



Conceitos e procedimentos avançados do AMS

Guia do usuário avançado do AMS



Versão October 3, 2025

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

Guia do usuário avançado do AMS: Conceitos e procedimentos avançados 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

O que é o AWS Managed Services?	1
Sobre este Guia	2
Planos de operações	2
Acelere o plano de operações	3
Plano de operações avançado	3
Conceitos básicos	4
Principais termos	4
Service description (Descrição do serviço)	10
Recursos do plano operacional do AWS Managed Services (AMS) AMS Advanced	11
O que fazemos, o que não fazemos	16
Matriz de responsabilidade da AMS (RACI)	18
Componentes básicos do ambiente AMS	41
Limites da conta AMS	44
Objetivos de nível de serviço do AMS (SLOs)	47
AWS Serviços suportados	48
Configurações compatíveis	51
Sistemas operacionais não suportados	54
Interfaces avançadas do AMS	55
VPC endpoints	56
Namespaces protegidos por AMS	57
Prefixos reservados do AMS	58
Janela de manutenção do AMS	59
Recursos de informação do AMS	59
Conformidade AMS	60
Padrões de conformidade suportados pelo AMS	61
Responsabilidade compartilhada	65
Imagens de máquinas AMS Amazon (AMIs)	65
Segurança aprimorada AMIs	68
Como funciona a integração entre o AD FS e o AMS	68
Active Directory gerenciado pelo AMS	70
Implantações de aplicações	73
Gerenciamento de serviços	75
Governança de contas	75
Início do serviço	76

Gestão do relacionamento com o cliente (CRM)	76
Processo de CRM	77
Reuniões de CRM	78
Organizações de reuniões de CRM	79
Relatórios mensais de CRM	80
Otimização de custo	81
Estrutura de otimização de custos	81
Matriz de responsabilidade de otimização de custos	84
Horário de atendimento	86
Como obter ajuda	87
Gestão planejada de eventos	88
Critérios AMS PEM	88
Tipos de PEM	88
O processo AMS PEM	89
PEM FAQs	90
Arquitetura de rede	91
Arquitetura de rede MALZ	91
Sobre a arquitetura de rede de landing zone com várias contas	91
Escolhendo um único MALZ ou vários MALZs	94
Contas de várias contas da Landing Zone	99
Arquitetura de rede SALZ	134
Serviços compartilhados de landing zone com conta única do AMS	134
Configurando o AMS	136
Configurações padrão do AMS	137
Padrões de resolução de DNS (MALZ)	137
EC2 Perfil de instância do IAM	138
Alertas do monitoramento de linha de base no AMS	145
Padrões de retenção e rotação de registros	162
Usando os consoles AMS	163
Usando a API e a CLI do AMS	165
Pontos de extremidade HTTP da API AMS para chamadas REST	165
Instalando ou atualizando a CLI do AMS	165
Usando a API AMS em CLI, Ruby, Python e Java	167
AMS: traga seu próprio EPS	176
Ative o BYOEPS para sua conta	178
Recebendo notificações do AMS	181

Notificações AMI do AMS com SNS	183
Notificações de serviço	186
Notificações de alteração de estado do RFC	187
Configurando DNS público e privado	191
Gerenciamento de tráfego de saída do AMS	192
Implantação de recursos do IAM	194
Provisionamento automatizado do IAM	194
Definindo permissões com funções e perfis do IAM	218
Solicitar uma nova função de usuário ou perfil de instância do IAM	218
Restrinja as permissões com declarações de política de função do IAM	219
Restrinja as permissões com perfis de instância EC2 do Amazon IAM	221
Regra de declaração do AD FS e configurações de SAML	221
Configurações de regras de declaração do ADFS	222
Console web	223
Acesso à API e CLI com SAML	223
Restringir com ACL de rede	226
AMS em Outposts	227
AWS Outposts gerenciamento operacional e de instalação	228
Provisionamento de recursos gerenciados pelo AMS em AWS Outposts	230
Limitações do AMS em AWS Outposts	231
AMS sobre AWS Outposts conformidade	232
AMS ativado AWS Outposts FAQs	233
Usar tags	235
Etiquetagem automática da infraestrutura AMS	236
Tags recomendadas pelo AMS	238
Marcar notas de atualização em massa	242
Programador de recursos	244
Implantando o Agendador de Recursos	245
Personalizando o Agendador de Recursos	245
Usando o Agendador de Recursos	246
Estimador de custos do AMS Resource Scheduler	247
Melhores práticas do AMS Resource Scheduler	248
AWS Systems Manager no AMS Advanced	250
Documentos SSM do AMS Advanced disponíveis	251
Versões do documento AMS Advanced SSM	251
Preços do Systems Manager	251

Contas AMS externas	252
Externamente de contas de landing zone de conta única	253
Extraia contas de várias contas na landing zone	257
Modos de gerenciamento de alterações	280
Visão geral dos modos	281
Tipos de modos e contas no AMS	282
Modos e aplicativos ou cargas de trabalho do AMS	285
Casos de uso do mundo real para modos AMS	294
Modo RFC	297
Saiba mais sobre RFCs	298
Quais são os tipos de mudança?	338
Solução de problemas de erros de RFC	351
Modo de mudança direta	362
Introdução ao modo Direct Change	363
Segurança e conformidade	365
Gerenciamento de alterações no modo Direct Change	371
Criação de pilhas usando o modo Direct Change	373
Casos de uso do Modo de Mudança Direta	376
Modo de desenvolvedor	377
Começando com o modo Desenvolvedor	378
Segurança e conformidade	380
Gerenciamento de alterações	382
Provisionar infraestrutura	387
Controles de detecção	388
Registro, monitoramento e gerenciamento de eventos	388
Gerenciamento de incidentes	388
Gerenciamento de patches	389
Gerenciamento de continuidade	389
Gerenciamento de segurança e acesso	390
Modo de provisionamento de autoatendimento no AMS	390
Introdução ao modo SSP no AMS	391
Amazon API Gateway	391
Alexa for Business	393
Amazon AppStream 2.0	394
Amazon Athena	397
Amazon Bedrock	398

Amazon CloudSearch	399
Amazon CloudWatch Synthetics	400
Amazon Cognito	402
Amazon Comprehend	404
Amazon Connect	405
Amazon Data Firehose	407
DevOpsGuru da Amazon	408
Amazon DocumentDB (compatível com MongoDB)	409
Amazon DynamoDB	410
Amazon Elastic Container Registry	411
EC2 Image Builder	412
Amazon ECS em AWS Fargate	414
Amazon EKS em AWS Fargate	417
Amazon EMR	420
Amazon EventBridge	423
Amazon Forecast	425
Amazon FSx	428
Amazon FSx para OpenZFS	430
Amazon FSx para NetApp ONTAP	431
Amazon Inspector Classic	433
Amazon Kendra	434
Amazon Kinesis Data Streams	435
Amazon Kinesis Video Streams	436
Amazon Lex	437
Amazon MQ	438
Amazon Managed Service for Apache Flink	439
Amazon Managed Streaming for Apache Kafka	440
Amazon Managed Service para Prometheus	442
Amazon Personalize	443
Amazon QuickSight	445
Amazon Rekognition	447
SageMaker IA da Amazon	448
Amazon Simple Email Service	452
Amazon Simple Workflow Service	453
Amazon Textract	454
Amazon Transcribe	455

Amazon WorkSpaces	456
Serviços de código AMS	458
AWS Amplify	461
AWS AppSync	462
AWS App Mesh	463
AWS Audit Manager	464
AWS Batch	465
AWS Certificate Manager	467
Autoridade de Certificação Privada da AWS	468
AWS CloudEndure	471
AWS CloudHSM	472
AWS CodeBuild	474
AWS CodeCommit	475
AWS CodeDeploy	477
AWS CodePipeline	478
AWS Compute Optimizer	480
AWS DataSync	481
AWS Device Farm	482
AWS Elastic Disaster Recovery	483
AWS Elemental MediaConvert	485
AWS Elemental MediaLive	485
AWS Elemental MediaPackage	487
AWS Elemental MediaStore	488
AWS Elemental MediaTailor	489
AWS Global Accelerator	490
AWS Glue	490
AWS Lake Formation	492
AWS Lambda	493
AWS License Manager	495
AWS Migration Hub	496
AWS Outposts	496
AWS Resilience Hub	497
AWS Secrets Manager	498
AWS Security Hub CSPM	501
AWS Service Catalog AppRegistry	502
AWS Shield	503

AWS Snowball Edge	504
AWS Step Functions	506
AWS Systems Manager Armazenamento de parâmetros	507
AWS Systems Manager Automation	508
AWS Transfer Family	512
AWS Transit Gateway	513
AWS WAF	514
AWS Well-Architected Tool	515
AWS X-Ray	516
VM Import/Export	517
Modo gerenciado pelo cliente	518
Introdução ao modo Gerenciado pelo Cliente	519
AMS e AWS Service Catalog	519
Introdução ao Service Catalog	520
Service Catalog no AMS antes de você começar	520
Encontrando os dados de que você precisa (SKMS)	525
O que é gerenciamento de conhecimento de serviços?	525
Encontre uma VPC IDs	526
Encontre a sub-rede IDs	528
Encontre a AMI IDs	531
Encontre o grupo de segurança (SG) IDs	532
Encontre entidades do IAM	532
Encontre a pilha IDs	533
Encontre endereços IP IDs ou de instância	535
Encontre ARNs	538
Encontre recursos por ARN	539
Encontre as configurações da conta	541
Encontre FQDNs	542
Encontre zonas de disponibilidade (AZs)	543
Encontre tópicos do SNS	544
Encontre configurações de backup	544
Gerenciamento de acesso	546
O que é gerenciamento de acesso?	546
Por que e quando acessamos sua conta	547
Como e quando usar o root	552
Console AMS Advanced e EC2 acesso à Amazon	553

Acessando o console AWS de gerenciamento e o console AMS	554
Acesso temporário ao console AMS	554
Acessando instâncias usando bastiões	555
Nomes de bastiões compatíveis com DNS	557
Economizando custos em bastiões de landing zone de conta única (SALZ)	558
Usando endereços IP bastion	559
Exemplos de acesso à instância	559
Controle de acesso baseado em equipe ou função em uma conta AMS	570
Configuração automatizada de EC2 instâncias	571
Pré-requisitos para configuração automatizada de instâncias	571
Instalação automática do SSM Agent	572
Pré-requisitos	572
Solicitar instalação automática do SSM Agent	573
Como funciona a instalação automática do SSM Agent	573
Mudanças automatizadas	574
Atualize automaticamente o código em instâncias Linux	574
Atualize automaticamente o PBIS em instâncias Linux	575
Atualize automaticamente a versão mínima do SSM e CloudWatch dos agentes	576
CloudWatch arquivos de configuração, detalhes da atualização	577
Registros configurados automaticamente	577
Monitoramento e gerenciamento de eventos	579
O que é monitoramento?	580
O que o sistema de monitoramento AMS monitora?	581
Monitoramento proativo do Active Directory Trust na zona de destino com uma única conta	582
Como funciona o monitoramento	582
EC2 notificações agrupadas por instâncias	584
Notificação de alerta baseada em tag	585
Visualizando a configuração de monitoramento de uma conta	586
Alterando a configuração de monitoramento de uma conta	586
Notificações de incidentes com reconhecimento de aplicativos no AMS	587
Provisione AppRegistry sua conta AMS e crie aplicativos	587
Crie tags para permitir o enriquecimento de casos	588
Personalize a gravidade do caso de suporte do AMS para seus aplicativos	588
Revise as permissões necessárias	589
Usando OpsCenter	590

Notificação de alerta	590
Recebendo alertas	591
Notificações de alerta baseadas em tags	591
Remediação automática de alertas pelo AMS	592
Criação de CloudWatch alarmes adicionais	601
Criação de CloudWatch métricas e alarmes personalizados	603
Usando o CloudWatch Application Insights para servidores do .Net e SQL	604
Roteador de eventos AMS	605
Amazon EventBridge Managed Rules implantadas pelo AMS	605
Criação de regras gerenciadas para AMS	606
Editando regras gerenciadas para AMS	606
Excluindo regras gerenciadas para AMS	606
Remediador confiável	606
Benefícios principais	607
Como funciona o Trusted Remediator	607
Principais termos	608
Comece a usar o Trusted Remediator	609
Recomendações compatíveis do Compute Optimizer	612
Trusted Advisor Verificações suportadas	616
Configurar a remediação de cheques	677
Fluxo de trabalho de decisão do modo execução	681
Configurar tutoriais de remediação	681
Trabalhe com remediações	684
Registros de remediação	688
Práticas recomendadas	691
FAQs	691
Gerenciamento de logs	694
O que é gerenciamento de registros?	694
Como funciona o registro do AMS	694
Acessar os logs no	695
Registros de serviços agregados do AMS	695
Registros de serviços compartilhados do AMS	711
Amazon Elastic Compute Cloud (Amazon EC2) — registros em nível de sistema	714
Integração com o Splunk	716
Personalizando sua configuração de log	716
Alterando a retenção de CloudWatch registros	716

Habilitando o registro para serviços compatíveis	717
Gerenciamento de segurança	718
Proteção de dados no AMS	718
Amazon Macie	719
GuardDuty	721
Firewall DNS do Amazon Route 53 Resolver	724
AWS Certificate Manager certificado (ACM)	725
Criptografia de dados no AMS	726
Gerenciamento de identidade e acesso	727
Proteções IAM da Multi-Account Landing Zone (MALZ)	728
Autenticação com identidades	728
Registro e monitoramento de eventos de segurança no	750
Segurança de terminais (EPS)	751
Processo de mitigação de malware	756
Segurança do Amazon Inspector	757
Resposta ao incidente do AMS	759
Validação de conformidade	760
Zona de destino de várias contas visualizando o status de conformidade de seu Regras do AWS Config	761
Restrições da política de controle de serviços de landing zone multicontas do AMS	762
Resiliência	762
Segurança da infraestrutura	763
Práticas recomendadas de segurança	795
Configurações não padrão de EPS da landing zone multiconota do AMS	795
Guardrails AMS	795
Políticas de controle de serviços MALZ	796
Resposta a incidentes de segurança	796
Como funciona	797
Preparar	797
Detectar	798
Analisar	799
Contenção	800
Erradicação	802
Recuperar	803
Relatório pós-incidente	803
Runbooks de resposta a incidentes de segurança	804

Revisões de segurança de solicitações de alteração no AMS Advanced	810
Processo de gerenciamento de riscos de segurança do cliente	811
Padrões técnicos avançados do AMS	812
Controles padrão no AMS Advanced	812
Alterações que introduzem riscos de segurança altos ou muito altos em seu ambiente	839
Gerenciamento de continuidade	843
O que é gerenciamento de continuidade?	843
Como funciona o gerenciamento de continuidade	843
Planos de backup	844
Cofres de backup	847
Tipos de alteração de backup	848
Monitoramento e emissão de relatórios para backups	849
Resposta de recuperação de desast	850
planejamento de recuperação de desastres	850
Vários sites ou de alta disponibilidade (HA)	851
Standby passivo	852
Luz piloto	853
Backup e restauração	854
Gerenciamento de patches	860
AMS Patch Orchestrator: um modelo de patch baseado em tags	861
Usando o Patch Orchestrator	863
Pré-requisitos do Patch Orchestrator	866
Janelas de patch	868
Notificações de patch	869
Linhas de base de patch	872
Tags reservadas do Patch Orchestrator	872
Aplicação de patches sob demanda	872
Correção padrão do AMS	873
Sistemas operacionais compatíveis	874
Patches compatíveis	875
Patching e design de infraestrutura	877
Como funciona a correção padrão do AMS	878
Falhas de patches padrão do AMS	883
Ações que você pode realizar na aplicação de patches padrão do AMS	884
Correção padrão do AMS FAQs	887
Compromissos de serviços de correção	890

Aplicação de patches padrão	890
Correção crítica	892
Relatórios e opções	896
Relatórios sob solicitação	896
Relatórios do AMS Patch	897
Relatórios de backup do AMS	906
Incidentes evitados e monitoramento dos relatórios do Top Talkers	908
Relatório de detalhes de cobranças	910
Relatórios do Trusted Remediator	912
Relatórios de autoatendimento	915
Operações internas de API	916
Relatório de patch (diário)	919
Relatório de backup (diário)	929
Relatório de incidentes (semanal)	934
Relatório de cobrança (mensal)	937
Relatórios agregados	940
Painéis de relatórios de autoatendimento do AMS	942
Política de retenção de dados	950
Fora do SSR	950
Obter suporte	952
Gerenciamento de incidentes	952
O que é gerenciamento de incidentes?	954
Compromissos do serviço de gerenciamento de incid	955
Exemplos de gerenciamento de incidentes	958
Gerenciamento de solicitações de serviço	964
Quando usar uma solicitação de serviço	965
Como funciona o gerenciamento de solicitações de serviço	966
Testando uma solicitação de serviço	966
Criando uma solicitação de serviço	967
Monitoramento e atualização de solicitações de serviço	969
Respondendo a uma solicitação de serviço gerada pelo AMS	971
Perguntas sobre faturamento	971
Operações sob demanda	973
Solicitando operações de AMS sob demanda	983
Fazendo alterações nas ofertas do Operations on Demand	984
Histórico do documento	985

Atualizações anteriores	1003
.....	mxxxv

O que é o AWS Managed Services?

Bem-vindo ao AWS Managed Services (AMS), gerenciamento de operações de infraestrutura para Amazon Web Services (AWS). O AMS é um serviço corporativo que fornece gerenciamento contínuo de sua AWS infraestrutura.

Este guia do usuário é destinado a profissionais de TI e desenvolvedores de aplicativos. Presume-se uma compreensão básica dos termos e práticas de funcionalidade de TI, rede e implantação de aplicativos.

O AMS implementa as melhores práticas e mantém sua infraestrutura para reduzir a sobrecarga e o risco operacionais. O AMS fornece serviços de ciclo de vida completo para provisionar, executar e dar suporte à sua infraestrutura, além de automatizar atividades comuns, como solicitações de mudança, monitoramento, gerenciamento de patches, segurança e serviços de backup. O AMS aplica suas políticas de infraestrutura corporativa e de segurança e permite que você desenvolva soluções e aplicativos usando sua abordagem de desenvolvimento preferida.

