevantes.

    Com a visualização padrão dos cartões selecionada, os cartões CT correspondentes aparecem conforme você digita, seleciona um cartão e clica em Criar RFC. Com a exibição de tabela selecionada, escolha o CT relevante e clique em Criar RFC. Ambos os métodos abrem a página Executar RFC.
- Como alternativa, e para explorar as opções de tipo de alteração, clique em Escolher por categoria na parte superior da página para abrir uma série de caixas de opções suspensas.
- Escolha uma categoria, uma subcategoria, um item e uma operação. A caixa de informações desse tipo de alteração aparece e um painel aparece na parte inferior da página.
- Quando estiver pronto, pressione Enter e uma lista dos tipos de alteração correspondentes será exibida.
- Escolha um tipo de alteração na lista. A caixa de informações desse tipo de alteração aparece na parte inferior da página.
- Depois de ter o tipo de alteração correto, escolha Criar RFC.

> **Note**
>
> A CLI do AMS deve estar instalada para que esses comandos funcionem. Para instalar a API ou a CLI do AMS, acesse a página Recursos para desenvolvedores do console AMS. Para obter material de referência sobre a API AMS CM ou a API AMS SKMS, consulte a seção Recursos de informação do AMS no Guia do usuário. Talvez seja necessário adicionar uma `--profile` opção para autenticação; por exemplo,`aws amsskms` *`ams-cli-command`* `--profile SAML`. Talvez você também precise adicionar a `--region` opção, pois todos os comandos do AMS saem de us-east-1; por exemplo. `aws amscm` *`ams-cli-command`* `--region=us-east-1`

> **Note**
>
> Os endpoints AMS API/CLI (amscm e amsskms) estão na região da AWS Norte da Virgínia,. `us-east-1` Dependendo de como sua autenticação está configurada e em qual região da AWS sua conta e seus recursos estão, talvez seja necessário adicioná-la `--region us-east-1` ao emitir comandos. Talvez você também precise adicionar`--profile saml`, se esse for o seu método de autenticação.

Para pesquisar um tipo de alteração usando a API AMS CM (consulte ListChangeTypeClassificationSummaries) ou a CLI:

Você pode usar um filtro ou uma consulta para pesquisar. A ListChangeTypeClassificationSummaries operação tem opções de filtros para `CategorySubcategory`,`Item`, `e0peration`, mas os valores devem corresponder exatamente aos valores existentes. Para obter resultados mais flexíveis ao usar a CLI, você pode usar a `--query` opção.

Altere a filtragem de tipo com a API/CLI do AMS CM

Atributo	Valores válidos	Condição válida/padrão	Observações
ChangeTypeId	Qualquer string representando um ChangeTypeId (por exemplo: ct-abc123 xyz7890)	Igual	Para o tipo de alteração IDs, consulte a Referência do tipo de alteração. Para o tipo de alteração IDs, consulte Encontrando um tipo de alteração ou CSIO.
Categoria	Qualquer texto de formato livre	Contém	Expressões regulares em cada campo individual não são suportadas. Pesquisa
Subcategory			
Item			

Atributo	Valores válidos	Condição válida/padrão	Observações
Operação			sem distinção entre maiúsculas e min

1. Aqui estão alguns exemplos de classificações de tipo de alteração de listagem:

   O comando a seguir lista todas as categorias de tipo de alteração.

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

   O comando a seguir lista as subcategorias pertencentes a uma categoria especificada.

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

   O comando a seguir lista os itens pertencentes a uma categoria e subcategoria especificadas.

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

2. Aqui estão alguns exemplos de pesquisa de tipos de alteração com consultas CLI:

   O comando a seguir pesquisa resumos de classificação de CT para aqueles que contêm “S3" no nome do item e cria a saída da categoria, subcategoria, item, operação e ID do tipo de alteração em forma de tabela.

   ```
   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. Em seguida, você pode usar o ID do tipo de alteração para obter o esquema de CT e examinar os parâmetros. O comando a seguir gera o esquema em um arquivo JSON chamado Creates3Params.schema.json.

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

   Para obter informações sobre o uso de consultas CLI, consulte Como filtrar a saída com a opção --query e a referência da linguagem de consulta, Especificação. JMESPath

4. Depois de ter o ID do tipo de alteração, recomendamos verificar a versão do tipo de alteração para garantir que seja a versão mais recente. Use esse comando para encontrar a versão de um tipo de alteração especificado:

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

   Para encontrar o `AutomationStatus` para um tipo de alteração específico, execute este comando:

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

   Para encontrar o `ExpectedExecutionDurationInMinutes` para um tipo de alteração específico, execute este comando:

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

Solução de problemas de erros de RFC no AMS

Muitas falhas de RFC de provisionamento do AMS podem ser investigadas por meio da documentação. CloudFormation Consulte Solução de problemas da AWS CloudFormation: Solução de problemas de erros

Sugestões adicionais de solução de problemas são fornecidas nas seções a seguir.

Erros de RFC de “gerenciamento” no AMS

Os tipos de alteração de categoria (CTs) de “Gerenciamento” do AMS permitem que você solicite acesso aos recursos, bem como gerencie os recursos existentes. Esta seção descreve alguns problemas comuns.

Erros de acesso ao RFC

- Verifique se o nome de usuário e o FQDN especificados na RFC estão corretos e existem no domínio. Para obter ajuda para encontrar seu FQDN, consulte Encontrando seu FQDN.
- Certifique-se de que a ID da pilha que você especificou para acesso seja uma pilha EC2 relacionada. Pilhas como ELB e Amazon Simple Storage Service (S3) não são candidatas ao acesso. Em vez disso, use sua função de RFCs acesso somente de leitura para acessar esses recursos de pilhas. Para obter ajuda para encontrar uma ID de pilha, consulte Como encontrar uma pilha IDs
- Verifique se o ID da pilha que você forneceu está correto e pertence à conta relevante.

Para obter ajuda com outras falhas de RFC de acesso, consulte Gerenciamento de acesso.

YouTube Vídeo: Como faço para gerar uma Solicitação de Mudança (RFC) adequadamente para evitar rejeições e falhas?

Erros de agendamento de RFC (manual) CT

A maioria dos tipos de alteração são ExecutionMode =Automatizados, mas alguns são ExecutionMode =Manual e isso afeta como você deve programá-los para evitar falhas no RFC.

Programado RFCs com ExecutionMode =Manual, deve ser configurado para ser executado pelo menos 24 horas no futuro se você estiver usando o console AMS para criar o RFC. Essa ressalva não se aplica à API/CLI do AMS, mas ainda é importante agendar o Manual com RFCs pelo menos 8 horas de antecedência.

O AMS visa responder a uma tomografia computadorizada manual em quatro horas e corresponderá o mais rápido possível, mas pode levar muito mais tempo para que a RFC seja realmente executada.

Usando RFCs com atualização manual CTs

Gerenciamento de rejeição de operações do AMS | Outros | Outros RFCs para atualizações em pilhas, quando há um tipo de alteração de atualização para o tipo de pilha que você deseja atualizar.

Erros de exclusão de pilha de RFC

Falhas de exclusão de pilha por RFC: se você usar o Gerenciamento | Pilhas padrão | Pilha | Excluir CT, verá os eventos detalhados no CloudFormation console da pilha com o nome da pilha AMS. Você pode identificar sua pilha comparando-a com o nome que ela tem no console do AMS. O CloudFormation console fornece mais detalhes sobre as causas da falha.

Antes de excluir uma pilha, você deve considerar como a pilha foi criada. Se você criou a pilha usando um AMS CT e não adicionou nem editou os recursos da pilha, pode esperar excluí-la sem problemas. No entanto, é uma boa ideia remover todos os recursos adicionados manualmente de uma pilha antes de enviar uma RFC de exclusão de pilha contra ela. Por exemplo, se você criar uma pilha usando a pilha completa CT (HA Two Tier), ela incluirá um grupo de segurança -. SG1 Se você então usar o AMS para criar outro grupo de segurança - SG2 e referenciar o novo SG2 no grupo SG1 criado como parte da pilha completa e, em seguida, usar a pilha de exclusão CT para excluir a pilha, ele não SG1 será excluído, pois é referenciado por. SG2

Important

A exclusão de pilhas pode ter consequências indesejadas e imprevistas. O AMS prefere *não* excluir pilhas ou recursos em nome dos clientes por esse motivo. Observe que o AMS excluirá somente recursos em seu nome (por meio de um tipo de alteração enviado em Gerenciamento | Outro | Outro | Atualizar) que não possam ser excluídos usando o tipo de alteração apropriado e automatizado para excluir. Considerações adicionais:

- Se os recursos estiverem habilitados para “proteção contra exclusão”, o AMS poderá ajudar a desbloqueá-los se você enviar um tipo de alteração Gerenciamento | Outros | Outros | Atualizar e, depois que a proteção contra exclusão for removida, você poderá usar a CT automatizada para excluir esse recurso.
- Se houver vários recursos em uma pilha e você quiser excluir somente um subconjunto dos recursos da pilha, use o tipo de alteração CloudFormation Atualizar (consulte Pilha de CloudFormation ingestão: atualização). Você também pode enviar um tipo de alteração de Gerenciamento | Outros | Outros | Atualizar e os engenheiros da AMS podem ajudá-lo a criar o conjunto de alterações, se necessário.
- Se houver problemas ao usar o CloudFormation Update CT devido a desvios, o AMS pode ajudar se você enviar uma atualização de Gerenciamento | Outro | Outro | Outro | para resolver o desvio (desde que suportado pelo CloudFormation Serviço da AWS) e forneça uma ChangeSet que você possa validar e executar usando a CT, o Management/

Custom Stack/Stack From CloudFormation Template/Approve Changeset e o Update automatizados.

O AMS mantém as restrições acima para ajudar a garantir que não haja exclusões inesperadas ou imprevistas de recursos.

Para obter mais informações, consulte Solução de problemas da AWS CloudFormation: falhas na exclusão da pilha.

Erros de DNS de atualização de RFC

Várias atualizações RFCs de uma zona hospedada por DNS podem falhar, algumas sem motivo. Criar várias RFCs ao mesmo tempo para atualizar as zonas hospedadas do DNS (privadas ou públicas) pode fazer RFCs com que algumas falhem porque estão tentando atualizar a mesma pilha ao mesmo tempo. O gerenciamento de alterações do AMS rejeita ou falha os RFCs que não conseguem atualizar uma pilha porque a pilha já está sendo atualizada por outro RFC. O AMS recomenda que você crie uma RFC por vez e espere que a RFC seja bem-sucedida antes de criar uma nova para a mesma pilha.

Erros de entidades do RFC IAM

O AMS provisiona várias funções e perfis padrão do IAM em contas do AMS, projetados para atender às suas necessidades. No entanto, talvez seja necessário solicitar recursos adicionais do IAM ocasionalmente.

O processo de envio da RFCs solicitação de recursos personalizados do IAM segue o fluxo de trabalho padrão do manual RFCs, mas o processo de aprovação também inclui uma análise de segurança para garantir que os controles de segurança apropriados estejam em vigor. Portanto, o processo normalmente leva mais tempo do que outros manuais RFCs. Para reduzir o tempo de ciclo deles RFCs, siga as diretrizes a seguir.

Para obter informações sobre o que queremos dizer com uma revisão do IAM e como ela se relaciona com nossos padrões técnicos e processo de aceitação de riscos, consulteEntenda as análises de segurança da RFC.

Solicitações comuns de recursos do IAM:

- Se você estiver solicitando uma política referente a um grande aplicativo compatível com a nuvem, como CloudEndure, consulte a CloudEndure política IAM pré-aprovada pelo

AMS: Descompacte o arquivo de exemplo do WIGs Cloud Endure Landing Zone e abra o `customer_cloud_endure_policy.json`

> **Note**
>
> Se você quiser uma política mais permissiva, discuta suas necessidades com você CloudArchitect/CSDM e obtenha, se necessário, uma revisão e aprovação de segurança do AMS antes de enviar uma RFC implementando a política.

- Se você quiser modificar um recurso implantado pelo AMS em sua conta por padrão, recomendamos que você solicite uma cópia modificada desse recurso em vez de alterações na existente.
- Se você estiver solicitando permissões para um usuário humano (em vez de anexar as permissões ao usuário), anexe as permissões a uma função e, em seguida, conceda ao usuário permissão para assumir essa função. Para obter detalhes sobre como fazer isso, consulte Acesso temporário ao console AMS Advanced.
- Se você precisar de permissões excepcionais para uma migração temporária ou fluxo de trabalho, forneça uma data de término para essas permissões em sua solicitação.
- Se você já discutiu o assunto de sua solicitação com sua equipe de segurança, forneça evidências de sua aprovação ao CSDM com o máximo de detalhes possível.

Se o AMS rejeitar uma RFC do IAM, fornecemos um motivo claro para a rejeição. Por exemplo, podemos rejeitar uma solicitação de criação de política do IAM e explicar o que a política é inadequada. Nesse caso, você pode fazer as alterações identificadas e reenviar a solicitação. Se for necessária mais clareza sobre o status de uma solicitação, envie uma solicitação de serviço ou entre em contato com seu CSDM.

A lista a seguir descreve os riscos típicos que o AMS tenta mitigar ao analisarmos seu IAM RFCs. Se sua RFC do IAM tiver algum desses riscos, isso poderá resultar na rejeição da RFC. Nos casos em que você precisa de uma exceção, o AMS solicita a aprovação da sua equipe de segurança. Para buscar essa exceção, coordene com seu CSDM.

> **Note**
>
> O AMS pode, por qualquer motivo, recusar qualquer alteração nos recursos do IAM dentro de uma conta. Em caso de dúvidas sobre qualquer rejeição de RFC, entre em contato com

a AMS Operations por meio de uma solicitação de serviço ou entre em contato com seu CSDM.

- Escalonamento de privilégios, como permissões que permitem que você modifique suas próprias permissões ou modifique as permissões de outros recursos dentro da conta. Exemplos:
  - O uso de `iam:PassRole` com outro papel mais privilegiado.
  - Permissão para políticas do attach/detach IAM de uma função ou usuário.
  - A modificação das políticas do IAM na conta.
  - A capacidade de fazer chamadas de API no contexto da infraestrutura de gerenciamento.
- Permissões para modificar recursos ou aplicativos necessários para fornecer serviços de AMS a você. Exemplos:
  - Modificação da infraestrutura do AMS, como bastiões, host de gerenciamento ou infraestrutura EPS.
  - Exclusão do gerenciamento de registros, funções ou fluxos de log do AWS Lambda.
  - A exclusão ou modificação do aplicativo de CloudTrail monitoramento padrão.
  - A modificação do Active Directory (AD) dos Serviços de Diretório.
  - Alarmes de desativação CloudWatch (CW).
  - A modificação dos princípios, políticas e namespaces implantados na conta como parte da landing zone.
- Implantação de infraestrutura fora das melhores práticas, como permissões que permitem a criação de infraestrutura em um estado que coloca em risco a segurança das informações. Exemplos:
  - A criação de buckets S3 públicos ou não criptografados ou o compartilhamento público de volumes do EBS.
  - O provisionamento de endereços IP públicos.
  - A modificação dos grupos de segurança para permitir amplo acesso.
- Permissões excessivamente amplas capazes de causar impacto nos aplicativos, como permissões que podem resultar em perda de dados, perda de integridade, configuração inadequada ou interrupções no serviço de sua infraestrutura e dos aplicativos dentro da conta. Exemplos:
  - Desabilitar ou redirecionar o tráfego de rede por meio APIs de like ou. `ModifyNetworkInterfaceAttribute` `UpdateRouteTable`

  - A desativação da infraestrutura gerenciada por meio da separação de volumes dos hosts gerenciados.
- Permissões para serviços que não fazem parte da descrição do serviço do AMS e não são suportadas pelo AMS.

  Os serviços não listados na descrição do serviço AMS não podem ser usados nas contas do AMS. Para solicitar suporte para um recurso ou serviço, entre em contato com seu CSDM.
- Permissões que não atendem à meta declarada, pois são muito generosas ou muito conservadoras ou são aplicadas aos recursos errados. Exemplos:
  - Uma solicitação de `s3:PutObject` permissões para um bucket do S3 que tem criptografia KMS obrigatória, sem `KMS:Encrypt` permissões para a chave relevante.
  - Permissões que dizem respeito a recursos que não existem na conta.
  - IAM RFCs em que a descrição da RFC parece não corresponder à solicitação.

Erros de RFC de “implantação”

Os tipos de alteração de categoria “Implantação” do AMS (CTs) permitem que você solicite que vários recursos suportados pelo AMS sejam adicionados à sua conta.

A maioria dos AMS CTs que criam um recurso é baseada em CloudFormation modelos. Como cliente, você tem acesso somente de leitura a todos os serviços da AWS CloudFormation, inclusive, você pode identificar rapidamente a CloudFormation pilha que representa sua pilha com base na descrição da pilha usando o console. CloudFormation A pilha com falha provavelmente estará em um estado de DELETE_COMPLETE. Depois de identificar a CloudFormation pilha, os eventos mostrarão o recurso específico que falhou na criação e por quê.

Usando a CloudFormation documentação para solucionar problemas

A maioria dos aprovisionamentos do AMS RFCs usa um CloudFormation modelo e essa documentação pode ser útil para solucionar problemas. Veja a documentação desse CloudFormation modelo:

- Falha na criação do balanceador de carga do aplicativo: AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer)
- Criar grupo de Auto Scaling: AWS::AutoScaling::AutoScalingGroup (Grupo de Auto Scaling)
- Crie o cache do memcached: AWS::ElastiCache::CacheCluster (cluster de cache)
- Criar cache Redis: AWS::ElastiCache::CacheCluster (cluster de cache)

- Criar zona hospedada de DNS (usada com Criar DNS privado/público): AWS::Route53::HostedZone (zona hospedada R53)
- Criar conjunto de registros DNS (usado com Criar DNS privado/público): AWS::Route53::RecordSet (conjuntos de registros de recursos)
- Crie uma EC2 pilha: AWS::EC2::Instance (Elastic Compute Cloud)
- Crie o Elastic File System (EFS): AWS::EFS::FileSystem (Elastic File System)
- Crie um balanceador de carga: AWS::ElasticLoadBalancing::LoadBalancer (Elastic Load Balancer)
- Criar banco de dados RDS: AWS::RDS::DBInstance (banco de dados relacional)
- Crie o Amazon S3: AWS::S3::Bucket (Serviço de armazenamento simples)
- Criar fila: AWS::SQS::Queue (Serviço de fila simples)

RFC criando erros AMIs

Uma imagem de máquina da Amazon (AMI) é um modelo que contém uma configuração de software (por exemplo, sistema operacional, servidor de aplicação e aplicações). Em uma AMI, você executa uma instância, que é uma cópia da AMI em execução como um servidor virtual na nuvem. AMIs são muito úteis e necessários para criar EC2 instâncias ou grupos de Auto Scaling; no entanto, você deve observar alguns requisitos:

- A instância que você especifica `Ec2InstanceId` deve estar em um estado interrompido para que a RFC seja bem-sucedida. Não use instâncias do grupo Auto Scaling (ASG) para esse parâmetro porque o ASG encerrará uma instância parada.
- Para criar uma Amazon Machine Image (AMI) do AMS, você deve começar com uma instância do AMS. Antes de usar a instância para criar a AMI, você deve prepará-la garantindo que ela seja interrompida e separada de seu domínio. Para obter detalhes, consulte Criar uma imagem de máquina padrão da Amazon usando o Sysprep
- O nome que você especificar para a nova AMI deve ser exclusivo na conta ou o RFC falhará. Como fazer isso está descrito em AMI | Create e, para obter mais detalhes, consulte AWS AMI Design.

> **Note**
>
> Para obter informações adicionais sobre como se preparar para a criação de AMI, consulte AMI | Create.

RFCs criação EC2s ou ASGs erros

Para EC2 falhas do ASG com tempos limite, o AMS recomenda que você confirme se a AMI usada é personalizada. Se estiver, consulte as etapas de criação da AMI incluídas neste guia (consulte AMI | Criar) para garantir que a AMI tenha sido criada corretamente. Um erro comum ao criar uma AMI personalizada é não seguir as etapas do guia para renomear ou invocar o Sysprep.

RFCs criando erros de RDS

As falhas do Amazon Relational Database Service (RDS) podem ocorrer por vários motivos diferentes, pois você pode usar vários mecanismos diferentes ao criar o RDS, e cada mecanismo tem seus próprios requisitos e limitações. Antes de tentar criar uma pilha do AMS RDS, analise cuidadosamente os valores dos parâmetros do AWS RDS, consulte Criar. DBInstance

Para saber mais sobre o Amazon RDS em geral, incluindo recomendações de tamanho, consulte a documentação do Amazon Relational Database Service.

RFCs criando erros do Amazon S3s

Um erro comum ao criar um bucket de armazenamento S3 é não usar um nome exclusivo para o bucket. Se você enviasse um bucket do S3 Create CT com o mesmo nome de outro enviado anteriormente, ele falharia porque já existiria um bucket do S3 com ele. BucketName Isso seria detalhado no CloudFormation console, onde você verá que o evento stack mostra que o nome do bucket já está em uso.

Validação de RFC versus erros de execução

As falhas de RFC e as mensagens relacionadas diferem nas mensagens de saída na página de detalhes da RFC do console AMS para uma RFC selecionada:

- Os motivos das falhas de validação estão disponíveis somente no campo Status
- Os motivos das falhas de execução estão disponíveis nos campos Saída de execução e Status.

Mensagens de erro de RFC

Ao se deparar com o seguinte erro para os tipos de alteração listados (CTs), você pode usar essas soluções para ajudá-lo a encontrar a origem dos problemas e corrigi-los.

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

Se você precisar de mais assistência após consultar as seguintes opções de solução de problemas, entre em contato com o AMS por meio de correspondência RFC ou crie uma solicitação de serviço. Consulte Correspondência e anexo RFC (console) e Criação de uma solicitação de serviço no AMS para obter mais detalhes.

Erros de ingestão de carga de trabalho (WIGS)

> **Note**
>
> As ferramentas de validação para Windows e Linux podem ser baixadas e executadas diretamente em seus servidores locais, bem como em EC2 instâncias na AWS. Eles podem ser encontrados no Guia do Desenvolvedor de Aplicativos Avançados do AMS Migração de cargas de trabalho: Validação de pré-ingestão do Linux e Migração de cargas de trabalho: validação de pré-ingestão do Windows.

- Verifique se a EC2 instância existe na conta AMS de destino. Por exemplo, se você compartilhou sua AMI de uma conta que não é da AMS com uma conta do AMS, precisará criar uma EC2 instância na sua conta do AMS com a AMI compartilhada antes de enviar uma RFC de ingestão de carga de trabalho.
- Verifique se os grupos de segurança vinculados à instância têm tráfego de saída permitido. O agente SSM precisa ser capaz de se conectar ao seu endpoint público.
- Verifique se a instância tem as permissões corretas para se conectar ao agente SSM. Essas permissões vêm com `ocustomer-mc-ec2-instance-profile`, você pode verificar isso no EC2 console:

EC2 erros de parada de pilha de instâncias

- Verifique se a instância já está em um estado interrompido ou encerrado.
- Se a EC2 instância estiver on-line e você ver o `InternalError` erro, envie uma solicitação de serviço para que o AMS investigue.
- Observe que você não pode usar o tipo de alteração Management | Advanced stack components | EC2 instance stack | Stop ct-3mvvt2zkyveqj para interromper uma instância de grupo do Auto

Scaling (ASG). Se você precisar interromper uma instância do ASG, envie uma solicitação de serviço.

EC2 erros de criação da pilha de instâncias

A `InternalError` mensagem é de CloudFormation; um motivo do status CREATION_FAILED. Você pode encontrar detalhes sobre a falha da pilha nos eventos da CloudWatch pilha seguindo estas etapas:

- No console de gerenciamento da AWS, você pode ver uma lista de eventos da pilha enquanto sua pilha está sendo criada, atualizada ou excluída. Nessa lista, encontre o evento de falha e, em seguida, visualize o motivo do status desse evento.

  O motivo do status pode conter uma mensagem de erro da AWS CloudFormation ou de um serviço específico que pode ajudar você a entender o problema.
- Para obter mais informações sobre a visualização de eventos da pilha, consulte Visualização de dados e recursos do AWS CloudFormation Stack no AWS Management Console.

EC2 erros de restauração do volume da instância

O AMS cria um RFC interno para solução de problemas quando a restauração do volume da EC2 instância falha. Isso é feito porque a restauração do volume da EC2 instância é uma parte importante da recuperação de desastres (DR) e o AMS cria automaticamente essa RFC interna de solução de problemas para você.

Quando a RFC de solução de problemas interna é criada, um banner é exibido fornecendo links para a RFC. Essa RFC interna de solução de problemas fornece mais visibilidade das falhas de RFC e, em vez de enviar uma nova tentativa que RFCs leva aos mesmos erros ou fazer com que você entre em contato manualmente com o AMS em caso de falha, você pode acompanhar suas alterações e saber que a falha está sendo corrigida pelo AMS. Isso também reduz a métrica time-to-recovery (TTR) de sua alteração, pois os operadores do AMS trabalham proativamente na falha de RFC em vez de aguardar sua solicitação.

Como obter ajuda com um RFC

Você pode entrar em contato com a AMS para identificar a causa raiz de sua falha. O horário comercial do AMS é 24 horas por dia, 7 dias por semana, 365 dias por ano.

O AMS oferece vários meios para você pedir ajuda ou fazer solicitações de serviço.

- Para solicitar informações ou conselhos, acessar um serviço de TI gerenciado pelo AMS ou solicitar um serviço adicional do AMS, use o console do AMS e envie uma solicitação de serviço. Para obter detalhes, consulte Criação de uma solicitação de serviço. Para obter informações gerais sobre solicitações de serviço do AMS, consulte Gerenciamento de solicitações de serviço.
- Para relatar um problema de desempenho do serviço da AWS ou do AMS que afeta seu ambiente gerenciado, use o console do AMS e envie um relatório de incidentes. Para obter detalhes, consulte Relatar um incidente. Para obter informações gerais sobre o gerenciamento de incidentes do AMS, consulte Resposta a incidentes.
- Para perguntas específicas sobre como você ou seus recursos ou aplicativos estão trabalhando com o AMS, ou para escalar um incidente, envie um e-mail para um ou mais dos seguintes:
  1. Primeiro, se você não estiver satisfeito com a solicitação de serviço ou com a resposta do relatório de incidentes, envie um e-mail para seu CSDM: ams-csdm@amazon.com
  2. Em seguida, se o escalonamento for necessário, você pode enviar um e-mail para o gerente de operações do AMS (mas seu CSDM provavelmente fará isso): ams-opsmanager@amazon.com
  3. Uma escalada adicional seria para o diretor da AMS: ams-director@amazon.com
  4. Finalmente, você sempre pode entrar em contato com o vice-presidente do AMS: ams-vp@amazon.com

Modo de mudança direta no AMS

Tópicos

- Introdução ao modo Direct Change
- Segurança e conformidade
- Gerenciamento de alterações no modo Direct Change
- Criação de pilhas usando o modo Direct Change
- Casos de uso do Modo de Mudança Direta

O modo Direct Change (DCM) do AWS Managed Services (AMS) amplia o gerenciamento de alterações do AMS Advanced ao fornecer AWS acesso nativo às contas AMS Advanced Plus e Premium para provisionar e atualizar AWS recursos. Com o DCM, você tem a opção de usar a AWS API nativa (console ou CLI/SDK) ou solicitações de mudança do AMS Advanced Change (RFCs) e, em ambos os casos, os recursos e as alterações neles são totalmente suportados pelo AMS, incluindo monitoramento, patch, backup e gerenciamento de respostas a incidentes. Os recursos

provisionados por meio do DCM são registrados no sistema de gerenciamento de conhecimento do serviço AMS (SKMS), associados ao domínio gerenciado do Active Directory pelo AMS (quando aplicável) e executam agentes de gerenciamento do AMS. Use as ferramentas existentes (por exemplo CloudFormation, AWS SDK e CDK) para desenvolver e implantar pilhas gerenciadas pelo AMS. CloudFormation

> **Note**
>
> O modo Direct Change não remove o gerenciamento de alterações do AMS RFCs. Você tem acesso total ao AMS RFCs com o DCM.

Assista ao vídeo de Akash para saber mais (6:30)

Introdução ao modo Direct Change

Comece verificando os pré-requisitos e, em seguida, enviando uma solicitação de alteração (RFC) em sua conta qualificada do AMS Advanced.

1. Confirme se a conta que você deseja usar com o DCM atende aos requisitos:
   - A conta é AMS Advanced Plus ou Premium.
   - A conta não tem o Service Catalog ativado. Atualmente, não oferecemos suporte à integração de contas no DCM e no Service Catalog ao mesmo tempo. Se você já está integrado ao Service Catalog, mas está interessado no DCM, discuta suas necessidades com seu gerente de prestação de serviços em nuvem (CSDM). Se você decidir mudar do Service Catalog para o DCM, fora do Service Catalog, para fazer isso, inclua a solicitação na solicitação de alteração abaixo. Para obter detalhes sobre o Service Catalog no AMS, consulte AMS e Service Catalog.
2. Envie uma solicitação de alteração (RFC) usando o Gerenciamento | Conta gerenciada | Modo de alteração direta | Ativar tipo de alteração (ct-3rd4781c2nnhp). Para ver um exemplo de apresentação, consulte Modo de mudança direta | Ativar.

   Depois que a CT é processada, o IAM predefinido funciona `AWSManagedServicesCloudFormationAdminRole` e `AWSManagedServicesUpdateRole` é provisionado na conta especificada.
3. Atribua a função apropriada aos usuários que precisam de acesso ao DCM usando seu processo interno de federação.

> **Note**
>
> Você pode especificar qualquer número de SAMLIdentity provedores, AWS serviços e entidades do IAM (funções, usuários etc.) para assumir as funções. Você deve fornecer pelo menos um:`SAMLIdentityProviderARNs`,`IAMEntityARNs`, ou`AWSServicePrincipals`. Para obter mais informações, consulte o departamento de IAM da sua empresa ou o arquiteto de nuvem (CA) do AMS.

Funções e políticas do IAM do modo Direct Change

Quando o modo Direct Change é ativado em uma conta, essas novas entidades do IAM são implantadas:

`AWSManagedServicesCloudFormationAdminRole`: essa função concede acesso ao CloudFormation console, cria e atualiza CloudFormation pilhas, visualiza relatórios de deriva e cria e executa. CloudFormation ChangeSets O acesso a essa função é gerenciado por meio do seu provedor de SAML.

As políticas gerenciadas que são implantadas e anexadas à função `AWSManagedServicesCloudFormationAdminRole` são:

- Conta do aplicativo AMS Advanced multi-account landing zone (MALZ)
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
    - Essa política representa as permissões concedidas a`AWSManagedServicesCloudFormationAdminRole`. Você e seus parceiros usam essa política para conceder acesso a uma função existente na conta e permitir que essa função lance e atualize CloudFormation pilhas na conta. Isso pode exigir atualizações adicionais da política de controle de serviço (SCP) do AMS para permitir que outras entidades do IAM iniciem CloudFormation pilhas.
- Conta AMS Advanced single-account landing zone (SALZ)
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
  - cdk-legacy-mode-s3 acessos [política em linha]
  - AWS ReadOnlyAccess política

`AWSManagedServicesUpdateRole`: essa função concede acesso restrito ao AWS serviço APIs downstream. A função é implantada com políticas gerenciadas que fornecem operações de API mutantes e não mutantes, mas, em geral, restringe as operações mutantes (comoCreate/Delete/PUT) em relação a determinados serviços, como IAM, KMS, GuardDuty VPC, recursos e configuração de infraestrutura do AMS e assim por diante. O acesso a essa função é gerenciado por meio do seu provedor de SAML.

As políticas gerenciadas que são implantadas e anexadas à função `AWSManagedServicesUpdateRole` são:

- Conta de aplicativo AMS Advanced com várias contas landing zone
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyPolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2E RDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolítica
- Conta de landing zone de conta única AMS Advanced
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2E RDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolítica 1
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolítica 2

Além disso, a `AWSManagedServicesUpdateRole` função de política gerenciada também tem a política AWS `ViewOnlyAccess` gerenciada anexada a ela.

Segurança e conformidade

Segurança e conformidade são uma responsabilidade compartilhada entre a AMS Advanced e você, como nosso cliente. O modo AMS Advanced Direct Change não altera essa responsabilidade compartilhada.

Segurança no modo Direct Change

O AMS Advanced oferece valor adicional com uma landing zone prescritiva, um sistema de gerenciamento de mudanças e gerenciamento de acesso. Ao usar o modo Direct Change, esse modelo de responsabilidade não muda. No entanto, você deve estar ciente dos riscos adicionais.

A função “Atualização” do Modo de Alteração Direta (consulteFunções e políticas do IAM do modo Direct Change) fornece permissões elevadas, permitindo que a entidade com acesso a ela faça alterações nos recursos de infraestrutura dos serviços suportados pela AMS em sua conta. Com permissões elevadas, existem riscos variados, dependendo do recurso, do serviço e das ações, especialmente em situações em que uma alteração incorreta é feita devido a supervisão, erro ou falta de adesão ao processo interno e à estrutura de controle.

De acordo com os Padrões Técnicos da AMS, os seguintes riscos foram identificados e as recomendações são feitas da seguinte forma. Informações detalhadas sobre as Normas Técnicas da AMS estão disponíveis em AWS Artifact. Para acessar AWS Artifact, entre em contato com seu CSDM para obter instruções ou acesse Introdução ao. AWS Artifact

AMS-STD-001: Marcação

Padrões	Isso quebra?	Riscos	Recomendações
Todos os recursos de propriedade da AMS devem ter o seguinte par de valores-chave Todas as tags de propriedade da AMS, exceto as listadas acima, devem ter prefixos como `AMS*` ou `MC*` no caso. upper/lower/mix	Sim. Interrupções para CloudFormationCloudTrail,, EFS OpenSearch, CloudWatch Logs, SQS, SSM, API de marcação, pois esses serviços não oferecem suporte à `aws:TagsKey` condição de restringir a marcação no namespace AMS. O padrão fornecido na tabela AMS-	A marcação incorreta dos recursos do AMS pode afetar adversamente as operações de emissão de relatórios, alertas e correções de seus recursos, no lado do AMS.	O acesso deve ser restrito para fazer qualquer alteração nos requisitos de marcação padrão do AMS para qualquer pessoa que não seja as equipes do AMS.

Padrões	Isso quebra?	Riscos	Recomendações
	STD-003, a seguir, afirma que você pode alterar o ambiente AppId AppName, mas não os recursos de propriedade da AMS. Não é possível por meio de permissões do IAM.		
Qualquer tag nas pilhas de propriedade da AMS não deve ser excluída com base em suas solicitações de alteração.	Sim. CloudFormation não suporta a `aws:TagsKey` condição de restringir tags para o namespace AMS.		
Você não tem permissão para usar a convenção de nomenclatura de tags do AMS em sua infraestrutura, conforme mencionado na tabela AMS-STD-002, a seguir.	Sim. Pausas para CloudFormation CloudTrail,, Amazon Elastic File System (EFS) OpenSearch, CloudWatch Logs, Amazon Simple Queue Service (SQS), Amazon EC2 Systems Manager (SSM), Tagging API; esses serviços não `aws:TagsKey` suportam a condição de restringir a marcação para o namespace AMS.		

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

Padrões	Isso quebra?	Riscos	Recomendações
4.7 Ações que ignoram o processo de gerenciamento de mudanças (RFC) não devem ser permitidas, como iniciar ou interromper uma instância, criar buckets do S3 ou instâncias do RDS e assim por diante. As contas do modo Desenvolvedor e os serviços do modo Self-Service Provisioned (SSPS) estão isentos, desde que as ações sejam executadas dentro dos limites da função atribuída.	Sim. O objetivo das ações de autoatendimento permite que você execute ações ignorando o sistema AMS RFC.	O modelo de acesso seguro é uma faceta técnica central do AMS e um usuário do IAM para console ou acesso programático contorna esse controle de acesso. O acesso dos usuários do IAM não é monitorado pelo gerenciamento de alterações do AMS. O acesso está CloudTrail somente logado.	O usuário do IAM deve ter um limite de tempo e receber permissões com base no privilégio mínimo e. need-to-know

AMS-STD-003: Segurança de rede

Padrões	Isso quebra?	Riscos	Recomendações
S2. O Elastic IP em EC2 instâncias deve ser usado somente com um acordo formal de aceitação de risco ou com um caso	Sim. As ações de autoatendimento permitem associar e desassociar endereços IP elásticos (EIP).	Adicionar um IP elástico a uma instância a expõe à Internet. Isso aumenta o risco de divulgação de informações	Bloqueie qualquer tráfego desnecessário para essa instância por meio de grupos de segurança e verifique se seus

Padrões	Isso quebra?	Riscos	Recomendações
de uso válido por equipes internas.		e atividades não autorizadas.	grupos de segurança estão conectados à instância para garantir que ela permita o tráfego somente quando necessário por motivos comerciais.
S14. O emparelhamento de VPC e as conexões de endpoint entre contas que pertencem ao mesmo cliente podem ser permitidos.	Sim. Não é possível por meio da política do IAM.	O tráfego que sai da sua conta do AMS não é monitorado depois de sair do limite da conta.	Recomendamos fazer peering somente com contas AMS que você possui. Se seu caso de uso exigir isso, use grupos de segurança e tabelas de rotas para limitar quais faixas de tráfego, recursos e tipos podem sair pela conexão relevante.
A base do AMS AMIs pode ser compartilhada entre contas gerenciadas e não gerenciadas pelo AMS, desde que possamos verificar se elas pertencem à mesma organização. AWS		AMIs podem conter dados confidenciais e podem ser expostos a contas indesejadas.	Compartilhe somente AMIs com a conta de propriedade da sua organização ou valide o caso de uso e as informações da conta antes de compartilhar fora da organização.

AMS-STD-007: Registro

Padrões	Isso quebra?	Riscos	Recomendações
19. Qualquer registro pode ser encaminhado de uma conta AMS para outra conta AMS do mesmo cliente.			
20. Qualquer registro pode ser encaminhado do AMS para uma conta que não seja do AMS somente se a conta não pertencer ao mesmo cliente do AMS (confirmando que eles estão na mesma AWS Organizations conta ou combinando o domínio do e-mail com o nome da empresa do cliente e a conta vinculada ao PAYER) usando ferramentas internas.	Sim. A possível insegurança dos registros do cliente, pois a verificação de que as contas dos clientes estão na mesma organização, não pode ser alcançada por meio da política do IAM.	Os registros podem conter dados confidenciais e podem ser expostos a contas indesejadas.	Compartilhe registros somente com contas gerenciadas pela sua AWS organização ou valide o caso de uso e as informações da conta antes de compartilhá-los fora da sua organização. Podemos verificar isso de várias maneiras, consulte seu gerente de prestação de serviços em nuvem (CSDM).

Trabalhe com sua equipe interna de autorização e autenticação para controlar adequadamente as permissões para as funções do modo Direct Change.

Conformidade no modo Direct Change

O modo Direct Change é compatível com cargas de trabalho de produção e não produtivas. É sua responsabilidade garantir a adesão a quaisquer padrões de conformidade (por exemplo, PHI, HIPAA, PCI) e garantir que o uso do modo Direct Change esteja em conformidade com suas estruturas e padrões de controle interno.

Gerenciamento de alterações no modo Direct Change

O gerenciamento de mudanças é o processo que o AMS Advanced usa para implementar solicitações de mudança. Uma solicitação de alteração (RFC) é uma solicitação criada por você ou pelo AMS Advanced por meio da interface do AMS Advanced para fazer uma alteração em seu ambiente gerenciado e inclui uma ID do tipo de alteração (CT) do AMS Advanced para uma operação específica. Para obter mais informações, consulte Gerenciamento de mudanças.

> **Note**
>
> O modo Direct Change não remove o gerenciamento de alterações do AMS RFCs, você ainda tem acesso total ao AMS RFCs com o DCM.

O modo AMS Direct Change (DCM) estende o gerenciamento avançado de alterações do AMS, fornecendo AWS acesso nativo às contas AMS Advanced Plus e Premium para provisionar e atualizar AWS recursos. Os usuários que receberam a permissão do modo Direct Change por meio das funções do IAM podem usar o acesso nativo à AWS API para provisionar e fazer alterações nos recursos em suas contas do AMS Advanced. Os usuários ainda podem usar o gerenciamento avançado de alterações do AMS RFCs usando as mesmas funções do IAM. Em ambos os casos, os recursos e as alterações neles são totalmente suportados pelo AMS, incluindo monitoramento, patches, backup e gerenciamento de respostas a incidentes. Os usuários que não têm a função apropriada nessas contas devem usar o processo RFC de gerenciamento de alterações avançado do AMS para fazer alterações.

Casos de uso do gerenciamento de mudanças

Por motivos de segurança, algumas alterações no AMS Advanced só podem ser feitas por meio do processo de solicitação de mudança (RFC) de gerenciamento de alterações. O `AWSManagedServicesCloudFormationAdminRole` é restrito às ações realizadas por meio do CloudFormation (CFN). Para saber mais sobre como criar pilhas por meio do DCM, consulte Criação de pilhas usando o modo Direct Change. O `AWSManagedServicesUpdateRole` é restrito para as seguintes ações.

Por exemplo, orientações para cada tipo de alteração, incluindo o tipo de alteração Gerenciamento | Conta gerenciada | Modo de alteração direta | Ativar (ct-3rd4781c2nnhp), consulte a seção “Informações adicionais” para o tipo de alteração relevante na seção Tipos de alteração de referência do tipo de alteração do AMS Advanced por classificação.

Serviço	Ação
AWS Key Management Service (AWS KMS)	Atualizar
AWS Certificate Manager	Criar
AWS Identity and Access Management (IAM)	Any
Site-to-Site VPN	Any
Agendador de recursos do AMS	
AWS Backup	Crie um plano de backup
Ingestão de carga de trabalho do AMS () WIGs	Any
Filtragem de saída AMS (gerenciada em Palo Alto)	
Alterações na conta AMS Advanced MALZ	
Amazon GuardDuty	
Acesso avançado ao AMS Stack	Any
Volume do Amazon Elastic Block Store (EBS)	Excluir
Criptografia padrão do Amazon Elastic Block Store (EBS)	Ativar criptografia padrão
Nuvem de computação elástica da Amazon (Amazon EC2)	Alterar nome do host
Imagens de máquina da Amazon (AMI)	Excluir, compartilhar
Grupo de EC2 segurança da Amazon	Any
SSPS avançado do AMS	
AWS Microsoft AD gerenciado	

Serviço	Ação
Modo de desenvolvedor avançado do AMS	
Amazon Simple Storage Service (Amazon S3)	Crie políticas de bucket do S3
AWS Systems Manager	Criar

Criação de pilhas usando o modo Direct Change

Há dois requisitos ao iniciar pilhas CloudFormation usando o`AWSManagedServicesCloudFormationAdminRole`, para que a pilha seja gerenciada pelo AMS:

- O modelo deve conter um`AmsStackTransform`.
- O nome da pilha deve começar com o prefixo `stack-` seguido por uma sequência alfanumérica de 17 caracteres.

> **Note**
>
> Para usar o com sucesso`AmsStackTransform`, você deve reconhecer que seu modelo de pilha contém a `CAPABILITY_AUTO_EXPAND` capacidade para que CloudFormation (CFN) crie ou atualize a pilha. Você faz isso passando o `CAPABILITY_AUTO_EXPAND` como parte de sua solicitação de criação da pilha. O CFN rejeita a solicitação se esse recurso não for reconhecido quando incluído no modelo. `AmsStackTransform` O console CFN garante que você transmita esse recurso se tiver a transformação em seu modelo, mas isso pode passar despercebido quando você estiver interagindo com o CFN por meio deles. APIs
> Você deve transmitir esse recurso sempre que usar as seguintes chamadas de API CFN:
>
> - CreateChangeSet
> - CreateStack
> - UpdateStack

Ao criar ou atualizar uma pilha com o DCM, as mesmas validações e aprimoramentos do CFN Ingest e do Stack Update CTs são realizados na pilha. Para obter mais informações, consulte

CloudFormation Diretrizes, melhores práticas e limitações de ingestão. A exceção é que os grupos de segurança padrão do AMS (SGs) não serão anexados a nenhuma EC2 instância autônoma ou EC2 instância em grupos de Auto Scaling (). ASGs Ao criar seu CloudFormation modelo, com EC2 instâncias autônomas ou ASGs, você pode anexar o padrão. SGs

> **Note**
>
> Agora, as funções do IAM podem ser criadas e gerenciadas com `AWSManagedServicesCloudFormationAdminRole` o.

O padrão do AMS SGs tem regras de entrada e saída que permitem que as instâncias sejam iniciadas com êxito e sejam acessadas posteriormente por meio de SSH ou RDP pelas operações do AMS e por você. Se você achar que os grupos de segurança padrão do AMS são muito permissivos, você pode criar seus próprios SGs com regras mais restritivas e anexá-los à sua instância, desde que isso ainda permita que você e as operações do AMS acessem a instância durante incidentes.

Os grupos de segurança padrão do AMS são os seguintes:

- SentinelDefaultSecurityGroupPrivateOnly: Pode ser acessado no modelo CFN por meio desse parâmetro SSM `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- SentinelDefaultSecurityGroupPrivateOnlyEgressAll: Pode ser acessado no modelo CFN por meio desse parâmetro SSM `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

Transformação AMS

Adicione uma `Transform` declaração ao seu CloudFormation modelo. Isso adiciona uma CloudFormation macro que valida e registra a pilha no AMS no momento da inicialização.

Exemplo de JSON

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

Exemplo de YAML

```
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

Adicione também a `Transform` instrução ao atualizar o modelo de uma pilha existente.

Exemplo de 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"}
      }
    }
  }
}
```

Exemplo de YAML

```
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
```

Nome da pilha

O nome da pilha deve começar com o prefixo `stack-` seguido por uma sequência alfanumérica de 17 caracteres. Isso é para manter a compatibilidade com outros sistemas AMS que operam na pilha IDs AMS.

Veja a seguir exemplos de maneiras de gerar uma pilha IDs compatível:

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]$_}) )
```

Casos de uso do Modo de Mudança Direta

A seguir estão os casos de uso do Modo de Alteração Direta:

Provisão e gerenciamento de recursos por meio de CloudFormation

- Integre CloudFormation ferramentas e processos existentes.

Gerenciamento contínuo de recursos e atualizações

- Pequenas mudanças atômicas com baixo risco.
- Alterações que, de outra forma, seriam executadas por meio de um RFC manual ou automatizado.
- Ferramentas que exigem acesso nativo à AWS API.
- A função DCM pode ser utilizada se você estiver no estágio de migração. As equipes de migração utilizam as permissões no DCM para criar ou modificar pilhas.
- As funções do DCM podem ser usadas no CI/CD pipeline para criar novas AMIs tarefas do Amazon ECS e assim por diante.

Modo AMS Advanced Developer

Tópicos

- Introdução ao modo AMS Advanced Developer
- Segurança e conformidade no modo Desenvolvedor
- Gerenciamento de alterações no modo Desenvolvedor
- Infraestrutura de provisionamento no modo AMS Developer
- Controles de detetive no modo AMS Developer
- Registro, monitoramento e gerenciamento de eventos no modo AMS Developer
- Gerenciamento de incidentes no modo AMS Developer
- Gerenciamento de patches no modo AMS Developer
- Gerenciamento de continuidade no modo AMS Developer
- Gerenciamento de segurança e acesso no modo AMS Developer

O modo Desenvolvedor do AWS Managed Services (AMS) usa permissões elevadas nas contas AMS Advanced Plus e Premium para provisionar e atualizar recursos da AWS fora do processo de gerenciamento de alterações do AMS Advanced. O modo Desenvolvedor Avançado do AMS faz isso aproveitando as chamadas de API nativas da AWS na Nuvem Privada Virtual (VPC) do AMS Advanced, permitindo que você projete e implemente infraestrutura e aplicativos em seu ambiente gerenciado.

Ao usar uma conta com o modo Desenvolvedor ativado, o gerenciamento de continuidade, o gerenciamento de patches e o gerenciamento de alterações são fornecidos para recursos

provisionados por meio do processo de gerenciamento de alterações do AMS Advanced ou usando uma AMS Amazon Machine Image (AMI). No entanto, esses recursos de gerenciamento do AMS não são oferecidos para recursos provisionados por meio de recursos nativos. AWS APIs

Você é responsável por monitorar os recursos de infraestrutura que são provisionados fora do processo de gerenciamento de alterações do AMS Advanced. O modo de desenvolvedor é compatível com cargas de trabalho de produção e não produção. Com permissões elevadas, você tem uma responsabilidade maior de garantir a adesão aos controles internos.

> **Important**
>
> Os recursos que você cria usando o modo Desenvolvedor só podem ser gerenciados pelo AMS Advanced se forem criados usando os processos de gerenciamento de alterações do AMS Advanced.

O modo de desenvolvedor é um dos modos avançados do AMS que você pode empregar. Para obter mais informações, consulte Visão geral dos modos.

Introdução ao modo AMS Advanced Developer

Aprenda as várias contas do AMS Advanced com o modo Desenvolvedor Avançado do AMS e como implementar com êxito o modo Desenvolvedor.

Tópicos

- Antes de começar com o modo AMS Developer
- Pré-requisitos para o modo AMS Developer
- Como implementar o modo AMS Advanced Developer
- Permissões do modo Desenvolvedor Avançado do AMS

Antes de começar com o modo AMS Developer

Antes de implementar o modo Desenvolvedor, há algumas coisas que você deve saber.

O AMS Advanced não pode gerenciar pilhas ou recursos existentes em uma DevMode conta criada fora do processo de gerenciamento de alterações do AMS Advanced por meio de solicitações de alteração (RFCs). No entanto, enquanto a conta está ativa DevMode, o AMS Advanced continua

gerenciando os recursos provisionados por meio do processo de gerenciamento de alterações do AMS Advanced com. RFCs

Você não pode começar com uma DevMode conta e depois convertê-la em uma conta de aplicativo gerenciada pelo AMS Advanced.

Pré-requisitos para o modo AMS Developer

A seguir estão os pré-requisitos para implementar o modo Desenvolvedor:

- Você deve ser um cliente do AMS Advanced com pelo menos uma conta AMS Advanced Plus ou Premium integrada.
- Qualquer conta que você usa deve ser uma conta AMS Advanced Plus ou Premium.
- Zona de destino de várias contas (MALZ): você deve usar a função `AWSManagedServicesDevelopmentRole` predefinida AWS Identity and Access Management (IAM). Você solicita essa função. A próxima seção descreve como adquirir as permissões do modo Desenvolvedor.
- Zona de destino de conta única (SALZ): você deve usar a função `customer_developer_role` predefinida AWS Identity and Access Management (IAM). Você solicita essa função. A próxima seção descreve como adquirir as permissões do modo Desenvolvedor.

Como implementar o modo AMS Advanced Developer

Você implementa o modo Desenvolvedor solicitando que sua conta qualificada do AMS Advanced seja provisionada com a função predefinida do IAM:

- MALZ: `AWSManagedServicesDevelopmentRole`
- SAL: `customer_developer_role`

Em seguida, você atribui a função aos usuários relevantes em sua rede federada.

O AMS Advanced recomenda que você garanta que o uso do modo Desenvolvedor esteja em conformidade com suas estruturas e padrões de controle interno, pois o modo Desenvolvedor cria dois vetores de mudança: gerenciamento avançado de alterações do AMS para recursos gerenciados pelo AMS Advanced e federação de funções gerenciadas pelo cliente para recursos que você, como nosso cliente, gerencia. Embora os processos do AMS Advanced permaneçam em conformidade com nossas declarações, os processos do cliente e as estruturas de controle talvez precisem ser atualizados.

Para implementar o modo Desenvolvedor em sua conta do AMS Advanced

1. Confirme se a conta que você deseja usar com o modo Desenvolvedor atende aos requisitos listados emPré-requisitos para o modo AMS Developer.
2. Envie uma solicitação de alteração (RFC) usando o tipo de alteração (CT) Gerenciamento | Conta gerenciada | Modo de desenvolvedor | Ativar (revisão necessária). Para obter um exemplo de como usar essa CT, consulte Modo de desenvolvedor | Ativar (revisão necessária).

   Depois que a CT é processada, a função predefinida do IAM (`AWSManagedServicesDevelopmentRole`para MALZ, `customer_developer_role` para SALZ) é provisionada na conta solicitada.
3. Atribua a função apropriada aos usuários que precisam de acesso ao modo Desenvolvedor usando seu processo interno de federação.

   O AMS Advanced recomenda que você limite o acesso para evitar o provisionamento indesejado ou não aprovado de recursos ou alterações nos mesmos.

Permissões do modo Desenvolvedor Avançado do AMS

A função predefinida (`AWSManagedServicesDevelopmentRole`para MALZ, para SALZ) concede permissão `customer_developer_role` para criar recursos de infraestrutura de aplicativos dentro da VPC avançada do AMS, incluindo funções do IAM, ao mesmo tempo em que restringe o acesso aos componentes de serviços compartilhados que são operados pelo AMS Advanced (por exemplo, hosts de gerenciamento, controladores de domínio, Trend Micro EPS, bastiões e serviços da AWS sem suporte). A função também restringe o acesso aos seguintes registros Serviços da AWS: Amazon GuardDuty,, AWS Organizations AWS Directory Service APIs, e AMS Advanced.

Embora a função permita que você crie funções adicionais do IAM, os mesmos limites de permissões incluídos no acesso ao modo Desenvolvedor são aplicados em qualquer função do IAM criada pelo`AWSManagedServicesDevelopmentRole`.

Segurança e conformidade no modo Desenvolvedor

Segurança e conformidade são uma responsabilidade compartilhada entre a AMS Advanced e você como nosso cliente. O modo Desenvolvedor Avançado do AMS transfere para você a responsabilidade compartilhada pelos recursos provisionados fora do processo de gerenciamento de alterações ou provisionados por meio do gerenciamento de alterações, mas atualizados com

as permissões do modo Desenvolvedor. Para obter mais informações sobre responsabilidade compartilhada, consulte AWS Managed Services.

Precauções:

- DevMode permite que você e sua equipe autorizada ignorem os deny-by-default princípios fundamentais da segurança do AMS. As vantagens, o autoatendimento e o menor tempo de espera pelo AMS, devem ser comparadas às desvantagens. Qualquer pessoa pode realizar ações inesperadas e destrutivas sem o conhecimento de sua equipe de segurança. Os tipos de alteração automatizados para ativar o modo Dev e o modo Direct Change são expostos, e qualquer pessoa autorizada em sua organização pode executá-los CTs e habilitar esses modos.
- Você é responsável por gerenciar as permissões de execução de CT da sua base de usuários.
- O AMS não gerencia as permissões de execução de CT

Recomendações:

- Proteja
  - Os clientes podem impedir o acesso a essa CT por meio de permissão, consulte Restringir permissões com declarações de política de função do IAM
  - Impeça o acesso a essa CT implementando um proxy, como um sistema ITSM
  - Utilize políticas de controle de serviço (SCPs) que previnam políticas e comportamentos conforme necessário, consulte a Biblioteca de Controles Preventivos e Detectivos do AMS
- Detectar
  - Monitore seus RFCs para ver se eles CTs (habilitar o modo de desenvolvedor ct-1opjmhuddw194 e modo de mudança direta, habilitar ct-3rd4781c2nnhp) estão sendo executados e responda adequadamente
  - Analise a presença dos recursos do IAM em suas and/or contas para identificar as contas em que o modo Desenvolvedor ou o modo de Alteração Direta foram implantados.
- Responda
  - Remova contas no modo Desenvolvedor conforme necessário

Segurança no modo Desenvolvedor

O AMS Advanced oferece valor adicional com uma landing zone prescritiva, um sistema de gerenciamento de mudanças e gerenciamento de acesso. Ao usar o modo Desenvolvedor,

o valor de segurança do AMS Advanced é mantido usando a mesma configuração de conta das contas padrão do AMS Advanced que estabelece a linha de base da rede reforçada de segurança do AMS Advanced. A rede é protegida pelo limite de permissões imposto na função (`AWSManagedServicesDevelopmentRole`para MALZ, **`customer_developer_role`** para SALZ), o que impede o usuário de quebrar as proteções de parâmetros estabelecidas quando a conta é configurada.

Por exemplo, usuários com a função podem acessar o Amazon Route 53, mas a zona hospedada interna do AMS Advanced é restrita. Os mesmos limites de permissões são aplicados em uma função do IAM criada pelo`AWSManagedServicesDevelopmentRole`, impondo limites de permissões à `AWSManagedServicesDevelopmentRole` que impede o usuário de detalhar as proteções de parâmetros estabelecidas quando a conta é integrada ao AMS Advanced.

Conformidade no modo Desenvolvedor

O modo de desenvolvedor é compatível com cargas de trabalho de produção e não produção. É sua responsabilidade garantir a adesão a quaisquer padrões de conformidade (por exemplo, PHI, HIPAA, PCI) e garantir que o uso do modo Desenvolvedor esteja em conformidade com suas estruturas e padrões de controle interno.

Gerenciamento de alterações no modo Desenvolvedor

O gerenciamento de mudanças é o processo que o serviço AMS Advanced usa para implementar solicitações de mudança. Uma solicitação de alteração (RFC) é uma solicitação criada por você ou pelo AMS Advanced por meio da interface do AMS Advanced para fazer uma alteração em seu ambiente gerenciado e inclui uma ID de tipo de alteração (CT) para uma operação específica. Para obter mais informações, consulte Modos de gerenciamento de alterações.

O gerenciamento de alterações não é aplicado nas contas avançadas do AMS, nas quais as permissões do modo Desenvolvedor são concedidas. Os usuários que receberam a permissão do modo Desenvolvedor com a função IAM (`AWSManagedServicesDevelopmentRole`para MALZ, **`customer_developer_role`** para SALZ) podem usar o acesso nativo à AWS API para provisionar e fazer alterações nos recursos em suas contas do AMS Advanced. Os usuários que não têm a função apropriada nessas contas devem usar o processo de gerenciamento de alterações do AMS Advanced para fazer alterações.

> **Important**
>
> Os recursos que você cria usando o modo Desenvolvedor só podem ser gerenciados pelo AMS Advanced se forem criados usando os processos de gerenciamento de alterações do AMS Advanced. As solicitações de alterações enviadas ao AMS Advanced para recursos criados fora do processo de gerenciamento de alterações do AMS Advanced são rejeitadas pelo AMS Advanced porque devem ser tratadas por você.

Restrições da API de serviços de provisionamento de autoatendimento

Todos os serviços autoprovisionados do AMS Advanced são compatíveis com o modo Desenvolvedor. O acesso aos serviços autoprovisionados está sujeito às limitações descritas nas respectivas seções do guia do usuário de cada um. Se um serviço autoprovisionado não estiver disponível com sua função do modo Desenvolvedor, você poderá solicitar uma função atualizada por meio do tipo de alteração do modo Desenvolvedor.

Os seguintes serviços não fornecem acesso total ao serviço APIs:

Serviços autoprovisionados restritos no modo Desenvolvedor

Serviço	Observações
Amazon API Gateway	Todas as APIs chamadas do Gateway são permitidas, exceto`SetWebACL` .
Application Auto Scaling	Só é possível registrar ou cancelar o registro de alvos escaláveis e colocar ou excluir uma política de escalabilidade.
AWS CloudFormation	Não é possível acessar ou modificar CloudFormation pilhas que tenham um nome prefixado com. `mc-`
AWS CloudTrail	Não é possível acessar ou modificar CloudTrai l recursos que tenham um nome prefixado com `ams-` and/or `mc-`.
Amazon Cognito (grupos de usuários)	Não é possível associar tokens de software.

Serviço	Observações
	Não é possível criar grupos de usuários, trabalhos de importação de usuários, servidores de recursos ou provedores de identidade.
AWS Directory Service	Somente as Directory Service ações a seguir são `Connect` exigidas pelos `WorkSpaces` serviços. Todas as outras ações do Directory Service são negadas pela política de limite de permissão do modo Desenvolvedor: • `ds:AuthorizeApplication` • `ds:CreateAlias` • `ds:CreateIdentityPoolDirectory` • `ds:DeleteDirectory` • `ds:DescribeDirectories` • `ds:GetAuthorizedApplication Details` • `ds:ListAuthorizedApplications` • `ds:UnauthorizeApplication` Em contas de landing zone de conta única, a política de limites nega explicitamente o acesso ao diretório gerenciado do AMS Advanced usado pelo AMS Advanced para manter o acesso às contas habilitadas para o modo dev.
Amazon Elastic Compute Cloud	Não é possível acessar a Amazon EC2 APIs que contém a string: `DhcpOptions` `GatewaySubnet`,`VPC`,, `VPN` e. Não é possível acessar ou modificar EC2 recursos da Amazon que tenham uma tag prefixada com`AMS`,, `mcManagementHostASG` , and/or `sentinel`.

Serviço	Observações
Amazon EC2 (relatórios)	Somente o acesso de visualização é concedido (não é possível modificar). Observação: o Amazon EC2 Reports está mudando. O item de menu Relatórios será removido do menu de navegação EC2 do console Amazon. Para visualizar seus relatórios EC2 de uso da Amazon após sua remoção, use o AWS Billing console de gerenciamento de custos.
AWS Identity and Access Management (IAM)	Não é possível excluir os limites de permissão existentes nem modificar as políticas de senha de usuário do IAM. Não é possível criar ou modificar recursos do IAM, a menos que você esteja usando a função correta do IAM (`AWSManagedServices DevelopmentRole` para MALZ, `customer_ developer_role` para SALZ)). Não é possível modificar os recursos do IAM prefixados com:`ams`,, `mccustomer_ deny_policy` , and/or `sentinel`. Ao criar um novo recurso do IAM (função, usuário ou grupo), o limite de permissão (MALZ:**`AWSManagedServicesDevelopme ntRolePermissionsBoundary`** , SALZ:`ams-app-infra-permissions-b oundary`) deve ser anexado.
AWS Key Management Service (AWS KMS)	Não é possível acessar ou modificar as chaves KMS gerenciadas pelo AMS Advanced.
AWS Lambda	Não é possível acessar ou modificar AWS Lambda funções prefixadas com`AMS`.

Serviço	Observações
CloudWatch Registros	Não é possível acessar fluxos de CloudWatch log com um nome prefixado com:`mc`,,`aws`,`lambda`. and/or `AMS`
Amazon Relational Database Service (Amazon RDS)	Não é possível acessar ou modificar bancos de dados do Amazon Relational Database Service (Amazon RDS) DBs () que tenham um nome prefixado com:. `mc-`
AWS Resource Groups	Só é possível acessar `GetList`, e ações da API `Search` Resource Group.
Amazon Route 53	Não é possível acessar ou modificar os recursos mantidos pelo Route53 AMS Advanced.
Amazon S3	Não é possível acessar buckets do Amazon S3 que tenham um nome prefixado com:`ams-*`,,, `ams` ou. `ms-a` `mc-a`
AWS Security Token Service	A única API de serviço de token de segurança permitida é`DecodeAuthorizatio nMessage` .
Amazon SNS	Não é possível acessar tópicos do SNS que tenham um nome prefixado com:`AMS-`,`Energon-Topic` , ou. `MMS-Topic`
AWS Systems Manager Gerente (SSM)	Não é possível modificar os parâmetros SSM prefixados com `amsmc`, ou. `svc` Não é possível usar a API SSM em `SendCommand` EC2 instâncias da Amazon que tenham uma tag prefixada com `ams` ou. `mc`

Serviço	Observações
AWS marcação	Você só tem acesso às ações da API de AWS marcação prefixadas com. `Get`
AWS Lake Formation	As seguintes ações de AWS Lake Formation API foram negadas: • `lakeformation:DescribeResource` • `lakeformation:GetDataLakeSettings` • `lakeformation:DeregisterResource` • `lakeformation:RegisterResource` • `lakeformation:UpdateResource` • `lakeformation:PutDataLakeSettings`
Amazon Elastic Inference	Você só pode chamar a ação da API Elastic Inference. `elastic-inference:Connect` Essa permissão está incluída no `customer_sagemaker_admin_policy` que está anexado ao`customer_sagemaker_admin_role` . Essa ação dá acesso ao acelerador Elastic Inference.
AWS Shield	Sem acesso a nenhum desses serviços APIs ou console.
Amazon Simple Workflow Service	Sem acesso a nenhum desses serviços APIs ou console.

Infraestrutura de provisionamento no modo AMS Developer

Os usuários que não têm a função IAM do modo DesenvolvedorAWSManagedServicesDevelopmentRole, em contas em que o modo

Desenvolvedor está ativado, devem seguir o processo de gerenciamento de alterações do AMS Advanced que aproveita o AMS Advanced AMIs. Usuários com a função correta (MALZ:**`AWSManagedServicesDevelopmentRole`**, SALZ:`customer_developer_role`) podem usar o sistema de gerenciamento de alterações AMS Advanced e o AMS Advanced AMIs , mas não precisam.

> **Note**
>
> Uma AWS AMI que não tenha sido processada por meio da ingestão de carga de trabalho do AMS Advanced ou criada em uma conta do AMS Advanced não incluirá as configurações exigidas pelo AMS Advanced.

Controles de detetive no modo AMS Developer

Esta seção foi redigida porque contém informações confidenciais relacionadas à segurança do AMS. Essas informações estão disponíveis na documentação do console AMS. Para acessar o AWS Artifact, você pode entrar em contato com seu CSDM para obter instruções ou acessar Getting Started with AWS Artifact.

Registro, monitoramento e gerenciamento de eventos no modo AMS Developer

O registro, o monitoramento e o gerenciamento de eventos não estão disponíveis para recursos provisionados fora do processo de gerenciamento de alterações do AMS Advanced ou para recursos provisionados por meio do gerenciamento de alterações e depois alterados por uma conta usando as permissões do modo Desenvolvedor.

Gerenciamento de incidentes no modo AMS Developer

Nenhuma alteração nos tempos de resposta a incidentes. A resolução de incidentes é o melhor esforço para recursos provisionados fora do processo de gerenciamento de alterações ou recursos provisionados por meio do gerenciamento de alterações e depois alterados por uma conta usando as permissões do modo Desenvolvedor.

> **Note**
>
> O acordo de nível de serviço (SLA) do AMS não se aplica aos recursos criados ou atualizados fora do sistema de gerenciamento de alterações do AMS (solicitações de mudança ou RFCs), incluindo o modo Desenvolvedor; portanto, os recursos atualizados ou criados no modo Desenvolvedor são automaticamente degradados para P3, e o suporte do AMS é o melhor esforço.

Gerenciamento de patches no modo AMS Developer

O gerenciamento de patches não está disponível para recursos provisionados fora do processo de gerenciamento de alterações do AMS Advanced ou para recursos provisionados por meio do gerenciamento de alterações e depois alterados por uma conta usando as permissões do modo Desenvolvedor. Tempos de aplicação de patches:

- Para uma atualização crítica de segurança: dentro de 10 dias úteis após o lançamento pelo fornecedor dos recursos provisionados por meio do gerenciamento de alterações e depois alterados por uma conta usando as permissões do modo Desenvolvedor.
- Para uma atualização importante: dentro de 2 meses após o lançamento pelo fornecedor dos recursos provisionados por meio do gerenciamento de alterações e depois alterados por uma conta usando as permissões do modo Desenvolvedor.

Gerenciamento de continuidade no modo AMS Developer

O gerenciamento de continuidade não está disponível para recursos provisionados fora do processo de gerenciamento de alterações do AMS Advanced ou para recursos provisionados por meio do gerenciamento de alterações e depois alterados por uma conta usando as permissões do modo Desenvolvedor.

O tempo de início da recuperação do ambiente pode levar até 12 horas para recursos provisionados fora do processo de gerenciamento de alterações do AMS Advanced ou para recursos provisionados por meio do gerenciamento de alterações e depois alterados por uma conta usando as permissões do modo Desenvolvedor.

Gerenciamento de segurança e acesso no modo AMS Developer

A proteção antimalware é de sua responsabilidade pelos recursos provisionados fora do processo de gerenciamento de alterações do AMS Advanced ou pelos recursos provisionados por meio do gerenciamento de alterações e depois alterados por uma conta usando as permissões do modo Desenvolvedor. O acesso às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não provisionadas por meio do gerenciamento avançado de alterações do AMS pode ser controlado por pares de chaves em vez de fornecer acesso federado.

Modo de provisionamento de autoatendimento no AMS

O modo Self-Service Provisioning (SSP) do AWS Managed Services (AMS) fornece acesso total aos recursos nativos de AWS serviços e APIs nas contas gerenciadas do AMS. Você acessa os serviços por meio de funções padronizadas e com escopo reduzido. AWS Identity and Access Management O AMS fornece solicitações de serviço e gerenciamento de incidentes. Alertas, monitoramento, registro, patches, backup e gerenciamento de alterações são de sua responsabilidade. Em muitos casos, os serviços de provisionamento de autoatendimento (SSPS) são autogerenciados ou sem servidor e não exigem o gerenciamento de determinadas tarefas operacionais, como a aplicação de patches. Você se beneficia do uso desses serviços dentro do limite do ambiente definido pelas proteções do AMS e quaisquer alterações do IAM (incluindo funções vinculadas a serviços, funções de serviço, funções entre contas ou atualizações de políticas) precisam ser aprovadas pelas operações do AMS para manter a segurança básica da plataforma. Você pode aproveitar CloudFormation modelos para automatizar a implantação desses serviços, mas isso não é compatível com todos os serviços SSP.

> **Important**
>
> Use o modo SSP em suas contas do AWS Managed Services (AMS) para acessar e empregar AWS serviços, com restrições conforme indicado.

Existem alguns Serviços da AWS que você pode usar sem o gerenciamento do AMS, na sua conta do AMS. Os serviços do modo de provisionamento de autoatendimento, ou SSPS, abreviadamente, como adicioná-los à sua conta do AMS e FAQs para cada um deles, estão descritos na seção.

Os serviços de provisionamento de autoatendimento são oferecidos no estado em que se encontram, e você é responsável por gerenciá-los. O AMS não fornece alertas, monitoramento, registro ou correção para os recursos associados a esses serviços. O AMS fornece funções do IAM que permitem que você use o serviço em sua conta do AMS com segurança. O AMS SLAs não se aplica.

Para recursos que você provisiona por meio de autoatendimento, o AMS fornece gerenciamento de incidentes, controles e barreiras de proteção de detetives, relatórios, recursos designados (Cloud Service Delivery Manager e Cloud Architect), segurança e acesso e suporte técnico por meio de solicitações de serviço. Além disso, quando aplicável, você assume a responsabilidade pelo gerenciamento de continuidade, gerenciamento de patches, monitoramento da infraestrutura e gerenciamento de alterações para recursos provisionados ou configurados fora do sistema de gerenciamento de alterações do AMS.

Introdução ao modo SSP no AMS

O provisionamento por autoatendimento é um dos modos AMS para a landing zone de várias contas (MALZ) que você pode empregar. Para obter mais informações, consulte Visão geral dos modos.

Para fornecer recursos de provisionamento por autoatendimento, o AMS criou funções elevadas do IAM com limites de permissão para limitar as alterações não intencionais do acesso direto. AWS service (Serviço da AWS) As funções não impedem todas as mudanças e você deve seguir seus controles internos e políticas de conformidade e validar se todos os que Serviços da AWS estão sendo usados atendem às certificações exigidas. Esse é o modo de provisionamento de autoatendimento. Para obter detalhes sobre os requisitos de AWS conformidade, consulte AWS Conformidade.

Para adicionar um serviço de provisionamento de autoatendimento à sua conta multiconta do aplicativo landing zone, use o Management AWS | service | Self-provisioned service | Add change type (CT), seja o CT exigido pela revisão ou o CT automatizado, conforme as instruções do serviço.

> **Note**
>
> Para solicitar que o AMS forneça um serviço adicional de provisionamento de autoatendimento, registre uma solicitação de serviço.

Use o AMS SSP para provisionar o Amazon API Gateway em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon API Gateway diretamente em sua conta gerenciada pelo AMS. O Amazon API Gateway é um serviço totalmente gerenciado que facilita aos desenvolvedores criar, publicar, manter, monitorar e proteger APIs em qualquer escala. Usando o, Console de gerenciamento da AWS você pode criar REST e

WebSocket APIs isso funcionar como porta de entrada para aplicativos acessarem dados, lógica de negócios ou funcionalidade de seus serviços de back-end, como cargas de trabalho executadas na Amazon Elastic Compute Cloud (Amazon EC2), código executado em AWS Lambdaqualquer aplicativo web ou aplicativos de comunicação em tempo real.

O API Gateway lida com todas as tarefas envolvidas na aceitação e processamento de até centenas de milhares de chamadas de API simultâneas, incluindo gerenciamento de tráfego, autorização e controle de acesso, monitoramento e gerenciamento de versões de API. O API Gateway não tem taxas mínimas nem custos iniciais. Você paga somente pelas chamadas de API recebidas e pela quantidade de dados transferidos. Com o modelo de preços em camadas do API Gateway, você pode reduzir seus custos à medida que o uso da API aumenta. Para saber mais, consulte Amazon API Gateway.

Perguntas frequentes: API Gateway no AMS

P: Como solicito acesso ao Amazon API Gateway na minha conta AMS?

Solicite acesso ao API Gateway enviando uma RFC com o tipo de alteração Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Essa RFC provisiona as seguintes funções do IAM para sua conta: `customer_apigateway_author_role` e. `customer_apigateway_cloudwatch_role` Depois de provisionado em sua conta, você deve integrar as funções em sua solução de federação.

P: Quais são as restrições ao uso do Amazon API Gateway na minha conta AMS?

- A configuração do API Gateway é limitada a recursos sem prefixos `AMS-` ou `MC-` prefixos para evitar modificações na infraestrutura do AMS.
- `CREATE`os privilégios de VPCLink são desativados para evitar a criação não regulamentada de Elastic Load Balancers. VPCLinks Se necessário, consulte Application Load Balancer | Create.

P: Quais são os pré-requisitos ou dependências para usar o Amazon API Gateway na minha conta AMS?

Depende do tipo de API Gateway que você deseja implantar. Ele pode ser um serviço independente, mas também pode solicitar acesso aos serviços existentes (por exemplo, balanceador de carga de rede).

Use o AMS SSP para provisionar o Alexa for Business em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Alexa for Business diretamente em sua conta gerenciada pelo AMS. O Alexa for Business é um serviço que permite que sua organização e seus funcionários usem a Alexa para realizar mais trabalhos. Com o Alexa for Business, você pode usar a Alexa como sua assistente inteligente para ser mais produtivo nas salas de reunião, na sua mesa e até mesmo com os dispositivos Alexa que você já usa em casa ou em qualquer lugar. Os gerentes de TI e instalações podem usar o Alexa for Business para medir e aumentar a utilização das salas de reunião existentes em seu local de trabalho.

Para saber mais, consulte Alexa for Business.

Perguntas frequentes sobre o Alexa for Business no AWS Managed Services

P: Como solicito acesso ao Alexa for Business na minha conta AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_alexa_console_role`. A também `customer_alexa_device_setup_user` é criada para a ferramenta de configuração de dispositivos fornecida pelo Alexa for Business; essa ferramenta de configuração de dispositivos pode então ser usada para configurar seus dispositivos. Depois de provisionado em sua conta, você deve integrar as funções em sua solução de federação.

O gateway Alexa for Business permite que você conecte o Alexa for Business aos seus endpoints Cisco Webex e Poly Group Series para controlar reuniões com sua voz. O software de gateway é executado em seu hardware local e transfere com segurança as diretivas de conferência do Alexa for Business para seu endpoint Cisco. O gateway precisa de dois pares de AWS credenciais para se comunicar com o Alexa for Business. Fornecemos dois usuários do IAM com acesso limitado: `customer_alexa_gateway_installer_user` e `customer_alexa_gateway_execution_user` para seus gateways do Alexa for Business, um para instalar o gateway e outro para operar o gateway; eles podem ser solicitados enviando uma RFC com o tipo de alteração Deployment | Advanced stack components | Identity and Access Management (IAM) | Criar entidade ou política (revisão obrigatória) do tipo de alteração (ct-3dpd8mdd9jn1r).

> **Note**
>
> Para gerar relatórios de uso e enviá-los para o Amazon S3, especifique o nome do bucket do Amazon S3 na RFC do serviço autoprovisionado.

P: Quais são as restrições para usar o Alexa for Business na minha conta AMS?

Não há restrições. A funcionalidade completa do Alexa for Business está disponível com a função de serviço autoprovisionado do Alexa for Business.

P: Quais são os pré-requisitos ou dependências para usar o Alexa for Business na minha conta AMS?

- Se você pretende usar o WPA2 Enterprise Wi-Fi para configurar seus dispositivos compartilhados, especifique esse tipo de segurança de rede na Ferramenta de configuração do dispositivo, para o qual Autoridade de Certificação Privada da AWS é necessário um.
- O AMS cria apenas chaves secretas que começam com o namespace “A4B”. Isso é restritivo somente a esse namespace.

P: Quais funcionalidades do Alexa for Business precisam RFCs ser separadas?

Para registrar um dispositivo Alexa Voice Service (AVS) no Alexa for Business, forneça acesso ao fabricante de dispositivos integrado da Alexa. Para fazer isso, uma função do IAM precisa ser criada no console do Alexa for Business, que pode ser implantada usando o tipo de alteração Management | Other | Other. Isso permite que o fabricante do dispositivo AVS registre e gerencie dispositivos com o Alexa for Business em seu nome.

Use o AMS SSP para provisionar o Amazon AppStream 2.0 em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos da Amazon AppStream 2.0 (AppStream 2.0) diretamente na sua conta gerenciada do AMS. AppStream 2.0 permite que você mova seus aplicativos de desktop para AWS, sem precisar reescrevê-los. Você pode instalar seus aplicativos na AppStream versão 2.0, definir configurações de inicialização e disponibilizar seus aplicativos para os usuários. AppStream A versão 2.0 oferece uma ampla seleção de opções de máquina virtual para que você possa selecionar o tipo de instância que melhor atenda aos requisitos do seu aplicativo e definir os parâmetros de escala automática para que você possa

atender facilmente às necessidades de seus usuários finais. AppStream 2.0 permite que você inicie aplicativos em sua própria rede, o que significa que seus aplicativos podem interagir com seus AWS recursos existentes.

A Amazon AppStream 2.0 permite que você instale, teste e atualize seus aplicativos de forma rápida e fácil usando o criador de imagens. Qualquer aplicativo executado no Microsoft Windows Server 2012 R2, Windows Server 2016 ou Windows Server 2019 tem suporte e você não precisa fazer nenhuma modificação. Quando o teste estiver concluído, você poderá definir as configurações de inicialização do aplicativo, as configurações padrão do usuário e publicar sua imagem para que os usuários acessem.

Para saber mais, consulte AppStream 2.0.

AppStream Perguntas frequentes sobre 2.0 no AWS Managed Services

P: Como faço para solicitar acesso ao AppStream 2.0 na minha conta do AMS?

Solicite acesso ao AppStream 2.0 enviando um RFC com o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (ct-3qe6io8t6jtny). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_appstream_console_role`.

`customer_appstream_stream_role`A também é implantado para transmitir aplicativos que exigem que os usuários sejam autenticados usando suas credenciais de login do Active Directory.

Depois de provisionado em sua conta, você deve integrar as funções em sua solução de federação.

P: Quais são as restrições ao uso da AppStream versão 2.0 na minha conta AMS?

- A funcionalidade a seguir deve ser configurada pela equipe de suporte do AMS e requer funcionalidades específicas RFCs. As instruções sobre como solicitar funcionalidades adicionais podem ser encontradas na seção 4.
  - Criação e streaming a partir de endpoints de interface VPC.
  - Support for Amazon S3 endpoints para pastas pessoais e persistência de configurações de aplicativos em uma rede privada.
  - Criar e escolher a função do IAM que estará disponível em todas as instâncias de streaming da frota.
  - Unindo frotas AppStream 2.0 e construtores de imagens aos domínios do Microsoft Active Directory.
  - Criação de relatórios de uso personalizados AppStream 2.0.

- Atualmente, a identidade visual personalizada não é suportada.

P: Quais são os pré-requisitos ou dependências para usar AppStream 2.0 na minha conta do AMS?

Ao enviar o RFC para o onboard AppStream 2.0, inclua o nome do bucket do Amazon S3 a ser usado no relatório de uso do 2.0. AppStream O nome do bucket é adicionado ao `customer-appstream-usagereports-policy` que é criado quando AppStream 2.0 é integrado.

P: Quais funcionalidades AppStream 2.0 precisam ser separadas RFCs?

- Para escolher uma interface VPC endpoint para AppStream 2.0, envie um RFC de tipo de alteração Management | Other | Other | Update para criar um VPC endpoint em sua conta. Para ver as etapas para criar endpoints personalizados para AppStream 2.0, consulte Criação e streaming a partir de endpoints de interface VPC no guia AppStream do usuário 2.0.
- O suporte para endpoints do Amazon S3 para pastas iniciais e persistência de configurações de aplicativos em uma rede privada pode ser configurado solicitando endpoints VPC do Amazon S3 com um RFC de gerenciamento | Outro | Outro | Crie o tipo de alteração. O RFC deve incluir o bucket do Amazon S3 de destino que hospeda o conteúdo da pasta inicial ou as configurações do aplicativo, os buckets do Amazon S3, respectivamente. Essa RFC fornecerá à AppStream 2.0 as permissões necessárias para acessar os endpoints VPC do Amazon S3. Para ver as etapas para criar endpoints personalizados para streams, consulte Uso de endpoints VPC do Amazon S3 para pastas domésticas e persistência de configurações de aplicativos no guia do usuário 2.0. AppStream
- Para criar e escolher uma função do IAM que estará disponível em todas as instâncias de streaming da frota, envie uma RFC de implantação | Advanced stack components | Identity and Access Management (IAM) | Crie uma entidade ou política (revisão obrigatória) do tipo de alteração (ct-3dpd8mdd9jn1r) solicitando a função do IAM com a política necessária. O nome da função do IAM deve sempre começar com o prefixo: “customer_appstream”.
- As frotas e os criadores de imagens da Amazon AppStream 2.0 podem ser unidos a domínios no Microsoft Active Directory enviando um RFC de gerenciamento | Outro | Outro | Atualizar do tipo de alteração para a criação da conta de serviço no Active Directory (AD). As permissões mínimas necessárias para ingressar no Microsoft Active Directory estão definidas na documentação AppStream 2.0 em Concedendo permissões para criar e gerenciar objetos de computador do Active Directory.
- Para criar relatórios de uso AppStream 2.0 personalizados, envie um RFC de gerenciamento | Outro | Outro | Crie um tipo de alteração RFC solicitando o seguinte:

- “AppStreamUsageReports" Criação da pilha CFN
- “customer_appstream_usagereports_role” seja provisionado na conta
- Além disso, forneça os seguintes detalhes:
  - Forneça a expressão CRON para programar a execução do Crawler. Por padrão, são 23:00 UTC todos os dias.
  - ARN do bucket do Amazon S3 a ser usado para resultados de consulta do Athena. Esse bucket deve ter o prefixo: `aws-athena-query-results`
  - ARN do bucket Amazon S3 para registros de relatórios de uso AppStream 2.0.