Para entender melhor a arquitetura do AMS, veja [esses diagramas](#).

Tópicos

- [Sobre este guia do usuário do AMS](#)
- [Planos de operações do AMS](#)
- [Comece a usar o AWS Managed Services](#)
- [Termos-chave do AMS](#)
- [Service description \(Descrição do serviço\)](#)
- [Recursos de informação do AMS](#)
- [Conformidade AMS](#)
- [Imagens de máquinas AMS Amazon \(AMIs\)](#)
- [Como funciona a integração entre o AD FS e o AMS](#)
- [Active Directory gerenciado pelo AMS](#)
- [Implantações de aplicativos AMS](#)

Note

Novas Regiões da AWS são adicionadas com frequência. Para obter os sistemas operacionais mais recentes compatíveis com o AMS Regiões da AWS e os mais recentes com suporte para o AMS, consulte [Configurações compatíveis](#). Para saber mais sobre isso Regiões da AWS, consulte [Gerenciando Regiões da AWS](#).

A AMS busca melhorar continuamente nossos serviços com base em seus comentários. Usamos vários mecanismos para viabilizar seu autoatendimento, automatizar tarefas repetitivas e implementar novos Serviços da AWS recursos à medida que são lançados. Você pode enviar uma solicitação de serviço do AMS a qualquer momento para sugerir novos recursos ou melhorias nos recursos.

O horário comercial do AMS é 24 horas por dia, 7 dias por semana, 365 dias por ano.

O AMS segue um conjunto de práticas de gerenciamento de serviços de TI (ITSM) que se concentra em alinhar os serviços de TI às necessidades de sua empresa.

Sobre este guia do usuário do AMS

Este guia do usuário é destinado a clientes do AMS Advanced com um landing zone com várias contas ou uma única conta. Para obter mais detalhes sobre as ofertas da zona de pouso do AMS, consulte os [Termos-chave do AMS](#); consulte também a arquitetura da zona de [pouso com várias contas e a arquitetura da zona de pouso com conta única](#).

Planos de operações do AMS

O AWS Managed Services (AMS) está disponível com dois planos operacionais: AMS Accelerate e AMS Advanced. Um plano de operações oferece um conjunto específico de recursos e tem diferentes níveis de serviço, capacidades técnicas, requisitos, preços e restrições. Nossos planos de operações oferecem a flexibilidade de selecionar os recursos operacionais do tamanho certo para cada uma de suas AWS cargas de trabalho. Esta seção descreve os recursos e as diferenças, bem como as responsabilidades, os recursos e os benefícios associados a cada plano, para que você possa entender qual plano de operações é melhor para suas contas.

Para uma comparação detalhada dos recursos dos dois planos de operações, consulte [AWS Managed Services Features](#).

Plano de operações do AMS Accelerate

O AMS Accelerate é o plano de operações do AMS que ajuda você a operar o gerenciamento da day-to-day infraestrutura de seu AWS ambiente novo ou existente. O AMS Accelerate fornece serviços operacionais, como monitoramento, gerenciamento de incidentes e segurança. O AMS Accelerate também oferece um complemento de patch opcional para cargas de trabalho EC2 baseadas na Amazon que exigem patches regulares.

Com o AMS Accelerate, você decide quais Contas da AWS deseja que o AMS Accelerate opere, as regiões da AWS nas quais deseja que o AMS Accelerate opere, os complementos necessários e os acordos de nível de serviço (SLAs) necessários. Para obter mais detalhes, consulte [Usando o plano de operações e a descrição do serviço do AMS Accelerate](#).

Plano de operações do AMS Advanced

O AMS Advanced fornece serviços de ciclo de vida completo para provisionar, executar e dar suporte à sua infraestrutura. Além dos serviços operacionais fornecidos pelo AMS Accelerate, o AMS Advanced também inclui serviços adicionais, como gerenciamento de landing zone, mudanças e provisionamento de infraestrutura, gerenciamento de acesso e segurança de terminais.

O AMS Advanced implanta uma landing zone para a qual você migra suas AWS cargas de trabalho e recebe serviços operacionais do AMS. Nossas zonas de destino gerenciadas com várias contas são pré-configuradas com a infraestrutura para facilitar a autenticação, a segurança, a rede e o registro.

O AMS Advanced também inclui um sistema de gerenciamento de alterações e acesso que protege suas cargas de trabalho impedindo o acesso não autorizado ou a implementação de mudanças arriscadas em sua infraestrutura. AWS Os clientes precisam criar uma solicitação de mudança (RFC) usando nosso sistema de gerenciamento de alterações para implementar a maioria das alterações em suas contas do AMS Advanced. Você cria RFCs a partir de uma biblioteca de alterações automatizadas que são pré-avaliadas por nossas equipes de segurança e operações ou solicita alterações manuais que são revisadas e implementadas por nossa equipe de operações, caso sejam consideradas seguras e suportadas pelo AMS Advanced.

O AMS Advanced também oferece diferentes SLAs. Para obter mais informações, consulte a [descrição do serviço AWS Managed Services AMS Advanced](#).

Comece a usar o AWS Managed Services

Para obter detalhes sobre como começar a usar o serviço AMS de várias contas da landing zone, consulte a Introdução ao [AWS Managed Services Onboarding](#). Os dois guias de integração fornecem descrições do serviço e perguntas a serem consideradas para ajudar você a começar. Analise o conjunto de recursos do [AWS Managed Services Features](#) e os recursos atuais em [AWS Managed Services Resources](#).

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.

Service description (Descrição do serviço)

O AMS Advanced (AMS) é um plano operacional do serviço AWS Managed Services para gerenciar as operações da sua AWS infraestrutura. O AMS Advanced fornece operações de infraestrutura de rotina, como patches, gerenciamento de continuidade, gerenciamento de segurança e processos de gerenciamento de TI, como gerenciamento de incidentes, mudanças e solicitações de serviços. Para obter uma lista dos serviços compatíveis, consulte [AWS Serviços suportados](#).

YouTube Vídeo: [Como o AMS pode me ajudar a alcançar a excelência operacional na nuvem?](#)

Tópicos

- [Recursos do plano operacional do AWS Managed Services \(AMS\) AMS Advanced](#)
- [O que fazemos, o que não fazemos](#)
- [Matriz de responsabilidade da AMS \(RACI\)](#)
- [Componentes básicos do ambiente AMS](#)
- [Limites da conta AMS](#)
- [Objetivos de nível de serviço do AMS \(SLOs\)](#)
- [AWS Serviços suportados](#)
- [Configurações compatíveis](#)
- [Capacidades para sistemas operacionais não suportados no AMS](#)
- [Interfaces avançadas do AMS](#)
- [Endpoints VPC do AMS](#)
- [Namespaces protegidos por AMS](#)
- [Prefixos reservados do AMS](#)
- [Janela de manutenção do AMS](#)

Recursos do plano operacional do AWS Managed Services (AMS) AMS Advanced

O AMS Advanced oferece os seguintes recursos para AWS serviços compatíveis:

- Registro, monitoramento, grades de proteção e gerenciamento de eventos:

O AMS configura e monitora seu ambiente gerenciado para registrar atividades e define alertas com base em uma variedade de verificações de saúde. Os alertas são investigados pelo AMS para os serviços aplicáveis da AWS, e aqueles que afetam negativamente o uso desses serviços resultam na criação de incidentes. O AMS agrega e armazena todos os registros gerados como resultado de todas as operações e registros do sistema no Amazon S3. CloudWatch CloudTrail Você pode solicitar que alertas adicionais sejam implementados. Além dos controles preventivos da AMS, a AMS implanta proteções de configuração e controles de detetive para fornecer proteção contínua contra configurações incorretas que poderiam reduzir a integridade operacional e de segurança das contas gerenciadas, para reforçar seus controles, como marcação e conformidade. Quando um controle monitorado é detectado, é gerado um alarme que resulta em notificação, modificação ou encerramento de recursos com base nos padrões predefinidos do AMS que podem ser modificados por você.

- Gerenciamento de continuidade (backup e restauração):

O AMS fornece backups de recursos usando a funcionalidade padrão existente do AWS Backup em um intervalo programado determinado por você. As ações de restauração de instantâneos específicos podem ser realizadas pelo AMS com seu RFC. As alterações de dados que ocorrem entre os intervalos de captura de imagens são de sua responsabilidade pelo backup. Você pode enviar uma RFC para solicitações de backup ou snapshot fora dos intervalos programados. No caso de indisponibilidade da Zona de Disponibilidade (AZ) em uma AWS região, com sua permissão, o AMS restaura o ambiente gerenciado recriando novas pilhas com base em modelos e snapshots disponíveis do EBS das pilhas afetadas.

- Gerenciamento de segurança e acesso:

O AMS fornece segurança de terminais (EPS), como configuração de proteção antivírus e antimalware. Você também pode usar sua própria ferramenta e processos de EPS e não usar o AMS para EPS usando um recurso chamado traga seu próprio EPS (BYOEPS). O AMS também configura recursos de AWS segurança padrão que são aprovados por você durante a integração, como funções AWS Identity and Access Management (IAM) e grupos de EC2 segurança da Amazon, e usa AWS ferramentas padrão (por exemplo AWS Security Hub CSPM, Amazon Macie, GuardDuty Amazon) para monitorar e responder a problemas de segurança. Você gerencia seus usuários por meio de um serviço de diretório aprovado fornecido por você. Para obter uma lista dos serviços de diretório aprovados, consulte [Configurações compatíveis](#).

O AMS inclui segurança de terminais (EPS), que inclui antivírus (AV), e proteção antimalware, detecção de malware e intrusão (Trend Micro). Os grupos de segurança são definidos por modelo de pilha e modificados na inicialização, dependendo da visibilidade dos grupos de segurança do aplicativo (público/privado).

O acesso aos sistemas é solicitado por meio de solicitações de gerenciamento de mudanças para mudança (RFCs). O gerenciamento de acesso fornece acesso a recursos distintos, como EC2 instâncias da Amazon Console de gerenciamento da AWS, APIs e. Depois de estabelecer uma relação de confiança unidirecional com uma implantação do AMS Microsoft Active Directory durante a integração e a federação na AWS, você pode usar suas credenciais corporativas existentes para todas as interações.

- Gerenciamento de patches:

O AMS aplica e instala atualizações em EC2 instâncias para sistemas operacionais compatíveis (OSs) e software pré-instalado com sistemas operacionais compatíveis. Para obter uma lista dos sistemas operacionais compatíveis, consulte [Configurações compatíveis](#).

O AMS oferece dois modelos para aplicação de patches:

- Patch padrão do AMS para patches tradicionais baseados em contas, e
- AMS Patch Orchestrator, para aplicação de patches baseada em tags.

No patch padrão do AMS, você escolhe uma janela de manutenção mensal para que o AMS execute a maioria das atividades de correção. O AMS aplica atualizações críticas de segurança fora da janela de manutenção selecionada (com notificações apropriadas) e atualizações importantes durante a janela de manutenção selecionada. Além disso, o AMS aplica atualizações às ferramentas de gerenciamento de infraestrutura durante a janela de manutenção selecionada. Você pode excluir pilhas do gerenciamento de patches ou rejeitar atualizações, se quiser.

Com o AMS Patch Orchestrator, uma janela de manutenção padrão por conta é definida por você para que o AMS execute atividades de correção. Você pode programar janelas de manutenção personalizadas adicionais para o AMS corrigir um conjunto específico de instâncias definido por você com tags. O AMS aplica todas as atualizações disponíveis, mas você pode filtrar ou rejeitar atualizações criando uma linha de base de patch personalizada. Para ambos os modelos, se você aprovar ou rejeitar uma atualização fornecida no gerenciamento de patches, mas depois mudar de ideia, você é responsável por iniciar a atualização por meio de um RFC. O AMS monitora o status do patch dos recursos e destaca os sistemas que não estão atualizados na análise comercial mensal. O gerenciamento de patches é limitado às pilhas no ambiente gerenciado, incluindo todos os aplicativos gerenciados pelo AMS e os serviços compatíveis da AWS com recursos de correção (por exemplo, RDS). Para oferecer suporte a todos os tipos de configurações de infraestrutura quando uma atualização é lançada, o AMS a) atualiza a EC2 instância e b) fornece uma AMI do AMS atualizada para você usar. É sua responsabilidade instalar, configurar, corrigir e monitorar quaisquer aplicativos adicionais não abordados especificamente acima.

- Gerenciamento de mudanças:

O gerenciamento de alterações do AMS é o mecanismo para você controlar as mudanças em seu ambiente gerenciado. O AMS usa uma combinação de controles preventivos e de detecção para facilitar esse processo e fornece diferentes níveis de controle e risco associado, dependendo do modo AMS selecionado.

Todas as ações em seu ambiente AMS são registradas AWS CloudTrail.

Para obter mais informações sobre o AMS Change Management e os diferentes modos, consulte o [guia de gerenciamento de alterações do AMS e os modos do AMS](#).

- Gerenciamento de provisionamento automatizado e de autoatendimento:

Você pode provisionar recursos da AWS no AMS Advanced de várias maneiras:

- Enviar solicitações de provisionamento e configuração para alteração () RFCs
- Implemente por meio do AWS Service Catalog
- Implemente por meio do [modo Direct Change](#)
- Implante por meio [do modo Desenvolvedor](#). Lembre-se de que os recursos criados por meio do modo Desenvolvedor não são gerenciados pelo AMS.
- Configure os serviços da AWS diretamente usando o provisionamento de autoatendimento para selecionar Serviços da AWS (consulte). [AWS Serviços suportados](#)
- Gerenciamento de incidentes:

O AMS notifica você de forma proativa sobre incidentes detectados pelo AMS. O AMS responde aos incidentes enviados pelo cliente e gerados pelo AMS e resolve os incidentes com base na prioridade do incidente. A menos que seja instruído de outra forma por você, os incidentes que são determinados pela AMS como um risco à segurança do seu ambiente gerenciado e os incidentes relacionados à disponibilidade do AMS e de outros serviços da AWS são acionados proativamente. O AMS age em todos os outros incidentes assim que sua autorização for recebida. Os incidentes recorrentes são tratados pelo processo de gerenciamento de problemas.

- Gerenciamento de problemas:

O AMS realiza análises de tendências para identificar e investigar problemas e identificar a causa raiz. Os problemas são corrigidos com uma solução alternativa ou permanente que evite a recorrência de um impacto similar no futuro no serviço. Um relatório pós-incidente (PIR) pode ser solicitado para qualquer incidente “alto”, após a resolução. O PIR captura a causa raiz e as ações preventivas tomadas, incluindo a implementação de medidas preventivas.

- Relatórios:

O AMS fornece um relatório mensal de serviço que resume as principais métricas de desempenho do AMS, incluindo um resumo executivo e insights, métricas operacionais, recursos gerenciados, adesão ao acordo de nível de serviço (SLA) do AMS e métricas financeiras sobre gastos, economias e otimização de custos. Os relatórios são entregues pelo gerente de prestação de serviços em nuvem (CSDM) do AMS atribuído a você.

- Gerenciamento de solicitações de serviço:

Para solicitar informações sobre seu ambiente gerenciado, AMS ou ofertas AWS de serviços, envie solicitações de serviço usando o console do AMS. Você pode enviar uma solicitação de

serviço para perguntas do tipo “Como fazer” sobre AWS serviços e recursos ou para solicitar serviços adicionais do AMS.

- Central de atendimento:

A AMS realiza operações de engenharia com funcionários em tempo integral da Amazon para atender a solicitações não automatizadas, incluindo gerenciamento de incidentes, gerenciamento de solicitações de serviços e gerenciamento de mudanças. O Service Desk opera 24 horas por dia, 7 dias por semana, 365 dias por ano.

- Recursos designados:

Cada cliente recebe um Cloud Service Delivery Manager (CSDM) e um Cloud Architect (CA).

- CSDMs pode ser contatado diretamente. Eles realizam análises de serviços e fornecem relatórios e insights em todas as fases da implementação, migração e ciclo de vida operacional. CSDMs conduza análises comerciais mensais e detalhe itens como gastos financeiros, recomendações de redução de custos, utilização de serviços e relatórios de risco. Eles se aprofundam nas estatísticas de desempenho operacional e fornecem recomendações de áreas de melhoria.
- CAs pode ser contatado diretamente e fornecer conhecimento técnico para ajudá-lo a otimizar o uso da AWS nuvem. Exemplos de atividades da CA incluem selecionar cargas de trabalho para migração, auxiliar na integração de contas e cargas de trabalho adicionais, atuar como líder técnico em atividades operacionais, como dias de jogos, testes de recuperação de desastres, gerenciamento de problemas e aconselhamento técnico para aproveitar ao máximo o AMS e. AWS CAs promova discussões técnicas em todos os níveis de sua organização e ajude no gerenciamento de incidentes, fazendo concessões, estabelecendo melhores práticas e mitigando riscos técnicos.
- Modo de desenvolvedor:

Esse recurso permite que você itere projetos e implantações de infraestrutura rapidamente em contas configuradas pelo AMS [1], permitindo acesso direto ao serviço da AWS e ao console da AWS, além APIs do acesso ao processo de gerenciamento de alterações do AMS. Os recursos provisionados ou configurados com permissões do modo de desenvolvedor fora do processo de gerenciamento de alterações são de sua responsabilidade gerenciá-los (consulte “Gerenciamento de provisionamento automatizado e de autoatendimento”). Os recursos provisionados por meio do processo de gerenciamento de mudanças do AMS são suportados como outras cargas de trabalho provisionadas pelo gerenciamento de mudanças no AMS.

- Suporte da AWS:

Os clientes do AMS podem escolher o nível de AWS Support de que precisam para complementar seu plano de operações do AMS. As contas inscritas no AMS podem ser inscritas no Business Support ou no Enterprise Support. Para saber mais sobre as diferenças nos planos de suporte, consulte os [planos de suporte da AWS](#).