Depois que a função for provisionada, integre-a à sua solução de federação, faça login e acesse o AWS GlueAWS Glue Athena para gerar relatórios personalizados usando a função de relatório de uso. Para obter detalhes sobre o uso de relatórios de uso AppStream 2.0, consulte Criar relatórios personalizados e analisar dados de uso AppStream 2.0, na documentação AppStream 2.0.

Use o AMS SSP para provisionar o Amazon Athena em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Athena (Athena) diretamente na sua conta gerenciada do AMS. O Athena é um serviço de consulta interativo que ajuda você a analisar dados no Amazon S3 usando SQL padrão. Como o Athena é sem servidor, não há infraestrutura para gerenciar, e você paga apenas pelas consultas executadas. Você aponta para seus dados no Amazon S3, define o esquema e começa a consultar usando o SQL padrão. A maioria dos resultados é entregue em segundos. Com o Athena, não há necessidade de trabalhos complexos extract-transform-load (ETL) para preparar seus dados para análise. Isso torna fácil para qualquer pessoa com habilidades em SQL analisar rapidamente conjuntos de dados em grande escala. Para saber mais, consulte Amazon Athena.

Perguntas frequentes: Athena no AMS

P: Como solicito acesso ao Amazon Athena na minha conta do AMS?

Solicite acesso ao Athena enviando uma RFC com o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_athena_console_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições para usar o Amazon Athena na minha conta AMS?

Não há restrições. A funcionalidade completa do Amazon Athena está disponível em sua conta do AMS.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Athena na minha conta AMS?

Athena tem uma grande dependência do AWS Glue serviço, pois usa os dados catalog/metastore criados com. AWS Glue Portanto, AWS Glue as permissões são incluídas no RFC bem-sucedido do Athena.

A função `customer_athena_console_role` tem um pré-requisito para um bucket do Amazon S3. Para criar um novo bucket, use a CT automatizada `ct-1a68ck03fn98r` (Implantação | Componentes avançados de pilha | Armazenamento S3 | Criar). Quando você usa essa CT automatizada para criar um bucket S3 para o Athena, o nome do bucket deve começar com o prefixo. `athena-query-results-*`

Use o AMS SSP para provisionar o Amazon Bedrock em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Bedrock diretamente em sua conta gerenciada pelo AMS. O Amazon Bedrock é um serviço totalmente gerenciado que disponibiliza modelos básicos de alto desempenho (FMs) das principais startups de IA para seu uso por meio de uma API unificada. AWS É possível escolher entre uma ampla variedade de modelos de base para encontrar o modelo mais adequado ao seu caso de uso. O Amazon Bedrock também oferece um amplo conjunto de recursos para criar aplicações de IA generativa com segurança, privacidade e IA responsável. Usando o Amazon Bedrock, você pode fazer testes e avaliar com facilidade os principais modelos de base para os seus casos de uso, personalizá-los de forma privada com dados próprios usando técnicas que incluem ajuste fino e geração aumentada via recuperação (RAG) e criar agentes que executem tarefas usando seus sistemas corporativos e fontes de dados.

Com a experiência sem servidor do Amazon Bedrock, você pode começar rapidamente, personalizar de forma privada os modelos de fundação com seus próprios dados e integrá-los e implantá-los de forma fácil e segura em seus aplicativos usando as ferramentas da AWS sem precisar gerenciar nenhuma infraestrutura. Para obter mais informações, consulte Amazon Bedrock.

Perguntas frequentes: Amazon Bedrock no AMS

P: Como solicito acesso ao Amazon Bedrock na minha conta AMS?

Para solicitar acesso ao Amazon Bedrock, envie uma RFC com o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny). Este RFC

provisiona a seguinte função do IAM para sua conta:`customer_bedrock_console_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições para usar o Amazon Bedrock na minha conta AMS?

- As bases de conhecimento do Amazon Bedrock não são suportadas por padrão como parte da função SSPS devido à sua dependência do OpenSearch Amazon Service Serverless, que atualmente não é suportado pelo AMS.
- O Bedrock Studio não é suportado devido à sua dependência de serviços não suportados, como a Amazon. DataZone

P: Quais são os pré-requisitos ou dependências para usar o Amazon Bedrock na minha conta AMS?

- As assinaturas de modelos de terceiros que exigem AWS Marketplace permissões devem ser feitas pela função padrão (`AWSManagedServicesAdminRole`no MALZ e `Customer_ReadOnly_Role` no SALZ). Isso ocorre porque a função padrão inclui AWS Marketplace permissões.
- Se a criptografia de dados for usada, você deverá fornecer o ARN da AWS KMS chave ao solicitar a criação da função de console. Além disso, o bucket do Amazon S3 em uso deve ter “alicerce” em seu nome.

Use o AMS SSP para provisionar a Amazon CloudSearch em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os CloudSearch recursos da Amazon diretamente em sua conta gerenciada pelo AMS. CloudSearch A Amazon é um serviço gerenciado na AWS nuvem que você usa de forma econômica para configurar, gerenciar e escalar uma solução de pesquisa para seu site ou aplicativo. A Amazon CloudSearch oferece suporte a 34 idiomas e recursos de pesquisa populares, como destaque, preenchimento automático e pesquisa geoespacial. Para saber mais, consulte Amazon CloudSearch.

> **Note**
>
> AWS fechou o acesso de novos clientes à Amazon CloudSearch, a partir de 25 de julho de 2024. Os clientes CloudSearch existentes da Amazon podem continuar usando o serviço normalmente. AWS continua investindo em melhorias de segurança, disponibilidade e desempenho para a Amazon CloudSearch, mas não planejamos introduzir novos recursos.

Para entender as diferenças entre a Amazon CloudSearch e o Amazon OpenSearch Service e como você pode fazer a transição para o OpenSearch Service, entre em contato com seu arquiteto de nuvem (CA) para obter orientação. Para obter mais informações sobre a transição para o OpenSearch serviço, consulte Transição do serviço Amazon para o CloudSearch Amazon OpenSearch Service.

Perguntas frequentes sobre a Amazon CloudSearch in AWS Managed Services

P: Como solicito acesso à Amazon CloudSearch na minha conta do AMS?

Solicite acesso à Amazon CloudSearch enviando uma RFC com o Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Essa RFC provisiona as seguintes funções do IAM para sua conta: `customer_csearch_admin_role` e. `customer_csearch_dev_role` Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições para usar a Amazon CloudSearch na minha conta do AMS?

A funcionalidade completa da Amazon CloudSearch está disponível em sua conta do AMS. Atualmente, todas as soluções de banco de dados suportadas pela AMS são suportadas pela Amazon. CloudSearch Observe que, atualmente, o DynamoDB é a única solução de banco de dados AWS gerenciado que não pode ser indexada.

P: Quais são os pré-requisitos ou dependências para usar a Amazon CloudSearch na minha conta do AMS?

A Amazon CloudSearch depende do Amazon S3 trabalhando com provedores de identidade para analisar automaticamente os dados de entrada e determinar os campos da tabela. O acesso ao Amazon S3 não é fornecido com esta RFC e deve ser solicitado separadamente em uma solicitação de serviço.

Use o AMS SSP para provisionar Amazon CloudWatch Synthetics em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon CloudWatch Synthetics diretamente em sua conta gerenciada do AMS. Você pode usar o Amazon CloudWatch Synthetics para criar “canários” para monitorar seus endpoints e. APIs

Canários são scripts configuráveis, escritos em Node.js ou Python, que são executados em um cronograma. Eles criam funções do Lambda em sua conta que usam Node.js ou Python como framework. Os canaries trabalham por meio de protocolos HTTP e HTTPS. O Canaries verifica a disponibilidade e a latência de seus endpoints e pode armazenar dados de tempo de carregamento e capturas de tela da interface do usuário. Eles monitoram o REST APIs e o conteúdo do site e podem verificar se há alterações não autorizadas causadas por phishing, injeção de código e scripts entre sites. URLs

As Canárias seguem as mesmas rotas e realizam as mesmas ações de um cliente, possibilitando que você verifique continuamente a experiência do cliente, mesmo quando você não tem tráfego de clientes em seus aplicativos. Ao usar canaries, é possível descobrir problemas antes que seus clientes o façam. Para saber mais, consulte Amazon CloudWatch: usando monitoramento sintético.

Perguntas frequentes sobre o Amazon CloudWatch Synthetics in AWS Managed Services

P: Como solicito acesso ao Amazon CloudWatch Synthetics na minha conta AMS?

Solicite acesso ao Amazon CloudWatch Synthetics enviando uma RFC com o tipo de alteração Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Essa RFC provisiona a seguinte função do IAM para sua conta: 'customer_cw_synthetics_console_role' e 'customer_cw_synthetics_canary_lambda_role'. Depois de provisionado em sua conta, você deve integrar a função 'customer_cw_synthetics_console_role' em sua solução de federação.

P: Quais são as restrições ao uso do Amazon CloudWatch Synthetics na minha conta AMS?

Não há restrições para o uso do Amazon CloudWatch Synthetics em sua conta AMS. É proibido criar funções para canários fora da função de serviço 'customer_cw_synthetics_canary_lambda_role' fornecida pela AMS.

P: Quais são os pré-requisitos ou dependências para usar o Amazon CloudWatch Synthetics na minha conta AMS?

Os canários criam e usam um bucket padrão do Amazon CloudWatch Synthetics S3: cw-syn-results "- -" *${accountnumber} ${default-region}*

Use o AMS SSP para provisionar grupos de usuários do Amazon Cognito em sua conta do AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos de grupos de usuários do Amazon Cognito diretamente na sua conta gerenciada pelo AMS. Os grupos de usuários do Amazon Cognito fornecem um diretório de usuários seguro que pode ser escalado para centenas de milhões de usuários. Como um serviço totalmente gerenciado, os grupos de usuários do Amazon Cognito podem ser configurados sem se preocupar com a manutenção da infraestrutura do servidor. Esse serviço permite gerenciar um pool de usuários finais que você pode usar para integrar com seus aplicativos internos. Esse serviço fornece uma alternativa a um banco de dados personalizado ou a um diretório de usuários finais para aplicativos web ou móveis. Ao mesmo tempo, os grupos de usuários do Amazon Cognito fornecem o conjunto completo de funcionalidades de um serviço de diretório, como políticas de senhas, autenticação multifatorial, recuperação de senha e inscrição automática em serviços. Também permite que o aplicativo federe o acesso em outros serviços públicos populares, como OpenID, Facebook, Amazon ou Google.

O Amazon Cognito é dividido em dois produtos principais. Grupos de usuários do Amazon Cognito e provedor de identidade do Amazon Cognito. Esta seção se concentra nos grupos de usuários do Amazon Cognito, que fornecem acesso a outros AWS serviços, como Amazon S3 ou DynamoDB. O serviço permite que você use grupos de usuários do Amazon Cognito ou um provedor de identidade terceirizado para fornecer acesso aos AWS serviços. Ele também fornece acesso a AWS serviços usando acesso de convidado anônimo. Devido à natureza poderosa dos grupos de usuários do Amazon Cognito, eles seriam gerenciados manualmente como case-by-case um serviço manual de operação, a fim de evitar possíveis falhas de segurança na conta. Para saber mais, consulte Grupos de usuários do Amazon Cognito.

Perguntas frequentes sobre grupos de usuários do Amazon Cognito no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso aos grupos de usuários do Amazon Cognito na minha conta do AMS?

A implementação dos grupos de usuários do Amazon Cognito no AMS é um processo de duas etapas:

1. Envie um tipo de alteração Gerenciamento | Outro | Outro | Crie (ct-1e1xtak34nx76) e solicite a criação dos grupos de usuários do Amazon Cognito em sua conta AMS. Inclua as seguintes informações:

- AWS Região.
- Nome do Grupo de Usuários do Cognito.
- Se você quiser usar o Amazon Simple Email Service (Amazon SES) para enviar mensagens e notificações em vez do serviço de e-mail interno padrão do Cognito, o cliente deverá fornecer um endereço de e-mail já validado para o Amazon SES Service na conta. Esse endereço será usado para os campos “De” e “RESPONDER PARA” da mensagem. Eles também devem indicar a região em que o Amazon SES foi ativado (us-east-1, eu-west-1 ou us-west-2).
- Se você quiser usar mensagens SMS para senhas e verificação únicas, o cliente deve indicar isso.

2. Solicite o acesso do usuário enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Essa RFC provisiona as seguintes funções do IAM para sua conta: `customer_cognito_admin_role` e. `customer_cognito_importjob_role` Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação. Essas funções permitem que você gerencie os grupos de usuários do Amazon Cognito, gerencie seus usuários e grupos no pool, crie tarefas de importação para usuários, modifique as mensagens de notificação e assinatura, associe aplicativos ao grupo de usuários, gerencie automaticamente a adição de serviços de federação ao pool e exclua os pools já criados.

P: Quais são as restrições ao uso de grupos de usuários do Amazon Cognito na minha conta do AMS?

Você não poderá criar os grupos de usuários do Amazon Cognito. Essa ação exige a criação de funções do IAM para aproveitar os serviços usados pelo Amazon Cognito, como o Amazon SES e o Amazon Simple Notification Service (Amazon SNS).

P: Quais são os pré-requisitos ou dependências para usar grupos de usuários do Amazon Cognito na minha conta do AMS?

Se você quiser usar o Amazon SES para enviar mensagens e notificações por e-mail para seus grupos de usuários, eles já devem ativar o serviço Amazon SES na conta e validar o endereço de e-mail que deve ser usado nos campos “DE” e “RESPOSTA PARA” dos e-mails enviados. Para obter mais informações sobre a validação de endereços de e-mail usando o Amazon SES, consulte Verificação de endereços de e-mail no Amazon SES.

Use o AMS SSP para provisionar o Amazon Comprehend em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Comprehend diretamente em sua conta gerenciada pelo AMS. O Amazon Comprehend é um serviço de processamento de linguagem natural (NLP) que usa aprendizado de máquina para encontrar insights e relacionamentos em texto, sem necessidade de experiência em aprendizado de máquina. O Amazon Comprehend usa aprendizado de máquina para ajudar você a descobrir os insights e os relacionamentos em seus dados não estruturados. O serviço identifica o idioma do texto; extrai frases-chave, lugares, pessoas, marcas ou eventos; compreende o quão positivo ou negativo o texto é; analisa o texto usando tokenização e partes do discurso; e organiza automaticamente uma coleção de arquivos de texto por tópico. Você também pode usar os recursos do AutoML no Amazon Comprehend para criar um conjunto personalizado de entidades ou modelos de classificação de texto adaptados exclusivamente às necessidades da sua organização. Para saber mais, consulte Amazon Comprehend.

Perguntas frequentes sobre o Amazon Comprehend in AWS Managed Services

P: Como solicito acesso ao Amazon Comprehend na minha conta do AMS?

O console do Amazon Comprehend e as funções de acesso a dados podem ser solicitadas por meio do envio de dois serviços AMS: RFCs

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_comprehend_console_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Amazon Comprehend na minha conta do AMS?

A funcionalidade de criar uma nova função do IAM por meio do console do Amazon Comprehend é restrita. Caso contrário, a funcionalidade completa do Amazon Comprehend estará disponível em sua conta do AMS.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Comprehend na minha conta AMS?

O Amazon S3 e AWS Key Management Service (AWS KMS) são necessários para usar o Amazon Comprehend, se os buckets do Amazon S3 estiverem criptografados com chaves. AWS KMS

Use o AMS SSP para provisionar o Amazon Connect em sua conta AMS

> **Note**
>
> Após uma análise cuidadosa, decidimos encerrar o suporte para o Amazon Connect Voice ID, a partir de 20 de maio de 2026. O Amazon Connect Voice ID não aceitará mais novos clientes a partir de 20 de maio de 2025. Como cliente existente com uma conta cadastrada no serviço antes de 20 de maio de 2025, você pode continuar usando os recursos de ID de voz do Amazon Connect. Depois de 20 de maio de 2026, você não poderá mais usar o Amazon Connect Voice ID.

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Connect diretamente em sua conta gerenciada pelo AMS. O Amazon Connect é uma central de atendimento omnicanal na nuvem que ajuda as empresas a oferecer um atendimento superior ao cliente a um custo menor. O Amazon Connect oferece uma experiência perfeita em voz e chat para clientes e agentes. Isso inclui um conjunto de ferramentas para roteamento baseado em habilidades, análises poderosas em tempo real e históricas e ferramentas de gerenciamento easy-to-use intuitivas, tudo com preços. pay-as-you-go

Você pode criar uma ou mais instâncias das instâncias do contact center virtual na zona de destino com várias contas do AMS ou nas contas da zona de destino com uma única conta. Você pode usar os provedores de identidade SAML 2.0 existentes para acessar agentes ou usar o suporte nativo do Amazon Connect para o gerenciamento do ciclo de vida do usuário.

Além disso, você pode solicitar números de telefone com free/direct ligação direta para cada instância do Amazon Connect a partir do console do Amazon Connect. Você pode criar fluxos de contato avançados para alcançar a experiência e o roteamento desejados do cliente usando uma interface easy-to-use gráfica de usuário. Os fluxos de contato podem aproveitar AWS Lambda funções para integração com repositórios de dados e APIs locais. Você também pode ativar o streaming de dados usando o Kinesis Streams e o Firehose.

As gravações de chamadas, transcrições de bate-papo e relatórios são armazenados em um bucket do Amazon S3 criptografado usando uma chave. AWS KMS Os registros do fluxo de contatos podem ser salvos em grupos de CloudWatch registros.

Para saber mais, consulte Amazon Connect.

Perguntas frequentes sobre o Amazon Connect no AWS Managed Services

P: Como solicito acesso ao Amazon Connect na minha conta AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Essa RFC provisiona as seguintes funções do IAM para sua conta: `customer_connect_console_role` e. `customer_connect_user_role` Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Amazon Connect na minha conta AMS?

Não há restrições. A funcionalidade completa do Amazon Connect está disponível em sua conta AMS.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Connect na minha conta AMS?

- Você deve criar uma AWS KMS chave e um bucket do Amazon S3 usando o AMS padrão RFCs; o bucket do Amazon S3 é necessário para armazenar gravações de chamadas e transcrições de bate-papo.
- Se você quiser se integrar ao Active Directory (AD), é necessário um AD Connector para a integração entre as instâncias do Amazon Connect hospedadas pelo AMS e seus serviços de diretório locais. O AD Connector pode ser configurado em sua conta solicitando um RFC “Gerenciamento | Outros | Outros”.
- Você pode ativar os seguintes serviços opcionais autoprovisionados com base em seus requisitos de fluxo de contatos.
  - AWS Lambda: Você pode usar as funções do Lambda para estender os fluxos de contato para aproveitar os armazenamentos de dados locais existentes ou. APIs Você pode usar o serviço autoprovisionado do Lambda para criar as funções do Lambda.
  - Amazon Kinesis Data Streams: você pode criar fluxos de dados para permitir o streaming de dados para aplicativos externos. Você pode transmitir registros de rastreamento de contatos ou eventos do agente.
  - Amazon Kinesis Data Firehose: você pode criar o Data Firehose para transmitir registros de rastreamento de contatos de alto volume para aplicativos externos.
  - Amazon Lex: você pode aproveitar os chatbots do Amazon Lex para criar fluxos de contato inteligentes utilizando os serviços Amazon Alexa para proporcionar uma experiência rica ao cliente e automação.
- P: Como solicito a adição de uma lista de países para chamadas de entrada e saída?

Para adicionar uma lista de países para chamadas de entrada ou saída, envie uma solicitação de serviço ao AMS.

Use o AMS SSP para provisionar o Amazon Data Firehose em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Data Firehose diretamente em sua conta gerenciada pelo AMS. O Firehose é a maneira mais fácil de carregar dados de streaming de forma confiável em lagos de dados, armazenamentos de dados e ferramentas de análise. Ele pode capturar, transformar e carregar dados de streaming no Amazon S3, Amazon Redshift, OpenSearch Amazon Service e Splunk, permitindo análises quase em tempo real com ferramentas e painéis de inteligência de negócios existentes que você já usa atualmente. É um serviço totalmente gerenciado que se expande automaticamente para corresponder à taxa de transferência de seus dados e não requer administração contínua. Ele também pode agrupar, compactar, transformar e criptografar os dados antes de carregá-los, minimizando a quantidade de armazenamento usada no destino e aumentando a segurança. Para saber mais, consulte O que é o Amazon Data Firehose?

Perguntas frequentes sobre Firehose in AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao Amazon Data Firehose na minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_kinesis_firehose_user_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Firehose na minha conta AMS?

Não há restrições. A funcionalidade completa do Amazon Data Firehose está disponível em sua conta AMS.

P: Quais são os pré-requisitos ou dependências para usar o Firehose na minha conta AMS?

Novas funções do IAM vinculadas ao serviço devem ser solicitadas para cada stream de entrega. Você também pode reutilizar uma única função vinculada ao serviço para todos os streams

atualizando a política de função com as permissões de recursos necessárias (incluindo buckets do S3/Chaves KMS/Funções Lambda/Streams do Kinesis).

Depois de enviar a RFC para adicionar o Firehose, um engenheiro de operações do AMS entrará em contato com você por meio de uma solicitação de serviço para ARNs os recursos que você gostaria de conectar ao Data Firehose (por exemplo AWS KMS, S3, Lambda e Kinesis Streams).

Use o AMS SSP para provisionar o Amazon DevOps Guru em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon DevOps Guru diretamente em sua conta gerenciada pelo AMS. O Amazon DevOps Guru é um serviço de operações totalmente gerenciado que facilita que desenvolvedores e operadores melhorem o desempenho e a disponibilidade de seus aplicativos. DevOpsO Guru permite que você descarregue as tarefas administrativas associadas à identificação de problemas operacionais para que você possa implementar rapidamente recomendações para melhorar seu aplicativo. DevOpsO Guru cria insights reativos que você pode usar para melhorar seu aplicativo agora. Ele também cria insights proativos para ajudá-lo a evitar problemas operacionais que possam afetar seu aplicativo no futuro. DevOpsO Guru aplica o aprendizado de máquina para analisar seus dados operacionais e métricas e eventos de aplicativos para identificar comportamentos que se desviam dos padrões operacionais normais. Você é notificado quando o DevOps Guru detecta um problema ou risco operacional. Para cada problema, o DevOps Guru apresenta recomendações inteligentes para abordar problemas operacionais atuais e futuros previstos.

Para saber mais, consulte O que é o Amazon DevOps Guru.

Perguntas frequentes sobre o Amazon DevOps Guru in AWS Managed Services

P: Como solicito acesso ao Amazon DevOps Guru na minha conta do AMS?

Para solicitar acesso, envie um tipo de alteração Gerenciamento | AWS Serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_devopsguru_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições para usar o Amazon DevOps Guru na minha conta AMS?

Não há restrições. A funcionalidade completa do Amazon DevOps Guru está disponível em sua conta do AMS.

P: Quais são os pré-requisitos ou dependências para usar o Amazon DevOps Guru na minha conta AMS?

Não há pré-requisitos. DevOpsO Guru utiliza os seguintes AWS serviços: Amazon CloudWatch Logs, RDS Insights,, AWS X-Ray, e. AWS Lambda AWS CloudTrail

Use o AMS SSP para provisionar o Amazon DocumentDB (com compatibilidade com o MongoDB) em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon DocumentDB (com compatibilidade com o MongoDB) diretamente na sua conta gerenciada do AMS. O Amazon DocumentDB (com compatibilidade com o MongoDB) é um serviço de banco de dados de documentos rápido, escalável, altamente disponível e totalmente gerenciado que oferece suporte às cargas de trabalho do MongoDB. O Amazon DocumentDB oferece o desempenho, a escalabilidade e a disponibilidade de que você precisa para operar cargas de trabalho essenciais do MongoDB em grande escala. O Amazon DocumentDB implementa a API MongoDB 3.6 de código aberto Apache 2.0 emulando as respostas que um cliente MongoDB espera de um servidor MongoDB, permitindo que você use seus drivers e ferramentas MongoDB existentes com o Amazon DocumentDB. No Amazon DocumentDB, o armazenamento e a computação são desacoplados, permitindo que cada um seja escalado de forma independente, e você pode aumentar a capacidade de leitura para milhões de solicitações por segundo adicionando até 15 réplicas de leitura de baixa latência, independentemente do tamanho dos seus dados. O Amazon DocumentDB foi projetado para oferecer disponibilidade de 99,99% e replica seis cópias dos seus dados em três AWS zonas de disponibilidade (). AZs Você pode usar o AWS Database Migration Service (DMS) gratuitamente (por seis meses) para migrar seus bancos de dados EC2 MongoDB locais ou do Amazon Elastic Compute Cloud (Amazon) para o Amazon DocumentDB sem praticamente nenhum tempo de inatividade. Para saber mais, consulte Amazon DocumentDB (com compatibilidade com o MongoDB).

Perguntas frequentes sobre o Amazon DocumentDB no AWS Managed Services

P: Como solicito acesso ao Amazon DocumentDB na minha conta AMS?

As funções de console e acesso a dados do Amazon DocumentDB podem ser solicitadas por meio do envio de dois AMS RFCs, acesso ao console e acesso a dados:

Solicite acesso ao Amazon DocumentDB enviando uma RFC com o tipo de alteração Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC provisiona a seguinte

função do IAM para sua conta:`customer_documentdb_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Amazon DocumentDB na minha conta AMS?

O Amazon DocumentDB exige permissões específicas do Amazon RDS. Como o AMS gerencia totalmente o Amazon RDS, a função do IAM para o Amazon DocumentDB inclui algumas restrições às ações no Amazon RDS. As seguintes restrições são aplicáveis:

- O acesso ao `DeleteDBInstance` e `DeleteDBCluster` APIs foi restrito. Para usar essas exclusões APIs, envie um RFC com os componentes Management | Advanced stack | Identity and Access Management (IAM) | Atualizar entidade ou política (revisão necessária) do tipo de alteração (ct-27tuth19k52b4).
- Você não pode adicionar ou remover tags das instâncias do Amazon RDS.
- Você não pode tornar pública sua instância do Amazon DocumentDB.

P: Quais são os pré-requisitos ou dependências para usar o Amazon DocumentDB na minha conta AMS?

O Amazon S3 e AWS KMS são necessários para usar o Amazon DocumentDB, se os buckets do Amazon S3 estiverem criptografados com chaves. AWS KMS

Use o AMS SSP para provisionar o Amazon DynamoDB em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon DynamoDB (DynamoDB) diretamente na sua conta gerenciada do AMS. O Amazon DynamoDB é um banco de dados de valores e documentos essenciais que oferece desempenho de um dígito em milissegundos em qualquer escala. É um banco de dados totalmente gerenciado, multirregional e multiativo com segurança, backup e restauração integrados e armazenamento em cache na memória para aplicativos de escala da Internet. Para saber mais, consulte Amazon DynamoDB.

O Amazon DynamoDB Accelerator (DAX) é um serviço de armazenamento em cache por gravação simultânea (write-through) projetado para simplificar o processo de adição de um cache a tabelas do DynamoDB. O DAX foi projetado para aplicações que exigem leituras de alta performance.

Perguntas frequentes sobre o DynamoDB no AWS Managed Services

P: Como solicito acesso ao DynamoDB e ao DAX na minha conta AMS?

Solicite acesso ao DynamoDB e ao DAX enviando uma RFC com o tipo de alteração Management AWS | service | Self-provisioned service | Add (ct-1w8z66n899dct). Essa RFC provisiona as seguintes funções e políticas do IAM para sua conta:

- Nome da função do DynamoDB: `customer_dynamodb_role`

  Nome da função de serviço DAX: `customer_dax_service_role`
- Nome da política do DynamoDB: `customer_dynamodb_policy`

  Política de serviço do DAX: `customer_dax_service_policy`

Depois de provisionado em sua conta, você deve integrá-lo à `customer_dynamodb_role` sua solução de federação.

P: Quais são as restrições ao uso do DynamoDB na minha conta do AMS?

Todas as funcionalidades do DynamoDB são suportadas, incluindo o DynamoDB Accelerator (DAX).

Ao criar alarmes para qualquer tabela, o nome do alarme deve ser prefixado com “cliente*”; por exemplo,. `customer-employee-table-high-put-latency`

Ao criar um tópico do Amazon SNS para o DynamoDB, ele deve ser nomeado:. `dynamodb`

Para excluir o tópico do Amazon SNS criado pelo DynamoDB, envie um RFC do tipo de alteração Management | Other | Other | Update.

P: Quais são os pré-requisitos ou dependências para usar o DynamoDB na minha conta do AMS?

Não há pré-requisitos ou dependências para usar o DynamoDB em sua conta do AMS.

Use o AMS SSP para provisionar o Amazon Elastic Container Registry em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Elastic Container Registry (Amazon ECR) diretamente na sua conta gerenciada do AMS. O Amazon Elastic Container Registry é um registro de contêineres Docker totalmente gerenciado que facilita para os desenvolvedores armazenar, gerenciar e implantar imagens de contêineres do Docker. O Amazon ECR é integrado ao Amazon Elastic Container Service (Amazon ECS), simplificando seu fluxo de trabalho de desenvolvimento para produção. O Amazon ECR elimina a necessidade de operar

seus próprios repositórios de contêineres ou a preocupação com a escalabilidade da infraestrutura subjacente. O Amazon ECS hospeda suas imagens em uma arquitetura altamente disponível e escalável, permitindo que você implante contêineres de forma confiável para seus aplicativos. A integração com AWS Identity and Access Management (IAM) fornece controle em nível de recursos de cada repositório. Com o Amazon ECR, não há taxas ou compromissos iniciais. Você paga somente pela quantidade de dados que armazena em seus repositórios e pelos dados transferidos para a Internet.

Para saber mais, consulte Amazon Elastic Container Registry.

Perguntas frequentes sobre o Amazon Elastic Container Registry no AWS Managed Services

P: Como solicito acesso ao Amazon ECR na minha conta AMS?

Solicite acesso ao Amazon ECR enviando uma RFC com o tipo de alteração Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Essa RFC provisiona as seguintes funções do IAM para sua conta: `customer_ecr_console_role`, e `customer_ecr_poweruser_instance_profile` com as políticas do IAM associadas, `customer_ecr_console_policy` `ecustomer_ecr_poweruser_instance_profile_policy`, respectivamente. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Amazon ECR na minha conta AMS?

Há restrições em relação aos namespaces do AMS para o uso do Amazon ECR em sua conta do AMS. As imagens do contêiner não podem ter o prefixo “AMS-” ou “Sentinel-”.

P: Quais são os pré-requisitos ou dependências para usar o Amazon ECR na minha conta AMS?

Não há pré-requisitos ou dependências para usar o Amazon ECR em sua conta AMS.

Use o AMS SSP para provisionar o EC2 Image Builder em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Image Builder EC2 diretamente na sua conta gerenciada pelo AMS. EC2 O Image Builder é um AWS serviço totalmente gerenciado que facilita a automatização da criação, do gerenciamento e da implantação de imagens de servidor personalizadas, seguras e up-to-date “douradas”, pré-instaladas e pré-configuradas com software e configurações para atender a padrões específicos de TI.

Você pode usar Console de gerenciamento da AWS a AWS CLI ou APIs criar imagens personalizadas em sua AWS conta. Quando você usa o Console de gerenciamento da AWS, o assistente do Amazon EC2 Image Builder orienta você pelas etapas para:

- Forneça artefatos iniciais
- Adicionar e remover software
- Personalizar configurações e scripts
- Executar os testes selecionados
- Distribua imagens para AWS regiões

As imagens que você cria são criadas em sua conta e podem ser configuradas continuamente para patches do sistema operacional. Para saber mais, consulte EC2 Image Builder.

EC2 Perguntas frequentes sobre o Image Builder no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao EC2 Image Builder na minha conta AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Por meio deste RFC, a seguinte função do IAM será provisionada em sua conta:. `customer_ec2_imagebuilder_role` Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições do EC2 Image Builder?

O AMS não suporta o uso de padrões de serviço para configuração de infraestrutura. Você pode criar uma nova configuração de infraestrutura ou usar uma existente.

Atualmente, o AMS não oferece suporte à criação de receitas de contêineres.

P: Quais são os pré-requisitos ou dependências para habilitar o Image Builder? EC2

- EC2 Função vinculada ao serviço do Image Builder: você não precisa criar manualmente uma função vinculada ao serviço. Quando você cria seu primeiro recurso do Image Builder no Console de gerenciamento da AWS, na AWS CLI ou na AWS API, o Image Builder cria a função vinculada ao serviço para você.

- As instâncias usadas para criar imagens e executar testes usando o Image Builder devem ter acesso ao serviço Systems Manager. O Agente SSM será instalado na imagem de origem, se ainda não estiver presente, e será removido antes da criação da imagem.
- AWS IAM: a função do IAM que você associa ao seu perfil de instância precisa ter permissões para executar os componentes de criação e teste incluídos na sua imagem. As seguintes políticas de função do IAM devem ser anexadas à função do IAM associada aos perfis da instância: `EC2InstanceProfileForImageBuilder` `AmazonSSMManagedInstanceCore` e. O nome da função do IAM deve conter a `*imagebuilder*` palavra-chave.
- Se você configurar o registro em log, o perfil de instância especificado na configuração da sua infraestrutura deverá ter `s3:PutObject` permissões para o bucket de destino (`arn:aws:s3:::{bucket-name}/*`). Por exemplo:

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::{bucket-name}/*"
        }
    ]
}
```

- Crie um tópico do SNS com o nome 'imagebuilder' para receber alertas e notificações do Image Builder EC2 .

Use o AMS SSP para provisionar o Amazon ECS AWS Fargate em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Fargate recursos do Amazon ECS diretamente em sua conta gerenciada pelo AMS. AWS Fargate é uma tecnologia que você pode usar com o Amazon ECS para executar contêineres (consulte Contêineres ativados AWS) sem precisar gerenciar servidores ou clusters de EC2 instâncias da Amazon. Com AWS Fargate isso, você não precisa mais provisionar, configurar ou escalar clusters de máquinas virtuais para

executar contêineres. Isso elimina a necessidade de escolher tipos de servidor, decidir quando dimensionar clusters ou otimizar o agrupamento de clusters.

Para saber mais, consulte Amazon ECS on AWS Fargate.

Perguntas frequentes sobre o Amazon ECS on Fargate no AWS Managed Services

P: Como solicito acesso ao Amazon ECS no Fargate na minha conta AMS?

Solicite acesso ao Amazon ECS no Fargate enviando uma RFC com o tipo de alteração Management AWS | service | Self-provisioned service | Add (ct-1w8z66n899dct). Essa RFC provisiona as seguintes funções do IAM para sua conta: `customer_ecs_fargate_console_role` (se nenhuma função do IAM existente for fornecida para associar a política do ECS),`customer_ecs_fargate_events_service_role`, `customer_ecs_task_execution_service_rolecustomer_ecs_codedeploy_service_role`, e. `AWSServiceRoleForApplicationAutoScaling_ECSService` Depois de provisionado em sua conta, você deve integrar as funções em sua solução de federação.

P: Quais são as restrições para usar o Amazon ECS no Fargate na minha conta AMS?

- O monitoramento e o registro de tarefas do Amazon ECS são considerados de sua responsabilidade, pois as atividades em nível de contêiner ocorrem acima do hipervisor, e os recursos de registro são limitados pelo Amazon ECS no Fargate. Como usuário do Amazon ECS no Fargate, recomendamos que você tome as medidas necessárias para habilitar o registro em suas tarefas do Amazon ECS. Para obter mais informações, consulte Habilitando o driver de log awslogs para seus contêineres.
- A segurança e a proteção contra malware no nível do contêiner também são consideradas de sua responsabilidade. O Amazon ECS no Fargate não inclui o Trend Micro nem componentes de segurança de rede pré-configurados.
- Esse serviço está disponível para contas AMS com várias contas na zona de pouso e na zona de pouso com uma única conta.
- O Amazon ECS Service Discovery é restrito por padrão na função autoprovisionada, pois são necessárias permissões elevadas para criar zonas hospedadas privadas do Route 53. Para habilitar o Service Discovery em um serviço, envie um tipo de alteração Management | Other | Other | Update. Para fornecer as informações necessárias para habilitar o Service Discovery para seu Amazon ECS Service, consulte o manual Service Discovery.
- Atualmente, o AMS não gerencia nem restringe imagens usadas para implantação em contêineres no Amazon ECS Fargate. Você poderá implantar imagens do Amazon ECR, do Docker Hub ou de

qualquer outro repositório privado de imagens. Portanto, aconselhamos que imagens públicas ou quaisquer imagens não seguras não sejam implantadas, pois elas podem resultar em atividades maliciosas na conta.

P: Quais são os pré-requisitos ou dependências para usar o Amazon ECS no Fargate na minha conta AMS?

- A seguir estão as dependências do Amazon ECS no Fargate; no entanto, nenhuma ação adicional é necessária para habilitar esses serviços com sua função autoprovisionada:
  - CloudWatch troncos
  - CloudWatch eventos
  - CloudWatch alarmes
  - CodeDeploy
  - App Mesh
  - Cloud Map
  - Route 53
- Dependendo do seu caso de uso, a seguir estão os recursos dos quais o Amazon ECS depende e pode exigir antes de usar o Amazon ECS no Fargate em sua conta:
  - Grupo de segurança a ser usado com o serviço Amazon ECS. Você pode usar Deployment | Advanced stack components | Security Group | Create (auto) (ct-3pc215bnwb6p7) ou, se seu grupo de segurança exigir regras especiais, usar Deployment | Advanced stack components | Security Group | Create (revisão obrigatória) (ct-1oxx2g2d7hc90). Nota: O grupo de segurança selecionado com o Amazon ECS deve ser criado especificamente para o Amazon ECS, onde o serviço ou cluster do Amazon ECS reside. Você pode aprender mais na seção Grupo de segurança em Configuração com o Amazon ECS e Segurança no Amazon Elastic Container Service.
  - Balanceador de carga de aplicativos (ALB), balanceador de carga de rede (NLB), balanceador de carga clássico (ELB) para balanceamento de carga entre tarefas.
  - Grupos-alvo para ALBs.
  - Recursos de malha de aplicativos (por exemplo, roteadores virtuais, serviços virtuais, nós virtuais) para integração com seu cluster Amazon ECS.
- Atualmente, não há como o AMS mitigar automaticamente o risco associado ao suporte às permissões dos grupos de segurança quando criado fora dos tipos de alteração padrão do AMS. Recomendamos que você solicite um grupo de segurança específico para uso com seu cluster

Fargate para limitar a possibilidade de usar um grupo de segurança não designado para uso com o Amazon ECS.

Use o AMS SSP para provisionar o Amazon EKS AWS Fargate em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Fargate recursos do Amazon EKS diretamente em sua conta gerenciada pelo AMS. AWS Fargate é uma tecnologia que fornece capacidade computacional sob demanda e do tamanho certo para contêineres (para entender os contêineres, consulte O que são contêineres?). Com AWS Fargate isso, você não precisa mais provisionar, configurar ou escalar grupos de máquinas virtuais para executar contêineres. Isso elimina a necessidade de escolher tipos de servidor, de decidir quando dimensionar os grupos de nós ou de otimizar o pacote de clusters.

O Amazon Elastic Kubernetes Service (Amazon EKS) integra o AWS Fargate Kubernetes usando controladores AWS criados usando o modelo upstream e extensível fornecido pelo Kubernetes. Esses controladores são executados como parte do plano de controle Kubernetes gerenciado pelo Amazon EKS e são responsáveis por programar pods nativos do Kubernetes no Fargate. Os controladores do Fargate incluem um novo agendador que é executado com o agendador do Kubernetes, além de vários controladores de admissão de mutação e de validação. Ao iniciar um pod que atende aos critérios de execução no Fargate, os controladores do Fargate em execução no cluster reconhecem, atualizam e agendam o pod no Fargate.

Para saber mais, consulte Amazon EKS on AWS Fargate Now Generally Available e o Guia de melhores práticas de segurança do Amazon EKS (inclui “Recomendações”, como “Revisar e revogar acesso anônimo desnecessário” e muito mais).

> **Tip**
>
> O AMS tem um tipo de alteração, Deployment | Advanced stack components | Identity and Access Management (IAM) | Create OpenID Connect provider (ct-30ecvfi3tq4k3), que você pode usar com o Amazon EKS. Para ver um exemplo, consulte Identity and Access Management (IAM) | Create OpenID Connect Provider.

Perguntas frequentes sobre o Amazon EKS on AWS Fargate in AWS Managed Services

P: Como solicito acesso ao Amazon EKS no Fargate na minha conta AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Essa RFC provisiona a seguinte função do IAM para sua conta.

- `customer_eks_fargate_console_role`.

  Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.
- Essas funções de serviço dão ao Amazon EKS on Fargate permissão para ligar para outros AWS serviços em seu nome:
  - `customer_eks_pod_execution_role`
  - `customer_eks_cluster_service_role`

P: Quais são as restrições para usar o Amazon EKS no Fargate na minha conta AMS?

- A criação de EC2 grupos de nós gerenciados ou autogerenciados não é suportada no AMS. Se você precisar usar nós de EC2 trabalho, entre em contato com seu AMS Cloud Service Delivery Manager (CSDM) ou Cloud Architect (CA).
- O AMS não inclui o Trend Micro nem componentes de segurança de rede pré-configurados para imagens de contêineres. Espera-se que você gerencie seus próprios serviços de digitalização de imagens para detectar imagens de contêineres maliciosas antes da implantação.
- O EKSCTL não é suportado devido a CloudFormation interdependências.
- Durante a criação do cluster, você tem permissões para desativar o registro do plano de controle do cluster. Para obter mais informações, consulte Registro em log do ambiente de gerenciamento do Amazon EKS. Recomendamos que você ative todos os registros importantes de API, autenticação e auditoria na criação do cluster.
- Durante a criação do cluster, o acesso ao endpoint do cluster para clusters do Amazon EKS é padronizado como público; para obter mais informações, consulte Controle de acesso ao endpoint do cluster do Amazon EKS. Recomendamos que os endpoints do Amazon EKS sejam definidos como privados. Se os endpoints forem necessários para acesso público, é uma prática recomendada defini-los como públicos somente para intervalos CIDR específicos.

- O AMS não tem um método para forçar e restringir imagens usadas para implantação em contêineres no Amazon EKS Fargate. Você pode implantar imagens do Amazon ECR, do Docker Hub ou de qualquer outro repositório privado de imagens. Portanto, existe o risco de implantar uma imagem pública que possa realizar atividades maliciosas na conta.
- A implantação de clusters EKS por meio do kit de desenvolvimento em nuvem (CDK) ou do CloudFormation Ingest não é suportada no AMS.
- Você deve criar o grupo de segurança necessário usando ct-3pc215bnwb6p7 Deployment | Advanced stack components | Security group | Create e referencie no arquivo manifesto para criação de entrada. Isso ocorre porque a função `customer-eks-alb-ingress-controller-role` não está autorizada a criar grupos de segurança.

P: Quais são os pré-requisitos ou dependências para usar o Amazon EKS no Fargate na minha conta AMS?

Para usar o serviço, as seguintes dependências devem ser configuradas:

- Para fazer a autenticação no serviço, tanto o KUBECTL quanto o KUBECTL aws-iam-authenticator devem estar instalados; para obter mais informações, consulte Gerenciando a autenticação de cluster.
- O Kubernetes se baseia em um conceito chamado “contas de serviço”. Para utilizar a funcionalidade de contas de serviço dentro de um cluster kubernetes no EKS, é necessário um RFC de gerenciamento | Outro | Outro | Atualizar com as seguintes entradas:
  - [Obrigatório] Nome do cluster Amazon EKS
  - [Obrigatório] Namespace do Amazon EKS Cluster em que a conta de serviço (SA) será implantada.
  - [Obrigatório] Nome do Amazon EKS Cluster SA.
  - [Obrigatório] Nome da política do IAM e permissions/document a ser associada.
  - [Obrigatório] O nome da função do IAM está sendo solicitado.
  - [Opcional] URL do provedor do OpenID Connect. Para obter mais informações, consulte
    - Habilitando funções do IAM para contas de serviço em seu cluster
    - Apresentando funções refinadas do IAM para contas de serviço
- Recomendamos que as regras de Config sejam configuradas e monitoradas para
  - Endpoints de cluster público
  - Registro de API desativado

É sua responsabilidade monitorar e corrigir essas regras do Config.

Se você quiser implantar um controlador ALB Ingress, envie um RFC Management | Other | Other Update para provisionar a função IAM necessária para ser usada com o pod do ALB Ingress Controller. As seguintes entradas são necessárias para criar recursos do IAM a serem associados ao ALB Ingress Controller (inclua-os com sua RFC):

- [Obrigatório] Nome do cluster Amazon EKS
- [Opcional] URL do provedor do OpenID Connect
- [Opcional] Namespace do Amazon EKS Cluster em que o serviço de controlador de entrada do Application Load Balancer (ALB) será implantado. [padrão: kube-system]
- [Opcional] Nome da conta de serviço (SA) do Amazon EKS Cluster. [padrão: aws-load-balancer-controller]

Se você quiser habilitar a criptografia de segredos de envelope em seu cluster (o que recomendamos), forneça a chave KMS que IDs você pretende usar no campo de descrição da RFC para adicionar o serviço (Gerenciamento | serviço | Serviço autoprovisionado | AWS Adicionar (ct-1w8z66n899dct). Para saber mais sobre criptografia de envelope, consulte Amazon EKS adiciona criptografia de envelope para segredos com o AWS KMS.

Use o AMS SSP para provisionar o Amazon EMR em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon EMR diretamente em sua conta gerenciada pelo AMS. O Amazon EMR é a plataforma de big data na nuvem líder do setor para processar grandes quantidades de dados usando ferramentas de código aberto, como Apache Spark, Apache Hive, Apache, Apache Flink, Apache Hudi e HBase Presto. Com o Amazon EMR, você pode executar análises em escala de petabytes por menos da metade do custo das soluções locais tradicionais e mais de 3 vezes mais rápido do que o Apache Spark padrão. Para trabalhos de curta duração, você pode ativar e desativar clusters e pagar por segundo pelas instâncias usadas. Para cargas de trabalho de longa duração, você pode criar clusters altamente disponíveis que se escalam automaticamente para atender à demanda.

Você pode criar uma ou mais instâncias dos clusters do Amazon EMR em contas AMS com várias contas de landing zone ou em contas de landing zone de conta única para suportar clusters transitórios e persistentes do Amazon EMR. Você também pode habilitar a autenticação Kerberos para habilitar a autenticação de usuários do domínio local do Active Directory.

Você pode aproveitar vários armazenamentos de dados com os clusters do Amazon EMR para oferecer suporte a ferramentas e bibliotecas Hadoop específicas para cada caso de uso. Os clusters do Amazon EMR podem ser criados usando OnDemand ou instâncias spot e configurar o escalonamento automático para gerenciar a capacidade e reduzir o custo.

Os arquivos de log do cluster podem ser arquivados em um bucket do Amazon S3 para registro e depuração. Você também pode acessar as interfaces web hospedadas no cluster do Amazon EMR para atender aos requisitos de administração do hadoop ou às experiências de cadernos de notas dos clientes.

Para saber mais, consulte Amazon EMR.

Perguntas frequentes sobre o Amazon EMR no AWS Managed Services

P: Como solicito acesso ao Amazon EMR na minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Essa RFC provisiona as seguintes funções do IAM para sua conta:

- `customer_emr_cluster_instance_profile`
- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

Depois de provisionado em sua conta, você deve integrar o customer_emr_console_role em sua solução de federação.

P: Quais são as restrições ao uso do Amazon EMR na minha conta AMS?

Ao criar o Amazon EMR em um EC2 cluster a partir do console da AWS, recomendamos que você use a opção Create Cluster — Advanced. Os clusters do Amazon EMR devem ser criados adicionando a tag com a chave "for-use-with-amazon-emr-managed-policies" com o valor “true”. Selecione as seguintes configurações nas opções de Segurança:

- Selecione funções personalizadas para seu cluster:
  - Função do EMR: customer_emr_cluster_service_role
  - EC2 Perfil da instância: customer_emr_cluster_instance_profile

  - Função de Auto Scaling: customer_emr_cluster_autoscaling_role
- EC2 Grupos de segurança:
  - Mestre: ams-emr-master-security -group
  - Núcleo e tarefa: ams-emr-worker-security -grupo
  - Acesso ao serviço: ams-emr-serviceaccess-security -group

P: Quais são os pré-requisitos ou dependências para usar o Amazon EMR na minha conta AMS?

O AMS cria grupos de segurança padrão para os nós mestre, trabalhador e serviços do Amazon EMR.

Os modelos de lançamento e os grupos de segurança a serem usados com os clusters do Amazon EMR devem ter a chave de tag "for-use-with-amazon-emr-managed-policies" com o valor “true”.

O perfil padrão da instância de cluster do Amazon EMR permite o acesso aos recursos, como buckets s3 e tabelas dynamodb, com seus nomes contendo “emr”. Você pode solicitar políticas adicionais do IAM para usar quaisquer recursos adicionais a serem usados com o Amazon EMR. Os seguintes ARNs de recursos podem ser usados com trabalhos do Amazon EMR usando o customer_emr_cluster_instance_profile:

- arn:aws:dynamodb: *:*:table/*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: *:*:domínio: *emr*
- arn:aws:3: ::*emr*

Se a autenticação kerberos for necessária para o cluster do Amazon EMR:

- Forneça o nome do território a ser usado para cada cluster kerberizado do Amazon EMR e os endereços IP locais do Active Directory.
- Requisitos de infraestrutura:

  Multi-Account Landing Zone (MALZ): envie uma RFC para criar uma nova conta de aplicativo gerenciado ou uma nova VPC em uma conta de aplicativo existente.

Zona de destino de conta única (SALZ): envie uma RFC para criar uma nova sub-rede em sua VPC.

- Configure a confiança de entrada para o território do cluster no Active Directory local.
- Envie um RFC para configurar zonas DNS para o território no AD gerenciado.
- Configuração do reino:

  MALZ: Envie um RFC de gerenciamento | Outro | Outro | Atualize (ct-0xdawir96cy7k) para atualizar o conjunto de opções DHCP da VPC para usar o nome do território como sufixo do nome de domínio.

  SALZ: Envie um RFC de gerenciamento | Outro | Outro | Atualize (ct-0xdawir96cy7k) para gerar uma nova AMI do Amazon EMR para usar a região específica para o sufixo do nome de domínio.

Para implantar o Amazon EMR Studio, a função `customer_emr_cluster_service_role` tem um pré-requisito para um bucket do Amazon Simple Storage Service. Para criar o bucket, use a CT automatizada `ct-1a68ck03fn98r` (Implantação | Componentes avançados de pilha | Armazenamento S3 | Criar). Quando você usa essa CT automatizada para criar um bucket do Amazon S3 para o Amazon EMR, o nome do bucket deve começar com o prefixo. `customer-emr-*` Além disso, você deve criar o bucket na mesma AWS região do cluster do Amazon EMR.

Use o AMS SSP para provisionar a Amazon EventBridge em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os EventBridge recursos da Amazon diretamente em sua conta gerenciada pelo AMS. EventBridge A Amazon é um serviço de ônibus de eventos sem servidor que facilita a conexão de seus aplicativos com dados de várias fontes. EventBridge fornece um fluxo de dados em tempo real de seus próprios aplicativos, aplicativos Software-as-a-Service (SaaS) e AWS serviços e encaminha esses dados para destinos como. AWS Lambda Você pode configurar regras de roteamento para determinar para onde enviar seus dados a fim de criar arquiteturas de aplicativos que reagem em tempo real a todas as suas fontes de dados. O EventBridge permite que você crie arquiteturas orientadas a eventos, que são livremente acopladas e distribuídas.

Para saber mais, consulte Amazon EventBridge.

EventBridge perguntas frequentes sobre o AWS Managed Services

P: Como faço para solicitar acesso à EventBridge minha conta do AMS?

Solicite acesso ao EventBridge enviando uma RFC com o serviço Management | AWS | Self-provisioned service | Adicionar (ct-1w8z66n899dct) tipo de alteração. Essa RFC provisiona as seguintes funções do IAM para sua conta: `customer_eventbridge_role` e. `customer_eventbridge_scheduler_execution_role` Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

A função de execução `customer_eventbridge_scheduler_execution_role` é uma função do IAM que o EventBridge Scheduler assume para interagir com outras pessoas Serviços da AWS em seu nome. As políticas de permissão anexadas a essa função concedem ao EventBridge Agendador acesso para invocar alvos.

> **Note**
>
> Por padrão, o EventBridge Scheduler usa chaves AWS próprias EventBridge para criptografar os dados. Para usar uma chave gerenciada pelo cliente EventBridge para criptografar os dados, envie a RFC usando o serviço Gerenciamento | AWS | Serviço autoprovisionado | Adicione (revisão obrigatória) tipo de alteração (ct-3qe6io8t6jtny) para provisionamento de serviços.

P: Quais são as restrições de uso EventBridge na minha conta AMS?

Você deve enviar o AMS RFCs e criar os seguintes recursos: funções de serviço para acionar o trabalho em lotes, fila SQS, CodeBuild CodePipeline, e comandos SSM.

P: Quais são os pré-requisitos ou dependências para usar EventBridge na minha conta do AMS?

Você deve solicitar uma função de EventBridge serviço com uma RFC usando os componentes Deployment | Advanced stack | Identity and Access Management (IAM) | Crie o tipo de alteração de entidade ou política (revisão necessária) (ct-3dpd8mdd9jn1r) antes de usar para acionar outros recursos EventBridge, como AWS Lambda, Amazon SNS, Amazon SQS ou Amazon Logs. AWS Batch CloudWatch Especifique os serviços a serem invocados ao solicitar sua função de serviço. Para saber mais sobre as permissões necessárias para invocar alvos, consulte Usando políticas baseadas em recursos para. EventBridge

EventBridge é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um AWS service (Serviço da AWS) usuário EventBridge. CloudTrail deve estar habilitado e autorizado a armazenar os arquivos de log nos buckets do S3. Nota: Todas as contas do AMS foram CloudTrail ativadas, portanto, nenhuma ação é necessária.

P: A função customer_eventbridge_scheduler_execution_role tem um pré-requisito para uma chave (opcional, se usada para criptografia). AWS Key Management Service Como adoto a criptografia de dados AWS KMS CMKs em repouso/trânsito?

Por padrão, o EventBridge Scheduler criptografa metadados de eventos e dados de mensagens que ele armazena sob uma chave AWS própria (criptografia em repouso). EventBridge O Scheduler também criptografa os dados que passam entre o EventBridge Scheduler e outros serviços usando o Transport Layer Security (TLS) (criptografia em trânsito).

Se seu caso de uso específico exigir que você controle e audite as chaves de criptografia que protegem seus dados no EventBridge Scheduler, você pode usar uma chave gerenciada pelo cliente.

Você deve solicitar um RFC usando o serviço Management | AWS service (Serviço da AWS) | Autoprovisionado | Adicionar (revisão obrigatória) do tipo de alteração antes de usar a Amazon EventBridge para integrar a permissão. AWS KMS

Use o AMS SSP para provisionar o Amazon Forecast em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Forecast (Forecast) diretamente em sua conta gerenciada pelo AMS. O Amazon Forecast é um serviço totalmente gerenciado que usa aprendizado de máquina para fornecer previsões altamente precisas.

> **Note**
>
> AWS fechou o acesso de novos clientes ao Amazon Forecast, a partir de 29 de julho de 2024. Os clientes existentes do Amazon Forecast podem continuar usando o serviço normalmente. AWS continua investindo em melhorias de segurança, disponibilidade e desempenho do Amazon Forecast, mas AWS não planeja introduzir novos recursos.
> Se você quiser usar o Amazon Forecast, entre em contato com seu CSDM para que eles possam orientá-lo mais sobre como fazer a transição do uso do Amazon Forecast para o Amazon SageMaker Canvas.

Com base na mesma tecnologia usada na Amazon.com, a Forecast usa aprendizado de máquina para combinar dados de séries temporais com variáveis adicionais para criar previsões. O Forecast não requer experiência em aprendizado de máquina para começar. Você só precisa fornecer dados históricos, além de quaisquer dados adicionais que você acredite que possam afetar suas previsões. Por exemplo, a demanda por uma cor específica de uma camisa pode mudar com as estações do ano e a localização da loja. Essa relação complexa é difícil de determinar sozinha, mas o aprendizado de máquina é ideal para reconhecê-la. Depois de fornecer seus dados, o Forecast os examinará automaticamente, identificará o que é significativo e produzirá um modelo de previsão capaz de fazer previsões até 50% mais precisas do que analisar apenas dados de séries temporais.

Para saber mais, consulte Amazon Forecast.

Perguntas frequentes sobre o Amazon Forecast in AWS Managed Services

P: Como solicito acesso ao Forecast na minha conta do AMS?

Solicite acesso AWS Firewall Manager enviando um RFC com o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_forecast_admin_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Forecast na minha conta do AMS?

O acesso padrão ao bucket do S3 só permite que você acesse buckets com o padrão de nomenclatura 'customer-forecast-*'. Se você tiver sua própria convenção de nomenclatura para intervalos de dados, discuta a nomenclatura do intervalo e a configuração do acesso relacionado com seu Cloud Architect (CA). Por exemplo:

- Você pode definir sua função específica do serviço Amazon Forecast com nomes como 'AmazonForecast- ExecutionRole -*' e o acesso adequado associado ao bucket do S3. Veja a função do serviço - AmazonForecast-ExecutionRole-Admin e a política do IAM - customer_forecast_default_s3_access_policy, no console do IAM.
- Talvez seja necessário associar o acesso relacionado aos buckets do S3 à função de federação do IAM. Veja a política do IAM - customer_forecast_default_s3_access_policy, no console do IAM.

P: Quais são os pré-requisitos ou dependências para usar o Forecast na minha conta do AMS?

- Os buckets apropriados do Amazon S3 devem ser criados antes de usar o Forecast. Especialmente, o acesso padrão aos buckets do S3 é com o padrão de nomenclatura 'customer-forecast-*'
- Se você quiser usar padrões de nomenclatura em buckets do S3 diferentes de 'customer-forecast-*', você deve criar uma nova função de serviço com permissões de acesso do S3 nos buckets:
  1. Uma nova função de serviço a ser criada com o nome 'AmazonForecast- ExecutionRole -{suffix}'.
  2. Uma nova política do IAM a ser criada, semelhante à customer_forecast_default_s3_access_policy e associada à nova função de serviço e à função de administrador da federação relacionada (por exemplo, 'customer_forecast_admin_role')

P: Como posso melhorar a segurança dos dados ao usar o Amazon Forecast?

- Para criptografia de dados em repouso, você pode usar AWS KMS para provisionar uma CMK gerenciada pelo cliente para proteger o armazenamento de dados no serviço Amazon S3:
  - Ative a criptografia padrão no bucket com a chave de provisão e configure a política do bucket para aceitar a criptografia de AWS KMS dados ao colocar dados.
  - Ative a função do serviço Amazon Forecast 'AmazonForecast- ExecutionRole -*' e a função de administrador da federação (por exemplo,' customer_forecast_admin_role ') como o usuário principal. AWS KMS
- Para criptografia de dados em trânsito, você pode configurar o protocolo HTTPS, que é necessário durante a transferência de objetos na política de bucket do Amazon S3.
- Restrições adicionais ao controle de acesso permitem uma política de bucket para acesso aprovado para a função de serviço 'AmazonForecast- ExecutionRole -*' do Amazon Forecast e a função de administrador (por exemplo,' customer_forecast_admin_role ').

P: Quais são as melhores práticas ao usar o Amazon Forecast?

- Você deve ter um bom entendimento de suas práticas de classificação de dados e mapear as necessidades de segurança de dados relacionadas ao usar buckets S3 com o Amazon Forecast.
- Para a configuração do bucket do Amazon S3, recomendamos fortemente que você habilite a imposição de HTTPS em sua política de bucket do S3.
- Você deve estar ciente de que a função de administrador 'customer_forecast_admin_role' suporta acesso permissivo (objetos do S3) nos buckets do Amazon Get/Delete/Put S3 com o nome de

'customer-forecast-*'. OBSERVAÇÃO: Se você precisar de um controle de acesso refinado para várias equipes, siga estas práticas:

- Defina sua identidade IAM de acesso baseada em equipe (função/usuário) com o menor privilégio de acesso aos buckets Amazon S3 relacionados.
- Crie team/project com base na AWS KMS CMKs concessão de acesso adequado às identidades do IAM correspondentes. (acesso do usuário e 'AmazonForecast- ExecutionRole - {equipe/projeto}'.
- Configure a criptografia padrão do bucket S3 com o criado AWS KMS CMKs.
- Aplique os tráfegos da API do S3 com o protocolo HTTPS na política de bucket do S3.
- Aplique a configuração do bucket do S3 para acesso aprovado às identidades do IAM relacionadas (acesso do usuário e 'AmazonForecast- ExecutionRole - {team/project}' aos buckets.

- Se você quiser usar o 'customer_forecast_admin_role' para fins gerais, considere os pontos listados anteriormente para proteger os buckets do S3.

P: Onde estão as informações de conformidade sobre o Amazon Forecast?

Veja o Programa de Conformidade de AWS serviços.

Use o AMS SSP para provisionar a Amazon FSx em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os FSx recursos da Amazon diretamente em sua conta gerenciada pelo AMS. A Amazon FSx fornece sistemas de arquivos de terceiros totalmente gerenciados. A Amazon FSx oferece a compatibilidade nativa de sistemas de arquivos de terceiros com conjuntos de recursos para cargas de trabalho, como armazenamento baseado em Windows, computação de alto desempenho (HPC), aprendizado de máquina e automação eletrônica de design (EDA). A Amazon FSx automatiza as tarefas administrativas demoradas, como provisionamento de hardware, configuração de software, aplicação de patches e backups. A Amazon FSx integra os sistemas de arquivos aos AWS serviços nativos da nuvem, tornando-os ainda mais úteis para um conjunto mais amplo de cargas de trabalho.

FSx A Amazon oferece dois sistemas de arquivos para você escolher: Amazon para Windows File Server FSx para aplicativos baseados em Windows e Amazon for Lustre para cargas de trabalho com uso FSx intensivo de computação. Para saber mais, consulte Amazon FSx.

Perguntas frequentes sobre a Amazon FSx in AWS Managed Services

P: Como solicito acesso à Amazon FSx na minha conta do AMS?

Solicite acesso à Amazon FSx enviando uma RFC com o serviço Management | AWS | Self-provisioned service | Add (ct-1w8z66n899dct) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_fsx_admin_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições para usar a Amazon FSx na minha conta do AMS?

Não há restrições. A funcionalidade completa do serviço está disponível.

P: Quais são os pré-requisitos ou dependências para usar a Amazon FSx na minha conta do AMS?

Não há pré-requisitos. No entanto, para configurações avançadas como Multi-AZ, você deve instalar e gerenciar os serviços de Replicação DFS e Namespaces DFS. Para obter mais informações, consulte Implantação de sistemas de arquivos Multi-AZ.

P: Como faço para integrar meu sistema de FSx arquivos da Amazon ao meu AD gerenciado de várias contas na landing zone?

Ao criar um sistema de FSx arquivos da Amazon, você pode especificar seu MALZ Managed AD como o “Microsoft Active Directory AWS gerenciado” para autenticação do Windows. Para obter mais informações, consulte Usando a Amazon FSx com o AWS Directory Service Microsoft Active Directory

Você também deve primeiro compartilhar o AD gerenciado com a conta do aplicativo. Faça isso enviando um RFC com o tipo de alteração de diretório Management | Directory | Directory | Share directory (ct-369odosk0pd9w).

P: Quais usuários pertencem ao grupo de FSx administradores delegados da AWS?

Somente administradores de servidores de arquivos de TI. Esse grupo tem privilégios de acesso total em todos os compartilhamentos de arquivos.

P: Devo usar o compartilhamento de arquivos padrão, o compartilhamento, que é criado quando o FSx sistema é provisionado?

Não, não recomendamos usar o compartilhamento de arquivos padrão, share, conforme provisionado. Ele concede acesso total a todos, o que viola o princípio do menor privilégio. Em vez

disso, crie compartilhamentos de arquivos menores e personalizados que atendam às necessidades da sua empresa.

P: Como posso criar compartilhamentos de arquivos personalizados para organizações específicas da minha empresa?

Consulte Compartilhamentos de arquivos para obter instruções sobre como criar compartilhamentos de arquivos personalizados. Restrinja o acesso em cada compartilhamento de arquivos usando o princípio do menor privilégio.

Use o AMS SSP para provisionar o Amazon FSx for OpenZFS em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon FSx for OpenZFS diretamente em sua conta gerenciada pelo AMS. FSx for OpenZFS é um serviço de armazenamento de arquivos totalmente gerenciado que facilita a transferência de dados residentes no ZFS local ou em outros servidores de arquivos baseados em Linux para a AWS sem alterar o código do aplicativo ou a forma como você gerencia os dados. Ele oferece armazenamento de arquivos altamente confiável, escalável, de alto desempenho e rico em recursos, construído no sistema de arquivos OpenZFS de código aberto, fornecendo os recursos e capacidades familiares dos sistemas de arquivos OpenZFS com a agilidade, escalabilidade e simplicidade de um serviço totalmente gerenciado. AWS Para desenvolvedores que criam aplicativos nativos da nuvem, ele oferece armazenamento simples e de alto desempenho com recursos avançados para trabalhar com dados.

FSx para OpenZFS, os sistemas de arquivos são amplamente acessíveis a partir de contêineres e instâncias de computação Linux, Windows e macOS usando o protocolo NFS padrão do setor (v3, v4.0, v4.1, v4.2). Equipado com processadores AWS Graviton e com as mais recentes tecnologias de AWS disco e rede (incluindo redes de datagramas confiáveis AWS escaláveis e o sistema AWS Nitro), FSx o OpenZFS oferece até 1 milhão de IOPS com latências de centenas de microssegundos. Com suporte completo aos recursos do OpenZFS, como instantâneos point-in-time instantâneos e clonagem de dados, FSx o OpenZFS facilita a substituição de seus servidores de arquivos locais por um AWS armazenamento que fornece recursos familiares do sistema de arquivos e elimina a necessidade de realizar longas qualificações e alterar ou rearquitetar aplicativos ou ferramentas existentes. E, ao combinar o poder dos recursos de gerenciamento de dados do OpenZFS com o alto desempenho e a economia das tecnologias mais recentes da AWS, o FSx for OpenZFS permite que você crie e execute aplicativos de alto desempenho e com uso intenso de dados.

Como um serviço totalmente gerenciado, FSx o OpenZFS facilita o lançamento, a execução e a escalabilidade de sistemas de arquivos totalmente gerenciados AWS que substituem os servidores de arquivos que você executa localmente, ajudando a fornecer maior agilidade e menores custos. Com FSx o OpenZFS, você não precisa mais se preocupar em configurar e provisionar servidores de arquivos e volumes de armazenamento, replicar dados, instalar e corrigir software de servidor de arquivos, detectar e solucionar falhas de hardware e realizar backups manualmente. Ele também fornece uma integração avançada com outros AWS serviços, como AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS) CloudWatch, Amazon AWS CloudTrail e.

FSx A Amazon oferece dois sistemas de arquivos para você escolher: Amazon para Windows File Server FSx para aplicativos baseados em Windows e Amazon for Lustre para cargas de trabalho com uso FSx intensivo de computação. Para saber mais, consulte Amazon FSx.

Perguntas frequentes sobre FSx o Amazon for OpenZFS no AWS Managed Services

P: Como solicito acesso FSx para usar o OpenZFS na minha conta AMS?

Solicite acesso ao Amazon FSx OpenZFS enviando uma RFC com o tipo de alteração Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_fsx_ontap_admin_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições de uso FSx do OpenZFS na minha conta AMS?

A substituição do grupo de segurança nas interfaces de rede FSx elástica da Amazon (ENIs) exige que você envie Management | Other | Other | Update, RFCs pois os grupos de segurança são um perímetro crítico para o ambiente AMS. Essa é a única restrição.

P: Quais são os pré-requisitos ou dependências FSx para usar o OpenZFS na minha conta AMS?

Não há pré-requisitos. No entanto, você deve ter Use o AMS SSP para provisionar a Amazon FSx em sua conta AMS instalado.

Use o AMS SSP para provisionar o Amazon FSx for NetApp ONTAP em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon FSx for NetApp ONTAP diretamente em sua conta gerenciada pelo AMS. O Amazon FSx for NetApp ONTAP é um serviço totalmente gerenciado que fornece armazenamento de arquivos altamente confiável,

escalável, de alto desempenho e rico em recursos, baseado no NetApp popular sistema de arquivos ONTAP. Ele fornece os recursos, o desempenho, os recursos e os sistemas APIs de NetApp arquivos familiares com a agilidade, a escalabilidade e a simplicidade de um sistema totalmente gerenciado. AWS service (Serviço da AWS)

O Amazon FSx for NetApp ONTAP fornece armazenamento de arquivos compartilhado rico em recursos, rápido e flexível que é amplamente acessível a partir de instâncias computacionais Linux, Windows e macOS executadas no local ou no local. AWS FSx for ONTAP oferece armazenamento SSD de alto desempenho com latências inferiores a um milissegundo e facilita e agiliza o gerenciamento de seus dados, permitindo que você capture, clone e replique seus arquivos com o clique de um botão. Ele também classifica automaticamente seus dados em camadas para um armazenamento elástico de baixo custo, eliminando a necessidade de provisionar ou gerenciar capacidade e permitindo que você alcance níveis de desempenho de SSD para sua carga de trabalho pagando apenas pelo armazenamento SSD para uma pequena fração de seus dados. Ele fornece armazenamento altamente disponível e durável com backups totalmente gerenciados e suporte para recuperação de desastres entre regiões, além de oferecer suporte a aplicativos populares de segurança de dados e antivírus que facilitam ainda mais a proteção e a proteção de seus dados. Para clientes que usam o NetApp ONTAP no local, o FSx for ONTAP é a solução ideal para migrar, fazer backup ou expandir seus aplicativos baseados em arquivos do local para AWS sem a necessidade de alterar o código do aplicativo ou a forma como você gerencia seus dados.

Como um serviço totalmente gerenciado, o Amazon FSx for NetApp ONTAP simplifica o lançamento e a escalabilidade de um armazenamento de arquivos compartilhado confiável, eficiente e seguro na nuvem. Com o Amazon FSx for NetApp ONTAP, você não precisa mais se preocupar em configurar e provisionar servidores de arquivos e volumes de armazenamento, replicar dados, instalar e corrigir software de servidor de arquivos, detectar e resolver falhas de hardware, gerenciar failover e failback e realizar backups manualmente. Ele também fornece uma rica integração com outros Serviços da AWS AWS Identity and Access Management, como Amazon WorkSpaces AWS Key Management Service, AWS CloudTrail e.

FSx A Amazon oferece dois sistemas de arquivos para você escolher: Amazon para Windows File Server FSx para aplicativos baseados em Windows e Amazon for Lustre para cargas de trabalho com uso FSx intensivo de computação. Para saber mais, consulte Amazon FSx.

Perguntas frequentes sobre FSx o Amazon for NetApp ONTAP no AWS Managed Services

P: Como solicito acesso ao Amazon FSx for NetApp ONTAP na minha conta AMS?

Solicite acesso à Amazon FSx para NetApp ONTAP enviando uma RFC com o tipo de alteração Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_fsx_ontap_admin_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições para usar o Amazon FSx for NetApp ONTAP na minha conta AMS?

A substituição do grupo de segurança na Amazon FSx pelas interfaces de rede elástica NetApp ONTAP (ENIs) exige que você envie Management | Other | Other | Update, RFCs pois os grupos de segurança são um perímetro crítico para o ambiente AMS. Essa é a única restrição.

P: Quais são os pré-requisitos ou dependências para usar o Amazon FSx for NetApp ONTAP na minha conta AMS?

Não há pré-requisitos. No entanto, você deve ter Use o AMS SSP para provisionar a Amazon FSx em sua conta AMS instalado.

Use o AMS SSP para provisionar o Amazon Inspector Classic em sua conta AMS

> **Note**
>
> Aviso de fim do suporte: em 20 de maio de 2026, AWS encerrará o suporte para o Amazon Inspector Classic. Depois de 20 de maio de 2026, você não poderá mais acessar o console do Amazon Inspector Classic ou os recursos do Amazon Inspector Classic. O Amazon Inspector Classic não estará mais disponível para novas contas e contas que não concluíram uma avaliação nos últimos seis meses. Para todas as outras contas, o acesso permanecerá válido até 20 de maio de 2026, após o qual você não poderá mais acessar o console do Amazon Inspector Classic ou os recursos do Amazon Inspector Classic. Para obter mais informações, consulte Fim do suporte do Amazon Inspector Classic.

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Inspector Classic diretamente na sua conta gerenciada do AMS. O Amazon Inspector Classic é um serviço automatizado de avaliação de segurança que ajuda a melhorar a segurança e a conformidade dos aplicativos implantados em. AWS O Amazon Inspector Classic avalia automaticamente os aplicativos quanto à exposição, vulnerabilidades e desvios das melhores práticas. Depois de realizar uma avaliação, o Amazon Inspector Classic produz uma lista detalhada de descobertas de segurança

priorizadas por nível de severidade. Essas descobertas podem ser analisadas diretamente ou como parte de relatórios de avaliação detalhados, que estão disponíveis por meio do console ou da API do Amazon Inspector Classic. Para saber mais, consulte Amazon Inspector Classic.

Perguntas frequentes sobre o Amazon Inspector no AWS Managed Services

P: Como solicito acesso ao Amazon Inspector Classic na minha conta AMS?

Solicite acesso ao Amazon Inspector Classic enviando um RFC com o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (ct-1w8z66n899dct). Essa RFC provisiona a função `customer_inspector_admin_role` do IAM em sua conta. A função inclui a AmazonInspectorFullAccess política AWS gerenciada. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições para usar o Amazon Inspector Classic na minha conta AMS?

Não há restrições. A funcionalidade completa do Amazon Inspector Classic está disponível em sua conta AMS.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Inspector Classic na minha conta AMS?

Não há pré-requisitos ou dependências para usar o Amazon Inspector Classic em sua conta AMS.

Use o novo Amazon Inspector no AMS

Agora você pode usar o novo Amazon Inspector na sua conta AMS.

Para o Amazon Inspector Classic, o `customer-inspector-admin-role-ssm-inspector-agent-policy` e `AmazonInspectorFullAccess` era necessário. No entanto, houve uma atualização na função SSPS`customer-inspector-admin-role`, que agora inclui outra. `policyAmazonInspector2FullAccess` Esta nova política permite permissões de API para a nova versão do Amazon Inspector.

Use o AMS SSP para provisionar o Amazon Kendra em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Kendra diretamente em sua conta gerenciada pelo AMS. O Amazon Kendra é um serviço de pesquisa inteligente que usa processamento de linguagem natural e algoritmos avançados de aprendizado

de máquina para retornar respostas específicas às perguntas de pesquisa de seus dados. Diferentemente da pesquisa tradicional baseada em palavras-chave, o Amazon Kendra usa seus recursos de compreensão semântica e contextual para determinar se um documento é relevante para uma consulta de pesquisa. O Amazon Kendra retorna respostas específicas às perguntas, então sua experiência está próxima de interagir com um especialista humano. O Amazon Kendra é altamente escalável, capaz de atender às demandas de desempenho, está totalmente integrado a AWS outros serviços, como o Amazon S3 e o Amazon Lex, e oferece segurança de nível empresarial. Para saber mais, consulte Amazon Kendra;.

Perguntas frequentes sobre o Amazon Kendra no AWS Managed Services

P: Como solicito acesso ao Amazon Kendra na minha conta AMS?

Para solicitar acesso ao Amazon Inspector Classic, envie uma RFC com o tipo de alteração Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny). Essa RFC provisiona a função `customer_kendra_console_role` do IAM em sua conta. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições para usar o Amazon Kendra na minha conta AMS?

Não há restrições. A funcionalidade completa do Amazon Kendra está disponível em sua conta AMS.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Kendra na minha conta AMS?

Não há pré-requisitos ou dependências para começar a usar o Amazon Kendra. No entanto, dependendo do seu caso de uso específico, você pode precisar de acesso a outros AWS serviços.

Use o AMS SSP para provisionar o Amazon Kinesis Data Streams em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Kinesis Data Streams (KDS) diretamente na sua conta gerenciada do AMS. O Amazon Kinesis Data Streams é um serviço de streaming de dados em tempo real altamente escalável e durável. O KDS pode capturar continuamente gigabytes de dados por segundo de centenas de milhares de fontes, como fluxos de cliques de sites, fluxos de eventos de banco de dados, transações financeiras, feeds de mídia social, registros de TI e eventos de rastreamento de localização. Os dados coletados estão disponíveis em milissegundos para permitir casos de uso de análises em tempo real, como painéis em tempo real, detecção de anomalias em tempo real, preços dinâmicos e muito mais. Para saber mais, consulte Amazon Kinesis Data Streams.

Perguntas frequentes sobre Kinesis Data Streams in AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao Amazon Kinesis Data Streams na minha conta do AMS?

Solicite acesso ao Amazon Kinesis Data Streams enviando uma RFC com o serviço Management | AWS | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_kinesis_data_streaming_user_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Amazon Kinesis Data Streams na minha conta AMS?

Não há restrições. A funcionalidade completa do Amazon Kinesis Data Streams está disponível em sua conta do AMS.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Kinesis Data Streams na minha conta AMS?

Não há pré-requisitos ou dependências para usar o Amazon Kinesis Data Streams em sua conta do AMS.

Use o AMS SSP para provisionar o Amazon Kinesis Video Streams em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Kinesis Video Streams (KVS) diretamente na sua conta gerenciada do AMS. O Amazon Kinesis Video Streams ajuda você a transmitir vídeos com segurança de AWS dispositivos conectados para análise, aprendizado de máquina (ML), reprodução e outros processamentos. O Kinesis Video Streams provisiona automaticamente e dimensiona de forma elástica toda a infraestrutura necessária para ingerir dados de streaming de vídeo de milhões de dispositivos. Ele também armazena, criptografa e indexa de forma durável os dados de vídeo em seus streams e permite que você acesse seus dados por meio de. easy-to-use APIs O Kinesis Video Streams permite que você reproduza vídeo para visualização ao vivo e sob demanda e crie rapidamente aplicativos que aproveitam a visão computacional e a análise de vídeo por meio da integração com o Amazon Rekognition Video e bibliotecas para estruturas de ML, como Apache e OpenCV. MxNet TensorFlow Para saber mais, consulte Amazon Kinesis Video Streams.

Perguntas frequentes sobre o Amazon Kinesis Video Streams in AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao Amazon Kinesis Video Streams na minha conta AMS?

Solicite acesso ao Amazon Kinesis Video Streams enviando uma RFC com o AWS Management | service | Service self-provisioned | Add change type (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_kinesis_video_streaming_user_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Amazon Kinesis Video Streams na minha conta AMS?

Não há restrições. A funcionalidade completa do Amazon Kinesis Video Streams está disponível em sua conta AMS.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Kinesis Video Streams na minha conta AMS?

Não há pré-requisitos ou dependências para usar o Amazon Kinesis Video Streams em sua conta AMS.

Use o AMS SSP para provisionar o Amazon Lex em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Lex diretamente na sua conta gerenciada do AMS. O Amazon Lex é um serviço para criar interfaces de conversação em qualquer aplicativo usando voz e texto. O Amazon Lex fornece as funcionalidades avançadas de aprendizado profundo de reconhecimento automático de fala (ASR) para converter fala em texto e compreensão de linguagem natural (NLU) para reconhecer a intenção do texto, permitindo que você crie aplicativos com experiências de usuário altamente envolventes e interações conversacionais realistas. Com o Amazon Lex, as mesmas tecnologias de aprendizado profundo que impulsionam o Amazon Alexa agora estão disponíveis para qualquer desenvolvedor, permitindo que você crie de forma rápida e fácil bots de conversação ou chatbots sofisticados em linguagem natural. Para saber mais, consulte Amazon Lex.

Perguntas frequentes sobre o Amazon Lex no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao Amazon Lex na minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_lex_author_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Amazon Lex na minha conta do AMS?

A integração do Amazon Lex com o Lambda é limitada às funções do Lambda sem o prefixo “AMS-”, a fim de evitar modificações na infraestrutura do AMS.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Lex na minha conta AMS?

Não há pré-requisitos ou dependências para usar o Amazon Lex em sua conta do AMS.

Use o AMS SSP para provisionar o Amazon MQ em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon MQ diretamente em sua conta gerenciada pelo AMS. O Amazon MQ é um serviço gerenciado de agente de mensagens para o Apache ActiveMQ que ajuda você a configurar e operar agentes de mensagens na nuvem. Os corretores de mensagens permitem que diferentes sistemas de software, geralmente usando linguagens de programação diferentes e em plataformas diferentes, se comuniquem e troquem informações. O Amazon MQ reduz sua carga operacional gerenciando o provisionamento, a configuração e a manutenção do ActiveMQ, um popular agente de mensagens de código aberto. A conexão de seus aplicativos atuais ao Amazon MQ usa protocolos APIs e padrões do setor para mensagens, incluindo JMS, NMS, AMQP, STOMP, MQTT e. WebSocket Usar padrões significa que, na maioria dos casos, não há necessidade de reescrever nenhum código de mensagem ao migrar para o. AWS Para saber mais, consulte O que é o Amazon MQ?

Perguntas frequentes sobre o Amazon MQ no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao Amazon MQ na minha conta do AMS?

A utilização do Amazon MQ em sua conta do AMS é um processo de duas etapas:

1. Provisione o Amazon MQ Broker. Para fazer isso, envie um modelo de CFN, com o Amazon MQ Broker incluído, por meio de uma RFC com a opção Deployment | Inestion | Stack CloudFormation

from Template | Create change type (ct-36cn2avfrrj9v) ou envie uma RFC com o Management | Other | Other | Crie o tipo de alteração (ct-1e1xtak34nx76) solicitando que o Amazon MQ Broker seja provisionado em sua conta.

2. Acesse o console do Amazon MQ. Depois que o Amazon MQ Broker for provisionado, obtenha acesso ao console do Amazon MQ enviando uma RFC com o campo Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_mq_console_role`.

Depois que a função for provisionada em sua conta, você deverá integrá-la à sua solução de federação.

P: Quais são as restrições para usar o Amazon MQ na minha conta AMS?

A funcionalidade completa do Amazon MQ está disponível em sua conta do AMS; no entanto, o provisionamento do Amazon MQ Broker não está disponível por meio da política devido à elevada permissão necessária. Veja acima os detalhes sobre como provisionar o corretor Amazon MQ em suas contas.

P: Quais são os pré-requisitos ou dependências para usar o Amazon MQ na minha conta AMS?

Não há pré-requisitos ou dependências para usar o Amazon MQ em sua conta do AMS.

Use o AMS SSP para provisionar o Amazon Managed Service para Apache Flink em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Managed Service for Apache Flink diretamente em sua conta gerenciada do AMS. O Managed Service para Apache Flink é a maneira mais fácil de analisar dados de streaming, obter insights acionáveis e responder às necessidades de sua empresa e de seus clientes em tempo real. O Amazon Managed Service para Apache Flink reduz a complexidade de criar, gerenciar e integrar aplicativos de streaming com outros serviços. AWS Os usuários do SQL podem consultar facilmente dados de streaming ou criar aplicativos de streaming inteiros usando modelos e um editor SQL interativo. Os desenvolvedores de Java podem criar rapidamente aplicativos de streaming sofisticados usando bibliotecas e AWS integrações Java de código aberto para transformar e analisar dados em tempo real. O Amazon Managed Service para Apache Flink cuida de tudo o que é necessário para executar seus aplicativos em tempo real continuamente e escala automaticamente para corresponder ao volume e à taxa de transferência dos dados recebidos. Com o Amazon Managed Service para Apache Flink, você paga apenas pelos recursos que seus aplicativos de streaming consomem. Não

há taxa mínima nem custo de instalação. Para saber mais, consulte Amazon Managed Service para Apache Flink.

Perguntas frequentes sobre o Managed Service for Apache Flink no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao Amazon Managed Service para Apache Flink na minha conta AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_kinesis_analytics_application_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Amazon Managed Service para Apache Flink na minha conta AMS?

- As configurações são limitadas a recursos sem os prefixos 'AMS-' ou 'MC-' para evitar qualquer modificação na infraestrutura do AMS.
- A permissão para excluir ou criar novos Kinesis Data Streams ou Firehose foi removida da política. Temos outra política que permite isso.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Kinesis Data Streams na minha conta AMS?

Existem algumas dependências:

- O Amazon Managed Service para Apache Flink exige que o Kinesis Data Streams ou o Firehose sejam criados antes da configuração de um aplicativo com o Managed Service for Apache Flink.
- As permissões da política baseada em recursos devem indicar uma fonte de dados de entrada específica.

Use o AMS SSP para provisionar o Amazon Managed Streaming para Apache Kafka em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Managed Streaming for Apache Kafka (Amazon MSK) diretamente na sua conta gerenciada do AMS. O

Amazon Managed Streaming for Apache Kafka é um serviço de streaming de dados AWS totalmente gerenciado que facilita a criação e a execução de aplicativos que usam o Apache Kafka para processar dados de streaming sem precisar se tornar um especialista na operação de clusters do Apache Kafka. O Amazon MSK gerencia o provisionamento, a configuração e a manutenção dos clusters do Apache Kafka e dos nós do Apache para você. ZooKeeper O Amazon MSK também mostra as principais métricas de desempenho do Apache Kafka no console. AWS

O Amazon MSK fornece vários níveis de segurança para seus clusters do Apache Kafka, incluindo isolamento de rede VPC, AWS IAM para autorização de API no plano de controle, criptografia em repouso, criptografia TLS em trânsito, autenticação de certificado baseada em TLS, autenticação protegida por. SASL/SCRAM AWS Secrets Manager Para saber mais, consulte Amazon MSK.

Perguntas frequentes sobre o Amazon MSK no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao Amazon MSK na minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Essa RFC provisiona as seguintes políticas e funções do IAM em sua conta:

- `customer-msk-admin-policy.json`
- `AmazonMSKFullAccess`
- `customer-msk-admin-role.json`

Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Amazon MSK?

Para que o Amazon MSK entregue os registros do agente aos destinos que você configura, certifique-se de que a `AmazonMSKFullAccess` política esteja vinculada à sua função do IAM. Portanto, as permissões de acesso total já estão em vigor.

P: Quais são os pré-requisitos ou dependências para usar o Amazon MSK?

Antes de criar seu cluster MSK, você deve ter uma VPC e sub-redes dentro dessa VPC. Por padrão, o AMS aborda isso como parte da criação padrão da VPC do AMS.

Para saber mais sobre a limitação do Amazon MSK, consulte Limites do Amazon MSK.

Use o AMS SSP para provisionar o Amazon Managed Service para Prometheus em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Managed Service for Prometheus (AMP) diretamente na sua conta gerenciada do AMS. O Amazon Managed Service for Prometheus é um serviço de monitoramento sem servidor compatível com o Prometheus para métricas de contêiner que facilita o monitoramento seguro de ambientes de contêiner em escala. Com o Amazon Managed Service for Prometheus, você pode usar o mesmo modelo de dados e linguagem de consulta de código aberto do Prometheus que você usa atualmente para monitorar o desempenho de suas workloads em contêineres e também desfrutar de maior escalabilidade, disponibilidade e segurança sem precisar gerenciar a infraestrutura subjacente.

O Amazon Managed Service for Prometheus escala automaticamente a ingestão, o armazenamento e a consulta de métricas operacionais à medida que as cargas de trabalho aumentam e diminuem. Ele se integra aos serviços AWS de segurança para permitir acesso rápido e seguro aos dados. Para obter mais informações, consulte O que é o Amazon Managed Service para Prometheus?

Perguntas frequentes sobre o Amazon Managed Service for Prometheus no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao Amazon Managed Service for Prometheus na minha conta AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer-prometheus-console-role`. Depois de provisionado em sua conta, você deve integrar a `customer-prometheus-console-role` função em sua solução de federação.

P: Quais são as restrições ao uso do Amazon Managed Service for Prometheus na minha conta AMS?

Todos os recursos são suportados.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Managed Service for Prometheus na minha conta AMS?

Não há pré-requisitos ou dependências para começar a usar o Amazon Managed Service for Prometheus. No entanto, dependendo do seu caso de uso específico, você pode precisar de acesso a outros AWS serviços.

Use o AMS SSP para provisionar o Amazon Personalize em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Personalize diretamente em sua conta gerenciada do AMS. O Amazon Personalize é um serviço de aprendizado de máquina que facilita aos desenvolvedores a criação de recomendações individualizadas para clientes que usam seus aplicativos.

O aprendizado de máquina está sendo cada vez mais usado para melhorar o engajamento do cliente, promovendo recomendações personalizadas de produtos e conteúdos, resultados de pesquisa personalizados e promoções de marketing direcionadas. No entanto, o desenvolvimento dos recursos de aprendizado de máquina necessários para produzir esses sofisticados sistemas de recomendação está fora do alcance da maioria das organizações atualmente devido à complexidade. O Amazon Personalize permite que desenvolvedores sem experiência prévia em aprendizado de máquina criem facilmente recursos sofisticados de personalização em seus aplicativos, usando a tecnologia de aprendizado de máquina aperfeiçoada a partir de anos de uso na Amazon.com.

Com o Amazon Personalize, você fornece um fluxo de atividades do seu aplicativo — cliques, visualizações de páginas, inscrições, compras e assim por diante — bem como um inventário dos itens que você deseja recomendar, como artigos, produtos, vídeos ou músicas. Você também pode optar por fornecer ao Amazon Personalize informações demográficas adicionais de seus usuários, como idade ou localização geográfica. O Amazon Personalize processará e examinará os dados, identificará o que é significativo, selecionará os algoritmos certos e treinará e otimizará um modelo de personalização personalizado para seus dados. Todos os dados analisados pelo Amazon Personalize são mantidos privados e seguros e usados somente para suas recomendações personalizadas. Você pode começar a oferecer recomendações personalizadas por meio de uma simples chamada de API. Você paga somente pelo que usa e não há taxas mínimas nem compromissos iniciais.

Para saber mais, consulte Amazon Personalize.

Perguntas frequentes sobre o Amazon Personalize no AWS Managed Services

P: Como solicito acesso ao Amazon Personalize na minha conta do AMS?

Solicite acesso enviando um tipo de alteração Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) e você precisará especificar qual bucket do S3 contém os dados a serem usados pela personalização para gerar as recomendações. AWS Essa RFC provisiona as seguintes funções do IAM para sua conta: `customer_personalize_console_role` e. `customer_personalize_service_role`

- Depois de `customer_personalize_console_role` provisionado em sua conta, você deve integrar a função em sua solução de federação. Você também pode anexar o `customer_personalize_console_policy` a outra função existente que não sejaCustomer_ReadOnly_Role.
- Depois que o `customer_personalize_service_role` for fornecido à sua conta, você poderá consultar seu ARN ao criar um novo grupo de conjuntos de dados.

Nesse momento, o AMS Operations também implantará essa função de serviço em sua conta:`aws_code_pipeline_service_role_policy`.

P: Quais são as restrições para usar o Amazon Personalize na minha conta do AMS?

A configuração do Amazon Personalize é limitada a recursos sem os prefixos 'ams-' ou 'mc-', para evitar qualquer modificação na infraestrutura do AMS.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Personalize na minha conta AMS?

- Se o bucket do S3 em que os dados são armazenados for criptografado, o ID da chave KMS deverá ser fornecido, para que possamos permitir que a função usada pelo Amazon Personalize decodifique o bucket.

  O Amazon Personalize não oferece suporte à chave KMS S3 padrão. Se for necessário usar o KMS, crie uma chave personalizada e adicione a seguinte política a ela abrindo uma RFC com o tipo de alteração KMS Key | Create (revisão obrigatória):

  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": "*"
        }
    ]
}
```

- Um bucket S3 deve ser criado com a seguinte política de bucket. Faça isso enviando um RFC com o tipo de alteração S3 Storage | Create Policy. Essa política permite que o Amazon Personalize acesse dados; esse bucket conterá os dados a serem usados pelo 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/*"
]
}
]
}
```

Use o AMS SSP para provisionar a Amazon QuickSight em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os QuickSight recursos diretamente em sua conta gerenciada pelo AMS. QuickSight é um serviço de business intelligence rápido

e baseado em nuvem que fornece insights para todos em sua organização. Como um serviço totalmente gerenciado, QuickSight permite criar e publicar facilmente painéis interativos que incluem insights de aprendizado de máquina (ML). Para saber mais, consulte Amazon QuickSight.

QuickSight perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à QuickSight minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_quicksight_console_admin_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições de uso QuickSight na minha conta AMS?

- AWS as configurações de recursos ativadas QuickSight não estarão acessíveis para você devido à dependência da política do IAM. No entanto, a equipe do AMS habilita cada recurso para você em resposta à sua solicitação para habilitar o serviço.
- O acesso a recursos para usuários e grupos individuais não é suportado nesse modelo porque esse recurso permite que os usuários alterem as permissões do IAM que poderiam comprometer a infraestrutura do AMS.
- A capacidade de convidar identidades do IAM de dentro não QuickSight é suportada devido ao risco envolvido na alteração de objetos do IAM.
- QuickSight O serviço oferece duas edições: Enterprise e Standard. Ambos fornecem uma opção de login único (SSO) compatível com o AMS. No entanto, a Enterprise Edition tem a opção de integração QuickSight com o Active Directory (AD). QuickSight on AMS não oferece suporte à integração com o AD devido a incompatibilidades entre a estrutura da conta do AMS e os requisitos de QuickSight confiança.

P: Quais são os pré-requisitos ou dependências para usar QuickSight na minha conta do AMS?

- Quando o AMS recebe esse RFC para adicionar QuickSight, você recebe uma solicitação de serviço para obter informações adicionais; forneça o seguinte:
  - QuickSight nome da conta (por exemplo, *`CustomerName`*`-quicksight`
  - QuickSight Edição (Standard versus Enterprise)
  - A AWS região na qual habilitar o QuickSight serviço (o padrão é sua AWS região do AMS).

- Um endereço de e-mail de notificação para a QuickSight conta.
- (Opcional) O bucket do S3 em que os arquivos de dados a serem analisados estão localizados.
- A VPC e a sub-rede IDs que se conectam oferecem QuickSight suporte a um recurso para adicionar uma conexão VPC, que permite conectividade privada entre recursos QuickSight e dentro da conta.

Um operador de AMS realiza o processo de inscrição em seu nome e configura duas QuickSight funcionalidades:

- Descoberta automática de fontes de dados.
- Conexões VPC.

> **Note**
>
> Essas ações precisam ser executadas por um operador de AMS porque permissões elevadas de IAM e VPC são necessárias durante o processo de login.

Use o AMS SSP para provisionar o Amazon Rekognition em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Rekognition diretamente em sua conta gerenciada pelo AMS. O Amazon Rekognition facilita a adição de análises de imagens e vídeos aos seus aplicativos usando uma tecnologia comprovada e altamente escalável de aprendizado profundo que não requer experiência em aprendizado de máquina para ser usada. Com o Amazon Rekognition, você pode identificar objetos, pessoas, textos, cenas e atividades em imagens e vídeos, bem como detectar qualquer conteúdo impróprio. O Amazon Rekognition também fornece recursos de análise facial e pesquisa facial altamente precisos que você pode usar para detectar, analisar e comparar faces em uma ampla variedade de casos de uso de verificação de usuários, contagem de pessoas e segurança pública.

Com as etiquetas personalizadas do Amazon Rekognition, você pode identificar objetos e cenas em imagens que são específicas para suas necessidades comerciais. Por exemplo, você pode criar um modelo para classificar peças específicas da máquina em sua linha de montagem ou para detectar plantas insalubres. O Amazon Rekognition Custom Labels cuida do trabalho pesado de desenvolvimento do modelo para você, portanto, nenhuma experiência em aprendizado de máquina

é necessária. Você só precisa fornecer imagens de objetos ou cenas que deseja identificar, e o serviço cuida do resto.

Para saber mais, consulte Amazon Rekognition.

Perguntas frequentes sobre o Amazon Rekognition in AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao Amazon Rekognition na minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_rekognition_console_role & customer_rekognition_service_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Amazon Rekognition na minha conta AMS?

A funcionalidade completa do Amazon Rekognition está disponível com a função de serviço autoprovisionado do Amazon Rekognition.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Rekognition na minha conta AMS?

Se você usa o Kinesis Video Streams que fornece a fonte de streaming de vídeo para um processador de stream de vídeo Amazon Rekognition Video ou um stream de dados como destino para gravar dados no Kinesis Data Streams, forneça um ao AMS ao criar o RFC. `kinesisStreamName`

Use o AMS SSP para provisionar o Amazon SageMaker AI em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos de SageMaker IA da Amazon diretamente em sua conta gerenciada pelo AMS. SageMaker A IA fornece a todos os desenvolvedores e cientistas de dados a capacidade de criar, treinar e implantar modelos de aprendizado de máquina rapidamente. O Amazon SageMaker AI é um serviço totalmente gerenciado que abrange todo o fluxo de trabalho de aprendizado de máquina para rotular e preparar seus dados, escolher um algoritmo, treinar o modelo, ajustá-lo e otimizá-lo para implantação, fazer previsões e agir. Seus modelos chegam à produção mais rapidamente com muito menos esforço e menor custo. Para saber mais, consulte Amazon SageMaker AI.

SageMaker Perguntas frequentes sobre IA no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso à SageMaker IA na minha conta do AMS?

Solicite acesso enviando um tipo de alteração Gerenciamento | AWS Serviço | Serviço autoprovisionado | Adicionar (ct-1w8z66n899dct). Essa RFC provisiona as seguintes funções do IAM para sua conta: `customer_sagemaker_admin_role` e função `AmazonSageMaker-ExecutionRole-Admin` de serviço. Depois que a SageMaker IA for provisionada em sua conta, você deverá integrar a `customer_sagemaker_admin_role` função na sua solução de federação. A função de serviço não pode ser acessada diretamente por você; o serviço de SageMaker IA a usa ao realizar várias ações, conforme descrito aqui: Passando funções.

P: Quais são as restrições ao uso da SageMaker IA na minha conta do AMS?

- Os seguintes casos de uso não são compatíveis com a função AMS Amazon SageMaker AI IAM:
  - SageMaker O AI Studio não é suportado no momento.
  - SageMaker O AI Ground Truth para gerenciar forças de trabalho privadas não é suportado, pois esse recurso exige acesso excessivamente permissivo aos recursos do Amazon Cognito. Se for necessário gerenciar uma força de trabalho privada, você pode solicitar uma função personalizada do IAM com permissões combinadas de SageMaker IA e Amazon Cognito. Caso contrário, recomendamos o uso de força de trabalho pública (apoiada pela Amazon Mechanical Turk) AWS Marketplace ou provedores de serviços para rotulagem de dados.
- Criação de VPC Endpoints para oferecer suporte a chamadas de API para serviços de SageMaker IA (aws.sagemaker). {region} .notebook, com.amazonaws. {region} .sagemaker.api e com.amazonaws. {region} .sagemaker.runtime) não é suportado, pois as permissões não podem ser reduzidas apenas aos serviços relacionados à IA. SageMaker Para dar suporte a esse caso de uso, envie um RFC Management | Other | Other para criar VPC endpoints relacionados.
- SageMaker O escalonamento automático de endpoints de IA não é suportado, pois a SageMaker IA exige `DeleteAlarm` permissões em qualquer recurso (“*”). Para oferecer suporte ao escalonamento automático de endpoint, envie um RFC de gerenciamento | Outro | Outro para configurar o escalonamento automático para um endpoint de IA. SageMaker

P: Quais são os pré-requisitos ou dependências para usar a SageMaker IA na minha conta do AMS?

- Os seguintes casos de uso exigem uma configuração especial antes do uso:

- Se um bucket do S3 for usado para armazenar artefatos e dados do modelo, você deverá solicitar um bucket do S3 nomeado com as palavras-chave necessárias (" SageMaker ", "Sagemaker", "sagemaker" ou "aws-glue") com um Deployment | Advanced stack components | S3 storage | Create RFC.
- Se o Elastic File Store (EFS) for usado, o armazenamento do EFS deverá ser configurado na mesma sub-rede e permitido por grupos de segurança.
- Se outros recursos exigirem acesso direto aos serviços de SageMaker IA (notebooks, API, tempo de execução etc.), a configuração deverá ser solicitada por:
  - Enviando uma RFC para criar um grupo de segurança para o endpoint (Implantação | Componentes avançados da pilha | Grupo de segurança | Criar (automático)).
  - Enviando um gerenciamento | Outro | Outro | Crie RFC para configurar endpoints VPC relacionados.

P: Quais são as convenções de nomenclatura suportadas para recursos que eles **`customer_sagemaker_admin_role`** podem acessar diretamente? (O seguinte é para atualizar e excluir permissões; se você precisar de convenções de nomenclatura adicionais suportadas para seus recursos, entre em contato com um arquiteto de nuvem do AMS para obter consultoria.)

- Recurso: `AmazonSageMaker-ExecutionRole-*` Papel de passagem
  - Permissões: a SageMaker função de serviço autoprovisionada de IA oferece suporte ao uso da função de serviço de SageMaker IA (`AmazonSageMaker-ExecutionRole-*`) com AWS Glue, e. AWS RoboMaker AWS Step Functions
- Recurso: Segredos no AWS Secrets Manager
  - Permissões: descrever, criar, obter e atualizar segredos com um `AmazonSageMaker-*` prefixo.
  - Permissões: descreva, obtenha segredos quando a tag do `SageMaker` recurso estiver definida como`true`.
- Recurso: Repositórios em AWS CodeCommit
  - Permissões: crie/exclua repositórios com um prefixo. `AmazonSageMaker-*`
  - Permissões: Git Pull/Push em repositórios com os seguintes prefixos,, e. `*sagemaker*` `*SageMaker*` `*Sagemaker*`
- Recurso: Repositórios do Amazon ECR (Amazon Elastic Container Registry)
  - Permissões: Permissões: defina, exclua políticas do repositório e faça upload de imagens de contêiner, quando a seguinte convenção de nomenclatura de recursos for usada,. `*sagemaker*`

- Recurso: buckets Amazon S3
  - Permissões: Obter, colocar, excluir objeto, interromper o upload de objetos do S3 em várias partes quando os recursos tiverem os seguintes prefixos:`*SageMaker*`, e. `*Sagemaker*` `*sagemaker*` `aws-glue`
  - Permissões: obtenha objetos do S3 quando a `SageMaker` tag estiver definida como. `true`
- Recurso: Amazon CloudWatch Log Group
  - Permissões: Criar grupo ou transmissão de log, colocar evento de registro, listar, atualizar, criar, excluir entrega de log com o seguinte prefixo:`/aws/sagemaker/*`.
- Recurso: Amazon CloudWatch Metric
  - Permissões: coloque dados métricos quando os seguintes prefixos forem usados: `AWS/SageMakerAWS/SageMaker/`,`aws/SageMaker`,`aws/SageMaker/`,`aws/sagemaker`,`aws/sagemaker/`, e. `/aws/sagemaker/.`
- Recurso: Amazon CloudWatch Dashboard
  - Permissões: Create/Delete painéis quando os seguintes prefixos são usados:. `customer_*`
- Recurso: tópico Amazon SNS (Simple Notification Service)
  - Permissões: Subscribe/Create tópico quando os seguintes prefixos são usados: `*sagemaker**SageMaker*`, e. `*Sagemaker*`

P: Qual é a diferença entre **`AmazonSageMakerFullAccess`** e**`customer_sagemaker_admin_role`**?

O `customer_sagemaker_admin_role` with the `customer_sagemaker_admin_policy` fornece quase as mesmas permissões, AmazonSageMakerFullAccess exceto:

- Permissão para se conectar com AWS RoboMaker o Amazon Cognito e AWS Glue os recursos.
- SageMaker Escalonamento automático de endpoints de IA. Você deve enviar uma RFC com Management | Advanced stack components | Identity and Access Management (IAM) | Atualizar o tipo de alteração de entidade ou política (revisão obrigatória) (ct-27tuth19k52b4) para elevar as permissões de escalonamento automático temporariamente ou permanentemente, pois o escalonamento automático exige acesso permissivo no serviço. CloudWatch

P: Como adoto a chave gerenciada pelo AWS KMS cliente na criptografia de dados em repouso?

Você deve garantir que a política de chaves tenha sido configurada adequadamente nas chaves gerenciadas pelo cliente para que os usuários ou funções relacionados do IAM possam usar as chaves. Para obter mais informações, consulte o documento de política de AWS KMS chaves.

Use o AMS SSP para provisionar o Amazon Simple Email Service em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Simple Email Service (Amazon SES) diretamente na sua conta gerenciada pelo AMS. O Amazon Simple Email Service é um serviço de envio de e-mails baseado em nuvem projetado para ajudar profissionais de marketing digital e desenvolvedores de aplicativos a enviar e-mails de marketing, notificações e transações.

Você pode usar a interface SMTP ou uma delas AWS SDKs para integrar o Amazon SES diretamente aos seus aplicativos existentes. Você também pode integrar os recursos de envio de e-mail do Amazon SES ao software que você já usa, como sistemas de emissão de bilhetes e clientes de e-mail.

Para saber mais, consulte Amazon Simple Email Service.

Perguntas frequentes sobre o Amazon SES no AWS Managed Services

P: Como solicito acesso ao Amazon SES na minha conta do AMS?

Solicite acesso ao Amazon SES enviando uma RFC com o serviço Management | AWS | Self-provisioned service | Add (ct-1w8z66n899dct) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_ses_admin_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são os pré-requisitos ou dependências para usar o Amazon SES na minha conta AMS?

- Você deve configurar uma política de bucket do S3 para permitir que o Amazon SES publique eventos no bucket.
- Você deve usar uma chave padrão (AWS SES) ou configurar uma chave CMK para permitir que o Amazon SES criptografe e-mails e envie eventos para outros recursos de serviço, como Amazon S3, Amazon SNS, Lambda e Firehose, pertencentes à conta.

P: Quais são as restrições ao uso do Amazon SES na minha conta do AMS?

Você deve aumentar RFCs para criar os seguintes recursos:

- Um usuário SMTP e uma função de serviço do IAM com PutEvents permissão para um stream do Kinesis Firehose.
- Você deve criar novos AWS recursos, como bucket do S3, stream do Firehose e tópico do SNS, usando os tipos de alteração do AMS para que os destinos das regras e dos conjuntos de configuração do Amazon SES funcionem com esses recursos.
- Credenciais SMTP. Para solicitar novas credenciais SMTP, use o Tipo de alteração (Gerenciamento | Outro | Outro | Criar). O AMS cria as credenciais e as adiciona ao Secrets Manager para você.

Use o AMS SSP para provisionar o Amazon Simple Workflow Service em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Simple Workflow Service (Amazon SWF) diretamente na sua conta gerenciada do AMS. O Amazon Simple Workflow Service ajuda os desenvolvedores a criar, executar e escalar trabalhos em segundo plano que tenham etapas paralelas ou sequenciais. Você pode pensar no Amazon SWF como um rastreador de estado totalmente gerenciado e coordenador de tarefas na nuvem. Se as etapas do seu aplicativo levarem mais de 500 milissegundos para serem concluídas, você precisar rastrear o estado do processamento ou precisar recuperar ou tentar novamente se uma tarefa falhar, o Amazon SWF pode ajudá-lo. Para saber mais, consulte Amazon Simple Workflow Service.

Perguntas frequentes sobre o Amazon SWF no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao Amazon SWF na minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_swf_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Amazon SWF na minha conta AMS?

As `InvokeFunction` permissões do Lambda foram incluídas nesse serviço. No entanto, o AMS `customer_deny_policy` que é adicionado a todas as funções do cliente do AMS nega

explicitamente o acesso às funções do AMS Lambda e aos recursos de propriedade da AMS. Para marcar ou desmarcar recursos no Amazon SWF, envie um tipo de alteração Management | Other | Other.

P: Quais são os pré-requisitos ou dependências para usar o Amazon SWF na minha conta AMS?

O Amazon SWF depende do AWS Lambda serviço, portanto, as permissões para invocar o Lambda foram fornecidas como parte dessa função e nenhuma permissão adicional é necessária para invocar o Lambda do Amazon SWF. Caso contrário, não há pré-requisitos para usar o Amazon SWF.

Use o AMS SSP para provisionar o Amazon Textract em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Textract diretamente em sua conta gerenciada pelo AMS. O Amazon Textract é um serviço de aprendizado de máquina totalmente gerenciado que extrai automaticamente texto impresso, manuscrito e outros dados de documentos digitalizados que vão além do simples reconhecimento óptico de caracteres (OCR) para identificar, entender e extrair dados de formulários e tabelas. Para saber mais, consulte Amazon Textract.

Perguntas frequentes sobre o Amazon Textract no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito que o Amazon Textract seja configurado na minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Essa RFC provisiona as seguintes funções do IAM em sua conta: `customer_textract_console_rolecustomer_textract_human_review_execution_role`, e. `customer_ec2_textract_instance_profile` Depois de provisionado em sua conta, você deve integrar a função `customer_textract_console_role` em sua solução de federação.

P: Quais são as restrições ao uso do Amazon Textract na minha conta do AMS?

Não há restrições para o uso do Amazon Textract em sua conta do AMS.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Textract na minha conta AMS?

Você deve solicitar a criação de um bucket do S3 enviando um RFC Deployment | Advanced stack components |S3 storage | Create (ct-1a68ck03fn98r).

Use o AMS SSP para provisionar o Amazon Transcribe em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Amazon Transcribe diretamente em sua conta gerenciada pelo AMS. O Amazon Transcribe é um serviço de reconhecimento automático de fala totalmente gerenciado e continuamente treinado que gera automaticamente transcrições de texto com data e hora a partir de arquivos de áudio. O Amazon Transcribe facilita que os desenvolvedores speech-to-text adicionem recursos aos seus aplicativos. Os dados de áudio são praticamente impossíveis de serem pesquisados e analisados por computadores. Portanto, a fala gravada precisa ser convertida em texto antes de poder ser usada em aplicativos. Historicamente, os clientes precisavam trabalhar com fornecedores de transcrição que exigiam que eles assinassem contratos caros e eram difíceis de integrar às suas pilhas de tecnologia para realizar essa tarefa. Muitos desses provedores usam tecnologia desatualizada que não se adapta bem a diferentes cenários, como áudio telefônico de baixa fidelidade comum em centrais de atendimento, o que resulta em baixa precisão.

O Amazon Transcribe usa um processo de aprendizado profundo chamado reconhecimento automático de fala (ASR) para converter fala em texto com rapidez e precisão. O Amazon Transcribe pode ser usado para transcrever chamadas de atendimento ao cliente, automatizar legendas ocultas e legendagem e gerar metadados para ativos de mídia para criar um arquivo totalmente pesquisável. Você pode usar o Amazon Transcribe Medical para adicionar recursos speech-to-text médicos aos aplicativos de documentação clínica. Para saber mais, consulte Amazon Transcribe.

Perguntas frequentes sobre o Amazon Transcribe no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito que o Amazon Transcribe seja configurado na minha conta AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_transcribe_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Amazon Transcribe na minha conta do AMS?

Você deve usar 'customer-transcribe*' como prefixo para seus buckets ao trabalhar com transcribe, a menos que RA e especifique o contrário.

Você não pode criar uma função do IAM no Amazon Transcribe.

Você não pode usar um bucket S3 gerenciado por serviços para dados de saída no SSPS padrão (se isso for necessário, entre em contato com a CA da sua conta).

Você deve enviar a Aceitação de Risco se quiser usar chaves KMS gerenciadas pelo cliente que não se enquadrem no namespace AMS.

P: Quais são os pré-requisitos ou dependências para usar o Amazon Transcribe na minha conta do AMS?

O S3 deve ter acesso aos buckets com o nome 'customer-transcribe*'. O KMS é necessário para usar o Amazon Transcribe se seus buckets do S3 estiverem criptografados com chaves KMS. Se um bucket não precisar ser criptografado, "KMStranscribePermitir” poderá ser removido.

Use o AMS SSP para provisionar a Amazon WorkSpaces em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os WorkSpaces recursos diretamente em sua conta gerenciada pelo AMS. WorkSpaces permite que você provisione desktops Microsoft Windows ou Amazon Linux virtuais baseados em nuvem para seus usuários, conhecidos como. WorkSpaces WorkSpaces elimina a necessidade de adquirir e implantar hardware ou instalar software complexo. Você pode rapidamente adicionar ou remover usuários à medida que suas necessidades mudarem. Os usuários os acessam WorkSpaces usando um aplicativo cliente de um dispositivo compatível ou, para Windows WorkSpaces, de um navegador da Web e fazem login usando suas credenciais locais existentes do Active Directory (AD).

Para saber mais, consulte Amazon WorkSpaces.

WorkSpaces perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à WorkSpaces minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_workspaces_console_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições de uso WorkSpaces na minha conta AMS?

A funcionalidade completa do Workspaces está disponível com a função de WorkSpaces serviço autoprovisionado da Amazon.

P: Quais são os pré-requisitos ou dependências para usar WorkSpaces na minha conta do AMS?

- WorkSpaces são limitados por AWS região; portanto, o AD Connector deve ser configurado na mesma AWS região em que as WorkSpaces instâncias estão hospedadas.

  Os clientes podem se conectar WorkSpaces ao AD do cliente usando um dos dois métodos a seguir:

  1. Usando o conector AD para autenticação de proxy para o serviço local do Active Directory (preferencial):

     Configure o conector do Active Directory (AD) em sua conta do AMS antes de integrar sua WorkSpaces instância com seu serviço de diretório local. O AD Connector atua como um proxy para que seus usuários existentes do AD (do seu domínio) se conectem WorkSpaces usando as credenciais locais existentes do AD. Isso é preferível porque WorkSpaces estão diretamente vinculados ao domínio local do cliente, que atua como floresta de recursos e de usuários, levando a um maior controle do lado do cliente.

     Para obter mais informações, consulte Melhores práticas para implantar a Amazon WorkSpaces (Cenário 1).

  2. Usando o AD Connector com o AWS Microsoft AD, o Shared Services VPC e uma confiança unidirecional no local:

     Você também pode autenticar usuários com seu diretório local estabelecendo primeiro uma confiança de saída unidirecional do AD gerenciado pelo AMS para seu AD local. WorkSpaces ingressará no AD gerenciado pelo AMS usando um AD Connector. WorkSpaces as permissões de acesso serão então delegadas às WorkSpaces instâncias por meio do AD gerenciado pelo AMS, sem a necessidade de estabelecer uma relação de confiança bidirecional com seu ambiente local. Nesse cenário, a floresta de usuários estará no AD do cliente e a floresta de recursos estará no AD gerenciado pelo AMS (alterações no AD gerenciado pelo AMS podem ser solicitadas via RFC). Observe que a conectividade entre a WorkSpaces VPC e a VPC do MALZ Shared Services executando o AD gerenciado pelo AMS é estabelecida por meio do Transit Gateway.

     Para obter mais informações, consulte Melhores práticas para implantar a Amazon WorkSpaces (cenário 6).

> **Note**
>
> O AD Connector pode ser configurado enviando um RFC Management | Other | Other | Create Change Type com os detalhes de configuração do AD necessários; para obter mais informações, consulte Create an AD Connector. Se o método 2 for usado para criar uma floresta de recursos no AD gerenciado pelo AMS, envie outro Gerenciamento | Outro | Outro | Crie o tipo de alteração RFC na conta de serviços compartilhados do AMS executando o AD gerenciado pelo AMS.

Use o AMS SSP para provisionar serviços do Código AMS em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos dos serviços do AMS Code diretamente em sua conta gerenciada pelo AMS. Os serviços de código do AMS são um pacote proprietário dos serviços de gerenciamento de código da AWS, conforme detalhado a seguir. Você pode optar por implantar todos os serviços no AMS com os serviços de código do AMS ou pode implantá-los no AMS individualmente.

Os serviços do Código AMS incluem os seguintes serviços:

- AWS CodeCommit: um serviço de controle de origem totalmente gerenciado que hospeda repositórios seguros baseados em Git. Isso permite que as equipes possam colaborar no código em um ecossistema seguro e altamente escalável. CodeCommit elimina a necessidade de operar seu próprio sistema de controle de origem ou a preocupação com a escalabilidade de sua infraestrutura. Você pode usar o CodeCommit para armazenar com segurança quaisquer dados, de códigos-fonte a binários. Além disso, ele funciona perfeitamente com as ferramentas de Git existentes. Para saber mais, consulte AWS CodeCommit

  Para implantar isso em sua conta AMS independentemente dos serviços do Código AMS, consulteUse o AMS SSP para provisionar AWS CodeCommit em sua conta AMS.
- AWS CodeBuild: um serviço de integração contínua totalmente gerenciado que compila o código-fonte, executa testes e produz pacotes de software prontos para implantação. Com CodeBuild, você não precisa provisionar, gerenciar e escalar seus próprios servidores de compilação. CodeBuild escala continuamente e processa várias compilações simultaneamente, para que suas compilações não fiquem esperando em uma fila. Você pode começar a usar ambientes de compilação pré-empacotados rapidamente ou criar ambientes de compilação personalizados que

usem suas próprias ferramentas de compilação. Com CodeBuild, você é cobrado por minuto pelos recursos computacionais que usa. Para saber mais, consulte AWS CodeBuild

Para implantar isso em sua conta AMS independentemente dos serviços do Código AMS, consulteUse o AMS SSP para provisionar AWS CodeBuild em sua conta AMS.

- AWS CodeDeploy: Um serviço de implantação totalmente gerenciado que automatiza as implantações de software em uma variedade de serviços de computação, como a Amazon EC2 e seus servidores locais. AWS CodeDeploy ajuda você a lançar rapidamente novos recursos, ajuda a evitar o tempo de inatividade durante a implantação do aplicativo e lida com a complexidade da atualização de seus aplicativos. Você pode usar AWS CodeDeploy para automatizar implantações de software, eliminando a necessidade de operações manuais propensas a erros. O serviço é dimensionado para atender às suas necessidades de implantação. Para saber mais, consulte AWS CodeDeploy

  Para implantar isso em sua conta AMS independentemente dos serviços do Código AMS, consulteUse o AMS SSP para provisionar AWS CodeDeploy em sua conta AMS.
- AWS CodePipeline: Um serviço de entrega contínua totalmente gerenciado que ajuda você a automatizar seus pipelines de lançamento para atualizações rápidas e confiáveis de aplicativos e infraestrutura. CodePipeline automatiza as fases de criação, teste e implantação do seu processo de lançamento sempre que houver uma alteração no código, com base no modelo de lançamento que você define. Isso permite entregar recursos e atualizações de forma rápida e confiável. Você pode se integrar facilmente AWS CodePipeline a serviços de terceiros, como GitHub ou com seu próprio plug-in personalizado. Com AWS CodePipeline, você paga apenas pelo que usa. Não há tarifas antecipadas nem compromissos de longo prazo. Para saber mais, consulte AWS CodePipeline

  Para implantar isso em sua conta AMS independentemente dos serviços do Código AMS, consulteUse o AMS SSP para provisionar AWS CodePipeline em sua conta AMS.

Perguntas frequentes sobre serviços de código AMS no AWS Managed Services

P: Como solicito acesso aos serviços do Código AMS na minha conta AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_code_suite_console_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação. Nesse momento, o AMS

Operations também implantará as funções `aws_code_pipeline_service_role` de serviço `customer_codebuild_service_rolecustomer_codedeploy_service_role`, CodeBuild, em sua conta CodeDeploy e CodePipeline serviços. Se forem necessárias permissões adicionais do IAM para `ocustomer_codebuild_service_role`, envie uma solicitação de serviço do AMS.

> **Note**
>
> Você também pode adicionar esses serviços separadamente; para obter informaçõesUse o AMS SSP para provisionar AWS CodeBuild em sua conta AMS, consulteUse o AMS SSP para provisionar AWS CodeDeploy em sua conta AMS, eUse o AMS SSP para provisionar AWS CodePipeline em sua conta AMS, respectivamente.

P: Quais são as restrições ao uso dos serviços do Código AMS na minha conta AMS?

- AWS CodeCommit: O recurso de gatilhos ativado CodeCommit está desativado devido aos direitos associados à criação de tópicos do SNS. A autenticação direta CodeCommit é restrita; os usuários devem se autenticar com o Credential Helper. Alguns comandos do KMS também são restritos: kms: Criptografar, kms: Descriptografar,,, e. kms: ReEncrypt kms: GenereteDataKey kms: GenerateDataKeyWithoutPlaintext kms: DescribeKey
- CodeBuild: para o acesso do administrador do AWS CodeBuild console, as permissões são limitadas no nível do recurso; por exemplo, CloudWatch as ações são limitadas em recursos específicos e a `iam:PassRole` permissão é controlada.
- CodeDeploy: Atualmente, CodeDeploy oferece suporte a implantações somente na EC2 Amazon/no local. Implantações em ECS e Lambda por meio CodeDeploy de não são suportadas.
- CodePipeline: CodePipeline recursos, estágios e fornecedores estão limitados ao seguinte:
  - Etapa de implantação: Amazon S3 e AWS CodeDeploy
  - Estágio de origem: Amazon S3 AWS CodeCommit, Bit Bucket e GitHub
  - Estágio de construção: AWS CodeBuild e Jenkins
  - Estágio de aprovação: Amazon SNS
  - Estágio de teste: Jenkins AWS CodeBuild BlazeMeter, teste de interface do usuário do Ghost Inspector, Micro StormRunner Focus Load, monitoramento da API Runscope
  - Invoke Stage: Step Functions e Lambda

> **Note**
>
> O AMS Operations implanta o `customer_code_pipeline_lambda_policy` em sua conta; ele deve estar vinculado à função de execução do Lambda para o estágio de invocação do Lambda. Forneça o nome da service/execution função Lambda com a qual você deseja que essa política seja adicionada. Se não houver uma service/execution função personalizada do Lambda, o AMS cria uma nova função chamada`customer_code_pipeline_lambda_execution_role`, que é uma cópia de `customer_lambda_basic_execution_role` junto com. `customer_code_pipeline_lambda_policy`

P: Quais são os pré-requisitos ou dependências para usar os serviços do Código AMS na minha conta AMS?

- CodeCommit: se os buckets do S3 estiverem criptografados com AWS KMS chaves, é necessário usar o S3 e AWS KMS o S3. AWS CodeCommit
- CodeBuild: se forem necessárias permissões adicionais do IAM para a função de AWS CodeBuild serviço definida, solicite-as por meio de uma solicitação de serviço do AMS.
- CodeDeploy: Nenhum.
- CodePipeline: Nenhum. AWS os serviços suportados—AWS CodeCommit AWS CodeBuild,, AWS CodeDeploy—devem ser lançados antes ou junto com o lançamento do CodePipeline. No entanto, isso é feito por um engenheiro da AMS.

Use o AMS SSP para provisionar AWS Amplify em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Amplify recursos diretamente em sua conta gerenciada pelo AMS. AWS Amplify É uma solução completa que permite que desenvolvedores front-end web e móveis criem, conectem e hospedem facilmente aplicativos fullstack. O Amplify oferece flexibilidade para aproveitar a variedade de AWS serviços à medida que seus casos de uso evoluem. O Amplify fornece produtos para criar aplicativos completos para iOS, Android, Flutter, Web e React Native. Para saber mais, consulte AWS Amplify.

AWS Amplify perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço AWS Amplify para solicitar a configuração na minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_amplify_console_role`. Depois de provisionado para sua conta, você deve integrar a função em sua solução de federação.

Além disso, você deve fornecer uma aceitação de risco porque AWS Amplify tem permissões de mutação de infraestrutura. Para fazer isso, trabalhe com seu Cloud Service Delivery Manager (CSDM).

P: Quais são as restrições de uso AWS Amplify na minha conta AMS?

Você deve usar `'amplify*'` como prefixo para seus buckets ao trabalhar com o Amplify, a menos que RA e especifique o contrário.

P: Quais são os pré-requisitos ou dependências para usar AWS Amplify na minha conta do AMS?

Não há pré-requisitos para o uso de AWS Amplify em sua conta do AMS.

Somente ambientes Malz: a função integrada padrão do Amplify é “customer_amplify_console_role”. Para usar um papel personalizado, primeiro implante as entidades do IAM. Em seguida, crie uma RFC adicional para adicionar sua função personalizada à lista de permissões da Política de Controle de Serviços para Contas de Aplicativos.

Use o AMS SSP para provisionar AWS AppSync

Use o modo AMS Self-Service Provisioning (SSP) para acessar AWS AppSync recursos diretamente em sua conta gerenciada pelo AMS. AWS AppSync simplifica o desenvolvimento de aplicativos ao permitir que você crie uma API flexível para acessar, manipular e combinar dados de uma ou mais fontes de dados com segurança. AWS AppSync é um serviço gerenciado que usa o GraphQL para facilitar que os aplicativos obtenham exatamente os dados de que precisam.

Com AWS AppSync, você pode criar aplicativos escaláveis, incluindo aqueles que exigem atualizações em tempo real, em uma variedade de fontes de dados, como armazenamentos de dados NoSQL, bancos de dados relacionais, APIs HTTP e suas fontes de dados personalizadas com. AWS Lambda Para aplicativos móveis e da web, AWS AppSync também fornece acesso local aos dados quando os dispositivos ficam off-line e sincronização de dados com resolução de conflitos personalizável quando eles estão online novamente. Para saber mais, consulte AWS AppSync.

AWS AppSync perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS AppSync minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Essa RFC provisiona as seguintes funções do IAM para sua conta: `customer_appsync_service_role` e. `customer_appsync_author_role` Depois de provisionado em sua conta, você deve integrá-lo à `customer_appsync_author_role` sua solução de federação.

P: Quais são as restrições ao uso do AWS AppSync?

- Ao criar uma fonte de dados sobre AppSync a necessidade do cliente especificar a função de serviço criada anteriormente, a criação de uma nova função não é permitida e, portanto, retornará um acesso negado.
- AppSync as funções são configuradas para restringir as permissões aos recursos que contêm os prefixos 'AMS-' ou 'MC-' para evitar modificações na infraestrutura do AMS.

P: Quais são os pré-requisitos ou dependências do uso? AWS AppSync

O serviço permite que vários outros serviços sejam usados como fonte de dados.
As permissões básicas para usá-los como tal estão incluídas na função de serviço (`customer_appsync_service_role`), mas você deve selecionar manualmente a função de serviço ao usar o serviço.

Use o AMS SSP para provisionar AWS App Mesh em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS App Mesh recursos diretamente em sua conta gerenciada pelo AMS. AWS App Mesh fornece rede em nível de aplicativo para facilitar a comunicação entre seus serviços em vários tipos de infraestrutura computacional. O App Mesh padroniza a forma como seus serviços se comunicam, oferecendo end-to-end visibilidade e garantindo alta disponibilidade para seus aplicativos.

AWS App Mesh facilita a execução de serviços, fornecendo visibilidade consistente e controles de tráfego de rede para serviços criados em vários tipos de infraestrutura computacional. O App Mesh elimina a necessidade de atualizar o código do aplicativo para alterar a forma como os dados de monitoramento são coletados ou o tráfego é roteado entre os serviços. O App Mesh configura cada

serviço para exportar dados de monitoramento e implementa uma lógica de controle de comunicação consistente em todo o seu aplicativo. Isso facilita a identificação rápida da localização exata dos erros e o redirecionamento automático do tráfego da rede quando há falhas ou quando mudanças de código precisam ser implantadas. Para saber mais, consulte AWS App Mesh.

AWS App Mesh perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS App Mesh minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_app_mesh_console_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do AWS App Mesh?

A funcionalidade completa do AWS App Mesh está disponível em sua conta AMS.

P: Quais são os pré-requisitos ou dependências do uso? AWS App Mesh

Não há pré-requisitos ou dependências para usar AWS App Mesh em sua conta do AMS.

Use o AMS SSP para provisionar AWS Audit Manager em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Audit Manager diretamente em sua conta gerenciada pelo AMS. O Audit Manager ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você avalia o risco e a conformidade com os regulamentos e padrões do setor. O Audit Manager automatiza a coleta de evidências para tornar mais fácil avaliar se suas políticas, procedimentos e atividades estão funcionando de modo eficaz. Quando chega a hora de fazer uma auditoria, o Audit Manager ajuda você a gerenciar as revisões de seus controles pelas partes interessadas e ajuda a criar relatórios prontos para auditoria com muito menos esforço manual. Para saber mais, consulte Audit Manager.

AWS Audit Manager perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS Audit Manager minha conta AMS?

Você pode solicitar acesso por meio do envio dos AWS Serviços RFC Management | AWS service | Self-provisioned service | Add (revisão obrigatória) (ct-3qe6io8t6jtny). Este RFC provisiona a seguinte função do IAM em sua conta:`customer-audit-manager-admin-Role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições de uso AWS Audit Manager?

Não há restrições para o uso de AWS Audit Manager em sua conta AMS. A funcionalidade completa AWS Audit Manager é fornecida.

P: Quais são os pré-requisitos ou dependências do uso? AWS Audit Manager

1. Você precisa fornecer ao AMS o bucket s3 em que deseja reports/assessments residir.
2. Se você quiser ter criptografia com o serviço, precisará fornecer ao AMS o ARN da CMK do KMS para usar.
3. Se quiser enviar notificações de SNS para um tópico, você deve fornecer o nome do tópico ou arn.
4. (Opcional) Há um pré-requisito adicional se você quiser habilitar Organizations como parte de sua landing zone de várias contas no Audit Manager e quiser uma conta de administrador delegado: no campo de descrição do RFC (Management | AWS service | Compatible Service | Add), mencione que você deseja usar a conta de administrador delegado como parte da configuração do Audit Manager e forneça os detalhes abaixo:
   - KMS CMK ARN (usado inicialmente para configurar o Audit Manager)
   - ID da conta de administrador delegado para o Audit Manager usar como parte dessa landing zone de várias contas (pode ser uma conta do aplicativo MALZ)

Use o AMS SSP para provisionar AWS Batch em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Batch recursos diretamente em sua conta gerenciada pelo AMS. AWS Batch permite que desenvolvedores, cientistas e engenheiros executem com facilidade e eficiência centenas de milhares de trabalhos de computação em lotes no AWS. AWS Batch provisiona dinamicamente a quantidade e o tipo ideais de recursos computacionais (como instâncias otimizadas para CPU ou memória) com base no volume e nos requisitos de recursos específicos dos trabalhos em lote enviados. Com AWS Batch, não há necessidade de instalar e gerenciar software de computação em lote ou clusters de servidores que você usa para executar seus trabalhos, permitindo que você se concentre na análise de resultados e na solução de problemas. Para saber mais, consulte AWS Batch.

AWS Batch perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS Batch minha conta do AMS?

1. Para solicitar acesso a AWS Batch, envie o serviço RFC Management | AWS | Self-provisioned service | Add (ct-1w8z66n899dct). Essa RFC provisiona as seguintes funções e políticas do IAM em sua conta:

Funções do IAM:

- `customer_batch_console_role`
- `customer_batch_ecs_instance_role`
- `customer_batch_events_service_role`
- `customer_batch_service_role`
- `customer_batch_ecs_task_role`

Políticas:

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`
- `customer_batch_events_service_role_policy`

2. Depois de provisionado em sua conta, você deve integrar a função `customer_batch_console_role` em sua solução de federação.

P: Quais são as restrições de uso AWS Batch?

Ao criar o ambiente de computação, você deve marcar as EC2 instâncias como “customer_batch” ou “customer-batch”. Se as instâncias não forem marcadas, as instâncias não serão encerradas em lote quando o trabalho for concluído.

P: Quais são os pré-requisitos ou dependências do uso? AWS Batch

Não há pré-requisitos ou dependências para usar AWS Batch em sua conta do AMS.

Use o AMS SSP para provisionar AWS Certificate Manager em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos AWS Certificate Manager (ACM) diretamente em sua conta gerenciada pelo AMS. AWS Certificate Manager é um serviço que permite provisionar, gerenciar e implantar certificados Secure Layer/Transport Sockets Layer Security (SSL/TLS) públicos e privados para uso com AWS serviços e seus recursos internos conectados. SSL/TLS os certificados são usados para proteger as comunicações de rede e estabelecer a identidade de sites na Internet, bem como recursos em redes privadas. AWS Certificate Manager elimina o demorado processo manual de compra, upload e renovação SSL/TLS de certificados.

Com isso AWS Certificate Manager, você pode solicitar um certificado, implantá-lo em AWS recursos integrados ao ACM, como Elastic Load Balancers, CloudFront distribuições da Amazon e no API APIs Gateway, e deixar AWS Certificate Manager que os certificados sejam renovados. Ele também permite que você crie certificados privados para seus recursos internos e gerencie o ciclo de vida do certificado de forma centralizada. Os certificados públicos e privados provisionados AWS Certificate Manager para uso com serviços integrados ao ACM são gratuitos. Você paga somente pelos AWS recursos criados para executar seu aplicativo. Com Autoridade de Certificação Privada da AWS, você paga mensalmente pela operação CA privada da AWS e pelos certificados privados emitidos. Para saber mais, consulte AWS Certificate Manager - AWS Documentação.

Perguntas frequentes sobre o ACM no AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS Certificate Manager minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_acm_create_role`. Você pode usar essa função para criar e gerenciar certificados ACM. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

Os certificados do ACM podem ser criados usando os seguintes tipos de alteração, mesmo que você não tenha adicionado a função do `customer_acm_create_role` IAM:

- ACM | Criar certificado público
- ACM | Criar certificado privado

- Certificado ACM com adicional SANs | Criar

P: Quais são as restrições ao uso do AWS Certificate Manager?

Você deve enviar uma Solicitação de Alteração (RFC) ao AMS para excluir ou modificar certificados existentes, pois essas ações exigem acesso total do administrador (use o tipo de alteração Gerenciamento | Outros | Outros | Atualizar (ct-0xdawir96cy7k). Observe que a política do IAM não pode excluir direitos com base nos nomes das tags (mc*, ams* etc.). Os certificados não têm custos, portanto, a exclusão de certificados não utilizados não é urgente.

P: Quais são os pré-requisitos ou dependências para usar o Certificate Manager?

Nome DNS público existente e acesso para criar registros DNS CNAME, mas eles não precisam estar hospedados na conta gerenciada.

Use o AMS SSP para provisionar Autoridade de Certificação Privada da AWS em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os Autoridade de Certificação Privada da AWS recursos diretamente em sua conta gerenciada pelo AMS. Os certificados privados são usados para identificar e proteger a comunicação entre recursos conectados em redes privadas, como servidores, dispositivos móveis e aplicativos de IoT. CA privada da AWS é um serviço gerenciado de CA privada que ajuda você a gerenciar com facilidade e segurança o ciclo de vida de seus certificados privados. CA privada da AWS fornece um serviço de CA privada de alta disponibilidade sem o investimento inicial e os custos de manutenção contínuos de operar sua própria CA privada. CA privada da AWS estende os recursos de gerenciamento de certificados do ACM para certificados privados, permitindo que você crie e gerencie certificados públicos e privados de forma centralizada. Você pode criar e implantar facilmente certificados privados para seus AWS recursos usando o AWS Management Console ou a API do ACM. Para EC2 instâncias, contêineres, dispositivos de IoT e recursos locais, você pode criar e rastrear facilmente certificados privados e usar seu próprio código de automação do lado do cliente para implantá-los. Você também tem a flexibilidade de criar certificados privados e gerenciá-los você mesmo para aplicativos que exigem tempos de vida de certificados personalizados, algoritmos-chave ou nomes de recursos. Para saber mais, consulte CA privada da AWS.

CA privada da AWS perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à CA privada da AWS minha conta do AMS?

Solicite acesso por meio do envio do RFC de AWS Serviços (Gerenciamento | AWS serviço | Serviço compatível). Por meio dessa RFC, a seguinte função do IAM será provisionada em sua conta:. `customer_acm_pca_role` Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do CA privada da AWS?

Atualmente, AWS Resource Access Manager (AWS RAM) não pode ser usado para compartilhar sua CA privada da AWS conta cruzada.

P: Quais são os pré-requisitos ou dependências do uso? CA privada da AWS

1. Se você planeja criar uma CRL, precisará de um bucket do S3 para armazená-la. CA privada da AWS deposita automaticamente a CRL no bucket do Amazon S3 que você designar e a atualiza periodicamente. É um pré-requisito que o bucket do S3 tenha a política de bucket abaixo antes que você possa configurar uma CRL. Para continuar com essa solicitação, crie um RFC com ct-0fpjlxa808sh2 (Gerenciamento | Componentes avançados de pilha | Armazenamento S3 | Política de atualização) da seguinte forma:

- Forneça o nome ou ARN do bucket do S3.
- Copie a política abaixo no RFC e `bucket-name` substitua pelo nome do bucket S3 desejado.

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. Se o bucket do S3 acima estiver criptografado, o responsável pelo serviço acm-pca.amazonaws.com precisará de permissões para descriptografar. Para continuar com essa solicitação, crie um RFC com ct-3ovo7px2vsa6n (Gerenciamento | Componentes avançados da pilha | Chave KMS | Atualização) da seguinte forma:

- Forneça o ARN da chave KMS no qual a política deve ser atualizada.
- Copie a política abaixo no RFC e `bucket-name` substitua pelo nome do bucket S3 desejado.

```
{
   "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. CA privada da AWS CRLs não suportam a configuração do S3 “Bloquear acesso público a buckets e objetos concedidos por meio de novas listas de controle de acesso (ACLs)”. Você deve desabilitar

essa configuração com a conta e o bucket do S3 para permitir a CA privada da AWS gravação, CRLs conforme mencionado em Como criar e armazenar com segurança sua CRL para a CA privada do ACM. Se quiser desativá-la, crie uma nova RFC com ct-0xdawir96cy7k (Gerenciamento | Outros | Outros | Atualização) e anexe uma Aceitação de Risco. Se você tiver alguma dúvida sobre aceitação de riscos, entre em contato com seu arquiteto de nuvem.

Use o AMS SSP para provisionar AWS CloudEndure em sua conta AMS

> **Note**
>
> Após o lançamento bem-sucedido do AWS Application Migration Service, o serviço de CloudEndure migração está encerrado em todas as AWS regiões. Recomendamos que os clientes AWS Application Migration Service o usem para migrações de elevador e turno para GovCloud regiões e regiões comerciais. Para obter informações, consulte O que é AWS Application Migration Service? .
> Se você quiser usar o AWS Application Migration Service, entre em contato com seu CA para que eles possam orientá-lo.

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS CloudEndure recursos diretamente em sua conta gerenciada pelo AMS. AWS CloudEndure a migração simplifica, agiliza e automatiza migrações em grande escala da infraestrutura física, virtual e baseada em nuvem para o. AWS CloudEndure O Disaster Recovery (DR) protege contra o tempo de inatividade e a perda de dados de qualquer ameaça, incluindo ransomware e corrupção do servidor.

AWS CloudEndure perguntas frequentes sobre o AWS Managed Services

P: Como faço para solicitar acesso à CloudEndure minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona o seguinte usuário do IAM para sua conta:`customer_cloud_endure_user`. Depois de provisionada em sua conta, a chave de acesso e a chave secreta do usuário são compartilhadas no AWS Secrets Manager.

Essas políticas também são provisionadas para a conta: e. `customer_cloud_endure_policy` `customer_cloud_endure_deny_policy`

Além disso, você deve fornecer uma aceitação de risco, pois a solução de CloudEndure DR para integração de aplicativos tem permissões que alteram a infraestrutura. Para fazer isso, trabalhe com seu gerente de entrega de serviços em nuvem (CSDM).

P: Quais são as restrições de uso CloudEndure na minha conta AMS?

As instâncias de replicação e conversão duradouras na nuvem só podem ser iniciadas na sub-rede que você indicar.

P: Quais são os pré-requisitos ou dependências para usar CloudEndure na minha conta do AMS? Compartilhe o seguinte por meio de correspondência bidirecional RFC:

- Detalhes da sub-rede VPC para instâncias de replicação e conversão a serem lançadas.
- A chave KMS Amazon Resource Name (ARN) se os volumes do EBS estiverem criptografados.

Use o AMS SSP para provisionar AWS CloudHSM em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS CloudHSM recursos diretamente em sua conta gerenciada pelo AMS. AWS CloudHSM ajuda você a atender aos requisitos de conformidade corporativa, contratual e regulatória para segurança de dados usando instâncias dedicadas do Módulo de Segurança de Hardware (HSM) na AWS nuvem. AWS, e os parceiros do AWS Marketplace oferecem uma variedade de soluções para proteger dados confidenciais na AWS plataforma, mas para alguns aplicativos e dados sujeitos a exigências contratuais ou regulatórias para o gerenciamento de chaves criptográficas, proteção adicional pode ser necessária. AWS CloudHSM complementa as soluções de proteção de dados existentes e permite que você proteja suas chaves de criptografia HSMs que são projetadas e validadas de acordo com os padrões governamentais para o gerenciamento seguro de chaves. AWS CloudHSM permite gerar, armazenar e gerenciar com segurança as chaves criptográficas usadas para criptografia de dados, de forma que as chaves sejam acessíveis somente por você. Para saber mais, consulte AWS CloudHSM.

AWS CloudHSM perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS CloudHSM minha conta do AMS?

A utilização de em sua conta AMS é um processo de duas etapas:

1. Solicite um AWS CloudHSM cluster. Faça isso enviando um RFC com o tipo de alteração Management | Other | Other | Create (ct-1e1xtak34nx76). Inclua os seguintes detalhes:
   - AWS Região.
   - ID/ARN. Provide a VPC ID/VPCARN da VPC que está na mesma conta da RFC que você envia.
   - Especifique pelo menos duas zonas de disponibilidade para o cluster.
   - ID de EC2 instância da Amazon que se conectará ao cluster do HSM.
2. Acesse o AWS CloudHSM console. Faça isso enviando uma RFC com o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_cloudhsm_console_role`.

Depois que a função for provisionada em sua conta, você deverá integrá-la à sua solução de federação.

P: Quais são as restrições de uso AWS CloudHSM na minha conta AMS?

O acesso ao AWS CloudHSM console não permite que você crie, encerre ou restaure seu cluster. Para fazer essas coisas, envie um tipo de alteração Management | Other | Other | Create change type (ct-1e1xtak34nx76).

P: Quais são os pré-requisitos ou dependências para usar AWS CloudHSM na minha conta do AMS?

Você deve permitir o tráfego TCP usando a porta 2225 por meio de uma EC2 instância cliente da Amazon em uma VPC ou usar o Direct Connect VPN para servidores locais que desejam acessar o cluster do HSM. AWS CloudHSM depende da Amazon EC2 para grupos de segurança e interfaces de rede. Para monitoramento ou auditoria de registros, o HSM conta com CloudTrail (operações de AWS API) e CloudWatch registros para todas as atividades do dispositivo HSM local.

P: Quem aplicará as atualizações ao AWS CloudHSM cliente e às bibliotecas de software relacionadas?

Você é responsável por aplicar as atualizações da biblioteca e do cliente. Você deve monitorar a página do histórico de versões do CloudHSM para ver os lançamentos e, em seguida, aplicar as atualizações usando o upgrade do cliente CloudHSM.

> **Note**
>
> Os patches de software para o dispositivo HSM são sempre aplicados automaticamente pelo AWS CloudHSM serviço.

Use o AMS SSP para provisionar AWS CodeBuild em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS CodeBuild recursos diretamente em sua conta gerenciada pelo AMS. AWS CodeBuild é um serviço de integração contínua totalmente gerenciado que compila o código-fonte, executa testes e produz pacotes de software prontos para implantação. Com CodeBuild, você não precisa provisionar, gerenciar e escalar seus próprios servidores de compilação. CodeBuild escala continuamente e processa várias compilações simultaneamente, para que suas compilações não fiquem esperando em uma fila. Você pode começar a usar ambientes de compilação pré-empacotados rapidamente ou criar ambientes de compilação personalizados que usem suas próprias ferramentas de compilação. Com CodeBuild, você é cobrado por minuto pelos recursos computacionais que usa. Para saber mais, consulte AWS CodeBuild.

> **Note**
>
> Para integrar CodeCommit, CodeBuild, e CodePipeline com um único RFC CodeDeploy, envie o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) e solicite os três serviços: e. CodeBuild CodeDeploy CodePipeline Em seguida, todas as três funções`customer_codebuild_service_role`,`customer_codedeploy_service_role`, e `aws_code_pipeline_service_role` são provisionadas em sua conta. Depois de provisionar sua conta, você deve integrar a função em sua solução de federação.

CodeBuild perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS CodeBuild minha conta AMS?

A utilização de AWS CodeBuild em sua conta AMS é um processo de duas etapas:

1. Provisione o processo de criação `CodeBuild Service Role` para coordenar com buckets AWS S3, Amazon e grupos Log CloudWatch
2. Solicitar acesso ao CodeBuild console

Você pode solicitar que ambos sejam configurados em sua conta do AMS enviando uma RFC com o Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições de uso AWS CodeBuild na minha conta AMS?

Para o acesso do administrador do AWS CodeBuild console, as permissões são limitadas no nível do recurso; por exemplo, CloudWatch as ações são limitadas em recursos específicos e a `iam:PassRole` permissão é controlada.

P: Quais são os pré-requisitos ou dependências para usar CodeBuild na minha conta do AMS?

Se forem necessárias permissões adicionais do IAM para a função de AWS CodeBuild serviço definida, solicite-as por meio de uma solicitação de serviço do AMS.

Use o AMS SSP para provisionar AWS CodeCommit em sua conta AMS

> **Note**
>
> AWS encerrou o acesso de novos clientes ao AWS CodeCommit, a partir de 25 de julho de 2024. AWS CodeCommit os clientes existentes podem continuar usando o serviço normalmente. AWS continua investindo em melhorias de segurança, disponibilidade e desempenho AWS CodeCommit, mas não planejamos introduzir novos recursos. Para migrar repositórios AWS CodeCommit Git para outros provedores de Git, entre em contato com seu arquiteto de nuvem (CA) para obter orientação. Para obter mais informações sobre como migrar seus repositórios Git, consulte Como migrar seu CodeCommit repositório AWS para outro provedor Git.

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS CodeCommit recursos diretamente em sua conta gerenciada pelo AMS. AWS CodeCommit é um serviço de controle de origem totalmente gerenciado que hospeda repositórios seguros baseados em Git. Ele ajuda as equipes a colaborar no código em um ecossistema seguro e altamente escalável. CodeCommit

elimina a necessidade de operar seu próprio sistema de controle de origem ou a preocupação com a escalabilidade de sua infraestrutura. Você pode usar CodeCommit para armazenar com segurança qualquer coisa, desde código-fonte até binários, e funciona perfeitamente com suas ferramentas Git existentes. Para saber mais, consulte AWS CodeCommit.

> **Note**
>
> Para integrar CodeCommit, CodeBuild, e CodePipeline com um único RFC CodeDeploy, envie o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) e solicite os três serviços: e. CodeBuild CodeDeploy CodePipeline Em seguida, todas as três funções`customer_codebuild_service_role`,`customer_codedeploy_service_role`, e `aws_code_pipeline_service_role` são provisionadas em sua conta. Depois de provisionar sua conta, você deve integrar a função em sua solução de federação.

CodeCommit perguntas frequentes sobre o AWS Managed Services

P: Como faço para solicitar acesso à CodeCommit minha conta do AMS?

AWS CodeCommit as funções de console e acesso a dados podem ser solicitadas por meio do envio de dois AWS serviços RFCs, acesso ao console e acesso a dados:

- Solicite acesso AWS CodeCommit enviando um RFC com o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_codecommit_console_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

  O acesso aos dados (como listas de treinamento e de entidades) exige uma separação CTs para cada fonte de dados, especificando a fonte de dados do S3 (obrigatório), o bucket de saída (obrigatório) e o KMS (opcional). Não há limitações para a criação de AWS CodeCommit empregos, desde que todas as fontes de dados tenham recebido funções de acesso. Para solicitar acesso aos dados, envie um RFC com o Management | Other | Other | Create (ct-1e1xtak34nx76).

P: Quais são as restrições de uso AWS CodeCommit na minha conta AMS?

O recurso de gatilhos ativado CodeCommit está desativado devido aos direitos associados à criação de tópicos do SNS. A autenticação direta contra CodeCommit é restrita; os usuários

devem se autenticar com o Credential Helper. Alguns comandos do KMS também são restritos: `kms:Encryptkms:Decrypt`,`kms:ReEncrypt`,`kms:GenereteDataKey`,`kms:GenerateDataKeyWithou` e. `kms:DescribeKey`

P: Quais são os pré-requisitos ou dependências para usar AWS CodeCommit na minha conta do AMS?

Se os buckets do S3 forem criptografados com chaves KMS, será necessário usar o S3 e o KMS. AWS CodeCommit

Use o AMS SSP para provisionar AWS CodeDeploy em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS CodeDeploy recursos diretamente em sua conta gerenciada pelo AMS. AWS CodeDeploy é um serviço de implantação totalmente gerenciado que automatiza implantações de software em uma variedade de serviços de computação, como Amazon EC2,, AWS Fargate AWS Lambda, e seus servidores locais. AWS CodeDeploy ajuda você a lançar rapidamente novos recursos, ajuda a evitar o tempo de inatividade durante a implantação do aplicativo e lida com a complexidade da atualização de seus aplicativos. Você pode usar AWS CodeDeploy para automatizar implantações de software, eliminando a necessidade de operações manuais propensas a erros. O serviço é dimensionado para atender às suas necessidades de implantação. Para saber mais, consulte AWS CodeDeploy.

> **Note**
>
> Para integrar CodeCommit, CodeBuild, e CodePipeline com um único RFC CodeDeploy, envie o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) e solicite os três serviços: e. CodeBuild CodeDeploy CodePipeline Em seguida, todas as três funções`customer_codebuild_service_role`,`customer_codedeploy_service_role`, e `aws_code_pipeline_service_role` são provisionadas em sua conta. Depois de provisionar sua conta, você deve integrar a função em sua solução de federação.

CodeDeploy perguntas frequentes sobre o AWS Managed Services

P: Como faço para solicitar acesso à CodeDeploy minha conta do AMS?

Solicite acesso ao CodeDeploy enviando uma RFC com o serviço Management | AWS | Self-provisioned service | Adicionar (ct-1w8z66n899dct) tipo de alteração. Essa RFC provisiona

as seguintes funções do IAM para sua conta: `customer_codedeploy_console_role` e. `customer_codedeploy_service_role` Depois de provisionado em sua conta, você deve integrar a `customer_codedeploy_console_role` função em sua solução de federação.

P: Quais são as restrições de uso CodeDeploy na minha conta AMS?

Atualmente, oferecemos suporte apenas à Compute Platform como — EC2 Amazon/On-Premises. Blue/Green Não há suporte para implantações.

P: Quais são os pré-requisitos ou dependências para usar CodeDeploy na minha conta do AMS?

Não há pré-requisitos ou dependências para usar CodeDeploy em sua conta do AMS.

Use o AMS SSP para provisionar AWS CodePipeline em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS CodePipeline recursos diretamente em sua conta gerenciada pelo AMS. AWS CodePipeline é um serviço de entrega contínua totalmente gerenciado que ajuda você a automatizar seus pipelines de lançamento para atualizações rápidas e confiáveis de aplicativos e infraestrutura. CodePipeline automatiza as fases de criação, teste e implantação do seu processo de lançamento sempre que houver uma alteração no código, com base no modelo de lançamento que você define. Isso permite entregar recursos e atualizações de forma rápida e confiável. Você pode se integrar facilmente AWS CodePipeline a serviços de terceiros, como GitHub ou com seu próprio plug-in personalizado. Com AWS CodePipeline, você paga apenas pelo que usa. Não há tarifas antecipadas nem compromissos de longo prazo. Para saber mais, consulte AWS CodePipeline.

> **Note**
>
> Para integrar CodeCommit, CodeBuild, e CodePipeline com um único RFC CodeDeploy, envie o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) e solicite os três serviços: e. CodeBuild CodeDeploy CodePipeline Em seguida, todas as três funções`customer_codebuild_service_role`,`customer_codedeploy_service_role`, e `aws_code_pipeline_service_role` são provisionadas em sua conta. Depois de provisionar sua conta, você deve integrar a função em sua solução de federação. CodePipeline no AMS, não oferece suporte a “Amazon CloudWatch Events” para o Source Stage porque precisa de permissões elevadas para criar a função e a política de serviço, o que ignora o modelo de privilégios mínimos e o processo de gerenciamento de alterações do AMS.

CodePipeline perguntas frequentes sobre o AWS Managed Services

P: Como faço para solicitar acesso à CodePipeline minha conta AMS?

Solicite acesso ao CodePipeline enviando uma solicitação de serviço para `customer_code_pipeline_console_role` a conta relevante. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

Nesse momento, o AMS Operations também implantará essa função de serviço em sua conta:`aws_code_pipeline_service_role_policy`.

P: Quais são as restrições de uso CodePipeline na minha conta AMS?

Sim. CodePipeline recursos, estágios e fornecedores estão limitados ao seguinte:

1. Estágio de implantação: limitado ao Amazon S3 e AWS CodeDeploy
2. Estágio de origem: limitado ao Amazon S3,, AWS CodeCommit, e BitBucket GitHub
3. Estágio de construção: limitado a AWS CodeBuild, e Jenkins
4. Estágio de aprovação: limitado ao Amazon SNS
5. Estágio de teste: limitado a Jenkins AWS CodeBuild, Ghost Inspector UI Testing BlazeMeter, Micro StormRunner Focus Load e Runscope API Monitoring
6. Invoke Stage: limitado a Step Functions e Lambda

> **Note**
>
> As operações do AMS serão implantadas `customer_code_pipeline_lambda_policy` em sua conta; elas devem ser vinculadas à função de execução do Lambda para o estágio de invocação do Lambda. Forneça o nome da service/execution função Lambda com a qual você deseja adicionar essa política. Se não houver uma service/execution função personalizada do Lambda, o AMS criará uma nova função chamada`customer_code_pipeline_lambda_execution_role`, que será uma cópia de `customer_lambda_basic_execution_role` junto com. `customer_code_pipeline_lambda_policy`

P: Quais são os pré-requisitos ou dependências para usar CodePipeline na minha conta do AMS?

AWS serviços suportados AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy devem ser lançados antes ou junto com o lançamento do CodePipeline.

Use o AMS SSP para provisionar AWS Compute Optimizer em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar AWS Compute Optimizer recursos diretamente em sua conta gerenciada pelo AMS. AWS Compute Optimizer recomenda recursos de AWS computação ideais para suas cargas de trabalho a fim de reduzir custos e melhorar o desempenho usando o aprendizado de máquina para analisar métricas históricas de utilização. O provisionamento excessivo da computação (EC2 Amazon e) pode levar a custos de infraestrutura desnecessários, ASGs e o provisionamento insuficiente da computação pode levar a um baixo desempenho do aplicativo. O Compute Optimizer ajuda você a escolher os tipos ideais de instância da EC2 Amazon, incluindo aquelas que fazem parte de um grupo do Amazon Auto EC2 Scaling, com base nos seus dados de utilização. Para saber mais, consulte AWS Compute Optimizer.

Perguntas frequentes sobre o Compute Optimizer no AWS Managed Services

P: Como solicito acesso ao Compute Optimizer na minha conta AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_compute_optimizer_readonly_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Compute Optimizer na minha conta AMS?

Não há restrições. A funcionalidade completa do AWS Compute Optimizer está disponível em sua conta AMS.

P: Quais são os pré-requisitos ou dependências para usar o Compute Optimizer na minha conta AMS?

- Você deve enviar um RFC (Gerenciamento | Outro | Outro | Atualização) autorizando o AMS Ops a ativar o serviço na conta. Durante a implantação, uma função vinculada ao serviço (SLR) é criada para permitir a coleta de métricas e a geração de relatórios. A SLR é rotulada como "" AWSServiceRoleForComputeOptimizer. Para obter mais informações, consulte Usando funções vinculadas ao serviço para AWS Compute Optimizer
- CloudWatch as métricas devem ser ativadas para as seguintes métricas:
  - Utilização da CPU: a porcentagem de unidades EC2 computacionais alocadas da Amazon que estão em uso na instância. Essa métrica identifica a capacidade de processamento necessária para executar um aplicativo em uma instância selecionada.

- Utilização da memória: a quantidade de memória que foi usada de alguma forma durante o período da amostra. Essa métrica identifica a memória necessária para executar um aplicativo em uma instância selecionada. A utilização da memória é analisada somente para recursos que têm o CloudWatch agente unificado instalado neles. Para obter mais informações, consulte Habilitando a utilização da memória com o CloudWatch agente (p. 10).
- Rede em: o número de bytes recebidos em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de rede de entrada para uma única instância.
- Saída de rede: o número de bytes enviados em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de rede de saída de uma única instância.
- Disco local input/output (E/S): o número de input/output operações do disco local. Essa métrica identifica o desempenho do volume raiz de uma instância

Use o AMS SSP para provisionar AWS DataSync em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS DataSync recursos diretamente em sua conta gerenciada pelo AMS. AWS DataSync move grandes quantidades de dados on-line entre o armazenamento local e o Amazon S3, o Amazon Elastic File System (Amazon Elastic File System) ou a Amazon. FSx Tarefas manuais relacionadas às transferências de dados podem retardar as migrações e sobrecarregar as operações de TI. DataSync elimina ou gerencia automaticamente muitas dessas tarefas, incluindo a criação de scripts de tarefas de cópia, o agendamento e o monitoramento de transferências, a validação de dados e a otimização da utilização da rede. O agente DataSync de software se conecta ao armazenamento do Sistema de Arquivos de Rede (NFS) e do Bloco de Mensagens do Servidor (SMB), para que você não precise modificar seus aplicativos. DataSync pode transferir centenas de terabytes e milhões de arquivos em velocidades até 10 vezes mais rápidas do que ferramentas de código aberto, pela Internet ou por links. AWS Direct Connect Você pode usar DataSync para migrar conjuntos de dados ou arquivos ativos AWS, transferir dados para a nuvem para análise e processamento oportunos ou replicar dados AWS para continuidade dos negócios.

Para saber mais, consulte AWS DataSync.

DataSync perguntas frequentes sobre o AWS Managed Services

P: Como faço para solicitar acesso à DataSync minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_datasync_console_role`.

Depois de provisionado em sua conta, você deve integrar as funções em sua solução de federação.

O grupo de CloudWatch registros a ser usado para transmitir registros de tarefas é “/aws/datasync”.

P: Quais são as restrições de uso DataSync na minha conta AMS?

A funcionalidade completa do AWS DataSync está disponível em sua conta AMS.

P: Quais são os pré-requisitos ou dependências para usar DataSync na minha conta do AMS?

- O Amazon S3 (ARNs Amazon Resource Names) é obrigatório para todos os buckets do S3 associados às DataSync tarefas que serão executadas usando a função de serviço. DataSync `customer_datasync_service_role`
- Os VPC Endpoints e os grupos de segurança para DataSync agentes devem ser solicitados com um RFC com o tipo de alteração Management | Other | Other | Create (ct-1e1xtak34nx76) antes de usar os VPC Endpoints.
- AWS DataSync os agentes são executados no AMS como um dispositivo. O AWS DataSync agente é corrigido e atualizado pelo serviço; para obter detalhes, consulte AWS DataSync Perguntas frequentes.
- Para iniciar um AWS DataSync agente, envie um RFC com o tipo de alteração Management | Other | Other | Create (ct-1e1xtak34nx76), solicitando que o agente seja implantado. Forneça o ID da AWS DataSync Amazon EC2 AMI, o tipo de instância, a sub-rede, o grupo de segurança e faça referência a um EC2 par de chaves existente da Amazon ou solicite a criação de um novo par de chaves.

> **Note**
>
> O AMS provisiona o AWS DataSync agente manualmente em nome do cliente e não exige o processo de ingestão do WIGS na Amazon AWS DataSync AMI EC2 .

Use o AMS SSP para provisionar AWS Device Farm em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Device Farm recursos diretamente em sua conta gerenciada pelo AMS. AWS Device Farm é um serviço de teste de

aplicativos que permite melhorar a qualidade de seus aplicativos móveis e da Web testando-os em uma ampla variedade de navegadores de desktop e dispositivos móveis reais, sem precisar provisionar e gerenciar nenhuma infraestrutura de teste. O serviço permite que você execute seus testes simultaneamente em vários navegadores de desktop ou dispositivos reais para acelerar a execução de sua suíte de testes e gera vídeos e registros para ajudá-lo a identificar rapidamente problemas com seu aplicativo.

Para saber mais, consulte AWS Device Farm.

AWS Device Farm perguntas frequentes sobre o AWS Managed Services

P: Como faço para solicitar acesso à AWS Device Farm minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_devicefarm_role`.

Depois de provisionado em sua conta, você deve integrar as funções em sua solução de federação.

P: Quais são as restrições de uso AWS Device Farm na minha conta AMS?

O acesso total ao AWS Device Farm serviço é fornecido, com exceção do uso do namespace AMS na tag “Nome”.

P: Quais são os pré-requisitos ou dependências para usar AWS Device Farm na minha conta do AMS?

Nenhum.

Use o AMS SSP para provisionar AWS Elastic Disaster Recovery em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar AWS Elastic Disaster Recovery recursos diretamente em sua conta gerenciada pelo AMS. AWS Elastic Disaster Recovery minimiza o tempo de inatividade e a perda de dados com a recuperação rápida e confiável de aplicativos locais e baseados na nuvem usando armazenamento acessível, computação e recuperação mínimas. point-in-time Você pode aumentar a resiliência de TI ao usar AWS Elastic Disaster Recovery para replicar aplicativos locais ou baseados em nuvem executados em sistemas operacionais compatíveis. Use o Console de gerenciamento da AWS para definir as configurações de replicação e inicialização, monitorar a replicação de dados e iniciar instâncias para exercícios ou recuperação.

Para saber mais, consulte AWS Elastic Disaster Recovery.

AWS Elastic Disaster Recovery perguntas frequentes sobre o AWS Managed Services

P: Como faço para solicitar acesso à AWS Elastic Disaster Recovery minha conta AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_drs_console_role`.

Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições de uso AWS Elastic Disaster Recovery na minha conta AMS?

Não há restrições para uso AWS Elastic Disaster Recovery em sua conta AMS.

P: Quais são os pré-requisitos ou dependências para usar AWS Elastic Disaster Recovery na minha conta do AMS?

- Depois de ter acesso à função do console, você deve inicializar o serviço Elastic Disaster Recovery para criar as funções do IAM necessárias na conta.
  - Você deve enviar o tipo de alteração Management | Applications | IAM instance profile | Create (revisão obrigatória) o tipo de alteração ct-0ixp4ch2tiu04 RFC para criar um clone do perfil da instância e anexar a política. `customer-mc-ec2-instance-profile` `AWSElasticDisasterRecoveryEc2InstancePolicy` Você deve especificar a quais máquinas anexar a nova política.
  - Se a instância não estiver usando o perfil de instância padrão, o AMS poderá se conectar `AWSElasticDisasterRecoveryEc2InstancePolicy` por meio da automação.
- Você deve usar uma chave KMS de propriedade do cliente para recuperação entre contas. A chave KMS da conta de origem deve ser atualizada de acordo com a política para permitir o acesso à conta de destino. Para obter mais informações, consulte Compartilhar a chave de criptografia do EBS com a conta de destino.
- A política de chaves do KMS deve ser atualizada para permitir `customer_drs_console_role` a visualização da política se você não quiser trocar de função para visualização.
- Para a recuperação de desastres entre contas e regiões, o AMS deve configurar a conta de origem e de destino como contas confiáveis e implantar as funções de failback e dimensionamento correto por meio AWS de. CloudFormation

Use o AMS SSP para provisionar AWS Elemental MediaConvert em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Elemental MediaConvert recursos diretamente em sua conta gerenciada pelo AMS. AWS Elemental MediaConvert é um serviço de transcodificação de vídeo baseado em arquivo com recursos de nível de transmissão. Ele permite que você crie conteúdo video-on-demand (VOD) para transmissão e entrega em várias telas em grande escala. O serviço combina recursos avançados de vídeo e áudio com uma interface e pay-as-you-go preços simples de serviços da Web. Com AWS Elemental MediaConvert, você pode se concentrar em oferecer experiências de mídia convincentes sem precisar se preocupar com a complexidade de criar e operar sua própria infraestrutura de processamento de vídeo.

Para saber mais, consulte AWS Elemental MediaConvert.

MediaConvert perguntas frequentes sobre o AWS Managed Services

P: Como faço para solicitar acesso à MediaConvert minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_mediaconvert_author_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

Uma segunda função será fornecida`customer_MediaConvert_Default_Role`, usada por para ler do bucket S3 de origem e gravar a saída MediaConvert no bucket S3 de destino, além de invocar o gateway de API caso você precise de gerenciamento de direitos digitais (DRM).

P: Quais são as restrições de uso MediaConvert na minha conta AMS?

Não há restrições para o uso do MediaConvert no AMS.

P: Quais são os pré-requisitos ou dependências para usar MediaConvert na minha conta do AMS?

Não há pré-requisitos ou dependências para usar MediaConvert em sua conta do AMS.

Use o AMS SSP para provisionar AWS Elemental MediaLive em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Elemental MediaLive recursos diretamente em sua conta gerenciada pelo AMS. AWS Elemental MediaLive é um serviço

de processamento de vídeo ao vivo de nível de transmissão. Ele permite que você crie fluxos de vídeo de alta qualidade para entrega em televisores de transmissão e dispositivos multitela conectados à Internet, como tablets TVs, smartphones e decodificadores conectados à Internet. O serviço funciona codificando suas transmissões de vídeo ao vivo em tempo real, pegando uma fonte de vídeo ao vivo de tamanho maior e compactando-a em versões menores para distribuição aos espectadores. Com AWS Elemental MediaLive, você pode configurar facilmente transmissões para eventos ao vivo e canais 24 horas por dia, 7 dias por semana, com recursos avançados de transmissão, alta disponibilidade e preços. pay-as-you-go AWS Elemental MediaLive permite que você se concentre na criação de experiências de vídeo ao vivo atraentes para seus espectadores sem a complexidade de criar e operar uma infraestrutura de processamento de vídeo de nível de transmissão.

Para saber mais, consulte AWS Elemental MediaLive.

MediaLive perguntas frequentes sobre o AWS Managed Services

P: Como faço para solicitar acesso à MediaLive minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_medialive_author_role`.

Como parte dessa RFC, uma segunda função é implantada em sua conta; `customer_medialive_service_role` função, essa função pode ser atribuída aos seus canais e entradas do Media Live para interagir com outros serviços, como Amazon S3 e Logs. MediaStore CloudWatch

Depois que as funções forem provisionadas em sua conta, você deverá integrá-las à sua solução de federação.