- Conta gerenciada pelo cliente:

Esse recurso permite que você solicite contas da AWS dentro do mesmo ambiente gerenciado, mas as operações contínuas das cargas de trabalho e dos recursos da AWS nessas contas são de sua responsabilidade. O AMS provisiona contas gerenciadas pelo cliente, mas depois que as contas são criadas, nenhum outro recurso ou serviço do AMS é fornecido a essas contas. A AWS não inscreverá contas gerenciadas pelo cliente no suporte premium de nível corporativo. Será sua responsabilidade inscrever contas gerenciadas pelo cliente no AWS Support com a taxa de suporte que você escolher.

- Gerenciamento de firewall:

O AMS fornece uma solução opcional de firewall gerenciado para serviços de firewall compatíveis, que permite a filtragem de tráfego de saída vinculado à Internet para redes em seu ambiente gerenciado. Isso exclui serviços voltados ao público que não usam a infraestrutura de rede da AWS e cujo tráfego vai diretamente para a Internet. A solução combina a tecnologia de firewall líder do setor com os recursos de gerenciamento de infraestrutura do AMS para implantar, monitorar, gerenciar, escalar e restaurar a infraestrutura de firewall.

Ao integrar o AMS, você recebe uma lista completa da sua infraestrutura de rede AMS. Para obter uma lista atualizada dos serviços em execução para dar suporte à sua infraestrutura de AMS a qualquer momento, registre uma solicitação de serviço com detalhes específicos sobre as informações que você deseja. Para solicitar uma alteração no design da sua rede, crie uma solicitação de serviço descrevendo as alterações que você deseja fazer, por exemplo, adicionar uma VPC ou solicitar uma alteração na regra do grupo de segurança.

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.

Matriz de responsabilidade da AMS (RACI)

Note

Para cumprir suas obrigações em tempo hábil, o AWS Managed Services (AMS) pode exigir suas contribuições para decidir um curso de ação apropriado. A AMS entrará em contato com o contato designado do cliente para obter todos esses esclarecimentos e informações. A AMS espera uma resposta a essas perguntas dentro de 24 horas úteis. Caso não haja resposta dentro de 24 horas úteis, o AMS pode escolher uma ação em seu nome.

A matriz responsável, responsável, consultada e informada da AMS, ou RACI, atribui a responsabilidade primária ao cliente ou à AMS por uma variedade de atividades.

O AMS gerencia sua infraestrutura da AWS. A tabela a seguir fornece uma visão geral das responsabilidades do cliente e do AMS pelas atividades no ciclo de vida de um aplicativo executado em um ambiente gerenciado pelo AMS.

O AMS não é responsável por nenhuma das seguintes atividades nas contas gerenciadas pelo cliente ou pela infraestrutura em execução nelas; portanto, este RACI não é aplicável.

- R significa parte responsável que faz o trabalho para realizar a tarefa.
- C significa consultado; uma parte cujas opiniões são solicitadas, normalmente como especialistas no assunto; e com quem há comunicação bilateral.
- I significa informado; uma parte que é informada sobre o progresso, geralmente apenas após a conclusão da tarefa ou do resultado final.
- O provisionamento por autoatendimento se refere aos recursos que são provisionados pelo cliente com autoatendimento por meio da AWS API ou do console, incluindo o Modo de Desenvolvedor e os Serviços Provisionados de Autoatendimento.

Note

Algumas seções contêm 'R' para AMS e Clientes. Isso ocorre porque, no modelo de Responsabilidade AWS Compartilhada, tanto a AMS quanto os clientes assumem a propriedade conjunta para responder aos problemas de infraestrutura e aplicativos.

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 ao serviço. AWS As funções não impedem todas as mudanças e você é responsável por seguir seus controles internos, cumprir a conformidade e validar se todos os AWS serviços usados atendem às certificações exigidas. Chamamos isso de modo de provisionamento de autoatendimento. Para obter detalhes sobre os requisitos de AWS conformidade, consulte [AWS Conformidade](#).

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.

Atividades	Cliente	AWS Managed Services (AMS)
Ciclo de vida do aplicação		
Desenvolvimento de aplicações	R	eu
Análise e projeto de requisitos de infraestrutura de aplicações	R	C
Projeto e otimização para pilhas AMS não padrão	R	C
Projeto e otimização da pilha padrão AMS	eu	R
Implantação de aplicações	R	C
Implantação da infraestrutura da AWS	C	R
Monitoramento de aplicações	R	eu
Teste/otimização de aplicativos	R	eu

Atividades	Cliente	AWS Managed Services (AMS)
Orientação de otimização da infraestrutura da AWS	eu	R
Monitoramento da infraestrutura da AWS	eu	R
Solucione e resolva problemas de aplicativos	R	C
Solucione e resolva problemas de rede da AWS	C	R
Solucionar e resolver problemas do sistema operacional e da infraestrutura	C	R
	R	C
Provisionamento de autoatendimento		
Integração de aplicativos e ITSM		
Integração de aplicativos com ofertas de serviços da AWS	R	C
Integração do ITSM com a AWS Managed Services Interface	R	C
Redes		
Ambiente gerenciado: VPC e instalação e configuração de VPC	C	R
Aloque espaço de endereço privado para VPCs (por exemplo, /16)	R	C
Configurar e operar serviços gerenciados não pertencentes à AWS, gerenciados pelo cliente Firewalls/Proxy/Bastions/HOSTs	R	C

Atividades	Cliente	AWS Managed Services (AMS)
Configure e opere a segurança da AWS Groups/NAT/Customer Bastions/NACL dentro do ambiente gerenciado	eu	R
Configuração e implementação de rede (por exemplo DirectConnect) na rede do cliente	R	C
Configuração e implementação de rede no ambiente gerenciado	C	R
Configuração do ambiente gerenciado		
Defina as configurações padrão do Auto Scaling para modelos básicos de pilha	eu	R
Recomende a otimização do RI	C	R
Compre capacidade de RI e PIOP	R	C
Remova a capacidade quando a capacidade estiver superprovisionada (quando suportada pelo aplicativo do cliente)	C	R
Crie/atualize informações específicas de clientes da AWS para o AWS Managed Services	C	R
Configuração S3	C	R
Provisionamento por autoatendimento	R	C
Configuração do Glacier	C	R
Defina a política de arquivamento	R	C
Configuração da política de arquivamento	C	R

Atividades	Cliente	AWS Managed Services (AMS)
Seleção da janela de manutenção do cliente	R	eu
Gerenciamento do AWS RDS		
Monitore a source/replica/RO integridade da replicação	eu	R
Identifique o RCA do failover de origem	eu	R
Configuração automatizada de instantâneos (backup)	C	R
	R	C
Provisionamento por autoatendimento		
Coordene e agende o gerenciamento de patches do mecanismo de banco de dados	C	R
	R	C
Provisionamento por autoatendimento		
Recomende armazenamento de banco de dados e capacidade PIOP	C	R
	R	C
Provisionamento por autoatendimento		
Recomendar o dimensionamento de instâncias para executar bancos de dados	C	R
	R	C
Provisionamento por autoatendimento		
Recomendar a otimização de RI para ambiente gerenciado	C	R
	R	C
Provisionamento por autoatendimento		
Monitoramento de desempenho do RDS () CloudWatch	C	R
	R	C
Provisionamento por autoatendimento		

Atividades	Cliente	AWS Managed Services (AMS)
Configuração de assinatura de eventos do RDS (SNS)	C	R
Provisionamento por autoatendimento	R	C
Configuração do grupo de segurança do RDS	C	R
Provisionamento por autoatendimento	R	C
Configuração do mecanismo parameter/option RDS	R	C
Design de tabela de banco de dados	R	eu
Indexação de banco de dados	R	eu
Análise de log do banco de dados	R	eu
Gerenciamento de mudanças do AMS		
Criação de clientes RFCs (por exemplo, acesso a recursos, creating/updating/deleting managed stacks, deploying/updating aplicativos, alterações na configuração das ofertas de AWS serviços)	R	eu
Cliente aprovador RFCs	eu	R
Criação de AWS Managed Services RFCs (por exemplo, acesso a recursos, criação de recursos em nome do cliente, aplicação de atualizações ao sistema operacional como parte do gerenciamento de patches)	eu	R
Aprovação não automatizada RFCs	R	eu

Atividades	Cliente	AWS Managed Services (AMS)
Enviando solicitação para novos tipos de alteração	R	C
Criação de novos tipos de alteração	eu	R
Manutenção do calendário de alterações do aplicativo	R	C
Aviso da próxima janela de manutenção	eu	R
AWS Service Catalog		
Crie portfólios e produtos	R	eu
Distribua produtos para usuários finais	R	eu
Crie tags e biblioteca de opções de tags	R	C
Compartilhamento de portfólios e produtos com usuários finais	R	eu
Revise/atualize portfólios e produtos	R	eu
Crie e atribua restrições a portfólios e produtos	R	C
Associe ações de serviço aos produtos	R	C
Atualize os recursos provisionados com a nova versão do produto	R	eu
Provisionamento		
Adições específicas do cliente à AMI básica do AWS Managed Services	R	C
Configurar tipos de alteração aprovados adicionais usados para provisionar modelos de pilha	C	R

Atividades	Cliente	AWS Managed Services (AMS)
Lance pilhas gerenciadas e recursos associados da AWS enviados por meio do processo de gerenciamento de mudanças do AMS ou do AWS Service Catalog.	eu	R
Provisionamento por autoatendimento	R	eu
Install/Update aplicativos personalizados e de terceiros em instâncias provisionadas por meio do processo de gerenciamento de alterações do AMS ou do AWS Service Catalog.	R	eu
Provisionamento - Stack Architecture		
Fornecimento de licenças de sistema operacional (incluindo taxas de uso para os serviços aplicáveis da AWS — por exemplo, EC2 e RDS)	eu	R
Provisionamento de autoatendimento	R	I
Defina modelos de infraestrutura de linha de base (pilhas) para implantação de aplicativos por meio do sistema de gerenciamento de alterações AMS.	eu	R
Provisionamento de autoatendimento	R	I
Criação da linha de base aprovada 8 AMIs	eu	R
Avalie o inventário de aplicativos do cliente e determine a adequação aos modelos de infraestrutura disponíveis (pilhas)	R	C
Defina pilhas exclusivas que se somam às ofertas de modelos básicos	R	C

Atividades	Cliente	AWS Managed Services (AMS)
Registro, monitoramento e gerenciamento de eventos		
Registro de registros de alterações na infraestrutura da AWS	eu	R
Gravando todos os registros de alterações do aplicativo	R	C
Instalação e configuração de agentes e scripts para aplicação de patches, segurança , monitoramento etc. da infraestrutura da AWS provisionada por meio do processo de gerenciamento de alterações da AMS.	eu	R
	R	C
Provisionamento de autoatendimento		
Defina os requisitos específicos de monitoramento e incidentes do cliente	R	C
Configurando alertas para ambiente gerenciado	eu	R
Monitorando todos os alertas configurados pelo AM	eu	R
	R	C
Provisionamento de autoatendimento		
Investigando alertas de infraestrutura para notificação de incidentes	eu	R
	R	C
Provisionamento de autoatendimento		
Investigando alarmes de aplicativos	R	C
Gerenciamento de incidentes		

Atividades	Cliente	AWS Managed Services (AMS)
Notifique proativamente incidentes na infraestrutura da AWS com base no monitoramento	eu	R
Provisionamento de autoatendimento	R	C
Lide com problemas e interrupções de desempenho de aplicativos	R	eu
Categorize a prioridade do incidente	eu	R
Forneça resposta a incidentes	eu	R
Forneça resolução de incidentes e restauração da infraestrutura	C	R
 Note SLAs não se aplicam a recursos baseados em instâncias provisionados fora do gerenciamento de alterações do AMS, incluindo aqueles provisionados usando provisionamento de autoatendimento e modo de desenvolvedor.		
Gerenciamento de problemas		
Identifique problemas no ambiente gerenciado	C	R
Execute o RCA para problemas no ambiente gerenciado	C	R
Remediação de problemas no ambiente gerenciado	C	R
Identifique e corrija problemas de aplicativos	R	eu

Atividades	Cliente	AWS Managed Services (AMS)
Gerenciamento de segurança		
Segurança da infraestrutura do cliente and/or estabelecendo a linha de base para o processo de conformidade de segurança, conforme determinado e acordado durante a integração do cliente.	C	R
	R	C
Provisionamento de autoatendimento		
Manutenção de licenças válidas para EPS gerenciado	R	C
Configurar o EPS gerenciado	eu	R
Provisionamento de autoatendimento	R	C
Atualizar EPS gerenciado	eu	R
Provisionamento de autoatendimento	R	C
Monitoramento de malware em instâncias provisionadas por meio do processo AMS CM.	eu	R
	R	C
Provisionamento de autoatendimento		
Manutenção e atualização de assinaturas de vírus.	eu	R
	R	C
Provisionamento de autoatendimento		
Correção de instâncias infectadas com malware.	C	R
	R	C
Provisionamento de autoatendimento		
Gerenciamento de eventos de segurança	C	R

Atividades	Cliente	AWS Managed Services (AMS)
Segurança - Gerenciamento de acesso		
Gerencie o ciclo de vida dos usuários e suas permissões para serviços de diretórios locais, que são usados para acessar o AWS Managed Services	R	eu
Opere sistemas de autenticação federada para acesso do cliente ao console/ AWS APIs	R	C
Aceite e mantenha a confiança do Active Directory (AD) do AWS Managed Services AD para o AD gerenciado pelo cliente	R	C
Durante a integração, crie funções de administrador do IAM entre contas em cada conta gerenciada	R	C
Proteja a credencial AWS raiz de cada conta	eu	R
Definir recursos do IAM para ambiente gerenciado	C	R
Gerencie credenciais privilegiadas para acesso ao sistema operacional para engenheiros do AMS	eu	R
Gerencie credenciais privilegiadas para acesso ao sistema operacional fornecidas ao cliente pelo AMS	R	eu
Resposta a incidentes de segurança - Prepare-se		
Comunicações		

Atividades	Cliente	AWS Managed Services (AMS)
Forneça detalhes de contato de segurança do cliente para o AMS usar durante eventos de segurança, notificações e escalonamentos de segurança	R	eu
Armazene e gerencie os detalhes de contato de segurança do cliente fornecidos para uso durante eventos e escalonamentos de segurança	CI	R
Treinamento		
Forneça ao cliente documentação para apoiar o AMS durante o processo de resposta a incidentes	eu	R
Pratique a responsabilidade compartilhada durante os processos de resposta a incidentes por meio de dias de jogos de segurança	RI	RC
Gerenciamento de recursos		
Configure o gerenciamento de segurança suportado Serviços da AWS para alertas, correlação de alertas, redução de ruído e regras adicionais	eu	R
Mantenha o inventário de ativos (AWS recursos) e conheça o valor dos ativos e a criticidade dos ativos. Essas informações são úteis durante a estratégia de contenção de incidentes	R	CI
Use AWS tags para identificar recursos e cargas de trabalho	R	CI

Atividades	Cliente	AWS Managed Services (AMS)
Definir e configurar a retenção e o arquivamento de registros	CI	R
Linhas de base seguras Conta da AWS, configurações, políticas e gerenciamento de acesso	CI	RC
Resposta a incidentes de segurança - Detecte		
Registro, indicadores e monitoramento		
Configure o registro e o monitoramento para permitir o gerenciamento de eventos, por exemplo e contas	CI	R
Monitor compatível com Serviços da AWS alertas de segurança	eu	R
Implemente e gerencie ferramentas de segurança de terminais	CI	R
Monitore o malware em instâncias usando a ferramenta de segurança de endpoints compatível com AMS	eu	R
Notifique o cliente sobre eventos detectados por meio de mensagens de saída	eu	R
Encaminhe a notificação e quaisquer atualizações subsequentes para os tomadores de decisão sobre contas e cargas de trabalho específicas para melhorar o tempo de resposta a incidentes	R	CI

Atividades	Cliente	AWS Managed Services (AMS)
Defina, implante e mantenha os serviços de detecção padrão do AMS (por exemplo, Amazon GuardDuty e AWS Config)	CI	R
Registre registros de alterações na AWS infraestrutura	eu	RC
Ative e configure o registro e o monitoramento para permitir o gerenciamento de eventos para o aplicativo	R	C
Implemente e mantenha uma lista de permissões, uma lista de negação e detecções personalizadas em serviços de AWS segurança compatíveis (por exemplo, Amazon GuardDuty)	RCI	R
Relatórios de eventos de segurança		
Notifique o AMS sobre uma atividade suspeita ou uma investigação de segurança ativa	R	CI
Notifique eventos e incidentes de segurança detectados ao cliente	eu	R
Notificar o evento planejado que pode acionar o processo de resposta a incidentes de segurança	R	CI
Resposta a incidentes de segurança - Analise		
Investigação e análise		
Execute a resposta inicial para o alerta de segurança compatível gerado por uma fonte de detecção compatível	eu	RC

Atividades	Cliente	AWS Managed Services (AMS)
Avalie false/true os pontos positivos usando os dados disponíveis	RI	RC
Gere um instantâneo das instâncias afetadas para ser compartilhado com o cliente, se necessário	eu	R
Execute tarefas forenses, como cadeia de custódia, análise do sistema de arquivos, análise forense de memória e análise binária	R	CI
Colete registros de aplicativos para ajudar na investigação	R	eu
Colete dados e registros para auxiliar na investigação de alertas de segurança	RCI	RC
SMEs Participe Serviços da AWS de investigações de segurança	CI	R
Envolve fornecedores terceirizados durante a investigação (por exemplo, para investigação antimalware da EPS e interação com a equipe de TrendMicro suporte)	RCI	eu
Compartilhe registros de investigação do suporte Serviços da AWS com os clientes durante uma investigação	eu	R
Comunicação		
Envie alertas e notificações de fontes de detecção de AMS para recursos gerenciados	eu	R
Gerencie alertas e notificações para eventos de segurança de aplicativos	R	eu

Atividades	Cliente	AWS Managed Services (AMS)
Interaja com o ponto de contato de segurança do cliente durante uma investigação de incidente de segurança	R	eu