P: Quais são as restrições de uso MediaLive na minha conta AMS?

Não há restrições para o uso do MediaLive no AMS.

P: Quais são os pré-requisitos ou dependências para usar MediaLive na minha conta do AMS?

Não há pré-requisitos ou dependências para usar MediaLive em sua conta do AMS.

Use o AMS SSP para provisionar AWS Elemental MediaPackage em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar AWS Elemental MediaPackage recursos diretamente em sua conta gerenciada pelo AMS. AWS Elemental MediaPackage prepara e protege de forma confiável seu vídeo para entrega pela Internet. A partir de uma única entrada de vídeo, AWS Elemental MediaPackage cria fluxos de vídeo formatados para serem reproduzidos em telefones celulares TVs, computadores, tablets e consoles de jogos conectados. Isso facilita a implementação de recursos de vídeo populares para os espectadores (recomeçar, pausar, retroceder etc.), como os comumente encontrados em. DVRs AWS Elemental MediaPackage também pode proteger seu conteúdo usando o Gerenciamento de Direitos Digitais (DRM). AWS Elemental MediaPackage é dimensionado automaticamente em resposta à carga, para que seus espectadores sempre tenham uma ótima experiência sem que você precise prever com precisão a capacidade necessária.

Para saber mais, consulte AWS Elemental MediaPackage.

MediaPackage perguntas frequentes sobre o AWS Managed Services

P: Como faço para solicitar acesso à AWS Elemental MediaPackage minha conta AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_mediapackage_author_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

Uma segunda função será fornecida`customer_mediapackage_service_role`, que pode ser atribuída aos seus canais e entradas do Media Live para interagir com outros serviços, como S3 e Secrets Manager.

P: Quais são as restrições de uso MediaPackage na minha conta AMS?

Não há restrições para o uso do MediaPackage no AMS.

P: Quais são os pré-requisitos ou dependências para usar MediaPackage na minha conta do AMS?

Não há pré-requisitos ou dependências para usar MediaPackage em sua conta do AMS.

Use o AMS SSP para provisionar AWS Elemental MediaStore em sua conta AMS

> **Note**
>
> Após uma análise cuidadosa, AWS tomou a decisão de descontinuar MediaStore, a partir de 13 de novembro de 2025. Se você for um cliente ativo do MediaStore, poderá usar normalmente MediaStore até 13 de novembro de 2025, quando o suporte ao serviço será encerrado. Após essa data, você não poderá mais usar MediaStore nem nenhum dos recursos fornecidos por esse serviço.

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Elemental MediaStore recursos diretamente em sua conta gerenciada pelo AMS. AWS Elemental MediaStore é um serviço AWS de armazenamento otimizado para mídia. Ele oferece o desempenho, a consistência e a baixa latência necessários para fornecer conteúdo de vídeo ao vivo. AWS Elemental MediaStore atua como a loja de origem em seu fluxo de trabalho de vídeo. Seus recursos de alto desempenho atendem às necessidades das cargas de trabalho de entrega de mídia mais exigentes, combinados com armazenamento econômico e de longo prazo. Para saber mais, consulte AWS Elemental MediaStore.

MediaStore perguntas frequentes sobre o AWS Managed Services

P: Como faço para solicitar acesso à MediaStore minha conta do AMS?

Solicite acesso ao MediaStore enviando uma RFC com o serviço Management | AWS | Self-provisioned service | Adicionar (ct-1w8z66n899dct) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_mediastore_author_role`. Como parte dessa RFC, uma segunda função é implantada em sua conta; `MediaStoreAccessLogs` função, que é usada pelo MediaStore serviço para fazer login CloudWatch, se você optar por ativar esse recurso. Depois de provisionado em sua conta, você deve integrar as funções em sua solução de federação.

Nesse momento, o AMS Operations também implantará essa função de serviço em sua conta:`aws_code_pipeline_service_role_policy`.

P: Quais são as restrições de uso MediaStore na minha conta AMS?

Não há restrições para o uso do MediaStore no AMS.

P: Quais são os pré-requisitos ou dependências para usar MediaStore na minha conta do AMS?

Não há pré-requisitos ou dependências para usar MediaStore em sua conta do AMS.

Use o AMS SSP para provisionar AWS Elemental MediaTailor em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Elemental MediaTailor recursos diretamente em sua conta gerenciada pelo AMS. AWS Elemental MediaTailor permite que os provedores de vídeo insiram publicidade direcionada individualmente em seus streams de vídeo sem sacrificar o nível de transmissão. quality-of-service Com AWS Elemental MediaTailor, cada espectador do seu vídeo ao vivo ou sob demanda recebe uma transmissão que combina seu conteúdo com anúncios personalizados para eles. Mas, diferentemente de outras soluções de anúncios personalizados, todo o AWS Elemental MediaTailor seu stream — vídeo e anúncios — é entregue com qualidade de vídeo de nível de transmissão para melhorar a experiência de seus espectadores. AWS Elemental MediaTailor fornece relatórios automatizados com base nas métricas de entrega de anúncios do lado do cliente e do servidor, para medir com precisão as impressões publicitárias e o comportamento do espectador. Você pode monetizar facilmente eventos inesperados de visualização de alta demanda sem custos iniciais de uso. AWS Elemental MediaTailor Ele também melhora as taxas de entrega de anúncios, ajudando você a ganhar mais dinheiro com cada vídeo, e funciona com uma variedade maior de redes de entrega de conteúdo, servidores de decisão de anúncios e dispositivos clientes.

Para saber mais, consulte AWS Elemental MediaTailor.

MediaTailor perguntas frequentes sobre o AWS Managed Services

P: Como faço para solicitar acesso à MediaTailor minha conta do AMS?

Solicite acesso ao MediaTailor enviando uma RFC com o serviço Management | AWS | Self-provisioned service | Adicionar (ct-1w8z66n899dct) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer-mediatailor-role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições de uso MediaTailor na minha conta AMS?

Não há restrições para o uso do MediaTailor no AMS.

P: Quais são os pré-requisitos ou dependências para usar MediaTailor na minha conta do AMS?

Não há pré-requisitos ou dependências para usar MediaTailor em sua conta do AMS.

Use o AMS SSP para provisionar AWS Global Accelerator em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Global Accelerator diretamente em sua conta gerenciada pelo AMS. O Global Accelerator é um serviço de camada de rede no qual você cria aceleradores para melhorar a disponibilidade e o desempenho de aplicativos de Internet usados por um público global. Para saber mais, consulte Global Accelerator.

Perguntas frequentes sobre o Global Accelerator in AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito que o Global Accelerator seja configurado na minha conta AMS?

Solicite acesso por meio do envio do RFC de AWS Serviços (Gerenciamento | AWS serviço | Serviço autoprovisionado). Por meio deste RFC, as seguintes funções do IAM serão provisionadas em sua conta:. `customer_global_accelerator_console_role` Depois de provisionado em sua conta, você deve integrar a função de console em sua solução de federação.

P: Quais são as restrições ao uso do Global Accelerator na minha conta AMS?

O Global Accelerator é um serviço global que oferece suporte a endpoints em várias AWS regiões, listadas na tabela de AWS regiões.

P: Quais são os pré-requisitos ou dependências para usar o Global Accelerator na minha conta AMS?

Ao configurar seu acelerador com o Global Accelerator, você associa os endereços IP estáticos aos endpoints regionais em uma ou mais regiões. AWS Para aceleradores padrão, os endpoints são Network Load Balancers, Application Load Balancers, instâncias da EC2 Amazon ou endereços IP elásticos. Para aceleradores de roteamento personalizados, os endpoints são sub-redes de nuvem privada virtual (VPC) com uma ou mais instâncias. EC2

Use o AMS SSP para provisionar AWS Glue em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Glue recursos diretamente em sua conta gerenciada pelo AMS. AWS Glue é um serviço totalmente gerenciado de extração, transformação e carregamento (ETL) que ajuda você a preparar e carregar seus dados para análise. Você pode criar e executar uma tarefa de ETL com alguns cliques no. Console de gerenciamento da AWS Você aponta AWS Glue para seus dados armazenados em AWS, AWS Glue descobre

seus dados e armazena os metadados associados (por exemplo, definição de tabela e esquema) no. AWS Glue Data Catalog Depois de catalogados, seus dados são imediatamente pesquisáveis, consultáveis e disponíveis para ações de ETL. Para saber mais, consulte AWS Glue.

AWS Glue perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço AWS Glue para solicitar a configuração na minha conta do AMS?

Solicite acesso ao AWS Glue enviando uma RFC com o serviço Management | AWS | Self-provisioned service | Add change type (ct-1w8z66n899dct). Essa RFC provisiona as seguintes funções do IAM para sua conta:

- `customer_glue_console_role`
- `customer_glue_service_role`

As funções anteriores incluem as seguintes políticas anexadas:

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

Depois que as funções forem provisionadas em sua conta, você deverá integrá-las à sua solução de federação.

Para acessar rastreadores, tarefas e endpoints de desenvolvimento (funções necessárias para casos de uso específicos), envie uma RFC com os componentes Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entity or policy (ct-3dpd8mdd9jn1r).

P: Quais são as restrições de uso AWS Glue na minha conta AMS?

Não há restrições. A funcionalidade completa do AWS Glue está disponível em sua conta AMS. Para um ambiente interativo onde você pode criar e testar scripts ETL, use Notebooks on AWS Glue Studio. AWS Glue Interactive Sessions e Job Notebooks são recursos sem servidor AWS Glue que você pode usar AWS Glue e que fazem uso da AWS Glue função de serviço.

AWS Glue antes da versão 2.0: os AWS Glue notebooks são um recurso não gerenciado que executa EC2 instâncias da Amazon em uma conta. É uma prática recomendada lançar suas próprias EC2 instâncias da Amazon e instalar o software necessário para dar suporte ao ambiente e ao desenvolvimento de um notebook. Para obter mais informações, consulte Tutorial: Configurar

um notebook Apache Zeppelin local para testar e depurar scripts ETL e usar endpoints de desenvolvimento para desenvolver scripts.

P: Quais são os pré-requisitos ou dependências para usar AWS Glue na minha conta do AMS?

AWS Glue depende do Amazon S3 CloudWatch e do Logs. CloudWatch As dependências transitivas variam de acordo com as fontes de dados, e outros recursos do AWS Glue serviço podem estar interagindo com eles (exemplo: Amazon Redshift, Amazon RDS, Athena).

Use o AMS SSP para provisionar AWS Lake Formation em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Lake Formation recursos diretamente em sua conta gerenciada pelo AMS. AWS Lake Formation é um serviço que facilita a configuração de um data lake seguro em dias. Um data lake é um repositório centralizado, controlado e seguro que armazena todos os dados, tanto em sua forma original quanto preparados para análise. Um data lake permite que você desfaça monopólios de dados e combine diferentes tipos de análises para obter insights e orientar decisões de negócios melhores.

Criar um data lake com o Lake Formation é tão simples quanto definir fontes de dados e políticas de segurança e acesso a dados você deseja aplicar. O Lake Formation então ajuda você a coletar e catalogar dados de bancos de dados e armazenamento de objetos, mover os dados para o novo data lake do Amazon S3, limpar e classificá-los usando algoritmos de machine learning e proteger o acesso aos dados sigilosos. Seus usuários podem acessar um catálogo de dados centralizado (para obter detalhes, consulte AWS Glue Perguntas frequentes) que descreve os conjuntos de dados disponíveis e seu uso adequado. Em seguida, seus usuários aproveitam esses conjuntos de dados com serviços de análise e aprendizado de máquina de sua escolha, como Amazon Redshift, Amazon Athena e (em versão beta) Amazon EMR para Apache Spark. O Lake Formation se baseia nos recursos disponíveis em AWS Glue.

Para saber mais, consulte AWS Lake Formation.

Perguntas frequentes sobre o Lake Formation no AWS Managed Services

P: Como faço para solicitar acesso à AWS Lake Formation minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_lakeformation_data_analyst_role`. Depois de provisionado em sua conta, você deve integrar as funções em sua solução de federação.

Além disso, as duas funções a seguir são opcionais:

- `customer_lakeformation_admin_role`
- `customer_lakeformation_workflow_role`

Para obter permissões de administrador, você pode optar por integrar a função `customer_lakeformation_admin_role` como parte do mesmo tipo de alteração de SSPS (ct-3qe6io8t6jtny).

Se quiser criar Blueprints no AWS Lake Formation console, você precisa enviar um RFC Management | Other | Other (ct-1e1xtak34nx76) para implantar o. `customer_lakeformation_workflow_role` No RFC, você deve fornecer o nome do bucket do S3 se o bucket for uma origem quando os Blueprints forem criados. O bucket do S3 é aplicável se o tipo de blueprint for AWS CloudTrail Classic Load Balancer Logs ou Application Load Balancer Logs.

P: Quais são as restrições de uso AWS Lake Formation na minha conta AMS?

A funcionalidade completa do Lake Formation está disponível no AMS.

P: Quais são os pré-requisitos ou dependências para usar AWS Lake Formation na minha conta do AMS?

O Lake Formation se integra ao AWS Glue serviço, portanto, AWS Glue os usuários podem acessar somente os bancos de dados e tabelas nos quais eles têm permissões do Lake Formation. Além disso, os usuários do AWS Athena e do Amazon Redshift só podem consultar AWS Glue os bancos de dados e tabelas nos quais tenham permissões do Lake Formation.

Use o AMS SSP para provisionar AWS Lambda em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Lambda recursos diretamente em sua conta gerenciada pelo AMS. AWS Lambda permite que você execute código sem provisionar ou gerenciar servidores. Você paga somente pelo tempo de computação que consome. Não há cobrança quando seu código não está em execução. Com o Lambda, você pode executar código para praticamente qualquer tipo de aplicativo ou serviço de back-end, tudo sem nenhuma administração. Faça o upload do seu código e o Lambda cuidará de tudo o que for necessário para executar e escalar seu código com alta disponibilidade. Você pode configurar seu código para ser acionado automaticamente a partir de outros AWS serviços ou chamá-lo diretamente de qualquer aplicativo móvel ou da Web. Para saber mais, consulte AWS Lambda.

Perguntas frequentes sobre o Lambda no AWS Managed Services

P: Como faço para solicitar acesso à AWS Lambda minha conta do AMS?

Solicite acesso enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) tipo de alteração. Essa RFC provisiona as seguintes funções do IAM para sua conta: `customer_lambda_admin_role` e. `customer_lambda_basic_execution_role` Depois de provisionado em sua conta, você deve integrar as funções em sua solução de federação.

P: Quais são as restrições de uso AWS Lambda na minha conta AMS?

- Uma função Lambda foi projetada para ser invocada por fontes de eventos. Para obter uma lista de serviços que podem ser usados como fonte de eventos do Lambda, consulte Usando AWS Lambda com outros serviços. No momento, nem todos esses serviços estão disponíveis nas contas do AMS. Se você precisar de um serviço que não esteja disponível, trabalhe com o CSDM do AMS para registrar uma exceção.
- Por padrão, o AMS fornece uma função básica de iniciação do Lambda contendo as `AWSXrayWriteOnlyAccess` permissões `AWSLambdaBasicExecutionRole` e; para obter informações, consulte AWS Lambda Função de iniciação. Se você precisar de permissões adicionais, como a capacidade de provisionar funções do Lambda em sua VPC do AMS, envie uma RFC com o tipo de alteração Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny).

P: Quais são os pré-requisitos ou dependências para usar AWS Lambda na minha conta do AMS?

Não há pré-requisitos ou dependências para começar AWS Lambda; no entanto, dependendo do seu caso de uso específico, você pode precisar de acesso a outros AWS serviços para criar fontes de eventos ou de permissões adicionais para que sua função execute várias ações. Se forem necessárias permissões adicionais, envie uma RFC com o serviço Management | AWS | Self-provisioned service | Adicionar (revisão obrigatória) tipo de alteração (ct-3qe6io8t6jtny).

P: O que preciso fazer para executar uma função do Lambda em qualquer uma das minhas contas?

Para implantar uma função Lambda em uma conta principal, use as seguintes diretrizes:

- Certifique-se de que o SSPS for AWS Lambda esteja integrado.
- Não há restrições específicas que proíbam essa implantação sob as responsabilidades do AMS, desde que seus recursos do AMS estejam protegidos e em conformidade.
- Se você quiser que o AMS crie a função Lambda, você deve primeiro usar a função SSPS fornecida. AWS Lambda Então, se você ainda quiser assistência do AMS para implantar ou dar suporte à função, entre em contato com sua CA e inicie o processo fora do escopo (OOS).

Use o AMS SSP para provisionar AWS License Manager em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS License Manager recursos diretamente em sua conta gerenciada pelo AMS. AWS License Manager se integra aos AWS serviços para simplificar o gerenciamento de licenças em várias AWS contas, catálogos de TI e no local, por meio de uma única conta. AWS AWS License Manager permite que os administradores criem regras de licenciamento personalizadas que emulam os termos de seus contratos de licenciamento e, em seguida, apliquem essas regras quando uma instância da Amazon é lançada. EC2 As regras AWS License Manager permitem que você limite uma violação de licenciamento interrompendo fisicamente a inicialização da instância ou notificando os administradores sobre a violação. Para saber mais, consulte AWS License Manager.

Perguntas frequentes sobre o License Manager in AWS Managed Services

Perguntas e respostas comuns:

P: Como faço AWS License Manager para solicitar a configuração na minha conta do AMS?

Solicite acesso AWS License Manager enviando um RFC com o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_license_manager_role`. Depois que a função do License Manager IAM for provisionada em sua conta, você deverá integrá-la à sua solução de federação.

P: Quais são as restrições de uso AWS License Manager na minha conta AMS?

Você pode associar AWS License Manager regras às AMIs suas (filtradas em “De minha propriedade”). Se você optar por impor uma associação de limite a uma AMI (exemplo: só pode suportar 100 vCPU dessa AMI) e esgotar o limite, futuros lançamentos com essa AMI serão bloqueados e retornarão um erro informando “Nenhuma licença disponível”. Esse é o comportamento pretendido desse serviço (não permitindo o esgotamento da licença). Caso você esgote o limite, mas precise iniciar a AMI novamente, você deverá modificar a regra configurada em AWS License Manager.

P: Quais são os pré-requisitos ou dependências para usar AWS License Manager na minha conta do AMS?

Não há pré-requisitos ou dependências para usar AWS License Manager em sua conta do AMS.

Use o AMS SSP para provisionar AWS Migration Hub em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Migration Hub recursos diretamente em sua conta gerenciada pelo AMS. AWS Migration Hub fornece um único local onde você pode acompanhar o progresso das migrações de aplicativos em várias soluções AWS e de parceiros. O uso do Migration Hub permite que você escolha as ferramentas de migração AWS e os parceiros que melhor atendam às suas necessidades, ao mesmo tempo em que fornece visibilidade do status das migrações em todo o seu portfólio de aplicativos. O Migration Hub também fornece métricas e progresso importantes para aplicativos individuais, independentemente de quais ferramentas estão sendo usadas para migrá-los. Isso permite que você obtenha rapidamente atualizações de progresso em todas as suas migrações, identifique e solucione facilmente quaisquer problemas e reduza o tempo e o esforço gerais gastos em seus projetos de migração. Para saber mais, consulte AWS Migration Hub.

Perguntas frequentes sobre o Migration Hub no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao Migration Hub na minha conta do AMS?

Solicite acesso ao Migration Hub enviando uma RFC com o tipo de alteração Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_migrationhub_author_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições do Migration Hub?

Nenhum.

P: Quais são os pré-requisitos para habilitar o Migration Hub?

Não há pré-requisitos para começar a usar o Migration Hub em sua conta do AMS. No entanto, permissões fora do Migration Hub podem ser necessárias durante o gerenciamento do serviço, como permissões de gravação no Amazon S3 para carregar informações do servidor.

Use o AMS SSP para provisionar AWS Outposts em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Outposts recursos diretamente em sua conta gerenciada pelo AMS. AWS Outposts é um serviço totalmente gerenciado que estende a AWS infraestrutura APIs, AWS os serviços e as ferramentas a praticamente qualquer

data center, espaço de co-localização ou instalação local para uma experiência híbrida consistente. AWS Outposts é bom para cargas de trabalho que exigem acesso de baixa latência a sistemas locais, processamento de dados local ou armazenamento de dados local. Para saber mais, consulte AWS Outposts.

AWS Outposts perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço AWS Outposts para solicitar a configuração na minha conta do AMS?

Solicite acesso AWS Outposts enviando um RFC com o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_outposts_role`. Depois que a função for provisionada em sua conta, você deverá integrá-la à sua solução de federação.

P: Quais são as restrições de uso AWS Outposts na minha conta AMS?

Não há restrições para o uso de AWS Outposts em sua conta AMS.

P: Quais são os pré-requisitos ou dependências para usar AWS Outposts na minha conta do AMS?

Não há pré-requisitos ou dependências para usar AWS Outposts em sua conta do AMS.

Use o AMS SSP para provisionar AWS Resilience Hub em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Resilience Hub recursos diretamente em sua conta gerenciada pelo AMS. AWS Resilience Hub ajuda você a preparar e proteger proativamente seus AWS aplicativos contra interrupções. O Resilience Hub oferece avaliação e validação de resiliência que se integram ao seu ciclo de vida de desenvolvimento de software para descobrir pontos fracos de resiliência. O Resilience Hub ajuda você a estimar se seus aplicativos podem ou não atingir as metas de objetivo de tempo de recuperação (RTO) e objetivo de ponto de recuperação (RPO), além de ajudar a resolver problemas antes que eles sejam lançados em produção. Depois de implantar um AWS aplicativo na produção, você pode usar o Resilience Hub para continuar monitorando a postura de resiliência do seu aplicativo. Se ocorrer uma interrupção, o Resilience Hub envia uma notificação ao operador para iniciar o processo de recuperação associado.

AWS Resilience Hub perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS Resilience Hub minha conta do AMS?

Solicite acesso ao Resilience Hub enviando uma RFC com o tipo de alteração Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Essa RFC provisiona as seguintes funções e políticas do IAM para sua conta:

IAM roles

- `customer_resiliencehub_console_role`
- `customer_resiliencehub_service_role`

Políticas

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

Depois que a função for provisionada em sua conta, você deverá integrá-la à sua solução de `customer_resiliencehub_console_role` federação.

P: Quais são as restrições de uso AWS Resilience Hub na minha conta AMS?

Não há restrições. A funcionalidade completa do Resilience Hub está disponível em sua conta AMS.

P: Quais são os pré-requisitos ou dependências para usar AWS Resilience Hub na minha conta do AMS?

Não há pré-requisitos ou dependências para usar o Resilience Hub em sua conta do AMS.

Use o AMS SSP para provisionar AWS Secrets Manager em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Secrets Manager recursos diretamente em sua conta gerenciada pelo AMS. AWS Secrets Manager ajuda você a proteger os segredos necessários para acessar seus aplicativos, serviços e recursos de TI. O serviço permite que você alterne, gerencie e recupere facilmente credenciais de banco de dados, chaves de API e outros segredos em todo o ciclo de vida. Usuários e aplicativos recuperam segredos com uma chamada para o Secrets Manager APIs, eliminando a necessidade de codificar informações confidenciais em texto simples. O Secrets Manager oferece alternância secreta com integração embutida para o Amazon RDS, o Amazon Redshift e o Amazon DocumentDB. Além disso, o serviço é extensível a outros tipos de segredos, incluindo chaves e OAuth tokens de API. Para saber mais, consulte AWS Secrets Manager.

> **Note**
>
> Por padrão, os operadores do AMS podem acessar segredos criptografados usando a AWS KMS chave padrão da conta (CMK). AWS Secrets Manager Se você quiser que seus segredos fiquem inacessíveis às operações do AMS, use uma CMK personalizada, com uma política de chaves AWS Key Management Service (AWS KMS) que defina as permissões apropriadas aos dados armazenados no segredo.

Perguntas frequentes sobre o Secrets Manager in AWS Managed Services

P: Como faço para solicitar acesso à AWS Secrets Manager minha conta do AMS?

Solicite acesso ao Secrets Manager enviando uma RFC com o tipo de alteração Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny). Essa RFC provisiona as seguintes funções do IAM para sua conta: `customer_secrets_manager_console_role` e. `customer-rotate-secrets-lambda-role` O `customer_secrets_manager_console_role` é usado como uma função de administrador para provisionar e gerenciar os segredos, e `customer-rotate-secrets-lambda-role` é usado como a função de execução do Lambda para as funções do Lambda que alternam os segredos. Depois de provisionado em sua conta, você deve integrar a `customer_secrets_manager_console_role` função em sua solução de federação.

P: Quais são as restrições de uso AWS Secrets Manager na minha conta AMS?

A funcionalidade completa do AWS Secrets Manager está disponível em sua conta AMS, junto com a funcionalidade de rotação automática de segredos. No entanto, observe que configurar sua rotação usando “Criar uma nova função Lambda para realizar a rotação” não é suportado porque requer permissões elevadas para criar a pilha (criação da função IAM e da função Lambda), CloudFormation o que ignora o processo de gerenciamento de alterações. O AMS Advanced suporta apenas “Usar uma função Lambda existente para realizar rotação”, onde você gerencia suas funções do Lambda para alternar segredos usando a função de administrador do Lambda SSPS. AWS O AMS Advanced não cria nem gerencia o Lambda para alternar os segredos.

P: Quais são os pré-requisitos ou dependências para usar AWS Secrets Manager na minha conta do AMS?

Os namespaces a seguir estão reservados para uso pelo AMS e não estão disponíveis como parte do acesso direto a: AWS Secrets Manager

- arn:aws:secretsmanager: *:*:secret:ams-shared/*
- arn:aws:secretsmanager: *:*:secret:customer-shared/*
- arn:aws:secretsmanager: *:*:secret:ams/*

Compartilhamento de chaves usando o Secrets Manager (AMS SSPS)

Compartilhar segredos com o AMS no texto simples de um RFC, solicitação de serviço ou relatório de incidente resulta em um incidente de divulgação de informações, e o AMS retira essas informações do caso e solicita que você regenere as chaves.

Você pode usar AWS Secrets Manager(Secrets Manager) sob este namespace,. `customer-shared`

Perguntas frequentes sobre compartilhamento de chaves usando o Secrets Manager

P: Que tipo de segredos devem ser compartilhados usando o Secrets Manager?

Alguns exemplos são chaves pré-compartilhadas para criação de VPN, chaves confidenciais, como chaves de autenticação (IAM, SSH), chaves de licença e senhas.

P: Como posso compartilhar as chaves com o AMS usando o Secrets Manager?

1. Faça login no console AWS de gerenciamento usando seu acesso federado e a função apropriada:

   para SALZ, o `Customer_ReadOnly_Role`

   para MALZ,`AWSManagedServicesChangeManagementRole`.
2. Navegue até o AWS Secrets Manager console e clique em Armazenar um novo segredo.
3. Selecione Other type of secrets (Outro tipo de segredos).
4. Insira o valor secreto como texto sem formatação e use a criptografia KMS padrão. Clique em Next.
5. Insira o nome secreto e a descrição, o nome sempre começa com customer-shared/. Por exemplo, customer-shared/mykey2022. Clique em Next.
6. Deixe a rotação automática desativada, clique em Avançar.
7. Revise e clique em Armazenar para salvar o segredo.

8. Responda-nos com o nome secreto por meio da solicitação de serviço, RFC ou relatório de incidente, para que possamos identificar e recuperar o segredo.

P: Quais permissões são necessárias para compartilhar as chaves usando o Secrets Manager?

SALZ: Procure a política `customer_secrets_manager_shared_policy` gerenciada do IAM e verifique se o documento da política é o mesmo anexado nas etapas de criação abaixo. Confirme se a política está anexada às seguintes funções do IAM:`Customer_ReadOnly_Role`.

MALZ: Valide se o`AMSSecretsManagerSharedPolicy`, está anexado à `AWSManagedServicesChangeManagementRole` função que permite a `GetSecretValue` ação no `ams-shared` namespace.

Exemplo:

```
{
 "Action": "secretsmanager:*",
 "Resource": [
 "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
 "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
 ],
 "Effect": "Allow",
 "Sid": "AllowAccessToSharedNameSpaces"
 }
```

> **Note**
>
> As permissões necessárias são concedidas quando você adiciona um serviço AWS Secrets Manager provisionado de autoatendimento.

Use o AMS SSP para provisionar AWS Security Hub CSPM em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Security Hub CSPM recursos diretamente em sua conta gerenciada pelo AMS. AWS Security Hub CSPM fornece uma visão abrangente de seu estado de segurança interno AWS e de sua conformidade com os padrões e as melhores práticas do setor de segurança. O Security Hub centraliza e prioriza as descobertas de segurança e conformidade de várias AWS contas, serviços e parceiros terceirizados suportados para

ajudá-lo a analisar suas tendências de segurança e identificar os problemas de segurança de maior prioridade. Para saber mais, consulte AWS Security Hub CSPM.

Perguntas frequentes sobre o Security Hub no AWS Managed Services

P: Como faço para solicitar acesso à AWS Security Hub CSPM minha conta do AMS?

Solicite acesso ao Security Hub enviando uma RFC com o serviço Management | AWS | Self-provisioned service | Add (ct-1w8z66n899dct) change type. Este RFC provisiona a seguinte função do IAM para sua conta:`customer_securityhub_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do Security Hub na minha conta do AMS?

A funcionalidade de arquivamento foi considerada um risco operacional e de segurança potencial e foi restringida como parte da função de segurança do serviço autoprovisionado.

P: Quais são os pré-requisitos ou dependências para usar AWS Security Hub CSPM na minha conta do AMS?

Não há pré-requisitos ou dependências para usar AWS Security Hub CSPM em sua conta do AMS.

Use o AMS SSP para provisionar AWS Service Catalog AppRegistry em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AppRegistry recursos diretamente em sua conta gerenciada pelo AMS. AppRegistry permite ações de pesquisa, geração de relatórios e gerenciamento de aplicativos a partir de um local central. Os criadores raramente criam aplicativos em uma única AWS conta. Eles normalmente separam os recursos do aplicativo por fases do ciclo de vida, como desenvolvimento, teste e produção. AppRegistry permite que você agrupe e visualize todas as suas coleções de recursos nas AWS contas que você define.

Com AppRegistry, você pode armazenar seus AWS aplicativos, a coleção de recursos associados aos seus aplicativos e os grupos de atributos do aplicativo. Para saber mais, consulte O que é AppRegistry.

Perguntas frequentes: AWS Service Catalog AppRegistry no AMS

P: Como faço para solicitar acesso à AWS Service Catalog AppRegistry minha conta do AMS?

Solicite acesso AppRegistry enviando um RFC com o tipo de alteração Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny). Este RFC

provisiona a seguinte função do IAM para sua conta:`customer-appregistry-console-role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições de uso AWS Service Catalog AppRegistry na minha conta AMS?

O acesso total ao AppRegistry serviço é fornecido, com exceção do uso do namespace AMS na `'Name'` tag.

P: Quais são os pré-requisitos ou dependências para usar AWS Service Catalog AppRegistry na minha conta do AMS?

Não há pré-requisitos ou dependências para usar AppRegistry em sua conta do AMS.

Use o AMS SSP para provisionar AWS Shield Advanced em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Shield Advanced recursos diretamente em sua conta gerenciada pelo AMS. AWS Shield Advanced é um serviço gerenciado de proteção distribuída de negação de serviço (DDoS) que protege os aplicativos em execução. AWS O Shield Advanced fornece detecção sempre ativa e mitigações automáticas em linha que minimizam o tempo de inatividade e a latência do aplicativo, portanto, não há necessidade de contratar o Support para se beneficiar da proteção S. AWS DDo Existem dois níveis: Standard e Advanced; o AMS oferece o Shield Advanced. AWS Shield Para saber mais, consulte Shield Advanced.

Todos os AWS clientes se beneficiam das proteções automáticas do AWS Shield Standard, sem custo adicional. AWS Shield Standard se defende contra os ataques mais comuns e frequentes da camada DDo S de rede e transporte que visam seu site ou aplicativos. Ao usar AWS Shield Standard com a Amazon CloudFront e o Amazon Route 53, você recebe proteção abrangente de disponibilidade contra todos os ataques de infraestrutura conhecidos (camadas 3 e 4).

Para obter níveis mais altos de proteção contra ataques direcionados aos seus aplicativos executados nos recursos Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), CloudFront Amazon e AWS Global Accelerator Amazon Route 53, você pode se inscrever em. AWS Shield Advanced

Além das proteções da camada de rede e transporte fornecidas AWS Shield Standard, AWS Shield Advanced fornecem detecção e mitigação adicionais contra ataques DDo S grandes e sofisticados, visibilidade quase em tempo real dos ataques e integração com AWS WAF um firewall de aplicativos da web. AWS Shield Advanced também oferece acesso 24 horas por dia, 7 dias por semana à Equipe de AWS Shield Resposta (SRT) e proteção contra picos relacionados a DDo S em suas

cobranças do Amazon Elastic Compute Cloud (EC2Amazon), Elastic Load Balancing (Elastic Load Balancing) CloudFront AWS Global Accelerator, Amazon e Amazon Route 53.

Perguntas frequentes sobre o Shield Advanced in AWS Managed Services

P: Como solicito acesso ao Shield Advanced na minha conta do AMS?

Solicite acesso ao Shield Advanced enviando uma RFC com o tipo de alteração Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Essa RFC provisiona as seguintes funções do IAM para sua conta: `customer_shield_role` e. `aws_drt_shield_role` Depois de provisionado em sua conta, você deve integrar as funções em sua solução de federação.

Depois que as funções forem implantadas em sua conta, você poderá usar o `customer_shield_role` para confirmar sua assinatura AWS Shield Advanced em sua conta.

> **Note**
>
> Observe que há uma taxa mensal e um compromisso de um ano associados ao uso de AWS Shield Advanced. Além disso, o uso AWS Shield Advanced no AMS autoriza o AMS a encaminhar para o AWS Shield (SRT), que pode fazer alterações nas regras do firewall de seu aplicativo web (AWS WAF) durante incidentes escalonados de negação de serviço distribuída (S). DDo Essas mudanças serão feitas em coordenação com a AMS.

P: Quais são as restrições ao uso do Shield Advanced na minha conta AMS?

Embora não seja uma restrição, você deve entender que o uso do Shield Advanced implanta o`aws_drt_shield_role`, que permite que AWS Shield as equipes (SRT) façam alterações emergenciais nas AWS WAF regras das contas do AMS durante incidentes S DDo escalonados. Isso é recomendado pelo AMS para a remediação mais rápida dos ataques DDo S e ocorreria após uma escalação do AMS para o SRT.

P: Quais são os pré-requisitos ou dependências para usar o Shield Advanced na minha conta AMS?

Não há pré-requisitos ou dependências para usar o Shield Advanced em sua conta do AMS.

Use o AMS SSP para provisionar AWS Snowball Edge em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do Snowball Edge diretamente na sua conta gerenciada do AMS. O Snowball Edge é uma solução de transporte de

dados em escala de petabytes que usa dispositivos projetados para serem seguros, para transferir grandes quantidades de dados para dentro e para fora da nuvem. AWS O Snowball Edge aborda desafios comuns com transferências de dados em grande escala, incluindo altos custos de rede, longos tempos de transferência e questões de segurança. Você pode usar o Snowball Edge para migrar dados analíticos, dados genômicos, bibliotecas de vídeo, repositórios de imagens, backups e arquivar parte de projetos de encerramento de data centers, substituição de fitas ou migração de aplicativos. Transferir dados com o Snowball Edge é simples, rápido, mais seguro e pode custar apenas um quinto do custo da transferência de dados por meio da Internet de alta velocidade.

Com o Snowball Edge, você não precisa escrever nenhum código ou comprar nenhum hardware para transferir seus dados. Comece usando o AWS Management Console para criar um trabalho de importação para o Snowball, e um dispositivo Snowball será enviado automaticamente para você. Quando ele chegar, conecte o dispositivo à sua rede local, baixe e execute o Snowball Client ("Cliente") para estabelecer uma conexão e, em seguida, use o Cliente para selecionar os diretórios de arquivos que você deseja transferir para o dispositivo. O cliente então criptografa e transfere os arquivos para o dispositivo em alta velocidade. Quando a transferência for concluída e o dispositivo estiver pronto para ser devolvido, a etiqueta de remessa E Ink é atualizada automaticamente e você pode acompanhar o status do trabalho com o Amazon Simple Notification Service (Amazon SNS), mensagens de texto ou diretamente no console. Para saber mais, consulte AWS Snowball Edge.

Perguntas frequentes sobre o Snowball Edge no AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS Snowball Edge minha conta AMS?

A implementação do Snowball Edge no AMS é um processo de duas etapas:

1. Envie um tipo de alteração de gerenciamento | Outro | Outro | Crie (ct-1e1xtak34nx76) e solicite uma função de serviço para o Snowball Edge em sua conta AMS.
2. Solicite o acesso do usuário enviando um Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Essa RFC provisiona as seguintes funções do IAM em sua conta: `customer_snowball_console_rolecustomer_snowball_export_role`, e. `customer_snowball_import_role` Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições de uso AWS Snowball Edge na minha conta AMS?

A funcionalidade completa do AWS Snowball Edge está disponível em sua conta AMS.

P: Quais são os pré-requisitos ou dependências para usar AWS Snowball Edge na minha conta do AMS?

Você deve ter a conta da função de serviço conforme mencionado acima.

Use o AMS SSP para provisionar AWS Step Functions em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar AWS Step Functions recursos diretamente em sua conta gerenciada pelo AMS. AWS Step Functions é um serviço da Web que permite coordenar os componentes de aplicativos e microsserviços distribuídos usando fluxos de trabalho visuais. Os aplicativos são desenvolvidos a partir de componentes individuais que executam uma função ou uma tarefa distinta e permitem dimensionar e alterar rapidamente os aplicativos. O Step Functions oferece uma maneira confiável de coordenar componentes e percorrer as funções da aplicação. O Step Functions oferece um console gráfico para visualizar os componentes do seu aplicativo como uma série de etapas. Ele aciona e rastreia automaticamente cada etapa e tenta novamente quando há erros, para que seu aplicativo seja executado sempre na ordem e conforme o esperado. O Step Functions registra o estado de cada etapa, de modo que, quando algo dá errado, é possível diagnosticar e depurar problemas rapidamente. Para saber mais, consulte AWS Step Functions.

Perguntas frequentes sobre Step Functions in AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS Step Functions minha conta AMS?

Solicite acesso AWS Step Functions enviando um RFC com o Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_step_functions_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições de uso AWS Step Functions na minha conta AMS?

A funcionalidade completa do AWS Step Functions está disponível em sua conta AMS.

P: Quais são os pré-requisitos ou dependências para usar AWS Step Functions na minha conta do AMS?

Em tempo de execução, a função usada pelo Step Functions deve ter acesso aos serviços usados pela função step. Por exemplo, uma função de etapa pode depender das funções Lambda. É provável que alguém que crie uma função de etapa esteja criando funções Lambda ao mesmo tempo e também precise solicitar acesso a esse serviço.

Use o AMS SSP para provisionar o AWS Systems Manager Parameter Store em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos do AWS Systems Manager Parameter Store diretamente em sua conta gerenciada pelo AMS. AWS Systems Manager O Parameter Store fornece armazenamento seguro e hierárquico para gerenciamento de dados de configuração e gerenciamento de segredos. Você pode armazenar dados, como senhas, strings de banco de dados e códigos de licença como valores de parâmetro. É possível armazenar valores como texto sem formatação ou dados criptografados. Depois você pode fazer referência a valores usando o nome exclusivo que especificou ao criar o parâmetro. Altamente escalável, disponível e durável, o Parameter Store é apoiado pela AWS nuvem. Para saber mais, consulte AWS Systems Manager Parameter Store.

> **Note**
>
> Se você quiser um armazenamento de segredos dedicado com gerenciamento do ciclo de vida, use Use o AMS SSP para provisionar AWS Secrets Manager em sua conta AMS em vez do Parameter Store. O Secrets Manager ajuda você a atender aos seus requisitos de segurança e conformidade, permitindo que você alterne os segredos automaticamente. O Secrets Manager oferece integração integrada para MySQL, PostgreSQL e Amazon Aurora no Amazon RDS, que é extensível a outros tipos de segredos por meio da personalização das funções do Lambda.

AWS Systems Manager Perguntas frequentes sobre o Parameter Store no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao Systems Manager Parameter Store na minha conta AMS?

Solicite acesso ao AWS Systems Manager Parameter Store enviando uma RFC com o Management | AWS service | Self-provisioned service | Add change type

(ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_systemsmanager_parameterstore_console_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições ao uso do AWS Systems Manager Parameter Store na minha conta AMS?

É necessário usar chaves AWS gerenciadas; o acesso é restrito à criação de chaves KMS personalizadas. No entanto, se uma chave personalizada for necessária, envie uma RFC para criar uma chave gerenciada pelo cliente (CMK) usando Deployment | Advanced Stack Components | KMS Key | Create change type (ct-1d84keiri1jhg) com essa função do IAM, como o valor dos parâmetros e. `customer_systemsmanager_parameterstore_console_role` `IAMPrincipalsRequiringDecryptPermissions` `IAMPrincipalsRequiringEncryptPermissionsPrincipal` Depois que a chave KMS for criada, você poderá criar uma string segura usando-a.

P: Quais são os pré-requisitos ou dependências para usar o AWS Systems Manager Parameter Store na minha conta AMS?

Não há pré-requisitos; no entanto, o SSM Parameter Store depende do KMS para criar uma string segura para que você possa criptografar e descriptografar seus valores armazenados no Parameter Store.

Use o AMS SSP para provisionar a AWS Systems Manager automação em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos de AWS Systems Manager automação diretamente em sua conta gerenciada pelo AMS. AWS Systems Manager A automação simplifica as tarefas comuns de manutenção e implantação de instâncias do Amazon Elastic Compute Cloud e outros AWS recursos usando runbooks, ações e cotas de serviços. Ele permite que você crie, execute e monitore automações em grande escala. A automação do Systems Manager é um tipo de documento do Systems Manager que define as ações que o Systems Manager executa em suas instâncias gerenciadas. Um runbook que você usa para realizar tarefas comuns de manutenção e implantação, como executar comandos ou scripts de automação em suas instâncias gerenciadas. O Systems Manager inclui recursos que ajudam você a atingir grandes grupos de instâncias usando tags do Amazon Elastic Compute Cloud e controles de velocidade que ajudam a implementar alterações de acordo com os limites definidos. Os runbooks são escritos usando JavaScript Object Notation (JSON) ou YAML. No entanto, usando o Document Builder no console do Systems Manager Automation, você pode criar um runbook sem precisar criar em JSON ou YAML

nativo. Como alternativa, você pode usar os runbooks fornecidos pelo Systems Manager com etapas predefinidas que atendam às suas necessidades. Para saber mais, consulte Como trabalhar com runbooks na AWS Systems Manager documentação.

> **Note**
>
> Embora o Systems Manager Automation ofereça suporte a 20 tipos de ação que podem ser usados no runbook, há um número limitado de ações que você pode usar ao criar o runbook para ser usado em sua conta do AMS Advanced. Da mesma forma, um número limitado de runbooks fornecidos pelo Systems Manager pode ser usado diretamente ou de dentro do seu próprio runbook. Para obter detalhes, consulte as restrições nas perguntas frequentes a seguir.

AWS Systems Manager Perguntas frequentes sobre automação no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso ao Systems Manager Automation na minha conta AMS?

Solicite acesso à AWS Systems Manager automação enviando uma RFC com o Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_systemsmanager_automation_console_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as limitações de usar a AWS Systems Manager automação na minha conta do AMS?

Você precisa criar seu runbook, com um conjunto limitado de ações suportadas pelo Systems Manager para automação, somente para executar and/or scripts de comandos em suas instâncias gerenciadas. As ações que estão disponíveis para você, juntamente com quaisquer restrições, estão descritas abaixo.

AWS Systems Manager Limitações de automação

Ação	Descrição	Limitação
aws: assertAwsResource Propriedade —	Afirmar um estado AWS de recurso ou estado de evento	Somente EC2 instâncias

Ação	Descrição	Limitação
aws:aws:branch —	Execute etapas de automação condicional	Sem limitação
AWS: criar tags —	Crie tags para AWS recursos	Somente para os runbooks de automação SSM que você cria
AWS: Execute a automação —	Execute outra automação	Somente o runbook de automação que você cria
aws:ExecuteScript —	Executar um script	Único script que não faz nenhuma chamada de API para nenhum serviço
aws:pause —	Pausar uma automação	Sem limitação
AWS: RunCommand —	Executar um comando em uma instância gerenciada	Usando somente o documento fornecido pelo System Manager - AWS- RunShellS cript e AWS- RunPowerS hellScript
aws:sleep —	Atrasar uma automação	Sem limitação
leis: waitForAws ResourceP roperty —	Aguarde uma propriedade AWS de recurso	Somente EC2 instâncias

Você também pode optar por executar o comando ou script diretamente com o runbook AWS RunShellScript e AWS fornecido pelo Systems Manager RunPowerShellScript usando o recurso “Executar comando” no console do Systems Manager. Você também pode agrupar esses runbooks em seu runbook, que fornece validação adicional antes da and/or pós-validação ou qualquer lógica de automação complexa.

A função segue o princípio do menor privilégio e fornece apenas a permissão necessária para criar, executar e recuperar detalhes de execução de runbooks destinados à execução de and/or scripts de comando em suas instâncias gerenciadas. Ele não fornece permissão para nenhum outro recurso fornecido AWS Systems Manager pelo serviço. Embora o recurso permita que você crie runbooks

de automação, a execução dos runbooks não pode ser direcionada para recursos de propriedade do AMS.

P: Quais são os pré-requisitos ou dependências para usar a AWS Systems Manager automação na minha conta do AMS?

Não há pré-requisitos; no entanto, você deve garantir que seus controles internos de and/or conformidade do processo sejam cumpridos durante a criação de runbooks. Também recomendamos testar minuciosamente os runbooks antes de executá-los nos recursos de produção.

P: A política do Systems Manager pode **`customer_systemsmanager_automation_policy`** ser anexada a outras funções do IAM?

Não, diferentemente de outros serviços habilitados para autoprovisionamento, essa política só pode ser atribuída à função padrão provisionada. `customer_systemsmanager_automation_console_role`

Diferentemente das políticas de outras funções SSPS, essa política SSM SSPS não pode ser compartilhada com outras funções personalizadas do IAM, porque esse serviço AMS serve apenas para executar comandos ou scripts de automação em suas instâncias gerenciadas. Se essas permissões pudessem ser anexadas a outras funções personalizadas do IAM, potencialmente com permissões em outros serviços, o escopo das ações permitidas poderia se estender aos serviços gerenciados e, potencialmente, reduzir a postura de segurança da sua conta.

Para avaliar qualquer solicitação de mudança (RFCs) de acordo com nossos padrões técnicos do AMS, trabalhe com seu respectivo arquiteto de nuvem ou gerente de entrega de serviços, consulte as análises de segurança da RFC.

> **Note**
>
> AWS Systems Manager permite que você use runbooks que são compartilhados com sua conta. Recomendamos que você tenha cuidado e realize uma verificação de devida diligência ao usar runbooks compartilhados e certifique-se de revisar o conteúdo para entender se command/scripts eles são executados antes de executar os runbooks. Para obter detalhes, consulte Práticas recomendadas para documentos SSM compartilhados.

Use o AMS SSP para provisionar AWS Transfer Family em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos (Transfer AWS Transfer Family Family) diretamente em sua conta gerenciada pelo AMS. AWS Transfer Family é um AWS serviço totalmente gerenciado que permite transferir arquivos pelo Secure File Transfer Protocol (SFTP) para dentro e para fora do armazenamento do Amazon Simple Storage Service (Amazon S3). O SFTP também é conhecido como Secure Shell (SSH) File Transfer Protocol. O SFTP é usado em fluxos de trabalho de intercâmbio de dados em diferentes setores, como serviços financeiros, saúde, publicidade e varejo, entre outros.

Com o AWS SFTP, você obtém acesso a um servidor SFTP AWS sem a necessidade de executar nenhuma infraestrutura de servidor. Você pode usar esse serviço para migrar seus fluxos de trabalho baseados em SFTP e, ao AWS mesmo tempo, manter os clientes e as configurações dos usuários finais como estão. Primeiro, você associa seu nome de host ao endpoint do servidor SFTP, depois adiciona seus usuários e fornece a eles o nível certo de acesso. Depois disso, as solicitações de transferência dos seus usuários são atendidas diretamente do endpoint do servidor AWS SFTP. Para saber mais AWS Transfer for SFTP, consulte também Criar um servidor habilitado para SFTP.

AWS Transfer for SFTP perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS Transfer for SFTP minha conta AMS?

Solicite acesso AWS Transfer for SFTP enviando um RFC com o Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Por meio dessa RFC, as seguintes funções do IAM e uma política são provisionadas em sua conta:

- `customer_transfer_author_role`. Essa função foi projetada para você gerenciar o serviço SFTP por meio do console.
- `customer_transfer_sftp_server_logging_role`. Essa função foi projetada para ser anexada ao servidor SFTP. Ele permite que o servidor SFTP faça login CloudWatch.
- `customer_transfer_sftp_user_role`. Essa função foi projetada para ser anexada aos usuários do SFTP. Ele permite que os usuários do SFTP interajam com o bucket do S3.
- `policy customer_transfer_scope_down_policy`. Essa política é uma política de escopo reduzido que pode ser aplicada ao usuário do SFTP para limitar seu acesso no bucket do S3 às suas pastas pessoais.

- `customer_transfer_sftp_efs_user_role`. Essa função foi projetada para ser anexada aos usuários do SFTP. Ele permite que os usuários do SFTP interajam com o sistema de arquivos EFS.

Depois de provisionado em sua conta, você deve integrar as funções em sua solução de federação.

P: Quais são as restrições de uso AWS Transfer for SFTP na minha conta AMS?

AWS A transferência para a configuração do SFTP é limitada a recursos sem os prefixos “AMS-” ou “MC-” para evitar modificações na infraestrutura do AMS.

P: Quais são os pré-requisitos ou dependências para usar AWS Transfer for SFTP na minha conta do AMS?

- Você deve ter um bucket do Amazon S3 com um nome que contenha a palavra-chave “transferência” antes de criar o AWS Transfer for SFTP servidor e os usuários.
- Para usar um “Provedor de Identificação do Cliente”, você deve implantar o API Gateway, a função Lambda e seu repositório de usuários (AD, Secrets Manager e assim por diante). Para obter mais informações, consulte Habilitar a autenticação por senha para AWS Transfer for SFTP usar AWS Secrets Manager e trabalhar com provedores de identidade.

Use o AMS SSP para provisionar AWS Transit Gateway em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS Transit Gateway recursos diretamente em sua conta gerenciada pelo AMS. AWS Transit Gateway é um serviço que permite conectar sua Amazon Virtual Private Cloud (VPCs) e suas redes locais a um único gateway. À medida que você aumenta o número de cargas de trabalho em execução AWS, você precisa ser capaz de escalar suas redes em várias contas e na Amazon VPCs para acompanhar o crescimento. Hoje, você pode conectar pares da Amazon VPCs usando peering. No entanto, gerenciar a point-to-point conectividade em muitas Amazon VPCs, sem a capacidade de gerenciar centralmente as políticas de conectividade, pode ser operacionalmente caro e complicado. Para conectividade local, você precisa conectar sua AWS VPN a cada Amazon VPC individual. Essa solução pode ser demorada de criar e difícil de gerenciar quando o número VPCs cresce para centenas. Para saber mais, consulte AWS Transit Gateway.

AWS Transit Gateway perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS Transit Gateway minha conta do AMS?

Solicite acesso AWS Transit Gateway enviando um RFC com o Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_tgw_console_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições de uso AWS Transit Gateway na minha conta AMS?

A funcionalidade completa do AWS Transit Gateway está disponível em sua conta de landing zone de conta única do AMS, com exceção das modificações na tabela de rotas para o roteamento do Transit Gateway. Solicite alterações na tabela de rotas enviando um Management | Other | Other | Create change type (ct-1e1xtak34nx76).

> **Note**
>
> Esse serviço só é compatível com a zona de pouso com uma única conta (SALZ), não com a zona de pouso com várias contas (MALZ).

P: Quais são os pré-requisitos ou dependências para usar AWS Transit Gateway na minha conta do AMS?

Não há pré-requisitos ou dependências para usar AWS Transit Gateway em sua conta do AMS.

Use o AMS SSP para provisionar AWS WAF - Web Application Firewall em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os AWS WAF recursos diretamente em sua conta gerenciada pelo AMS. AWS WAF é um firewall de aplicativos da Web (AWS WAF) que ajuda a proteger seus aplicativos da Web contra explorações comuns da Web que podem afetar a disponibilidade dos aplicativos, comprometer a segurança ou consumir recursos excessivos. AWS WAF dá a você controle sobre qual tráfego permitir ou bloquear em seus aplicativos da web, definindo regras de segurança da web personalizáveis. Você pode usar AWS WAF para criar regras personalizadas que bloqueiam padrões de ataque comuns, como injeção de SQL ou scripts entre sites; e regras projetadas para seu aplicativo específico.

Para saber mais, consulte AWS WAF - Web Application Firewall.

O AMS não oferece suporte ao monitoramento (CloudWatch alarmes/eventos/alertas MMS) para. AWS WAF Devido à natureza do AWS WAF, você deve criar regras personalizadas para seus aplicativos; o AMS não pode quantificar e criar alarmes para você, sem o contexto do seu aplicativo. Para saber mais, consulte AWS WAF - Web Application Firewall.

AWS WAF perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço AWS WAF para solicitar a configuração na minha conta do AMS?

Solicite acesso ao AWS WAF enviando uma RFC com o serviço Management | AWS | Self-provisioned service | Add change type (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_waf_role`. Depois que a função AWS WAF do IAM for provisionada em sua conta, você deverá integrá-la à sua solução de federação.

P: Quais são as restrições de uso AWS WAF?

Depois que as permissões são provisionadas, você tem a funcionalidade completa do. AWS WAF

P: Quais são os pré-requisitos ou dependências do uso? AWS WAF

Não há pré-requisitos ou dependências para usar AWS WAF em sua conta do AMS.

Use o AMS SSP para provisionar AWS Well-Architected Tool em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar AWS Well-Architected Tool recursos diretamente em sua conta gerenciada pelo AMS. AWS Well-Architected Tool Isso ajuda você a analisar o estado de suas cargas de trabalho e as compara com as melhores práticas AWS arquitetônicas mais recentes. A ferramenta é baseada no AWS Well-Architected Framework, desenvolvido para ajudar os arquitetos de nuvem a criar uma infraestrutura de aplicativos segura, de alto desempenho, resiliente e eficiente. Essa estrutura fornece uma abordagem consistente para você avaliar arquiteturas, foi usada em dezenas de milhares de análises de carga de trabalho conduzidas pela equipe de arquitetura de AWS soluções e fornece orientação para ajudar a implementar projetos que se adaptam às necessidades do aplicativo ao longo do tempo. Para saber mais, consulte AWS Well-Architected Tool.

AWS WA Tool perguntas frequentes sobre o AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS Well-Architected Tool minha conta AMS?

Solicite acesso ao AWS Well-Architected Tool enviando uma RFC com o serviço Management | AWS | Self-provisioned service | Add change type (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_well_architected_tool_console_admin_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

P: Quais são as restrições de uso AWS Well-Architected Tool na minha conta AMS?

A funcionalidade completa do AWS Well-Architected Tool está disponível em sua conta AMS.

P: Quais são os pré-requisitos ou dependências para usar AWS Well-Architected Tool na minha conta do AMS?

Não há pré-requisitos ou dependências para usar AWS Well-Architected Tool em sua conta do AMS.

Use o AMS SSP para provisionar AWS X-Ray em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar os recursos (AWS X-Ray X-Ray) diretamente em sua conta gerenciada do AMS. AWS X-Ray ajuda os desenvolvedores a analisar e depurar aplicativos distribuídos e de produção, como aqueles criados usando uma arquitetura de microsserviços. Com o X-Ray, você pode entender o desempenho do aplicativo e dos serviços subjacentes para identificar e solucionar a causa raiz dos problemas e erros de desempenho. O X-Ray fornece uma end-to-end visão das solicitações à medida que elas percorrem seu aplicativo e mostra um mapa dos componentes subjacentes do seu aplicativo. Você pode usar o X-Ray para analisar aplicativos em desenvolvimento e produção, desde aplicativos simples de três camadas até aplicativos complexos de microsserviços que consistem em milhares de serviços. Para saber mais, consulte AWS X-Ray.

Perguntas frequentes sobre o X-Ray in AWS Managed Services

Perguntas e respostas comuns:

P: Como faço para solicitar acesso à AWS X-Ray minha conta do AMS?

Solicite acesso enviando um tipo de alteração Gerenciamento | AWS Serviço | Serviço autoprovisionado | Adicionar (ct-1w8z66n899dct). Este RFC provisiona a seguinte função do IAM para sua conta:`customer_xray_console_role`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação. Além disso, você deve ter a opção de `customer_xray_daemon_write_instance_profile` enviar dados de suas

EC2 instâncias da Amazon para o X-Ray. Esse perfil de instância é criado quando você recebe `customer_xray_console_role` o.

Você pode enviar uma solicitação de serviço à AMS Operations para atribuí-la `customer_xray_daemon_write_policy` ao perfil de instância existente ou pode usar o perfil de instância criado quando o AMS Operations ativa o X-Ray para você.

P: Quais são as restrições de uso AWS X-Ray na minha conta AMS?

A funcionalidade completa do AWS X-Ray está disponível em sua conta AMS, exceto para criptografia com chave AWS KMS (chave KMS). AWS X-Ray criptografa todos os dados de rastreamento por padrão. Por padrão, o X-Ray criptografa rastreamentos e dados relacionados em repouso. Se precisar criptografar dados em repouso com uma chave, você pode escolher a chave KMS gerenciada (aws/xray) ou a chave AWS gerenciada pelo cliente KMS. Para a chave KMS Customer-Managed para criptografia X-Ray, envie um Management | Other | Other | Create change type (ct-1e1xtak34nx76).

P: Quais são os pré-requisitos ou dependências para usar AWS X-Ray na minha conta do AMS?

AWS X-Ray depende do Amazon S3 CloudWatch e do Logs CloudWatch, que já estão implementados nas contas do AMS. As dependências transitivas variam de acordo com as fontes de dados e outros AWS serviços com os quais os recursos AWS X-Ray possam estar interagindo (por exemplo, Amazon Redshift, Amazon RDS, Athena).

Use o AMS SSP para provisionar a VM Import/Export em sua conta AMS

Use o modo AMS Self-Service Provisioning (SSP) para acessar a VM Import/Exportcapabilities diretamente na sua conta gerenciada pelo AMS. A VM Import/Export permite que você importe facilmente imagens de máquinas virtuais do seu ambiente existente para as EC2 instâncias da Amazon e as exporte de volta para o seu ambiente local. Essa oferta permite que você aproveite seus investimentos existentes nas máquinas virtuais que você criou para atender aos requisitos de segurança, gerenciamento de configuração e conformidade de TI, trazendo essas máquinas virtuais para a Amazon EC2 como ready-to-use instâncias. Você também pode exportar instâncias importadas de volta para sua infraestrutura de virtualização local, permitindo que você implante cargas de trabalho em toda a sua infraestrutura de TI. Para saber mais, consulte VM Import/Export.

Perguntas frequentes sobre VM Import/Export no AWS Managed Services

Perguntas e respostas comuns:

P: Como solicito acesso à VM Import/Export na minha conta do AMS?

Solicite acesso à VM Import/Export enviando uma RFC com o Gerenciamento | AWS serviço | Serviço autoprovisionado | Adicionar tipo de alteração (ct-1w8z66n899dct). Este RFC provisiona a seguinte política do IAM para sua conta:`customer_vmimport_policy`. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.

Uma função adicional, a função Import/Export Serviço de VM, é necessária para que o serviço execute ações em sua conta.

P: Quais são as restrições ao uso da VM Import/Export na minha conta do AMS?

- A funcionalidade para importar imagens de máquinas e volumes de dados personalizados está disponível no AMS VM Import/Export. No entanto, as permissões para o S3 foram reduzidas para limitar as ações aos buckets correspondentes ao nome, a `customer-vmimport-*` fim de limitar o acesso às informações na conta.
- A importação de imagens e instantâneos é suportada no AMS VM Import/Export. No entanto, a funcionalidade de importação e exportação de instâncias não está disponível devido a medidas de segurança.
- Além disso, a funcionalidade de exportação foi desativada para reduzir o risco de exportar dados restritos e confidenciais.

P: Quais são os pré-requisitos ou dependências para usar a VM Import/Export na minha conta do AMS?

- Você deve fornecer uma imagem de disco compatível para importar para o AWS ambiente. Para obter informações, consulte Import/Export Requisitos de VM.
- A VM Import/Export não pode ser acessada pelo AWS console. Você deve acessar esse serviço por meio do AWS CLI, Ferramentas da AWS para PowerShell, ou do AWS SDKs. Ou você pode solicitar um perfil de instância enviando o tipo de alteração ct-117rmp64d5mvb: Deployment | Advanced stack components | Identity and Access Management (IAM) | Create instance profile. EC2 Esse perfil de instância permite que as ferramentas executem comandos de uma instância.

Modo gerenciado pelo cliente

O modo Customer Managed Services (AMS) da AWS Managed Services (AMS) fornece um modelo de governança que é flexível e pode ser adaptado às suas necessidades. Isso pode ser considerado uma opção alternativa para serviços e aplicativos que o AMS não consegue operar para você. O AMS não opera infraestrutura hospedada em contas criadas sob esse modo. No entanto, você pode

aproveitar o gerenciamento centralizado de várias contas nesse modo. Os seguintes recursos da Zona de Aterrissagem de Várias Contas podem ser aproveitados nesse modo:

- Implantação automatizada de contas
- Conectividade por meio do Transit Gateway na conta de rede
- Biblioteca de regras de configuração do AMS
- Armazene cópias dos registros na conta de registro
- Agregação de alertas do Guard Duty gerenciados pelo cliente à conta de segurança
- Faturamento consolidado
- Ativação de políticas personalizadas de controle de serviços.

Por exemplo: se você quiser executar cargas de trabalho no Ubuntu Pro, que não é um sistema operacional gerenciado pelo AMS, você pode usar uma conta gerenciada pelo cliente para hospedá-la. Você também pode consolidar cargas de trabalho por meio de contas gerenciadas pelo cliente, para aproveitar o desconto em massa nos Instances/Sharing planos reservados disponíveis por meio do compartilhamento em uma organização da AWS.

Introdução ao modo Gerenciado pelo Cliente

O modo AMS Customer Managed está disponível por meio de uma conta especial do aplicativo landing zone com várias contas.

Para obter detalhes, incluindo como criar uma conta de aplicativo gerenciado pelo cliente, consulte Contas de aplicativos gerenciados pelo cliente.

AMS e AWS Service Catalog

O Service Catalog no AWS Managed Services (AMS) permite que as organizações criem e gerenciem catálogos de serviços de tecnologia da informação (TI) da AWS e permite que os administradores de TI criem, gerenciem e distribuam catálogos de produtos aprovados para usuários finais em suas contas, que podem então acessar os produtos de que precisam em um portal personalizado de serviços. Os administradores podem controlar quais usuários têm acesso a cada produto para garantir a conformidade com as políticas de negócios organizacionais. Os administradores também podem configurar funções para que os usuários finais só precisem de acesso do IAM ao Service Catalog para implantar recursos aprovados. O Service Catalog permite

que sua organização se beneficie do aumento da agilidade e da redução de custos, pois os usuários finais podem encontrar e lançar somente os produtos de que precisam em um catálogo controlado por você.

O Service Catalog fornece uma alternativa ao processo de solicitação de mudança (RFC) do AMS para provisionar e atualizar recursos em suas contas gerenciadas do AMS. O AMS gerencia todas as tarefas operacionais de infraestrutura necessárias para executar a AWS em grande escala para todos os recursos de infraestrutura provisionados por meio do Service Catalog, incluindo segurança, conformidade, provisionamento, disponibilidade, patches, monitoramento, alertas, relatórios, resposta a incidentes e otimização de custos. A utilização do Service Catalog em sua conta gerenciada do AMS fornece um mecanismo para gerenciar centralmente os serviços de TI comumente implantados e ajuda você a obter uma governança consistente, permitindo que os usuários implantem rapidamente somente os serviços de TI aprovados de que precisam em seus ambientes gerenciados.

Introdução ao Service Catalog

Para começar a usar o Service Catalog no AMS, envie uma solicitação de serviço pelo console do AMS para solicitar acesso ao Service Catalog. Após o envio da solicitação, três funções do IAM serão implantadas em suas contas junto com uma pilha gerenciada pelo AMS contendo a CloudFormation macro que invoca o AMS `Transform` (descrita anteriormente) para que possamos registrar os produtos em nossos sistemas e realizar operações na infraestrutura provisionada por meio do Service Catalog. As três funções do IAM implantadas incluem uma função para administradores de TI gerenciarem produtos como administradores do Service Catalog; uma função para proprietários de aplicativos e usuários finais configurarem, lançarem e gerenciarem produtos; e uma função que será usada como uma restrição de lançamento, que define as permissões que o Service Catalog usará ao lançar ou atualizar seu produto.

Service Catalog no AMS antes de você começar

O Service Catalog substitui o processo existente de solicitação de mudança (RFC) do AMS?

> Nas contas em que o Service Catalog está ativado, ele atuará como o sistema de gerenciamento de mudanças no qual você provisiona e atualiza os serviços de TI em sua conta do AMS por meio de seu catálogo de produtos predefinido; o AMS fornecerá um portfolio/product catálogo padrão e seus administradores de TI poderão criar e configurar o seu próprio. O Service Catalog reconhecerá somente as pilhas provisionadas por meio do Service Catalog. Da mesma forma, os serviços provisionados por meio do Service Catalog não poderão ser modificados por meio

do processo de RFC do AMS, pois modificações fora do Service Catalog desviarão a pilha da configuração aprovada do produto.

Posso ver as pilhas provisionadas por meio do catálogo de serviços no console do AMS?

Sim. Você pode visualizar todas as pilhas provisionadas por meio do catálogo de serviços no console do AMS. As pilhas provisionadas por meio do catálogo de serviços são facilmente identificáveis pelo ID da pilha “SC-”. Embora as pilhas possam ser visualizadas no console do AMS, você não poderá atualizá-las por meio do processo RFC do AMS. O acesso ao sistema de gerenciamento de alterações do AMS (RFCs) é limitado somente à solicitação de acesso, orquestração de patches e backup RFCs .

Se eu provisionar uma and/or atualização de uma pilha por meio do Service Catalog, haverá uma RFC correspondente no console do AMS?

A única RFC que será exibida no console do AMS é uma RFC para registrar a pilha no AMS quando uma pilha é provisionada inicialmente. Essa RFC é arquivada automaticamente pelo processo de validação do AMS, que é acionado quando uma pilha é iniciada por meio do Service Catalog. Todos os outros provisionamentos e alterações são rastreados diretamente no Service Catalog e podem ser visualizados no console do Service Catalog. Além disso, você pode usar o recurso Provisioned Product Plan no Service Catalog para visualizar a lista de alterações que serão feitas nos recursos antes do provisionamento ou da atualização do produto.

Preciso fazer algo específico para provisionar produtos na minha conta gerenciada do AMS?

Sim. Todos os produtos do Service Catalog provisionados em contas do AMS devem conter essa linha de JSON no modelo CFN que define esse produto:

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

Esse trecho de CloudFormation código aciona as validações do AMS necessárias antes que o recurso possa ser provisionado em sua conta gerenciada do AMS. É sua responsabilidade incluir essa linha de código como parte da definição do produto. Se não estiver incluído, o provisionamento falhará e a seguinte mensagem de erro será exibida: “Falha na criação do produto. Essa conta é gerenciada pelo AMS. Todos os produtos nas contas AMS devem ter o `Transform` código AMS no modelo.”

Há alguma funcionalidade do Service Catalog não disponível and/or limitada para clientes do AMS no lançamento?

Sim, os seguintes recursos do SC não estão disponíveis para clientes do AMS no lançamento inicial:

- Criação de conta por meio do Service Catalog
- Capacidade de lançar todos os serviços da AWS por meio do Service Catalog em uma conta gerenciada pela AMS. A disponibilidade do AWS Service é limitada aos serviços suportados pelo AMS (gerenciados e autoprovisionados). Para obter mais informações sobre os serviços suportados pelo AMS, consulte a descrição do serviço AMS.
- Os conectores do Service Catalog IT Service Manager (ITSM) não se comunicarão com os relatórios de incidentes e solicitações de serviço do AMS.
- Capacidade de aproveitar os inícios rápidos e as arquiteturas de referência do Service Catalog sem modificação. Lembre-se de que os produtos do Service Catalog para contas AMS devem conter esta linha de código JSON:

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

  no modelo CNF. Observe que essa linha não faz parte de um CloudFormation modelo típico da AWS e deve ser adicionada explicitamente.
- Atualmente, o Terraform não é compatível com o AMS para provisionamento de produtos do Service Catalog.
- Os conjuntos de pilhas CFN da AWS não são compatíveis com o AMS.
- Você não pode criar funções personalizadas do IAM.
- As ações de serviço estão limitadas a:
  - AWS- RebootRdsInstance
  - Instância AWS-Restart EC2
  - Instância AWS Start EC2
  - AWS- StartRdsInstance
  - Instância AWS-Stop EC2
  - AWS- StopRdsInstance
  - AWS- CreateImage
  - AWS- CreateRdsSnapshot

- AWS- CreateSnapshot

> **Note**
>
> Ao criar ações de serviço, você pode configurar a função de execução para ser a permissão do usuário final, a função de lançamento ou uma função personalizada do IAM de sua escolha. A função de execução selecionada deve ter permissões suficientes para realizar a ação do serviço e ter uma TrustPolicy que permita que ela seja assumida pelo Service Catalog, caso contrário, a ação do serviço falhará no momento da execução. Recomendamos usar o AWSManagedServicesServiceCatalogLaunchRole, que tem as permissões e a política de confiança corretas para ser usado como uma ação de serviço.

Para que ainda precisarei usar o sistema AMS RFC?

Na disponibilidade geral (GA), você ainda precisará usar o RFCS para executar as seguintes ações:

- Configurando o Patch Orchestrator
- Configurando políticas de backup
- Solicitando acesso à instância
- Criação e atribuição de grupos de segurança que estejam fora das diretrizes do AMS.
- Executando a ingestão de carga de trabalho (WIGS)
- Criação de perfis do IAM

Posso usar a CLI do Service Catalog para acessar o Service Catalog na minha conta gerenciada do AMS?

Sim, o Service Catalog APIs está disponível e habilitado por meio da CLI. Ações do gerenciamento dos artefatos do Service Catalog por meio do provisionamento e encerramento desses artefatos estão disponíveis. Para obter mais informações, consulte os recursos do AWS Service Catalog ou baixe o SDK ou a CLI mais recente da AWS.

Quem cria, gerencia e distribui os catálogos de produtos aprovados dos clientes?

O administrador do catálogo do cliente, o administrador de and/or TI ou o recurso designado, é responsável pelo gerenciamento dos catálogos do Service Catalog e dos produtos aprovados.

Posso usar o AMS AMIs?

O AMIs AMS vendido após março de 2020 pode ser implantado por meio do AWS Service Catalog.

Como faço para migrar para o AMS usando o Service Catalog?

Para migrar sua carga de trabalho para o AMS usando o Service Catalog, você começa seguindo o processo Workload Ingest (WIGs) para criar uma AMI no AMS. Você usa a AMI produzida pela WIGS para criar um produto no Service Catalog. Como fazer isso está detalhado em AWS Service Catalog — Getting Started.

Integração do AMS Multi-Account Landing Zone (MALZ)

Arquitetura de rede MALZ

Sobre a arquitetura de rede de landing zone com várias contas

Antes de iniciar o processo de integração na zona de pouso multiconta (MALZ) do AWS Managed Services (AMS), é importante entender a arquitetura básica, ou zona de aterrissagem, que o AMS cria em seu nome, seus componentes e funções.

O landing zone multiconta do AMS é uma arquitetura de várias contas, pré-configurada com a infraestrutura para facilitar a autenticação, a segurança, a rede e o registro.

> **Note**
>
> Para estimativas de custos, consulte os componentes básicos do ambiente de landing zone com várias contas do AMS.

Tópicos

- Região de serviço
- Unidades organizacionais
- Políticas de controle de serviços e organização da AWS

O diagrama a seguir descreve em alto nível a estrutura da conta e como a infraestrutura é segregada em cada uma das contas:

Região de serviço

Todos os recursos em uma landing zone multiconta do AMS são implantados em uma única região da AWS de sua escolha, devido à limitação atual entre regiões com o Active Directory e o Transit Gateway.

Unidades organizacionais

Uma landing zone típica de várias contas do AMS consiste em quatro unidades organizacionais de alto nível ()OUs:

- A unidade organizacional principal (OU) (usada para agrupar contas para administrá-las como uma única unidade)
- Os aplicativos OU
- A OU gerenciada pelo cliente
- A UO acelerada

A landing zone de várias contas gerenciada pela AMS também permite que você crie contas personalizadas OUs para agrupar e organizar contas da AWS e SCPs associá-las a elas. Para exemplos de como fazer isso, consulte Conta de gerenciamento | Criar conta personalizada OUs e de gerenciamento | Criar SCP personalizada (revisão obrigatória), respectivamente. O AMS fornece quatro contas existentes OUs sob OUs as quais novas contas podem ser solicitadas: accelerate, aplicativos > gerenciados, aplicativos > desenvolvimento e gerenciados pelo cliente.

- acelere a OU:

  Esta é uma OU de alto nível na landing zone de várias contas do AMS (MALZ). As contas nesta OU são provisionadas pelo AMS com um RFC (Implantação | Landing zone gerenciada | Conta de gerenciamento | Crie uma conta Accelerate, altere o ID do tipo: ct-2p93tyd5angmi). Nessas contas de aplicativos acelerados, você pode se beneficiar de serviços operacionais acelerados, como monitoramento e alertas, gerenciamento de incidentes, gerenciamento de segurança e gerenciamento de backup. Para obter mais detalhes, consulte Contas do AMS Accelerate.
- aplicativos > OU gerenciada:

  Nessa unidade suborganizacional da UO de Aplicativos, as contas são totalmente gerenciadas pelo AMS, incluindo todas as tarefas operacionais. As tarefas operacionais incluem gerenciamento de solicitações de serviços, gerenciamento de incidentes, gerenciamento de segurança, gerenciamento de continuidade, gerenciamento de patches, otimização de custos, monitoramento e gerenciamento de eventos. Essas tarefas são realizadas para o gerenciamento da sua infraestrutura. Vários filhos OUs podem ser criados conforme necessário, até que o limite máximo de aninhados OUs seja atingido para as organizações da AWS. Para obter detalhes, consulte Cotas para AWS Organizations.
- aplicações > desenvolvimento OU:

Sob essa sub-OU da UO do aplicativo na landing zone gerenciada pelo AMS, as contas são contas no modo Desenvolvedor que fornecem permissões elevadas para provisionar e atualizar recursos da AWS fora do processo de gerenciamento de alterações do AMS. Essa OU também apoia a criação de novas unidades organizacionais secundárias, conforme necessário.

- OU gerenciada pelo cliente:

  Esta é uma OU de alto nível na landing zone de várias contas do AMS. As contas sob essa OU são provisionadas pelo AMS com uma RFC. Nessas contas, as operações das cargas de trabalho e dos recursos da AWS são de sua responsabilidade. Essa OU também apoia a criação de novas unidades organizacionais secundárias, conforme necessário.

Como prática recomendada, recomendamos que as contas sob essas OUs e as subcontas solicitadas de forma personalizada OUs sejam agrupadas com base em suas funcionalidades e políticas.

Políticas de controle de serviços e organização da AWS

A AWS fornece políticas de controle de serviços (SCPs) para gerenciamento de permissões em uma organização da AWS. SCPs são usados para definir grades de proteção adicionais para quais ações os usuários podem realizar em quais. OUs Por padrão, o AMS fornece um conjunto de contas de gerenciamento SCPs implantadas que fornecem proteções em diferentes níveis padrão de OU. Para restrições de SCP, entre em contato com seu CSDM.

Você também pode criar itens personalizados SCPs e anexá-los a itens específicos OUs. Eles podem ser solicitados na sua conta de gerenciamento usando o tipo de alteração ct-33ste5yc7hprs. Em seguida, o AMS analisa a SCPs solicitação personalizada antes de aplicá-la ao alvo OUs. Para exemplos, consulte Conta de gerenciamento | Criar conta personalizada OUs e de gerenciamento | Criar SCP personalizado (revisão obrigatória).

Escolhendo um único MALZ ou vários MALZs

A tabela a seguir fornece algumas considerações de alto nível sobre como decidir entre uma única zona de aterrissagem com várias contas (MALZ) e várias zonas de aterrissagem com várias contas (por exemplo, duas zonas de pouso com várias contas - Prod e não Prod). Em geral, a escolha depende das necessidades individuais, dos requisitos legais e das práticas operacionais.

Zona de pouso única com várias contas versus várias zonas de aterrissagem com várias contas

Entidade	Zona de pouso única do AMS	Várias (duas ou mais) zonas de pouso
Custo base	Menor, otimizado em aproximadamente $3.000 por mês.	Mais alto, um custo adicional de aproximadamente $3.000 por ambiente.
Faturamento	Fatura única, devido a uma única conta de faturamento/gerenciamento.	Fatura separada para cada landing zone com várias contas. Atualmente, a AWS Org não oferece suporte a contas de gerenciamento múltiplo com uma única fatura.
Portabilidade das instâncias reservadas existentes () RIs	Baixo. RIs Atualmente, a AWS não é conversível em várias contas de faturamento. Você reutilizaria a zona de pouso existente RIs para várias contas.	Mais baixo. Você reutilizaria e distribuiria RIs em todas as landing zone de várias contas.
Descontos por escalonamento de produtos	Alta. Consulte Descontos por volume.	Baixo. Consulte Descontos por volume.
Sobrecarga de configuração inicial (nos project/ migration cronogramas)	Baixo. Integrações de Active Directory, rede e login único (SSO) apenas uma vez.	Alta. Você executaria o Active Directory, a integração de rede e as integrações de SSO para cada landing zone. Isso pode causar possíveis atrasos em qualquer projeto de migração.
Configurabilidade de serviços comuns	Esforços baixos. Você configura common/shared serviços como DNS, backup, monitoramento, registro, etc.	Grandes esforços. É necessário um planejamento adicional para abordar onde a infraestrutura ou os serviços comuns estarão localizados. O tráfego atravessando vários gateways de

Entidade	Zona de pouso única do AMS	Várias (duas ou mais) zonas de pouso
		trânsito (TGWs) em cada landing zone pode gerar custos extras.
Escalabilidade	Médio. O AMS tem um limite prático atual de 150 contas por landing zone com várias contas. Várias equipes ou fornecedores executando aplicativos na mesma conta podem ter acesso a pilhas pertencentes a equipes diferentes. Essa limitação pode ser mitigada controlando o acesso às pilhas específicas do aplicativo na ServiceNow camada (integrando o aplicativo AMS ServiceNow Connector e fazendo uso de tags). Pergunte aos gerentes de entrega técnica (TDMs) ou arquitetos de nuvem (CAs) do AMS como implementar isso.	Alta. Capacidade de aproveitar várias landing zone de várias contas para distribuir as contas e, ao mesmo tempo, atingir um nível de segregação de contas ou aplicativos. O gerenciamento de um grande número de contas pode gerar despesas operacionais ou de custos.
Risco operacional	(Depende) Baixo. Integração operacional e prontidão apenas uma vez. Menos chance de desvios no processo.	(Depende) Baixo. Várias atividades operacionais e de integração. A deriva em várias zonas de pouso durante o período pode levar a riscos operacionais.
Várias regiões da AWS	Região única da AWS. A landing zone multiconta do AMS é restrita a uma única região da AWS. Para abranger várias regiões da AWS, use várias landing zone com várias contas.	Várias regiões da AWS. Com várias zonas de aterrissagem com várias contas, você pode implantar cada MALZ em uma região e interconectá-las usando o peering de gateway de trânsito (TGW).

Entidade	Zona de pouso única do AMS	Várias (duas ou mais) zonas de pouso
Migração ou portabilidade da conta	Sim. É possível mover contas de uma OU para outra dentro da mesma organização da AWS.	Não. O AMS não suporta a migração de uma conta entre zonas de destino, ou seja, entre AWS Organizations. As cargas de trabalho podem alcançar várias zonas de aterrissagem com gateway de trânsito (TGW) ou emparelhamento de VPC.
Gerenciamento de alterações	Médio. Fazer alterações destrutivas em componentes comuns, como TGW, Active Directory (AD) ou outbound (egress), pode afetar todas as cargas de trabalho em uma landing zone com várias contas. No entanto, as alterações nos componentes gerenciados pelo AMS são testadas internamente e incluídas em atualizações contínuas.	Baixo. Fazer alterações destrutivas em componentes comuns, como TGW, AD ou outbound (egress), pode afetar somente as cargas de trabalho nessa landing zone específica de várias contas.
Controles de dados e acesso	(Depende) Baixo controle se você quiser se conectar a diferentes redes locais e locais para cargas de trabalho produtivas ADs e não produtivas. A federação SAML, os domínios TGW e os grupos de segurança (SGs) também podem ajudar a implementar os controles necessários.	(Depende) Alto controle se você quiser se conectar a diferentes redes locais e locais para cargas de trabalho produtivas ADs e não produtivas. Use zonas de pouso separadas para requisitos rigorosos de conformidade.
Conformidade e segurança	(Depende) Baixo se houver necessidades estritas de conformidade para separar completamente as cargas de trabalho materiais e não materiais. Controles preventivos e de detetive padrão da AMS em vigor.	(Depende) Até mesmo uma landing zone com várias contas pode ajudar a atingir requisitos rígidos de conformidade ao separar completamente as cargas de trabalho materiais das não materiais. Controles preventivos e de detetive padrão da AMS em vigor.

Recomendação: Sem conformidade estrita ou necessidade multirregional, começar com uma única landing zone com várias contas do AMS alcançaria um bom equilíbrio entre custo, segurança, excelência operacional e complexidade da migração. Você sempre pode configurar uma landing zone adicional, se alguma restrição de conta ou negócio for encontrada.

Zona de pouso com uma única conta versus zona de pouso com várias contas FAQs

Algumas perguntas frequentes ao escolher configurar uma única zona de pouso com várias contas ou várias zonas de destino com várias contas:

P1: Posso começar com uma única landing zone com várias contas e passar para uma landing zone com várias contas, se houver algum limite de conta ou restrição comercial?

R: Sim. Você pode optar por configurar outra landing zone com várias contas a qualquer momento:

- Será necessário configurar uma nova conta de pagador de faturamento (atualmente, a AWS não oferece suporte a contas com vários pagadores em uma única organização da AWS).
- A construção da base da zona de aterrissagem com várias contas leva até 2 semanas após o preenchimento do questionário da zona de aterrissagem com várias contas.
- Cada landing zone com várias contas significa um custo operacional adicional de aproximadamente 3 mil dólares/mês.
- A integração N/W, AD, DNS e SSO será necessária para estabelecer o novo MALZ.
- Quaisquer instâncias reservadas (RIs) e planos de economia de custos precisarão ser configurados para a nova landing zone de várias contas (não RIs são transferíveis).
- A landing zone multiconta do AMS não oferece suporte à migração de uma conta entre contas de várias contas da landing zone; por exemplo, entre organizações da AWS. No entanto, é possível mover aplicativos de uma conta para outra usando métodos de migração padrão.

Q2: Qual é a abordagem da AMS à MALZ updates/changes para underlying/shared infraestrutura e quantificação do risco para os clientes? Forneça detalhes sobre quais garantias estão incluídas no processo. Como os clientes se sentem confortáveis de que o MALZ não updates/changes afetará os clientes? Há alguma medida que o Cliente precise tomar para evitar interrupções?

R: A AMS segue uma metodologia de mudança rígida usando ferramentas internas que nos permitem definir, revisar, programar e executar mudanças nos ambientes dos clientes.

O processo de lançamento de atualizações impõe análises de código, testes de integração, implantação em ambientes gama e beta, além de tempo adicional de preparação e testes em

ambientes beta e gama antes do lançamento para os ambientes dos clientes. Todos os lançamentos incluem procedimentos de reversão e são monitorados de perto pela equipe de lançamentos e pela equipe que criou e solicitou a alteração. O escopo dos lançamentos está limitado às pilhas pertencentes e provisionadas pela AMS. Em média, executamos pelo menos uma versão por semana.

Além disso:

- O AMS SLA é aplicável. De acordo com a descrição do serviço AMS, qualquer incidente gerado após a atividade compartilhada de manutenção de infraestrutura cumpriria o SLA autorizado para resolução ou créditos.
- Nenhuma medida preventiva especial é exigida pelos Clientes para evitar interrupções na infraestrutura comum. Os clientes têm permissões de somente leitura nas contas AWS Org ou Core OU, portanto, os clientes não podem fazer alterações destrutivas no ambiente principal do MALZ. Todas as solicitações do cliente à infraestrutura principal exigem análise e aprovação do AMS.
- Os clientes podem testar determinadas alterações no nível da organização, como SCPs/Roles em níveis individuais de contas não produtivas, antes de propagar as alterações no nível da OU do aplicativo. Está no roteiro do AMS permitir vários APP OUs (segundo trimestre de 2020), o que aliviaria ainda mais o risco de fazer algumas mudanças no nível da ORG. A equipe da MALZ já lançou uma OU separada para contas do “Modo Construção”, para garantir uma segregação clara da propriedade do cliente e controles separados.
- A maioria dessas mudanças permitem que o AMS opere a carga de trabalho de maneira eficaz e eficiente e não necessariamente afeta a carga de trabalho dos clientes. Quando a AMS acredita que uma mudança de infraestrutura compartilhada pode ter um impacto na carga de trabalho dos clientes, ela é então alinhada à janela de mudança dos clientes.

Recomendação de alto nível, comece com várias zonas de destino com várias contas se:

- Se isso ajudar você a obter alguma conformidade específica.
- Se você precisar usar o Multi-Region.
- Se você tiver diferentes cargas de trabalho locais ADs e de redes para Prod/Material cargas de trabalho externasProd/Non-Material workloads, to clearly segregate b/w.

Contas de várias contas da Landing Zone

Tópicos

- Conta de gerenciamento
- Conta de rede
- Conta do Shared Services
- Conta do Log Archive
- Conta de segurança
- Tipos de conta de aplicativo
- Conta do AMS Tools (migrando cargas de trabalho)

Conta de gerenciamento

A conta de gerenciamento é sua conta inicial da AWS quando você inicia a integração com o AMS. Ele utiliza o AWS Organizations como uma conta de gerenciamento (também conhecida como a conta do pagador que paga as cobranças de todas as contas dos membros), o que dá à conta a capacidade de criar e gerenciar financeiramente as contas dos membros. Ele contém a estrutura da AWS landing zone (ALZ), conjuntos de pilhas de configuração de contas, políticas de controle de serviços da AWS Organization (SCPs) etc.

Para obter mais informações sobre como usar uma conta de gerenciamento, consulte Melhores práticas para a conta de gerenciamento.

O diagrama a seguir fornece uma visão geral de alto nível dos recursos contidos na conta de gerenciamento.

Recursos na conta de gerenciamento

Além dos serviços padrão acima, nenhum recurso adicional da AWS é criado na conta de gerenciamento durante a integração. As seguintes informações são necessárias durante a integração no AMS:

- ID da conta de gerenciamento: ID da conta da AWS criada inicialmente por você.
- E-mails de contas principais: forneça os e-mails a serem associados a cada uma das contas principais: rede, serviços compartilhados, registro e conta de segurança.

- Região de serviço: forneça a região da AWS na qual todos os recursos da sua landing zone do AMS serão implantados.

Conta de rede

A conta de rede serve como o hub central para o roteamento de rede entre contas de landing zone com várias contas do AMS, sua rede local e o tráfego de saída para a Internet. Além disso, essa conta contém bastiões públicos da DMZ que são o ponto de entrada para os engenheiros do AMS acessarem os hosts no ambiente AMS. Para obter detalhes, consulte o diagrama de alto nível da conta de rede a seguir.

Arquitetura da conta de rede

O diagrama a seguir mostra o ambiente de landing zone de várias contas do AMS, mostrando os fluxos de tráfego de rede em todas as contas, e é um exemplo de uma configuração altamente disponível.

O AMS configura todos os aspectos da rede para você com base em nossos modelos padrão e nas opções selecionadas fornecidas durante a integração. Um design de rede padrão da AWS é aplicado à sua conta da AWS, e uma VPC é criada para você e conectada ao AMS por VPN ou Direct Connect. Para obter mais informações sobre o Direct Connect, consulte AWS Direct Connect. VPCs Os padrões incluem a DMZ, serviços compartilhados e uma sub-rede de aplicativos. Durante o processo de integração, outros VPCs podem ser solicitados e criados para atender às suas necessidades (por exemplo, divisões de clientes, parceiros). Após a integração, você recebe um diagrama de rede: um documento de ambiente que explica como sua rede foi configurada.

> **Note**
>
> Para obter informações sobre limites e restrições de serviço padrão para todos os serviços ativos, consulte a documentação de limites de serviços da AWS.

Nosso design de rede é construído em torno do "Princípio do Privilégio Mínimo" da Amazon. Para fazer isso, roteamos todo o tráfego, entrada e saída, por meio de uma DMZ, exceto o tráfego

proveniente de uma rede confiável. A única rede confiável é aquela configurada entre seu ambiente local e a VPC por meio do uso de uma and/or VPN e do AWS Direct Connect (DX). O acesso é concedido por meio do uso de instâncias bastion, impedindo assim o acesso direto a quaisquer recursos de produção. Todos os seus aplicativos e recursos residem em sub-redes privadas que podem ser acessadas por meio de balanceadores de carga públicos. O tráfego de saída pública flui pelos Gateways NAT na VPC de saída (na conta de rede) para o Internet Gateway e depois para a Internet. Como alternativa, o tráfego pode fluir pela VPN ou pelo Direct Connect para o ambiente local.

Conectividade de rede privada com o ambiente AMS Multi-account landing zone

A AWS oferece conectividade privada por meio de conectividade de rede privada virtual (VPN) ou linhas dedicadas com o AWS Direct Connect. A conectividade privada em seu ambiente de várias contas é configurada usando um dos métodos descritos a seguir:

- Conectividade de borda centralizada usando o Transit Gateway
- Conectando a and/or VPN Direct Connect (DX) às nuvens privadas virtuais da conta () VPCs

Conectividade de borda centralizada usando gateway de trânsito

O AWS Transit Gateway é um serviço que permite conectar sua rede VPCs e sua rede local a um único gateway. O Transit Gateway (TGW) pode ser usado para consolidar sua conectividade de borda existente e roteá-la por meio de um único ingress/egress ponto. O Transit Gateway é criado na conta de rede do seu ambiente de várias contas do AMS. Para obter mais detalhes sobre o gateway de trânsito, consulte AWS Transit Gateway.

O gateway AWS Direct Connect (DX) é usado para conectar sua conexão DX por meio de uma interface virtual de trânsito ao VPCs ou VPNs que estão conectados ao seu gateway de trânsito. Você associa um gateway do Direct Connect com o gateway de trânsito. Em seguida, crie uma interface virtual de trânsito para sua conexão do AWS Direct Connect com o gateway Direct Connect. Para obter informações sobre interfaces virtuais DX, consulte Interfaces virtuais do AWS Direct Connect.

Essa configuração oferece os benefícios abaixo. É possível:

- Gerencie uma única conexão para várias VPCs ou VPNs que estejam na mesma região da AWS.
- Anuncie prefixos do local para a AWS e da AWS para o local.

> **Note**
>
> Para obter informações sobre o uso de um DX com serviços da AWS, consulte a seção Classic do Resiliency Toolkit. Para obter mais informações, consulte Associações do Transit Gateway.

Para aumentar a resiliência da sua conectividade, recomendamos que você conecte pelo menos duas interfaces virtuais de trânsito de diferentes locais do AWS Direct Connect ao gateway Direct Connect. Para obter mais informações, consulte a recomendação de resiliência do AWS Direct Connect.

Conectando DX ou VPN à conta VPCs

Com essa opção, os ambientes VPCs de landing zone com várias contas do AMS são conectados diretamente ao Direct Connect ou VPN. O tráfego flui diretamente do VPCs para o Direct Connect ou VPN sem passar pelo gateway de trânsito.

Recursos na conta de rede

Conforme mostrado no diagrama da conta de rede, os componentes a seguir são criados na conta e exigem sua entrada.

A conta de rede contém duas VPCs: VPC de saída e VPC DMZ, também conhecida como VPC de perímetro.

Gerente de rede da AWS

O AWS Network Manager é um serviço que permite que você visualize suas redes de gateway de trânsito (TGW) sem custo adicional para o AMS. Ele fornece monitoramento de rede centralizado em recursos da AWS e em redes locais, uma visão global única de sua rede privada em um diagrama de topologia e em um mapa geográfico e métricas de utilização, como status de conexão de bytes. in/out, packets in/out, packets dropped, and alerts for changes in the topology, routing, and up/down Para mais informações, consulte AWS Network Manager.

Use uma das seguintes funções para acessar esse recurso:

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole

- AWSManagedServicesChangeManagementRole

VPC de saída

A VPC de saída é usada principalmente para tráfego de saída para a Internet e é composta por sub-redes em até três zonas public/private de disponibilidade (). AZs Os gateways de conversão de endereços de rede (NAT) são provisionados nas sub-redes públicas e os anexos VPC do gateway de trânsito (TGW) são criados nas sub-redes privadas. O tráfego de saída ou saída da Internet de todas as redes entra pela sub-rede privada via TGW, onde é então roteado para um NAT por meio de tabelas de rotas VPC.

Para aqueles VPCs que contêm aplicativos voltados para o público em uma sub-rede pública, o tráfego proveniente da Internet está contido nessa VPC. O tráfego de retorno não é roteado para o TGW ou para a VPC de saída, mas é roteado de volta pelo gateway da Internet (IGW) na VPC.

> **Note**
>
> Intervalo CIDR da VPC em rede: ao criar uma VPC, você deve especificar uma faixa de endereços IPv4 para a VPC na forma de um bloco de roteamento entre domínios sem classe (CIDR); por exemplo, 10.0.16.0/24. Este é o bloco CIDR principal da VPC.
> A equipe de várias contas da landing zone do AMS recomenda o intervalo de 24 (com mais endereço IP) para fornecer algum buffer caso outros recursos/dispositivos sejam implantados no futuro.

Firewall de saída gerenciado de Palo Alto

O AMS fornece uma solução gerenciada de firewall de saída de Palo Alto, que permite a filtragem do tráfego de saída da Internet para todas as redes no ambiente Multi-Account Landing Zone (excluindo serviços públicos). Essa solução combina a tecnologia de firewall líder do setor (Palo Alto VM-300) com os recursos de gerenciamento de infraestrutura da AMS para implantar, monitorar, gerenciar, escalar e restaurar a infraestrutura em ambientes operacionais compatíveis. Terceiros, incluindo a Palo Alto Networks, não têm acesso aos firewalls; eles são gerenciados exclusivamente pelos engenheiros da AMS.

Controle de tráfego

A solução gerenciada de firewall de saída gerencia uma lista de permissões de domínio composta por domínios exigidos pelo AMS para serviços como backup e patch, bem como seus domínios

definidos. Quando o tráfego de saída da Internet é roteado para o firewall, uma sessão é aberta, o tráfego é avaliado e, se corresponder a um domínio permitido, o tráfego é encaminhado para o destino.

Arquitetura

A solução de firewall de saída gerenciada segue um modelo de alta disponibilidade, em que dois a três firewalls são implantados dependendo do número de zonas de disponibilidade (). AZs A solução utiliza parte do espaço IP da VPC de saída padrão, mas também provisiona uma extensão de VPC (/24) para os recursos adicionais necessários para gerenciar os firewalls.

Fluxo de rede

Em um alto nível, o roteamento do tráfego de saída pública permanece o mesmo, exceto pela forma como o tráfego é roteado para a Internet a partir da VPC de saída:

1. O tráfego de saída destinado à Internet é enviado ao Transit Gateway (TGW) por meio da tabela de rotas da VPC
2. O TGW roteia o tráfego para a VPC de saída por meio da tabela de rotas TGW
3. A VPC roteia o tráfego para a Internet por meio das tabelas de rotas de sub-rede privada
   a. No ambiente padrão da Multi-Account Landing Zone, o tráfego da Internet é enviado diretamente para um gateway de conversão de endereços de rede (NAT). A solução de firewall gerenciado reconfigura as tabelas de rotas da sub-rede privada para apontar a rota padrão (0.0.0.0/0) para uma interface de firewall.

Os firewalls em si contêm três interfaces:

1. Interface confiável: interface privada para receber tráfego a ser processado.
2. Interface não confiável: interface pública para enviar tráfego para a Internet. Como os firewalls executam NAT, os servidores externos aceitam solicitações desses endereços IP públicos.
3. Interface de gerenciamento: interface privada para API de firewall, atualizações, console e assim por diante.

Em todo o roteamento, o tráfego é mantido na mesma zona de disponibilidade (AZ) para reduzir o tráfego entre AZ. O tráfego só passa AZs quando ocorre um failover.

Modificação da lista de permissões

Após a integração, uma lista de permissões padrão chamada `ams-allowlist` é criada, contendo endpoints públicos exigidos pelo AMS, bem como endpoints públicos para corrigir hosts Windows e Linux. Depois de operar, você pode criar RFCs no console AMS na categoria Management | Managed Firewall | Outbound (Palo Alto) para criar ou excluir listas de permissões ou modificar os domínios. Esteja ciente de que `ams-allowlist` não pode ser modificado. Os RFCs são manipulados com automação total (eles não são manuais).

Política de segurança personalizada

As políticas de segurança determinam se uma sessão deve ser bloqueada ou permitida com base nos atributos do tráfego, como a zona de segurança de origem e destino, o endereço IP de origem e destino e o serviço. Políticas de segurança personalizadas são suportadas de forma totalmente automatizada RFCs. CTs a opção para criar ou excluir uma política de segurança pode ser encontrada na categoria Gerenciamento | Firewall Gerenciado | Saída (Palo Alto), e a CT para editar uma política de segurança existente pode ser encontrada na categoria Implantação | Firewall Gerenciado | Saída (Palo Alto). Você poderá criar novas políticas de segurança, modificar políticas de segurança ou excluir políticas de segurança.

> **Note**
>
> A política de segurança padrão `ams-allowlist` não pode ser modificada

CloudWatch Painéis de saída do PA

Dois painéis podem ser encontrados CloudWatch para fornecer uma visão agregada de Palo Alto (PA). O AMS-MF-PA-Egress-Config-Dashboard fornece uma visão geral da configuração do PA, links para listas de permissões e uma lista de todas as políticas de segurança, incluindo seus atributos. O painel AMS-MF-PA-Egress-Dashboard pode ser personalizado para filtrar registros de tráfego. Por exemplo, para criar um painel para uma política de segurança, você pode criar uma RFC com um filtro como:

```
fields @timestamp, @message
| filter @logStream like /pa-traffic-logs/
```

```
| filter @message like /<Security Policy Name>/
| parse @message
 "*,*,*,
```

Os engenheiros do AMS podem realizar a restauração dos backups de configuração, se necessário. Se for necessária uma restauração, ela ocorrerá em todos os hosts para manter a configuração entre os hosts sincronizada.

A restauração também pode ocorrer quando um host exige a reciclagem completa de uma instância. Uma restauração automática do backup mais recente ocorre quando uma nova EC2 instância é provisionada. Em geral, os hosts não são reciclados regularmente e são reservados para falhas graves ou trocas de AMI necessárias. As reciclagens do host são iniciadas manualmente e você é notificado antes que uma reciclagem ocorra.

Além dos backups da configuração do firewall, suas regras específicas da lista de permissões são copiadas separadamente. Um backup é criado automaticamente quando suas regras de lista de permissões definidas são modificadas. A restauração do backup da lista de permissões pode ser realizada por um engenheiro do AMS, se necessário.

Atualizações

A solução AMS Managed Firewall requer várias atualizações ao longo do tempo para adicionar melhorias ao sistema, recursos adicionais ou atualizações ao sistema operacional (SO) ou ao software do firewall.

A maioria das mudanças não afetará o ambiente em execução, como a atualização da infraestrutura de automação, mas outras mudanças, como rotação de instâncias de firewall ou atualização do sistema operacional, podem causar interrupções. Quando uma possível interrupção do serviço devido a atualizações for avaliada, o AMS coordenará com você para acomodar as janelas de manutenção.

Acesso do operador

Os operadores do AMS usam suas ActiveDirectory credenciais para fazer login no dispositivo Palo Alto e realizar operações (por exemplo, aplicar patches, responder a um evento etc.). A solução retém registros padrão de autenticação e alteração de configuração do operador AMS para rastrear as ações realizadas nos Palo Alto Hosts.

Registros padrão

Por padrão, os registros gerados pelo firewall residem no armazenamento local de cada firewall. Com o tempo, os registros locais serão excluídos com base na utilização do armazenamento. A solução AMS fornece o envio em tempo real dos registros das máquinas para CloudWatch os registros; para obter mais informações, consulteCloudWatch Integração de registros.

Os engenheiros do AMS ainda podem consultar e exportar registros diretamente das máquinas, se necessário. Além disso, os registros podem ser enviados para um Panorama de propriedade do cliente; para obter mais informações, consulte. Integração Panorama

Os registros coletados pela solução são os seguintes:

Códigos de status RFC

Tipo de log	Descrição
Tráfego	Exibe uma entrada para o início e o fim de cada sessão. Cada entrada inclui data e hora, zonas de origem e destino, endereços e portas, nome do aplicativo, nome da regra de segurança aplicada ao fluxo, ação da regra (permitir, negar ou descartar), interface de entrada e saída, número de bytes e motivo do término da sessão. A coluna Tipo indica se a entrada é para o início ou o fim da sessão, ou se a sessão foi negada ou cancelada. Uma “queda” indica que a regra de segurança que bloqueou o tráfego especificou “qualquer” aplicativ o, enquanto uma “negação” indica que a regra identificou um aplicativo específico. Se o tráfego for descartado antes que o aplicativo seja identificado, como quando uma regra elimina todo o tráfego de um serviço específico, o aplicativo é mostrado como “não aplicável”.
Ameaça	Exibe uma entrada para cada alarme de segurança gerado pelo firewall. Cada entrada inclui a data e a hora, o nome ou URL da ameaça, as zonas de origem e destino, endereços e portas, o nome do aplicativo e a ação do alarme (permitir ou bloquear) e a gravidade. A coluna Tipo indica o tipo de ameaça, como “vírus” ou “spyware”; a coluna Nome é a descrição ou URL da ameaça; e a coluna Categoria é a categoria de ameaça (como “keylogger”) ou categoria de URL.
Filtragem de URL	Exibe registros de filtros de URL, que controlam o acesso a sites e se os usuários podem enviar credenciais para sites.
Configuração	Exibe uma entrada para cada alteração de configuração. Cada entrada inclui a data e a hora, o nome de usuário do administrador, o endereço

Tipo de log	Descrição
	IP de onde a alteração foi feita, o tipo de cliente (interface web ou CLI), o tipo de comando executado, se o comando foi bem-sucedido ou falhou, o caminho de configuração e os valores antes e depois da alteração.
Sistema	Exibe uma entrada para cada evento do sistema. Cada entrada inclui a data e a hora, a gravidade do evento e uma descrição do evento.
alarmes	O registro de alarmes registra informações detalhadas sobre os alarmes gerados pelo sistema. As informações nesse registro também são relatadas em Alarmes. Consulte “Definir configurações de alarme”.
Autenticação	Exibe informações sobre eventos de autenticação que ocorrem quando os usuários finais tentam acessar recursos de rede cujos acessos são controlados pelas regras da política de autenticação. Os usuários podem usar essas informações para ajudar a solucionar problemas de acesso e ajustar a política de autenticação do usuário conforme necessário. Em conjunto com objetos de correlação, os usuários também podem usar os registros de autenticação para identificar atividades suspeitas na rede do usuário, como ataques de força bruta. Opcionalmente, os usuários podem configurar as regras de autentica ção para registrar os tempos limite de autenticação. Esses tempos limite estão relacionados ao período em que um usuário precisa se autentica r para um recurso apenas uma vez, mas pode acessá-lo repetidamente. Ver informações sobre os tempos limite ajuda os usuários a decidir se e como ajustá-los.
Unificado	Exibe as entradas mais recentes do registro de tráfego, ameaças, filtragem de URL, WildFire envios e filtragem de dados em uma única visualização. A visualização coletiva de registros permite que os usuários investiguem e filtrem esses diferentes tipos de registros juntos (em vez de pesquisar cada conjunto de registros separadamente). Ou os usuários podem escolher quais tipos de registro exibir: clique na seta à esquerda do campo de filtro e selecione tráfego, ameaça, URL, dados, and/or incêndio para exibir somente os tipos de registro selecionados.

Gerenciamento de eventos

O AMS monitora continuamente a capacidade, o status de saúde e a disponibilidade do firewall. As métricas geradas pelo firewall, bem como as métricas AWS/AMS geradas, são usadas para criar alarmes que são recebidos pelos engenheiros de operações do AMS, que investigarão e resolverão o problema. Os alarmes atuais abrangem os seguintes casos:

Alarmes de eventos:

- Utilização da CPU do Firewall Dataplane
  - Utilização da CPU - CPU do Dataplane (tráfego de processamento)
- A utilização do pacote de plano de dados do firewall está acima de 80%
  - Utilização de pacotes - Dataplane (processamento de tráfego)
- Utilização da sessão do Firewall Dataplane
- Sessão ativa do Firewall Dataplane
- Utilização agregada da CPU do firewall
  - Utilização da CPU em todos CPUs
- Failover pela AZ
  - Alarmes quando ocorre um failover em uma AZ
- Host de Syslog não íntegro
  - O host do Syslog falha na verificação de integridade

Alarmes de gerenciamento:

- Alarme de falha do Health Check Monitor
  - Quando o fluxo de trabalho de verificação de integridade falha inesperadamente
  - Isso é para o fluxo de trabalho em si, não se uma verificação de integridade do firewall falhar
- Alarme de falha de rotação de senha
  - Quando a rotação da senha falha
  - A senha do usuário da API/serviço é trocada a cada 90 dias

Métricas

Todas as métricas são capturadas e armazenadas CloudWatch na conta de rede. Eles podem ser visualizados obtendo acesso ao console à conta de rede e navegando até o CloudWatch console.

Métricas individuais podem ser visualizadas na guia de métricas ou em um painel de painel único de métricas selecionadas e métricas agregadas podem ser visualizadas navegando até a guia Painel e selecionando AMS-MF-PA-Egress-Dashboard.

Métricas personalizadas:

- Verificação de integridade
  - Namespace: AMS/MF/PA/Egress
    - PARouteTableConnectionsByAZ
    - PAUnhealthyByInstance
    - PAUnhealthyAggregatedByAZ
    - PAHealthCheckLockState
- Firewall gerado
  - Espaço para nomes:/AMS/MF/PA/Egress<instance-id>
    - DataPlaneCPUUtilizationPct
    - DataPlanePacketBuffferUtilization
    - panela GPGateway UtilizationPct
    - panSessionActive
    - panSessionUtilization

CloudWatch Integração de registros

CloudWatch A integração de registros encaminha os registros dos firewalls para o CloudWatch Logs, o que reduz o risco de perda de registros devido à utilização do armazenamento local. Os registros são preenchidos em tempo real à medida que os firewalls os geram e podem ser visualizados sob demanda por meio do console ou da API.

Consultas complexas podem ser criadas para análise de registros ou exportadas para CSV usando o Insights. CloudWatch Além disso, o CloudWatch painel personalizado do AMS Managed Firewall também mostrará uma visão rápida de consultas específicas de registros de tráfego e uma visualização gráfica do tráfego e dos impactos de políticas ao longo do tempo. A utilização de CloudWatch registros também permite a integração nativa com outros serviços da AWS, como o AWS Kinesis.

> **Note**
>
> Os registros de PA não podem ser encaminhados diretamente para um coletor Syslog existente no local ou de terceiros. A solução AMS Managed Firewall fornece o envio em tempo real dos registros das máquinas de PA para o AWS CloudWatch Logs. Você pode usar o recurso CloudWatch Logs Insight para executar consultas ad-hoc. Além disso, os registros podem ser enviados para a solução de gerenciamento de Panorama de Palo Alto. CloudWatch os registros também podem ser encaminhados para outros destinos usando filtros de CloudWatch assinatura. Saiba mais sobre Panorama na seção a seguir. Para saber mais sobre o Splunk, consulte Integração com o Splunk.

Integração Panorama

O AMS Managed Firewall pode, opcionalmente, ser integrado ao seu Panorama existente. Isso permite que você visualize as configurações do firewall do Panorama ou encaminhe os registros do firewall para o Panorama. A integração do Panorama com o AMS Managed Firewall é somente para leitura, e as alterações de configuração nos firewalls do Panorama não são permitidas. O Panorama é totalmente gerenciado e configurado por você. O AMS será responsável apenas por configurar os firewalls para se comunicar com ele.

Licenciamento

O preço do AMS Managed Firewall depende do tipo de licença usada, por hora ou traga sua própria licença (BYOL), e do tamanho da instância na qual o dispositivo é executado. Você deve solicitar o tamanho das instâncias e as licenças do firewall de Palo Alto de sua preferência por meio do AWS Marketplace.

- Licenças do Marketplace: aceite os termos e condições do VM-Series Next-Generation Firewall Bundle 1 da conta de rede no MALZ.
- Licenças BYOL: aceite os termos e condições do VM-Series Next-Generation Firewall (BYOL) da conta de rede no MALZ e compartilhe o “código de autenticação BYOL” obtido após a compra da licença para a AMS.

Limitações

No momento, o AMS oferece suporte ao firewall da série VM-300 ou da série VM-500. As configurações podem ser encontradas aqui: Modelos da série VM em instâncias da AWS, EC2

> **Note**
>
> A solução AMS é executada no modo Ativo-Ativo, pois cada instância de PA em sua AZ processa o tráfego de saída de sua respectiva AZ. Portanto, com duas AZs, cada instância PA processa o tráfego de saída de até 5 Gbps e fornece efetivamente uma taxa de transferência geral de 10 Gbps em duas. AZs O mesmo vale para todos os limites em cada AZ. Se a verificação de integridade do AMS falhar, transferimos o tráfego da AZ com o PA incorreto para outra AZ e, durante a substituição da instância, a capacidade é reduzida até os AZs limites restantes.
>
> Atualmente, o AMS não oferece suporte a outros pacotes de Palo Alto disponíveis no AWS Marketplace; por exemplo, você não pode solicitar o “VM-Series Next-Generation Firewall Bundle 2". Observe que a solução AMS Managed Firewall usando Palo Alto atualmente fornece apenas uma oferta de filtragem de tráfego de saída, portanto, o uso de pacotes avançados da série VM não forneceria nenhum recurso ou benefício adicional.

Requisitos de integração

- Você deve revisar e aceitar os termos e condições do firewall de próxima geração da série VM de Palo Alto no AWS Marketplace.
- Você deve confirmar o tamanho da instância que deseja usar com base na carga de trabalho esperada.
- Você deve fornecer um bloco CIDR /24 que não entre em conflito com as redes em seu ambiente de zona de destino de várias contas ou no local. Ela deve ser da mesma classe da VPC de saída (a solução fornece uma extensão de VPC /24 para a VPC de saída).

Preços

Os custos da infraestrutura básica do AMS Managed Firewall são divididos em três fatores principais: a EC2 instância que hospeda o firewall Palo Alto, a licença de software, as licenças da série VM da Palo Alto e as integrações. CloudWatch

Os preços a seguir são baseados no firewall da série VM-300.

- EC2 Instâncias: O firewall de Palo Alto é executado em um modelo de alta disponibilidade de 2 a 3 EC2 instâncias, em que a instância é baseada nas cargas de trabalho esperadas. O custo da instância depende da região e do número de AZs

  - Por exemplo, us-east-1, m5.xlarge, 3 AZs
    - $0,192 * 24 * 30* 3 = $414,72
  - https://aws.amazon.com/ec2/preços/sob demanda/
- Licenças Palo Alto: O custo da licença de software de um firewall de próxima geração do Palo Alto VM-300 depende do número de AZ e do tipo de instância.
  - Por exemplo, us-east-1, m5.xlarge, 3 AZs
    - $0,87 * 24 * 30* 3 = $1879,20
    - https://aws.amazon.com/marketplace/PP/B083M7JPKB? ref_=srh_res_product_title #pdp - pricing
- CloudWatch Integração de CloudWatch registros: a integração de registros utiliza SysLog servidores (EC2 - t3.medium), NLB e registros. CloudWatch O custo dos servidores é baseado na região e no número de AZs, e o custo dos NLB/CloudWatch registros varia de acordo com a utilização do tráfego.
  - Por exemplo, us-east-1, t3.medium, 3AZ
    - 0,0416 USD* 24 * 30* 3 = 89,86 US$
  - https://aws.amazon.com/ec2/preços/sob demanda/
  - https://aws.amazon.com/cloudwatch/preços/

Perímetro (DMZ) VPC

O VPC Perimeter, ou DMZ, contém os recursos necessários para que os engenheiros de operações do AMS acessem as redes AMS. Ele contém sub-redes públicas de 2 a 3 AZs, com hosts SSH Bastions em um grupo de Auto Scaling (ASG) para os engenheiros de operações do AMS acessarem ou passarem por túneis. Os grupos de segurança conectados aos bastiões da DMZ contêm regras de entrada da porta 22 da Amazon Corp Networks.

Intervalo CIDR DMZ VPC: ao criar uma VPC, você deve especificar uma faixa de endereços IPv4 para a VPC na forma de um bloco de roteamento entre domínios sem classe (CIDR); por exemplo, 10.0.16.0/24. Este é o bloco CIDR principal da VPC.

> **Note**
>
> A equipe do AMS recomenda o intervalo de 24 (com mais endereço IP) para fornecer algum buffer caso outros recursos, como um firewall, sejam implantados no futuro.

AWS Transit Gateway

O AWS Transit Gateway (TGW) é um serviço que permite conectar suas Amazon Virtual Private Clouds (VPCs) e suas redes locais a um único gateway. O Transit Gateway é o backbone de rede que gerencia o roteamento entre redes de contas AMS e redes externas. Para obter informações sobre o Transit Gateway, consulte AWS Transit Gateway.

Forneça a seguinte entrada para criar esse recurso:

- Número ASN do Transit Gateway *: forneça o Número do Sistema Autônomo (ASN) privado para seu gateway de trânsito. Ele deve ser o ASN para o lado da AWS de uma sessão de Border Gateway Protocol (BGP). O intervalo é de 64512 a 65534 para 16 bits. ASNs

Conta do Shared Services

A conta de Serviços Compartilhados serve como hub central para a maioria dos serviços de plano de dados do AMS. A conta contém a infraestrutura e os recursos necessários para gerenciamento de acesso (AD), gerenciamento de segurança de terminais (Trend Micro) e contém os bastiões do cliente (SSH/RDP). Uma visão geral de alto nível dos recursos contidos na Conta de Serviços Compartilhados é mostrada no gráfico a seguir.

A VPC do Shared Services é composta pela sub-rede AD, pela sub-rede EPS e pela sub-rede Customer Bastions nas três zonas de disponibilidade (). AZs Os recursos criados na VPC do Shared Services estão listados abaixo e exigem sua contribuição.

- Intervalo CIDR da VPC do Shared Services: ao criar uma VPC, você deve especificar uma faixa de endereços IPv4 para a VPC na forma de um bloco de roteamento entre domínios sem classe (CIDR); por exemplo, 10.0.1.0/24. Este é o bloco CIDR principal da VPC.

  > **Note**
  >
  > A equipe do AMS recomenda o intervalo de /23.

- Detalhes do Active Directory: O Microsoft Active Directory (AD) é utilizado para user/resource gerenciamento, autenticação/autorização e DNS em todas as suas contas de landing zone com várias contas do AMS. O AMS AD também é configurado com uma confiança unidirecional em seu Active Directory para autenticação baseada em confiança. A entrada a seguir é necessária para criar o AD:

  - Nome de domínio totalmente qualificado (FQDN): o nome de domínio totalmente qualificado para o diretório AWS Managed Microsoft AD. O domínio não deve ser um domínio existente ou um domínio secundário de um domínio existente na sua rede.
  - Nome NetBIOS do domínio: Se você não especificar um nome NetBIOS, o AMS padronizará o nome para a primeira parte do DNS do seu diretório. Por exemplo, corp para o diretório DNS corp.example.com.

- Trend Micro — segurança de proteção de terminais (EPS): A proteção de terminais (EPS) da Trend Micro é o principal componente do AMS para segurança do sistema operacional. O sistema é composto pelo Deep Security Manager (DSM), EC2 instâncias, instâncias de retransmissão e um agente presente em todas as EC2 instâncias do plano de dados e do cliente. EC2

  Você deve assumir o `EPSMarketplaceSubscriptionRole` na conta de Serviços Compartilhados e assinar a AMI do Trend Micro Deep Security (BYOL) ou o Trend Micro Deep Security (Marketplace).

  As seguintes entradas padrão são necessárias para criar o EPS (se você quiser mudar dos padrões):

  - Tipo de instância de retransmissão: valor padrão - m5.large
  - Tipo de instância DSM: valor padrão - m5.xlarge
  - Tamanho da instância de banco de dados: valor padrão - 200 GB
  - Tipo de instância do RDS: valor padrão - db.m5.large

- Bastions do cliente: você recebe bastiões SSH ou RDP (ou ambos) na Conta de Serviços Compartilhados para acessar outros hosts em seu ambiente AMS. Para acessar a rede AMS como usuário (SSH/RDP), you must use "customer" Bastions as the entry point. The network path originates from the on-premise network, goes through DX/VPNpara o gateway de trânsito (TGW) e, em seguida, ser roteada para a VPC do Shared Services. Depois de acessar o bastion, você pode ir para outros hosts no ambiente AMS, desde que a solicitação de acesso tenha sido concedida.
  - As seguintes entradas são necessárias para os bastiões SSH.
    - Capacidade de instância desejada do SSH Bastion: valor padrão - 2.
    - Instâncias máximas do SSH Bastion: valor padrão - 4.
    - Instâncias mínimas do SSH Bastion: valor padrão -2.

- Tipo de instância SSH Bastion: Valor padrão - m5.large (pode ser alterado para economizar custos; por exemplo, um t3.medium).
- SSH Bastion Ingress CIDRs: intervalos de endereços IP a partir dos quais os usuários da sua rede acessam o SSH Bastions.

- As entradas a seguir são necessárias para os bastiões do Windows RDP.
  - Tipo de instância do RDP Bastion: Valor padrão - t3.medium.
  - Sessões mínimas desejadas do RDP Bastion: valor padrão - 2.
  - Sessões máximas de RDP: valor padrão -10.
  - Tipo de configuração RDP Bastion: Você pode escolher uma das configurações abaixo
    - SecureStandard = Um usuário recebe um bastião e somente um usuário pode se conectar ao bastião.
    - SecureHA = Um usuário recebe dois bastiões em duas AZs diferentes para se conectar e somente um usuário pode se conectar ao bastião.
    - SharedStandard = Um usuário recebe um bastião para se conectar e dois usuários podem se conectar ao mesmo bastião ao mesmo tempo.
    - SharedHA = Um usuário recebe dois bastiões em duas AZs diferentes para se conectar e dois usuários podem se conectar ao mesmo bastião ao mesmo tempo.
  - Entrada RDP do cliente CIDRs: intervalos de endereços IP a partir dos quais os usuários da sua rede acessarão o RDP Bastions.

Atualizações nos serviços compartilhados: Zona de destino com várias contas

O AMS aplica lançamentos de planos de dados às contas gerenciadas mensalmente, sem aviso prévio.

O AMS usa a OU principal para fornecer serviços compartilhados, como acesso, rede, EPS, armazenamento de registros e agregação de alertas em sua zona de destino de várias contas. O AMS é responsável por lidar com vulnerabilidades, corrigir e implantar esses serviços compartilhados. O AMS atualiza regularmente os recursos usados para fornecer esses serviços compartilhados para que os usuários tenham acesso aos recursos mais recentes e às atualizações de segurança. As atualizações geralmente acontecem mensalmente. Os recursos que fazem parte dessas atualizações são:

- Contas que fazem parte da OU principal.

A conta de gerenciamento, a conta de serviços compartilhados, a conta de rede, a conta de segurança e a conta de arquivamento de registros têm recursos para bastiões RDP e SSH, proxies, hosts de gerenciamento e segurança de endpoint (EPS), que normalmente são atualizados todos os meses. O AMS usa EC2 implantações imutáveis como parte da infraestrutura de serviços compartilhados.

- Novo AMS AMIs incorporando as atualizações mais recentes.

> **Note**
>
> Os operadores do AMS utilizam um tipo de alteração de supressão de alarme (CT) interno ao executar alterações no plano de dados e o RFC desse CT aparece na sua lista de RFC. Isso ocorre porque, à medida que a versão do plano de dados é implantada, várias infraestruturas podem ser desligadas, reinicializadas, colocadas off-line, ou pode haver picos de CPU ou outros efeitos da implantação que acionam alarmes que, durante a implantação do plano de dados, são estranhos. Quando a implantação estiver concluída, verifica-se que toda a infraestrutura está funcionando corretamente e os alarmes são reativados.

Conta do Log Archive

A conta Log Archive serve como o hub central para arquivar registros em seu ambiente de landing zone com várias contas do AMS. Há um bucket S3 na conta que contém cópias dos arquivos de log do AWS CloudTrail e do AWS Config de cada uma das contas do ambiente de landing zone de várias contas do AMS. Você pode usar essa conta para sua solução de registro centralizado com AWS Firehose, Splunk e assim por diante. O acesso do AMS a essa conta é limitado a alguns usuários; restrito a auditores e equipes de segurança para investigações forenses e de conformidade relacionadas à atividade da conta.

Conta de segurança

A conta Security é o hub central para abrigar as operações relacionadas à segurança e o ponto principal para canalizar notificações e alertas para os serviços do plano de controle da AMS. Além disso, a conta de segurança abriga a conta de gerenciamento do Amazon Guard Duty e o agregador AWS Config.

Tipos de conta de aplicativo

As contas de aplicativos são contas da AWS dentro da arquitetura de landing zone gerenciada pela AMS que você usa para hospedar suas cargas de trabalho. O AMS oferece três tipos de contas de aplicativos:

- Contas de aplicativos gerenciadas pela AMS
- Contas AMS Accelerate
- Contas de aplicativos gerenciadas pelo cliente

As contas de aplicativos são agrupadas OUs em diferentes organizações da AWS, dependendo do tipo de conta de aplicativo:

- UO raiz:
  1. Aplicativos OU
     - OU gerenciada: contas gerenciadas pelo AMS
     - OU de desenvolvimento: contas gerenciadas pela AMS com o modo Desenvolvedor ativado
  2. Acelere a OU: contas de aplicativos AMS Accelerate
  3. OU gerenciada pelo cliente: contas de aplicativos gerenciadas pelo cliente

As contas de aplicativos são provisionadas por meio de uma RFC enviada pela conta de gerenciamento:

- Crie uma conta de aplicativo com VPC ct-1zdasmc2ewzrs
- Criar conta de aceleração ct-2p93tyd5angmi
- Crie uma conta de aplicativo gerenciada pelo cliente ct-3pwbixz27n3tn

Contas de aplicativos gerenciadas pela AMS

As contas de aplicativos que são totalmente gerenciadas pelo AMS são chamadas de contas de aplicativos gerenciadas pelo AMS, em que algumas ou todas as tarefas operacionais, como gerenciamento de solicitações de serviços, gerenciamento de incidentes, gerenciamento de segurança, gerenciamento de continuidade (backup), gerenciamento de patches, otimização de custos ou monitoramento e gerenciamento de eventos da infraestrutura, são executadas pelo AMS.

A quantidade de tarefas executadas pelo AMS depende do modo de gerenciamento de alterações selecionado. As contas gerenciadas pelo AMS oferecem suporte a diferentes modos de gerenciamento de mudanças:

- Modo RFC
- Modo de mudança direta no AMS
- AMS e AWS Service Catalog
- Modo AMS Advanced Developer
- Modo de provisionamento de autoatendimento no AMS

Para obter mais informações sobre gerenciamento de mudanças e modos diferentes, consulteModos de gerenciamento de alterações.

Há alguns serviços da AWS que você pode usar em sua conta gerenciada pelo AMS sem o gerenciamento do AMS. A lista desses serviços da AWS e como adicioná-los à sua conta do AMS estão descritos na seção Provisionamento de autoatendimento.

Contas AMS Accelerate

O AMS Accelerate é o plano de operações do AMS que pode operar a infraestrutura da AWS que suporta cargas de trabalho. Você pode se beneficiar dos serviços operacionais do AMS Accelerate, como monitoramento e alertas, gerenciamento de incidentes, gerenciamento de segurança e gerenciamento de backup, sem passar por uma nova migração, passar por períodos de inatividade ou alterar a forma como você usa a AWS. O AMS Accelerate também oferece um complemento de patch opcional para cargas de trabalho EC2 baseadas que exigem patches regulares.

Com o AMS Accelerate, você tem a liberdade de usar, configurar e implantar todos os serviços da AWS de forma nativa ou com suas ferramentas preferidas. Você usará seus mecanismos preferidos de acesso e mudança, enquanto o AMS aplica consistentemente práticas comprovadas que ajudam a escalar sua equipe, otimizar custos, aumentar a segurança e a eficiência e melhorar a resiliência.

> **Note**
>
> As contas do AMS Accelerate no AMS Advanced não têm o gerenciamento de alterações do AMS (RFCs) ou o console do AMS Advanced. Em vez disso, eles têm o console e a funcionalidade do AMS Accelerate.

As contas Accelerate só podem ser provisionadas a partir de sua conta de gerenciamento de landing zone multiconta do AMS. O Accelerate oferece diferentes capacidades operacionais. Para saber mais, consulte a descrição do serviço Accelerate.

- Você continuará aproveitando alguns dos recursos das contas principais do multi-account landing zone (MALZ), como registro centralizado, cobrança única, Config Aggregator na conta de segurança e. SCPs
- O AMS Accelerate não fornece alguns serviços avançados do AMS, como EPS, gerenciamento de acesso, gerenciamento de alterações e provisionamento. Recomendamos que você siga as próximas etapas para obter acesso e configurar o gateway de trânsito (TGW).

Para obter mais detalhes sobre o Accelerate, consulte O que é Accelerate.

Criando sua conta Accelerate

Para criar uma conta do Accelerate, siga as etapas descritas aqui Crie uma conta do Accelerate.

Acessando sua conta Accelerate

Depois de provisionar uma conta Accelerate em sua conta multi-account landing zone (MALZ), uma função com permissões de acesso administrativo está na conta para você assumir. `AccelerateDefaultAdminRole`

Para acessar a nova conta do Accelerate:

1. Faça login no console do IAM da conta de gerenciamento com a `CustomerDefaultAssumeRole` função.
2. No console do IAM, na barra de navegação, escolha seu nome de usuário.
3. Selecione Mudar de perfil. Se esta for a primeira vez que esta opção é selecionada, uma página será exibida com mais informações. Depois de ler, escolha Switch Role (Mudar de função). Se você limpar seus cookies do navegador, esta página poderá ser exibida novamente.
4. Na página Alternar função, digite o ID da conta Accelerate e o nome da função a ser assumida:`AccelerateDefaultAdminRole`.

Agora que você tem acesso, pode criar novas funções do IAM para continuar acessando seu ambiente. Se você quiser aproveitar o SAML Federation para sua conta do Accelerate, consulte Habilitar usuários federados do SAML 2.0 para acessar o AWS Management Console.

Conectando sua conta Accelerate ao Transit Gateway

O AMS não gerencia a configuração de rede de uma conta do Accelerate. Você tem a opção de gerenciar sua própria rede usando a AWS APIs (consulte Soluções de rede) ou conectar-se à rede MALZ gerenciada pelo AMS, usando o Transit Gateway (TGW) existente implantado no AMS MALZ.

> **Note**
>
> Você só pode ter uma VPC conectada ao TGW se a conta Accelerate estiver na mesma região da AWS. Para obter mais informações, consulte Transit Gateways.

Para adicionar sua conta Accelerate ao Transit Gateway, solicite uma nova rota usando o tipo de alteração Deployment | Managed landing zone | Networking account | Add static route (ct-3r2ckznmt0a59) e inclua estas informações:

- Blackhole: Verdadeiro para indicar que o alvo da rota não está disponível. Faça isso quando o tráfego da rota estática for descartado pelo Transit Gateway. Falso para rotear o tráfego para o ID de anexo TGW especificado. O valor padrão é falso.
- DestinationCidrBlock: o intervalo IPV4 CIDR usado para correspondências de destino. As decisões de roteamento são baseadas na correspondência mais específica. Exemplo: 10.0.2.0/24.
- TransitGatewayAttachmentId: O ID do anexo TGW que servirá como destino da tabela de rotas. Se Blackhole for falso, esse parâmetro será obrigatório, caso contrário, deixe esse parâmetro em branco. Exemplo: tgw-attach-04eb40d1e14ec7272.
- TransitGatewayRouteTableId: O ID da tabela de rotas do TGW. Exemplo: tgw-rtb-06ddc751c0c0c881c.

Crie rotas nas tabelas de rotas do TGW para se conectar a essa VPC:

1. Por padrão, essa VPC não poderá se comunicar com nenhuma outra VPCs na sua rede MALZ.
2. Decida com seu arquiteto de soluções com o que VPCs você deseja que essa Accelerate VPC se comunique.
3. Envie uma implantação | Managed landing zone | Conta de rede | Adicione o tipo de alteração da rota estática (ct-3r2ckznmt0a59), inclua estas informações:
   - Blackhole: Verdadeiro para indicar que o alvo da rota não está disponível. Faça isso quando o tráfego da rota estática for descartado pelo Transit Gateway. Falso para rotear o tráfego para o ID de anexo TGW especificado. O valor padrão é falso.

- DestinationCidrBlock: o intervalo IPV4 CIDR usado para correspondências de destino. As decisões de roteamento são baseadas na correspondência mais específica. Exemplo: 10.0.2.0/24.
- TransitGatewayAttachmentId: O ID do anexo TGW que servirá como destino da tabela de rotas. Se Blackhole for falso, esse parâmetro será obrigatório, caso contrário, deixe esse parâmetro em branco. Exemplo: tgw-attach-04eb40d1e14ec7272.
- TransitGatewayRouteTableId: O ID da tabela de rotas do TGW. Exemplo: tgw-rtb-06ddc751c0c0c881c.

Conectando uma nova conta Accelerate VPC à rede AMS Multi-Account Landing Zone (criando um anexo TGW VPC):

1. Em sua conta de rede multi-conta landing zone, abra o console Amazon VPC.
2. No painel de navegação, selecione Gateways de trânsito. Registre o ID TGW do gateway de trânsito que você vê.
3. Na sua conta do Accelerate, abra o console da Amazon VPC.
4. No painel de navegação, escolha Transit Gateway Attachments > Create Transit Gateway Attachments. Faça essas escolhas:
   - Para a ID do Transit Gateway, escolha a ID do Transit Gateway que você registrou na Etapa 2.
   - Em Tipo de anexo, escolha VPC.
   - Como opção, em VPC Attachment (Anexo da VPC), insira um nome para Attachment name tag (Tag de nome do anexo).
   - Escolha se deseja ativar o DNS Support and IPv6 Support.
   - Em ID da VPC, escolha a VPC a ser anexada ao gateway de trânsito. Essa VPC precisa estar associada a pelo menos uma sub-rede.
   - Em Sub-rede IDs, selecione uma sub-rede para cada zona de disponibilidade a ser usada pelo gateway de trânsito para rotear o tráfego. É necessário selecionar pelo menos uma sub-rede. Você pode selecionar somente uma sub-rede por zona de disponibilidade.
5. Escolha Create attachment (Criar anexo). Registre a ID do anexo TGW recém-criado.

Associando o anexo TGW a uma tabela de rotas:

1. Decida a qual tabela de rotas do TGW você deseja associar a VPC. Recomendamos criar uma nova tabela de rotas de aplicativos para a conta Accelerate VPCs usando o tipo de alteração

Deployment | Managed landing zone | Networking account | Create transit gateway route table (ct-3dscwaeyi6cup).

2. Envie um RFC Management | Managed landing zone | Networking | Associe o anexo TGW (ct-3nmhh0qr338q6) na conta de rede para associar o anexo VPC ou TGW à tabela de rotas selecionada.

Crie rotas nas tabelas de rotas do TGW para se conectar a essa VPC:

1. Por padrão, essa VPC não conseguirá se comunicar com nenhuma outra VPCs na sua rede de landing zone de várias contas.
2. Decida com seu arquiteto de soluções com o que VPCs você deseja que essa conta Accelerate VPC se comunique.
3. Envie uma implantação | Managed landing zone | Conta de rede | Adicione uma rota estática (ct-3r2ckznmt0a59) RFC à conta de rede para criar as rotas TGW de que você precisa.

Configurando suas tabelas de rotas VPC para apontar para o gateway de trânsito multiconta da landing zone do AMS:

1. Decida com seu arquiteto de soluções qual tráfego você deseja enviar para o gateway de trânsito do AMS Multi-Account Landing Zone.
2. Envie uma implantação | Managed landing zone | Conta de rede | Adicione uma rota estática (ct-3r2ckznmt0a59) RFC à conta de rede para criar as rotas TGW de que você precisa.

Contas de aplicativos gerenciadas pelo cliente

Você pode criar contas que o AMS não gerencia da maneira padrão. Essas contas são chamadas de contas gerenciadas pelo cliente e oferecem controle total para operar a infraestrutura dentro das contas por conta própria, enquanto aproveita os benefícios da arquitetura centralizada gerenciada pelo AMS.

As contas gerenciadas pelo cliente não têm acesso ao console do AMS nem a nenhum dos serviços que fornecemos (patch, backup etc.).

As contas gerenciadas pelo cliente só podem ser provisionadas a partir da sua conta de gerenciamento de landing zone com várias contas do AMS.

Diferentes modos do AMS funcionam com contas de aplicativos de forma diferente; para saber mais sobre os modos, consulte os modos do AWS Managed Services.

Para criar sua conta de aplicativo gerenciada pelo cliente, consulte Conta de gerenciamento | Criar conta de aplicativo gerenciada pelo cliente.

Para excluir uma conta de aplicativo gerenciada pelo cliente, use Conta de gerenciamento | Conta de aplicativo externo. (O Confirm Offboarding CT não se aplica às contas de aplicativos gerenciados pelo cliente.)

Acessando sua conta gerenciada pelo cliente

Depois de provisionar uma conta gerenciada pelo cliente (CMA) na landing zone de várias contas, (MALZ), uma função de administrador,`CustomerDefaultAdminRole`, está na conta para você assumir, por meio da federação SAML, configurar a conta.

Para acessar o CMA:

1. Faça login no console do IAM da conta de gerenciamento com a CustomerDefaultAssumeRolefunção.
2. No console do IAM, na barra de navegação, escolha seu nome de usuário.
3. Selecione Mudar de perfil. Se esta for a primeira vez que esta opção é selecionada, uma página será exibida com mais informações. Depois de ler, escolha Switch Role (Mudar de função). Se você limpar seus cookies do navegador, esta página poderá ser exibida novamente.
4. Na página Alternar função, digite o ID da conta gerenciada pelo cliente e o nome da função a ser assumida: CustomerDefaultAdminRole.

Agora que você tem acesso, pode criar novas funções do IAM para continuar acessando seu ambiente. Se você quiser aproveitar o SAML Federation para sua conta do CMA, consulte Habilitar usuários federados do SAML 2.0 para acessar o AWS Management Console.

Conectando seu CMA com o Transit Gateway

O AMS não gerencia a configuração de rede das contas gerenciadas pelo cliente (CMAs). Você tem a opção de gerenciar sua própria rede usando a AWS APIs (consulte Soluções de rede) ou conectar-se à rede de várias contas de landing zone gerenciada pelo AMS, usando o Transit Gateway (TGW) existente implantado no AMS MALZ.

> **Note**
>
> Você só pode ter uma VPC conectada ao TGW se o CMA estiver na mesma região da AWS. Para obter mais informações, consulte Transit Gateways.

Para adicionar seu CMA ao Transit Gateway, solicite uma nova rota com a conta de rede | Adicione o tipo de alteração da rota estática (ct-3r2ckznmt0a59) e inclua estas informações:

- Blackhole: Verdadeiro para indicar que o alvo da rota não está disponível. Faça isso quando o tráfego da rota estática for descartado pelo Transit Gateway. Falso para rotear o tráfego para o ID de anexo TGW especificado. O valor padrão é falso.
- DestinationCidrBlock: o intervalo IPV4 CIDR usado para correspondências de destino. As decisões de roteamento são baseadas na correspondência mais específica. Exemplo: `10.0.2.0/24`.
- TransitGatewayAttachmentId: O ID do anexo TGW que servirá como destino da tabela de rotas. Se Blackhole for falso, esse parâmetro será obrigatório, caso contrário, deixe esse parâmetro em branco. Exemplo: `tgw-attach-04eb40d1e14ec7272`.
- TransitGatewayRouteTableId: O ID da tabela de rotas do TGW. Exemplo: `tgw-rtb-06ddc751c0c0c881c`.

Conectando uma nova VPC gerenciada pelo cliente à rede AMS Multi-Account Landing Zone (criando um anexo TGW VPC):

1. Na sua conta de rede de várias contas na landing zone, abra o console da Amazon VPC.
2. No painel de navegação, escolha Transit Gateways. Registre o ID TGW do gateway de trânsito que você vê.
3. Na sua conta gerenciada pelo cliente, abra o console da Amazon VPC.
4. No painel de navegação, escolha Transit Gateway Attachments > Create Transit Gateway Attachments. Faça essas escolhas:
    a. Para a ID do Transit Gateway, escolha a ID do Transit Gateway que você registrou na Etapa 2.
    b. Em Tipo de anexo, escolha VPC.
    c. Como opção, em VPC Attachment (Anexo da VPC), insira um nome para Attachment name tag (Tag de nome do anexo).

d. Escolha se deseja ativar o DNS Support and IPv6 Support.

e. Em ID da VPC, escolha a VPC a ser anexada ao gateway de trânsito. Essa VPC precisa estar associada a pelo menos uma sub-rede.

f. Em Sub-rede IDs, selecione uma sub-rede para cada zona de disponibilidade a ser usada pelo gateway de trânsito para rotear o tráfego. É necessário selecionar pelo menos uma sub-rede. Você pode selecionar somente uma sub-rede por zona de disponibilidade.

5. Escolha Create attachment (Criar anexo). Registre a ID do anexo TGW recém-criado.

Associando o anexo TGW a uma tabela de rotas:

Decida a qual tabela de rotas do TGW você deseja associar a VPC. Recomendamos criar uma nova tabela de rotas de aplicativos para Customer Managed VPCs enviando uma RFC Deployment | Managed landing zone | Networking account | Create transit gateway route table (ct-3dscwaeyi6cup). Para associar o anexo VPC ou TGW à tabela de rotas selecionada, envie uma RFC Deployment | Managed landing zone | Networking account | Associate TGW attachment (ct-3nmhh0qr338q6) na conta Networking.

Crie rotas nas tabelas de rotas do TGW para se conectar a essa VPC:

1. Por padrão, essa VPC não conseguirá se comunicar com nenhuma outra VPCs na sua rede de zona de destino de várias contas.
2. Decida com seu arquiteto de soluções com o que VPCs você deseja que essa VPC gerenciada pelo cliente se comunique. Envie uma implantação | Managed landing zone | Conta de rede | Adicione uma rota estática (ct-3r2ckznmt0a59) RFC à conta de rede para criar as rotas TGW de que você precisa.

> **Note**
>
> Este CT (ct-3r2ckznmt0a59) não permite adicionar rotas estáticas à tabela de rotas principal EgressRouteDomain; se seu CMA precisar permitir tráfego de saída, envie um RFC Management | Other | Other (MOO) com ct-0xdawir96cy7k.

Configurando suas tabelas de rotas de VPC para apontar para o gateway de trânsito da zona de aterrissagem multiconta do AMS:

Decida com seu arquiteto de soluções qual tráfego você deseja enviar para o gateway de trânsito do AMS Multi-Account Landing Zone. Atualize suas tabelas de rotas de VPC para enviar tráfego para o anexo TGW criado anteriormente

Obter ajuda operacional com suas contas gerenciadas pelo cliente

O AMS pode ajudá-lo a operar as cargas de trabalho que você implantou em suas contas gerenciadas pelo cliente integrando a conta ao AMS Accelerate. Com o AMS Accelerate, você pode se beneficiar de serviços operacionais, como monitoramento e alertas, gerenciamento de incidentes, gerenciamento de segurança e gerenciamento de backup, sem passar por uma nova migração, passar por períodos de inatividade ou alterar a forma como você usa. AWS O AMS Accelerate também oferece um complemento de patch opcional para cargas de trabalho EC2 baseadas que exigem patches regulares. Com o AMS Accelerate, você continua usando, configurando e implantando todos os AWS serviços de forma nativa ou com suas ferramentas preferidas; como você faz com as contas gerenciadas pelo cliente avançado do AMS. Você usa seus mecanismos preferidos de acesso e mudança, enquanto o AMS aplica práticas comprovadas que ajudam a escalar sua equipe, otimizar custos, aumentar a segurança e a eficiência e melhorar a resiliência. Para saber mais, consulte a descrição do serviço Accelerate.

Para integrar sua conta gerenciada pelo cliente ao Accelerate, entre em contato com seu CSDM e siga as etapas em Introdução ao AMS Accelerate.

> **Note**
>
> As contas do AMS Accelerate no AMS Advanced não têm gerenciamento de alterações do AMS (solicitações de alteração ou RFCs) nem o console do AMS Advanced. Em vez disso, eles têm o console e a funcionalidade do AMS Accelerate.

Conta do AMS Tools (migrando cargas de trabalho)

Sua conta de ferramentas Multi-Account Landing Zone (com VPC) ajuda a acelerar os esforços de migração, aumenta sua posição de segurança, reduz custos e complexidade e padroniza seu padrão de uso.

Uma conta de ferramentas fornece o seguinte:

- Um limite bem definido para acesso às instâncias de replicação para integradores de sistemas fora de suas cargas de trabalho de produção.
- Permite criar uma câmara isolada para verificar se há malware em uma carga de trabalho ou rotas de rede desconhecidas antes de colocá-la em uma conta com outras cargas de trabalho.
- Como uma configuração de conta definida, ela fornece um tempo mais rápido de integração e configuração para migrar cargas de trabalho.
- Rotas de rede isoladas para proteger o tráfego do local -> -> Conta de ferramentas CloudEndure -> Imagem ingerida pelo AMS. Depois que uma imagem é ingerida, você pode compartilhá-la com a conta de destino por meio de um AMS Management | Advanced stack components | AMI | Share (ct-1eiczxw8ihc18) RFC.

Diagrama de arquitetura de alto nível:

Use o tipo de alteração Deployment | Managed landing zone | Management account | Create tools account (com VPC) (ct-2j7q1hgf26x5c) para implantar rapidamente uma conta de ferramentas e instanciar um processo de ingestão de carga de trabalho em um ambiente de zona de destino com várias contas. Consulte Conta de gerenciamento, Conta de ferramentas: criação (com VPC).

> **Note**
>
> Recomendamos ter duas zonas de disponibilidade (AZs), já que esse é um hub de migração. Por padrão, o AMS cria os dois grupos de segurança a seguir (SGs) em cada conta. Confirme se esses dois SGs estão presentes. Se eles não estiverem presentes, abra uma nova solicitação de serviço com a equipe do AMS para solicitá-los.
>
> - SentinelDefaultSecurityGroupPrivateOnlyEgressAll
> - InitialGarden-SentinelDefaultSecurityGroupPrivateOnly
>
> Garanta que CloudEndure as instâncias de replicação sejam criadas na sub-rede privada, onde há rotas de volta para o local. Você pode confirmar isso garantindo que as tabelas de rotas da sub-rede privada tenham uma rota padrão de volta para o TGW. No entanto, realizar um corte CloudEndure de máquina deve ir para a sub-rede privada “isolada”, onde não há nenhuma rota de volta para o local, somente o tráfego de saída da Internet é permitido. É

fundamental garantir que a transferência ocorra na sub-rede isolada para evitar possíveis problemas nos recursos locais.

Pré-requisitos:

1. Nível de suporte Plus ou Premium.
2. A conta do aplicativo IDs para a chave KMS em que AMIs eles são implantados.
3. A conta de ferramentas, criada conforme descrito anteriormente.

AWS Serviço de migração de aplicativos (AWS MGN)

AWS O Application Migration Service (AWS MGN) pode ser usado em sua conta do MALZ Tools por meio da função `AWSManagedServicesMigrationRole` IAM que é criada automaticamente durante o provisionamento da conta do Tools. Você pode usar o AWS MGN para migrar aplicativos e bancos de dados executados em versões compatíveis dos sistemas operacionais Windows e Linux.

Para up-to-date obter mais informações sobre Região da AWS suporte, consulte a Lista de serviços AWS regionais.

Se sua preferência não Região da AWS for suportada atualmente pela AWS MGN, ou se o sistema operacional no qual seus aplicativos são executados não for atualmente suportado pela AWS MGN, considere usar a CloudEndure Migração em sua conta de Ferramentas.

Solicitando a inicialização do AWS MGN

O AWS MGN deve ser inicializado pelo AMS antes do primeiro uso. Para solicitar isso para uma nova conta de Ferramentas, envie um RFC de Gerenciamento | Outro | Outro da conta de Ferramentas com estes detalhes:

```
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.
```

Depois que o AMS concluir com êxito o RFC e inicializar o AWS MGN em sua conta de Ferramentas, você poderá usá-lo `AWSManagedServicesMigrationRole` para editar o modelo padrão de acordo com seus requisitos.

Habilitar o acesso à nova conta do AMS Tools

Depois que a conta de ferramentas é criada, o AMS fornece um ID de conta. Sua próxima etapa é configurar o acesso à nova conta. Siga estas etapas.

1. Atualize os grupos apropriados do Active Directory para a conta apropriada IDs.

   As novas contas criadas pelo AMS são provisionadas com a política de funções e com uma ReadOnly função para permitir que os usuários arquivem. RFCs

   A conta Tools também tem uma função e um usuário adicionais do IAM disponíveis:

   - Perfil do IAM: `AWSManagedServicesMigrationRole`
   - Usuário do IAM: `customer_cloud_endure_user`
2. Solicite políticas e funções para permitir que os membros da equipe de integração de serviços configurem o próximo nível de ferramentas.

   Navegue até o console do AMS e registre o seguinte RFCs:

   a. Crie uma chave KMS. Use Criar chave KMS (automático) ou Criar chave KMS (revisão obrigatória).

      Ao usar o KMS para criptografar recursos ingeridos, o uso de uma única chave KMS que é compartilhada com o restante das contas do aplicativo Multi-Account Landing Zone fornece segurança para imagens ingeridas, onde elas podem ser descriptografadas na conta de destino.

   b. Compartilhe a chave KMS.

      Use o tipo de alteração Gerenciamento | Componentes avançados da pilha | Chave KMS | Compartilhar (revisão obrigatória) (ct-05yb337abq3x5) para solicitar que a nova chave KMS seja compartilhada com as contas do aplicativo onde residirá a ingestão. AMIs

Exemplo de gráfico da configuração final de uma conta:

Exemplo de política de IAM CloudEndure pré-aprovada pelo AMS

Para ver uma CloudEndure política IAM pré-aprovada pelo AMS: Descompacte o arquivo de exemplo do WIGS Cloud Endure Landing Zone e abra o. `customer_cloud_endure_policy.json`

Testando a conectividade e a end-to-end configuração da conta do AMS Tools

1. Comece configurando CloudEndure e instalando o CloudEndure agente em um servidor que será replicado para o AMS.
2. Crie um projeto em CloudEndure.
3. Insira as AWS credenciais compartilhadas quando você executou os pré-requisitos, por meio do gerenciador de segredos.
4. Nas configurações de replicação:
   a. Selecione os dois grupos de segurança “Sentinel” do AMS (somente privado e EgressAll) para a opção Escolher os grupos de segurança a serem aplicados aos servidores de replicação.
   b. Defina as opções de transição para as máquinas (instâncias). Para obter informações, consulte a Etapa 5. Cortar
   c. Sub-rede: sub-rede privada.
5. Grupo de segurança:
   a. Selecione os dois grupos de segurança “Sentinel” do AMS (somente privado e EgressAll).
   b. As instâncias de transferência precisam se comunicar com o Active Directory (MAD) gerenciado pelo AMS e com endpoints públicos: AWS
      i. IP elástico: nenhum
      ii. IP público: não
      iii. Função do IAM: perfil de customer-mc-ec 2 instâncias
   c. Defina as tags de acordo com sua convenção interna de marcação.
6. Instale o CloudEndure agente na máquina e procure a instância de replicação que aparecerá na sua conta do AMS no EC2 console.

O processo de ingestão do AMS:

Higiene da conta AMS Tools

Você vai querer limpar depois de concluir que a conta compartilhou a AMI e não precisa mais das instâncias replicadas:

- WIGs Ingestão de pós-instância:
  - Instância de transição: no mínimo, interrompa ou encerre essa instância, após a conclusão do trabalho, por meio do console da AWS

  - Backups de AMI de pré-ingestão: remova quando a instância for ingerida e a instância local encerrada
  - Instâncias ingeridas pelo AMS: desative a pilha ou encerre depois que a AMI for compartilhada
  - Ingerido pelo AMS AMIs: exclua quando o compartilhamento com a conta de destino for concluído
- Limpeza do fim da migração: documente os recursos implantados por meio do modo Desenvolvedor para garantir que a limpeza ocorra regularmente, por exemplo:
  - Grupos de segurança
  - Recursos criados por meio do Cloud-formation
  - Rede ACK
  - Sub-rede
  - VPC
  - Tabela de rotas
  - Perfis
  - Usuários e contas

Migração em grande escala - Migration Factory

Consulte Apresentação da solução AWS CloudEndure Migration Factory.

MALZ: Integração da conta principal

As principais tarefas que você precisará realizar ao se inscrever em uma AWS conta principal do landing zone com várias contas são as seguintes:.

Tópicos

- Crie uma AWS conta principal de landing zone com várias contas no AMS
- Crie uma função do IAM para que o AMS acesse sua conta
- Proteja a nova conta com autenticação multifator (MFA) para o usuário raiz no AMS
- Inscreva-se AWS Marketplace para receber o Trend Micro Endpoint Protection (EPS)
- Configurar redes
- Configurar o gerenciamento de acesso

Para perguntas de integração, entre em contato com seu arquiteto de nuvem.

Crie uma AWS conta principal de landing zone com várias contas no AMS

A zona de pouso com várias contas do AMS exige o provisionamento de uma nova conta da Amazon Web Services (AWS) para atuar como a conta de gerenciamento no ambiente da zona de pouso com várias contas do AMS. Para criar uma Conta da AWS, siga estas step-by-step instruções: Como faço para criar e ativar uma nova conta da Amazon Web Services?

As etapas simples são: Vá para Criar conta, clique em Inscrever-se agora e, na página que se abre, clique em Criar uma nova Conta da AWS. Siga as instruções na tela, que incluem receber uma chamada telefônica e inserir um PIN usando o teclado do telefone. Você também precisará inserir um cartão de crédito. O AMS usa essa conta como conta de gerenciamento, ou conta do pagador, para sua nova landing zone com várias contas.

> **Note**
>
> Depois de fazer a integração, converse com seu gerente de prestação de serviços em nuvem (CSDM) sobre como transferir o faturamento do seu cartão de crédito para um sistema de faturas. As seguintes informações serão necessárias:
>
> - Nome da empresa de cobrança
> - Nome do contato de cobrança
> - Número de telefone de contato de cobrança
> - E-mail de contato de cobrança
> - Endereço de faturamento
>
> Seu CSDM o ajudará com essa atualização. Depois de concluído, e para alterar a forma de pagamento, consulte Gerenciando suas AWS formas de pagamento.

> **Note**
>
> Não vincule sua nova conta a uma conta de gerenciamento ou conta de pagador existente. Certifique-se de que sua conta não faça parte de uma conta existente AWS Organizations; para obter informações, consulte O que é AWS Organizations?

> **Important**
>
> É muito importante garantir que um endereço de e-mail (uma lista de distribuição, não o endereço de e-mail de um indivíduo) e um número de telefone estejam associados à conta para que você receba respostas a possíveis incidentes de segurança. O número de telefone e o endereço de e-mail da conta não podem ser alterados sem redefinir a senha da conta, o que é uma tarefa importante para uma conta raiz do AMS. Para garantir que esses valores sejam estáveis, é fundamental selecionar informações de contato não associadas a indivíduos, que podem mudar. Escolha um alias de e-mail que possa apontar para um grupo. Siga essa mesma prática ao selecionar um número de telefone: escolha um número que possa apontar para um grupo ou para um número de propriedade da empresa e não de um indivíduo.

Para obter detalhes sobre as perguntas que você deverá fazer para integrar sua conta principal à landing zone multiconta do AMS, consulte. Apêndice: lista de consideração de integração da multi-account landing zone (MALZ)

Crie uma função do IAM para que o AMS acesse sua conta

Agora que você criou sua nova conta com sucesso Conta da AWS, a próxima etapa do processo é permitir que o AMS acesse a nova conta para criar e configurar seu ambiente AMS e atender às solicitações contínuas de mudança e provisionamento. Para obter detalhes, consulte Delegar acesso entre AWS contas usando funções do IAM.

AWS Identity and Access Management (IAM) é um serviço web que ajuda você a controlar com segurança o acesso aos AWS recursos para seus usuários. Você usa o IAM para controlar quem pode usar seus AWS recursos (autenticação) e quais recursos eles podem usar e de que forma (autorização).

Ative o acesso do IAM ao AWS console

1. Entre no console AWS de gerenciamento com as credenciais da sua conta raiz (o e-mail e a senha que você usou para criar sua Conta da AWS). Não faça login com outras credenciais do IAM. A página inicial do console de AWS gerenciamento é aberta.
2. Na barra de navegação superior, abra o menu suspenso do nome da sua conta e escolha Conta. A página inicial de faturamento é aberta.

3. Role para baixo até o acesso de usuário e função do IAM às informações de faturamento e escolha Editar. Uma área de acesso do Activate IAM é aberta.
4. Marque a caixa de seleção e escolha Atualizar. Agora é possível usar as políticas do IAM para controlar quais páginas o usuário pode acessar.

Crie uma função do IAM para o AMS usar

1. Obtenha um arquivo JSON ou YAML que defina uma função do IAM para o AMS usar para criar sua infraestrutura. Há duas opções:
   - Seu arquiteto de nuvem (CA) do AMS fornece um arquivo JSON ou YAML.
   - Você pode baixar o onboarding_iam_roles.zip e escolher uma das seguintes opções:
     - onboarding_role_admin.json (mais curto, concede acesso total ao administrador)
     - onboarding_role_minimal.json (mais longo, concede menos privilégios)
2. Faça login no Console de gerenciamento da AWS e abra o CloudFormation console em https://console.aws.amazon.com/cloudformation.
3. Selecione Create Stack (Criar pilha). Você vê a página a seguir.
4. Escolha Carregar um arquivo de modelo, faça upload do arquivo JSON ou YAML da função do IAM e escolha Avançar. Você vê a página a seguir.
5. Entre **`ams-onboarding-role`** na seção Nome da pilha e continue rolando para baixo e selecionando Avançar até chegar a esta página.
6. Verifique se a caixa de seleção está marcada e selecione Criar pilha.
7. Verifique se a pilha foi criada com sucesso.

Proteja a nova conta com autenticação multifator (MFA) para o usuário raiz no AMS

Esta seção foi redigida porque contém informações confidenciais relacionadas à segurança do AMS. Essas informações estão disponíveis na documentação do console AMS. Para acessar o AWS Artifact, você pode entrar em contato com seu CSDM para obter instruções ou acessar Getting Started with AWS Artifact.

Inscreva-se AWS Marketplace para receber o Trend Micro Endpoint Protection (EPS)

O Trend Micro Endpoint Protection (EPS) é o principal componente do AMS para segurança do sistema operacional. Para configurar o EPS após o início da criação da landing zone do AMS, você precisa fazer login na conta principal de serviços compartilhados e assinar a AMI do Trend Micro Deep Security em AWS Marketplace. Seu CSDM ou CA o aconselhará.

1. Faça login no AWS console usando a função ou o usuário que você especificou no Questionário de Integração para `CustomerEPSSubscriptionIAMRoleOrUser`
2. Navegue até a tela Switch Role.

   - Conta: Fornecida pela AMS
   - Função: `EPSMarketplaceSubscriptionRole`
   - Nome de exibição: Sessão de assinatura EPS

   Para assinar o Trend Micro Deep Security no AWS Marketplace, siga estas etapas depois de trocar a função no console:

   1. Navegue até o AWS Marketplace.
   2. Em Encontre AWS Marketplace produtos que atendam às suas necessidades, selecione as seguintes opções:
      a. Fornecedores: Trend Micro
      b. Plano de preços: traga sua própria licença se você tiver uma licença ou By Hosts Billing
      c. Métodos de entrega: Amazon Machine Image

3. Clique em Continuar para se inscrever no painel direito.
4. Revise os Termos e Condições e clique em Aceitar Termos no canto superior direito.
5. Saia da conta e confirme com seu arquiteto de nuvem se o procedimento foi concluído.

Nesse ponto, o AMS implanta a infraestrutura em seu ambiente AMS e o ambiente está pronto para você usar depois de conectar sua rede e configurar seu acesso.

Configurar redes

A rede no ambiente AMS é tratada principalmente na conta principal da rede.

Há vários processos que precisam ser concluídos para configurar a rede para o AWS Managed Services (AMS):

- Alocação de espaço IP para seu ambiente AMS
- Estabelecendo conectividade de rede privada para AWS
- Configurando seu firewall para permitir operações do AMS

Alocação de espaço IP para seu ambiente AMS

Você já deve ter trabalhado com seu arquiteto de nuvem na definição do espaço IP para seu ambiente AMS ao preencher o questionário de integração.

Estabelecendo conectividade de rede privada com AWS o AMS

AWS oferece conectividade privada usando conectividade VPN e linhas dedicadas por meio do AWS Direct Connect. A conectividade privada pode ser configurada de duas maneiras:

- Conectividade de borda centralizada usando o Transit Gateway
- Conectando o Direct Connect and/or VPN à conta VPCs

Conectividade de borda centralizada usando o Transit Gateway

AWS O Transit Gateway é um serviço que permite conectar suas Amazon Virtual Private Clouds (VPCs) e suas redes locais a um único gateway. O Transit Gateway pode ser usado para consolidar sua conectividade de borda existente e roteá-la por meio de um único ingress/egress ponto. Para obter mais detalhes, consulte AWS Transit Gateway.

Conectando o Direct Connect ao Transit Gateway

Você pode usar sua conexão Direct Connect existente ou criar uma nova conexão Direct Connect em uma de suas AWS contas existentes. A conexão Direct Connect deve ser uma conexão dedicada ou hospedada em execução a 1 Gbps ou mais.

> **Note**
>
> Para obter informações sobre como usar o Direct Connect com AWS serviços, consulte Introdução em um local do AWS Direct Connect.

Para usar uma conexão dedicada existente do Direct Connect, a conexão não deve ter mais de 3 interfaces virtuais de trânsito criadas nela. Isso ocorre porque as conexões Direct Connect dedicadas têm um limite de 4 interfaces virtuais de trânsito por conexão.

Para obter informações adicionais sobre os limites do Direct Connect, consulte Limites do AWS Direct Connect.

Depois que a conexão Direct Connect estiver disponível, ocorre o seguinte:

1. O AMS cria um Direct Connect Gateway na conta de rede. Você deve fornecer um número de Número de Sistema Autônomo (ASN) para o Direct Connect Gateway e os prefixos que devem ser anunciados no Direct Connect Gateway. Esse ASN é usado como Amazon ASN.
2. Você cria um novo Transit VIF e define o proprietário da interface virtual como a conta de rede.
3. O AMS faz login na conta de rede e aceita a proposta de conexão.
4. O AMS associa o gateway de trânsito ao gateway Direct Connect.
5. O AMS associa o anexo à tabela de roteamento local do Transit Gateway.

> **Note**
>
> O ASN fornecido para o gateway Direct Connect e o Transit Gateway deve ser diferente.

Para aumentar a resiliência de sua conectividade, é uma prática recomendada conectar pelo menos duas interfaces virtuais de trânsito, de diferentes locais do AWS Direct Connect, ao gateway Direct Connect. Para obter mais informações, consulte a recomendação de Direct Connect resiliência.

Conectando a VPN ao Transit Gateway

Para anexar uma conexão VPN ao seu gateway de trânsito, é necessário especificar o gateway do cliente. Para obter mais informações sobre os requisitos de um gateway de cliente, consulte Requisitos para seu gateway de cliente no Guia do administrador de rede Amazon VPC.

Você precisaria fornecer o número ASN do BGP, o endereço IP público estático e a opção de roteamento (estático ou dinâmico). Depois que esses detalhes forem fornecidos, o AMS criará o anexo VPN e o associará à tabela de roteamento local do Transit Gateway.

Para obter mais detalhes sobre os anexos do Transit Gateway, consulte Anexos VPN do Transit Gateway.

Conectando o Direct Connect and/or VPN à conta VPCs

Você também pode conectá-lo diretamente VPCs ao Direct Connect ou à VPN. O tráfego flui diretamente do VPCs Direct Connect ou VPN sem passar pelo gateway de trânsito.

> **Note**
>
> A VPC de serviços compartilhados e a conta do aplicativo VPCs precisam estar conectadas a uma conexão Direct Connect ou VPN para estabelecer uma conectividade privada.

Direct Connect configuração no AMS

Configure um Direct Connect para se comunicar entre sua VPC gerenciada pelo AMS e sua rede interna.

> **Note**
>
> Para obter informações sobre como usar o Direct Connect com AWS serviços, consulte Introdução em um Direct Connect local.

Para configurar uma conexão Direct Connect, conclua as seguintes etapas:

1. Cadastre-se na Amazon Web Services (AWS)
2. Envie uma solicitação de Direct Connect conexão.
3. Conclua o Cross Connect.
4. (Opcional) Configure conexões redundantes com. Direct Connect
5. Executado pelo AMS: crie uma interface virtual.
6. Executado pelo AMS: Baixe a configuração do roteador.
7. Verifique sua interface virtual.

Configuração de VPN

As etapas básicas que o AMS segue para configurar uma VPN para se comunicar entre sua VPC gerenciada pelo AMS e sua rede interna.

> **Note**
>
> Para obter uma compreensão geral sobre o uso de uma VPN com AWS serviços, consulte O que é AWS Site-to-Site VPN e seu gateway de cliente (seu dispositivo VPN).

Seguimos as seções do Guia do usuário da AWS VPN para começar e testar a conexão Site-to-Site VPN para concluir as seguintes etapas:

1. Em sua AWS VPC, crie um gateway do cliente.
2. Em sua AWS VPC, crie um gateway privado virtual.
3. Em sua AWS VPC, habilite a propagação de rotas em sua tabela de rotas.
4. Em sua AWS VPC, atualize seu grupo de segurança para habilitar o acesso SSH, RDP e ICMP de entrada.
5. Na sua rede interna, crie uma conexão VPN e configure o gateway do cliente.
6. Teste a conectividade VPN entre a VPC e sua rede interna.

Configurar o gerenciamento de acesso

Usar uma rede gerenciada pelo AWS Managed Services (AMS) significa dar acesso ao AMS para gerenciar sua infraestrutura de nuvem. Você precisará configurar um meio de conexão segura entre sua rede privada e o AMS. Isso começa com algumas decisões:

- Acesso ao AMS API/CLI e ao console: Você desejará instalar o AMS CLI (as instruções são fornecidas neste documento). Você usa a API de gerenciamento de alterações do AMS para fazer solicitações de alteração ao AMS e a API do AMS SKMS para saber mais sobre seus recursos gerenciados pelo AMS. Usando os Serviços de Federação do Active Directory (AD FS), você pode acessar o console AMS.
- Acesso do usuário: a conectividade precisa ser estabelecida entre o AD no lado do AMS (por meio dos Serviços de Diretório) e o diretório que você usa para gerenciar usuários.
- Acesso à instância: o acesso no nível da instância é realizado por meio de uma configuração de confiança unidirecional. Os Serviços de Diretório confiam nas credenciais em seu CORP AD, permitindo que pilhas no lado do AMS permitam o login com credenciais CORP.

> **Note**
>
> Seu Active Directory (AD), no qual o AMS configura a confiança, deve ser o diretório que tem as contas de usuários autorizados por você a obter acesso aos seus recursos da AWS.

Estabeleça uma confiança do Active Directory

Para configurar uma relação de confiança, o AMS exige que seu controlador de domínio Políticas locais -> Opções de segurança -> Acesso à rede: canais nomeados que podem ser acessados anonimamente, tenham os canais Netlogon e lsarpc listados. Esses canais são listados por padrão, mas às vezes são removidos por questões de segurança. Depois que a confiança for estabelecida, eles poderão ser removidos da lista novamente.

Configurar o encaminhador condicional

1. No AD DNS Manager -> Criar um novo encaminhador condicional, em Domínio DNS: Use o nome de domínio AMS fornecido a você; por exemplo, A523434123.amazonaws.com (altere-o para o nome de domínio selecionado no questionário de integração).
2. Em Endereços IP dos servidores principais: adicione os endereços IP fornecidos pela AMS. Verifique se não há um problema de conexão validando os dois endereços.
3. Selecione Armazenar este encaminhador condicional no Active Directory e replique da seguinte forma: Todos os servidores DNS neste domínio e pressione OK.

Configurar a confiança do AD

Siga este artigo do Microsoft AD Crie uma relação de confiança florestal unidirecional, de entrada, para um lado da relação de confiança, usando as configurações e opções descritas nesta seção.