Resposta a incidentes de segurança - Contenção

Estratégia e execução de contenção		
Decida sobre a execução da estratégia de contenção acordada e concorde com as consequências que podem afetar a disponibilidade dos serviços durante a janela de contenção	R	CI
Faça um backup dos sistemas afetados para análise posterior	CI	R
Contenha aplicativos e cargas de trabalho (por meio de configuração específica do aplicativo ou atividade de resposta)	R	CI
Defina a estratégia de contenção com base no incidente de segurança e no recurso afetado	CI	R
Habilite a criptografia e o armazenamento seguro de backups pontuais dos sistemas afetados	CI	R
Execute ações de contenção suportadas para AWS recursos, incluindo EC2 instâncias, rede e IAM	CI	R

Resposta a incidentes de segurança - Erradicar

Estratégia e execução da erradicação

Atividades	Cliente	AWS Managed Services (AMS)
Defina as opções de erradicação com base no incidente de segurança e no recurso afetado nas cargas de trabalho dos aplicativos do cliente	R	CI
Decida sobre a estratégia de erradicação acordada, o momento da execução da erradicação e as consequências	R	CI
Defina as etapas de erradicação com base no incidente de segurança e no recurso afetado nas cargas de trabalho gerenciadas pelo AMS	CI	R
Erradicar e fortalecer AWS recursos, incluindo EC2 instâncias, rede e erradicação do IAM	CI	R
Erradicar e fortalecer aplicativos e cargas de trabalho (por meio de configuração específica do aplicativo ou atividade de resposta)	R	eu
Resposta a incidentes de segurança - Recuperação		
Preparação e execução da recuperação		
Configure planos e metas de backup conforme solicitado pelo cliente	R	eu
Análise os planos de backup para restaurar cargas de trabalho gerenciadas pelo AMS	CI	R
Execute atividades de restauração de backup para obter recursos compatíveis Serviços da AWS	eu	R

Atividades	Cliente	AWS Managed Services (AMS)
Faça backup do aplicativo do cliente, da configuração do aplicativo e das configurações de implantação e revise os planos de backup para restaurar os aplicativos e as cargas de trabalho do cliente após o incidente	R	eu
Restaurar aplicativos e cargas de trabalho do cliente (por meio de etapas de restauração específicas do aplicativo)	R	eu
Resposta a incidentes de segurança — Relatório pós-incidente		
Relatórios pós-incidentes		
Compartilhe as lições aprendidas e os itens de ação apropriados com o cliente após o incidente, conforme necessário	eu	R
Gerenciamento de patches ⁹		
Monitore as atualizações aplicáveis do sistema operacional compatível e do software pré-instalado com sistema operacional compatível para EC2 instâncias.	eu	R
	R	C
Provisionamento de autoatendimento		
Notifique o cliente sobre atualizações futuras (aplica-se somente ao AMS Standard Patch)	eu	R
Exclua certas atualizações (and/or determina das pilhas) das atividades de correção	R	eu

Atividades	Cliente	AWS Managed Services (AMS)
Defina janelas de manutenção padrão e personalizadas, programações e outros parâmetros (por exemplo, duração da janela de manutenção) para aplicar patches (aplica-se ao AMS Patch)	R	eu
Somente orquestrador)		
Defina linhas de base de patches personalizadas para filtrar e excluir patches específicos (aplica-se somente ao AMS Patch Orchestrator)	R	eu
Marque instâncias para associá-las a janelas de manutenção personalizadas e linhas de base de patches (aplica-se somente ao AMS Patch Orchestrator)	R	eu
Acompanhe o status dos patches dos recursos e destaque os sistemas que não estão atualizados na análise comercial mensal.	C	R
Corrija o sistema operacional Windows e os pacotes da Microsoft instalados no sistema operacional que são regidos pelo Windows Update	eu	R
Provisionamento de autoatendimento	R	-
Corrija aplicativos, software ou dependências de aplicativos instalados não gerenciados pelo Windows Update	R	eu
Provisionamento por autoatendimento	R	-

Atividades	Cliente	AWS Managed Services (AMS)
Corrija o sistema operacional Linux e qualquer pacote habilitado para gerenciamento pelo gerenciador de pacotes nativo do sistema operacional (por exemplo, Yum, Apt, Zypper)	eu	R
	R	-
Provisionamento por autoatendimento		
Corrija aplicativos, software ou dependências de aplicativos instalados não gerenciados pelo gerenciador de pacotes nativo do sistema operacional Linux	R	eu
	R	-
Provisionamento por autoatendimento		
Gerenciamento de continuidade		
Especifique os agendamentos de backup	R	eu
Execute backups por agendamento.	eu	R
Provisionamento de autoatendimento	R	C
Validar backups	R	eu
Solicitar atividades de restauração de backup	R	eu
Execute atividades de restauração de backup.	eu	R
Provisionamento de autoatendimento	R	C
Restaure as pilhas afetadas e. VPCs	eu	R
Provisionamento de autoatendimento	R	C
Restaure o aplicativo personalizado/de terceiros afetado	R	C
Relatórios		

Atividades	Cliente	AWS Managed Services (AMS)
Prepare e entregue um relatório de serviço mensal	eu	R
AMS ativado AWS Outposts	R	eu
Configure e recupere o histórico de auditoria da API sob demanda (CloudTrail).	eu	R
Provisionamento por autoatendimento	R	eu
Forneça acesso ao histórico de incidentes por meio da AWS Managed Services Interface	eu	R
Forneça acesso ao histórico de alterações por meio da AWS Managed Services Interface.	eu	R
Provisionamento por autoatendimento	N/D	N/D
Gerenciamento de solicitações de serviço		
Solicitar informações usando solicitações de serviço	R	eu
Responder às solicitações de serviço	eu	R
Firewall gerenciado		
Solicite a implantação do firewall gerenciado pelo AMS	R	eu
Projeto e otimização da arquitetura de firewall gerenciada pelo AMS	eu	R
Implantação da infraestrutura da AWS e do dispositivo de firewall gerenciado pela AMS	eu	R

Atividades	Cliente	AWS Managed Services (AMS)
Fornecimento de licenças de firewall (incluindo o taxas de uso para os serviços aplicáveis da AWS, por exemplo) EC2	R	eu
Definir lista de permissões de domínio padrão	eu	R
Solicitação para adicionar, modificar e excluir listas de permissões e políticas de segurança personalizadas	R	eu
Configurando alertas para o firewall gerenciado pelo AMS	eu	R
Monitorando todos os alertas configurados do firewall gerenciado pelo AMS	eu	R
Execute backups da configuração do firewall	eu	R
Solicitar atividades de restauração de backup	R	eu
Atualize os recursos provisionados com a nova versão do produto	eu	R
Gravação de registros de firewall gerenciados pelo AMS	eu	R
Encaminhar registros do firewall gerenciado pelo AMS para CloudWatch	eu	R
Solicite alterações na configuração do firewall gerenciado pelo AMS	R	eu
Aprovar alterações de configuração no firewall gerenciado pelo AMS	eu	R
Execute alterações de configuração no firewall gerenciado pelo AMS	eu	R

⁸ O AMS fornece EC2 somente AMIs para a Amazon

⁹ A AMS é responsável pelo fim da vida útil OSES somente quando o cliente assina um contrato de suporte estendido com o fornecedor do sistema operacional

Componentes básicos do ambiente AMS

Multi-Account Landing Zone

Essa é uma estimativa dos componentes e dos custos potenciais da infraestrutura nas contas principais. Isso não inclui outros custos, como largura de banda, monitoramento CloudWatch detalhado, registro em log, alarmes, Route53, Amazon S3, Simple Notification Service (Amazon SNS), snapshots ou instâncias reservadas da Amazon. EC2

Você paga pelos componentes exigidos pela infraestrutura de landing zone da AWS gerenciada pela AMS. As estimativas colocam o custo de um ambiente simples de landing zone com várias contas do AMS em \$2.450 por mês e \$50 para uma conta simples de inscrição.

Para obter informações sobre preços, consulte os [preços da AWS](#).

Componentes básicos do ambiente

Componente	Esforço Custos	Descrição
Conta de gerenciamento	\$60	Uma conta do AWS Organizations Management; cria e gerencia financeiramente contas de membros. Ele contém a estrutura da AWS Landing Zone (ALZ), conjuntos de pilhas de configuração de contas e políticas de controle de serviços da AWS Organization (SCP). • Directory Service: \$35 • CloudTrail: \$7 • CloudWatch: \$6 • Outros: \$12
Conta de serviços compartilhados	2000 USD	Contém a infraestrutura e os recursos necessários para gerenciamento de acesso (ou seja, Active Directory), gerenciamento de segurança de terminais (Trend Micro) e seus bastiões (SSH/RDP); a estimativa é de

Componente	Esforço Custos	Descrição
		\$2400 por mês. Essa estimativa não inclui o custo das licenças da Trend Micro. • EC2: \$800 (com o número mínimo de Bastions) • VERMELHO: \$300 (EPS) • VPC (endpoints): \$400 • Directory Service: \$300 • CloudWatch: \$100 • GuardDuty : \$15 • Secrets Manager: \$10 • Transferência de dados: \$10 • Config: \$10 • Outros: \$45
Conta de rede	\$350	O hub central para roteamento de rede entre contas AMS, sua rede local e tráfego de saída para a Internet. Além disso, contém bastiões públicos da DMZ (o ponto de entrada para os engenheiros do AMS acessarem os hosts em seu ambiente AMS). O preço pode aumentar dependendo do tráfego que atravessa o Transit Gateway e o Direct Connect. • EC2: \$250 (Bastiões) • VPC: \$80 • Outros: \$20

Componente	Esforço Custos	Descrição
Conta de arquivamento de registros	\$20	Um bucket S3 com cópias dos arquivos de log do AWS CloudTrail e do AWS Config de cada uma das suas contas do ambiente AMS. Os custos aumentam à medida que mais registros são coletados. • S3: \$10 • CloudWatch: \$5 • Outros: \$5
Conta de segurança	\$20	O hub central para operações relacionadas à segurança e o ponto principal para canalizar notificações e alertas para os serviços do plano de controle da AMS. Além disso, abriga a conta de gerenciamento do Amazon Guard Duty. Os custos aumentam à medida que mais eventos são analisados usando a Amazon GuardDuty. • CloudWatch: \$15 • Outros: \$5

Single-Account Landing Zone

A tabela a seguir lista os componentes de um exemplo de infraestrutura gerenciada pelo AMS.

Componentes básicos do ambiente, última atualização em 2020/07/09

Nome	Tipo de instância	SO	Nº de componentes	
mc-eps-dsm	m5.large	Linux	2	
mc-management	m5.large	Windows	2	
mc-bastion-dmz-ssh	m5.large	Linux	2	

Nome	Tipo de instância	SO	Nº de componentes	
mc-bastion-customer-rdp	m5.large	Windows	2	
mc-eps-relay	m5.large	Linux	2	
serviços de diretório	N/D	N/D		
componentes adicionais	N/D	N/D		

Para obter informações sobre preços, consulte os [preços da AWS](#).

Limites da conta AMS

Há três tipos distintos de limites a serem considerados na landing zone multiconta do AMS: limites da API do AMS, limites de recursos do AMS e limites da AWS.

Há dois tipos distintos de limites a serem considerados na landing zone de conta única do AMS: limites da API do AMS e limites da AWS.

Limites da API da conta AMS

Esta seção descreve os limites no nível da conta após os quais o AWS Managed Services (AMS) limita o serviço de API AMS SKMS. Isso significa que, se você ligar para qualquer um dos listados APIs mais de 10 vezes em um segundo, uma das chamadas será “limitada” (você receberá uma `ThrottlingException`). Em raras situações, uma dependência externa ou posterior pode limitar a API do AMS e, em seguida, o AMS pode limitar suas chamadas de API a uma taxa possivelmente menor.

Note

Para obter informações sobre a API AMS SKMS, baixe a referência na guia Relatórios do console do AWS Artifact.

Para cada API AMS SKMS listada, a operação é limitada após 10 TPS (transações por segundo):

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

Limites de recursos da conta de landing zone com várias contas do AMS

Os limites de recursos da conta estão relacionados às contas e VPCs sub-redes do aplicativo de várias contas da landing zone do AMS.

Limites de recursos da conta de aplicativo

Há um limite flexível de 50 contas de aplicativos por organização. Se você tiver um caso de uso para mais de 50 contas de aplicativos, entre em contato com seu gerente de entrega de serviços em nuvem (CSDM) para transmitir seus requisitos.

VPCs e limites de recursos de sub-redes

Há um limite mínimo de 10 VPCs por conta de aplicativo dentro da região predefinida da AWS para a organização.

Cada VPC pode ter de 1 a 10 camadas de sub-rede privadas espalhadas por 2 a 3 zonas de disponibilidade. Além disso, cada VPC pode ter de 0 a 5 níveis de sub-rede pública distribuídos por 2 a 3 zonas de disponibilidade. Se você tiver requisitos além desses limites, informe seu CSDM ou Cloud Architect para analisar seu caso de uso.

Relação entre o aplicativo e a conta de landing zone multicontas do AMS

Uma conta por aplicativo é suportada na landing zone de várias contas do AMS; no entanto, cada conta de aplicativo tem um pequeno custo, e você é cobrado pelo número de conexões com o Transit Gateway por hora e pela quantidade de tráfego que flui pelo AWS Transit Gateway. Portanto, quanto mais aplicativos segregados estiverem em contas ou VPCs maiores serão os custos.

Para reduzir custos e ainda garantir uma segregação adequada de tarefas, a AMS recomenda que você 1) agrupe os aplicativos por equipes com processos de negócios fortemente acoplados e 2) não misture aplicativos que estejam em estágios diferentes (produção versus não produção) ou

gerenciados por equipes diferentes. Dessa forma, você terá menos contas, o gerenciamento de acesso e a segregação de tarefas serão mais fáceis e o custo do tráfego poderá ser mitigado.

Por exemplo: uma empresa tem em produção um aplicativo de negociação e um aplicativo de gerenciamento de portfólio. Ambos os aplicativos são gerenciados pela equipe de TI da Investments e trocam muito tráfego entre si. Nesse cenário, a empresa pode se beneficiar do agrupamento dos dois aplicativos na mesma conta e na mesma VPC, porque a equipe de TI da Investments não precisará solicitar acesso a várias contas de aplicativos e a empresa economizará nos custos de tráfego. Nesse caso, a empresa deve criar outra conta para os mesmos aplicativos em fase de desenvolvimento e fornecer acesso à equipe de desenvolvimento.

Em outro cenário, a empresa tem em produção um aplicativo de folha de pagamento e um aplicativo de contabilidade, gerenciados pelas equipes de TI de Recursos Humanos e TI de Contabilidade, respectivamente. Embora o aplicativo de folha de pagamento precise trocar informações com o aplicativo de contabilidade, recomendamos segregar os dois aplicativos em contas diferentes, uma por equipe, e estabelecer uma conexão entre os dois aplicativos VPCs usando a conta de rede. Dessa forma, a empresa evitará que a equipe de TI de RH solicite alterações que afetem a infraestrutura de aplicativos contábeis, da qual eles não teriam conhecimento.

Dicas sobre como agrupar contas em unidades organizacionais (OUs). Uma OU é um mecanismo de agrupamento lógico que permite categorizar contas (agrupar) e aplicar políticas e configurações com base nesses grupos. A abordagem recomendada para a criação OUs é baseá-las em políticas que precisam ser aplicadas a um grupo específico de contas, não na hierarquia interna das equipes em sua estrutura de relatórios. Uma OU não é equivalente a uma OU do Active Directory, e tentar replicar a estrutura AD OU AWS Organizations é desencorajada e resulta em uma estrutura operacional difícil de manter. and/or

AWS limites da conta

AWS os limites da conta se aplicam às suas contas do AWS Managed Services (AMS). O método mais fácil de determinar os limites padrão e atuais dos AWS serviços é usar as Cotas de [AWS Serviço](#). O AMS recomenda dimensionar corretamente os limites de serviço individuais para o tamanho apropriado para executar o (s) serviço (s) na conta. Os limites funcionam como barreiras para proteger suas contas contra a segurança e a redução de custos. Se você quiser aumentar um limite específico, envie uma solicitação de serviço ao AMS, e a AMS Operations aumentará o limite em seu nome. Por exemplo, o limite padrão (ou cota) para instâncias do RDS é 40; se sua carga de trabalho exigir 50 instâncias do RDS, faça uma solicitação de serviço para as operações do AMS para aumentar o limite até o valor necessário.

Objetivos de nível de serviço do AMS (SLOs)

A tabela a seguir descreve as metas do serviço AWS Managed Services (AMS). Os acordos de nível de serviço (SLAs) para outros aspectos do serviço AMS, incluindo gerenciamento de incidentes, são abordados no documento de SLA compartilhado com você quando você se inscreveu no AMS. Para obter mais informações, fale com seu CSDM.

Objetivos de nível de serviço AMS

Recurso	Indicador de desempenho (PI)	Mais (Business Days, M-F 8AM to 6PM local time)	Premium (Calendar Days, 24 x 7)
Gerenciamento de alterações	Tempo necessário para agendar ou rejeitar automatizado RFCs	<=30 minutos	<=30 minutos
	Horário de início do agendado RFCs em comparação com o tempo de execução programado	<=1 minuto	<=1 minuto
	Tempo gasto até que approve/reject não seja automatizado RFCs, disponível no catálogo de tomografi a computadorizada	<=48 horas	<=24 horas
	Tempo gasto até que approve/reject não seja automatizado RFCs não disponível no catálogo de tomografia computado rizada	<=5 dias	<=5 dias

Recurso	Indicador de desempenho (PI)	Mais (Business Days, M-F 8AM to 6PM local time)	Premium (Calendar Days, 24 x 7)
Gerenciamento de problemas	Tempo necessário para concluir a análise da causa raiz (RCA)	<=10 dias	<=10 dias
Gerenciamento de solicitações de serviço	Tempo de resposta para a primeira resposta e para cada resposta subsequente	<=8 horas	<=4 horas

AWS Serviços suportados

O AWS Managed Services (AMS) fornece serviços de suporte de gerenciamento operacional para os seguintes AWS serviços. Cada AWS serviço é distinto e, como resultado, o nível de gerenciamento operacional do AMS, o suporte varia de acordo com a natureza e as características do AWS serviço subjacente. Os AWS serviços específicos são agrupados com base na complexidade e no escopo do serviço de suporte ao gerenciamento operacional fornecido pela AMS.