1. Abra a caixa de diálogo Iniciar -> Ferramentas administrativas -> Domínios e relações de confiança do Active Directory. Clique com o botão direito do mouse no nó do domínio com o qual você deseja estabelecer uma relação de confiança e clique em Propriedades -> Relações de Confiança -> Nova Confiança para abrir o Assistente de Nova Confiança. Insira o nome de domínio fornecido pelo AMS para o nome confiável e pressione Avançar.
2. Em Tipo de confiança, selecione o nível de confiança apropriado (por exemplo, Forest Trust). Pressione Avançar.
3. Em Direção de Confiança, selecione Unidirecional: entrada. Pressione Próximo.
4. Em Lados da Confiança, selecione Somente este domínio. Pressione Próximo.
5. Em Senha confiável, digite uma senha de sua escolha. Pressione Próximo.
6. Para Seleções de confiança concluídas e Criação de confiança concluída, basta pressionar Avançar.
7. Em Confirmar confiança recebida, selecione Não, não confirme a confiança recebida. Pressione Próximo.
8. Em Concluído o Assistente de Nova Confiança, selecione Concluir e, em seguida, OK para fechar.
9. Forneça a senha de confiança (entre em contato conosco pelo número de telefone do seu CSDM por motivos de segurança). O AMS concluirá a configuração de confiança.

Sites e serviços do Active Directory

Para reduzir a latência de login, adicione o intervalo CIDR da VPC aos seus sites e serviços do Active Directory (Iniciar -> Ferramentas administrativas -> Sites e serviços do Active Directory). Adicione o intervalo CIDR da VPC a um site do Active Directory que contém controladores de domínio mais próximos da AWS.

Forneça ao seu CSDM o nome do site que você dedicou para o AMS. O AMS renomeará o site padrão no lado AMS do AD para corresponder ao nome fornecido.

Roteamento de sufixo de nome do Active Directory

Depois que a confiança unidirecional da floresta for estabelecida, conclua as etapas a seguir para validar o roteamento de sufixos:

1. Em Iniciar > Todos os Programas > Ferramentas Administrativas, clique em Domínios e Relações de Confiança do Active Directory.

   O console Domínios e Relações de Confiança do Active Directory é aberto.
2. Clique com o botão direito do mouse em seu domínio corporativo e clique em Propriedades

   A caixa de diálogo Propriedades desse domínio é aberta.
3. Clique na guia Confianças.

   A página Trusts é aberta.
4. Clique no nome de domínio da Amazon e clique em Propriedades.

   A página de propriedades do domínio fiduciário da Amazon é aberta.
5. Clique em Roteamento de sufixo de nome e clique em Atualizar.

   Certifique-se de que não haja conflitos para garantir que os nomes principais de serviço (SPNs) possam ser resolvidos sobre a confiança.

Federe seu Active Directory com as funções do AMS IAM

O objetivo de federar seu diretório com as funções do AMS IAM é permitir que os usuários corporativos usem suas credenciais corporativas para interagir com o AWS Console e a AWS e APIs, portanto, com o console AMS e. APIs

Exemplo de processo de federação

Este exemplo usa os Serviços de Federação do Active Directory (AD FS); no entanto, qualquer tecnologia que ofereça suporte à Federação AWS IAM é suportada. Para obter mais informações sobre a federação do IAM suportada pela AWS, consulte Parceiros do IAM e provedores de identidade e federação. Seu CSDM o ajudará nesse processo, que envolve um esforço conjunto com sua equipe de AD e o AMS.

Para obter informações detalhadas sobre a integração do SAML para acesso à API, consulte este blog da AWS, Como implementar o acesso federado à API e à CLI usando o SAML 2.0 e o AD FS.

Para ver um exemplo de instalação da CLI do AMS e do SAML, consulte o Apêndice: regra de declaração do AD FS e configurações do SAML.

Configurando a federação no console AMS (MALZ)

As funções do IAM e o provedor de identidade SAML (entidade confiável) detalhados na tabela a seguir foram provisionados como parte da infraestrutura do AMS. Essas funções permitem que você audite e visualize as contas principais do AMS.

Role (Função)	Permissões
AWSManagedServicesReadOnlyRole	Permite que você visualize a infraestrutura do AMS nas contas principais.
AWSManagedServicesCaseRole	Permite que você visualize os recursos em sua nova conta de aplicativo e registre incidentes e solicitações de serviço do AMS.
AWSManagedServicesChangeManagementRole	Permite que você visualize a infraestrutura do AMS nas contas principais, arquive tickets do AWS Support e solicite alguns RFCs.

Para obter a lista completa das funções disponíveis em diferentes contas, consulteFunção de usuário do IAM no AMS .

Verifique o acesso ao console

Depois de configurar o ADFS e ter a URL do AMS para usar na autenticação, siga estas etapas.

Com uma configuração do Active Directory Federated Service (ADFS), você pode seguir estas etapas:

1. Abra uma janela do navegador e acesse a página de login fornecida para sua conta. A IdpInitiatedSignOnpágina ADFS da sua conta é aberta.
2. Selecione o botão de rádio ao lado de Entrar em um dos sites a seguir. A lista de opções do site de login fica ativa.
3. Escolha o site signin.aws.amazon.com e clique em Entrar. As opções para inserir suas credenciais estão abertas.

4. Insira suas credenciais CORP e clique em Entrar. As Console de gerenciamento da AWS aberturas.
5. Cole na barra de localização o URL do console AMS e pressione Enter. O console AMS é aberto.

Verifique o acesso à API

O AMS usa a API da AWS, com algumas operações específicas da AMS que você pode ler na Referência da API do AMS.

A AWS fornece vários SDKs que você pode acessar em Tools for Amazon Web Services. Se você não quiser usar um SDK, você pode fazer chamadas diretas de API. Para obter informações sobre autenticação, consulte Assinar solicitações de API da AWS. Se você não estiver usando um SDK ou fazendo solicitações diretas de API HTTP, poderá usar o AMS CLIs for Change Management (CM) e o SKMS.

Instale o AMS CLIs

O AWS CLI é um pré-requisito para usar o AMS CLIs (Change Management and SKMS).

1. Para instalar a AWS CLI, consulte Instalação da interface de linha de comando da AWS e siga as instruções apropriadas. Observe que, na parte inferior dessa página, há instruções para usar diferentes instaladores, Linux, MS Windows, macOS, ambiente virtual, instalador empacotado (Linux, macOS ou Unix).
2. Após a instalação, execute aws help para verificar a instalação.
3. Depois que a CLI da AWS estiver instalada, para instalar ou atualizar a CLI do AMS, baixe o arquivo zip dos distribuíveis do AMS e descompacte-a. Você pode acessar os distribuíveis da CLI do AMS por meio do link Documentação no painel de navegação esquerdo do console do AMS ou pedir ao seu gerente de prestação de serviços em nuvem (CSDM) que envie o arquivo zip.
4. Abra o diretório Managed Cloud Distributables -> CLI -> Windows ou Managed Cloud Distributables -> CLI -> Linux/macOS, dependendo do seu sistema operacional, e:
5. Para Windows, execute o instalador apropriado (esse método só funciona em sistemas Windows de 32 ou 64 bits):

   - 32 bits: ManagedCloud API_x86.msi
   - 64 bits: ManagedCloud API_x64.msi

6. Para Mac/Linux, execute o arquivo chamado: MC_CLI.sh executando este comando: sh MC_CLI.sh. Observe que os diretórios amscm e amsskms e seu conteúdo devem estar no mesmo diretório do arquivo MC_CLI.sh.
7. Se suas credenciais corporativas forem usadas via federação com a AWS (a configuração padrão do AMS), você deverá instalar uma ferramenta de gerenciamento de credenciais que possa acessar seu serviço de federação. Por exemplo, você pode usar este blog de segurança da AWS Como implementar API federada e acesso à CLI usando SAML 2.0 e AD FS para ajudar a configurar suas ferramentas de gerenciamento de credenciais.
8. Após a instalação, execute `aws amscm help` e veja `aws amsskms help` os comandos e opções.

MALZ: Integração de conta de aplicativo

Você deve ter um ambiente de várias contas do AWS Managed Services (AMS) configurado com contas principais antes de solicitar uma nova conta de aplicativo. Aqui estão as etapas que você precisará seguir após configurar seu ambiente.

Tópicos

- Solicitando uma nova conta de aplicativo
- Configurando o Active Directory para federar o acesso às funções do AMS IAM
- Configurando a rede com a nova conta do aplicativo
- Configurando adicionais VPCs na conta do aplicativo

Para perguntas de integração, entre em contato com seu gerente de prestação de serviços em nuvem (CSDM). Consulte também Contas de aplicativos: gerenciadas pelo AMS, modo Dev-mode, gerenciadas pelo cliente. Para obter informações gerais sobre os modos, consulte Modos AMSGerenciamento de serviços no AWS Managed Services.

Para obter informações sobre os diferentes modos de contas de aplicativos, consulte Contas de aplicativos: gerenciadas pelo AMS, modo de desenvolvimento, gerenciadas pelo cliente. Para obter informações gerais sobre os modos, consulte Modos AMS.

Solicitando uma nova conta de aplicativo

Você deve ter um ambiente de várias contas do AWS Managed Services (AMS) configurado com contas principais antes de solicitar uma nova conta de aplicativo. Para obter informações sobre como

configurar um ambiente de várias contas com contas principais, consulteMALZ: Integração da conta principal.

Você pode escolher um dos seguintes tipos de Amazon VPC para a VPC inicial na conta do aplicativo:

- Privado: essa VPC não tem nenhum gateway de Internet conectado. Isso é adequado para aplicativos privados que não exigem acesso to/from à Internet.
- Pública: essa VPC tem um gateway de Internet conectado e sub-redes públicas e privadas. Isso é adequado para aplicativos públicos que exigem acesso to/from à Internet.

Você pode solicitar uma nova conta de aplicativo enviando uma RFC Deployment | Managed landing zone | Management account | Create application account (com VPC) (ct-1zdasmc2ewzrs) e fornecendo os seguintes valores na RFC:

- Nome da conta: um nome personalizado para a conta. Observe que o nome da conta tem um comprimento máximo de 50 caracteres.
- E-mail da conta: O e-mail da lista de distribuição da conta. Esse ID de e-mail é usado para criar a conta da AWS.
- Nível de suporte: o nível do AWS Support, Premium ou Plus.
- Nome da VPC: um nome para a VPC.
- Número de zonas de disponibilidade (AZs): 2 ou 3.
- VPC CIDR: o bloco CIDR para a VPC.
- Tipo de rota: Isso pode ser um `routable` ou outro`isolated`. `Routable`significa que o aplicativo VPCs associado à tabela de rotas do aplicativo Transit Gateway (TGW) pode se conectar a essa VPC. `Isolated`significa que o aplicativo VPCs associado à tabela de rotas do aplicativo TGW não pode se conectar a essa VPC. O padrão é `routable`.
- Tabela de rotas do aplicativo Transit Gateway: a tabela de rotas do Transit Gateway à qual a conta do aplicativo VPC deve ser associada. Se nenhum valor for fornecido, o padrão `defaultAppRouteDomain` será usado, o que significa que essa conta poderá se comunicar com todas as outras contas na mesma tabela de rotas.
- PublicSubnetAZ *<1-3>* CIDRCIDR para sub-rede pública em AZ 1: O CIDR para sub-rede pública na Zona de Disponibilidade 1.
- PrivateSubnet*<1-10>*AZ *<I-3>* CIDRCIDR para sub-rede pública em AZ 1: O CIDR para sub-rede pública na Zona de Disponibilidade 1.

Nesse ponto, o AMS implanta uma nova conta de aplicativo em sua conta de gerenciamento do AMS, com a configuração de VPC especificada.

Configurando o Active Directory para federar o acesso às funções do AMS IAM

Federe seu diretório com as funções do AMS IAM para permitir que os usuários corporativos usem suas credenciais corporativas para interagir com o AWS Console e a AWS APIs, e com o console AMS e o AMS. APIs

Exemplo de processo de federação

Este exemplo usa os Serviços de Federação do Active Directory (ADFS). No entanto, qualquer tecnologia que ofereça suporte à AWS IAM Federation é suportada. Para obter mais informações sobre a federação do IAM suportada pela AWS, consulte Parceiros do IAM e provedores de identidade e federação. Seu CSDM o ajudará nesse processo, que envolve um esforço conjunto com sua equipe de AD e o AMS.

Para obter informações detalhadas sobre a integração do SAML para acesso à API, consulte este blog da AWS, Como implementar o acesso federado à API e à CLI usando o SAML 2.0 e o AD FS.

Para ver um exemplo de instalação da CLI e do SAML do AMS, consulte o Apêndice: regra de declaração do AD FS e configurações do SAML no Guia do usuário do AMS.

Configurando a federação no console AMS

As funções do IAM e o provedor de identidade SAML (entidade confiável) detalhados na tabela a seguir são provisionados em sua nova conta do aplicativo. Essas funções permitem que você tenha acesso à nova conta e arquivo do aplicativo RFCs, grave nos buckets do S3 e execute outras ações.

Role (Função)	Permissões
AWSManagedServicesReadOnlyRole	Permite que você visualize os recursos em sua nova conta do aplicativo.
AWSManagedServicesCaseRole	Permite que você visualize os recursos em sua nova conta de aplicativo e registre tickets do AWS Support.

Role (Função)	Permissões
AWSManagedServicesChangeManagementRole	Permite que você visualize a infraestrutura do AMS nas contas do aplicativo, arquive RFCs, arquive tickets do AWS Support, grave nos buckets do S3, gerencie segredos do Secrets Manager e gerencie instâncias reservadas do Amazon Elastic Compute Cloud (Amazon EC2).
AWSManagedServicesSecurityOpsRole	Permite que você visualize a infraestrutura do AMS nas contas do aplicativo, gerencie segredos do Secrets Manager, gerencie regras do Web Application Firewall, gerencie certificados e arquive tickets do AWS Support.
AWSManagedServicesAdminRole	Permite que você visualize a infraestrutura do AMS nas contas do aplicativo, gerencie assinaturas do Marketplace, gerencie segredos do Secrets Manager, gerencie regras do Web Application Firewall, gerencie certificados, crie RFCs, gerencie EC2 instâncias reservadas da Amazon, grave em buckets do S3, arquive tickets do AWS Support e gerencie contratos do AWS Artifacts.

Enviando a solicitação de federação ao AMS

Se essa for sua primeira conta, trabalhe com seus CSDM (s) and/or Cloud Architect (s) para fornecer o arquivo XML de metadados para seu provedor de identidade.

Se você estiver integrando uma conta adicional ou provedor de identidade e tiver acesso à conta de gerenciamento ou à conta do aplicativo desejada, siga estas etapas.

1. Crie uma solicitação de serviço no console do AMS.

> **Note**
>
> - Se estiver criando um provedor de identidade para uma conta de aplicativo, envie essa solicitação da própria conta do aplicativo ou da conta de gerenciamento.
> - Se estiver criando um provedor de identidade para uma conta principal do AMS, envie essa solicitação da conta de gerenciamento.
> - Se estiver criando um provedor de identidade para a conta de gerenciamento, envie essa solicitação da conta de gerenciamento ou entre em contato com seu CSDM para obter assistência.

Na solicitação de serviço, forneça os detalhes necessários para adicionar o provedor de identidade:

- AccountId da conta em que o novo provedor de identidade será criado.
- O nome do provedor de identidade desejado, se não for fornecido, o padrão será customer-saml; normalmente, ele deve corresponder às configurações definidas no seu provedor de federação.
- Para contas existentes, inclua se o novo provedor de identidade deve ser propagado para todas as funções de console existentes ou forneça uma lista de funções que devem confiar no novo provedor de identidade.
- Anexe o arquivo XML de metadados exportado do seu agente de federação à solicitação de serviço como anexo de arquivo.

2. Na mesma conta em que você criou a solicitação de serviço, crie uma nova RFC usando CT-ID ct-1e1xtak34nx76 (Gerenciamento | Outros | Outros | Criar) com as seguintes informações.

   - Título: “SAML IDP integrado <Name>para conta < >AccountId”.
   - AccountId da conta em que o provedor de identidade será criado.
   - Nome do provedor de identidade.
   - Para contas existentes: se o provedor de identidade deve ser propagado para todas as funções de console existentes ou a lista de funções que devem confiar no novo provedor de identidade.
   - ID do caso da solicitação de serviço criada na Etapa 1, em que o arquivo XML de metadados é anexado.

Verifique o acesso ao console

Depois de configurar o AD FS e ter a URL do AMS a ser usada para autenticação, você pode executar o procedimento a seguir.

Com uma configuração do Active Directory Federated Service (AD FS), você pode seguir estas etapas:

1. Abra uma janela do navegador e acesse a página de login fornecida para sua conta. A IdpInitiatedSignOn página do AD FS da sua conta é aberta.
2. Selecione o botão de rádio ao lado de Entrar em um dos sites a seguir. A lista de sites de login fica ativa.
3. Escolha o site signin.aws.amazon.com e escolha Entrar. As opções para inserir suas credenciais estão abertas.
4. Insira suas credenciais CORP e escolha Entrar. O AWS Management Console é aberto.
5. Cole na barra de localização o URL do console AMS e pressione Enter. O console do AMS é aberto.

Verifique o acesso à API

O AMS usa a API da AWS, com algumas operações específicas da AMS que você pode ler na Referência da API do AMS.

A AWS fornece vários SDKs que você pode acessar em Tools for Amazon Web Services. Se você não quiser usar um SDK, pode fazer chamadas diretas à API. Para obter informações sobre autenticação, consulte Assinar solicitações de API da AWS. . Se você não estiver usando um SDK ou fazendo solicitações diretas de API HTTP, poderá usar o AMS CLIs for Change Management (CM) e o SKMS.

Configurando a rede com a nova conta do aplicativo

A configuração da rede para a conta do aplicativo inclui a configuração de regras de firewall e, potencialmente, a configuração de tabelas de rotas adicionais do Transit Gateway (TGW).

Configurando seu firewall

Para usar os aplicativos implantados em seu ambiente AMS, você deve criar algumas regras de firewall. Você não precisa dessas regras para acessar suas instâncias, você pode passar pelos bastiões até suas instâncias.

Regras de firewall para acesso a aplicativos

Você deve abrir as seguintes portas para tráfego através do seu firewall:

- Da sua rede local ao seu novo aplicativo VPC CIDRs nas direções de entrada e saída.
- Do seu novo aplicativo VPC CIDRs à sua rede local nas direções de entrada e saída (se seus aplicativos em nuvem precisarem alcançar seus aplicativos locais).

Porta	Protocolo	Serviço	De/Para	De/para
80	TCP	Acesso à Web HTTP	Rede local	Aplicação AMS VPC
443	TCP	Acesso via Web HTTPS	Rede local	Aplicação AMS VPC

Configurando tabelas adicionais de rotas do aplicativo Transit Gateway

A rede do AWS Managed Services (AMS) é flexível e oferece suporte a uma variedade de casos de uso de rede.

- Comunicação entre aplicativos VPCs na mesma conta.
- Comunicação entre aplicativos VPCs em contas diferentes.
- Isolamento entre aplicativos VPCs em contas diferentes.
- Isolamento entre aplicativos VPCs nas mesmas contas.

Se você tiver unique/special requisitos de rede, entre em contato com seu arquiteto de nuvem do AMS e eles desenvolverão um plano para que seus requisitos sejam atendidos pela arquitetura de rede do AMS.

Com base na decisão de rede tomada para a conta do aplicativo VPCs, você pode criar várias tabelas de rotas do aplicativo Transit Gateway (TGW) enviando um RFC Deployment | Managed landing zone | Networking account | Create transit gateway route table (ct-3dscwaeyi6cup).

O tipo de alteração exige que você especifique `TransitGatewayRouteTableName` (um nome significativo para a tabela de rotas do TGW)`TransitGatewayId`, e. `TGWRouteTableType`

> **Note**
>
> Se createCustomRoute Domínio for selecionado para TGWRouteTableType, a tabela de rotas criada estará vazia. Você deve registrar um RFC com o tipo de alteração Deployment | Managed landing zone | Networking account | Add static route (ct-3r2ckznmt0a59).

Configurando adicionais VPCs na conta do aplicativo

Você pode solicitar uma conta de aplicativo adicional VPC enviando um RFC Deployment | Managed landing zone | Application account | Create VPC (ct-1j3503fres5a5).

Isso funciona da mesma forma que configurar uma VPC para uma nova conta de aplicativo. Para obter mais detalhes, consulte Solicitando uma nova conta de aplicativo.

Apêndice: lista de consideração de integração da multi-account landing zone (MALZ)

Há várias considerações importantes que você precisará considerar ao planejar a implantação da landing zone multiconta do AMS. Suas escolhas fornecerão à AMS as informações necessárias para determinar os componentes de infraestrutura necessários. Seu Cloud Architect (CA) fornecerá um questionário para ajudar nesse trabalho.

Tópicos

- Configuração da conta de landing zone com várias contas do AMS
- Alertas de monitoramento de landing zone com várias contas do AMS
- Network configuration
- Configuração do Active Directory
- Proteção de terminais da Trend Micro (EPS)

- Acesso: Bastions, SSH e RDP
- Federação

> **Note**
>
> Para obter mais informações sobre os tipos de instância, consulte Tipos de EC2 instância da Amazon.
> Para obter mais informações sobre os tipos de instância de banco de dados, consulte Tipos de instância do Amazon RDS.
> Se você precisar do Direct Connect, consulte o Guia de integração da landing zone de conta única do AMS para criar uma conexão Direct Connect.

Você receberá um questionário de integração do seu Cloud Service Delivery Manager (CSDM) contendo perguntas sobre as configurações desejadas para sua conta. Trabalhe com seu CSDM para preencher o questionário antes de continuar.

Configuração da conta de landing zone com várias contas do AMS

- Novo ID da conta

  O Conta da AWS ID que você criou para a landing zone multiconta do AMS. Não deve fazer parte de uma AWS organização.

- Região de serviço

  A região principal na qual o ambiente de landing zone com várias contas do AMS será implantado.

- Os e-mails da conta principal para notificações. (todos devem estar no mesmo domínio). Forneça um endereço de e-mail para cada um:
  - Conta de Serviços Compartilhados
  - Conta de rede
  - Conta de registro
  - Conta de segurança
- Seu tipo de serviço, Premium ou Plus

  Isso determina os contratos de nível de serviço (SLAs) para resolver problemas em seu ambiente

Alertas de monitoramento de landing zone com várias contas do AMS

O AMS fornece uma maneira de você ser alertado diretamente (em vez de receber notificações do serviço AMS) para determinados alertas de monitoramento. Para se inscrever, certifique-se de que seu Cloud Architect (CA) ou Cloud Service Delivery Manager (CSDM) receba essas informações:

E-mail de alertas diretos: esses são os endereços de e-mail para os quais você deseja que o AMS envie determinados alertas baseados em recursos. Para obter detalhes sobre quais alertas são enviados diretamente para o e-mail, consulte Alertas do monitoramento de linha de base no AMS no Guia do Usuário Avançado do AMS. Para obter mais informações sobre o monitoramento do AMS, consulte Gerenciamento de monitoramento no Guia do usuário do AMS para a zona de destino de conta única.

Network configuration

- Número ASN do Transit Gateway

  Esse é o Número do Sistema Autônomo (ASN) do lado AWS de uma sessão do Border Gateway Protocol (BGP). Ele deve ser exclusivo e não pode ser o mesmo usado para seu Direct Connect ou VPN. O intervalo é de 64512 a 65534 (inclusive) para 16 bits. ASNs
- Sua infraestrutura de landing zone de várias contas do AMS VPC CIDR varia.

  Esses intervalos de CIDR não podem se sobrepor à sua rede local

  Você pode incluir um intervalo CIDR /22 ou fornecer cada CIDR de VPC individualmente. Observe que somente esses intervalos de CIDR são permitidos:
  - 10.0.0.0 - 10.255.255.255 (prefixo 10/8)
  - 172.16.0.0 - 172.31.255.255 (prefixo 172.16/12)
  - 192.168.0.0 - 192.168.255.255 (prefixo 192.168/16)

  Observe que o intervalo de IP 198.18.0.0/15 não pode ser usado (ele é reservado pelo AWS Directory Service).
  - Faixa CIDR VPC da infraestrutura principal (faixa /22 recomendada)
  - Intervalo CIDR de rede VPC (faixa /24 recomendada)
  - Intervalo CIDR VPC do Shared Services (faixa /23 recomendada)
  - Faixa CIDR DMZ VPC (faixa /25 recomendada)
- VPN ECMP (habilitar ou desabilitar)

Em VPN ECMP support, escolha enable (habilitar) se você precisar de suporte ao roteamento de múltiplos caminhos de mesmo custo (ECMP) entre as conexões VPN. Se as conexões anunciarem o mesmo CIDRs, o tráfego será distribuído igualmente entre elas.

Lista de controle de acesso à rede (NACL)

Uma lista de controle de acesso à rede (NACL) é uma camada opcional de segurança para sua VPC que atua como um firewall para controlar o tráfego de entrada e saída de uma ou mais sub-redes. Você pode configurar uma rede ACLs com regras semelhantes aos seus grupos de segurança para adicionar uma camada adicional de segurança à sua VPC. Para obter mais informações sobre as diferenças entre grupos de segurança e rede ACLs, consulte Comparação de grupos de segurança e rede ACLs.

No entanto, na landing zone multiconta do AMS, para que o AMS gerencie e monitore a infraestrutura com eficácia, o uso de NACLs é limitado ao seguinte escopo:

- NACLs não são suportadas nas contas principais de várias contas do landing zone: gerenciamento, rede, serviços compartilhados, registro e segurança.
- NACLs são suportados em contas de aplicativos com várias contas do landing zone, desde que sejam usadas apenas como uma lista de “Negar”. Além disso, eles devem ter a opção “Permitir tudo” configurada para garantir as operações de monitoramento e gerenciamento do AMS.

Em ambientes multicontas de grande escala, você também pode aproveitar recursos como firewalls de saída centralizados para controlar o tráfego de saída e/ou tabelas de roteamento do AWS Transit Gateway na landing zone de várias contas do AMS para segregar o tráfego de rede entre elas. VPCs

Configuração do Active Directory

FQDN de domínio para o Active Directory gerenciado por AMS

Proteção de terminais da Trend Micro (EPS)

- Tamanhos de instância para suas EC2 instâncias e grupos de Auto Scaling

  O Trend Micro Endpoint Protection (EPS) é o principal componente do AMS para segurança do sistema operacional. O sistema é composto por instâncias do Deep Security Manager (DSM), EC2

instâncias de retransmissão e um agente presente em todo o plano de dados do AMS e em suas EC2 instâncias. EC2

- Tipo de instância de retransmissão (o mínimo suportado pelo AMS é m5.large)
- Tamanho da instância de banco de dados (200 GB recomendados)
- Tipo de instância do RDS (somente db.m5.large ou db.m5.xlarge são permitidos)

- Tipo de licença DSM (Marketplace ou BYOL)

  Se você já tem uma licença, escolha BYOL (traga sua própria licença). A AMS entrará em contato com você para obter as informações necessárias sobre a licença.

- AWS Nome de recurso da Amazon (ARN) do usuário ou função do IAM para a assinatura do Trend Micro Deep Security (ARN da função: arn:aws:iam: ::role/) *ACCOUNT_ID ROLE_NAME*

  Forneça uma função do IAM; ARN, ou um ARN de usuário do IAM de um dos seus Contas da AWS ao qual você tenha acesso. O AMS cria uma função do IAM; em sua conta de serviços compartilhados da landing zone de várias contas do AMS e adiciona a função ou o usuário fornecido na confiança de uma função do IAM no Shared Services para que você possa assumir a função ao assinar o Trend Micro Deep Security em AWS Marketplace.

Acesso: Bastions, SSH e RDP

- Configurações do SSH Bastion

  O AMS fornece bastiões SSH em sua conta do Shared Services para acessar hosts no ambiente AMS. Para acessar a rede AMS como usuário SSH, você deve usar o SSH Bastions como ponto de entrada. O caminho da rede se origina na rede local, passa pelo gateway de trânsito (TGW) e, em seguida, é roteado DX/VPN para a VPC do Shared Services. Depois de acessar o bastion, você pode ir para outros hosts em seu ambiente AMS, desde que a solicitação de acesso adequada tenha sido concedida.

  - Contagem de instâncias desejada (2 recomendadas)
  - Máximo de instâncias (4 recomendadas)
  - Instâncias mínimas (2 recomendadas)
  - Tipo de instância (m5.large recomendado)
  - Entrada CIDRs: intervalos de endereços IP a partir dos quais os usuários em sua rede acessarão o SSH Bastions (faixa de IP 1, faixa de IP 2, faixa de IP 3,... etc)

- Configurações do RDP Bastion

Opcionalmente, o AMS fornece bastiões de RDP em sua conta do Shared Services para acessar hosts no ambiente AMS. Para acessar a rede AMS como usuário do RDP, você deve usar o RDP Bastions como ponto de entrada. O caminho da rede se origina na rede local, passa pelo TGW e, em seguida, é roteado DX/VPN para a VPC do Shared Services. Depois de acessar o bastion, você pode ir para outros hosts no ambiente AMS, desde que a solicitação de acesso adequada tenha sido concedida.

  - Tipo de instância (t3.medium recomendado)
  - Sessões mínimas desejadas (2 recomendadas)
  - Máximo de sessões desejadas (10 recomendadas)
- Tipo de configuração RDP Bastion, padrão compartilhado ou HA compartilhado (o padrão é Padrão compartilhado)

  SecureStandard = Um usuário recebe um bastião e somente um usuário pode se conectar ao bastião.

  SecureHA = Um usuário recebe dois bastiões em duas AZs diferentes para se conectar e somente um usuário pode se conectar ao bastião.

  SharedStandard = Um usuário recebe um bastião para se conectar e dois usuários podem se conectar ao mesmo bastião ao mesmo tempo.

  SharedHA = Um usuário recebe dois bastiões em duas AZs diferentes para se conectar e dois usuários podem se conectar ao mesmo bastião ao mesmo tempo.

Federação

Nome do provedor de identidade (IDP)

Padronizado como `customer-saml`

Integração do AMS Single-Account Landing Zone (SALZ)

Processo de integração do AMS SALZ

Para integrar contas AMS single-account landing zone (SALZ), você precisará seguir os seguintes passos:

1. Crie uma nova conta da AWS que o AMS configure como a conta de rede para hospedar o firewall. Crie a nova conta dentro da sua organização da AWS, se você tiver uma. O AMS seguirá o procedimento de criação de uma conta AMS normal, portanto, todas as informações necessárias devem ser coletadas (por exemplo, CIDR, licenças EPS e usuários). Nota: Uma alocação CIDR de /24 é boa.
2. Especifique se você deseja ou não remover os gateways da Internet (IGWs) das contas de tráfego de saída.
3. Determine seus domínios aprovados. O AMS permite a filtragem de destinos mantendo uma lista de domínios aprovados; a lista pode ser modificada posteriormente.
4. Confirme o tamanho da instância que você deseja usar com base na taxa de transferência esperada. Por padrão, a instância é criada em uma instância m4.xlarge em que descobrimos que a taxa de transferência do firewall é de 350 Mbps. O AMS pode aumentar o tamanho para uma instância C4.8xlarge em que a taxa de transferência esperada é de 1,25 Gbps.
5. Configure a rede entre o AMS e sua rede privada. Isso envolve várias tarefas:
    a. Aloque espaço IP
    b. Estabeleça conectividade de rede privada com a AWS
    c. Configure seu firewall
    d. Configurar o gerenciamento de acesso
    e. Agende backups
6. Forneça acesso à conta criada para o AMS.
7. Valide se o serviço AMS está funcionando corretamente.

O AMS poderá realizar a criação da conta (integração) de sua conta dentro de 2 semanas (10 dias úteis) a partir da data da solicitação inicial. Qualquer atividade de acompanhamento pode ser realizada usando o AMS Planned Event Management (PEM).

Note

- Leste dos EUA (Virgínia)
- Oeste dos EUA (Norte da Califórnia)
- Oeste dos EUA (Oregon)
- Leste dos EUA (Ohio)
- Canadá (Central)
- América do Sul (São Paulo)
- UE (Irlanda)
- UE (Frankfurt)
- UE (Londres)
- Oeste da UE (Paris)
- Ásia-Pacífico (Mumbai)
- Ásia-Pacífico (Seul)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Tóquio)

Novas regiões são adicionadas com frequência. Para obter a lista mais atual, consulte as regiões e zonas de disponibilidade da AWS.

Arquitetura de rede SALZ

O diagrama a seguir mostra o layout da rede VPC da zona de aterrissagem (SALZ) de conta única do AWS Managed Services (AMS) e é um exemplo da configuração altamente disponível.

O AMS configura todos os aspectos da rede para você com base em nossos modelos padrão e nas opções selecionadas fornecidas durante a integração. Um design de rede padrão da AWS é aplicado à sua conta da AWS, e uma nuvem privada virtual (VPC) é criada para você e conectada ao AMS por VPN ou Direct Connect. Saiba mais sobre o Direct Connect no AWS Direct Connect. VPCsOs

padrões incluem a DMZ, serviços compartilhados e uma sub-rede de aplicativos. Durante o processo de integração, outros VPCs podem ser solicitados e criados para atender às suas necessidades (por exemplo, divisões de clientes, parceiros). Após a integração, você recebe um diagrama de rede, um documento ambiental que explica como sua rede foi configurada.

> **Note**
>
> Para saber mais sobre os limites e restrições de serviço padrão para todos os serviços ativos, consulte a documentação de limites de serviços da AWS.

Nosso design de rede é construído em torno do "Princípio do Privilégio Mínimo" da Amazon. Para fazer isso, roteamos todo o tráfego, de entrada e saída, por meio de gateways, exceto o tráfego proveniente de uma rede confiável. A única rede confiável é aquela configurada entre seu ambiente local e a VPC por meio do uso de uma and/or VPN e do AWS Direct Connect (DX). O acesso é concedido por meio do uso de instâncias bastion, impedindo assim o acesso direto a quaisquer recursos de produção. Todos os seus aplicativos e recursos residem em sub-redes privadas que podem ser acessadas por meio de balanceadores de carga públicos. O tráfego de saída pública flui por meio de nossos proxies de encaminhamento para o Internet Gateway e depois para a Internet. Como alternativa, o tráfego pode fluir pela VPN ou pelo Direct Connect para o ambiente local.

Serviços compartilhados de landing zone com conta única do AMS

As sub-redes de serviços compartilhados contêm o AMS Directory Services, o host de gerenciamento que automatiza o provisionamento e as tarefas comuns, o servidor de gerenciamento de antivírus (TrendMicro) e os bastion hosts internos:

- Serviços de diretório AMS = Controlador de domínio AD

  Cria um Active Directory em contas AMS, cria o domínio AMS, une pilhas gerenciadas ao domínio na inicialização.
- Hosts de gerenciamento = Host de gerenciamento do AMS (provisionamento automatizado e tarefas comuns)

  Atue como um endpoint de API para modificar e interagir com Directory Service os controladores de Directory Service domínio.
- Serviços de segurança: servidor de gerenciamento de antivírus (TrendMicro) = EPS DSM + EPS Relay

Aproveita o software Trend Micro™ Deep Security (DSM), opera em um modelo cliente-servidor e tem um banco de dados de back-end, incluindo gerentes, agentes e retransmissores do Deep Security.

- Anfitriões de bastiões internos = bastiões do cliente

  Servidores para fins especiais projetados para serem o principal ponto de acesso da Internet e atuarem como proxy para suas outras EC2 instâncias da Amazon.

SALZ: Crie uma nova AWS conta para AMS

As cinco etapas para criar uma nova AWS conta para o AWS Managed Services (AMS) são:

1. Crie um Conta da AWS
2. Configurar o faturamento consolidado — vincular a nova conta à conta do pagador
3. Configure seu Conta da AWS para acesso ao AMS
4. Proteja a nova conta com autenticação multifator (MFA) para o usuário raiz no AMS
5. Inscreva-se AWS Marketplace para EPS

Entre em contato com seu gerente de atendimento ao cliente (CSDM) se tiver alguma dúvida.

Crie um Conta da AWS

O programa AMS exige o provisionamento de uma nova conta da Amazon Web Services (AWS). Instruções passo a passo estão disponíveis no seguinte vídeo: Como faço para criar e ativar uma nova conta da Amazon Web Services? As etapas simples são:

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

   Para obter instruções, consulte Habilitar o AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center .

> **Note**
>
> Se você já tiver uma conta, acesse a página de AWS preços e clique em Criar uma conta gratuita. Certifique-se de se inscrever no EC2 Serviço, pelo menos. Inscrever-se em um serviço permite que você acesse todos os serviços em AWS. A cobrança incorrerá apenas pelos serviços utilizados.
> Se você planeja vincular sua nova conta a uma conta pagante para fins de faturamento consolidado, não precisa inserir as informações da forma de pagamento quando solicitado. Em vez disso, quando você acessar a tela para inserir as informações do cartão de crédito, basta navegar para fora. Você precisará do endereço de e-mail associado à conta do pagador para enviar uma solicitação de billing/linked conta consolidada, detalhada na próxima seção.

> **Important**
>
> É fundamental que você garanta que um endereço de e-mail e um número de telefone estejam associados à conta para que você receba respostas a possíveis incidentes de segurança. O número de telefone e o endereço de e-mail da conta não podem ser alterados sem redefinir a senha da conta, o que é uma tarefa importante para uma conta raiz do AMS. Para garantir que esses valores sejam estáveis, é fundamental selecionar informações de contato não associadas a indivíduos, que podem mudar. Escolha um alias de e-mail que possa apontar para um grupo. Siga a mesma prática recomendada ao selecionar um número de telefone: escolha um número que possa apontar para um grupo ou para um número de propriedade da empresa e não de um indivíduo.

Configurar o faturamento consolidado — vincular a nova conta à conta do pagador

Se você quiser que sua nova Conta da AWS fatura gerenciada pela AMS seja incluída no pagamento de uma conta de AWS Organizations gerenciamento existente, você precisa configurar o faturamento consolidado e vincular as contas. Para obter detalhes sobre como fazer isso, consulte

- Faturamento consolidado AWS Organizations e estratégia de cobrança em AWS várias contas.
- Convidar um homem Conta da AWS para se juntar à sua organização

> **Note**
>
> Você pode executar essas etapas antes de transferir a conta para o AMS. Após a transferência, as etapas para ingressar na sua organização (fornecidas acima) podem ser realizadas por meio do processo de gerenciamento de mudanças. Consulte seu gerente de fornecimento de serviços em nuvem (CSDM) ou arquiteto de nuvem (CA) se precisar de ajuda.

Para obter informações gerais sobre faturamento, incluindo o gerenciamento do faturamento consolidado, consulte O que é faturamento. AWS Para AWS Organizations obter informações gerais sobre como as contas podem funcionar juntas, consulte O que é AWS Organizations. Para obter

orientação prescritiva sobre contas AWS Organizations de gerenciamento, consulte A conta de gerenciamento, acesso confiável e administradores delegados

Configure seu Conta da AWS para acesso ao AMS

Com as etapas acima concluídas, você garantiu com sucesso seus novos custos Conta da AWS e garantiu que os custos associados sejam cobrados adequadamente. A etapa final do processo é permitir que o AMS acesse a nova conta para a configuração inicial da pilha e para que as solicitações contínuas de alteração e provisionamento sejam atendidas. Para obter detalhes, leia Delegar acesso entre AWS contas usando funções do IAM. As etapas básicas são descritas nesta seção.

Ativar o acesso ao AWS site

Para conceder aos usuários do IAM acesso às informações e ferramentas de faturamento da sua conta, você deve ativar a funcionalidade.

Siga estas etapas:

1. Faça login no Console de gerenciamento da AWS com as credenciais da sua conta raiz (o e-mail e a senha que você usou para criar sua Conta da AWS). Não faça login com suas credenciais de usuário do IAM.

   A página Console de gerenciamento da AWS inicial é aberta.
2. Na barra de navegação superior, abra o menu suspenso do nome da sua conta e escolha Minha conta.

   A página inicial de faturamento é aberta.
3. Role para baixo até a área Acesso do usuário às informações de faturamento do IAM e clique em Editar no lado direito. *`The area does not appear unless you are logged in with root credentials`*.

   Uma área de acesso do Activate IAM é aberta.
4. Marque a caixa de seleção e clique em Atualizar.

   Agora é possível usar as políticas do IAM para controlar quais páginas o usuário pode acessar.

Para obter mais detalhes sobre esse processo em AWS, consulte Visão geral do gerenciamento de permissões de acesso.

Crie uma função do IAM com acesso ao AWS site

AWS Identity and Access Management (IAM) é um serviço web que ajuda você a controlar com segurança o acesso aos AWS recursos para seus usuários. Você usa o IAM para controlar quem pode usar seus AWS recursos (autenticação) e quais recursos eles podem usar e de que forma (autorização).

1. Acesse o console de gerenciamento do IAM e clique em Funções no painel de navegação esquerdo.

   A página de gerenciamento de funções é aberta com informações sobre as funções do IAM, uma opção Criar função e uma lista das funções existentes.

2. Clique em Criar função.

   A página Criar função Selecionar tipo de entidade confiável é aberta. Clique em Outro Conta da AWS e uma área de configurações se abrirá abaixo.

   Insira o ID da conta confiável do AMS fornecido pelo AMS. Deixe as opções Exigir ID externa e Exigir MFA desmarcadas.

3. Clique em Next: Permissions.

   A página Criar função Anexar políticas de permissões é aberta com opções para criar uma nova política, atualizar a página e pesquisar políticas existentes. É fornecida uma lista das políticas existentes.

4. Selecione a AdministratorAccesspolítica e clique em Avançar: Revisão.

   A página Criar revisão da função é aberta.

5. Nomeie a nova função aws_managedservices_onboarding_role e digite “AMS Onboarding Role” para a descrição da função. Revise as configurações da nova função e, se estiver satisfeito, clique em Criar função.

   A página de gerenciamento de funções é aberta com sua nova função listada.

Inscreva-se AWS Marketplace para EPS

Mudanças recentes na segurança de endpoint (EPS) do AMS exigem que você assine o TrendMicro Deep Security por meio do AWS Marketplace e aceite os termos do software.

TrendMicro oferece dois modelos de licença: por hora de instância protegida e Traga sua própria licença (BYOL).

- BYOL:
  1. Você usa sua própria licença que comprou por meio de canais externos.
  2. Você deve fornecer todas as chaves de licença ao AMS para criar a infraestrutura do EPS. Você pode fornecer um código de ativação que licencia todos os módulos ou códigos de ativação individuais que licenciam um determinado conjunto de módulos. O AMS cria somente os arquivos de licença que correspondem aos códigos de ativação fornecidos por você. Como a ativação da licença ocorre durante a integração, na presença de um engenheiro líder do AMS e do CSDM, você pode compartilhar essas informações então.
  3. Além disso, você deve assinar a assinatura BYOL TrendMicro Market Place AMI. Consulte Trend Micro Deep Security (BYOL).
- Por hora de instância protegida:
  1. Nesta assinatura, você não precisa ter nenhuma licença Trend adquirida anteriormente.
  2. No entanto, você deve assinar a assinatura do Marketplace.
  3. Nenhum compartilhamento de chave de licença com o AMS é necessário neste modelo, pois o uso do Trend é medido automaticamente, incluindo a licença de software e o uso da EC2 infraestrutura. Consulte Trend Micro Deep Security.

Para assinar a Trend Micro, siga estas etapas:

1. Faça login no seu Conta da AWS.
2. Navegue até a página do produto Trend Micro Deep Security (BYOL ou Per Protected Instance Hour).
3. Clique em Continuar para se inscrever no painel direito.
4. Clique em Aceitar termos no canto superior direito.

Habilite IDS e IPS no Trend Micro Deep Security

Você pode solicitar que o AMS habilite o Trend Micro Intrusion Detection System (IDS) e o Intrusion Protection Systems (IPS), recursos não padrão, para sua conta.

Para fazer isso, envie uma solicitação de atualização (Gerenciamento | Outros | Outros | Atualização) e inclua uma lista de endereços de e-mail para receber notificações de IDS e IPS. Esses endereços são adicionados a um tópico do SNS em sua conta, criado pelo AMS para você.

> **Note**
>
> O AMS não pode adicionar nenhum serviço da Trend Micro que possa interferir em nossa capacidade de fornecer outros serviços do AMS.

Próxima etapa: Proteja a nova conta com autenticação multifator (MFA) para o usuário raiz no AMS

Inscreva-se AWS Marketplace para CentOS 7.6

O AMS agora fornece o CentOS 7 (x86_64) - com atualizações HVM vendido pela Centos.org, como AMI do AMS. Para utilizar essa AMI, você deve optar pela licença GRATUITA do Cent OS e aceitar a licença em todas as suas contas do AMS.

Para se inscrever, acesse AWS Marketplacee siga as instruções para se inscrever.

Você não incorrerá em cobranças de software pelo uso deste produto, mas ainda será responsável por outras AWS cobranças, incluindo o EC2 uso. Se este for um produto do tipo “Traga sua própria licença”, você deve ter uma licença de software válida para usá-lo.

Você pode revisar as informações deste software no CentOS 7 (x86_64) - com o Updates HVM.

Proteja a nova conta com autenticação multifator (MFA) para o usuário raiz no AMS

Esta seção foi redigida porque contém informações confidenciais relacionadas à segurança do AMS. Essas informações estão disponíveis na documentação do console AMS. Para acessar o AWS Artifact, você pode entrar em contato com seu CSDM para obter instruções ou acessar Getting Started with AWS Artifact.

SALZ: Configure a rede

Há vários processos que precisam ser concluídos para configurar a rede para o AWS Managed Services (AMS):

1. Alocação de espaço IP para seu ambiente AMS
2. Estabelecendo conectividade de rede privada com a AWS
3. Configurando seu firewall para permitir operações do AMS

Aloque espaço IP para seu ambiente AMS

O AMS foi projetado e testado usando um bloco CIDR /16 como a alocação de rede recomendada. É importante que a rede confiável conectada ao AMS use um bloco CIDR que não se sobreponha ao bloco CIDR atribuído ao AMS. Esses endereços são necessários para configurar sua nuvem privada virtual (VPC) e sub-redes. Para obter mais informações sobre a AWS VPCs, consulte Amazon VPC Limits e Amazon VPC. FAQs

Embora um bloco CIDR /16 possa parecer um monte de endereços IP, uma VPC, uma vez criada, não pode ser expandida. Portanto, essa alocação garante que sua VPC gerenciada pelo AMS possa funcionar por um período considerável. Dentro do bloco CIDR, você deve alocar intervalos de endereços IP para, no mínimo, duas sub-redes privadas e duas sub-redes públicas.

A AWS aceita conectividade com o ambiente AMS por meio da funcionalidade nativa da rede privada virtual (VPN) da AWS. Do seu lado, isso pode ser feito por meio do AWS Direct Connect (DX), VPN de hardware ou VPN de software. No lado do AMS, usamos a funcionalidade Virtual Gateway do VPCs.

Componentes básicos do ambiente

Opções de Network-to-Amazon conectividade VPC do usuário	
Hardware VPN	Estabelece uma conexão VPN de hardware do seu equipamento de rede em uma rede remota com o equipamento de rede gerenciado pelo AMS conectado à sua VPC.
AWS Direct Connect (DX)	Estabelece uma conexão privada, lógica (ou criptografada se usada com uma VPN) da sua

Opções de Network-to-Amazon conectividade VPC do usuário	
	rede remota com a Amazon VPC, aproveitando o AWS Direct Connect.
Software VPN	Estabelece uma conexão VPN do seu equipamento em uma rede remota com um dispositivo VPN de software gerenciado pelo usuário executado dentro de uma Amazon VPC.

> **Note**
>
> O AMS recomenda VPN privada redundante para conexões DX. Seu gerente de atendimento ao cliente (CSDM) ajudará a configurar isso no momento da integração de sua conta.

Estabeleça conectividade de rede privada com a AWS

Adicione o AMS ao seu Active Directory corporativo para estabelecer conectividade. Talvez você queira realizar ações administrativas ou acessar o usuário por meio de uma conexão de rede privada. A AWS oferece conectividade VPN e linhas dedicadas via Direct Connect. As etapas a seguir explicam como trabalhar com o AMS para estabelecer um (ou ambos) meios de conectividade.

Configuração de VPN

Esta seção descreve as etapas básicas para configurar uma VPN para se comunicar entre sua VPC gerenciada pelo AMS e sua rede interna.

> **Note**
>
> Para obter uma compreensão geral sobre o uso de uma VPN com os serviços da AWS, consulte O que é a Site-to-Site VPN da AWS e tudo sobre o seu Customer Gateway (seu dispositivo de VPN).

Siga as seções do Guia do usuário de VPN da AWS para começar e testar a conexão Site-to-Site VPN para concluir as etapas a seguir.

- Etapa 1: Em sua AWS VPC, crie um gateway do cliente
- Etapa 2: Em sua AWS VPC, crie um gateway privado virtual
- Etapa 3: Em sua AWS VPC, habilite a propagação de rotas em sua tabela de rotas
- Etapa 4: Em sua AWS VPC, atualize seu grupo de segurança para habilitar o acesso SSH, RDP e ICMP de entrada
- Etapa 5: Na sua rede interna, crie uma conexão VPN e configure o gateway do cliente
- Etapa 6: testar a conectividade VPN entre a VPC e sua rede interna

Direct Connect Configuração

Esta seção descreve as etapas básicas para configurar um Direct Connect (DX) para comunicação entre sua VPC gerenciada pelo AMS e sua rede interna.

> **Note**
>
> Para obter informações sobre o uso de um DX com os serviços da AWS, consulte Conceitos básicos em um Direct Connect local.

Para configurar uma conexão DX, você precisa concluir as seguintes etapas:

1. Inscreva-se na Amazon Web Services
2. Envie a solicitação de conexão do AWS Direct Connect
3. Conclua o Cross Connect
4. (Opcional) Configure conexões redundantes com o AWS Direct Connect
5. Executado pelo AMS: criar uma interface virtual
6. Executado pelo AMS: Baixe a configuração do roteador
7. Verifique sua interface virtual

Configure seu Firewall

Esta seção foi redigida porque contém informações confidenciais relacionadas à segurança do AMS. Essas informações estão disponíveis na documentação do console AMS. Para acessar o AWS Artifact, você pode entrar em contato com seu CSDM para obter instruções ou acessar Getting Started with AWS Artifact.

Opções do AMS Bastion durante a migração/integração de aplicativos

Para oferecer a você a melhor experiência durante os esforços de migração, abaixo estão as possíveis opções que o AMS poderia aproveitar atualmente:

- Opção 1: Ignorar o Bastions apenas para fins de migração (você deve aprovar isso para fins de segurança como medida temporária).

  Observação: os recursos de auditoria ainda estarão disponíveis para garantir que o AMS tenha visibilidade de cada solicitação.
- Opção 2: Tunelamento SSH com uma ferramenta de escolha; por exemplo, PuTTy, conforme ilustrado.

  Os componentes do ambiente descritos já precisariam estar prontos para essa opção.

  O AMS forneceria notas e instruções adicionais.

Etapas de tunelamento SSH com Pu: TTy

No PuTTY, você criaria uma sessão SSH, com o IP público do bastion host, forneceria a chave PEM na seção AUTH e, em seguida, criaria um túnel. A porta de origem do túnel deve ser uma porta local não utilizada (por exemplo, 5000) e o IP seria o IP do host de destino (a caixa do Windows que você está tentando acessar) com a porta RDP anexada (3389). Certifique-se de salvar sua configuração, pois você não quer ter que fazer isso toda vez que fizer login na caixa. Conecte-se ao bastion host e faça login. Em seguida, inicie uma sessão RDP para localhost:5000 (ou qualquer porta que você escolher).

1. Defina o nome do host ou IP público do bastion host

2. Em SSH ->Auth, defina o arquivo de chave privada no formato.ppk

3. Em SSH ->Tunnels, adicione a nova porta encaminhada. A porta de origem deve ser a porta arbitrária não utilizada e o destino deve ser o IP do servidor de destino atrás do bastion host, com a porta RDP anexada.

4. Conecte-se ao bastion host via PuTTY e faça login.

5. Inicie uma sessão RDP em localhost:5000 para acessar o servidor de destino.

SALZ: Configurar o gerenciamento de acesso

Usar uma rede gerenciada pelo AWS Managed Services (AMS) significa dar acesso ao AMS para gerenciar sua infraestrutura de nuvem. Você precisará configurar um meio de conexão segura entre sua rede privada e o AMS. Isso começa com algumas decisões sobre os tipos de acesso que você deseja fornecer:

- Para acesso ao AMS API/CLI e ao console: você deve instalar o AMS CLI (as instruções são fornecidas neste documento). Você usa a API de gerenciamento de alterações do AMS para fazer solicitações de alteração ao AMS e a API do AMS SKMS para saber mais sobre seus recursos gerenciados pelo AMS. Usando os Serviços de Federação do Active Directory (AD FS), você pode acessar o console AMS.

  > **Note**
  >
  > Se você estiver configurando seu próprio ITSM, precisará usar a API do AWS Support (SAPI) para solicitações de serviços e relatórios de incidentes. A SAPI está documentada na AWS Support API Reference.

- Para acesso do usuário: se você gerencia usuários com o Windows Active Directory (AD) ou com uma Linux/LDAP solução, a conectividade precisa ser estabelecida entre o AD no lado do AMS (por meio dos Serviços de Diretório) e seu diretório.
- Por exemplo, acesso: o acesso no nível da instância é realizado por meio de uma configuração unidirecional do Forest Trust. Os Serviços de Diretório confiam nas credenciais em seu CORP AD, permitindo que pilhas no lado do AMS permitam o login com credenciais CORP.

  Observe que o Active Directory (AD) no qual o AMS configura a confiança deve ser o diretório que tem as contas de usuários autorizados por você a obter acesso aos seus recursos da AWS.

> **Important**
>
> Para configurar uma relação de confiança florestal, o AMS exige que seu controlador de domínio Políticas locais -> Opções de segurança -> Acesso à rede: canais nomeados que podem ser acessados anonimamente, tenham os canais Netlogon e lsarpc listados. Esses canais são listados por padrão, mas às vezes são removidos por questões de segurança. Depois que a confiança for estabelecida, eles poderão ser removidos da lista novamente.

Estabeleça uma relação de confiança do Active Directory (AD)

Antes de começar a estabelecer uma relação de confiança do Active Directory (AD) para sua conta do AWS Managed Services (AMS), certifique-se de que as portas de firewall apropriadas estejam abertas.

A confiança do Active Directory gerenciado pelo AMS e do seu serviço de diretório corporativo permite que você use suas credenciais gerenciadas pela empresa para acessar instâncias gerenciadas pelo AMS e realizar funções administrativas, de desenvolvimento ou de teste.

Criar uma conexão de confiança é um exercício de duas partes:

Primeiro, configure um encaminhamento condicional, uma configuração de DNS para que as consultas de DNS saibam para qual servidor DNS ir.

Segundo, configure uma relação de confiança, uma construção do Active Directory (AD) para permitir o acesso de usuários em um domínio para usar recursos em outro domínio.

Configurar o encaminhador condicional

Siga este artigo do Microsoft AD Atribuir um encaminhador condicional para um nome de domínio e use essas configurações e opções:

1. No AD DNS Manager -> Criar um novo encaminhador condicional, em Domínio DNS: use o nome de domínio AMS fornecido a você; por exemplo,. *A523434123.amazonaws.com*
2. Em Endereços IP dos servidores principais: adicione os endereços IP fornecidos pela AMS. Verifique se não há um problema de conexão validando os dois endereços.
3. Selecione Armazenar este encaminhador condicional no Active Directory e replique da seguinte forma: Todos os servidores DNS neste domínio e pressione OK.

Configurar a confiança

Para configurar a confiança da sua conta do AWS Managed Services (AMS), siga este artigo do MicroSoft AD Crie uma relação de confiança florestal unidirecional e de entrada para um lado da confiança, usando as configurações e opções descritas nesta seção.

1. Abra a caixa de diálogo Iniciar -> Ferramentas administrativas -> Domínios e relações de confiança do Active Directory. Clique com o botão direito do mouse no nó do domínio com o qual você deseja estabelecer uma relação de confiança e clique em Propriedades -> Relações de Confiança -> Nova Confiança para abrir o Assistente de Nova Confiança. Insira o nome de domínio fornecido pelo AMS para o nome confiável e pressione Avançar.
2. Em Tipo de confiança, selecione Forest Trust. Pressione Próximo.
3. Em Direção de Confiança, selecione Unidirecional: entrada. Pressione Próximo.
4. Em Lados da Confiança, selecione Somente este domínio. Pressione Próximo.
5. Em Senha confiável, digite uma senha de sua escolha. Pressione Próximo.
6. Para Seleções de confiança concluídas e Criação de confiança concluída, basta pressionar Avançar.
7. Em Confirmar confiança recebida, selecione Não, não confirme a confiança recebida. Pressione Próximo.
8. Em Concluído o Assistente de Nova Confiança, selecione Concluir e, em seguida, OK para fechar.
9. Forneça a senha confiável (entre em contato conosco pelo número de telefone do seu CSDM por motivos de segurança). O AMS concluirá a configuração de confiança.

Sites e serviços do Active Directory

Para reduzir a latência de login, adicione o intervalo CIDR da VPC aos seus sites e serviços do Active Directory (Iniciar -> Ferramentas administrativas -> Sites e serviços do Active Directory). Adicione o intervalo CIDR da VPC a um site do Active Directory que contém controladores de domínio mais próximos da AWS.

Roteamento de sufixo de nome do Active Directory

Depois que a confiança florestal unidirecional for estabelecida, conclua as etapas adicionais.

1. Em Iniciar > Todos os programas > Ferramentas administrativas, clique em Domínios e relações de confiança do Active Directory.

O console Domínios e Relações de Confiança do Active Directory é aberto.

2. Clique com o botão direito do mouse em seu domínio corporativo e clique em Propriedades

   A caixa de diálogo Propriedades desse domínio é aberta.

3. Clique na guia Confianças.

   A página Trusts é aberta.

4. Clique no nome de domínio da Amazon e clique em Propriedades.

   A página de propriedades do domínio fiduciário da Amazon é aberta.

5. Clique em Name Suffix Routing e clique em Atualizar.

   Essas etapas garantem que os nomes principais do serviço (SPNs) possam ser resolvidos sobre a confiança.

Solução de problemas

Algumas coisas para tentar se você tiver problemas:

- O grupo de segurança de saída do Active Directory gerenciado pelo AMS precisa ter permissão para se conectar por meio de seu bloco CIDR (por exemplo, 10.27.0.0/16) ao seu controlador de domínio.
- Rastreie a rota no console da AWS de controlador de domínio para controlador de domínio, verificando todos os grupos de segurança ao longo do caminho.
- Certifique-se de poder executar ping nos controladores de domínio do Active Directory gerenciados pelo AMS se o Internet Control Message Protocol (ICMP) for permitido.
- Certifique-se de que seu controlador de domínio possa se comunicar com os AWS Directory Services.
- Certifique-se de que os encaminhadores condicionais sejam resolvidos e validados.
- Se você não vê Forest Trust no assistente New Trust, então seus encaminhadores condicionais podem não estar funcionando corretamente:
  - Use nslookup para testar a resolução
  - Tente reinicializar o controlador de domínio

Active Directory gerenciado pelo AMS

O AMS agora oferece um novo serviço chamado Managed Active Directory (também conhecido como Managed AD), que permite que o AMS cuide das operações de infraestrutura do Active Directory (AD), mantendo você no controle da administração do Active Directory.

O suporte do AMS para o Managed AD é semelhante ao suporte do AMS para o Amazon Relational Database Service (Amazon RDS). Em ambos os casos, AWS (incluindo o AMS) suporta a criação e o gerenciamento da infraestrutura que executa o serviço, enquanto você executa o controle de acesso e todas as funções administrativas. Este modelo tem as seguintes vantagens:

- Limita os riscos de segurança: AWS e o AMS não precisa de privilégios administrativos em seu domínio.
- Integrações diretas: você pode usar seu modelo de autorização atual e integrá-lo ao AD sem precisar interagir com o AMS.

Observações:

- Nem o AMS nem você terão acesso aos controladores de domínio do AD gerenciado, portanto, nenhum software pode ser instalado nos controladores de domínio. Isso é importante porque soluções de terceiros que exigem a instalação de software em controladores de domínio não são permitidas.

  O Access funciona assim:

  - AWS Equipe do Directory Service: tem acesso aos controladores de domínio.
  - AMS: tem acesso ao Directory Service APIs para realizar determinadas ações no domínio. Essas ações incluem tirar instantâneos do AD, alterar o esquema do AD e outras ações.
  - Você: Tenha acesso ao domínio (AD) para criar usuários, grupos e assim por diante.
- Recomendamos que você faça uma prova de conceito no AD gerenciado antes de migrar seu AD corporativo, porque nem todas as funcionalidades de um ambiente AD tradicional estão disponíveis em um ambiente de AD gerenciado.
- O AMS não gerenciará nem fornecerá orientação sobre o gerenciamento do AD. Por exemplo, o AMS não fornecerá orientação sobre a estrutura da unidade organizacional, a estrutura da política de grupo, as convenções de nomenclatura de usuários do AD e assim por diante.

Funciona assim:

1. O AMS integra um novo Conta da AWS para você, separado e adicional à sua conta do AMS, e provisiona um ambiente do Active Directory (AD) por meio do AWS Directory Service (consulte também O que é o AWS Directory Service?).

   A seguir estão as informações que um integrador de sistemas precisaria coletar de você para que o AMS integrasse o Managed AD:

   - Informações da conta
     - ID da conta Conta da AWS que foi criada para seu AD gerenciado pelo AMS: número Conta da AWS
     - Região para integrar seu AD gerenciado para: Região da AWS
   - Informações gerenciadas do Active Directory:
     - Edição Microsoft AD: Padrão/Empresarial. O AWS Microsoft AD (Standard Edition) inclui 1 GB de armazenamento de objetos de diretório. Essa capacidade pode suportar até 5.000 usuários ou 30.000 objetos de diretório, incluindo usuários, grupos e computadores. O AWS Microsoft AD (Enterprise Edition) inclui 17 GB de armazenamento de objetos de diretório, que pode suportar até 100.000 usuários ou 500.000 objetos.

       Para obter mais informações, consulte AWS Directory Service FAQs.
     - FQDN de domínio: O FQDN do seu domínio AMS Managed AD.
     - Nome NetBIOS do domínio: o nome NetBIOS do seu domínio AMS Managed AD.
     - Números de contas padrão do AMS com as quais você gostaria de integrar o AD gerenciado (o AMS configura uma relação de confiança unidirecional do AD da conta padrão do AMS para o AD gerenciado)
     - As modificações no esquema do Active Directory são necessárias e, em caso afirmativo, quais modificações?
     - Por padrão, dois controladores de domínio são provisionados. Você precisa de mais? Em caso afirmativo, de quantos você precisa e por qual motivo?
   - Rede para informações gerenciadas do Active Directory:
     - CIDR gerenciado do AD VPC para controladores de domínio (um CIDR em seu intervalo de sub-rede privada para os controladores de domínio do AD gerenciado):
       - Sub-rede CIDR 1 para controladores de domínio: [seu CIDR precisa fazer parte do CIDR AD VPC AMS Managed]
       - Sub-rede CIDR 2 para controladores de domínio: [seu CIDR precisa fazer parte do CIDR AD VPC AMS Managed]

Por exemplo:

- CIDR gerenciado do AD VPC: 192.168.0.0/16
- CIDR 1 para controladores de domínio: 192.168.1.0/24
- CIDR 2 para controladores de domínio: 192.168.2.0/24

Para evitar conflitos de endereço IP, certifique-se de que o CIDR gerenciado da AD VPC especificado não entre em conflito com nenhum outro CIDR de sub-rede privada que você esteja usando na sua rede corporativa.

- Tecnologia VPN (opcional): [Direct Connect/Direct Connect e VPN]
  - Número do sistema autônomo BGP (ASN) do seu gateway: [ASN fornecido pelo cliente]
  - O endereço IP roteável pela Internet para a interface externa do seu gateway, o endereço deve ser estático: [Endereço IP fornecido pelo cliente]
  - Se sua conexão VPN requer rotas estáticas ou não: [sim/não]

2. O AMS fornece a senha da conta de administrador para o ambiente AD e solicita que você redefina a senha para que os engenheiros do AMS não possam mais acessar seu ambiente AD.
3. Para redefinir a senha da conta de administrador, conecte-se ao seu ambiente do Active Directory usando Usuários e Computadores do Active Directory (ADUC). O ADUC e outras Ferramentas de Administração de Servidor Remoto (RSAT) devem ser instalados e executados em hosts administrativos provisionados por você em uma infraestrutura que não seja do AMS. A Microsoft tem as melhores práticas para proteger esses hosts administrativos. Para obter informações, consulte Implementação de hosts administrativos seguros. Você gerencia seu ambiente do Active Directory usando esses hosts administrativos.
4. Nas operações diárias, o AMS gerencia Conta da AWS até o lado do AWS Directory Service; por exemplo, configuração de VPC, backups do AD, criação e exclusão de confiança do AD e assim por diante. Você usa e gerencia seu ambiente AD; por exemplo, criação de usuários, criação de grupos, criação de políticas de grupo e assim por diante.

Para ver a tabela RACI mais recente, consulte a seção “Funções e responsabilidades” na seção Consulte a descrição do serviço.

Federe seu Active Directory com as funções do AMS AWS Identity and Access Management

O objetivo de federar seu diretório com as funções do AMS IAM é permitir que os usuários corporativos usem suas credenciais corporativas para interagir com o Console de gerenciamento da AWS e o e, portanto AWS APIs, com o console do AMS e. APIs

Exemplo de processo de federação

Este exemplo usa os Serviços de Federação do Active Directory (AD FS); no entanto, qualquer tecnologia que ofereça suporte à AWS Identity and Access Management Federação é suportada. Para obter mais informações sobre a federação do IAM AWS compatível, consulte Parceiros do IAM e provedores de identidade e federação. Seu CSDM o ajudará nesse processo, que envolve um esforço conjunto com sua equipe de AD e o AMS.

Para obter informações detalhadas sobre a integração do SAML para acesso à API, consulte este AWS blog, Como implementar API federada e acesso à CLI usando SAML 2.0 e AD FS.

> **Note**
>
> Para obter um exemplo de instalação da CLI do AMS e do SAML, consulte. Apêndice: Regra de declaração dos Serviços de ActiveDirectory Federação (ADFS) e configurações de SAML

Configurando a federação no console AMS (SALZ)

As funções do IAM e o provedor de identidade SAML (entidade confiável) detalhados na tabela a seguir foram provisionados como parte da integração da sua conta. Essas funções permitem que você envie e monitore RFCs solicitações de serviço e relatórios de incidentes, além de obter informações sobre suas VPCs pilhas de anúncios.

Role (Função)	Provedor de identidades	Permissões
Customer_ _Função ReadOnly	SAML	Para contas AMS padrão. Permite que você envie RFCs para fazer alterações na infraestrutura gerenciada pelo AMS,

Role (Função)	Provedor de identidades	Permissões
		bem como crie solicitações de serviço e incidentes.
customer_managed_ad_user_role	SAML	Para contas do AMS Managed Active Directory. Permite que você faça login no console do AMS para criar solicitaç ões e incidentes de serviço (não RFCs).

Para obter a lista completa das funções disponíveis em diferentes contas, consulteFunção de usuário do IAM no AMS .

Um membro da equipe de integração carrega o arquivo de metadados da sua solução de federação para o provedor de identidade pré-configurado. Você usa um provedor de identidade SAML quando deseja estabelecer confiança entre um IdP (provedor de identidade) compatível com SAML, como Shibboleth ou Active Directory Federation Services, para que os usuários da sua organização possam acessar os recursos da AWS. Os provedores de identidade SAML no IAM são usados como principais em uma política de confiança do IAM com as funções acima.

Enquanto outras soluções de federação fornecem instruções de integração para a AWS, o AMS tem instruções separadas. O uso da postagem do blog a seguir, Habilitando a federação na AWS usando o Windows Active Directory, AD FS e SAML 2.0, junto com as emendas fornecidas abaixo, permitirá que seus usuários corporativos acessem várias contas da AWS a partir de um único navegador.

Depois de criar a confiança da parte confiável de acordo com a postagem do blog, configure as regras de reivindicações da seguinte maneira:

- NameId: Siga a postagem do blog.
- RoleSessionName: Use os seguintes valores:
  - Nome da regra de reivindicação: RoleSessionName
  - Armazenamento de atributos: Active Directory
  - Atributo LDAP: SAM-Account-Name
  - Tipo de reclamação de saída: https://aws.amazon.com/SAML/ Atributos/ RoleSessionName
- Obtenha grupos do AD: siga a postagem do blog.

- Reivindicação de função: siga a postagem do blog, mas para a regra personalizada, use o seguinte:

```
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/"));
```

Ao usar o AD FS, você deve criar grupos de segurança do Active Directory para cada função no formato mostrado na tabela a seguir (customer_managed_ad_user_role é somente para contas AD gerenciadas pelo AMS):

Grupo	Role (Função)
AWS- [AccountNo] ReadOnly -Cliente_ _Função	Customer_ _Função ReadOnly
AWS- [AccountNo] -customer_managed_ ad_user_role	customer_managed_ad_user_role

Para obter mais informações, consulte Configurando asserções SAML para a resposta de autenticação.

> **Tip**
>
> Para ajudar na solução de problemas, baixe o plug-in rastreador SAML para seu navegador.

Enviando a solicitação de federação ao AMS

Se essa for sua primeira conta, trabalhe com seus CSDM (s) and/or Cloud Architect (s) para fornecer o arquivo XML de metadados para seu provedor de identidade.

Se você estiver integrando uma conta adicional ou provedor de identidade e tiver acesso à conta de gerenciamento ou à conta do aplicativo desejada, siga estas etapas.

1. Crie uma solicitação de serviço no console do AMS e forneça os detalhes necessários para adicionar o provedor de identidade:

- AccountId da conta em que o novo provedor de identidade será criado.
- O nome do provedor de identidade desejado, se não for fornecido, o padrão será customer-saml; normalmente, ele deve corresponder às configurações definidas no seu provedor de federação.
- Para contas existentes, inclua se o novo provedor de identidade deve ser propagado para todas as funções de console existentes ou forneça uma lista de funções que devem confiar no novo provedor de identidade.
- Anexe o arquivo XML de metadados exportado do seu agente de federação à solicitação de serviço como anexo de arquivo.

2. Na mesma conta em que você criou a solicitação de serviço, crie uma nova RFC usando CT-ID ct-1e1xtak34nx76 (Gerenciamento | Outros | Outros | Criar) com as seguintes informações.

   - Título: “SAML IDP integrado <Name>para conta < >AccountId”.
   - AccountId da conta em que o provedor de identidade será criado.
   - Nome do provedor de identidade.
   - Para contas existentes: se o provedor de identidade deve ser propagado para todas as funções de console existentes ou a lista de funções que devem confiar no novo provedor de identidade.
   - ID do caso da solicitação de serviço criada na Etapa 1, em que o arquivo XML de metadados é anexado.

Verifique o acesso ao console

Depois de configurar o ADFS e ter a URL do AMS para usar na autenticação, siga estas etapas.

Com uma configuração do Active Directory Federated Service (ADFS), você pode seguir estas etapas:

1. Abra uma janela do navegador e acesse a página de login fornecida para sua conta. A IdpInitiatedSignOnpágina ADFS da sua conta é aberta.
2. Selecione o botão de rádio ao lado de Entrar em um dos sites a seguir. A lista de opções do site de login fica ativa.
3. Escolha o site signin.aws.amazon.com e clique em Entrar. As opções para inserir suas credenciais estão abertas.

4. Insira suas credenciais CORP e clique em Entrar. As Console de gerenciamento da AWS aberturas.
5. Cole na barra de localização o URL do console AMS e pressione Enter. O console AMS é aberto.

Verifique o acesso à API

O AMS usa a API da AWS, com algumas operações específicas da AMS que você pode ler na Referência da API do AMS.

A AWS fornece vários SDKs que você pode acessar em Tools for Amazon Web Services. Se você não quiser usar um SDK, pode fazer chamadas diretas à API. Para obter informações sobre autenticação, consulte Assinar solicitações de API da AWS. Se você não estiver usando um SDK ou fazendo solicitações diretas de API HTTP, poderá usar o AMS CLIs for Change Management (CM) e o SKMS.

Instale o AMS CLIs

Para obter um exemplo de instalação da CLI do AWS Managed Services (AMS) para usar com o SAML, consulte. Apêndice: Regra de declaração dos Serviços de ActiveDirectory Federação (ADFS) e configurações de SAML

Se você precisar de acesso temporário, para obter e instalar o AWS Managed Services (AMS) SDKs, consulte Acesso temporário ao console AMS.

> **Note**
>
> Você deve ter credenciais de administrador para esse procedimento.

A AWS CLI é um pré-requisito para usar o AWS Managed Services (AMS) CLIs (Change Management and SKMS).

1. Para instalar a AWS CLI, consulte Instalação da interface de linha de comando da AWS e siga as instruções apropriadas. Observe que, na parte inferior dessa página, há instruções para usar diferentes instaladores, Linux, MS Windows, macOS, ambiente virtual, instalador empacotado (Linux, macOS ou Unix).

   Após a instalação, execute `aws help` para verificar a instalação.

2. Depois que o AWS CLI estiver instalado, para instalar ou atualizar o AMS CLI, baixe o arquivo zip distribuível do AMS AMS CLI ou do SDK do AMS e descompacte. Você pode acessar os distribuíveis do AMS CLI por meio do link Developer's Resources no painel esquerdo do console do AMS.
3. O arquivo README fornece instruções para qualquer instalação.

   Abra uma das seguintes opções:

   - Zip da CLI: fornece somente a CLI do AMS.
   - Zip do SDK: fornece todo o AMS APIs e a CLI do AMS.

   Para Windows, execute o instalador apropriado (somente sistemas de 32 ou 64 bits):

   - 32 bits: ManagedCloudAPI_x86.msi
   - 64 bits: ManagedCloudAPI_x64.msi

   Para Mac/Linux, execute o arquivo chamado: AWSManagedServices_InstallCLI.sh executando este comando:. `sh AWSManagedServices_InstallCLI.sh` Observe que os diretórios amscm e amsskms e seu conteúdo devem estar no mesmo diretório do arquivo.sh. AWSManagedServices_InstallCLI
4. Se suas credenciais corporativas forem usadas por meio de federação com a AWS (a configuração padrão do AMS), você deverá instalar uma ferramenta de gerenciamento de credenciais que possa acessar seu serviço de federação. Por exemplo, você pode usar este blog de segurança da AWS Como implementar API federada e acesso à CLI usando SAML 2.0 e AD FS para ajudar a configurar suas ferramentas de gerenciamento de credenciais.
5. Após a instalação, execute `aws amscm help` e veja `aws amsskms help` os comandos e opções.

> **Note**
>
> A CLI do AMS deve estar instalada para que esses comandos funcionem. Para instalar a API ou a CLI do AMS, acesse a página Recursos para desenvolvedores do console AMS. Para obter material de referência sobre a API AMS CM ou a API AMS SKMS, consulte a seção Recursos de informação do AMS no Guia do usuário. Talvez seja necessário adicionar uma `--profile` opção para autenticação; por exemplo,`aws amsskms` *`ams-cli-command`* `--profile SAML`. Talvez você também precise

adicionar a `--region` opção, pois todos os comandos do AMS saem de us-east-1; por exemplo. `aws amscm ams-cli-command --region=us-east-1`

Programação de backups do AMS no nível da VPC

O agendamento de backup do AWS Managed Services (AMS) na VPC, onde as instâncias de destino são alocadas, é criado durante a integração da conta com uma tag padrão no esquema de criação da VPC. O sistema de backup agenda a execução dos instantâneos dependendo dessa tag VPC. A modificação do cronograma pode ser feita criando uma solicitação de serviço. Para obter mais informações, consulte VPC Tag and Defaults.

Para padrões de backup, consulte Entendendo os padrões do AMS

SALZ: Configurações padrão

Sua rede AWS Managed Services (AMS) é configurada de forma padronizada com padrões para a maioria dos serviços.

Esta seção descreve as configurações padrão que o AMS usa para segurança, acesso, monitoramento, registro, continuidade e gerenciamento de patches.

Para ver um exemplo de custos de infraestrutura, consulte Componentes básicos.

As regras de firewall são fornecidas em Configure seu Firewall

Segurança de terminais (EPS)

Os recursos que você provisiona em seu ambiente AMS Advanced incluem automaticamente a instalação de um cliente de monitoramento de segurança de terminais (EPS). Esse processo garante que os recursos gerenciados pelo AMS Advanced sejam monitorados e suportados 24 horas por dia, 7 dias por semana. Além disso, o AMS Advanced monitora todas as atividades do agente e um incidente é criado se algum evento de segurança for detectado.

> **Note**
>
> Os incidentes de segurança são tratados como incidentes; para obter mais informações, consulte Resposta a incidentes.

A segurança de terminais fornece proteção antimalware, especificamente, as seguintes ações são suportadas:

- EC2 registro de instâncias com EPS
- EC2 instâncias cancelam o registro do EPS
- EC2 instâncias de proteção antimalware em tempo real
- Batimento cardíaco iniciado pelo agente EPS
- EPS restaura arquivo em quarentena
- Notificação de evento EPS
- Relatórios de EPS

O AMS Advanced usa o Trend Micro para segurança de terminais (EPS). Essas são as configurações padrão de EPS. Para saber mais sobre a Trend Micro, consulte a Central de Ajuda do Trend Micro Deep Security; observe que links que não são da Amazon podem ser alterados sem aviso prévio.

As configurações padrão do AMS Advanced Multi-Account Landing Zone (MALZ) estão descritas nas seções a seguir; para configurações não padrão do EPS da zona de pouso multiconta do AMS, consulte Configurações não padrão do EPS da zona de aterrissagem multicontas do AMS Advanced.

> **Note**
>
> Você pode trazer seu próprio EPS, veja AMS trazer seu próprio EPS.

Configurações gerais de EPS

Configurações gerais de rede de segurança de terminais.

Padrões do EPS

Configuração	Padrão
Portas de firewall (grupo de segurança de instâncias)	Os agentes do EPS Deep Security Manager (DSMs) devem ter a porta 4120 aberta Agent/Relay para a comunicação com o Manager e a porta 4119 para o Manager Console. Os relés

Configuração	Padrão
	EPS devem ter a porta 4122 aberta Manager/Agent para a comunicação com o relé. Nenhuma porta específica deve estar aberta para a comunicação de entrada da instância do cliente porque os agentes iniciam todas as solicitações.
Direção de comunicação	Agente/equipamento iniciado
Intervalo de pulsação	Dez minutos
Número de batimentos cardíacos perdidos antes de um alerta	Dois
Desvio máximo permitido (diferença) entre os horários do servidor	Ilimitado
Gerar erros off-line para máquinas virtuais inativas (registradas, mas não on-line)	Não
Política padrão	Política básica (descrita a seguir)
Ativação de vários computadores com o mesmo nome de host	É permitido
Alertas para atualizações pendentes são gerados	Depois de sete dias

Configuração	Padrão
Cronograma de atualização	O AMS tem como meta um ciclo de lançamento mensal para as atualizações do software Trend Micro Deep Security Manager (DSM) / Deep Security Agent (DSA). No entanto, o AMS não mantém um SLA para atualizações. As atualizações são realizadas em toda a frota pelas equipes de desenvolvedores do AMS durante uma implantação. As atualizações do DSA/DSA são registradas nos eventos do sistema Trend Micro DSM que o AMS retém localmente por padrão por 13 semanas. Para obter a documentação do fornecedor, consulte Eventos do sistema na Central de Ajuda do Trend Micro Deep Security. Os registros também são exportados para o grupo de registros/aws/ams/eps/var/log/DSM.log na Amazon. CloudWatch
Fonte de atualização	Servidor de atualização Trend Micro (https://ipv6-iaus.trendmicro.com/iau_server.dll/)
Exclusão de dados de eventos ou registros	Eventos e registros são excluídos do banco de dados DSM após sete dias.
As versões do software do agente são mantidas	Até cinco
As atualizações de regras mais recentes são realizadas	Até dez
Armazenamento de registros	Por padrão, os arquivos de log são armazenados com segurança no Amazon S3, mas você também pode arquivá-los no Amazon Glacier para ajudar a atender aos requisitos de auditoria e conformidade.

Política básica

Configurações padrão da política básica de segurança de endpoints.

Política básica de EPS

Configuração	Padrão
Módulos habilitados	Anti-Malware
Módulos deficientes	Reputação na Web
	Firewall
	Proteção contra intrusões
	Monitoramento de integridade
	Inspeção de registros
	Controle de aplicativos

Antimalware

Configurações antimalware de segurança de terminais.

Padrões de antimalware EPS

Configuração	Padrão	Observações
Verificação em tempo real	Digitalize tudo	Coloque em quarentena todos os vírus suspeitos. Ativação IntelliTrap e spyware/grayware proteção. O spyware e o Grayware acionam o Anti-Malware
	Todos os Day/All dias (24 horas)	

Configuração	Padrão	Observações
		e resultam na quarentena do item.
Digitalização manual	Digitalize tudo	Deve ser solicitado e, em seguida, segue a configuração padrão de verificação em tempo real.
Escaneamento agendado	Digitalize tudo	Marcado para o último domingo de cada mês, às 6h.
Proteção inteligente	Desabilitado	N/D
Arquivos em quarentena	Gerenciador de segurança profunda da Trend Micro (DSM)	Aproximadamente 1 GB de disco reservado para quarentena.
Limitação de digitalização	Trend Micro DSM	Digitalize arquivos de todos os tamanhos.
Spyware ou grayware permitidos	Nenhum	N/D
Notificação de evento local	Sim	N/D

Grupos de segurança

Na AWS VPCs, os grupos de segurança da AWS atuam como firewalls virtuais, controlando o tráfego de uma ou mais pilhas (uma instância ou um conjunto de instâncias). Quando uma pilha é iniciada, ela é associada a um ou mais grupos de segurança, que determinam qual tráfego pode chegar até ela:

- Para pilhas em suas sub-redes públicas, os grupos de segurança padrão aceitam tráfego de HTTP (80) e HTTPS (443) de todos os locais (a Internet). As pilhas também aceitam tráfego SSH e RDP interno da sua rede corporativa e dos bastiões da AWS. Essas pilhas podem então sair por

qualquer porta para a Internet. Eles também podem sair para suas sub-redes privadas e outras pilhas em sua sub-rede pública.

- As pilhas em suas sub-redes privadas podem sair para qualquer outra pilha em sua sub-rede privada, e as instâncias dentro de uma pilha podem se comunicar totalmente entre si por meio de qualquer protocolo.

> **Important**
>
> O grupo de segurança padrão para pilhas em sub-redes privadas permite que todas as pilhas em sua sub-rede privada se comuniquem com outras pilhas nessa sub-rede privada. Se quiser restringir as comunicações entre pilhas em uma sub-rede privada, você deve criar novos grupos de segurança que descrevam a restrição. Por exemplo, se você quiser restringir as comunicações com um servidor de banco de dados para que as pilhas nessa sub-rede privada só possam se comunicar de um servidor de aplicativos específico por meio de uma porta específica, solicite um grupo de segurança especial. Como fazer isso está descrito nesta seção.

Security groups padrão

MALZ

A tabela a seguir descreve as configurações padrão do grupo de segurança de entrada (SG) para suas pilhas. O SG é chamado de "SentinelDefaultSecurityGroupPrivateOnly-VPC-ID”, onde está *ID* um ID de VPC em sua conta de landing zone com várias contas do AMS. Todo o tráfego pode ser enviado para "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly" por meio desse grupo de segurança (todo o tráfego local nas sub-redes da pilha é permitido).

Todo o tráfego pode ser enviado para 0.0.0.0/0 por um segundo grupo de segurança "". SentinelDefaultSecurityGroupPrivateOnly

> **Tip**
>
> Se você estiver escolhendo um grupo de segurança para um tipo de alteração do AMS, como EC2 OpenSearch criar ou criar domínio, você usaria um dos grupos de segurança padrão descritos aqui ou um grupo de segurança criado por você. Você pode encontrar a lista de grupos de segurança, por VPC, no console da AWS ou no EC2 console da VPC.

Há grupos de segurança padrão adicionais que são usados para fins internos do AMS.

Grupos de segurança padrão do AMS (tráfego de entrada)

Tipo	Protocolo	Intervalo de portas	Origem
Todo o tráfego	Tudo	Todos	SentinelDefaultSecurityGroupPrivateOnly (restringe o tráfego de saída a membros do mesmo grupo de segurança)
Todo o tráfego	Tudo	Todos	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (não restringe o tráfego de saída)
HTTP, HTTPS, SSH, RDP	TCP	80/443 (Fonte 0.0.0.0/0) O acesso SSH e RDP é permitido a partir dos bastiões	SentinelDefaultSecurityGroupPublic (não restringe o tráfego de saída)
Bastiões MALZ:			
SSH	TCP	22	SharedServices VPC CIDR e DMZ VPC CIDR, além de VPC CIDR fornecido pelo cliente CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
Bastiões de 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

A tabela a seguir descreve as configurações padrão do grupo de segurança de entrada (SG) para suas pilhas. O SG é denominado "mc-initial-garden- SentinelDefaultSecurityGroupPrivateOnly -*ID*", onde *ID* é um identificador exclusivo. Todo o tráfego pode ser enviado para "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly" por meio desse grupo de segurança (todo o tráfego local nas sub-redes da pilha é permitido).

Todo o tráfego pode ser enviado para 0.0.0.0/0 por um segundo grupo de segurança "- -". mc-initial-garden SentinelDefaultSecurityGroupPrivateOnlyEgressAll *ID*

> **Tip**
>
> Se você estiver escolhendo um grupo de segurança para um tipo de alteração do AMS, como EC2 OpenSearch criar ou criar domínio, você usaria um dos grupos de segurança padrão descritos aqui ou um grupo de segurança criado por você. Você pode encontrar a lista de grupos de segurança, por VPC, no console da AWS ou no EC2 console da VPC.

Há grupos de segurança padrão adicionais que são usados para fins internos do AMS.

Grupos de segurança padrão do AMS (tráfego de entrada)

Tipo	Protocolo	Intervalo de portas	Origem
Todo o tráfego	Tudo	Todos	SentinelDefaultSecurityGroupPrivateOnly (restringe o tráfego de saída a membros do mesmo grupo de segurança)
Todo o tráfego	Tudo	Todos	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (não restringe o tráfego de saída)
HTTP, HTTPS, SSH, RDP	TCP	80/443 (Fonte 0.0.0.0/0) O acesso SSH e RDP é permitido a partir dos bastiões	SentinelDefaultSecurityGroupPublic (não restringe o tráfego de saída)
Bastiões MALZ:			

Tipo	Protocolo	Intervalo de portas	Origem
SSH	TCP	22	SharedServices VPC CIDR e DMZ VPC CIDR, além de VPC CIDR fornecido pelo cliente CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
Bastiões de 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

Criar, alterar ou excluir grupos de segurança

Você pode solicitar grupos de segurança personalizados. Nos casos em que os grupos de segurança padrão não atendam às necessidades dos seus aplicativos ou da sua organização, você pode modificar ou criar novos grupos de segurança. Essa solicitação seria considerada necessária para aprovação e seria analisada pela equipe de operações da AMS.

Para criar um grupo de segurança fora das pilhas e VPCs enviar uma RFC usando o tipo de `Deployment | Advanced stack components | Security group | Create (review required)` alteração (ct-1oxx2g2d7hc90).

Para modificações no grupo de segurança do Active Directory (AD), use os seguintes tipos de alteração:

- Para adicionar um usuário: Envie um RFC usando Management | Directory Service | Usuários e grupos | Adicionar usuário ao grupo [ct-24pi85mjtza8k]
- Para remover um usuário: envie um RFC usando Management | Directory Service | Usuários e grupos | Remover usuário do grupo [ct-2019s9y3nfml4]

> **Note**
>
> Ao usar “revisão obrigatória” CTs, o AMS recomenda que você use a opção ASAP Scheduling (escolha ASAP no console, deixe a hora de início e término em branco na API/CLI), pois isso CTs exige que um operador do AMS examine a RFC e, possivelmente, se comunique com você antes que ela possa ser aprovada e executada. Se você agendá-los RFCs, aguarde pelo menos 24 horas. Se a aprovação não ocorrer antes do horário de início programado, a RFC será rejeitada automaticamente.

Encontre grupos de segurança

Para encontrar os grupos de segurança anexados a uma pilha ou instância, use o EC2 console. Depois de encontrar a pilha ou instância, você pode ver todos os grupos de segurança anexados a ela.

Para saber como encontrar grupos de segurança na linha de comando e filtrar a saída, consulte `describe-security-groups`.

EC2 Perfil de instância do IAM

Um perfil de instância é um contêiner para uma função do IAM que você pode usar para passar informações da função para uma EC2 instância quando a instância é iniciada.

MALZ

Há dois perfis de instância padrão do AMS `customer-mc-ec2-instance-profile` `customer-mc-ec2-instance-profile-s3` e. Esses perfis de instância fornecem as permissões descritas na tabela a seguir.

Descrições de políticas

Perfil	Políticas
`customer-mc-ec2-instance-profile`	`AmazonSSMManagedInstanceCore` : permite que as instâncias do Ec2 usem o agente SSM.
	`AMSInstanceProfileLoggingPolicy` : permite que instâncias do Ec2 enviem registros para o S3 e. CloudWatch

Perfil	Políticas
	`AMSInstanceProfileManagementPolicy` : permite que as instâncias do Ec2 executem ações de inicialização, como ingressar no Active Directory.
	`AMSInstanceProfileMonitoringPolicy` : permite que as instâncias do Ec2 relatem as descobertas aos serviços de monitoramento do AMS.
	`AMSInstanceProfilePatchPolicy` : permite que as instâncias do Ec2 recebam patches.
`customer-mc-ec2-instance-profile-s3`	`AMSInstanceProfileBYOEPSPolicy` : permite que as instâncias do Ec2 usem o AMS e tragam seu próprio EPS.
	`AMSInstanceProfileLoggingPolicy` : permite que instâncias do Ec2 enviem registros para o S3 e. CloudWatch
	`AMSInstanceProfileManagementPolicy` : permite que as instâncias do Ec2 executem ações de inicialização, como ingressar no Active Directory.
	`AMSInstanceProfileMonitoringPolicy` : permite que as instâncias do Ec2 relatem as descobertas aos serviços de monitoramento do AMS.
	`AMSInstanceProfilePatchPolicy` : permite que as instâncias do Ec2 recebam patches.
	`AMSInstanceProfileS3WritePolicy` : permite que instâncias Ec2 cheguem read/write aos buckets S3 do cliente.

SALZ

Há um perfil de instância padrão do AMS,`customer-mc-ec2-instance-profile`, que concede permissões da política de instância do IAM`customer_ec2_instance_profile_policy`. Esse perfil de instância fornece as permissões descritas na tabela a seguir. O perfil concede permissões aos aplicativos em execução na instância, não aos usuários que fazem login na instância.

As políticas geralmente incluem várias declarações, em que cada declaração concede permissões a um conjunto diferente de recursos ou concede permissões sob uma condição específica.

CW = CloudWatch. ARN = Nome do recurso da Amazon. * = curinga (qualquer).

EC2 permissões padrão de perfil de instância do IAM

CW = CloudWatch. ARN = Nome do recurso da Amazon. * = curinga (qualquer).			
Declaração da política	Efeito	Ações	Descrição e recurso (ARN)
Nuvem de computação elástica da Amazon (Amazon EC2)			
EC2 Ações de mensagem	Permitir	AcknowledgeMessage, DeleteMessage, FailMessage, GetEndpoint, GetMessages, SendReply	Permite ações de mensagens do EC2 Systems Manager em sua conta.
Ec2 Descrever	Permitir	* (Tudo)	Permite que o console exiba detalhes de configuração de um EC2 em sua conta.
Iam Get Role ID	Permitir	GetRole	Permite EC2 obter seu ID do IAM de `aws:iam::*:role/`

CW = CloudWatch. ARN = Nome do recurso da Amazon. * = curinga (qualquer).			
Declaração da política	Efeito	Ações	Descrição e recurso (ARN)
			`customer-* aws:iam::*:role/customer_*` e.
Instância para fazer upload de eventos de log	Permitir	Criar grupo de registros	Permite que os registros sejam criados em: `aws:logs:*:*:log-group:i-*`
		Criar fluxo de log	Permite que os registros sejam transmitidos para: `aws:logs:*:*:log-group:i-*`
CW para MMS	Permitir	DescribeAlarms, PutMetricAlarm, PutMetricData	Permite CloudWatch recuperar alarmes em sua conta. Permite que o CW crie ou atualize um alarme e o associe à métrica especificada. Permite que o CW publique pontos de dados métricos em sua conta.
Etiquetas Ec2	Permitir	CreateTags, DescribeTags,	Permite que as tags sejam adicionadas, substituídas e descritas nas instâncias especific adas em sua conta.
Negar explicita mente os registros do CW	Deny	DescribeLogStreams, FilterLogEvents, GetLogEvents	Não permite listar, filtrar ou obter os fluxos de log para: `aws:logs:*:*:log-group:/mc/*`
Amazon EC2 Simple Systems Manager (SSM)			

CW = CloudWatch. ARN = Nome do recurso da Amazon. * = curinga (qualquer).			
Declaração da política	Efeito	Ações	Descrição e recurso (ARN)
Ações do SSM	Permitir	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	Permite uma variedade de funções de SSM em sua conta.
Acesso SSM no S3	Permitir	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadPorts, ListBucketMultipartUploads	Permite que o SSM no EC2 obtenha e atualize objetos, aborte o upload de um objeto de várias partes e liste portas e compartimentos disponíveis para carregamentos de várias partes. `aws:s3:::mc-*-internal-*/aws/ssm*`
Amazon EC2 Simple Storage Service (S3)			
Obter objeto no S3	Permitir	Obtenção Lista	Permite que os EC2 aplicativos recuperem e listem objetos nos buckets do S3 em sua conta.
Acesso ao log criptografado do cliente S3	Permitir	PutObject	Permite que os EC2 aplicativos atualizem objetos no `aws:s3:::mc-*-logs-*/encrypted/app/*`

CW = CloudWatch. ARN = Nome do recurso da Amazon. * = curinga (qualquer).			
Declaração da política	Efeito	Ações	Descrição e recurso (ARN)
Patch Data Put Object S3	Permitir	PutObject	Permite que EC2 os aplicativos carreguem dados de patches para seus buckets do S3 em `aws:s3:::awsms-a*-patch-data-*`
Carregando seus próprios registros para o S3	Permitir	PutObject	Permite que os EC2 aplicativos carreguem registros personalizados para: `aws:s3:::mc-a*-logs-*/aws/instances/*/${aws:userid}/*`
Negar explicitamente os registros do MC Namespace S3	Deny	GetObject* Coloque*	Não permite que EC2 aplicativos obtenham ou coloquem objetos de ou para: `aws:s3:::mc-*-logs-*/encrypted/mc*` , `aws:s3:::mc-*-logs-*/mc/*`, `aws:s3:::mc-a*-logs-*-audit/*`
Negar explicitamente a exclusão do S3	Deny	* (tudo)	Não permite que EC2 aplicativos realizem qualquer ação em objetos em: `aws:s3:::mc-a*-logs-*/*` , `aws:s3:::mc-a*-internal-*/*` ,

CW = CloudWatch. ARN = Nome do recurso da Amazon. * = curinga (qualquer).			
Declaração da política	Efeito	Ações	Descrição e recurso (ARN)
Negar explicitamente o bucket CFN do S3	Deny	Delete*	Não permite que EC2 aplicativos excluam objetos de: `aws:s3:::cf-templates-*`
Negar explicitamente o List Bucket S3	Deny	ListBucket	Não permite que você liste objetos criptografados, de registro de auditoria ou reservados (mc) de: `aws:s3:::mc-*-logs-*`
AWS Secrets Manager na Amazon EC2			

CW = CloudWatch. ARN = Nome do recurso da Amazon. * = curinga (qualquer).			
Declaração da política	Efeito	Ações	Descrição e recurso (ARN)
Acesso aos segredos do Trend Cloud One	Permitir	GetSecretValue	Permite que EC2 a Amazon acesse segredos para a migração do 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 na Amazon EC2			
Chave de decodificação Trend Cloud One	Permitir	Decrypt	Permita que EC2 a Amazon decifre a AWS KMS chave com o nome de alias/-migration ams/eps/cloudone `arn:aws:kms:*:*:alias/ams/eps/cloudone-migration`

Se você não estiver familiarizado com as políticas do Amazon IAM, consulte Visão geral das políticas do IAM para obter informações importantes.

> **Note**
>
> As políticas geralmente incluem várias declarações, em que cada declaração concede permissões a um conjunto diferente de recursos ou concede permissões sob uma condição específica.

Padrões de métricas monitoradas

A tabela a seguir mostra o que é monitorado e os limites de alerta padrão. Você pode alterar os padrões com uma solicitação de mudança (RFC) de gerenciamento de alterações.

> **Note**
>
> CloudWatch lançou a retenção estendida de métricas em 1º de novembro de 2016. Para obter mais informações, consulte CloudWatch Limites.

Alertas do monitoramento de linha de base

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
Para alertas com estrela (*), o AMS avalia proativamente o impacto e corrige quando possível; se a remediação não for possível, o AMS cria um incidente. Quando a automação falha em corrigir o problema, o AMS informa você sobre o caso do incidente e um engenheiro do AMS é contratado. Além disso, esses alertas podem ser enviados diretamente para seu e-mail (se você tiver optado pelo tópico Direct-Customer-Alerts SNS).			
Instância do Application Load Balancer (ALB)	Não	RejectedConnectionCount soma > 0 por 1 min, 5 vezes consecutivas.	CloudWatch alarme se o número de conexões que foram rejeitadas porque o balanceador de carga atingiu seu máximo.

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
Destino do Application Load Balancer (ALB)	Não	TargetConnectionErrorCount soma > 0 por 1 min, 5 vezes consecutivas.	CloudWatch alarme se o número de conexões foi estabelecido sem sucesso entre o balanceador de carga e as instâncias registradas.
EC2 Instância da Amazon — Windows	Não	SecureChannelFailure > 0,0 para 10 dos últimos 15 pontos de dados.	CloudWatch alarme em instâncias do Windows para alertar quando a conexão Secure a Channel falhar.
Instância do Aurora	Não	CPUUtilization > 85% por 5 minutos, 2 vezes consecutivas.	CloudWatch alarme.
AWS Backup	Sim	DeleteRecoveryPoint Um principal de função do IAM inesperado ou um principal de usuário do IAM excluiu um ponto AWS Backup de recuperação.	CloudWatch evento. Emitido quando um ponto de recuperação de backup é excluído.
AWS Outposts	Sim	AMSOutpostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 80% por 5 minutos, 12 vezes consecutivas.	CloudWatch alarme sobre a disponibilidade da capacidade familiar de instâncias do AWS Outposts recurso.

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
EC2 instância - tudo OSs	Não	AMSOutpostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80% por 5 minutos, 12 vezes consecutivas.	CloudWatch alarme sobre a disponibilidade da capacidade e do tipo de instância do AWS Outposts recurso.
		AMSOutpostsConnectedStatusConnectedStatus < 1 por 5 minutos, 1 vez consecutiva.	CloudWatch alarme na conexão do link de AWS Outposts serviço, menos de 1 contagem está prejudicada.
		AMSOutpostsCapacityExceptionCapacityExceptions 0 por 5 minutos, 1 vez consecutiva.	CloudWatch alarme sobre erros de capacidade insuficiente, por exemplo, lançamentos AWS Outposts de um recurso .
		CPUUtilization* >= 95% por 5 minutos, 6 vezes consecutivas.	CloudWatch alarme. A alta utilização da CPU é um indicador de uma mudança no estado do aplicativo, como bloqueios sem saída, loops infinitos, ataques maliciosos e outras anomalias.
		StatusCheckFailed > 0 por 5 minutos, 3 vezes consecutivas.	CloudWatch alarme.
		Uso do volume raiz >= 95% por 5 minutos, 6 vezes consecutivas.	

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
		Uso do volume não raiz > 85% por 5 minutos, 2 vezes consecutivas. Desativado por padrão; para obter informações adicionais, consulte https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info.	
		Sem memória* MemoryFree < 5% por 5 minutos, 6 vezes consecutivas.	
	Sim	Malware EPS Malware encontrado na instância.	CloudWatch evento.
EC2 Instância da Amazon - Linux	Não	Uso do Inode do Volume Raiz Média >= 95% por 5 minutos, 6 vezes consecutivas.	CloudWatch alarme. Aplicado somente às instâncias do Linux.
		Grátis para troca* Troca de memória < 5% por 5 minutos, 6 vezes consecutivas.	

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
ElastiCache Cluster	Não	CurrConnections = 65000	Esse alarme notifica o AMS do limite máximo de conexão de um ElastiCache Host. CloudWatch Alarme. Se você quiser atualizar esse limite, entre em contato com o suporte do AMS.

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
ElastiCache Nodo	Não	CPUUtilization Média > valor predefinido por 15 minutos, 2 vezes consecutivas.	CloudWatch alarme. O padrão é 90. Se for Redis, use um dos seguintes valores com base no tipo de instância: • 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%

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
ElastiCache Node - memcached	Não	SwapUsage máximo > 50.000.000 bytes por 5 minutos, 5 vezes consecutivas.	CloudWatch alarme. Aplicado somente ao memcached.
OpenSearch agrupamento	Não	ClusterStatus.red o máximo é >= 1 por 1 minuto, 1 vez consecutiva. O AMS toma medidas proativas para reduzir o impacto operacional quando esse alerta é acionado.	CloudWatch alarme. Pelo menos um fragmento principal e suas réplicas não estão alocados para um nó. Para saber mais, consulte Red Cluster Status.
OpenSearch Domínio	Não	KMSKeyErro >= 1 por 1 minuto, 1 vez consecutiva.	CloudWatch alarme. A chave de criptografia do KMS que é usada para criptografar dados em repouso no seu domínio está desativada. Reative-a para restaurar as operações normais. Para saber mais, consulte Criptografia de dados em repouso para o OpenSearch Service Service.
		ClusterStatus.amarelo máximo é >= 1 por 1 minuto, 1 vez consecutiva O AMS toma medidas proativas para reduzir o impacto operacional quando esse alerta é acionado.	Pelo menos um fragmento de réplica não está alocado para um nó. Para saber mais, consulte Yellow Cluster Status.

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
		FreeStorageSpace o mínimo é <= 20480 por 1 minuto, 1 vez consecutiva O AMS toma medidas proativas para reduzir o impacto operacional quando esse alerta é acionado.	Um nó no seu cluster tem 20 GiB de espaço de armazenamento livre. Para saber mais, consulte Falta de espaço de armazenamento disponível.
		ClusterIndexWritesBlocked >= 1 por 5 minutos, 1 vez consecutiva O AMS toma medidas proativas para reduzir o impacto operacional quando esse alerta é acionado.	O cluster está bloqueando as solicitações de gravação. Para saber mais, consulte ClusterBlockException.
		Nós mínimo é < x por 1 dia, 1 vez consecutiva O AMS toma medidas proativas para reduzir o impacto operacional quando esse alerta é acionado.	x é o número de nós em seu cluster. Esse alarme indica que pelo menos um nó no cluster permaneceu inacessível por um dia. Para saber mais, consulte Failed Cluster Nodes.
		CPUUtilization a média é >= 80% por 15 minutos, 3 vezes consecutivas O AMS toma medidas proativas para reduzir o impacto operacional quando esse alerta é acionado.	A utilização de 100% da CPU é comum, mas altas médias sustentadas são problemáticas. Considere o uso de tipos de instância maiores ou a adição de instâncias.

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
		JVMMemoryPressão o máximo é >= 80% por 5 minutos, 3 vezes consecutivas O AMS toma medidas proativas para reduzir o impacto operacional quando esse alerta é acionado.	O cluster poderá apresentar erros de memória insuficiente se o uso aumentar. Considere a escalabilidade vertical. O Amazon ES usa metade da RAM de uma instância para o heap Java, até um tamanho de heap de 32 GiB. Você pode dimensionar instâncias verticalm ente até 64 GiB de RAM, sendo que nesse ponto você poderá dimensionar horizontalmente adicionando instâncias.
		Dominar CPUUtilization a média é >= 50% por 15 minutos, 3 vezes consecutivas O AMS toma medidas proativas para reduzir o impacto operacional quando esse alerta é acionado.	Considere usar tipos de instância maiores para seus nós principais dedicados. Devido à sua função na estabilidade e nas blue/gree n implantações do cluster, os nós mestres dedicados devem ter uma média de uso de CPU menor do que os nós de dados.
		JVMMemoryPressão principal o máximo é >= 80% por 15 minutos, 1 vez consecutiva O AMS toma medidas proativas para reduzir o impacto operacional quando esse alerta é acionado.	Considere usar tipos de instância maiores para seus nós principais dedicados. Devido à sua função na estabilidade e nas blue/gree n implantações do cluster, os nós mestres dedicados devem ter uma média de uso de CPU menor do que os nós de dados.

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
OpenSearch instância	Não	AutomatedSnapshotFailure o máximo é >= 1 por 1 minuto, 1 vez consecutiva.	CloudWatch alarme. Ocorreu falha em um snapshot automatizado. Essa falha normalmente é o resultado de um status de integridade vermelho do cluster. Consulte o status do cluster vermelho.
Instância do Elastic Load Balancing	Não	SurgeQueueLength > 100 por 1 minuto, 15 vezes consecutivas.	CloudWatch alarme se um número excessivo de solicitações estiver pendente de roteamento.
		HTTPCode_ELB_5xx_Contagem soma > 0 por 5 min, 3 vezes consecutivas.	CloudWatch alarme sobre o número excessivo de códigos de resposta HTTP 5XX que se originam do balanceador de carga.
		SpilloverCount > 1 por 1 minuto, 15 vezes consecutivas.	CloudWatch alarme se houver um número excessivo de solicitações rejeitadas porque a fila de sobrecarga está cheia.
GuardDuty serviço	Sim	Não aplicável; todas as descobertas (propósitos de ameaça) são monitoradas. Cada descoberta corresponde a um alerta. Mudanças nas GuardDuty descobertas. Essas alterações incluem descobertas recém-geradas ou as ocorrências subsequentes das descobertas existentes.	A lista dos tipos de GuardDuty descoberta compatíveis está em Tipos de descoberta GuardDuty ativos.

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
Saúde	Varia	AWS Health Dashboard	As notificações são enviadas quando há alterações no status dos eventos AWS Health Dashboard (AWS Health) em relação aos serviços básicos suportados pelo AMS. Para obter mais informações, consulte Serviços compatíveis.
AWS Managed Microsoft AD	Não	Status do Active Directory AWS Managed Microsoft AD instance envia um evento de status ativo.	Evento de serviço. Emitido quando o diretório está operando normalmente após um evento.
		Status do diretório prejudicado AWS Managed Microsoft AD instance envia um evento de status de diretório danificado.	Evento de serviço. Emitido quando o diretório está sendo executado em um estado degradado. Um ou mais problemas foram detectados, e talvez algumas operações do diretório não estejam funcionan do com capacidade operacional total.
		Status do diretório inoperável AWS Managed Microsoft AD instance envia um evento de status inoperável.	Evento de serviço. Emitido quando o diretório não está funcionando. Todos os endpoints do diretório relataram problemas.

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
		Excluindo o status do diretório AWS Managed Microsoft AD instance envia um evento de exclusão do status do diretório.	Evento de serviço. Emitido quando o diretório está sendo excluído no momento.
		Status do diretório com falha AWS Managed Microsoft AD a instância envia um evento de status com falha.	Evento de serviço. Emitido quando o diretório não pôde ser criado.
		RestoreFailed Status do diretório AWS Managed Microsoft AD a instância envia um evento de status do diretório com falha na restauraç ão.	Evento de serviço. Emitido ao restaurar o diretório a partir de um instantâneo falhou.
Instância do Amazon RDS	Não	O alerta de baixo armazenamento é acionado quando o armazenamento alocado para a instância de banco de dados se esgota.	RDS-EVENT-0007, veja detalhes em Usando a notificação de eventos do Amazon RDS.
		falha na instância de banco de dados Houve falha na instância de banco de dados devido a uma configura ção incompatível ou a um problema do armazenamento subjacente. Comece a point-in-time-restore para a instância de banco de dados.	Evento de serviço. RDS-EVENT -0031, categorias de eventos e mensagens de eventos do Amazon RDS.

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
		Failover não foi tentado O Amazon RDS não está tentando um failover solicitado porque ocorreu um failover recentemente na instância de banco de dados.	Evento de serviço. RDS-EVENT -0034, categorias de eventos e mensagens de eventos do Amazon RDS.
		Parâmetros inválidos da instância de banco de dados Por exemplo, o MySQL não pôde ser iniciado porque um parâmetro relacionado à memória está definido como alto demais para essa classe de instância, então a ação do cliente seria modificar o parâmetro de memória e reinicializar a instância de banco de dados.	Evento de serviço. RDS-EVENT -0035, categorias de eventos e mensagens de eventos do Amazon RDS.
		Instância de banco de dados de sub-rede IDs inválida A instância de banco de dados está em uma rede incompatível. Algumas das sub-redes especificadas IDs são inválidas ou não existem.	Evento de serviço. RDS-EVENT -0036, Categorias de eventos e mensagens de eventos do Amazon RDS.

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
		Erro de réplica de leitura da instância de banco de dados Ocorreu um erro no processo de replicação de leitura. Para ter mais informações, consulte a mensagem do evento. Para obter informaçõ es sobre como solucionar erros de réplica de leitura, consulte Solução de problemas de réplica de leitura do MySQL.	Evento de serviço. RDS-EVENT -0045, categorias de eventos e mensagens de eventos do Amazon RDS.
		A replicação de leitura da instância de banco de dados terminou A replicação na réplica de leitura foi encerrada.	Evento de serviço. RDS-EVENT -0057, categorias de eventos e mensagens de eventos do Amazon RDS.
		Erro ao criar conta de usuário do statspack Erro ao criar a conta de usuário do Statspack PERFSTAT. Descarte a conta antes de adicionar a opção Statspack.	Evento de serviço. RDS-EVENT -0058, categorias de eventos e mensagens de eventos do Amazon RDS.

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
		Início da recuperação da instância de banco de dados A instância de banco de dados do SQL Server está restabele cendo seu espelho. O performan ce será degradado até o espelho ser restabelecido. Um banco de dados foi encontrado com o modelo de recuperação não FULL. O modelo de recuperação foi alterado novamente para FULL e a recuperaç ão por espelhamento foi iniciada. (<dbname>: <recovery model found>[,...]).	Evento de serviço. RDS-EVENT -0066, categorias de eventos e mensagens de eventos do Amazon RDS.
		Um failover para o cluster de banco de dados falhou.	RDS-EVENT-0069, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
		Bucket S3 de recuperação de permissões inválidas O perfil do IAM que você usa para acessar seu bucket do Amazon S3 para backup e restauração nativos do SQL Server está configurado incorretamente. Para obter mais informações, consulte Configurando o Backup e a Restauração Nativos.	Evento de serviço. RDS-EVENT -0081, categorias de eventos e mensagens de eventos do Amazon RDS.

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
		O Aurora não pôde copiar dados de backup de um bucket do Amazon S3.	RDS-EVENT-0082, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
		Alerta de baixo armazenamento quando a instância de banco de dados consumiu mais de 90% de seu armazenamento alocado	RDS-EVENT-0089, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
		Serviço de notificação quando o escalonamento falhou para o cluster de banco de dados Aurora Serverless.	RDS-EVENT-0143, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
		A instância de banco de dados está em estado inválido. Nenhuma ação é necessária. A escalabilidade automática tentará novamente mais tarde.	RDS-EVENT-0219, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
		A instância de banco de dados atingiu o limite total de armazenamento e o banco de dados foi encerrado.	RDS-EVENT-0221, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
		Esse evento indica que o escalonamento automático do armazenamento da instância do RDS não pode ser escalado. Pode haver vários motivos pelos quais o escalonamento automático falhou.	RDS-EVENT-0223, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
		A escalabilidade automática do armazenamento acionou uma tarefa de armazenamento de escala pendente que atingiu o limite máximo de armazenamento.	RDS-EVENT-0224, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
		A instância de banco de dados tem um tipo de armazenamento que no momento está indisponível na zona de disponibilidade. A escalabilidade automática tentará novamente mais tarde.	RDS-EVENT-0237, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
		O RDS não conseguiu provisionar capacidade para o proxy porque não há endereços IP suficientes disponíveis em suas sub-redes.	RDS-EVENT-0243, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
		O armazenamento da sua conta da AWS excedeu a cota de armazenamento permitida.	RDS-EVENT-0254, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
		CPUUtilization Utilização média da CPU > 90% por 15 minutos, 2 vezes consecutivas.	CloudWatch alarme.
		DiskQueueDepth A soma é > 75 por 1 minuto, 15 vezes consecutivas.	

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
		FreeStorageSpace Média < 1.073.741.824 bytes por 5 minutos, 2 vezes consecutivas.	
		SwapUsage Média >= 104.857.600 bytes por 5 minutos, 2 vezes consecutivas.	
Cluster do Amazon Redshift	Não	RedshiftClusterStatus A integridade do cluster quando não está no modo de manutenção < 1 por 5 min.	1 representa um cluster saudável.
Amazon Macie	Sim	Alertas recém-gerados e atualizaç ões de alertas existentes. Macie encontra alguma mudança nas descobertas. Essas alterações incluem descobertas recém-geradas ou as ocorrências subsequentes das descobertas existentes.	Alerta do Amazon Macie. Para obter uma lista dos tipos de alerta do Macie compatíve is, consulte Analisando as descobertas do Amazon Macie. Observe que o Macie não está habilitado para todas as contas.

Padrões de retenção e rotação de registros

Esta seção descreve os padrões de gerenciamento de registros do AMS; para obter mais informações, consulte Gerenciamento de registros.

- Rotação = rotatividade de registros dentro das instâncias
- Retenção = Período de tempo em que mantemos os registros no Amazon CloudWatch Logs e no Amazon Simple Storage Service (S3)

Os registros são mantidos em CloudWatch Registros conforme necessário (você pode configurar isso) e no S3. Eles não expiram nem são excluídos e estão sujeitos à durabilidade do serviço. Para obter informações detalhadas sobre a durabilidade do S3, consulte Proteção de dados no Amazon S3.

Você pode solicitar uma alteração na retenção de registros para todos os registros, exceto os AWS CloudTrail registros, que são mantidos indefinidamente por motivos de auditoria e segurança.

A rotação de registros é configurada dentro das instâncias. Por padrão, os registros do sistema operacional e de segurança alternam de hora em hora se atingirem mais de 100 MB. Isso é feito para garantir que você não fique sem disco nas instâncias.

O agente de log dentro das instâncias carrega o log on-line para o CloudWatch Logs. A partir daí, os registros são arquivados no S3.

Os registros são armazenados no CloudWatch Logs e no S3 no formato bruto em que são gerados, sem pré-processamento.

Padrões de gerenciamento de continuidade

Esta seção descreve os padrões de gerenciamento de continuidade do AMS; para obter mais informações sobre backups do AMS, consulte o capítulo Gerenciamento de Continuidade do Guia do Usuário do AMS.

A configuração do backup é feita no momento da integração. Essas são as configurações de backup padrão (recomendadas).

Tag e padrões de VPC

Para obter as informações mais atuais sobre o backup do AMS, consulte Gerenciamento de continuidade.

> **Important**
>
> Por padrão, os backups em EC2 pilha estão desativados (Backup = False). Você pode ativar os backups da EC2 instância no momento da criação adicionando uma tag `Key: Backup, Value: True` ao solicitar uma EC2 pilha por meio de uma RFC (CT ct-14027q0sjyt1h). Se você quiser adicionar a tag após a criação da instância, envie uma RFC com Gerenciamento | Componentes avançados da pilha | pilha de EC2 instâncias | Atualizar CT (ct-38s4s4tm4ic4u).

EC2 tag e padrões da instância

A tag de backup da EC2 pilha especifica se a pilha exige ou não um snapshot dos volumes do EBS conectados.

Etiqueta `Key: Backup`

Etiqueta `Value: True, False`

Por padrão, o valor é que `False` a tag de backup não está presente e a pilha não tem backups agendados.

Altere a tag `Key: Backup` `Value: True` para ativar os backups, que são feitos de acordo com o cronograma definido com a tag de backup da VPC.

> **Note**
>
> As letras maiúsculas e minúsculas do valor da tag (somente valor) são insensíveis, portanto, True/true ou False/false são todas aceitáveis.

Backup e padrões da instância RDS

Os valores padrão do Amazon Relational Database Service (RDS) do Amazon Relational Database Service (RDS) são definidos nos modelos de pilha:

```
Backup: Yes

Backup Window: 22:00-23:00 (RDS local time zone)

Retention Period: 7 (7 snapshots stored)
```

Padrões de correção

Esta seção descreve os padrões de patches do AMS; para obter mais informações sobre os patches do AMS, consulte o capítulo Gerenciamento de patches do Guia do Usuário do AMS.

As versões do AMS são corrigidas AMIs mensalmente; todas as novas solicitações de pilha devem ser configuradas com a AMI mais recente do AMS.

> **Important**
>
> O AMS Patch Orchestrator, aplicação de patches baseada em tags, usa a funcionalidade do AWS Systems Manager (SSM) para permitir que você marque ou faça com que o AMS marque suas instâncias e faça com que essas instâncias sejam corrigidas usando uma linha de base e uma janela que você configura. Para saber mais, consulte Patch Orchestrator: um modelo de patch baseado em tags.

Correção padrão da AMS, baseada em contas: para cada conta com pilhas que recebem patches no local, uma notificação dos próximos patches aplicáveis é enviada logo após a “terça-feira de patches”. A notificação contém uma lista de todas as pilhas e os patches aplicáveis, bem como a janela de patch sugerida. Para patches críticos, a janela é definida com no máximo 10 dias de antecedência e, para patches padrão, com no máximo 14 dias de antecedência. Se você não responder à notificação, a correção não ocorrerá. Se você quiser excluir determinados patches, responda à notificação ou envie uma solicitação de serviço. Se você responder com consentimento à aplicação de patches, mas não solicitar especificamente um cronograma diferente, os patches serão aplicados conforme descrito na notificação que você recebe.

> **Note**
>
> A notificação do serviço de patch é um e-mail enviado aos contatos da conta e contém um link para o console do AWS Support. Você pode responder por meio do console do AWS Support ou da página de solicitação de serviço do AMS, onde a notificação aparece como uma notificação de serviço.

No momento do processo de aplicação de patches padrão da AMS, o AMS executa o seguinte:

1. Você recebe uma notificação do serviço de patches quatorze dias antes da janela de patch proposta. A notificação do serviço de patches é enviada por e-mail para o endereço de e-mail de contato que você registrou em sua conta.
2. Identifica todas as EC2 instâncias acessíveis na pilha com base na lista de pilhas fornecida na notificação de patch. Nesse caso, “Acessível” significa instâncias que estão no EC2 estado “Em execução” e têm o agente EC2 Run Command totalmente operacional.

3. O AMS executa a aplicação de patches de forma a garantir que um número suficiente de EC2 instâncias esteja sendo executado simultaneamente (configurado por meio da `healthy-host-threshold` configuração) para que a pilha permaneça íntegra.
4. Depois que a operação de correção for concluída para todas as EC2 instâncias, o AMS atualiza a RFC com o status da correção: Sucesso, Sucesso parcial ou Falha. No caso de qualquer status diferente de Sucesso, um ticket é criado para que um operador acompanhe os resultados da correção e tome quaisquer ações corretivas.

Validar o serviço AMS (SALZ)

Para validar se o serviço AWS Managed Services (AMS) está funcionando conforme o esperado, alguns exercícios que você pode fazer estão descritos neste capítulo.

Encontre as configurações da conta AMS

Configurações da conta que são usadas para criar AMS RFCs, definir horários e determinar quem recebe notificações.

Algumas configurações são criadas durante a integração e exigem uma solicitação de serviço para serem alteradas. Você deve anotar esses detalhes da conta porque você os usará ao se comunicar com o AMS:

- Credenciais: Se você precisar recuperar seu nome de usuário ou senha do AMS, entre em contato com o administrador de TI local. O AMS usa o Active Directory corporativo.
- Cloud Service Delivery Manager (CSDM): Essa pessoa é sua ligação com o AMS e está disponível para responder perguntas sobre serviços. Você recebe as informações de contato dessa pessoa no momento da integração e deve mantê-las disponíveis para todos em sua organização que interagem com o AMS. Você pode esperar receber relatórios mensais sobre seu serviço AMS dessa pessoa.
- Acesso ao console: você acessa o console do AMS em uma URL configurada especificamente para sua conta. Você pode obter o URL do seu CSDM.
- CLI do AMS: você pode obter a CLI do AMS por meio da página de recursos do desenvolvedor do console do AMS ou do pacote de distribuíveis que você obtém do seu CSDM. Depois de ter o pacote de distribuíveis, siga as etapas descritas em Instalação ou atualização da CLI do AMS.
- Janela de manutenção: sua janela de manutenção determina quando a correção ocorre para suas EC2 instâncias. A janela de manutenção do AWS Managed Services (ou janela de manutenção)

realiza atividades de manutenção para o AWS Managed Services (AMS) e ocorre na segunda quinta-feira de cada mês, das 15h às 16h, horário do Pacífico. O AMS pode alterar a janela de manutenção com 48 horas de antecedência. Você pode ter escolhido uma janela diferente na integração. Mantenha um registro da janela de manutenção escolhida.

- Monitoramento: o AMS fornece um conjunto de CloudWatch métricas por padrão, mas você também pode solicitar métricas adicionais. Se você fizer isso, mantenha um registro deles.
- Registros: por padrão, seus registros são armazenados em ams-a- *ACCOUNT_ID* -log-management-, *REGION* onde *REGION* é a região em que o registro foi gerado.
- Mitigação: na integração, o AMS registra a ação de mitigação de sua escolha, caso seja identificado um ataque de malware contra seus recursos. Por exemplo, entre em contato com certas pessoas. Mantenha essas informações disponíveis para todos em sua organização que interagem com o AMS.
- Região: você pode ver a página de detalhes da VPC no console do AMS. Você também pode executar esse comando depois de instalar a CLI do AMS SKMS (esse comando usa um perfil SAML, remova se o método de autenticação for diferente):

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

Important

Note

Os endpoints AMS API/CLI (amscm e amsskms) estão na região da AWS Norte da Virgínia,. `us-east-1` Dependendo de como sua autenticação está configurada e em qual região da AWS sua conta e seus recursos estão, talvez seja necessário adicioná-la `--region us-east-1` ao emitir comandos. Talvez você também precise adicionar`--profile saml`, se esse for o seu método de autenticação.

Encontre FQDNs no AMS

Os tipos de alteração de acesso () do AWS Managed Services (AMSCTs) exigem o nome de domínio totalmente qualificado, ou FQDN, do seu domínio confiável da AMS, na forma de. `C844273800838.amazonaws.com` Para descobrir seu AWS FQDN, faça o seguinte:

- Console AWS: veja o console do AWS Directory Service na coluna Nome do diretório.
- CLI: Use esses comandos enquanto estiver conectado ao seu domínio:

  Windows (retorna o usuário e o FQDN):

```
whoami /upn
```

  ou (DC+DC+DC=FQDN)

```
whoami /fqdn
```

  Linux

```
hostname --fqdn
```

> **Note**
>
> Os endpoints AMS API/CLI (amscm e amsskms) estão na região da AWS Norte da Virgínia,. `us-east-1` Dependendo de como sua autenticação está configurada e em qual região da AWS sua conta e seus recursos estão, talvez seja necessário adicioná-la `--region us-east-1` ao emitir comandos. Talvez você também precise adicionar`--profile saml`, se esse for o seu método de autenticação.

Encontre zonas de disponibilidade (AZs) no AMS

Zona de disponibilidade: todas as contas têm pelo menos duas zonas de disponibilidade. Para encontrar com precisão os nomes das zonas de disponibilidade, você deve primeiro saber a ID da sub-rede associada.

- Console AMS: no painel de navegação VPCs, clique em e, em seguida, clique na VPC relevante, se necessário. Na página de VPCs detalhes, selecione a sub-rede relevante na tabela de sub-redes para abrir a página de detalhes da sub-rede com o nome da zona de disponibilidade associada.
- API/CLI DO AMS SIMS:

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

> **Note**
>
> Os endpoints AMS API/CLI (amscm e amsskms) estão na região da AWS Norte da Virgínia,. `us-east-1` Dependendo de como sua autenticação está configurada e em qual região da AWS sua conta e seus recursos estão, talvez seja necessário adicioná-la `--region us-east-1` ao emitir comandos. Talvez você também precise adicionar`--profile saml`, se esse for o seu método de autenticação.

Encontre tópicos do SNS no AMS

Seus tópicos do SNS determinam quem é notificado em várias circunstâncias. O AMS fornece tópicos de SNS para notificações de AMI (consulte Notificações de AMI do AMS com SNS), CloudWatch alarmes e EC2 recursos (consulte Recebimento de alertas gerados pelo AMS) e muito mais. Para descobrir seus tópicos existentes do SNS:

- Console AWS: use o console do SNS para visualizar todos os tópicos, aplicativos e assinaturas, além de um gráfico de mensagens. Além disso, crie, exclua, assine e publique em tópicos.
- API/CLI (quando conectado à sua conta do AMS, requer o AWS CLI):

  Liste seus tópicos do SNS:

  ```
  aws sns list-topics
  ```

  Liste suas assinaturas do SNS:

  ```
  aws sns list-subscriptions
  ```

> **Note**
>
> Os endpoints AMS API/CLI (amscm e amsskms) estão na região da AWS Norte da Virgínia,. `us-east-1` Dependendo de como sua autenticação está configurada e em qual região da AWS sua conta e seus recursos estão, talvez seja necessário adicioná-la `--region us-east-1` ao emitir comandos. Talvez você também precise adicionar`--profile saml`, se esse for o seu método de autenticação.

Encontre configurações de backup no AMS

Os backups e instantâneos são gerenciados pelo AMS por meio do AWS Backupserviço nativo.

A configuração é gerenciada por meio AWS Backup de planos. Você pode ter vários AWS Backup planos que associem recursos marcados a agendas de backup e políticas de retenção. Para encontrar AWS Backup as configurações da sua conta AMS, use o console https://console.aws.amazon.com/backup ou a Referência de Comandos da AWS CLI para comandos de backup.

Para obter mais informações sobre o AMS e AWS Backup, consulte Gerenciamento de continuidade.

Como encontrar um ID de instância ou endereço IP

Você precisa de um endereço IP da instância para fazer login na instância.

- Para solicitar acesso a uma instância, fazer login em uma instância ou criar uma AMI, você deve ter o ID da instância. Para uma EC2 instância (independente ou parte de uma pilha) ou uma instância de banco de dados, você pode encontrar o ID de algumas maneiras diferentes:
  - O console AMS para uma instância em uma pilha ASG: procure na página de detalhes da RFC a RFC que criou a pilha. Na seção Saída de execução, você encontrará o ID da pilha ASG e, em seguida, poderá acessar a página Console Auto EC2 Scaling Groups, pesquisar esse ID da pilha e encontrar instâncias para ele. Ao encontrar a instância, selecione-a e uma área será aberta na parte inferior da página com detalhes, incluindo o endereço IP.
  - O console AMS para uma instância autônoma EC2 ou de banco de dados (banco de dados): procure na página de detalhes da RFC a RFC que criou a EC2 pilha ou a instância de banco de dados. Na seção Saída da execução, você encontrará o ID da instância e o endereço IP.
  - EC2 Console da AWS:

1. No painel de navegação, selecione Instances (Instâncias). A página Instâncias é aberta.
2. Clique na instância para a qual você quer o ID. A página de detalhes da instância é aberta e exibe o ID e o endereço IP.

- Console de banco de dados da AWS:
  1. Na página inicial, selecione Instâncias de banco de dados. A página Instâncias é aberta.
  2. Filtre a instância de banco de dados para a qual você deseja o ID. A página de detalhes da instância é aberta e exibe o ID.
- AMS CLI/API.

> **Note**
>
> A CLI do AMS deve estar instalada para que esses comandos funcionem. Para instalar a API ou a CLI do AMS, acesse a página Recursos para desenvolvedores do console AMS. Para obter material de referência sobre a API AMS CM ou a API AMS SKMS, consulte a seção Recursos de informação do AMS no Guia do usuário. Talvez seja necessário adicionar uma `--profile` opção para autenticação; por exemplo,`aws amsskms` *`ams-cli-command`* `--profile SAML`. Talvez você também precise adicionar a `--region` opção, pois todos os comandos do AMS saem de us-east-1; por exemplo. `aws amscm` *`ams-cli-command`* `--region=us-east-1`

> **Note**
>
> Os endpoints AMS API/CLI (amscm e amsskms) estão na região da AWS Norte da Virgínia,. `us-east-1` Dependendo de como sua autenticação está configurada e em qual região da AWS sua conta e seus recursos estão, talvez seja necessário adicioná-la `--region us-east-1` ao emitir comandos. Talvez você também precise adicionar`--profile saml`, se esse for o seu método de autenticação.

Execute o comando a seguir para obter detalhes da saída da execução da pilha:

```
aws amsskms get-stack --stack-id STACK_ID
```

A saída é semelhante a esta, InstanceId aparecendo na parte inferior, abaixo `Outputs` (os valores mostrados são exemplos):


```
{
    "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"
    }
}
```

Nomes de bastiões compatíveis com DNS

MALZ

Para Multi-account landing zone (MALZ), os registros DNS são criados para os bastiões no FQDN do Active Directory gerenciado pelo AMS. O AMS substitui os bastiões do Linux e do Windows conforme necessário. Por exemplo, se houver uma nova AMI do bastion que precisa ser implantada, os registros DNS do bastion são atualizados dinamicamente para apontar para bastions novos e válidos.

1. Para acessar os bastiões SSH (Linux), use registros DNS como estes: `sshbastion(1-4).Your_Domain.com`

   Por exemplo, onde o domínio está`Your_Domain`:

   - `sshbastion1.Your_Domain.com`
   - `sshbastion2.Your_Domain.com`
   - `sshbastion3.Your_Domain.com`
   - `sshbastion4.Your_Domain.com`

2. Para acessar os bastiões do RDP (Windows), use registros DNS como este:. `rdp-Username.Your_Domain.com`

   Por exemplo, onde o nome do usuário é`alex`,`test`,`demo`, ou`bob`, e o domínio é`Your_Domain.com`:

   - `rdp-alex.Your_Domain.com`
   - `rdp-test.Your_Domain.com`
   - `rdp-demo.Your_Domain.com`
   - `rdp-bob.Your_Domain.com`

SALZ

A landing zone de conta única (SALZ) substitui os bastiões do Linux e do Windows conforme necessário. Por exemplo, se houver uma nova AMI do bastion que precisa ser implantada, os registros DNS do bastion são atualizados dinamicamente para apontar para bastions novos e válidos.

1. Para acessar os bastiões SSH (Linux), use registros DNS como estes: `sshbastion(1-4).AAccountNumber.amazonaws.com.`

   Por exemplo, onde `123456789012` está o número da conta:

   - `sshbastion1.A123456789012.amazonaws.com`
   - `sshbastion2.A123456789012.amazonaws.com`
   - `sshbastion3.A123456789012.amazonaws.com`
   - `sshbastion4.A123456789012.amazonaws.com`

2. Para acessar os bastiões do RDP (Windows), use registros DNS como este:. `rdpbastion(1-4).AACCOUNT_NUMBER.amazonaws.com`

   Por exemplo, onde `123456789012` está o número da conta:

   - `rdpbastion1.A123456789012.amazonaws.com`
   - `rdpbastion2.A123456789012.amazonaws.com`
   - `rdpbastion3.A123456789012.amazonaws.com`
   - `rdpbastion4.A123456789012.amazonaws.com`

Encontrando endereços IP do Bastion

Os clientes do AMS podem usar bastions SSH e RDP, Nomes de bastiões compatíveis com DNS conforme descrito anteriormente, ou endereços IP bastion.

Para encontrar endereços IP bastion, SSH e RDP, para sua conta:

1. Somente para landing zone com várias contas: faça login na conta do Shared Services.
2. Abra o EC2 console e escolha Running Instances.

   A página Instâncias é aberta.

3. Na caixa de filtro na parte superior, insira ssh-bastion ou rdp-bastion.

   Na caixa de filtro na parte superior, insira customer-ssh ou customer-rdp.

   Os bastiões SSH and/or RDP da sua conta são exibidos.

   Observe que, além de seus bastiões SSH, você pode ver bastiões da rede de perímetro AMS na lista, que não estão disponíveis para isso.
4. Selecione um bastião SSH ou RDP. Se você estiver usando um computador Windows e quiser fazer login em uma instância Linux, use um SSH bastion. Se você quiser fazer login em uma instância do Windows, use um bastião RDP. Se você estiver em um sistema operacional Linux e quiser fazer login em uma instância do Windows, use um bastião SSH por meio de um túnel RDP (isso é para que você possa acessar a área de trabalho do Windows). Para acessar uma instância Linux a partir de um sistema operacional Linux, você usa um SSH bastion.

EC2 instâncias: Criação

Você pode usar o console do AMS ou API/CLI criar uma Amazon EC2 e uma Amazon EC2 com volumes adicionais.

Criar pilha

Criação de uma EC2 instância com o console

O seguinte mostra esse tipo de alteração no console AMS.

Como funciona:

1. Navegue até a página Criar RFC: No painel de navegação esquerdo do console AMS, clique RFCspara abrir a página da RFCs lista e, em seguida, clique em Criar RFC.
2. Escolha um tipo de alteração popular (CT) na visualização padrão Procurar tipos de alteração ou selecione uma CT na visualização Escolher por categoria.
   - Navegar por tipo de alteração: você pode clicar em um CT popular na área de criação rápida para abrir imediatamente a página Executar RFC. Observe que você não pode escolher uma versão mais antiga do CT com a criação rápida.

Para classificar CTs, use a área Todos os tipos de alteração na exibição Cartão ou Tabela. Em qualquer exibição, selecione uma CT e clique em Criar RFC para abrir a página Executar RFC. Se aplicável, a opção Criar com uma versão mais antiga aparece ao lado do botão Criar RFC.

- Escolha por categoria: selecione uma categoria, subcategoria, item e operação e a caixa de detalhes do CT será aberta com a opção Criar com uma versão mais antiga, se aplicável. Clique em Criar RFC para abrir a página Executar RFC.

3. Na página Executar RFC, abra a área do nome do CT para ver a caixa de detalhes do CT. É necessário um Assunto (preenchido se você escolher seu CT na visualização Procurar tipos de alteração). Abra a área Configuração adicional para adicionar informações sobre o RFC.

   Na área Configuração de execução, use as listas suspensas disponíveis ou insira valores para os parâmetros necessários. Para configurar parâmetros de execução opcionais, abra a área Configuração adicional.

4. Ao terminar, clique em Executar. Se não houver erros, a página RFC criada com sucesso será exibida com os detalhes da RFC enviada e a saída inicial de execução.

5. Abra a área Parâmetros de execução para ver as configurações que você enviou. Atualize a página para atualizar o status de execução do RFC. Opcionalmente, cancele a RFC ou crie uma cópia dela com as opções na parte superior da página.

Criação de uma EC2 instância com a CLI

Como funciona:

1. Use o Inline Create (você emite um `create-rfc` comando com todos os parâmetros de RFC e execução incluídos) ou o Template Create (você cria dois arquivos JSON, um para os parâmetros RFC e outro para os parâmetros de execução) e emita o `create-rfc` comando com os dois arquivos como entrada. Ambos os métodos são descritos aqui.
2. Envie o `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: com o ID RFC retornado.

   Monitore o `aws amscm get-rfc --rfc-id` *`ID`* comando RFC:.

Para verificar a versão do tipo de alteração, use este comando:

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

> **Note**
>
> Você pode usar qualquer `CreateRfc` parâmetro com qualquer RFC, independentemente de eles fazerem parte do esquema para o tipo de alteração. Por exemplo, para receber notificações quando o status da RFC mudar, adicione essa linha `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` à parte dos parâmetros da RFC da solicitação (não aos parâmetros de execução). Para obter uma lista de todos os CreateRfc parâmetros, consulte a Referência da API de gerenciamento de alterações do AMS.

CRIAÇÃO EM LINHA:

Execute o comando create RFC com os parâmetros de execução fornecidos em linha (aspas de escape ao fornecer parâmetros de execução em linha) e, em seguida, envie a ID de RFC retornada. Por exemplo, você pode substituir o conteúdo por algo assim:

```
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\"}}"
```

CRIAÇÃO DE MODELO:

1. Exiba os parâmetros de execução desse tipo de alteração em um arquivo JSON; este exemplo o chama de Create EC2 Params.json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-14027q0sjyt1h" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2Params.json
   ```

2. Modifique e salve o arquivo Create EC2 Params. Por exemplo, você pode substituir o conteúdo por algo assim:

   ```
   {
     "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. Envie o modelo RFC para um arquivo em sua pasta atual; este exemplo o chama de Create EC2 RFC.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2Rfc.json
```

4. Modifique e salve o arquivo Create EC2 RFC.json. Por exemplo, você pode substituir o conteúdo por algo assim:.

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-14027q0sjyt1h",
"Title":                "EC2-Create-RFC"
}
```

5. Crie o RFC, especificando o arquivo Create EC2 Rfc e o arquivo Create EC2 Params:

```
aws amscm create-rfc --cli-input-json file://CreateEC2Rfc.json  --execution-
parameters file://CreateEC2Params.json
```

Você recebe a ID da nova RFC na resposta e pode usá-la para enviar e monitorar a RFC. Até que você o envie, o RFC permanece no estado de edição e não inicia.

Dicas

> **Grupos de segurança**
>
> A partir da versão 3.0 desse tipo de alteração, o AMS não anexa os grupos de segurança padrão do AMS se você especificar seus próprios grupos de segurança. Se você não especificar seus próprios grupos de segurança na solicitação, o AMS anexará os grupos de segurança padrão do AMS. Nas versões anteriores, o AMS anexava os grupos de segurança padrão, independentemente de você ter fornecido ou não seus próprios grupos de segurança.
> Atualmente, se você especificar grupos de segurança personalizados, também deverá especificar os grupos IDs de segurança padrão do AMS para sua conta `mc-initial-garden-SG-name` `mc-initial-garden-SG-name` e.

> **Instance Types (Tipos de instâncias)**
>
> O AMS não recomenda os tipos t2.micro/t3.micro e t2.nano/t3.nano. Esses são tipos de instâncias menores e podem degradar o desempenho do seu aplicativo e das ferramentas do AMS. EC2 as instâncias precisam de capacidade suficiente para suportar ferramentas AMS, como EPS, SSM e Cloudwatch, além da carga de trabalho do aplicativo. Para obter mais informações, consulte Como escolher o tipo de EC2 instância certo para seu aplicativo.

Para criar uma EC2 pilha com volumes adicionais, consulte EC2 Pilha | Criar (com volumes adicionais).

Você pode adicionar até 50 tags, mas para isso você deve ativar a visualização de configuração adicional.

Se necessário, consulte Falha na criação da pilha de EC2 instâncias.

Criar pilha (com volumes adicionais)

Criação de uma EC2 instância e volumes adicionais com o console

O seguinte mostra esse tipo de alteração no console AMS.

Como funciona:

1. Navegue até a página Criar RFC: No painel de navegação esquerdo do console AMS, clique RFCspara abrir a página da RFCs lista e, em seguida, clique em Criar RFC.
2. Escolha um tipo de alteração popular (CT) na visualização padrão Procurar tipos de alteração ou selecione uma CT na visualização Escolher por categoria.
   - Navegar por tipo de alteração: você pode clicar em um CT popular na área de criação rápida para abrir imediatamente a página Executar RFC. Observe que você não pode escolher uma versão mais antiga do CT com a criação rápida.

     Para classificar CTs, use a área Todos os tipos de alteração na exibição Cartão ou Tabela. Em qualquer exibição, selecione uma CT e clique em Criar RFC para abrir a página Executar RFC. Se aplicável, a opção Criar com uma versão mais antiga aparece ao lado do botão Criar RFC.
   - Escolha por categoria: selecione uma categoria, subcategoria, item e operação e a caixa de detalhes do CT será aberta com a opção Criar com uma versão mais antiga, se aplicável. Clique em Criar RFC para abrir a página Executar RFC.
3. Na página Executar RFC, abra a área do nome do CT para ver a caixa de detalhes do CT. É necessário um Assunto (preenchido se você escolher seu CT na visualização Procurar tipos de alteração). Abra a área Configuração adicional para adicionar informações sobre o RFC.

   Na área Configuração de execução, use as listas suspensas disponíveis ou insira valores para os parâmetros necessários. Para configurar parâmetros de execução opcionais, abra a área Configuração adicional.
4. Ao terminar, clique em Executar. Se não houver erros, a página RFC criada com sucesso será exibida com os detalhes da RFC enviada e a saída inicial de execução.
5. Abra a área Parâmetros de execução para ver as configurações que você enviou. Atualize a página para atualizar o status de execução do RFC. Opcionalmente, cancele a RFC ou crie uma cópia dela com as opções na parte superior da página.

Criação de uma EC2 instância e volumes adicionais com a CLI

Como funciona:

1. Use o Inline Create (você emite um `create-rfc` comando com todos os parâmetros de RFC e execução incluídos) ou o Template Create (você cria dois arquivos JSON, um para os parâmetros RFC e outro para os parâmetros de execução) e emita o `create-rfc` comando com os dois arquivos como entrada. Ambos os métodos são descritos aqui.
2. Envie o `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: com o ID RFC retornado.

Monitore o `aws amscm get-rfc --rfc-id` *`ID`* comando RFC:.

Para verificar a versão do tipo de alteração, use este comando:

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

> **Note**
>
> Você pode usar qualquer `CreateRfc` parâmetro com qualquer RFC, independentemente de eles fazerem parte do esquema para o tipo de alteração. Por exemplo, para receber notificações quando o status da RFC mudar, adicione essa linha `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` à parte dos parâmetros da RFC da solicitação (não aos parâmetros de execução). Para obter uma lista de todos os CreateRfc parâmetros, consulte a Referência da API de gerenciamento de alterações do AMS.

CRIAÇÃO EM LINHA:

Execute o comando create RFC com os parâmetros de execução fornecidos em linha (aspas de escape ao fornecer parâmetros de execução em linha) e, em seguida, envie a ID de RFC retornada (o exemplo mostra somente os parâmetros necessários). Por exemplo, você pode substituir o conteúdo por algo assim:

```
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\"}}
```

CRIAÇÃO DE MODELO:

1. Envie os parâmetros de execução desse tipo de alteração para um arquivo JSON chamado Create EC2 AVParams .json.

   ```
   aws amscm get-change-type-version --change-type-id "ct-1aqsjf86w6vxg" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2AVParams.json
   ```

2. Modifique e salve o EC2 AVParams arquivo Create (o exemplo mostra a maioria dos parâmetros). Por exemplo, você pode substituir o conteúdo por algo assim:

```
{
"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. Envie o modelo RFC para um arquivo em sua pasta atual; este exemplo o chama de Create EC2 AVRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2AVRfc.json
```

4. Modifique e salve o EC2 AVRfc arquivo Create .json. Por exemplo, você pode substituir o conteúdo por algo assim:

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-1aqsjf86w6vxg",
"Title":                "EC2-Create-1-Addl-Volume-RFC"
}
```

5. Crie o RFC, especificando o EC2 AVRfc arquivo Create e o Create EC2 AVParams file:

```
aws amscm create-rfc --cli-input-json file://CreateEC2AVRfc.json  --execution-
parameters file://CreateEC2AVParams.json
```

Você recebe a ID da nova RFC na resposta e pode usá-la para enviar e monitorar a RFC. Até que você o envie, o RFC permanece no estado de edição e não inicia.

Dicas

Important

Há uma nova versão desse tipo de alteração, a v 4.0, que usa uma versão diferente StackTemplateId (stm-nn8v8ffhcal611bmo). Isso é importante se você estiver enviando o RFC com esse tipo de alteração na linha de comando. A nova versão introduz dois novos parâmetros (RootVolumeKmsKeyIde CreditSpecification) e altera o padrão para um parâmetro existente (InstanceType).

Instance Types (Tipos de instâncias)

- Se você optar por especificar o número de núcleos ou threads, deverá especificar valores para ambos. Use os parâmetros `InstanceCoreCount` `InstanceThreadsPerCore` e. Para encontrar combinações válidas de núcleos/threads, consulte Núcleos de CPU e threads por núcleo de CPU por tipo de instância.

- O AMS não recomenda os tipos de instância t2.micro/t3.micro ou t2.nano/t3.nano. Eles são pequenos demais para suportar ferramentas de AMS, como EPS, SSM e Cloudwatch, além da carga de trabalho da sua empresa. Para obter mais informações, consulte Como escolher o tipo de EC2 instância certo para seu aplicativo.
- Na versão 4.0, o tipo padrão foi aumentado de t2.large para t3.large. As instâncias T3 são iniciadas com “créditos ilimitados” por padrão. Você não experimentará a limitação da CPU, mesmo que a instância consuma todos os créditos da CPU. Em vez disso, você pode escolher instâncias T2 e usar a opção CreditSpecification ilimitada.
- Para obter mais informações sobre a Amazon EC2, incluindo recomendações de tamanho, consulte a documentação do Amazon Elastic Compute Cloud.

Para atualizar sua EC2 pilha com volumes adicionais após sua criação, consulte Pilha de EC2 instâncias: atualização (com volumes adicionais)

Acesso, solicitação

Solicitar acesso administrativo

Solicitando acesso de administrador com o console

O seguinte mostra esse tipo de alteração no console AMS.

Como funciona:

1. Navegue até a página Criar RFC: No painel de navegação esquerdo do console AMS, clique RFCspara abrir a página da RFCs lista e, em seguida, clique em Criar RFC.
2. Escolha um tipo de alteração popular (CT) na visualização padrão Procurar tipos de alteração ou selecione uma CT na visualização Escolher por categoria.
   - Navegar por tipo de alteração: você pode clicar em um CT popular na área de criação rápida para abrir imediatamente a página Executar RFC. Observe que você não pode escolher uma versão mais antiga do CT com a criação rápida.

     Para classificar CTs, use a área Todos os tipos de alteração na exibição Cartão ou Tabela. Em qualquer exibição, selecione uma CT e clique em Criar RFC para abrir a página Executar RFC. Se aplicável, a opção Criar com uma versão mais antiga aparece ao lado do botão Criar RFC.

- Escolha por categoria: selecione uma categoria, subcategoria, item e operação e a caixa de detalhes do CT será aberta com a opção Criar com uma versão mais antiga, se aplicável. Clique em Criar RFC para abrir a página Executar RFC.

3. Na página Executar RFC, abra a área do nome do CT para ver a caixa de detalhes do CT. É necessário um Assunto (preenchido se você escolher seu CT na visualização Procurar tipos de alteração). Abra a área Configuração adicional para adicionar informações sobre o RFC.

   Na área Configuração de execução, use as listas suspensas disponíveis ou insira valores para os parâmetros necessários. Para configurar parâmetros de execução opcionais, abra a área Configuração adicional.
4. Ao terminar, clique em Executar. Se não houver erros, a página RFC criada com sucesso será exibida com os detalhes da RFC enviada e a saída inicial de execução.
5. Abra a área Parâmetros de execução para ver as configurações que você enviou. Atualize a página para atualizar o status de execução do RFC. Opcionalmente, cancele a RFC ou crie uma cópia dela com as opções na parte superior da página.

Solicitando acesso de administrador com a CLI

Como funciona:

1. Use o Inline Create (você emite um `create-rfc` comando com todos os parâmetros de RFC e execução incluídos) ou o Template Create (você cria dois arquivos JSON, um para os parâmetros RFC e outro para os parâmetros de execução) e emita o `create-rfc` comando com os dois arquivos como entrada. Ambos os métodos são descritos aqui.
2. Envie o `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: com o ID RFC retornado.

   Monitore o `aws amscm get-rfc --rfc-id` *`ID`* comando RFC:.

Para verificar a versão do tipo de alteração, use este comando:

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

> **Note**
>
> Você pode usar qualquer `CreateRfc` parâmetro com qualquer RFC, independentemente de eles fazerem parte do esquema para o tipo de alteração. Por exemplo, para receber

notificações quando o status da RFC mudar, adicione essa linha `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` à parte dos parâmetros da RFC da solicitação (não aos parâmetros de execução). Para obter uma lista de todos os CreateRfc parâmetros, consulte a Referência da API de gerenciamento de alterações do AMS.

CRIAÇÃO EM LINHA:

Execute o comando create RFC com os parâmetros de execução fornecidos em linha (aspas de escape ao fornecer parâmetros de execução em linha) e, em seguida, envie a ID de RFC retornada. Por exemplo, você pode substituir o conteúdo por algo assim:

```
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\"}"
```

CRIAÇÃO DE MODELO:

1. Exiba os parâmetros de execução do esquema JSON para esse tipo de alteração em um arquivo; este exemplo o chama de .json: GrantAdminAccessParams

   ```
   aws amscm get-change-type-version --change-type-id "ct-1dmlg9g1l91h6"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantAdminAccessParams.json
   ```

   Modifique e salve o GrantAdminAccessParams arquivo. Por exemplo, você pode substituir o conteúdo por algo assim:

   ```
   {
   "DomainFQDN":           "mycorpdomain.acme.com",
   "StackIds":             [STACK_ID, STACK_ID],
   "TimeRequestedInHours": 12,
   "Username":             ["USERNAME", "USERNAME"],
   "VpcId":                "VPC_ID"
   }
   ```

Observe que o padrão da `TimeRequestedInHours` opção é de uma hora. Você pode solicitar até doze horas.

2. Envie o modelo RFC para um arquivo em sua pasta atual; este exemplo o chama de GrantAdminAccessRfc .json:

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

3. Modifique e salve o GrantAdminAccessRfc arquivo.json. Por exemplo, você pode substituir o conteúdo por algo assim:

```
{
"ChangeTypeId":          "ct-1dmlg9g1l91h6",
"ChangeTypeVersion":     "3.0",
"Title":                 "Request-Admin-Access-to-EC2-RFC"
}
```

4. Crie o RFC, especificando o GrantAdminAccessRfc arquivo e o GrantAdminAcessParams arquivo:

```
aws amscm create-rfc --cli-input-json file://GrantAdminAccessRfc.json --execution-
parameters file://GrantAdminAccessParams.json
```

Você recebe a ID da nova RFC na resposta e pode usá-la para enviar e monitorar a RFC. Até que você o envie, o RFC permanece no estado de edição e não inicia.

Para fazer login na instância por meio de um bastião, siga o próximo procedimento, Exemplos de acesso à instância.

Dicas

> **Note**
>
> Você pode enviar uma atualização para sua solicitação de acesso antes que ela expire. Para obter mais informações, consulte Stack Admin Access | Update.
> Para fazer login em uma instância que faz parte de um ASG, você solicita acesso à pilha ASG, que dá acesso a todas as instâncias associadas.

Para ver um exemplo sobre como solicitar ReadOnly acesso, consulte ReadOnly acesso: solicitação.

Solicitar ReadOnly acesso

Solicitando ReadOnly acesso com o console

O seguinte mostra esse tipo de alteração no console AMS.

Como funciona:

1. Navegue até a página Criar RFC: No painel de navegação esquerdo do console AMS, clique RFCspara abrir a página da RFCs lista e, em seguida, clique em Criar RFC.
2. Escolha um tipo de alteração popular (CT) na visualização padrão Procurar tipos de alteração ou selecione uma CT na visualização Escolher por categoria.
   - Navegar por tipo de alteração: você pode clicar em um CT popular na área de criação rápida para abrir imediatamente a página Executar RFC. Observe que você não pode escolher uma versão mais antiga do CT com a criação rápida.

     Para classificar CTs, use a área Todos os tipos de alteração na exibição Cartão ou Tabela. Em qualquer exibição, selecione uma CT e clique em Criar RFC para abrir a página Executar RFC. Se aplicável, a opção Criar com uma versão mais antiga aparece ao lado do botão Criar RFC.
   - Escolha por categoria: selecione uma categoria, subcategoria, item e operação e a caixa de detalhes do CT será aberta com a opção Criar com uma versão mais antiga, se aplicável. Clique em Criar RFC para abrir a página Executar RFC.
3. Na página Executar RFC, abra a área do nome do CT para ver a caixa de detalhes do CT. É necessário um Assunto (preenchido se você escolher seu CT na visualização Procurar tipos de alteração). Abra a área Configuração adicional para adicionar informações sobre o RFC.

   Na área Configuração de execução, use as listas suspensas disponíveis ou insira valores para os parâmetros necessários. Para configurar parâmetros de execução opcionais, abra a área Configuração adicional.
4. Ao terminar, clique em Executar. Se não houver erros, a página RFC criada com sucesso será exibida com os detalhes da RFC enviada e a saída inicial de execução.
5. Abra a área Parâmetros de execução para ver as configurações que você enviou. Atualize a página para atualizar o status de execução do RFC. Opcionalmente, cancele a RFC ou crie uma cópia dela com as opções na parte superior da página.

Solicitando ReadOnly acesso com a CLI

Como funciona:

1. Use o Inline Create (você emite um `create-rfc` comando com todos os parâmetros de RFC e execução incluídos) ou o Template Create (você cria dois arquivos JSON, um para os parâmetros RFC e outro para os parâmetros de execução) e emita o `create-rfc` comando com os dois arquivos como entrada. Ambos os métodos são descritos aqui.
2. Envie o `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: com o ID RFC retornado.

   Monitore o `aws amscm get-rfc --rfc-id` *`ID`* comando RFC:.

Para verificar a versão do tipo de alteração, use este comando:

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

> **Note**
>
> Você pode usar qualquer `CreateRfc` parâmetro com qualquer RFC, independentemente de eles fazerem parte do esquema para o tipo de alteração. Por exemplo, para receber notificações quando o status da RFC mudar, adicione essa linha `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` à parte dos parâmetros da RFC da solicitação (não aos parâmetros de execução). Para obter uma lista de todos os CreateRfc parâmetros, consulte a Referência da API de gerenciamento de alterações do AMS.

CRIAÇÃO EM LINHA:

Execute o comando create RFC com os parâmetros de execução fornecidos em linha (aspas de escape ao fornecer parâmetros de execução em linha) e, em seguida, envie a ID de RFC retornada. Por exemplo, você pode substituir o conteúdo por algo assim:

```
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\"}"
```

CRIAÇÃO DE MODELO:

1. Exiba os parâmetros de execução do esquema JSON para esse tipo de alteração em um arquivo; este exemplo o chama de .json: GrantReadOnlyAccessParams

```
aws amscm get-change-type-version --change-type-id "ct-199h35t7uz6jl"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 GrantReadOnlyAccessParams.json
```

   Modifique e salve o GrantReadOnlyAccessParams arquivo. Por exemplo, você pode substituir o conteúdo por algo assim:

```
{
"DomainFQDN":           "mycorpdomain.acme.com",
"StackIds":             [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Usernames":             ["USERNAME", "USERNAME"],
"VpcId":                "VPC_ID"
}
```

   Observe que o padrão da `TimeRequestedInHours` opção é de uma hora. Você pode solicitar até doze horas.

2. Envie o modelo RFC para um arquivo em sua pasta atual; este exemplo o chama de GrantReadOnlyAccessRfc .json:

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

3. Modifique e salve o GrantReadOnlyAccessRfc arquivo.json. Por exemplo, você pode substituir o conteúdo por algo assim:

```
{
"ChangeTypeId":         "ct-199h35t7uz6jl",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-ReadOnly-Access-to-EC2-RFC"
}
```

4. Crie o RFC, especificando o GrantReadOnlyAccessRfc arquivo e o GrantReadOnlyAcessParams arquivo:

```
aws amscm create-rfc --cli-input-json file://GrantReadOnlyAccessRfc.json --
execution-parameters file://GrantReadOnlyAccessParams.json
```

Você recebe a ID da nova RFC na resposta e pode usá-la para enviar e monitorar a RFC. Até que você o envie, o RFC permanece no estado de edição e não inicia.

Para fazer login na instância por meio de um bastião, siga o próximo procedimento, Exemplos de acesso à instância.

Dicas

> **Note**
>
> Você pode enviar uma atualização para sua solicitação de acesso antes que ela expire. Para obter detalhes, consulte Stack Read-Only Access | Update.
> Para fazer login em uma instância que faz parte de um grupo de EC2 Auto Scaling (ASG), você solicita acesso à pilha ASG, que dá acesso a todas as instâncias associadas.

Para ver um passo a passo sobre como solicitar acesso de administrador, consulte Acesso de administrador: solicitando.

Outros | Outro RFC, criação (CLI)

Este exemplo mostra como solicitar uma alteração em nenhum dos CTs endereços disponíveis, usando o Management | Other | Other | Create CT (ct-1e1xtak34nx76).

Use essa tomografia computadorizada quando não conseguir encontrar um tipo de alteração para o que deseja; no entanto, se não tiver certeza sobre a especificação de parâmetros em uma tomografia computadorizada existente, é melhor enviar uma solicitação de serviço para obter ajuda. Para obter informações sobre o envio de solicitações de serviço, consulte Exemplos de solicitações de serviço.

Esse tipo de RFC é exigido pela aprovação, o que significa que ele requer a aprovação do AMS antes de ser implementado. Depois de enviar a RFC, um operador de AMS entrará em contato com você para discutir a pilha que você deseja implantar.

> **Note**
>
> Ao usar “revisão obrigatória” CTs, o AMS recomenda que você use a opção ASAP Scheduling (escolha ASAP no console, deixe a hora de início e término em branco na API/CLI), pois isso CTs exige que um operador do AMS examine a RFC e, possivelmente, se comunique com você antes que ela possa ser aprovada e executada. Se você agendá-los RFCs, aguarde pelo menos 24 horas. Se a aprovação não ocorrer antes do horário de início programado, a RFC será rejeitada automaticamente.

DADOS NECESSÁRIOS:

- `Comment`: Para que serve o RFC.
- `ChangeTypeIdeChangeTypeVersion`: Use Other | Create (`ct-1e1xtak34nx76`) para solicitar novos recursos, use Other | Update (`ct-0xdawir96cy7k`) para alterar os recursos existentes; ambos sãov1.

DADOS OPCIONAIS`Priority`: Os valores aceitáveis são `High`Medium, ou`Low`.

CRIAÇÃO EM LINHA:

- Execute o comando create RFC com os parâmetros de execução fornecidos em linha (aspas de escape ao fornecer parâmetros de execução em linha). Exemplo de uso: Outro | Criar.

```
aws amscm create-rfc --change-type-id "ct-1e1xtak34nx76" --change-type-version "1.0"
 --title "TITLE" --execution-parameters "{\"Comment\": \"What you want created\"}"
```

- Envie a RFC usando a ID da RFC retornada na operação de criação da RFC. Até ser enviada, a RFC permanece no `Editing` estado e não é aplicada.

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

- Monitore o status da RFC e visualize a saída da execução:

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

CRIAÇÃO DE MODELO:

1. Crie e salve um arquivo JSON para os parâmetros de execução; o exemplo o chama de OtherParams .json e inclui o parâmetro opcional: `Priority`

```
{
"Comment":          "What you want created",
"Priority":         "Medium"
}
```

2. Crie e salve um arquivo JSON para os parâmetros RFC; o exemplo o chama de .json. OtherRfc

```
{
"ChangeTypeId":         "ct-1e1xtak34nx76",
"ChangeTypeVersion":    "1.0",
"Title":                "TITLE"
}
```

3. Crie o RFC, especificando o OtherRfc arquivo e o OtherParams arquivo:

```
aws amscm create-rfc --cli-input-json file://OtherRfc.json  --execution-parameters
 file://OtherParams.json
```

Você recebe o RfcId do novo RFC na resposta. Por exemplo:

```
{
"RfcId": "RFC-ID"
}
```

4. Envie o RFC:

```
aws amscm submit-rfc --rfc-id RFC-ID
```

Se nenhum erro for relatado, a operação foi bem-sucedida.

5. Para monitorar o status da solicitação e visualizar a Saída de Execução:

```
aws amscm get-rfc --rfc-id RFC-ID
```

Qualquer pilha: excluindo, reiniciando, iniciando, parando

Você pode usar o console AMS ou API/CLI excluir, reinicializar, iniciar ou parar uma pilha AMS.

Excluir pilha

Excluindo uma pilha com o console

Captura de tela desse tipo de alteração no console AMS:

Como funciona:

1. Navegue até a página Criar RFC: No painel de navegação esquerdo do console AMS, clique RFCspara abrir a página da RFCs lista e, em seguida, clique em Criar RFC.
2. Escolha um tipo de alteração popular (CT) na visualização padrão Procurar tipos de alteração ou selecione uma CT na visualização Escolher por categoria.
   - Navegar por tipo de alteração: você pode clicar em um CT popular na área de criação rápida para abrir imediatamente a página Executar RFC. Observe que você não pode escolher uma versão mais antiga do CT com a criação rápida.

     Para classificar CTs, use a área Todos os tipos de alteração na exibição Cartão ou Tabela. Em qualquer exibição, selecione uma CT e clique em Criar RFC para abrir a página Executar RFC. Se aplicável, a opção Criar com uma versão mais antiga aparece ao lado do botão Criar RFC.
   - Escolha por categoria: selecione uma categoria, subcategoria, item e operação e a caixa de detalhes do CT será aberta com a opção Criar com uma versão mais antiga, se aplicável. Clique em Criar RFC para abrir a página Executar RFC.
3. Na página Executar RFC, abra a área do nome do CT para ver a caixa de detalhes do CT. É necessário um Assunto (preenchido se você escolher seu CT na visualização Procurar tipos de alteração). Abra a área Configuração adicional para adicionar informações sobre o RFC.

   Na área Configuração de execução, use as listas suspensas disponíveis ou insira valores para os parâmetros necessários. Para configurar parâmetros de execução opcionais, abra a área Configuração adicional.
4. Ao terminar, clique em Executar. Se não houver erros, a página RFC criada com sucesso será exibida com os detalhes da RFC enviada e a saída inicial de execução.
5. Abra a área Parâmetros de execução para ver as configurações que você enviou. Atualize a página para atualizar o status de execução do RFC. Opcionalmente, cancele a RFC ou crie uma cópia dela com as opções na parte superior da página.

Excluindo uma pilha com a CLI

Como funciona:

1. Use o Inline Create (você emite um `create-rfc` comando com todos os parâmetros de RFC e execução incluídos) ou o Template Create (você cria dois arquivos JSON, um para os parâmetros RFC e outro para os parâmetros de execução) e emita o `create-rfc` comando com os dois arquivos como entrada. Ambos os métodos são descritos aqui.
2. Envie o `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: com o ID RFC retornado.

   Monitore o `aws amscm get-rfc --rfc-id` *`ID`* comando RFC:.

Para verificar a versão do tipo de alteração, use este comando:

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

> **Note**
>
> Você pode usar qualquer `CreateRfc` parâmetro com qualquer RFC, independentemente de eles fazerem parte do esquema para o tipo de alteração. Por exemplo, para receber notificações quando o status da RFC mudar, adicione essa linha `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` à parte dos parâmetros da RFC da solicitação (não aos parâmetros de execução). Para obter uma lista de todos os CreateRfc parâmetros, consulte a Referência da API de gerenciamento de alterações do AMS.

CRIAÇÃO EM LINHA:

Execute o comando create RFC com os parâmetros de execução fornecidos em linha (aspas de escape ao fornecer parâmetros de execução em linha) e, em seguida, envie a ID de RFC retornada. Por exemplo, você pode substituir o conteúdo por algo assim:

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0" --
title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CRIAÇÃO DE MODELO:

1. Envie o modelo RFC para um arquivo em sua pasta atual; este exemplo o chama de DeleteStackRfc .json:

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

2. Modifique e salve o DeleteStackRfc arquivo.json.

   As aspas internas na extensão ExecutionParameters JSON devem ser excluídas com uma barra invertida (\). Exemplo sem horário de início e término:

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-0q0bic0ywqk6c",
"Title":                "Delete-My-Stack-RFC"
"ExecutionParameters":  "{
        \"StackId\":\"STACK_ID\"}"
}
```

3. Crie o RFC:

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
```

   Você recebe a ID da nova RFC na resposta e pode usá-la para enviar e monitorar a RFC. Até que você o envie, o RFC permanece no estado de edição e não inicia.

Dicas

> **Note**
>
> Se você excluir um bucket do S3, primeiro ele deverá ser esvaziado de objetos.

> **Important**
>
> A exclusão de pilhas pode ter consequências indesejadas e imprevistas. Para ressalvas importantes, consulte a seção Solução de problemas de RFC RFCs para Excluir pilha.

Reinicialize a pilha

Reinicializando uma pilha com o console

Captura de tela desse tipo de alteração no console AMS:

Como funciona:

1. Navegue até a página Criar RFC: No painel de navegação esquerdo do console AMS, clique RFCspara abrir a página da RFCs lista e, em seguida, clique em Criar RFC.
2. Escolha um tipo de alteração popular (CT) na visualização padrão Procurar tipos de alteração ou selecione uma CT na visualização Escolher por categoria.
   - Navegar por tipo de alteração: você pode clicar em um CT popular na área de criação rápida para abrir imediatamente a página Executar RFC. Observe que você não pode escolher uma versão mais antiga do CT com a criação rápida.

     Para classificar CTs, use a área Todos os tipos de alteração na exibição Cartão ou Tabela. Em qualquer exibição, selecione uma CT e clique em Criar RFC para abrir a página Executar RFC. Se aplicável, a opção Criar com uma versão mais antiga aparece ao lado do botão Criar RFC.
   - Escolha por categoria: selecione uma categoria, subcategoria, item e operação e a caixa de detalhes do CT será aberta com a opção Criar com uma versão mais antiga, se aplicável. Clique em Criar RFC para abrir a página Executar RFC.
3. Na página Executar RFC, abra a área do nome do CT para ver a caixa de detalhes do CT. É necessário um Assunto (preenchido se você escolher seu CT na visualização Procurar tipos de alteração). Abra a área Configuração adicional para adicionar informações sobre o RFC.

   Na área Configuração de execução, use as listas suspensas disponíveis ou insira valores para os parâmetros necessários. Para configurar parâmetros de execução opcionais, abra a área Configuração adicional.
4. Ao terminar, clique em Executar. Se não houver erros, a página RFC criada com sucesso será exibida com os detalhes da RFC enviada e a saída inicial de execução.
5. Abra a área Parâmetros de execução para ver as configurações que você enviou. Atualize a página para atualizar o status de execução do RFC. Opcionalmente, cancele a RFC ou crie uma cópia dela com as opções na parte superior da página.

Reinicializando uma pilha com a CLI

Como funciona:

1. Use o Inline Create (você emite um `create-rfc` comando com todos os parâmetros de RFC e execução incluídos) ou o Template Create (você cria dois arquivos JSON, um para os parâmetros RFC e outro para os parâmetros de execução) e emita o `create-rfc` comando com os dois arquivos como entrada. Ambos os métodos são descritos aqui.
2. Envie o `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: com o ID RFC retornado.

   Monitore o `aws amscm get-rfc --rfc-id` *`ID`* comando RFC:.

Para verificar a versão do tipo de alteração, use este comando:

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

> **Note**
>
> Você pode usar qualquer `CreateRfc` parâmetro com qualquer RFC, independentemente de eles fazerem parte do esquema para o tipo de alteração. Por exemplo, para receber notificações quando o status da RFC mudar, adicione essa linha `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` à parte dos parâmetros da RFC da solicitação (não aos parâmetros de execução). Para obter uma lista de todos os CreateRfc parâmetros, consulte a Referência da API de gerenciamento de alterações do AMS.

CRIAÇÃO EM LINHA:

Execute o comando create RFC com os parâmetros de execução fornecidos em linha (aspas de escape ao fornecer parâmetros de execução em linha) e, em seguida, envie a ID de RFC retornada. Por exemplo, você pode substituir o conteúdo por algo assim:

```
aws amscm create-rfc --change-type-id "ct-02u0hoaa9grat" --change-type-version "1.0" --
title "Reboot My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CRIAÇÃO DE MODELO:

1. Envie o modelo RFC para um arquivo na sua pasta atual. Este exemplo o chama de RebootStackRfc .json. Observe que, como há apenas um parâmetro de execução para interromper (reinicializar ou iniciar) uma instância, o parâmetro de execução pode estar no próprio arquivo JSON do esquema e não há necessidade de criar um arquivo JSON de parâmetros de execução separado.