Note

Os três grupos, A, B e C, indicam os preços como uma porcentagem do gasto mensal total por conta do serviço AMS, com base no plano de suporte (Plus ou Premium), para clientes do AMS antes de 16 de março de 2021. Os clientes do AMS embarcados após 16 de março de 2021 devem enviar uma solicitação de serviço para obter informações adicionais sobre preços. O grupo A indica que não há cobrança adicional. O grupo B indica uma taxa adicional de 12% (Plus) ou 18% (Premium). O grupo C indica uma cobrança adicional de 25% (Plus) ou 42% (Premium).

Uma estrela (*) indica serviços que são implantados em um ambiente gerenciado pelo AMS por um cliente usando o AWS console e APIs. Consulte “Gerenciamento de provisionamento automatizado e de autoatendimento” em [Recursos do plano operacional do AWS Managed Services \(AMS\) AMS Advanced](#) para obter detalhes adicionais sobre as responsabilidades do cliente ao provisionar e configurar serviços dessa maneira.

Duas estrelas (**) indicam que o Amazon EC2 on AWS Outposts será cobrado como um serviço do Grupo B; todos os outros recursos hospedados no AWS Outposts serão cobrados de acordo com sua taxa padrão.

AWS Serviços suportados

Grupo A	Grupo B	Grupo C
Amazon Alexa for Business* Amazon Managed Streaming for Apache Kafka* Amazon CloudFront Amazon Elastic File System Amazon Glacier Amazon Simple Storage Service AWS Amplify* AWS AppMesh* AWS Auto Scaling AWS Backup AWS CloudFormation AWS Compute Optimizer AWS Global Accelerator* AWS Identity and Access Management AWS License Manager* AWS Management Console AWS Marketplace AWS Lake Formation* AWS Well Architected Tool* VM Import/ Export*	Amazon API Gateway* Amazon AppStream* Amazon Athena* Amazon Bedrock* Amazon CloudSearch* Amazon Cognito* Amazon Comprehend* Amazon Connect* Amazon Document DB (with MongoDB compatibility)* Amazon DynamoDB* Amazon EC2 Container Registry (ECR)* Amazon Elastic Container Service (ECS) on AWS Fargate* Amazon Elastic Kubernetes Service (EKS) on Fargate* Amazon Elemental MediaConvert* Amazon Elemental MediaPackage* Amazon Elemental MediaStore* Amazon Elemental MediaTailor* Amazon Elastic MapReduce* AmazonEventBridge* Amazon Forecast* Amazon FSx* Amazon Inspector*	Amazon Aurora Amazon CloudWatch Amazon Elastic Block Store (EBS) Amazon Elastic Compute Cloud** Amazon Elastic Load Balancing (classic, application, and network; not gateway) Amazon ElastiCache Amazon OpenSearch Service Amazon GuardDuty Amazon Macie Amazon Redshift Amazon Relational Database Service Amazon Route 53 Amazon Route 53 Resolver DNS Firewall Amazon Simple Email Service Amazon Simple Notification Service Amazon Simple Queue Service Amazon Virtual Private Cloud (VPC) AWS CloudTrail AWS Config AWS Database Migration Service

Grupo A	Grupo B	Grupo C
	Amazon Kendra* Amazon Kinesis Analytics* Amazon Kinesis Data Stream* Amazon Kinesis Firehose* Amazon Kinesis Video Streams* Amazon Lex* Amazon Managed Service for Prometheus* Amazon MQ* Amazon Personalize** Amazon Quantum Ledger Database (QLDB)* Amazon QuickSight* Amazon Rekognition* Amazon SageMaker* Amazon SimpleDB* Amazon Simple Workflow* Amazon Textract* Amazon Transcribe* Amazon Translate* Amazon WorkSpaces* AWS AppSync* AWS Audit Manager* AWS Batch* AWS Certificate Manager* AWS CloudEndure* AWS CloudHSM* AWS CodeBuild* AWS CodeCommit* AWS CodeDeploy* AWS CodePipeline* AWS DataSync* AWS Elemental MediaLive* AWS Glue* AWS Lambda* AWS MigrationHub* AWS Outposts**	AWS Data Transfer AWS Direct Connect AWS Directory Service AWS Key Management Service AWS Systems Manager (SSM)

Grupo A	Grupo B	Grupo C
	AWS Resilience Hub* AWS Secrets Manager* AWS Security Hub* AWS Service Catalog AWS Service Catalog AppRegistry* AWS Transfer for SFTP* AWS Shield* AWS Snowball* AWS Step Functions* AWS Transit Gateway* AWS WAF* AWS X-Ray*	

Se você solicitar que o AWS Managed Services forneça serviços para qualquer software ou serviço que não esteja expressamente identificado como suportado abaixo, qualquer AWS Managed Services fornecido para essas configurações solicitadas pelo cliente será tratado como um “Serviço Beta” de acordo com os Termos de Serviço.

Configurações compatíveis

Estas são as configurações que o AWS Managed Services (AMS) suporta:

- Idioma: O AMS está disponível em inglês.
- Serviços de firewall:
 - Firewall DNS do Amazon Route 53 Resolver
 - Firewall de próxima geração da série Palo Alto VM
- Software de segurança: Deep Security da Trend Micro (obrigatório). AWS Marketplace: [Trend Micro Deep Security](#)
- Serviços de diretório aprovados: Microsoft Active Directory (AD)
- [AWS Serviços suportados](#).
- AWS Regiões suportadas:

O AMS opera em um subconjunto de todas as AWS regiões; no entanto, o AMS API/CLI funciona somente na região “Leste dos EUA (Norte da Virgínia)”. Se você executar a API de gerenciamento de alterações do AMS (amscm) ou a API de gerenciamento de conhecimento do serviço do AMS

(amsskms), em uma região fora do Leste dos EUA), deverá adicionar `--region us-east-1` ao comando.

- 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)
- Imagens de máquina da Amazon (AMIs): O AMS fornece imagens de segurança aprimorada (AMIs) com base no benchmark CIS de nível 1 para um subconjunto de sistemas operacionais compatíveis com o AMS. Para encontrar sistemas operacionais que tenham uma imagem de segurança aprimorada disponível, consulte o Guia do usuário de segurança do AMS. Para acessar este guia, em AWS Artifact, filtre a guia Relatórios do AWS Managed Services. Para acessar AWS Artifact, entre em contato com seu CSDM ou consulte [Getting Started with AWS Artifact](#).
- Sistemas operacionais com suporte:

Sistemas operacionais compatíveis (x86-64)

- Amazon Linux 2023
- Amazon Linux 2 (data prevista de término do suporte ao AMS em 30 de junho de 2026)
- Oracle Linux 9.x, 8.x
- Red Hat Enterprise Linux (RHEL) 9.x, 8.x
- Servidor SUSE Linux Enterprise 15 SP6

- SUSE Linux Enterprise Server para SAP 15 SP3 e versões posteriores

- Microsoft Windows Server 2022, 2019, 2016
- Ubuntu 20.04, 22.04, 24.04

Sistemas operacionais compatíveis (ARM64)

- Amazon Linux 2023
- Amazon Linux 2 (data prevista de término do suporte ao AMS em 30 de junho de 2026)
- Sistemas operacionais End of Support (EOS) suportados:

Note

Os sistemas operacionais End of Support (EOS) estão fora do período de suporte geral do fabricante do sistema operacional e apresentam maior risco de segurança. Os sistemas operacionais EOS são considerados configurações suportadas somente se os agentes exigidos pelo AMS oferecerem suporte ao sistema operacional e...

1. você tem suporte estendido com o fornecedor do sistema operacional que permite receber atualizações, ou
2. todas as instâncias que usam um sistema operacional EOS seguem os [controles de segurança](#) conforme especificado pelo AMS no Guia Avançado do Usuário, ou
3. você cumpre quaisquer outros controles de segurança compensatórios exigidos pela AMS.

Caso o AMS não seja mais capaz de oferecer suporte a um sistema operacional EOS, o AMS emite uma [recomendação crítica](#) para atualizar o sistema operacional.

Os agentes exigidos pelo AMS podem incluir, mas não estão limitados a: AWS Systems Manager Amazon CloudWatch, agente Endpoint Security (EPS) e Active Directory (AD) Bridge (somente Linux).

- Ubuntu Linux 18.04
- SUSE Linux Enterprise Server 15 SP3, SP4, e SP5
- Servidor SUSE Linux Enterprise para SAP 15 SP2
- Servidor SUSE Linux Enterprise 12 SP5
- SUSE Linux Enterprise Service para SAP 12 SP5
- Microsoft Windows Server 2012/2012 R2
- Red Hat Enterprise Linux (RHEL) :7.x

- Oracle Linux 7.5-7.9

Capacidades para sistemas operacionais não suportados no AMS

Um sistema operacional não suportado é qualquer sistema operacional não listado no [Configurações compatíveis](#). O AMS considera as instâncias com sistemas operacionais sem suporte [AWS como “configurações solicitadas pelo cliente” que estão sujeitas aos termos de serviço de versões beta](#) e prévia.

O seguinte conjunto limitado de recursos do AMS está disponível para instâncias com sistemas operacionais sem suporte:

Recurso	Observações
Gerenciamento de incidentes	O AMS fornece resposta a incidentes.
Gerenciamento de solicitações de serviço	O AMS responde às solicitações de serviço.
Solicitações de mudança (RFCs)	O AMS avalia RFCs a execução. Sistemas operacionais não suportados podem afetar a capacidade de execução RFCs.
Monitoramento	O AMS monitora e responde às verificações de status EC2 do sistema e das instâncias da Amazon. As verificações de status do sistema incluem: perda de conectividade de rede, perda de energia do sistema, problemas de software no host físico e problemas de hardware no host físico que afetam a acessibilidade da rede. As verificações de status da instância incluem: configuração incorreta de rede ou inicialização, memória esgotada, sistema de arquivos corrompido e kernel incompatível.
Gerenciamento de segurança	O AMS monitora e responde às EC2 GuardDuty descobertas da Amazon.

Recurso	Observações
Gerenciamento de backups	O AMS fornece gerenciamento de continuidade no AMS Advanced para EC2 usar AWS Backup planos e cofres personalizados pelo AMS.

Interfaces avançadas do AMS

- **Console AMS Advanced:** você usa o console AMS Advanced para criar RFCs, relatar e responder a incidentes, fazer solicitações de serviço e encontrar informações sobre pilhas existentes VPCs e existentes. Em caso de dúvida sobre o que fazer ou quando precisar de ajuda com o AMS ou com seus recursos gerenciados, crie uma solicitação de serviço usando essa interface.
- **Console de gerenciamento da AWS:** muitos AWS consoles podem ser úteis para visualizar informações do AMS, por exemplo:
 - **EC2 Console da Amazon:** use para visualizar informações da instância, incluindo endereços IP do Bastion, grupos do Amazon EC2 Auto Scaling e balanceadores de carga.
 - **Conformidade com AWS Config** as regras da zona de destino de várias contas: você pode visualizar o status de conformidade em todas as suas contas e identificar recursos não compatíveis.
 - **AWS CloudFormation console:** use para visualizar as informações da pilha, incluindo a pilha IDs (você pode encontrar as pilhas do Amazon RDS e a IDs instância do Amazon RDS aqui, além das informações do evento).
 - **Console Amazon RDS:** use para visualizar informações do evento, como uma publicação feita em um WordPress aplicativo em um site da sua conta. Observe que você deve ter o ID da instância do Amazon RDS.

Dependendo do modo da sua função de login, você tem diferentes níveis de acesso ao AWS Management Console. Para obter mais informações sobre os modos, consulte [Modos AMS](#).

- **API avançada de gerenciamento de alterações do AMS — leitura/gravação:** use a API de gerenciamento de alterações (API CM) para solicitar adições e alterações específicas em sua infraestrutura gerenciada, incluindo monitoramento de recursos, configurações de log, backup e patch. Além disso, use essa API para solicitar acesso a recursos, excluir recursos AMIs, criar e criar perfis de instância do IAM. Você pode acessar a API do CM por meio da CLI do AMS e SDKs
- **API AMS SKMS — Somente leitura:** use essa API para listar recursos gerenciados e obter as informações necessárias para gerar relatórios ou preparar solicitações de alteração.

- Suporte API: use a Suporte API padrão para criar e responder programaticamente a incidentes e solicitações de serviço. Para saber mais, consulte [Introdução ao Suporte](#).
- AWS APIs— Somente leitura: seu administrador de TI principal pode usar o AWS APIs para ver todos os recursos sob gerenciamento, visualizar CloudTrail registros, informações de cobrança e muitas outras funções de leitura.

Endpoints VPC do AMS

Um VPC endpoint permite que você conecte sua VPC de forma privada sem precisar de um gateway de Internet. Serviços da AWS As instâncias na sua VPC não exigem que endereços IP públicos se comuniquem com recursos no serviço.

Endpoints são dispositivos virtuais. Eles são componentes de VPC altamente disponíveis, redundantes e escalados horizontalmente que permitem a comunicação entre instâncias na sua VPC e serviços sem impor riscos de disponibilidade ou restrições de largura de banda no tráfego da rede. Para saber mais, consulte [VPC Endpoints](#).

Há dois tipos de VPC endpoints: endpoints de interface e de gateway.

- Endpoints do gateway: a VPC na conta tem um endpoint do Amazon S3 Gateway habilitado por padrão.
- Endpoints de interface: as instâncias em seu ambiente AMS podem se comunicar com os serviços suportados sem sair da rede Amazon. Isso é opcional para a landing zone de conta única e não está habilitado na conta por padrão; envie uma solicitação de serviço às operações do AMS para que isso seja ativado. No entanto, para a landing zone com várias contas, os endpoints de interface são habilitados por padrão na conta do Shared Services.

Lista de endpoints de interface compatíveis com o AMS:

- AWS CloudFormation
- AWS CloudTrail
- AWS Config
- EC2 API da Amazon
- AWS Key Management Service
- Amazon CloudWatch
- CloudWatch Eventos da Amazon
- CloudWatch Registros da Amazon

- AWS Secrets Manager
- Amazon SNS
- AWS Systems Manager
- AWS Security Token Service

Namespaces protegidos por AMS

A lista de namespaces protegidos para o AWS Managed Services (AMS). Ao trabalhar com AWS recursos, evite conflitos com o AMS ao não usar esses namespaces. Para obter detalhes sobre outros namespaces AWS de serviços, consulte [Amazon Resource Names \(ARNs\) e AWS Service Namespaces](#).

- `ams-*` (esse é o padrão de nomenclatura preferido para novos recursos)
- `/ams/*` (esse é o padrão de nomenclatura preferido para recursos baseados em caminhos)
- `AWSManagedServices*` (esse é o padrão de nomenclatura preferido para recursos, quando CamelCase apropriado)
- `ams*` e `AMS*` e `Ams*`
- `AWS_*` e `aws*`
- `*/aws_reserved/*`
- `CloudTrail*` e `Cloudtrail*`
- `codedeploy_service_role`
- `customer-mc-*`
- `eps` e `EPS`
- `EPSTMarketplaceSubscriptionRole`
- `EPSDB*`
- `IAMPolicy*`
- `INGEST*`
- `LandingZone*`
- `Managed_Services*`
- `managementhost`
- `mc*` e `MC*` e `Mc*`

- MMS*
- ms-
- NewAMS*
- Root*
- sentinel* e Sentinel*
- sentinel.int.
- StateMachine*
- StackSet-ams*
- StackSet-AWS-Landing-Zone
- TemplateId*
- UnhealthyInServiceBastion
- VPC_*

Prefixos reservados do AMS

Os atributos dos recursos do AMS devem estar em conformidade com determinados padrões; por exemplo, nomes de perfis de instâncias do IAM, BackupVault nomes, nomes de tags e assim por diante, não devem começar com prefixos reservados do AMS. Esses prefixos reservados são:

```
*/aws_reserved/*  
ams- *  
/ams/*  
ams*  
AMS*  
Ams*  
aws*  
AWS*  
AWS_*  
AWSManagedServices*  
codedeploy_service_role  
CloudTrail*  
Cloudtrail*  
customer-mc-*  
eps  
EPSDB*  
IAMPolicy*
```

```
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion
```

Janela de manutenção do AMS

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. Isso é para o AWS Managed Services (AMS); para realizar atividades de manutenção de infraestruturas gerenciadas, como a implantação de um novo AMS. AMIs

Sua janela de manutenção é quando o AMS aplicará a correção e você determinará sua janela de manutenção na integração. Você também pode concordar com a janela de correção proposta fornecida na notificação do serviço de patches ou sugerir uma janela diferente.

Para obter orientação sobre como criar uma janela de manutenção, consulte [Janela de manutenção](#).

Recursos de informação do AMS

O AMS fornece vários recursos de informação para ajudá-lo a ter sucesso.

- Guia do usuário do AMS Accelerate: ajuda você a entender os componentes e recursos que o AMS Accelerate fornece e como usá-los. Veja aqui as informações básicas e os detalhes do AMS

Accelerate sobre configurações padrão, recursos de busca e exemplos de instruções. [Índice HTML](#), [PDF](#)

- Guia do usuário do AMS Advanced: ajuda você a entender os componentes e recursos que o AMS Advanced fornece e como usá-los. Veja aqui as informações básicas do AMS Advanced e detalhes sobre configurações padrão, recursos de busca e exemplos de instruções. [Índice HTML](#), [PDF](#)
- Guia de aplicativos avançados do AMS: descreve as etapas para a implantação de aplicativos na infraestrutura do AWS Managed Services. Veja aqui informações sobre metodologias e considerações de implantação e manutenção de aplicativos. [Índice HTML](#), [PDF](#).
- Guia de integração avançada do AMS: descreve as etapas iniciais para criar a infraestrutura básica de landing zone com várias contas ou conta única do AWS Managed Services em uma conta AMS. Veja aqui as informações básicas, a validação e as perguntas da conta AMS para prepará-lo para a integração no AMS. [Índice HTML](#), [PDF](#).
- Referência avançada de tipo de alteração do AMS: fornece material de referência sobre os tipos de alteração atuais fornecidos pelo AWS Managed Services, incluindo esquemas de tipo de alteração e exemplos de orientações para cada tipo de alteração e dicas. Inclui informações gerais sobre os tipos de alteração. Ajuda você a entender todos os aspectos das solicitações de mudança (RFCs) e dos tipos de alteração do AMS (CTs). Veja aqui detalhes específicos sobre os tipos de alteração, incluindo links para informações relevantes. [Índice HTML](#), [PDF](#).
- Referência da API AMS CM (gerenciamento de mudanças): descreve a API do AWS Managed Services CM, que fornece operações para criar e monitorar solicitações de mudança e fornece informações sobre seus recursos que são gerenciados pelo Managed Services. [Índice HTML](#).
- Guias de segurança do AMS: descreva as informações de segurança proprietárias do AMS.