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

2. Modifique e salve o RebootStackRfc arquivo.json.

   As aspas internas na extensão `ExecutionParameters` JSON devem ser excluídas com uma barra invertida (\). Exemplo:

```
{
"ChangeTypeId":          "ct-02u0hoaa9grat",
"Title":                 "Reboot-My-EC2-RFC",
"TimeoutInMinutes":      60,
"ExecutionParameters":   "{
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. Crie o RFC:

```
aws amscm create-rfc --cli-input-json file://RebootStackRfc.json
```

   Você recebe a ID da nova RFC na resposta e pode usá-la para enviar e monitorar a RFC. Até que você o envie, o RFC permanece no estado de edição e não inicia.

Dicas

Para obter informações sobre Application Load Balancers, consulte Application Load Balancers.

Iniciar pilha

Iniciando uma pilha com o console

Captura de tela desse tipo de alteração no console AMS:

Como funciona:

1. Navegue até a página Criar RFC: No painel de navegação esquerdo do console AMS, clique RFCspara abrir a página da RFCs lista e, em seguida, clique em Criar RFC.
2. Escolha um tipo de alteração popular (CT) na visualização padrão Procurar tipos de alteração ou selecione uma CT na visualização Escolher por categoria.
   - Navegar por tipo de alteração: você pode clicar em um CT popular na área de criação rápida para abrir imediatamente a página Executar RFC. Observe que você não pode escolher uma versão mais antiga do CT com a criação rápida.

     Para classificar CTs, use a área Todos os tipos de alteração na exibição Cartão ou Tabela. Em qualquer exibição, selecione uma CT e clique em Criar RFC para abrir a página Executar RFC. Se aplicável, a opção Criar com uma versão mais antiga aparece ao lado do botão Criar RFC.
   - Escolha por categoria: selecione uma categoria, subcategoria, item e operação e a caixa de detalhes do CT será aberta com a opção Criar com uma versão mais antiga, se aplicável. Clique em Criar RFC para abrir a página Executar RFC.
3. Na página Executar RFC, abra a área do nome do CT para ver a caixa de detalhes do CT. É necessário um Assunto (preenchido se você escolher seu CT na visualização Procurar tipos de alteração). Abra a área Configuração adicional para adicionar informações sobre o RFC.

   Na área Configuração de execução, use as listas suspensas disponíveis ou insira valores para os parâmetros necessários. Para configurar parâmetros de execução opcionais, abra a área Configuração adicional.
4. Ao terminar, clique em Executar. Se não houver erros, a página RFC criada com sucesso será exibida com os detalhes da RFC enviada e a saída inicial de execução.
5. Abra a área Parâmetros de execução para ver as configurações que você enviou. Atualize a página para atualizar o status de execução do RFC. Opcionalmente, cancele a RFC ou crie uma cópia dela com as opções na parte superior da página.

Iniciando uma pilha com a CLI

Como funciona:

1. Use o Inline Create (você emite um `create-rfc` comando com todos os parâmetros de RFC e execução incluídos) ou o Template Create (você cria dois arquivos JSON, um para os parâmetros RFC e outro para os parâmetros de execução) e emita o `create-rfc` comando com os dois arquivos como entrada. Ambos os métodos são descritos aqui.
2. Envie o `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: com o ID RFC retornado.

Monitore o `aws amscm get-rfc --rfc-id ID` comando RFC:.

Para verificar a versão do tipo de alteração, use este comando:

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

> **Note**
>
> Você pode usar qualquer `CreateRfc` parâmetro com qualquer RFC, independentemente de eles fazerem parte do esquema para o tipo de alteração. Por exemplo, para receber notificações quando o status da RFC mudar, adicione essa linha `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` à parte dos parâmetros da RFC da solicitação (não aos parâmetros de execução). Para obter uma lista de todos os CreateRfc parâmetros, consulte a Referência da API de gerenciamento de alterações do AMS.

CRIAÇÃO EM LINHA:

Execute o comando create RFC com os parâmetros de execução fornecidos em linha (aspas de escape ao fornecer parâmetros de execução em linha) e, em seguida, envie a ID de RFC retornada. Por exemplo, você pode substituir o conteúdo por algo assim:

```
aws amscm create-rfc --change-type-id "ct-1h5xgl9cr4bzy" --change-type-version "1.0" --
title "Start My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CRIAÇÃO DE MODELO:

1. Envie o modelo RFC para um arquivo na sua pasta atual. Este exemplo o chama de StartInstanceRfc .json. Observe que, como há apenas um parâmetro de execução para iniciar uma pilha, o parâmetro de execução pode estar no próprio arquivo JSON do esquema e não há necessidade de criar um arquivo JSON de parâmetros de execução separado.

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

2. Modifique e salve o StartStackRfc arquivo.json. Por exemplo, você pode substituir o conteúdo por algo assim:

```
{
"ChangeTypeId":          "ct-1h5xgl9cr4bzy",
"Title":                 "Start-My-EC2-RFC",
"TimeoutInMinutes":      60,
"ExecutionParameters":   "{
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. Crie o RFC:

```
aws amscm create-rfc --cli-input-json file://StartStackRfc.json
```

Você recebe a ID da nova RFC na resposta e pode usá-la para enviar e monitorar a RFC. Até que você o envie, o RFC permanece no estado de edição e não inicia.

Dicas

Para obter informações sobre Application Load Balancers, consulte Application Load Balancers.

Pare a pilha

Parando uma pilha com o console

Captura de tela desse tipo de alteração no console AMS:

Como funciona:

1. Navegue até a página Criar RFC: No painel de navegação esquerdo do console AMS, clique RFCspara abrir a página da RFCs lista e, em seguida, clique em Criar RFC.
2. Escolha um tipo de alteração popular (CT) na visualização padrão Procurar tipos de alteração ou selecione uma CT na visualização Escolher por categoria.
   - Navegar por tipo de alteração: você pode clicar em um CT popular na área de criação rápida para abrir imediatamente a página Executar RFC. Observe que você não pode escolher uma versão mais antiga do CT com a criação rápida.

Para classificar CTs, use a área Todos os tipos de alteração na exibição Cartão ou Tabela. Em qualquer exibição, selecione uma CT e clique em Criar RFC para abrir a página Executar RFC. Se aplicável, a opção Criar com uma versão mais antiga aparece ao lado do botão Criar RFC.

- Escolha por categoria: selecione uma categoria, subcategoria, item e operação e a caixa de detalhes do CT será aberta com a opção Criar com uma versão mais antiga, se aplicável. Clique em Criar RFC para abrir a página Executar RFC.

3. Na página Executar RFC, abra a área do nome do CT para ver a caixa de detalhes do CT. É necessário um Assunto (preenchido se você escolher seu CT na visualização Procurar tipos de alteração). Abra a área Configuração adicional para adicionar informações sobre o RFC.

   Na área Configuração de execução, use as listas suspensas disponíveis ou insira valores para os parâmetros necessários. Para configurar parâmetros de execução opcionais, abra a área Configuração adicional.

4. Ao terminar, clique em Executar. Se não houver erros, a página RFC criada com sucesso será exibida com os detalhes da RFC enviada e a saída inicial de execução.

5. Abra a área Parâmetros de execução para ver as configurações que você enviou. Atualize a página para atualizar o status de execução do RFC. Opcionalmente, cancele a RFC ou crie uma cópia dela com as opções na parte superior da página.

Interrompendo uma pilha com a CLI

Como funciona:

1. Use o Inline Create (você emite um `create-rfc` comando com todos os parâmetros de RFC e execução incluídos) ou o Template Create (você cria dois arquivos JSON, um para os parâmetros RFC e outro para os parâmetros de execução) e emita o `create-rfc` comando com os dois arquivos como entrada. Ambos os métodos são descritos aqui.
2. Envie o `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: com o ID RFC retornado.

   Monitore o `aws amscm get-rfc --rfc-id` *`ID`* comando RFC:.

Para verificar a versão do tipo de alteração, use este comando:

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

> **Note**
>
> Você pode usar qualquer `CreateRfc` parâmetro com qualquer RFC, independentemente de eles fazerem parte do esquema para o tipo de alteração. Por exemplo, para receber notificações quando o status da RFC mudar, adicione essa linha `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` à parte dos parâmetros da RFC da solicitação (não aos parâmetros de execução). Para obter uma lista de todos os CreateRfc parâmetros, consulte a Referência da API de gerenciamento de alterações do AMS.

CRIAÇÃO EM LINHA:

Execute o comando create RFC com os parâmetros de execução fornecidos em linha (aspas de escape ao fornecer parâmetros de execução em linha) e, em seguida, envie a ID de RFC retornada. Por exemplo, você pode substituir o conteúdo por algo assim:

```
aws amscm create-rfc --change-type-id "ct-3dgbnh6gpst4d" --change-type-version "1.0" --
title "Stop My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CRIAÇÃO DE MODELO:

1. Envie o modelo RFC para um arquivo na sua pasta atual. Este exemplo o chama de StopStackRfc .json. Observe que, como há apenas um parâmetro de execução para interromper (reinicializar ou iniciar) uma instância, o parâmetro de execução pode estar no próprio arquivo JSON do esquema e não há necessidade de criar um arquivo JSON de parâmetros de execução separado.

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

2. Modifique e salve o StopStackRfc arquivo.json. Por exemplo, você pode substituir o conteúdo por algo assim:

   ```
   {
   "ChangeTypeId":          "ct-3dgbnh6gpst4d",
   "Title":                 "Stop-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
   ```

```
    }"
}
```

3. Crie o RFC:

```
aws amscm create-rfc --cli-input-json file://StopInstanceRfc.json
```

Você recebe a ID da nova RFC na resposta e pode usá-la para enviar e monitorar a RFC. Até que você o envie, o RFC permanece no estado de edição e não inicia.

Dicas

As instâncias interrompidas permanecem paradas, a menos que você tenha programado reinicializações usando o Agendador de Recursos do AMS.

Se necessário, consulte EC2 Instance stack stop fail.

Exemplos de acesso

Esses exemplos mostram como fazer login em uma instância por meio de um bastion depois de receber acesso por meio de um RFC. Para obter detalhes sobre como obter acesso concedido, consulte Solicitações de acesso.

> **Note**
>
> Uma EC2 instância criada por meio de um grupo de Auto Scaling terá um endereço IP que entra e sai, e você precisará usar seu EC2 console para encontrar esse endereço IP.

Dados necessários:

- Nome ou endereço IP amigável do Bastion DNS: use um nome amigável do DNS conforme descrito em Nomes de bastiões compatíveis com DNS ou encontre os endereços IP do Bastion conforme descrito em. Encontrando endereços IP do Bastion
- Nome de usuário (por exemplo, username@customerdomain.com) e senha: credenciais da conta.
- Endereço IP da pilha: veja isso consultando a página Pilhas do console AMS da pilha na qual você deseja fazer login e, em seguida, filtrando essa ID da pilha no console da EC2 sua conta. Para uma única EC2 instância, você também pode usar o comando AMS SKMS. Para a referência da API AMS SKMS, consulte a guia Relatórios no AWS Artifact Console. para encontrar o ID da pilha

e, em seguida, para a referência da API AMS SKMS, consulte a guia Relatórios no AWS Artifact Console. para encontrar o endereço IP da pilha.

Acesse o endereço IP do bastion, SSH ou RDP, conforme apropriado, e faça login usando um dos procedimentos a seguir.

Computador Linux para instância Linux

Use o SSH para se conectar ao SSH bastion e depois à instância Linux.

MALZ

Para obter mais informações sobre os nomes amigáveis dos bastiões, consulte DNS bastions.

Para se conectar à instância Linux, você deve primeiro se conectar a um bastião SSH.

1. Abra uma janela de shell e digite:

```
ssh Domain_FQDN\\Username@SSH_bastion_name
    or SSH_bastion_IP
```

O que ficaria assim se seu domínio_FQDN fosse “corp.domain.com”, seu número de conta fosse “123456789123", seu domínio_domínio fosse “amazonaws.com”, você escolhesse bastião “4" e seu nome de usuário fosse" “: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. Faça login com suas credenciais corporativas do Active Directory.
3. Ao receber um prompt do Bash, entre por SSH na instância e, em seguida, digite:

```
ssh Domain_FQDN\\Username@Instance_IP
```

Ou você pode usar o sinalizador de login (-l):

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

Para obter mais informações sobre os nomes amigáveis dos bastiões, consulte DNS bastions.

Para se conectar à instância Linux, você deve primeiro se conectar a um bastião SSH.

1. Abra uma janela de shell e digite:

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name
    or SSH_BASTION_IP
```

O que ficaria assim se o número da sua conta fosse 123456789123, você escolhesse bastion 4 e seu nome de usuário fosse: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. Faça login com suas credenciais corporativas do Active Directory.
3. Ao receber um prompt do Bash, entre por SSH na instância e, em seguida, digite:

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Ou você pode usar o sinalizador de login (-l):

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Computador Linux para instância Windows

Use um túnel SSH e um cliente RDP para se conectar a uma instância do Windows a partir do seu computador Linux.

MALZ

Esse procedimento requer um cliente de Conexão de Área de Trabalho Remota para Linux; o exemplo usa o Microsoft Remote Desktop (um cliente UNIX de código aberto para conexão com os Serviços de Área de Trabalho Remota do Windows). O Rdesktop é uma alternativa.

> **Note**
>
> A forma como você faz login nas instâncias do Windows pode mudar com base no cliente de desktop remoto que está sendo usado.

Primeiro, você estabelece um túnel SSH e depois faz login.

Para obter mais informações sobre os nomes amigáveis dos bastiões, consulteNomes de bastiões compatíveis com DNS.

Antes de começar

- Solicite acesso à instância à qual você deseja se conectar; para obter informações, consulte Solicitações de acesso.
- Escolha um nome de bastião DNS SSH amigável para se conectar; por exemplo:

```
sshbastion(1-4).Your_Domain
```

O que ficaria assim se seu domain_FQDN fosse “corp.domain.com”, seu Your_Domain gerenciado pelo AMS fosse “amazonaws.com”, você escolhesse bastion “4" e seu nome de usuário fosse" “: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- Encontre o endereço IP da instância à qual você quer se conectar; para obter mais informações, consulte Como encontrar uma ID de instância ou endereço IP.

1. Configure o RDP em um túnel SSH de um desktop Linux para uma instância do Windows. Para emitir o `ssh` comando com os valores corretos, há algumas maneiras de proceder:

   - No shell do Linux, defina as variáveis e, em seguida, insira o comando de conexão 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
   ```

   Exemplo, se os seguintes valores forem usados:

   ```
   BASTION="sshbastion4.A123456789123.amazonaws.com"

   WINDOWS="172.16.3.254"

   AD="ACORP_example"
   ```

```
USER="john.doe"
```

- Adicione os valores das variáveis diretamente ao `ssh` comando.

Em ambos os casos, isso é o que a solicitação renderizada seria (assumindo o mesmo conjunto de valores variáveis):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
```

2. Ou: Abra o Cliente de Área de Trabalho Remota, digite o endereço de loopback e a porta 127.0.0. 1:3389 e, em seguida, abra a conexão.

   Ou faça login na instância do Windows usando um novo shell de desktop Linux. Se você usar RDesktop, o comando terá a seguinte aparência:

   ```
   rdesktop 127.0.0.1:3389
   ```

   Uma janela de área de trabalho remota para a instância do Windows aparece na sua área de trabalho Linux.

   > **Tip**
   >
   > Se a sessão da área de trabalho remota não for iniciada, verifique se a conectividade de rede com a instância do Windows a partir do SSH bastion é permitida na porta 3389 do shell na etapa 1 (substitua adequadamente): `private_ip_address_of_windows_instance`
   >
   > ```
   > nc private_ip_address_of_windows_instance 3389 -v -z
   > ```
   >
   > Sucesso:
   >
   > ```
   > 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

Esse procedimento para uma landing zone de conta única requer um cliente de Conexão de Área de Trabalho Remota para Linux; o exemplo usa o Microsoft Remote Desktop (um cliente UNIX de código aberto para conexão com os Serviços de Área de Trabalho Remota do Windows). O Rdesktop é uma alternativa.

> **Note**
>
> A forma como você faz login nas instâncias do Windows pode mudar com base no cliente de desktop remoto que está sendo usado.

Primeiro, você estabelece um túnel SSH e depois faz login.

Para obter mais informações sobre os nomes amigáveis dos bastiões, consulteNomes de bastiões compatíveis com DNS.

Antes de começar

- Solicite acesso à instância à qual você deseja se conectar; para obter informações, consulte Solicitações de acesso.
- Escolha um nome de bastião DNS SSH amigável para se conectar; por exemplo:

  ```
  sshbastion(1-4).AAMSAccountNumber.amazonaws.com
  ```

  O que ficaria assim se o número da sua conta fosse 123456789123 e você escolhesse o bastião 4:

  ```
  sshbastion4.A123456789123.amazonaws.com
  ```

- Encontre o endereço IP da instância à qual você quer se conectar; para obter mais informações, consulte Como encontrar uma ID de instância ou endereço IP.

1. Configure o RDP em um túnel SSH de um desktop Linux para uma instância do Windows. Para emitir o `ssh` comando com os valores corretos, há algumas maneiras de proceder:

   - No shell do Linux, defina as variáveis e, em seguida, insira o comando de conexão 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
```

Exemplo, se os seguintes valores forem usados:

```
BASTION="sshbastion4.A123456789123.amazonaws.com"

WINDOWS="172.16.3.254"

AD="ACORP_example"

USER="john.doe"
```

- Adicione os valores das variáveis diretamente ao `ssh` comando.

Em ambos os casos, isso é o que a solicitação renderizada seria (assumindo o mesmo conjunto de valores variáveis):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. Ou: Abra o Cliente de Área de Trabalho Remota, digite o endereço de loopback e a porta 127.0.0. 1:3389 e, em seguida, abra a conexão.

   Ou faça login na instância do Windows usando um novo shell de desktop Linux. Se você usar RDesktop, o comando terá a seguinte aparência:

   ```
   rdesktop 127.0.0.1:3389
   ```

   Uma janela de área de trabalho remota para a instância do Windows aparece na sua área de trabalho Linux.

   > **Tip**
   >
   > Se a sessão da área de trabalho remota não for iniciada, verifique se a conectividade de rede com a instância do Windows a partir do SSH bastion

é permitida na porta 3389 do shell na etapa 1 (substitua adequadamente): `private_ip_address_of_windows_instance`

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

Sucesso:

```
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
```

Computador Windows para instância Windows

Use o cliente de Conexão de Área de Trabalho Remota do Windows para se conectar a uma instância do Windows a partir do seu computador Windows.

MALZ

Para obter mais informações sobre os nomes amigáveis dos bastiões, consulteNomes de bastiões compatíveis com DNS.

1. Abra o programa Remote Desktop Connection, um programa padrão do Windows, e insira o nome DNS amigável do Windows Bastion no campo hostname.

2. Selecione Conectar. A Conexão de Área de Trabalho Remota tenta uma conexão RDP com o bastião.

   Se for bem-sucedido, uma caixa de diálogo de credenciais será aberta. Para obter acesso, use suas credenciais corporativas do Active Directory, como você faria com a instância do Windows.

3. Abra o programa Conexão de Área de Trabalho Remota no bastion e insira o endereço IP da instância do Windows à qual você gostaria de se conectar (por exemplo, 10.0.0.100) e escolha Conectar. Suas credenciais corporativas do Active Directory são novamente necessárias antes de você se conectar à instância do Windows.

SALZ

Para obter mais informações sobre os nomes amigáveis dos bastiões, consulteNomes de bastiões compatíveis com DNS.

1. Abra o programa Conexão de Área de Trabalho Remota, um programa padrão do Windows, e digite o nome DNS amigável do Windows Bastion no campo do nome do host; por exemplo,`rdpbastion(1-4).AAMSAccountNumber.amazonaws.com`, que ficaria assim se o número da sua conta fosse 123456789123 e você escolhesse bastion 4,. `rdpbastion4.A123456789123.amazonaws.com`

2. Selecione Conectar. A Conexão de Área de Trabalho Remota tenta uma conexão RDP com o bastião.

   Se for bem-sucedido, uma caixa de diálogo de credenciais será aberta. Para obter acesso, use suas credenciais corporativas do Active Directory, como você faria com a instância do Windows.

3. Abra o programa Conexão de Área de Trabalho Remota no bastion e insira o endereço IP da instância do Windows à qual você gostaria de se conectar (por exemplo, 10.0.0.100) e escolha Conectar. Suas credenciais corporativas do Active Directory são novamente necessárias antes de você se conectar à instância do Windows.

Computador Windows para instância Linux

Para RDP para um bastião SSH a partir de um ambiente Windows, siga estas etapas.

MALZ

Antes de começar

- Solicite acesso à instância à qual você deseja se conectar; para obter informações, consulte Solicitações de acesso.
- Escolha um nome de bastião DNS SSH amigável para se conectar; por exemplo:

```
sshbastion(1-4).YOUR_DOMAIN
```

O que ficaria assim se YOUR_DOMAIN fosse “myamsaddomain.com” e você escolhesse o bastião 4:

```
sshbastion4.myamsaddomain.com
```

- Encontre o endereço IP da instância à qual você quer se conectar; para obter mais informações, consulte Como encontrar uma ID de instância ou endereço IP.

Para se conectar à instância Linux a partir da sua máquina Windows, você deve primeiro se conectar a um bastião SSH.

Use o cliente OpenSSH nativo do Windows ou instale o PuTTY em sua máquina local. Para saber mais sobre o OpenSSH, consulte OpenSSH no Windows.

1. Use o Windows nativo ou abra o PuTTY e insira o nome do host SSH bastion ou o endereço IP do SSH bastion. Por exemplo, 10.65.2.214 (22 é a porta usada para SSH; ela será definida por padrão).
2. O OpenSSH ou o PuTTY tentam uma conexão SSH com o bastião e abrem uma janela de shell.
3. Use suas credenciais corporativas do Active Directory da mesma forma que faria com os hosts RDP para obter acesso.
4. Quando apresentado com um prompt do Bash, use SSH para a instância. Insira:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

Antes de começar

- Solicite acesso à instância à qual você deseja se conectar; para obter informações, consulte Solicitações de acesso.
- Escolha um nome de bastião DNS SSH amigável para se conectar; por exemplo:

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

O que ficaria assim se o número da sua conta fosse 123456789123 e você escolhesse o bastião 4:

```
sshbastion4.A123456789123.amazonaws.com
```

- Encontre o endereço IP da instância à qual você quer se conectar; para obter mais informações, consulte Como encontrar uma ID de instância ou endereço IP.

Para se conectar à instância Linux a partir da sua máquina Windows, você deve primeiro se conectar a um bastião SSH.

Use o cliente OpenSSH nativo do Windows ou instale o PuTTY em sua máquina local. Para saber mais sobre o OpenSSH, consulte OpenSSH no Windows.

1. Use o Windows nativo ou abra o PuTTY e insira o nome do host SSH bastion ou o endereço IP do SSH bastion. Por exemplo, 10.65.2.214 (22 é a porta usada para SSH; ela será definida por padrão).
2. O OpenSSH ou o PuTTY tentam uma conexão SSH com o bastião e abrem uma janela de shell.
3. Use suas credenciais corporativas do Active Directory da mesma forma que faria com os hosts RDP para obter acesso.
4. Quando apresentado com um prompt do Bash, use SSH para a instância. Insira:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

Relatar um incidente

Use o console do AMS para relatar um incidente. É importante criar um novo incidente para cada novo problema ou pergunta. Ao abrir casos relacionados a consultas antigas, é útil incluir o número do caso relacionado para que possamos consultar a correspondência anterior.

> **Note**
>
> Se a correspondência do caso se afastar do problema original, um operador do AMS poderá solicitar que você relate um novo incidente.

Para relatar um incidente usando o console do AMS:

1. No painel de navegação à esquerda, escolha Incidentes

   A lista de incidentes é aberta:

   Se sua lista de incidentes estiver vazia, a opção Limpar filtro redefinirá o filtro para Qualquer status.

   Se você sabe que quer usar o telefone ou o chat, clique em Criar incidente na Central de Suporte para abrir a página Criar incidente no console da Central de Suporte, preenchida automaticamente com o tipo de serviço AMS.

   > **Important**
   >
   > - As chamadas telefônicas iniciadas com Suporte são gravadas para melhorar a resposta. Se a ligação cair, você deverá ligar de volta pelo gabinete do Support Center, AWS que não tem mecanismo para ligar de volta.
   > - O suporte por telefone e chat foi projetado para ajudar com casos de suporte, incidentes e solicitações de serviço, não com RFC ou problemas de segurança.
   > - Para problemas de RFC, use a opção de correspondência na página de detalhes da RFC relevante para entrar em contato com um engenheiro da AMS.
   > - Para problemas de segurança, crie um caso de suporte de alta prioridade (P1 ou P2). O recurso de bate-papo ao vivo não é para eventos de segurança.

2. Se você quiser encontrar um incidente existente, selecione um filtro de status do incidente na lista suspensa.

   - Todos os incidentes que ainda não foram resolvidos.
   - Um novo incidente que ainda não foi atribuído.
   - Um incidente que foi atribuído.

- Um incidente que você reabriu.
- Um incidente designado e complicado.
- Incidentes que exigem seu feedback antes da próxima etapa.
- Incidentes para os quais você enviou informações recentemente.
- Um incidente que foi concluído.
- Todos os incidentes na conta.

3. Escolha Criar.

   A página Criar um incidente é aberta:

4. Selecione uma prioridade:

   - Baixo: as funções não críticas do seu serviço ou aplicativo comercial relacionadas aos recursos AWS/AMS são afetadas.
   - Médio: um serviço ou aplicativo comercial relacionado aos recursos AWS/AMS é moderadamente afetado e está funcionando em um estado degradado.
   - Alto: sua empresa é significativamente impactada. As funções críticas do seu aplicativo relacionadas aos recursos AWS/AMS não estão disponíveis. Reservado para as interrupções mais críticas que afetam os sistemas de produção.

5. Selecione uma categoria.

   > **Note**
   >
   > Se você for testar a funcionalidade do incidente, adicione o sinalizador de não ação (AMSTestNoOpsActionRequired) ao título do incidente.

6. Insira as informações para:

   - Assunto: Um título descritivo para o relatório do incidente.
   - E-mails CC: uma lista de endereços de e-mail das pessoas que você deseja que sejam informadas sobre o relatório e a resolução do incidente.

- Detalhes: uma descrição abrangente do incidente, dos sistemas afetados e do resultado esperado da resolução. Responda às perguntas predefinidas ou exclua-as e insira as informações relevantes.

Para adicionar um anexo, escolha Adicionar anexo, navegue até o anexo desejado e clique em Abrir. Para excluir o anexo, clique no ícone Excluir:

7. Selecione Enviar.

   Uma página de detalhes é aberta com informações sobre o incidente, como Tipo, Assunto, Criado, ID e Status, e uma área de correspondência que inclui a descrição da solicitação que você criou.

   Clique em Responder para abrir uma área de correspondência e fornecer detalhes adicionais ou atualizações no status.

   Clique em Fechar caso quando o incidente for resolvido.

   Clique em Carregar mais se houver mais correspondência do que caberá em uma página.

   Não se esqueça de avaliar a comunicação!

   Seu incidente é exibido na página da lista de incidentes.

Criando uma solicitação de serviço

Para criar uma solicitação de serviço usando o console do AWS Managed Services (AMS):

1. No painel de navegação à esquerda, escolha Solicitações de serviço.

   A lista de solicitações de serviço é aberta.

   Se sua lista de solicitações de serviço estiver vazia, a opção Limpar filtro redefinirá o filtro para Qualquer status.

Se você sabe que quer usar o telefone ou o chat, clique em Criar solicitação de serviço na Central de Suporte para abrir a página Criar solicitação de serviço no console da Central de Suporte, preenchida automaticamente com o tipo de serviço AMS.

> **Note**
>
> As chamadas telefônicas iniciadas com o Suporte centro são gravadas, para melhorar a resposta. Se a ligação cair, você deverá ligar de volta pelo gabinete do Support Center, AWS que não tem mecanismo para ligar de volta.

> **Important**
>
> O suporte por telefone e chat foi projetado para ajudar com casos de suporte, incidentes e solicitações de serviço. Para problemas de RFC, use a opção de correspondência na página de detalhes da RFC relevante para entrar em contato com um engenheiro da AMS.

2. Se você quiser encontrar uma solicitação de serviço existente, selecione um filtro de status da solicitação de serviço na lista suspensa.

	• Todas as solicitações de serviço que ainda não foram resolvidas. • Uma nova solicitação de serviço que ainda não foi atribuída. • Uma solicitação de serviço que foi atribuída. • Uma solicitação de serviço que você reabriu. • Uma solicitação de serviço atribuída e complicada. • Solicitações de serviço que exigem seu feedback antes da próxima etapa. • Solicitações de serviço para as quais você enviou informações recentemente.

	• Uma solicitação de serviço que foi concluída. • Todas as solicitações de serviço na conta.

3. Escolha Criar.

   A página Criar uma solicitação de serviço é aberta.

4. Selecione uma categoria.

   > **Note**
   >
   > Se você for testar a funcionalidade da solicitação de serviço, adicione a sinalização de não ação,`AMSTestNoOpsActionRequired`. ao título da solicitação de serviço.

5. Insira as informações para:

   - Assunto: Isso cria um link para os detalhes da solicitação de serviço na página da lista.
   - E-mails CC: esses e-mails recebem correspondência além dos seus contatos de e-mail padrão.
   - Detalhes: forneça o máximo de informações possível aqui.

   Para adicionar um anexo, escolha Adicionar anexo, navegue até o anexo desejado e clique em Abrir. Para excluir o anexo, clique no ícone Excluir:

6. Selecione Enviar.

   Uma página de detalhes é aberta com informações sobre a solicitação de serviço, como Tipo, Assunto, Criação, ID e Status, e uma área de correspondência que inclui a descrição da solicitação que você criou.

   Além disso, sua solicitação de serviço é exibida na página da lista de solicitações de serviço. Use isso quando tiver um alerta, mas ainda não tiver ouvido falar do AMS.

   Clique em Responder para abrir uma área de correspondência e fornecer detalhes adicionais ou atualizações de status.

Clique em Resolver caso quando a solicitação de serviço tiver sido resolvida.

Clique em Carregar mais para ver correspondências adicionais que não cabem na página inicial.

Não se esqueça de avaliar a comunicação!

Para consultas relacionadas ao faturamento, use a categoria Outra no console do AMS, a API do `ChangeTypeId ct-1e1xtak34nx76` AMS CM ou a API do `IssueType=AMS` AWS Support.

Etapas de pós-integração

Agora que você criou uma conta AMS, você vai querer ler mais documentação do AMS. Veja esses documentos:

- Em seguida, os tutoriais para usar o HA Two-Tier stack CT para criar uma pilha totalmente funcional fornecem uma WordPress experiência completa de AMS.
- Guia do usuário do AMS: O Guia do usuário do AMS descreve a funcionalidade do AMS, lista os principais termos, operações e interfaces e fornece uma visão geral de uma arquitetura típica de infraestrutura gerenciada do AMS. Além disso, os detalhes do gerenciamento de acesso e os padrões do AMS são fornecidos. Também são fornecidas descrições detalhadas de como usar o sistema de gerenciamento de mudanças do AMS e várias orientações. Conceitos adicionais de gerenciamento também são descritos.
- Referência de API AMS: essa referência de API fornece descrições de todas as chamadas de API, incluindo solicitação, resposta e exemplos.
- Guia de aplicativos do AMS: O Guia do aplicativo do AMS descreve diferentes opções e métodos para implantar e manter seus aplicativos no AMS.

Tutoriais

Os tutoriais a seguir detalham as etapas para criar uma pilha de duas camadas com o CT de alta disponibilidade (avançado) (ct-06mjngx5flwto), usando a CLI e o console. Um tutorial é fornecido para implantar um grupo Linux Auto Scaling (ASG) e para implantar um Windows ASG.

As descrições de todas as opções de tomografia computadorizada, inclusive, ChangeTypeId podem ser encontradas na Referência de tipo de alteração do AMS.

Tutorial de CLI: pilha de duas camadas de alta disponibilidade (Linux/RHEL)

Esta seção descreve como implantar uma pilha de duas camadas de alta disponibilidade (HA) em um ambiente AMS usando a CLI do AMS.

> **Note**
>
> Esse passo a passo de implantação foi testado em ambientes AMZN Linux e RHEL.

Resumo das tarefas e tarefas necessárias RFCs:

1. Crie infraestrutura (pilha HA de dois níveis)
2. Crie um bucket S3 para aplicativos CodeDeploy
3. Crie o pacote de WordPress aplicativos e faça o upload para o bucket do S3
4. Implante o aplicativo com CodeDeploy
5. Acesse o WordPress site e faça login para validar a implantação

Antes de começar

O Deployment | Advanced Stack Components | High Availability Two Tier Stack Advanced | Create CT cria um grupo de Auto Scaling, um balanceador de carga, um banco de dados e CodeDeploy um nome de aplicativo e grupo de implantação (com o mesmo nome que você dá ao aplicativo). Para obter informações sobre, CodeDeploy consulte O que é CodeDeploy?

Este passo a passo usa uma RFC de pilha de duas camadas de alta disponibilidade (avançada) que inclui UserData e também descreve como criar um WordPress pacote que pode ser implantado. CodeDeploy

O exemplo `UserData` mostrado no exemplo obtém metadados da instância, como ID da instância, região etc., de dentro de uma instância em execução, consultando o serviço de metadados da EC2 instância disponível em http://169.254.169.254/latest/meta-data/. Essa linha no script de dados do usuário:`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, recupera o nome da zona de disponibilidade do serviço de metadados na variável $REGION de nossas regiões suportadas e a usa para preencher a URL do bucket do S3 em que o agente é baixado. CodeDeploy O IP 169.254.169.254 é roteável somente dentro da VPC (todos podem consultar o serviço). VPCs Para obter informações sobre

o serviço, consulte Metadados da instância e dados do usuário. Observe também que os scripts inseridos como UserData são executados como usuário “root” e não precisam usar o comando “sudo”.

Essa explicação passo a passo deixa os seguintes parâmetros no valor padrão (mostrado):

- Grupo de 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`
- Balanceador de carga:. `HealthCheckInterval=30, HealthCheckTimeout=5`
- Banco de dados:`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`.
- Aplicação:`DeploymentConfigName=CodeDeployDefault.OneAtATime`.
- Balde S3:`AccessControl=Private`.

CONFIGURAÇÕES ADICIONAIS:

`RequestedStartTimee RequestedEndTime` se você quiser agendar sua RFC: você pode usar Time.is para determinar a hora UTC correta. Os exemplos fornecidos devem ser ajustados adequadamente. Uma RFC não pode continuar se a hora de início tiver passado. Como alternativa, você pode deixar esses valores desativados para criar um ASAP RFC que seja executado assim que as aprovações forem aprovadas.

> **Note**
>
> Há muitos parâmetros que você pode escolher definir de forma diferente dos mostrados. Os valores desses parâmetros mostrados no exemplo foram testados, mas podem não ser adequados para você.

Crie a infraestrutura

Coletar os dados a seguir antes de começar fará com que a implantação seja mais rápida.

OS DADOS NECESSÁRIOS TÊM UMA PILHA:

- AutoScalingGroup:
  - `UserData`: esse valor é fornecido neste tutorial. Ele inclui comandos para configurar o recurso CodeDeploy e iniciar o CodeDeploy agente.
  - `AMI-ID`: esse valor determina que tipo de EC2 instâncias seu grupo de Auto Scaling (ASG) criará. Certifique-se de selecionar uma AMI em sua conta que comece com “cliente-” e seja do sistema operacional que você deseja. Encontre a AMI IDs com a referência da API For the AMS SKMS, consulte a guia Relatórios no AWS Artifact Console. operação (CLI: list-amis) ou no console do AMS -> página de detalhes. VPCs VPCs Este passo a passo é para ASGs configurar o uso de uma AMI Linux.
- Banco de dados:
  - Esses parâmetros,`DBEngine`,`EngineVersion`, e `LicenseModel` devem ser definidos de acordo com sua situação, embora os valores mostrados no exemplo tenham sido testados.
  - Esses parâmetros,`RDSSubnetIds`,, `DBNameMasterUsername`, e `MasterUserPassword` são necessários ao implantar o pacote de aplicativos. Para RDSSubnet IDs, use duas sub-redes privadas.
- LoadBalancer:
  - Esses parâmetros,`DBEngine`,`EngineVersion`, e `LicenseModel` devem ser definidos de acordo com sua situação, embora os valores mostrados no exemplo tenham sido testados.
  - `ELBSubnetIds`: Use duas sub-redes públicas.
- Aplicativo: o `ApplicationName` valor define o nome do CodeDeploy aplicativo e o nome do grupo de CodeDeploy implantação. Você o usa para implantar seu aplicativo. Ele deve ser exclusivo na conta. Para verificar os CodeDeploy nomes da sua conta, consulte o CodeDeploy console. O

exemplo usa "WordPress", mas, se você usar esse valor, certifique-se de que ele ainda não esteja em uso.

Esse procedimento utiliza a CT de duas camadas (avançada) de alta disponibilidade (ct-06mjngx5flwto) e a CT de armazenamento Create S3 (ct-1a68ck03fn98r). Na sua conta autenticada, siga estas etapas na linha de comando.

1. Inicie a pilha de infraestrutura.

   a. Envie os parâmetros de execução do esquema JSON para a pilha HA de duas camadas CT em um arquivo em sua pasta atual chamado .json. CreateStackParams

   ```
   aws amscm get-change-type-version --change-type-id "ct-06mjngx5flwto"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    CreateStackParams.json
   ```

   b. Modifique o esquema. Substitua o *`variables`* conforme apropriado. Por exemplo, use o sistema operacional que você deseja para as EC2 instâncias que o ASG criará. Grave o `ApplicationName` como você o usará posteriormente para implantar o aplicativo. Observe que você pode adicionar até 50 tags.

   ```
   {
   "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. Envie o modelo CreateRfc JSON para um arquivo na sua pasta atual chamado CreateStackRfc .json:

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

d. Modifique o modelo RFC da seguinte forma e salve-o, você pode excluir e substituir o conteúdo. Observe que `RequestedStartTime` agora `RequestedEndTime` são opcionais; excluí-los cria um ASAP RFC que é executado assim que aprovado (o que geralmente acontece automaticamente). Para enviar um RFC agendado, adicione esses valores.

```
{
"ChangeTypeVersion":    "3.0",
"ChangeTypeId":         "ct-06mjngx5flwto",
"Title":                "HA-Stack-For-WP-RFC"
}
```

e. Crie o RFC, especificando o CreateStackRfc arquivo.json e o arquivo de parâmetros de execução CreateStackParams .json:

```
aws amscm create-rfc --cli-input-json file://CreateStackRfc.json --execution-
parameters file://CreateStackParams.json
```

Você recebe o ID do RFC na resposta. Salve o ID para as etapas subsequentes.

f. Envie o RFC:

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

Se o RFC for bem-sucedido, você não receberá nenhuma saída.

g. Para verificar o status do RFC, execute

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

Anote o ID do RFC.

2. Inicie um bucket S3

Coletar os dados a seguir antes de começar fará com que a implantação seja mais rápida.

BUCKET S3 DE DADOS NECESSÁRIO:

- `VPC-ID`: esse valor determina onde seu S3 Bucket estará. Use a mesma VPC ID que você usou anteriormente.
- `BucketName`: esse valor define o nome do S3 Bucket, você o usa para carregar seu pacote de aplicativos. Ele deve ser exclusivo em toda a região da conta e não pode incluir letras maiúsculas. Incluir o ID da sua conta como parte do não BucketName é obrigatório, mas facilita a identificação posterior do bucket. Para ver quais nomes de bucket do S3 existem na conta, acesse o console do Amazon S3 da sua conta.

a. Envie os parâmetros de execução do esquema JSON para o armazenamento S3 create CT em um arquivo JSON chamado createS3 .json. StoreParams

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3StoreParams.json
```

b. Modifique o esquema da seguinte forma, você pode excluir e substituir o conteúdo. Substitua *VPC_ID* adequadamente. Os valores no exemplo foram testados, mas podem não ser adequados para você.

> **Tip**
>
> O `BucketName` deve ser exclusivo em toda a região da conta e não pode incluir letras maiúsculas. Incluir o ID da sua conta como parte do não BucketName é obrigatório, mas facilita a identificação posterior do bucket. Para ver quais nomes de bucket do S3 existem na conta, acesse o console do Amazon S3 da sua conta.

```
{
"Description":      "S3BucketForWordPressBundle",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-s2b72beb000000000",
"Name":             "S3BucketForWP",
"TimeoutInMinutes":  60,
"Parameters":   {
    "AccessControl":    "Private",
    "BucketName":       "ACCOUNT_ID-BUCKET_NAME"
    }
}
```

c. Envie o modelo JSON CreateRfc para um arquivo, na sua pasta atual, chamado StoreRfc createS3 .json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateS3StoreRfc.json
```

d. Modifique e salve o arquivo CreateS3 StoreRfc .json, você pode excluir e substituir o conteúdo. Observe que `RequestedStartTime` agora `RequestedEndTime` são opcionais; excluí-los cria um ASAP RFC que é executado assim que aprovado (o que geralmente acontece automaticamente). Para enviar um RFC agendado, adicione esses valores.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-1a68ck03fn98r",
"Title":                "S3-Stack-For-WP-RFC"
}
```

e. Crie o RFC, especificando o arquivo CreateS3 .json e o arquivo de parâmetros de execução CreateS3 StoreRfc .json: StoreParams

```
aws amscm create-rfc --cli-input-json file://CreateS3StoreRfc.json  --
execution-parameters file://CreateS3StoreParams.json
```

Você recebe o RfcId do novo RFC na resposta. Salve o ID para as etapas subsequentes.

f. Envie o RFC:

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

Se o RFC for bem-sucedido, você não receberá nenhuma saída.

g. Para verificar o status do RFC, execute

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

Crie, carregue e implante o aplicativo

Primeiro, crie um pacote de WordPress aplicativos e, em seguida, use o CodeDeploy CTs para criar e implantar o aplicativo.

1. Baixe WordPress, extraia os arquivos e crie um. diretório /scripts.

   Comando Linux:

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: cole `https://github.com/WordPress/WordPress/archive/master.zip` em uma janela do navegador e baixe o arquivo zip.

   Crie um diretório temporário no qual montar o pacote.

   Linux

   ```
   mkdir /tmp/WordPress
   ```

   Windows: Crie um diretório WordPress "", você usará o caminho do diretório posteriormente.

2. Extraia a WordPress fonte para o diretório WordPress "" e crie um. diretório /scripts.

   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: vá para o diretório WordPress "" que você criou e crie um diretório de “scripts” lá.

   Se você estiver em um ambiente Windows, certifique-se de definir o tipo de interrupção dos arquivos de script como Unix (LF). No Notepad ++, essa é uma opção na parte inferior direita da janela.

3. Crie o arquivo CodeDeploy appspec.yml, no WordPress diretório (se estiver copiando o exemplo, verifique o recuo, cada espaço conta). IMPORTANTE: Certifique-se de que o caminho de “origem” esteja correto para copiar os WordPress arquivos (nesse caso, em seu WordPress diretório) para o destino esperado (/var/www/html/WordPress). No exemplo, o arquivo appspec.yml está no diretório com os WordPress arquivos, portanto, somente “/” é necessário. Além disso, mesmo que você tenha usado uma AMI RHEL para seu grupo de Auto Scaling, deixe a linha “os: linux” como está. Exemplo de arquivo 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. Crie scripts de arquivo bash no WordPress . diretório /scripts.

   Primeiro, crie `config_wordpress.sh` com o conteúdo a seguir (se preferir, você pode editar o arquivo wp-config.php diretamente).

   > **Note**
   >
   > *DBName*Substitua pelo valor fornecido no HA Stack RFC (por exemplo,`wordpress`).
   > *DB_MasterUsername*Substitua pelo `MasterUsername` valor fornecido no HA Stack RFC (por exemplo,`admin`).
   > *DB_MasterUserPassword*Substitua pelo `MasterUserPassword` valor fornecido no HA Stack RFC (por exemplo,`p4ssw0rd`).
   > *DB_ENDPOINT*Substitua pelo nome DNS do endpoint nas saídas de execução do HA Stack RFC (por exemplo,). `srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com` Você pode encontrar isso na GetRfcoperação (CLI: get-rfc --rfc-id RFC_ID) ou na página de detalhes do RFC do console AMS para o HA Stack RFC que você enviou anteriormente.

```
#!/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. No mesmo diretório, crie `install_dependencies.sh` com o seguinte conteúdo:

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
```

```
yum install -y mysql
service httpd restart
```

> **Note**
>
> O HTTPS é instalado como parte dos dados do usuário no lançamento para permitir que as verificações de saúde funcionem desde o início.

6. No mesmo diretório, crie `start_server.sh` com o seguinte conteúdo:

   - Para instâncias do Amazon Linux, use isso:

   ```
   #!/bin/bash
   service httpd start
   ```

   - Para instâncias do RHEL, use isso (os comandos extras são políticas que permitem que o SELINUX aceite): 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. No mesmo diretório, crie `stop_server.sh` com o seguinte conteúdo:

   ```
   #!/bin/bash
   service httpd stop
   ```

8. Crie o pacote zip.

   Linux

   ```
   $ cd /tmp/WordPress
   $ zip -r wordpress.zip .
   ```

   Windows: Vá para o diretório WordPress "", selecione todos os arquivos e crie um arquivo zip, não se esqueça de chamá-lo de wordpress.zip.

1. Faça o upload do pacote de aplicativos no bucket do S3.

   O pacote precisa estar pronto para continuar implantando a pilha.

   Você tem acesso automático a qualquer instância de bucket do S3 que você criar. Você pode acessá-lo por meio de seus bastiões ou do console S3 e fazer o upload do WordPress pacote drag-and-drop ou navegar até o arquivo zip e selecioná-lo.

   Você também pode usar o seguinte comando em uma janela de shell; verifique se você tem o caminho correto para o arquivo zip:

   ```
   aws s3 cp wordpress.zip s3://BUCKET_NAME/
   ```

2. Implante o pacote de WordPress aplicativos.

   Coletar os dados a seguir antes de começar fará com que a implantação seja mais rápida.

   DADOS NECESSÁRIOS:

   - `VPC-ID`: esse valor determina onde seu S3 Bucket estará. Use a mesma VPC ID que você usou anteriormente.
   - `CodeDeployApplicationNameeCodeDeployApplicationName`: O `ApplicationName` valor que você usou no HA 2-Tier Stack RFC definiu o CodeDeployApplicationName e o. CodeDeployDeploymentGroupName O exemplo usa "WordPress", mas você pode ter usado um valor diferente.
   - `S3Location`: Para`S3Bucket`, use o `BucketName` que você criou anteriormente. Os `S3BundleType` e `S3Key` são do pacote que você colocou na sua loja S3.

   a. Exiba os parâmetros de execução do esquema JSON para o CodeDeploy aplicativo deploy CT em um arquivo JSON chamado Deploy Params.json. CDApp

      ```
      aws amscm get-change-type-version --change-type-id "ct-2edc3sd1sqmrb"
       --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
       DeployCDAppParams.json
      ```

   b. Modifique o esquema da seguinte forma e salve-o como, você pode excluir e substituir o conteúdo.

      ```
      {
      ```

```
"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. Envie o modelo JSON CreateRfc para um arquivo, na sua pasta atual, chamado Deploy CDApp RFC.json:

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

d. Modifique e salve o arquivo Deploy CDApp RFC.json, você pode excluir e substituir o conteúdo. Observe que `RequestedStartTime` agora `RequestedEndTime` são opcionais; excluí-los cria um ASAP RFC que é executado assim que aprovado (o que geralmente acontece automaticamente). Para enviar um RFC agendado, adicione esses valores.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-2edc3sd1sqmrb",
"Title":                "CD-Deploy-For-WP-RFC"
}
```

e. Crie o RFC, especificando o arquivo Deploy CDApp Rfc e o arquivo de parâmetros de execução do Deploy CDApp Params:

```
aws amscm create-rfc --cli-input-json file://DeployCDAppRfc.json  --execution-
parameters file://DeployCDAppParams.json
```

Você recebe o RfcId do novo RFC na resposta. Salve o ID para as etapas subsequentes.

f. Envie o RFC:

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

Se o RFC for bem-sucedido, você não receberá nenhuma saída.

g. Para verificar o status do RFC, execute

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

Validar a implantação do aplicativo

Navegue até o endpoint (ELB CName) do balanceador de carga criado anteriormente, com o caminho implantado:/. WordPress WordPress Por exemplo:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

Elimine a implantação de aplicativos

Depois de concluir o tutorial, você deverá desmontar a implantação para não ser cobrado pelos recursos.

A seguir está uma operação genérica de exclusão de pilha. Você vai querer enviá-lo duas vezes, uma para a pilha HA de 2 níveis e outra para a pilha de buckets S3. Como acompanhamento final, envie uma solicitação de serviço para que todos os snapshots do bucket do S3 (incluindo o ID da pilha do bucket do S3 na solicitação de serviço) sejam excluídos. Eles são excluídos automaticamente após 10 dias, mas excluí-los antecipadamente economiza um pouco de custo.

Este passo a passo fornece um exemplo do uso do console AMS para excluir uma pilha do S3; esse procedimento se aplica à exclusão de qualquer pilha usando o console do AMS.

> **Note**
>
> Se você excluir um bucket do S3, primeiro ele deverá ser esvaziado de objetos.

DADOS NECESSÁRIOS:

- `StackId`: A pilha a ser usada. Você pode encontrar isso acessando a página AMS Console Stacks, disponível por meio de um link no painel de navegação esquerdo. Usando a API/CLI do AMS SKMS, execute a referência da API Para o AMS SKMS, consulte a guia Relatórios no AWS Artifact Console. operação (na CLI). `list-stack-summaries`
- O ID do tipo de alteração para este passo a passo `éct-0q0bic0ywqk6c`: a versão é “1.0". Para descobrir a versão mais recente, execute este comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-0q0bic0ywqk6c
```

CRIAÇÃO EM LINHA:

- Execute o comando create RFC com os parâmetros de execução fornecidos em linha (aspas de escape ao fornecer parâmetros de execução em linha). E

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0"
 --title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

- Envie a RFC usando a ID da RFC retornada na operação de criação da RFC. Até ser enviada, a RFC permanece no `Editing` estado e não é aplicada.

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

- Monitore o status da RFC e visualize a saída da execução:

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

CRIAÇÃO DE MODELO:

1. Envie o modelo RFC para um arquivo em sua pasta atual; o exemplo o chama de DeleteStackRfc .json:

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

2. Modifique e salve o DeleteStackRfc arquivo.json. Como a exclusão de uma pilha tem apenas um parâmetro de execução, os parâmetros de execução podem estar no próprio DeleteStackRfc

arquivo.json (não há necessidade de criar um arquivo JSON separado com parâmetros de execução).

As aspas internas na extensão ExecutionParameters JSON devem ser excluídas com uma barra invertida (\). Exemplo sem horário de início e término:

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-0q0bic0ywqk6c",
"Title":                "Delete-My-Stack-RFC"
"ExecutionParameters":  "{
        \"StackId\":\"STACK_ID\"}"
}
```

3. Crie o RFC:

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
```

Você recebe o RfcId do novo RFC na resposta. Por exemplo:

```
{
"RfcId": "daaa1867-ffc5-1473-192a-842f6b326102"
}
```

Salve o ID para as etapas subsequentes.

4. Envie o RFC:

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

Se o RFC for bem-sucedido, você não receberá nenhuma confirmação na linha de comando.

5. Para monitorar o status da solicitação e visualizar a Saída de Execução:

```
aws amscm get-rfc --rfc-id RFC_ID --query "Rfc.
{Status:Status.Name,Exec:ExecutionOutput}" --output table
```

Tutorial do console: pilha de dois níveis de alta disponibilidade (Linux/RHEL)

Esta seção descreve como implantar um WordPress site de alta disponibilidade (HA) em um ambiente AMS usando o console AMS.

> **Note**
>
> Esse passo a passo de implantação foi testado em ambientes AMZN Linux e RHEL.

Resumo das tarefas e tarefas necessárias RFCs:

1. Crie infraestrutura (pilha HA de dois níveis)
2. Crie um bucket S3 para aplicativos CodeDeploy
3. Crie o pacote de WordPress aplicativos e faça o upload para o bucket do S3
4. Implante o aplicativo com CodeDeploy
5. Acesse o WordPress site e faça login para validar a implantação
6. Destrua a implantação

As descrições de todas as opções de tomografia computadorizada ChangeTypeId, inclusive, podem ser encontradas na Referência de tipo de alteração do AMS.

Antes de começar

O Deployment | Advanced Stack Components | High Availability Two Tier Stack | Create CT cria um grupo de Auto Scaling, um balanceador de carga, um banco de dados e CodeDeploy um nome de aplicativo e grupo de implantação (com o mesmo nome que você dá ao aplicativo). Para obter informações sobre, CodeDeploy consulte O que é CodeDeploy?

Este passo a passo usa um RFC de pilha de duas camadas de alta disponibilidade que inclui `UserData` e também descreve como criar um WordPress pacote que pode ser implantado. CodeDeploy

O exemplo `UserData` mostrado no exemplo obtém metadados da instância, como ID da instância, região etc., de dentro de uma instância em execução, consultando o serviço de metadados da EC2 instância disponível em http://169.254.169.254/latest/meta-data/. Essa linha no script de dados do usuário:`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, recupera o nome da zona de disponibilidade do

serviço de metadados na variável $REGION de nossas regiões suportadas e a usa para preencher a URL do bucket do S3 em que o agente é baixado. CodeDeploy O IP 169.254.169.254 é roteável somente dentro da VPC (todos podem consultar o serviço). VPCs Para obter informações sobre o serviço, consulte Metadados da instância e dados do usuário. Observe também que os scripts inseridos como UserData são executados como usuário “root” e não precisam usar o comando “sudo”.

Essa explicação passo a passo deixa os seguintes parâmetros no valor padrão (mostrado):

- Grupo de 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`
- Balanceador de carga:. `HealthCheckInterval=30, HealthCheckTimeout=5`
- Banco de dados:`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`.
- Aplicação:`DeploymentConfigName=CodeDeployDefault.OneAtATime`.

Parâmetros variáveis:

O console fornece uma opção ASAP para a hora de início e este passo a passo recomenda usá-la. O ASAP faz com que o RFC seja executado assim que as aprovações forem aprovadas.

> **Note**
>
> Há muitos parâmetros que você pode escolher definir de forma diferente dos mostrados. Os valores desses parâmetros mostrados no exemplo foram testados, mas podem não ser

adequados para você. Somente os valores obrigatórios são mostrados nos exemplos. Os valores na *replaceable* fonte devem ser alterados, pois são específicos da sua conta.

Crie a infraestrutura

Esse procedimento utiliza a CT de pilha de duas camadas de alta disponibilidade seguida pela CT de armazenamento Create S3.

Coletar os dados a seguir antes de começar fará com que a implantação seja mais rápida.

OS DADOS NECESSÁRIOS TÊM UMA PILHA:

- AutoScalingGroup:
  - UserData: esse valor é fornecido neste tutorial. Ele inclui comandos para configurar o recurso CodeDeploy e iniciar o CodeDeploy agente.
  - AMI-ID: esse valor determina o sistema operacional das EC2 instâncias que seu grupo de Auto Scaling (ASG) criará. Selecione uma AMI em sua conta que comece com “cliente-” e seja do sistema operacional que você deseja. Encontre a AMI IDs no console do AMS VPCs -> página de VPCs detalhes. Este passo a passo é para ASGs configurar o uso de uma AMI Amazon Linux ou RHEL.
- Banco de dados:
  - Esses parâmetros, DBEngine, EngineVersion, e LicenseModeldevem ser definidos de acordo com sua situação, embora os valores mostrados no exemplo tenham sido testados. O tutorial usa esses valores, respectivamente:*MySQL*,*8.0.16*,*general-public-license*.
  - Esses parâmetros, DBName, MasterUserPassword, e MasterUsernamesão necessários ao implantar o pacote de aplicativos. O tutorial usa esses valores, respectivamente:*wordpressDB*,*p4ssw0rd*,*admin*. Observe que só DBName pode conter caracteres alfanuméricos.
  - Quando você insere o MasterUsernamepara o banco de dados do RDS, ele aparecerá em texto não criptografado, então faça login no banco de dados o mais rápido possível e altere a senha para garantir sua segurança.
  - Para RDSSubnetIDs, use duas sub-redes privadas. Digite-os um de cada vez, pressionando “Enter” após cada um. Encontre Subnet IDs com a referência da API For the AMS SKMS, consulte a guia Relatórios na operação do AWS Artifact Console. (CLI list-subnet-summaries:) ou no console AMS -> página de detalhes da VPC. VPCs
- LoadBalancer:

- Defina esse parâmetro, Public como true, pois o tutorial usa sub-redes públicas do ELB.
- ELBSubnetIDs: Use duas sub-redes públicas. Digite-os um de cada vez, pressionando “Enter” após cada um. Encontre Subnet IDs com a referência da API For the AMS SKMS, consulte a guia Relatórios na operação do AWS Artifact Console. (CLI list-subnet-summaries:) ou no console AMS -> página de detalhes da VPC. VPCs

- Aplicativo: o ApplicationNamevalor define o nome do CodeDeploy aplicativo e o nome do grupo de CodeDeploy implantação. Você o usa para implantar seu aplicativo. Ele deve ser exclusivo na conta. Para verificar os CodeDeploy nomes da sua conta, consulte o CodeDeploy console. O exemplo usa, *`WordPress`* mas, se você usar esse valor, certifique-se de que ele ainda não esteja em uso.

1. Inicie a pilha de alta disponibilidade.

   a. Na página Criar RFC, selecione a categoria Implantação, a subcategoria Pilhas padrão, o item Pilha de duas camadas de alta disponibilidade e a operação Criar, na lista.

   b. IMPORTANTE: Escolha Avançado e defina os valores conforme mostrado.

      Você só precisa inserir valores para as opções marcadas com estrela (*); os valores testados são mostrados no exemplo; você pode deixar as opções vazias não obrigatórias em branco.

   c. Para a seção Descrição do RFC:

      ```
      Subject: WP-HA-2-Tier-RFC
      ```

   d. Para a seção Informações sobre recursos, defina parâmetros para AutoScalingGroupBanco de Dados LoadBalancer, Aplicativo e Tags.

      Além disso, o objetivo da chave de tag AppName "" é que você possa pesquisar facilmente as instâncias do ASG no EC2 console; você pode chamar essa chave de tag de “Nome” ou qualquer outro nome de chave que desejar. Observe que você pode adicionar até 50 tags.

      ```
      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. Clique em Enviar quando terminar.

2. Faça login no banco de dados que você criou e altere a senha.
3. Inicie um bucket Stack do S3.

   Coletar os dados a seguir antes de começar fará com que a implantação seja mais rápida.

   BUCKET S3 DE DADOS NECESSÁRIO:

   - VPC-ID: esse valor determina onde seu S3 Bucket estará. Encontre uma VPC IDs com a referência da API For the AMS SKMS, consulte a guia Relatórios na operação do AWS Artifact Console. (CLI:) ou na página do console AMS. list-vpc-summaries VPCs

- BucketName: esse valor define o nome do S3 Bucket, você o usa para carregar seu pacote de aplicativos. Ele deve ser exclusivo em toda a região da conta e não pode incluir letras maiúsculas. Incluir o ID da sua conta como parte do não BucketName é obrigatório, mas facilita a identificação posterior do bucket. Para ver quais nomes de bucket do S3 existem na conta, acesse o console do Amazon S3 da sua conta.

a. Na página Criar RFC, selecione a categoria Implantação, a subcategoria Advanced Stack Components, o item Armazenamento S3 e a operação Criar na lista de opções RFC CT.

b. Mantenha a opção Básica padrão e defina os valores conforme mostrado.

```
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. Clique em Enviar quando terminar. O bucket implantado com esse tipo de alteração permite read/write acesso total a toda a conta.

Crie, carregue e implante o aplicativo

Primeiro, crie um pacote de WordPress aplicativos e, em seguida, use o CodeDeploy CTs para criar e implantar o aplicativo.

1. Baixe WordPress, extraia os arquivos e crie um. diretório /scripts.

   Comando Linux:

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: cole `https://github.com/WordPress/WordPress/archive/master.zip` em uma janela do navegador e baixe o arquivo zip.

   Crie um diretório temporário no qual montar o pacote.

   Linux

```
mkdir /tmp/WordPress
```

Windows: Crie um diretório WordPress "", você usará o caminho do diretório posteriormente.

2. Extraia a WordPress fonte para o diretório WordPress "" e crie um. diretório /scripts.

   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: vá para o diretório WordPress "" que você criou e crie um diretório de “scripts” lá.

   Se você estiver em um ambiente Windows, certifique-se de definir o tipo de interrupção dos arquivos de script como Unix (LF). No Notepad ++, essa é uma opção na parte inferior direita da janela.

3. Crie o arquivo CodeDeploy appspec.yml, no WordPress diretório (se estiver copiando o exemplo, verifique o recuo, cada espaço conta). IMPORTANTE: Certifique-se de que o caminho de “origem” esteja correto para copiar os WordPress arquivos (nesse caso, em seu WordPress diretório) para o destino esperado (/var/www/html/WordPress). No exemplo, o arquivo appspec.yml está no diretório com os WordPress arquivos, portanto, somente “/” é necessário. Além disso, mesmo que você tenha usado uma AMI RHEL para seu grupo de Auto Scaling, deixe a linha “os: linux” como está. Exemplo de arquivo 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. Crie scripts de arquivo bash no WordPress . diretório /scripts.

   Primeiro, crie `config_wordpress.sh` com o conteúdo a seguir (se preferir, você pode editar o arquivo wp-config.php diretamente).

   > **Note**
   >
   > *DBName*Substitua pelo valor fornecido no HA Stack RFC (por exemplo,`wordpress`).
   > *DB_MasterUsername*Substitua pelo `MasterUsername` valor fornecido no HA Stack RFC (por exemplo,`admin`).
   > *DB_MasterUserPassword*Substitua pelo `MasterUserPassword` valor fornecido no HA Stack RFC (por exemplo,`p4ssw0rd`).
   > *DB_ENDPOINT*Substitua pelo nome DNS do endpoint nas saídas de execução do HA Stack RFC (por exemplo,). `srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com` Você pode encontrar isso na GetRfcoperação (CLI: get-rfc --rfc-id RFC_ID) ou na página de detalhes do RFC do console AMS para o HA Stack RFC que você enviou anteriormente.

```
#!/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. No mesmo diretório, crie `install_dependencies.sh` com o seguinte conteúdo:

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> O HTTPS é instalado como parte dos dados do usuário no lançamento para permitir que as verificações de saúde funcionem desde o início.

6. No mesmo diretório, crie `start_server.sh` com o seguinte conteúdo:

   - Para instâncias do Amazon Linux, use isso:

```
#!/bin/bash
service httpd start
```

   - Para instâncias do RHEL, use isso (os comandos extras são políticas que permitem que o SELINUX aceite): 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. No mesmo diretório, crie `stop_server.sh` com o seguinte conteúdo:

```
#!/bin/bash
service httpd stop
```

8. Crie o pacote zip.

   Linux

```
$ cd /tmp/WordPress
```

```
$ zip -r wordpress.zip .
```

Windows: Vá para o diretório WordPress "", selecione todos os arquivos e crie um arquivo zip, não se esqueça de chamá-lo de wordpress.zip.

1. Faça o upload do pacote de aplicativos para o bucket do S3

   O pacote precisa estar pronto para continuar implantando a pilha.

   Você tem acesso automático a qualquer instância de bucket do S3 que você criar. Você pode acessá-lo por meio de seu Bastions (consulte Instâncias de acesso) ou por meio do console S3 e fazer o upload do CodeDeploy pacote com drag-and-drop, ou navegando até o arquivo e selecionando-o.

   Você também pode usar o seguinte comando em uma janela de shell; verifique se você tem o caminho correto para o arquivo zip:

   ```
   aws s3 cp wordpress/wordpress.zip s3://BUCKET_NAME/
   ```

2. Implantar o pacote WordPress CodeDeploy de aplicativos

   CÓDIGO DE DADOS NECESSÁRIO/IMPLANTAÇÃO DO APLICATIVO:

   - CodeDeployApplicationName: O nome que você deu ao CodeDeploy aplicativo.
   - CodeDeployGroupName: Como o CodeDeploy aplicativo e o grupo foram criados a partir do nome que você deu ao CodeDeploy aplicativo na RFC da pilha HA, esse é o mesmo nome do. CodeDeployApplicationName
   - S3Bucket: O nome que você deu ao bucket S3.
   - S3 BundleType e S3Key: fazem parte do pacote de WordPress aplicativos que você implantou.
   - VpcId: A VPC relevante.

   a. Na página Criar RFC, selecione a categoria Implantação, subcategoria Aplicativos, item CodeDeploy aplicativo e operação Implantar na lista de opções RFC CT.

   b. Mantenha a opção Básica padrão e defina os valores conforme mostrado.

> **Note**
>
> Faça referência ao CodeDeploy aplicativo, ao grupo de CodeDeploy implantação, ao bucket S3 e ao pacote criados anteriormente.

```
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. Clique em Enviar quando terminar.

Validar a implantação do aplicativo

Navegue até o endpoint (LoadBalancerCName) do balanceador de carga criado anteriormente, com o WordPress caminho implantado:/. WordPress Por exemplo:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

Você deve ver uma página como esta:

Elimine a implantação de alta disponibilidade

Para reduzir a implantação, você envia o Delete Stack CT para a pilha HA de dois níveis e para o bucket S3, e pode solicitar que os snapshots do RDS sejam excluídos (eles são excluídos automaticamente após dez dias, mas custam uma pequena quantia enquanto estão lá). Reúna a pilha IDs para a pilha HA e o bucket S3 e siga estas etapas. Consulte Stack | Delete.

Apêndice: questionário de integração da SALZ

Tópicos

- Resumo da implantação
- Considerações sobre a arquitetura do ambiente
- Alertas de monitoramento da zona de pouso com uma única conta
- Janela de manutenção
- Próximas etapas

Essas são algumas das informações que você precisará considerar antes de criar uma conta.

Resumo da implantação

Uma descrição da implantação. Por exemplo:

- Essa conta é para a implantação de um Line-of-Business aplicativo (em oposição à implantação de um aplicativo de produto).
- A implantação envolve um ARP (proxy reverso autenticado) escalonado automaticamente na sub-rede pública ou DMZ da conta.
- Os servidores web e de aplicativos serão implantados na sub-rede privada da conta.
- Uma instância do RDS (Amazon Relational Database Service) também será implantada na sub-rede privada da conta.
- Os servidores (ARP, web, aplicativo, banco de dados, balanceador de carga etc.) são separados em grupos de segurança distintos.
- A conta requer um design HA (alta disponibilidade) espalhado pelas zonas de disponibilidade (AZs), ou seja, “Multi-AZ”.

Considerações sobre a arquitetura do ambiente

Considere os critérios a seguir ao decidir como configurar seu ambiente e sua arquitetura.

- Seu data center virtual se conectará novamente à sua rede corporativa?
  - Você tem um AWS DirectConnect serviço existente ou precisa de um novo DirectConnect serviço?

  - Você tem uma conexão VPN existente ou precisa de um novo serviço de VPN?
- Qual é o intervalo de endereços internos de blocos CIDR disponível que você poderia alocar? (/16 recomendado, não deve se sobrepor aos intervalos da rede corporativa)
- Seu data center virtual exigirá acesso à Internet?
- Quais regiões você pretende usar? (Sydney/N. Virginia/Dublin)
- Você precisará de uma sub-rede do Shared Services para hospedar aplicativos que tenham conectividade com todas as outras sub-redes?
- Quais são suas divisões organizacionais que você gostaria que fossem hospedadas como sub-redes separadas. Para cada um:
  - De que conectividade com outras sub-redes você precisa?
  - A sub-rede exige acesso à Internet?
  - Há alguma restrição de implantação de aplicativos nessa sub-rede?
  - Há algum requisito de rede específico para essa sub-rede?
- Você gostaria de ambientes de and/or teste de desenvolvimento separados? (Incluirá serviços compartilhados duplicados para acesso a qualquer momento)
- Quais são seus requisitos de backup instantâneo?
- Você tem um processo de manutenção ou janelas de patch existentes que gostaria de manter?
- Quais são seus requisitos de registro de domínio?
- Você tem algum requisito de login único? (por exemplo, AD, LDAP)
- Quais são seus requisitos gerais de sistema operacional e de capacidade previstos?

Alertas de monitoramento da zona de pouso com uma única conta

O AMS fornece uma maneira de você ser alertado diretamente (em vez de receber notificações do serviço AMS) para determinados alertas de monitoramento. Para se inscrever, certifique-se de que seu Cloud Architect (CA) ou Cloud Service Delivery Manager (CSDM) receba estas informações:

E-mail de alertas diretos: esses são os endereços de e-mail para os quais você deseja que o AMS envie determinados alertas baseados em recursos. Para obter detalhes sobre quais alertas são enviados diretamente para o e-mail, consulte Alertas do monitoramento de linha de base no AMS no Guia do usuário do AMS para zona de destino de conta única. Para obter mais informações sobre o monitoramento do AMS, consulte Gerenciamento de monitoramento no Guia do usuário do AMS para a zona de destino de conta única.

Janela de manutenção

Você vai querer criar uma janela de manutenção que considere diferentes necessidades de aplicação Regiões da AWS, diferentes e diferentes períodos de estresse. Sua janela de manutenção é quando o AMS aplicará a correção. Veja aqui algumas diretrizes:

- Para limitar o impacto sobre os usuários, planeje sua janela de manutenção de acordo com o Região da AWS local em que seus ambientes estão implantados.
- Agende uma janela fora do horário comercial normal e quando o menor tráfego é esperado nos servidores de produção.
- Normalmente, as pilhas de infraestrutura exigem atualizações mensais.
- Agende uma janela de manutenção por pelo menos 300 minutos. A correção do sistema operacional leva de 60 a 90 minutos, a correção da pilha de infraestrutura leva de 180 a 300 minutos.

Próximas etapas

A equipe de integração do AMS ajudará você em todas as etapas da integração de sua conta ao AMS. Esses são os requisitos de integração:

- Provisione um novo Conta da AWS para usar no AMS e forneça um Conta da AWS ID.
- Inscreva-se para obter o nível de Support desejado.
- Crie uma função do IAM entre contas para conceder acesso à conta de aprovisionamento do AMS e fornecer o nome da função ao AMS.
- Adicione a conta 753102745277 como uma entidade confiável.

Apêndice: Regra de declaração dos Serviços de ActiveDirectory Federação (ADFS) e configurações de SAML

Para step-by-step obter instruções detalhadas sobre como instalar e configurar o AD FS, consulte Habilitando a federação na AWS usando o Windows Active Directory, o ADFS e o SAML 2.0.

Configurações de regras de declaração do ADFS

Se você já tiver uma implementação do ADFS, configure o seguinte:

- Confiança da parte confiável
- Regras de reivindicações

As etapas das regras de confiança e reivindicações da parte confiável foram seguidas do blog Habilitar a federação na AWS usando o Windows Active Directory, AD FS e SAML 2.0

- Regras de reivindicações:
  - Nameid: configuração por postagem do blog
  - RoleSessionName: Configure da seguinte forma
    - Nome da regra de reivindicação: **`RoleSessionName`**
    - Armazenamento de atributos: **`Active Directory`**
    - Atributo LDAP: **`SAM-Account-Name`**
    - Tipo de reclamação de saída: **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`**
    - Obtenha grupos do AD: configuração por postagem do blog
    - Reivindicação de função: configure da seguinte forma

```
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/"));
```

Console web

Você pode acessar o console web da AWS usando o link abaixo, *[ADFS-FQDN]* substituindo-o pelo FQDN da sua implementação do ADFS.

https://*[ADFS-FQDN]*/adfs/ls/IdpInitiatedSignOn.aspx

Seu departamento de TI pode implantar o link acima para a população de usuários por meio de uma Política de Grupo.

Acesso à API e à CLI com SAML

Como configurar o acesso à API e à CLI com SAML.

Os pacotes python são provenientes das postagens do blog abaixo:

- NTLM: Como implementar API federada e acesso à CLI usando SAML 2.0 e AD FS
- Formulários: Como implementar uma solução geral para API/CLI acesso federado usando o SAML 2.0
- PowerShell: Como configurar o acesso federado à API na AWS usando o Windows PowerShell

Configuração do script

1. Usando o Notepad++, altere a região padrão para a região correta
2. Usando o Notepad++, desative a verificação SSL para ambientes de teste e desenvolvimento
3. Usando o Notepad++, configure idpentryurl

   ```
   https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?
   loginToRp=urn:amazon:webservices
   ```

Configuração do Windows

As instruções abaixo são para os pacotes python. As credenciais geradas serão válidas por 1 hora.

1. Baixe e instale o python (2.7.11)
2. Baixe e instale as ferramentas de CLI da AWS
3. Instale a CLI do AMS:

   a. Faça o download do arquivo zip dos distribuíveis do AMS fornecido pelo seu gerente de entrega de serviços em nuvem (CSDM) e descompacte.

      Vários diretórios e arquivos são disponibilizados.

   b. Abra o diretório Managed Cloud Distributables -> CLI -> Windows ou Managed Cloud Distributables -> CLI -> Linux/macOS, dependendo do seu sistema operacional, e:

      Para Windows, execute o instalador apropriado (esse método só funciona em sistemas Windows de 32 ou 64 bits):

      - 32 bits: ManagedCloud API_x86.msi
      - 64 bits: ManagedCloud API_x64.msi

      Para Mac/Linux, execute o arquivo chamado: MC_CLI.sh. Você pode fazer isso executando este comando:`sh MC_CLI.sh`. Observe que os diretórios amscm e amsskms e seu conteúdo devem estar no mesmo diretório do arquivo MC_CLI.sh.

   c. Se suas credenciais corporativas forem usadas via federação com a AWS (a configuração padrão do AMS), você deverá instalar uma ferramenta de gerenciamento de credenciais que possa acessar seu serviço de federação. Por exemplo, você pode usar este blog de segurança da AWS Como implementar API federada e acesso à CLI usando SAML 2.0 e AD FS para ajudar a configurar suas ferramentas de gerenciamento de credenciais.

   d. Após a instalação, execute `aws amscm help` e veja `aws amsskms help` os comandos e opções.

4. Faça o download do script SAML necessário

   Faça o download em c:\aws\scripts

5. Baixar PIP

   Faça o download em c:\aws\downloads

6. Usando PowerShell, instale o PIP

   <pythondir>. \ python.exe c:\aws\downloads\get -pip.py

7. Usando PowerShell, instale o módulo de inicialização

   inicialização de<pythondir\ scripts> instalação do pip

8. Usando PowerShell e instalando o módulo de solicitações

   solicitações de<pythondir\ scripts> instalação de pip

9. Usando PowerShell e instalando o módulo de segurança de solicitações

   <pythondir\ scripts>solicitações de instalação do pip [segurança]

10. Usando PowerShell, instale o módulo beautifulsoup

    <pythondir\ scripts>pip install beautifulsoup4

11. Usando PowerShell, crie uma pasta chamada .aws no perfil do usuário (%userprofile%\ .aws)

    mkdir.aws

12. Usando PowerShell, crie um arquivo de credencial na pasta.aws

    Credenciais do novo item - tipo de arquivo —force

    O arquivo de credenciais não deve ter uma extensão de arquivo

    O nome do arquivo deve estar todo em letras minúsculas e ter as credenciais do nome

13. Abra o arquivo de credenciais com o bloco de notas e cole os seguintes dados, especificando a região correta

    ```
    [default]
    output = json
    region = us-east-1
    aws_access_key_id =
    aws_secret_access_key =
    ```

14. Usando PowerShell o script SAML e o logon

    <pythondir>. \ python.exe c:\aws\scripts\samlapi.py

    Nome de usuário: [NOME DE USUÁRIO] @upn

    Escolha a função que você gostaria de assumir

Configuração do Linux

As credenciais geradas serão válidas por 1 hora.

1. Usando o WinSCP, transfira o script SAML
2. Usando o WinSCP, transfira o certificado Root CA (ignore para teste e desenvolvimento)
3. Adicione a CA RAIZ aos certificados raiz confiáveis (ignore para teste e desenvolvimento)

   $ openssl x509 -inform der -in [certname] .cer -out certificate.pem (ignore para teste e desenvolvimento)

   Adicione o conteúdo do certificate.pem ao final do arquivo/etc/ssl/certs/ca-bundle.crt ((ignore para desenvolvimento de teste)
4. Crie uma pasta.aws em home/ec2-user 5

   ```
   [default]
   output = json
   region = us-east-1
   aws_access_key_id =
   aws_secret_access_key =
   ```
5. Usando o WinSCP, transfira o arquivo de credenciais para a pasta.aws
6. Instale o módulo de inicialização

   inicialização de instalação do $ sudo pip
7. Módulo de solicitações de instalação

   Solicitações de instalação do $ sudo pip
8. Instale o módulo beautifulsoup

   $ sudo pip install beautifulsoup4
9. Copie o script para home/ec2-user

   Defina as permissões necessárias

   Execute o script: samlapi.py

Histórico do documento

A tabela a seguir descreve as mudanças importantes na documentação desde a última versão do AMS.

- Versão da API: 2019-05-21
- Última atualização da documentação: 23 de setembro de 2025

Alteração	Descrição	Data
Tipo de alteração atualizado para escalonamento automático de endpoints em SageMaker IA na seção de perguntas frequentes do AWS Managed Services	Use o AMS SSP para provisionar o Amazon SageMaker AI em sua conta AMS. Envie um RFC com Gerenciamento | Componentes avançados da pilha | Identity and Access Management (IAM) | Atualize o tipo de alteração de entidade ou política (revisão obrigatória) (ct-27tuth19k52b4) para elevar as permissões de escalonamento automático temporária ou permanentemente, pois o escalonamento automático exige acesso permissivo no serviço. CloudWatch	25 de setembro de 2025
Referências precisas do tipo de alteração	Crie, altere ou exclua grupos de segurança. Para adicionar um usuário: Envie uma RFC usando Management | Directory Service | Usuários e grupos | Adicionar usuário ao grupo [ct-24pi85mjtza8k] e Para remover um usuário: Envie uma RFC usando Management | Directory Service | Usuários e grupos | Remover usuário do grupo [ct-2019s9y3nfml4]	08 de agosto de 2025
Link do TOC removido	O link do AWS glossário do TOC foi removido.	08 de agosto de 2025

Alteração	Descrição	Data
Link adicionado para orientação sobre prescrição	Configurar o faturamento consolidado — vincular a nova conta à conta do pagador.	08 de maio de 2025
Instruções atualizadas para ativar o acesso do IAM ao Console de gerenciamento da AWS	Esclareceu as instruções para ativar o acesso do IAM ao. Console de gerenciamento da AWS	Ative o acesso do IAM ao AWS console
Número atualizado de interfaces virtuais de trânsito permitidas nas conexões dedicadas do Direct Connect	As conexões dedicadas do Direct Connect agora têm um limite de 4 interfaces virtuais de trânsito por conexão	Conectando o Direct Connect ao Transit Gateway
Melhore a redação.	Especificou que “usado apenas como uma lista de “Negação”” deve incluir “Permitir tudo” para garantir as operações de monitoramento e gerenciamento do AMS.	Network configuration
Informações adicionais sobre o uso da CLI do AMS.	“Observação adicionada de que a `--region` opção pode ser necessária para alguns comandos da CLI”	Instale o AMS CLIs
Atualizado: os cabeçalhos dos capítulos para consistência e legibilidade mudaram algumas subseções do tópico para seções mais apropriadas	“Modos de gerenciamento de mudanças” é o novo título de “Gerenciamento de mudanças”	Modos de gerenciamento de alterações
Conteúdo atualizado	O modo AMS, anteriormente conhecido como “modo de gerenciamento de alterações” ou “modo CM padrão”, agora é conhecido como “modo RFC”. A seção de modos foi expandida.	Modo RFC.

Alteração	Descrição	Data
Conteúdo atualizado	O modo AMS, anteriormente conhecido como “modo de gerenciamento de alterações” ou “modo CM padrão”, agora é conhecido como “modo RFC”. A seção de modos foi reduzida e os links para as seções do Guia do Usuário Avançado do AMS sobre modos foram adicionados.	Modos AMS.
MALZ: Diagrama de arquitetura de rede atualizado	Arquitetura da conta de redem	16 de junho de 2022
Lista de tópicos movida para os parágrafos de abertura abaixo	Introdução ao AWS Managed Services Onboarding	16 de junho de 2022
Conteúdo atualizado, iniciativa de linguagem inclusiva	“Conta de gerenciamento” e não “Conta principal”.	Função de usuário do IAM no AMS , seção “Exemplos de políticas”
Conteúdo atualizado, ferramentas, contas, nomes de funções	Nome da função atualizado CustomerMigrationAccessRole para AWSManagedServicesMigrationRole.	AWS Serviço de migração de aplicativos (AWS MGN)
SALZ: Padrões de gerenciamento de continuidade	Link atualizado e informações obsoletas removidas de Tag e padrões de VPC	28 de fevereiro de 2022

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.