Privado; disponível na guia Relatórios do AMS no console do AWS Artifact.

- Recursos para desenvolvedores do AMS: acesso à CLI e ao SDK do AMS, tanto para amscm quanto para amsskms. Consulte <https://console.aws.amazon.com/managedservices/>.
- YouTube Vídeos do AMS: principais operações do cliente explicadas em vídeo. Veja os [vídeos YouTube instrucionais do AWS Managed Services](#).
- Publicações no blog do AMS: informações especializadas sobre AWS Managed Services. Veja os [blogs da AWS](#).

Conformidade AMS

O AMS passou por uma auditoria para os seguintes padrões e está qualificado para uso como parte de soluções para as quais você deve obter a certificação de conformidade.

Padrões de conformidade suportados pelo AMS

O AMS suporta padrões de AWS conformidade. Para saber mais sobre programas de AWS conformidade, consulte [AWS Conformidade](#).

Esses são os padrões de conformidade atuais suportados pelo AMS.

FedRAMP: O governo federal dos EUA se dedica a fornecer seus serviços ao povo americano da forma mais inovadora, segura e econômica. A computação em nuvem desempenha um papel fundamental na forma como o governo federal pode alcançar eficiências operacionais e inovar sob demanda para promover sua missão em todo o país. É por isso que muitas agências federais atualmente estão usando os serviços de nuvem da AWS para processar, armazenar e transmitir dados do governo federal.

Para obter mais informações, consulte [FedRAMP](#).

HIPAA: A [AWS expandiu seu programa de conformidade com a Lei de Portabilidade e Responsabilidade de Seguros de Saúde \(HIPAA\) para incluir o AMS como um serviço qualificado pela HIPAA](#). Se você tem um Acordo de Associado Comercial (BAA) com a AWS, você pode usar o AMS para ajudar a criar seus aplicativos em conformidade com a HIPAA.

Consulte o [whitepaper focado na HIPAA](#) para saber como aproveitar o AMS para o processamento e armazenamento de informações de saúde. Para obter mais informações, consulte [Conformidade com a HIPAA](#).

HITRUST: A Estrutura de Segurança Comum da Health Information Trust Alliance (HITRUST CSF) utiliza padrões e regulamentos aceitos nacional e internacionalmente, como GDPR, ISO, NIST, PCI e HIPAA, para criar um conjunto abrangente de controles básicos de segurança e privacidade.

Para obter mais informações, consulte [HITRUST CSF](#).

A ISO 27001: ISO/IEC 27001:2013 é um padrão de gerenciamento de segurança que especifica as melhores práticas de gerenciamento de segurança e controles de segurança abrangentes seguindo a orientação de melhores práticas 27002. ISO/IEC A base dessa certificação é o desenvolvimento e a implementação de um rigoroso programa de segurança, que inclui o desenvolvimento e a implementação de um Sistema de Gerenciamento de Segurança da Informação (ISMS) que define como a AWS gerencia perpetuamente a segurança de forma holística e abrangente.

Para obter mais informações, consulte [ISO/IEC 27001:2013](#).

A ISO ISO/IEC 27017:2015 fornece orientação sobre os aspectos de segurança da informação da computação em nuvem, recomendando a implementação de controles de segurança da informação específicos da nuvem que complementam a orientação dos padrões 27002 e 27001. ISO/IEC ISO/IEC Esse código de prática fornece diretrizes adicionais de implementação de controles de segurança da informação específicas para provedores de serviços de nuvem.

Para obter mais informações, consulte Conformidade com [ISO/IEC 27017:2015](#).

A ISO ISO/IEC 27018:2019 é um código de prática que se concentra na proteção de dados pessoais na nuvem. Ele se baseia no padrão de segurança da ISO/IEC informação 27002 e fornece orientação de implementação sobre os controles ISO/IEC 27002 aplicáveis às Informações de Identificação Pessoal (PII) da nuvem pública. Ele também fornece um conjunto de controles adicionais e orientações associadas destinadas a atender aos requisitos de proteção de PII da nuvem pública não atendidos pelo conjunto de controle ISO/IEC 27002 existente.

Para obter mais informações, consulte Conformidade com [ISO/IEC 27018:2019](#).

A ISO 9001: ISO 9001:2015 descreve uma abordagem orientada a processos para documentar e revisar a estrutura , as responsabilidades e os procedimentos necessários para alcançar um gerenciamento de qualidade eficaz dentro de uma organização. Seções específicas do padrão contêm informações sobre tópicos como:

- Requisitos para um sistema de gestão da qualidade, incluindo documentação de um manual de qualidade, controle de documentos e determinação das interações do processo
- Responsabilidades da gerência
- Gerenciamento de recursos, incluindo recursos humanos e o ambiente de trabalho de uma organização
- Desenvolvimento de serviços, incluindo as etapas do design à entrega
- Satisfação de cliente
- Medição, análise e melhoria do SGQ por meio de atividades como auditorias internas e ações corretivas e preventivas

Para obter mais informações, consulte Conformidade [com a ISO 9001:2015](#).

PCI: O AMS tem um Atestado de Conformidade para o Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI), versão 3.2, no nível 1 do provedor de serviços. Clientes que usam produtos e serviços da AWS para armazenar, processar ou transmitir dados de titulares de cartões podem usar o AMS para gerenciar sua própria certificação de conformidade com o PCI DSS.

Para obter mais informações sobre PCI DSS, incluindo como solicitar uma cópia do pacote de conformidade com PCI da AWS, consulte [Nível 1 do PCI DSS](#). É importante ressaltar que você deve configurar políticas de senha refinadas no AMS para serem consistentes com os padrões do PCI DSS versão 3.2. Para obter detalhes sobre quais políticas devem ser aplicadas, consulte [Habilitar a conformidade com PCI para seu diretório AWS Microsoft AD](#).

SOC: Os relatórios de Controle Organizacional e de Sistema (SOC) da AMS são relatórios de exame independentes e terceirizados que demonstram como a AMS alcança os principais objetivos e controles de conformidade. O objetivo desses relatórios é ajudar você e seus auditores a entender os controles do AMS estabelecidos para apoiar as operações e a conformidade. Há três tipos de relatórios SOC do AMS:

- Relatório SOC 1 da AWS — [Baixe com o AWS Artifact](#)
- AWS SOC 2: relatório de segurança, disponibilidade e confidencialidade — [Baixe com o AWS Artifact](#)
- [AWS SOC 3: relatório de segurança, disponibilidade e confidencialidade](#)

Para obter mais informações, consulte [Conformidade com o SOC](#).

Responsabilidade compartilhada

A segurança, incluindo a conformidade com o PCI, é uma [responsabilidade compartilhada](#). É importante entender que o status de conformidade do AMS não se aplica automaticamente aos aplicativos que você executa na AWS nuvem. Você precisa garantir que o uso dos AWS serviços esteja em conformidade com os padrões. Para obter mais detalhes sobre como o AMS trabalha em conjunto com clientes em atividades específicas, consulte o AMS [Matriz de responsabilidade da AMS \(RACI\)](#).

Imagens de máquinas AMS Amazon (AMIs)

O AMS produz Amazon Machine Images (AMIs) atualizado todos os meses para sistemas operacionais compatíveis com o AMS. Além disso, o AMS também produz imagens de segurança aprimorada (AMIs) com base no benchmark CIS de nível 1 para um subconjunto dos sistemas operacionais [suportados pelo AMS](#). Para descobrir quais sistemas operacionais têm uma imagem de segurança aprimorada disponível, consulte o Guia do usuário de segurança do AMS, que está disponível na página AWS Artifact -> Reports (encontre a opção Reports no painel de navegação esquerdo) filtrada para AWS Managed Services. Para acessar o AWS Artifact, entre em contato com seu CSDM para obter instruções ou acesse Getting [Started with AWS](#) Artifact.

Para receber alertas quando novos AMS AMIs forem lançados, você pode assinar um tópico de notificação do Amazon Simple Notification Service (Amazon SNS) chamado “AMS AMI”. Para obter detalhes, consulte [Notificações da AMI do AMS com SNS](#).

A convenção de nomenclatura AMI do AMS é: `customer-ams-<operating system>-<release date> - <version>`. (por exemplo, `customer-ams-rhel6-2018.11-3`)

Use somente AMS AMIs que começam com `customer`.

O AMS recomenda sempre usar a AMI mais recente. Você pode encontrar as mais recentes AMIs de qualquer uma das seguintes maneiras:

- Procurando no console do AMS, na AMI página.
- Visualizando o arquivo CSV da AMS AMI mais recente, disponível em seu CSDM ou por meio desse arquivo ZIP: [conteúdo da AMS 11.2024 AMI e arquivo CSV](#) em um ZIP.

Para arquivos ZIP da AMI anteriores, consulte o [Histórico do documento](#).

- Executando este SKMS comando AMS (é necessário o SDK AMS SKMS):


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

Conteúdo AMI do AMS adicionado à base AWS AMIs, por sistema operacional (SO)

- Linux AMIs:
 - [AWS Ferramentas CLI](#)
 - [NTP](#)
 - [Agente de serviços de proteção de terminais da Trend Micro](#)
 - [Implantação de código](#)
 - [PBIS//Beyond Trust AD Bridge](#)
 - [SSM Agent](#)
 - Atualização do Yum para patches críticos
 - Software de gerenciamento e scripts personalizados do AMS (controle de inicialização, junção de AD, monitoramento, segurança e registro)
- Servidor Windows AMIs:
 - [Microsoft.NET Framework 4.5](#)
 - [PowerShell 5.1](#)
 - [AWS Ferramentas para Windows PowerShell](#)
 - PowerShell Módulos AMS que controlam inicialização, junção, monitoramento, segurança e registro do AD
 - [Agente de serviços de proteção de terminais da Trend Micro](#)
 - [SSM Agent](#)
 - [CloudWatch Agente](#)
 - EC2Serviço de configuração (por meio do Windows Server 2012 R2)
 - EC2Lançamento (Windows Server 2016 e Windows Server 2019)
 - EC2LaunchV2 (Windows Server 2022 e versões posteriores)

Baseado em Linux: AMIs

- Amazon Linux 2023 (última versão secundária) (AMI mínima não suportada)

- Amazon Linux 2 (última versão secundária)
- Amazon Linux (2ARM64)
- Red Hat Enterprise 7 (última versão secundária)
- Red Hat Enterprise 8 (última versão secundária)
- Red Hat Enterprise 9 (última versão secundária)
- Servidor SUSE Linux Enterprise 15 SP6
- Ubuntu Linux 18.04
- Ubuntu Linux 20.04
- Ubuntu Linux 22.04
- Ubuntu Linux 24.04
- Amazon Linux: Para obter uma visão geral do produto, informações de preços, informações de uso e informações de suporte, consulte [Amazon Linux AMI \(HVM/64 bits\)](#) e [Amazon Linux 2](#).

Para obter mais informações, consulte [Amazon Linux 2 FAQs](#).

- RedHat Enterprise Linux (RHEL): Para obter uma visão geral do produto, informações de preços, informações de uso e informações de suporte, consulte [Red Hat Enterprise Linux \(RHEL\) 7 \(HVM\)](#).
- Ubuntu Linux 18.04: Para uma visão geral do produto, informações sobre preços, informações de uso e informações de suporte, consulte [Ubuntu 18.04 LTS](#) - Bionic.
- SUSE Linux Enterprise Server para aplicativos SAP 15 SP6:
 - Execute as seguintes etapas uma vez por conta:
 1. Navegue até o AWS Marketplace.
 2. Pesquise o produto SUSE 15 SAP.
 3. Escolha Continue para assinar.
 4. Escolha Aceitar termos.
 - Conclua as etapas a seguir sempre que precisar iniciar uma nova SP6 instância do SUSE Linux Enterprise Server for SAP Applications 15:
 1. Anote o ID da AMI da AMI assinada do SUSE Linux Enterprise Server for SAP Applications 15.
 2. Crie uma implantação | Componentes avançados da pilha | pilha | Crie o tipo de alteração EC2 ct-14027q0sjyt1h RFC. *InstanceAmiId* Substitua pela ID da AWS Marketplace AMI na qual você se inscreveu.

Baseado em Windows: AMIs

Microsoft Windows Server (2016, 2019 e 2022), com base no Windows mais recente AMIs.

Para ver exemplos de criação AMIs, consulte [Criar AMI](#).

Desembarcando o AMS AMIs:

O AMS não compartilha nada AMIs de você durante a desativação para evitar impacto em nenhuma de suas dependências. Se quiser remover o AMS AMIs da sua conta, você pode usar a `cancel-image-launch-permission` API para ocultar informações específicas AMIs. Por exemplo, você pode usar o script abaixo para ocultar todos os AMS AMIs que foram compartilhados com sua conta anteriormente:

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

Você deve ter a AWS CLI v2 instalada para que o script seja executado sem erros. Para ver as etapas de instalação da AWS CLI, consulte [Instalando ou atualizando a versão mais recente da AWS CLI](#). Para obter detalhes sobre o `cancel-image-launch-permission` comando, consulte [cancel-image-launch-permission](#).

Segurança aprimorada AMIs

O AMS fornece imagens de segurança aprimorada (AMIs) com base no benchmark CIS de nível 1 para um subconjunto dos sistemas operacionais suportados pelo AMS. Para descobrir quais sistemas operacionais têm uma imagem de segurança aprimorada disponível, consulte o Guia de segurança do cliente do AWS Managed Services (AMS). Para acessar esse guia, abra AWS Artifact, selecione Reports no painel de navegação esquerdo e, em seguida, filtre por AWS Managed Services. Para obter instruções sobre como acessar AWS Artifact, entre em contato com seu CSDM ou consulte [Introdução AWS Artifact](#) para obter mais informações.

Como funciona a integração entre o AD FS e o AMS

Uma relação de confiança unidirecional entre sua rede local e o domínio AMS é o meio padrão de acesso às pilhas e VPCs. Quando uma VPC e uma pilha são criadas, o acesso é concedido

por meio de grupos de segurança pré-configurados do Active Directory. Além disso, o acesso ao Console de gerenciamento da AWS pode ser configurado usando o Serviço de Federação do Active Directory (AD FS) ou qualquer software de federação que suporte SAML, para um login único (SSO) no Management Console. AWS

 Note

O AMS pode se federar em vários serviços de federação, Ping, Okta e assim por diante. Você não está limitado ao AD FS; fornecemos aqui um exemplo de uma tecnologia de federação disponível para você.

As informações aqui estão duplicadas desta postagem do blog: [Habilitando a federação para AWS usar o Windows Active Directory, AD FS e SAML 2.0.](#)

1. O fluxo é iniciado quando um usuário (vamos chamá-lo de Bob) navega até o site de amostra do AD FS (<https://Fully.Qualified.Domain.Name.Here/adfs/ls/IdpInitiatedSignOn.aspx>) dentro de seu domínio. Ao instalar o AD FS, você obtém um novo diretório virtual chamado adfs para seu site padrão, que inclui essa página.
2. A página de login autentica Bob em relação ao AD. Dependendo do navegador que Bob está usando, ele pode ser solicitado a fornecer seu nome de usuário e senha do AD.
3. O navegador de Bob recebe uma declaração SAML na forma de uma resposta de autenticação do AD FS.
4. O navegador de Bob publica a declaração SAML no endpoint de AWS login do SAML (/saml). <https://signin.aws.amazon.com> Nos bastidores, o login usa a API [AssumeRoleWithSAML](#) para solicitar credenciais de segurança temporárias e, em seguida, cria uma URL de login para o Console de gerenciamento da AWS
5. O navegador de Bob recebe a URL de login e é redirecionado para o console.

Do ponto de vista de Bob, o processo acontece de forma transparente. Ele começa em um site interno e acaba no Console de gerenciamento da AWS, sem precisar fornecer nenhuma AWS credencial.

 Note

Mais informações sobre como configurar a federação no console AMS são fornecidas em:

- Zona de aterrissagem com várias contas: [configurando a federação no console AMS](#)
- Zona de aterrissagem de conta única: [configurando a federação no console AMS](#)

Além disso, consulte o [Apêndice: regra de declaração do AD FS e](#) configurações de SAML. Para obter informações sobre como usar o AWS Microsoft AD para oferecer suporte aos aplicativos compatíveis com o Active Directory, na AWS nuvem, que estão sujeitos aos requisitos de conformidade, consulte Gerenciar a conformidade [do Microsoft AD](#).

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](#).

Implantações de aplicativos AMS

O guia do desenvolvedor de aplicativos AMS fornece descrições detalhadas e orientações para as seguintes implantações:

- A CT de ingestão de carga de trabalho do AMS permite que você e um parceiro de migração para a nuvem do AMS movam facilmente suas cargas de trabalho existentes para uma VPC gerenciada pelo AMS. Usando a ingestão de carga de trabalho do AMS, você pode criar uma AMI do AMS enviando uma RFC com a instância migrada Deployment | Inestion | Stack from migration partner migrated | Create CT (ct-257p9zjk14ija). Você deve ter uma instância migrada do seu local para a de um parceiro AWS de migração, bem como uma VPC e uma sub-rede do AMS de destino, nas quais a instância será ingerida.

Para obter detalhes, consulte o guia do desenvolvedor de aplicativos AMS em [Workload Ingest](#).

- O recurso de tipo de alteração de CloudFormation ingestão (ct-36cn2avfrrj9v) permite que você use facilmente um modelo existente para implantar pilhas personalizadas em uma VPC gerenciada pelo AMS. CloudFormation

Para obter detalhes, consulte o guia do desenvolvedor de aplicativos AMS em [CloudFormation Template Ingest](#).

- Você pode importar seu banco de dados local em um novo banco de dados para seu bucket Amazon S3 gerenciado pela AMS ou instância do Amazon RDS. Você faz isso usando um Deployment | Advanced stack components | Tipos de alteração do Database Migration Service (DMS), incluindo Criar instância de replicação (ct-27aplkhqr0ol), Criar grupo de sub-rede de replicação (ct-2q5azjd8p1ag5), Criar tarefa de replicação (ct-1d2fml15b9eth), Criar endpoint de origem (ct-0attesnj5) qy2cx) ou Criar endpoint de origem (S3) (ct-2oxl37nphsrjz) e Criar endpoint de destino (ct-3gf8dolbo8x9p) ou Criar endpoint de destino (S3) (ct-05muqzievnxk5).

Para obter detalhes, consulte o guia do desenvolvedor de aplicativos AMS no [Database Migration Service](#).

- Você pode importar seu banco de dados MS SQL local para um novo banco de dados em sua instância RDS SQL gerenciada pelo AMS. Você faz isso usando uma variedade de tipos de alteração do AMS e a API do Amazon RDS, além de AWS consoles.

Para obter detalhes, consulte o Guia do aplicativo AMS em [Importação de banco de dados \(DB\) para MS SQL RDS](#).

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	Análise 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: represent ante 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: represent ante 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

Atividade s	Cliente	AMS
Compilando recomendações de redução de custos e preparando o relatório	eu	R
Apresentando relatório de economia de custos	C	R
Planejando as 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

Atividade s	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](#).

Gerenciamento de eventos planejados no AWS Managed Services

O gerenciamento planejado de eventos (PEM) do AWS Managed Services (AMS) é uma oferta de serviço do AMS. O PEM se envolve, coordena e auxilia durante eventos e projetos de clientes usando os serviços do AMS. O PEM auxilia na coordenação de um conjunto de assuntos relacionados RFCs que se alinham com o escopo e o cronograma acordados do evento ou projeto do PEM.

Critérios AMS PEM

Um evento planejado é um projeto com limite de escopo e tempo. O AMS usa os detalhes que você fornece (incluindo plano e escopo, resultados esperados e mudanças que as operações do AMS devem realizar) para apoiá-lo efetivamente durante a atividade do PEM. Seus arquitetos de nuvem (CAs) então revisam e avaliam a atividade do PEM quanto à integridade, à implementação técnica e ao engajamento operacional do AMS. Após a análise da CA, as operações do AMS analisam os planos e coordenam com seu gerente de prestação de serviços em nuvem (CSDM) o engajamento da equipe de operações.

Tipos de PEM

A seguir estão os tipos de PEM disponíveis:

- Dias de jogos
 - Operational Gameday: Uma abordagem de resposta operacional baseada em cenários, com o objetivo de validar a integração de processos, pessoas e sistemas.
 - Security Gameday: uma estratégia de resposta a incidentes de segurança que emprega uma abordagem de jogo baseada em cenários para avaliar a integração de sistemas, processos e pessoal.
- BYOEPS: Use o recurso “traga sua própria segurança de endpoint” (BYOEPS) do AMS para substituir o agente padrão do Trend Micro Deep Security pela solução de segurança de endpoint de sua preferência ou por uma licença personalizada da Trend Micro. Para obter mais informações, consulte [AMS: traga seu próprio EPS](#).

- Recuperação de desastres: os eventos de recuperação de desastres envolvem a assistência do AMS durante suas atividades planejadas de DR. Para obter mais informações, consulte [planejamento de recuperação de desastres](#).
- Evento de segurança do cliente: eventos de segurança planejados. Por exemplo, atividade do usuário root e testes de penetração.
- Suporte à migração: Suporte para atividades planejadas de integração e migração.

Esse fluxo de trabalho facilita a colaboração com o AMS para coordenar eventos planejados e atividades de migração em relação ao suporte do AMS. Para execução prioritária RFCs, é uma prática recomendada usar o engajamento de Operações sob Demanda (OOD). Para obter mais informações, consulte [Operações sob demanda](#).

O processo AMS PEM

O processo PEM consiste nas seguintes fases:

- Iniciação do PEM: Você trabalha com seu CSDM para definir seu objetivo para o evento planejado e determinar o que é necessário das operações do AMS. O AMS CAs revisa os aspectos técnicos do plano PEM. O CAs trabalho com a AMS Security and Operations na conformidade, otimização e automação da execução e na definição de tarefas e resultados de execução pré-PEM. Em seguida, seu CSDM cria o tíquete PEM e fornece ao AMS as informações do projeto e os detalhes técnicos. O AMS exige um prazo de 14 dias corridos para permitir que a equipe de operações do AMS tenha tempo para planejar, fornecer análises técnicas e atribuir recursos.
- Revisão do PEM: a equipe de operações do AMS analisa a solicitação do PEM e trabalha com seu CSDM para verificar se as informações no plano do PEM estão corretas e completas.
- Aceitação do PEM: O AMS analisa as informações fornecidas e comunica ao CSDM qual será o nível de suporte durante a atividade do PEM. Se o PEM contiver informações completas e seu CSDM concordar com o escopo do trabalho, o PEM será aprovado.
- Prontidão e execução: O AMS garante que as tarefas necessárias antes do início do PEM sejam concluídas e facilita a comunicação interna e com o cliente. O AMS garante que o plano PEM seja executado corretamente e forneça relatórios de status e progresso.

PEM FAQs

Como faço para interagir com o AMS com uma RFC/Service solicitação (SR) durante um evento de PEM?

- Use o ID do PEM compartilhado pelo seu CSDM na linha de RFC/SR assunto do formato. *PEM-ID*
- Você também pode criar uma Solicitação de Serviço (SR) para discutir seus casos de uso ou tirar dúvidas sobre o evento planejado. Se você usa um SR, o PEM não precisa ser válido.

Quais validações são realizadas quando uma RFC relacionada ao PEM é enviada?

- Verificação de que o ID da conta está listado no PEM.
- Verificação de que o status do PEM foi aprovado e ativo entre as datas de início e término fornecidas.

Existem SLAs ou SLOs para solicitações de PEM?

- PEMs não estão associados a SLAs ou SLOs.
- SLAs e SLOs para itens de trabalho relacionados ao PEM (RFC/Solicitação de Serviço), são definidos pelo AMS. SLOs

Para obter mais informações, consulte [Objetivos de nível de serviço do AMS \(SLOs\)](#).

Podemos criar um PEM por meio de uma Solicitação de Serviço (SR)?

- Não, a criação do PEM deve ser gerenciada pelo Cloud Service Delivery Manager (CSDM).

Arquitetura de rede

O AWS Managed Services (AMS) oferece duas arquiteturas de rede:

- Multi-account landing zone (MALZ): fornece serviços comuns, como acesso, segurança de terminais e rede, a partir de contas compartilhadas para cargas de trabalho implantadas em contas de membros separadas.
- Single-account landing zone (SALZ): fornece contas independentes em que serviços comuns, como acesso, segurança de terminais e rede, são implantados na mesma conta da carga de trabalho. É recomendado para cargas de trabalho que exigem um alto nível de isolamento, pois gera custos mais altos da AWS.

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.

Entidade	Zona de pouso única do AMS	Várias (duas ou mais) zonas de pouso
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 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.

Entidade	Zona de pouso única do AMS	Várias (duas ou mais) zonas de pouso
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).
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.

Entidade	Zona de pouso única do AMS	Várias (duas ou mais) zonas de pouso
Conformidade e segurança	(Depende) Baixo se houver necessidade 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 externas Prod/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
    "*" as x1, @x2, @x3, @x4, @type, @x6, @x7, @source_ip, @destination_ip, @source_nat_ip,
@dest_nat_ip, @rule, @x13, @x14, @application, @x16, @from_zone, @to_zone,
@x19, @x20, @x21, @x22, @session_id, @x24, @source_port, @destination_port,
@source_nat_port, @destination_nat_port, @x29, @protocol, @action, @bytes,
@bytes_sent, @bytes_recieved, @packets, @x36, @x37, @category, @x39, @x40, @x41,
@source_country, @destination_country, @x44, @packets_sent, @packets_recieved,
@session_end_reason, @x48, @x49, @x50
| display @timestamp, @rule, @action, @session_end_reason, @protocol, @source_ip,
@destination_ip, @source_port, @destination_port, @session_id, @from_zone,
@to_zone, @category, @bytes_sent, @bytes_recieved, @packets_sent, @packets_recieved,
@source_country, @destination_country
```

Modelo de failover

A solução de firewalls inclui dois ou três hosts de Palo Alto (PA) (um por AZ). Os canários Healthy Check funcionam em um cronograma constante para avaliar a saúde dos hospedeiros. Se um host for identificado como não íntegro, o AMS será notificado e o tráfego dessa AZ será automaticamente transferido para um host íntegro em outra AZ por meio da alteração da tabela de rotas. Como o fluxo de trabalho da verificação de integridade está em execução constante, se o host ficar íntegro novamente devido a problemas transitórios ou à correção manual, o tráfego será direcionado de volta para a AZ correta com o host íntegro.

Escalabilidade

O AMS monitora o firewall quanto aos limites de taxa de transferência e escalabilidade. Quando os limites de taxa de transferência excedem os limites mais baixos da marca d'água (CPU/rede), o AMS recebe um alerta. Um limite baixo de produção de água indica que os recursos estão se aproximando da saturação, chegando a um ponto em que a AMS avaliará as métricas ao longo do tempo e tentará sugerir soluções de escalabilidade.

Backup e restauração

Os backups são criados durante a inicialização inicial, após qualquer alteração na configuração e em intervalos regulares. Os backups de inicialização inicial são criados por host, mas as alterações

na configuração e os backups com intervalos regulares são realizados em todos os hosts de firewall quando o fluxo de trabalho de backup é invocado. Os engenheiros do AMS podem criar backups adicionais fora dessas janelas ou fornecer detalhes do backup, se solicitado.

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, consulte [CloudWatch 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” aplicativo, 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.

Tipo de log	Descrição
	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 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 autenticação para registrar os tempos limite de autenticação. Esses tempos limite estão relacionados ao período em que um usuário precisa se autenticar 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.

Tipo de log	Descrição
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
 - DataPlanePacketBufferUtilization
 - 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
 - $0,0416 \text{ USD} * 24 * 30 * 3 = 89,86 \text{ US\$}$
 - <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 EPSTransmissionSubscriptionRole 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/VPN para 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, consulte [Modos 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 `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 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](#).

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.

Configurando o AMS

Tópicos

- [Entenda as configurações padrão do AMS](#)
- [Usando os consoles AMS](#)
- [Usando a API e a CLI do AMS](#)
- [AMS: traga seu próprio EPS](#)
- [Recebendo notificações do AMS](#)
- [Configurando DNS público e privado](#)
- [Gerenciamento de tráfego de saída do AMS](#)
- [Implantação de recursos do IAM no AMS Advanced](#)
- [Definindo permissões no AMS com funções e perfis do IAM](#)
- [Regra de declaração do AD FS e configurações de SAML](#)
- [Restringir com ACL de rede](#)
- [AMS em Outposts](#)
- [Usando tags no AMS](#)
- [Agendador de recursos do AWS Managed Services](#)
- [AWS Systems Manager no AMS Advanced](#)
- [Contas AMS externas](#)

Algumas tarefas de configuração do AMS podem ser concluídas na integração.

Para obter uma descrição completa das funções e responsabilidades, incluindo o AMS [AWS Serviços suportados](#), consulte [Matriz de responsabilidade da AMS \(RACI\)](#).

Note

Para solicitar que o AMS forneça um AWS serviço adicional, registre uma solicitação de serviço. Para obter informações sobre como fazer essa solicitação, consulte [Gerenciamento de solicitações de serviço](#).

Entenda as configurações padrão do AMS

Sua rede AWS Managed Services (AMS) tem uma configuração padronizada com padrões para a maioria dos serviços.

Esta seção descreve as configurações padrão que o AMS usa para acesso, monitoramento e gerenciamento de registros.

Para obter um exemplo de custos de infraestrutura de zona de pouso com várias contas ou zona de pouso com conta única, consulte [Componentes básicos do ambiente AMS](#)

Tópicos

- [Padrões de resolução de DNS \(MALZ\)](#)
- [EC2 Perfil de instância do IAM](#)
- [Alertas do monitoramento de linha de base no AMS](#)
- [Padrões de retenção e rotação de registros](#)

Padrões de resolução de DNS (MALZ)

Landing zone de várias contas do AWS Managed Services (AMS): nos ambientes da AWS, a resolução do sistema de nomes de domínio (DNS) entre o Resolver do Route 53 e os resolvedores de DNS em uma VPC pode ser integrada configurando as regras de encaminhamento do Resolver. Antes que essas regras possam ser usadas para encaminhar consultas de DNS, os endpoints do resolvidor de entrada e saída precisam ser configurados para os quais essas consultas possam ser encaminhadas.

Por padrão, as consultas de DNS dentro da conta do aplicativo VPCs em configurações de várias contas no AMS são encaminhadas para os encaminhadores condicionais do domínio AWS Directory Service for Microsoft Active Directory (também conhecido como Managed AD) presente na conta de serviços compartilhados. Opcionalmente, o AMS permite que você use o AmazonProvided DNS; por exemplo, o DNS para o qual encaminhar consultas de AmazonProvided DNS. Isso ajuda você a utilizar VPC endpoints que atualmente só oferecem suporte ao DNS fornecido pela Amazon por meio do Amazon Route 53. Da mesma forma, as regras do Resolver também são configuradas automaticamente para endpoints de VPC comuns que são implantados por padrão na conta de serviços compartilhados. Para obter mais informações sobre esses endpoints de VPC comuns, consulte [Endpoints VPC do AMS](#)

Para configurar conjuntos de opções do Dynamic Host Configuration Protocol (DHCP) em toda a sua conta de aplicativo VPCs para usar o DNS fornecido pela Amazon para endpoints VPC e fazer com que as regras do Route53 Resolver apontem para os endpoints VPC comuns em suas contas de serviços compartilhados (com uma regra de resolução opcional para domínio local), crie um Gerenciamento | Outro | Outro | Crie uma solicitação de alteração (RFC) especificando a conta de serviços compartilhados e solicitando a habilitação implementação das regras VPC, DNS local e Route 53 Resolver da conta do aplicativo para endpoints de VPC.

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
	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.

Perfil	Políticas
customer-mc-ec2-instance-profile-s3	AMSInstanceProfileBY0EPSPolicy : 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 <code>aws:iam::*:role/customer-*</code> <code>aws:iam::*:role/customer_*</code> e.
Instância para fazer upload de eventos de log	Permitir	Criar grupo de registros	Permite que os registros sejam criados em: <code>aws:logs:*:*:log-group:i-*</code>
		Criar fluxo de log	Permite que os registros sejam transmitidos para: <code>aws:logs:*:*:log-group:i-*</code>
CW para MMS	Permitir	DescribeAlarms, PutMetricAlarm,	Permite CloudWatch recuperar alarmes em sua conta.

CW = CloudWatch. ARN = Nome do recurso da Amazon. * = curinga (qualquer).

Declaração da política	Efeito	Ações	Descrição e recurso (ARN)
		PutMetricData	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 especificadas em sua conta.
Negar explicitamente os registros do CW	Deny	DescribeLogStreams, FilterLogEvents, GetLogEvents	Não permite listar, filtrar ou obter os fluxos de log para: <code>aws:logs:*:*:log-group:/mc/*</code>
Amazon EC2 Simple Systems Manager (SSM)			
Ações do SSM	Permitir	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	Permite uma variedade de funções de SSM em sua conta.

CW = CloudWatch. ARN = Nome do recurso da Amazon. * = curinga (qualquer).

Declaração da política	Efeito	Ações	Descrição e recurso (ARN)
Acesso SSM no S3	Permitir	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadParts, ListBucketMultipartUploads	Permite que o SSM no EC2 obtenha e atualize objetos, aborte o upload de um objeto de várias partes e liste partes e compartimentos disponíveis para carregamentos de várias partes. <code>aws:s3:::mc-**-internal-*/aws/ssm*</code>

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 <code>aws:s3:::mc-**-logs-*/encrypted/app/*</code>
Patch Data Put Object S3	Permitir	PutObject	Permite que EC2 os aplicativos carreguem dados de patches para seus buckets do S3 em <code>aws:s3:::awsms-a*-patch-data-*</code>
Carregando seus próprios registros para o S3	Permitir	PutObject	Permite que os EC2 aplicativos carreguem registros personalizados para: <code>aws:s3:::mc-a*-logs-*/aws/instances/*/\${aws:userid}/*</code>

CW = CloudWatch. ARN = Nome do recurso da Amazon. * = curinga (qualquer).

Declaração da política	Efeito	Ações	Descrição e recurso (ARN)
Negar explicitamente os registros do MC Namespace S3	Deny	GetObject* Coloque*	Não permite que EC2 aplicativos obtenham ou coloquem objetos de ou para: <code>aws:s3:::mc-*logs-*/encrypted/mc*</code> , <code>aws:s3:::mc-*logs-*/mc/*</code> , <code>aws:s3:::mc-a*-logs-*audit/*</code>
Negar explicitamente a exclusão do S3	Deny	* (tudo)	Não permite que EC2 aplicativos realizem qualquer ação em objetos em: <code>aws:s3:::mc-a*-logs-*/*</code> , <code>aws:s3:::mc-a*-internal-*/*</code> ,
Negar explicitamente o bucket CFN do S3	Deny	Delete*	Não permite que EC2 aplicativos excluam objetos de: <code>aws:s3:::cf-templates-*</code>
Negar explicitamente o List Bucket S3	Deny	ListBucket	Não permite que você liste objetos criptografados, de registro de auditoria ou reservados (mc) de: <code>aws:s3:::mc-*logs-*</code>

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: <pre>aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- id* , arn:aws:secretsman ager:~::~secret:/ams/ eps/cloud-one-agent- activation-token* , aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- id* , aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- guid*</pre>

AWS Key Management Service 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 <pre>arn:aws:kms:~::~alias/ ams/eps/cloudone-migrat ion</pre>

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.

Alertas do monitoramento de linha de base no AMS

Saiba mais sobre os padrões de monitoramento do AMS. Para obter mais informações, consulte [Monitoramento e gerenciamento de eventos no AMS](#).

A tabela a seguir mostra o que é monitorado e os limites de alerta padrão. Você pode alterar os limites de alerta com uma RFC Management | Other | Other | Update (ct-0xdawir96cy7k) depois de determinar quais alterações você deseja e assinar o tópico relevante do Amazon SNS. CloudWatch Para obter informações sobre como criar e assinar tópicos, consulte [Inscrever-se em um tópico](#). Para obter informações gerais, consulte [Amazon SNS FAQs](#). Para ser notificado diretamente quando os alarmes ultrapassarem seu limite, além do processo de alerta padrão do AMS, siga estas instruções sobre como substituir as configurações de alarme,. [Recebendo alertas gerados pelo AMS](#)

A Amazon CloudWatch fornece retenção estendida de métricas. Para obter mais informações, consulte [CloudWatch Limites](#).

 Note

O AMS calibra seu monitoramento de linha de base periodicamente. Novas contas são sempre integradas com o monitoramento de linha de base mais recente e a tabela descreve o monitoramento básico de uma conta recém-integrada. O AMS atualiza o monitoramento básico das contas existentes periodicamente e você pode enfrentar um intervalo de tempo antes que as atualizações sejam implementadas. Para obter mais informações, consulte [Visualizando a configuração de monitoramento de uma conta AMS](#).

Note

O alerta da EC2 instância Non-root volume usage está DESATIVADO por padrão. [Se você precisar de geração de alertas com base nesse alarme, deverá habilitá-lo usando o Tipo de Alteração RFC ct-0erkoad6uyvvg](#)

Alertas do monitoramento de linha de base

Serviço	Alerta de segurança	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.
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	CloudWatch alarme.

Serviço	Alerta de segurança	Nome do alerta e condição do gatilho	Observações
		> 85% por 5 minutos, 2 vezes consecutivas.	
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	AMSOupostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 80% por 5 minutos, 12 vezes consecutivas.	CloudWatch alarme sobre a disponibilidade da capacidade familiar de instâncias do AWS Outposts recurso.
		AMSOupostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80% por 5 minutos, 12 vezes consecutivas.	CloudWatch alarme sobre a disponibilidade da capacidade e do tipo de instância do AWS Outposts recurso.
		AMSOupostsConnectedStatus ConnectedStatus < 1 por 5 minutos, 1 vez consecutiva.	CloudWatch alarme na conexão do link de AWS Outposts serviço, menos de 1 contagem está prejudicada.
		AMSOupostsCapacityException CapacityExceptions 0 por 5 minutos, 1 vez consecutiva.	CloudWatch alarme sobre erros de capacidade insuficiente, por exemplo, lançamentos AWS Outposts de um recurso .

Serviço	Alerta de segurança	Nome do alerta e condição do gatilho	Observações
EC2 instância - tudo OSs	Não	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.	
		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.	

Serviço	Alerta de seguran	Nome do alerta e condição do gatilho	Observações
		Sem memória*	
		MemoryFree < 5% por 5 minutos, 6 vezes consecutivas.	
	Sim	Malware EPS	CloudWatch evento.
		Malware encontrado na instância.	
EC2 Instância da Amazon - Linux	Não	Uso do Inode do Volume Raiz	CloudWatch alarme. Aplicado somente às instâncias do Linux.
		Média >= 95% por 5 minutos, 6 vezes consecutivas.	
		Grátis para troca*	
		Troca de memória < 5% por 5 minutos, 6 vezes consecutivas.	
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 segurança	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 .
		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 segurança	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 $\geq 80\%$ 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 $\geq 80\%$ 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 verticalmente até 64 GiB de RAM, sendo que nesse ponto você poderá dimensionar horizontalmente adicionando instâncias.
		Mestre CPUUtilization a média é $\geq 50\%$ 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/green 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 $\geq 80\%$ 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/green 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 segurança	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 funcionando 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 segurança	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 restauração.	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 configuração 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 segurança	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 informações 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 segurança	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 restabelecendo seu espelho. O desempenho 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 recuperação 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 segurança	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% do 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 segurança	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. DiskQueueDepth A soma é > 75 por 1 minuto, 15 vezes consecutivas.	CloudWatch alarme.

Serviço	Alerta de segurança	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 atualizações 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 compatíveis, consulte Analisando as descobertas do Amazon Macie . Observe que o Macie não está habilitado para todas as contas.

O AMS realiza ações proativas (escalando o cluster) quando esse alerta é acionado.

Para obter informações sobre os esforços de remediação, consulte [Remediação automática de alertas pelo AMS](#).

[Assista ao vídeo de Andrew para saber mais \(7:03\)](#)

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.

Usando os consoles AMS

Os consoles AMS no AWS Management Console estão disponíveis para você interagir com o AMS e operar seus recursos gerenciados pelo AMS Advanced e pelo AMS Accelerate. Os consoles AMS geralmente se comportam como qualquer AWS console; no entanto, como o AMS é uma organização privada, somente contas habilitadas para o AMS podem acessar o console. Depois que o AMS estiver ativado em sua conta, você poderá acessar o console pesquisando por “Managed Services” na barra de pesquisa unificada.

Note

Dependendo da função da sua conta, você acessa o console do AMS Advanced ou o console do AMS Accelerate.

Ao usar os consoles AMS, esteja ciente das seguintes ressalvas:

- O console AMS é específico da conta. Portanto, se você estiver em uma conta de “Teste” da sua organização, não poderá ver os recursos na conta “Prod” dessa organização. Da mesma forma, você deve ter uma função do AMS Advanced para acessar o console do AMS Advanced.
- Os consoles AMS aplicam uma política do IAM quando você se autentica que determina qual console você pode acessar e o que você pode fazer lá. Seu administrador pode aplicar políticas adicionais à política padrão do AMS para restringir o que você pode ver e fazer no console.

O console AMS Advanced tem os seguintes recursos:

- Página de abertura: A página de abertura tem caixas de informações e links para facilitar seu acesso aos incidentes RFCs, solicitações de serviço e relatórios existentes.
- Páginas de destaque, links no painel de navegação esquerdo:
 - Painel: fornece uma visão geral do status atual da sua conta, incluindo:
 - Solicitações de mudança: veja quantas RFCs estão aguardando sua resposta e vá para a página da lista de RFC com esse filtro ativo. Veja quantos RFCs estão aguardando sua aprovação e vá para a página da lista de RFC com esse filtro ativo. Veja quantos RFCs estão abertos e vá para a página da lista de RFC com esse filtro ativo. Abra a página da lista RFCs clicando no link Exibir tudo.
 - Incidentes: veja quantos casos de incidentes estão aguardando sua resposta e vá para a página da lista de incidentes com esse filtro ativo. Veja quantos estão abertos e vá para a página da lista de incidentes com esse filtro ativo. Abra a página da lista de incidentes clicando no link Exibir tudo.
 - Solicitações de serviço: veja quantas solicitações de serviço estão aguardando sua resposta e vá para a página da lista de solicitações de serviço com esse filtro ativo. Veja quantas estão abertas e vá para a página da lista de solicitações de serviço com esse filtro ativo. Abra a página da lista de solicitações de serviço clicando no link Exibir tudo.
 - Atualizado recentemente RFCs: data, link para os detalhes do RFC e status
 - Incidentes e solicitações de serviço criados recentemente: data, link para os detalhes do caso e tipo (incidente ou solicitação de serviço)
 - RFCs: abre uma lista dos existentes RFCs para a conta
 - Incidentes: abre uma lista dos incidentes abertos da conta
 - Solicitações de serviço: abre uma lista das solicitações de serviço abertas para a conta
 - Relatórios: abre a página Relatórios e os relatórios padrão, Backup Diário, Patch Diário e Cobrança Mensal

- Recursos:
 - VPCs: abre uma lista dos existentes VPCs para a conta
 - Pilhas: abre uma lista das pilhas existentes para a conta
 - AMIs: Abre uma lista de AMS disponíveis AMIs
- Destaque do recurso: informações sobre as atualizações mais recentes do console
- Recursos para desenvolvedores: uma página de arquivos para download, incluindo o SDK de gerenciamento de alterações avançado do AMS e muito mais
- Documentação: A página inicial da documentação do AWS Managed Services

Usando a API e a CLI do AMS

A API do AWS Managed Services (AMS) é semelhante à APIs de outros AWS serviços. Você pode ler sobre a API do AMS na [Referência da API do AMS](#).

Pontos de extremidade HTTP da API AMS para chamadas REST

Além dos vários SDKs, o AMS fornece uma CLI; você também pode invocar chamadas de API REST no endpoint do AMS.

Há dois AMS APIs (o endpoint de ambos reside em us-east-1):

- Gerenciamento de mudanças: use essa API para solicitar acesso ou alterações em sua infraestrutura, incluindo criação e atualização RFCs, implantação de novas instâncias, atualização e exclusão de instâncias, obtenção de informações e criação. CTs AMIs O endpoint HTTP é:

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

- SKMS: use essa API para obter informações sobre sua infraestrutura VPCs, incluindo pilhas, sub-redes e. AMIs O endpoint HTTP é:

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

Instalando ou atualizando a CLI do AMS

A CLI do AMS é uma maneira fácil de interagir com a API do AMS e é usada nos exemplos desta seção. Para convenções de uso da CLI e da AWS CLI do AMS, [consulte Usando AWS](#) a interface de linha de comando.

Para obter informações sobre a instalação do SAML, consulte [Regra de declaração do AD FS e configurações de SAML](#).

Para instalar ou atualizar a CLI do AMS, siga estas instruções:

 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

- 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.
- 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`

Usando a API AMS em CLI, Ruby, Python e Java

Veja a seguir uma lista de trechos de código para a

ListChangeTypeClassificationSummaries operação da API AMS, em todos os idiomas disponíveis.

Para Python, Ruby e Java SDKs, consulte [Ferramentas para Amazon Web Services e role para baixo](#) até a seção. SDKs Cada instalador do SDK contém um README com trechos de código adicionais.

Exemplo de API AMS para CLI

Depois de instalar a CLI do AMS (requer a AWS CLI; consulte [Instalando ou atualizando a CLI do AMS](#)), você pode executar qualquer operação da API do AMS reformando a chamada, primeiro especificando qual API do AMS `aws amscm` ou `aws amsskms`, em seguida, executando a ação com hífen substituindo camel case. Por fim, forneça credenciais, como SAML.

Para saber mais, consulte [Usando a interface de linha de AWS comando](#).

Exemplo:

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

Note

Se você se autenticar com SAML, adicione `aws --profile saml` ao início do comando. Por exemplo,

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

Exemplo de API AMS para Python

Para usar a API AMS com Python, instale a CLI do AMS e instale o boto3. Siga estas etapas:

1. Instale o AMS CLI. Consulte [Instalando ou atualizando a CLI do AMS](#).
2. Instale o boto3, o AWS SDK para Python. Para obter mais informações, consulte esta postagem do blog [Agora disponível — AWS SDK para Python \(Boto3\)](#).

```
import boto3
```

3. Obtenha o cliente AMS Change Management:

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

4. Obtenha o AMS CTs:

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

```
print(cts)
```

Exemplos de Python

A seguir estão alguns exemplos de como usar o Python no AMS, para criar EC2 instâncias, use o and/or Lambda.

Exemplo em Python para criar um EC2

Este exemplo mostra como você pode usar a RESTFul API amscm de dentro do código Python para arquivar e executar processos RFC.

1. Instale a CLI do AMS em algum lugar ao qual você tenha acesso; você precisa dos arquivos que ela fornece.
2. Chame as bibliotecas do Python e crie a EC2 instância:

```
import boto3
import json
import time

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

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

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

# Extract the RFC ID from the response
```



```
NewRfcID = cts['RfcId']

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

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

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

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

Exemplo de Python com Lambda

Este exemplo mostra como agrupar os modelos AMS com seu código para que você possa usá-lo com o Lambda, EC2 ou; lugares que você não quer ou não pode instalar. `awscli`

Note

O AMS não fornece um SDK Python específico importável do AMS. O script de `awscli` instalação instala os modelos de dados do serviço AMS no caminho normal da CLI. Para o uso da CLI e do sistema Python, tudo bem, porque ambos `awscli` e `boto3` lêem seus modelos de serviço nos mesmos locais padrão (`~/.aws/models`). No entanto, quando você deseja usar serviços AMS via `boto3` no Lambda (ou em qualquer outro tempo de execução não local), ele falha, porque você não tem mais os modelos de dados. A seguir está um método para corrigir isso empacotando os modelos de dados com a função.

Há etapas simples que você pode seguir para executar seu código Python integrado ao AMS no Lambda ou em outro tempo de execução, como Fargate, etc. EC2 O fluxo de trabalho a seguir mostra as etapas necessárias para as funções Lambda integradas ao AMS.

Ao adicionar os modelos de dados ao pacote de implantação do código e atualizar o caminho de pesquisa do SDK, você pode simular uma experiência de SDK.

Important

Este exemplo e todos os comandos não python mostrados foram testados em um computador Mac.

Exemplo de fluxo de trabalho:

1. Instale o `amsccli`. Isso cria uma pasta `~/ .aws/models` no seu computador (Mac).
2. Copie os modelos para um diretório local: `cp ~/ .aws/models ./models`.
3. Inclua os modelos no pacote de implantação do seu código.
4. Atualize seu código de função para adicionar os novos modelos ao caminho do SDK. Observe que esse código deve ser executado antes da importação do `boto3` ou do `botocore`!

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

import boto3
import botocore
```

Note

Como os modelos de exemplo estão em um diretório chamado `models`, adicionamos `./models` ao `AWS_DATA_PATH`. Se o diretório fosse nomeado `ams/boto3models`, adicionaríamos o seguinte código:

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

import boto3
```

```
import boto3
```

Seu código deve encontrar com sucesso os modelos AMS. Como um exemplo mais específico sobre embalagem, aqui está o fluxo de trabalho específico do Lambda.

Exemplo de fluxo de trabalho do AMS Lambda:

Essas etapas aplicam o exemplo genérico anterior à criação de uma função do AWS Lambda.

1. Instale o `amscli`. Isso cria uma pasta `~/ .aws/models` no seu computador (Mac).
2. Copie os modelos para um diretório local:

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

3. Adicione os modelos ao arquivo zip de implantação da sua função:

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

Important

Atualize seu código de função para adicionar os novos modelos ao caminho do SDK. Observe que esse código deve ser executado antes da importação do `boto3` ou do `botocore`!

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

import boto3
import botocore
```

Note

Como os modelos de exemplo estão em um diretório chamado `models`, adicionamos `./models` ao `AWS_DATA_PATH`. Se o diretório fosse nomeado `/ams/boto3models`, adicionaríamos o seguinte código:

```
import os
```

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

import boto3
import botocore
```

Agora, implante sua função:

1. Adicione seu código de função ao arquivo zip de implantação (se você ainda não tiver feito isso):

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

2. Crie ou atualize sua função com o arquivo zip que você criou (console ou CLI):

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

Seu Python Lambda integrado ao AMS agora deve funcionar.

Note

Sua função deve ter permissões do IAM amscm ou você receberá um erro de permissão.

Exemplo de código da função Lambda para testar o amscm (conteúdo de.py): lambda-amscm-test

```
import json

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

import boto3
import botocore

def lambda_handler(event, context):
    use_session = boto3.session.Session(region_name="us-east-1")
    try:
        cm = use_session.client("amscm")
```

```
cts = cm.list_change_type_categories()
print(cts)
except botocore.exceptions.UnknownServiceError:
    print("amscm not found")

return {
    'statusCode': 200,
    'body': json.dumps('Hello from Lambda!')
}
```

Resultados do teste (sucesso):

Resposta da função:

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

Request ID:

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

Registros de funções:

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

Exemplo de API AMS para Ruby

Para usar a API AMS com Ruby, instale o SDK do AWS Ruby e a CLI do AMS. Siga estas etapas:

1. Instale o AMS CLI. Consulte [Instalando ou atualizando a CLI do AMS](#).
2. Instale o SDK do AWS Ruby. Consulte [Ferramentas para Amazon Web Services](#).
3. Configure o Ruby com estes comandos:

```
require 'aws-sdk'
```

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

4. Obtenha o AMS CTs:

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

Exemplo de API AMS para Java

Para usar a API AMS com Java, instale o AWS Java SDK e o AMS CLI. Siga estas etapas:

1. Instale o AMS CLI. Consulte [Instalando ou atualizando a CLI do AMS](#).
2. Instale o AWS Java SDK. Consulte [Ferramentas para Amazon Web Services](#).
3. Configure o Java com estes comandos:

```
import com.amazonaws.auth.BasicAWSCredentials;  
  
import com.amazonaws.services.amscm.model.AWSManagedServicesCMClient;  
  
import  
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesRequest;  
  
import  
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesResult;  
  
public static void getChangeTypeClassificationSummaries() {
```

4. Defina as credenciais. Recomendamos que você não codifique isso.

```
final BasicAWSCredentials awsCredsCm =  
  
  new BasicAWSCredentials("ACCESS_KEY", "SECRET_KEY");
```

5. Crie o cliente AMS Change Management:

```
final AWSManagedServicesCMClient cmClient =  
    new AWSManagedServicesCMClient(awsCredsCm);
```

6. Obtenha o AMS CTs:

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

AMS: traga seu próprio EPS

Use o recurso “traga sua própria segurança de endpoint” (BYOEPS) do AMS para substituir o agente padrão do Trend Micro Deep Security por sua própria solução de segurança de endpoint ou licença da Trend Micro. Se você já tem licenças econômicas para produtos que não sejam o Trend Micro Deep Security, ou uma equipe que fornece seu EPS, ou se quiser usar uma ferramenta EPS específica, use o BYOEPS em suas instâncias.

O BYOEPS funciona no nível da conta. Suas instâncias na conta usam o BYOEPS ou o EPS padrão gerenciado pelo AMS:

- multi-account landing zone (MALZ): você designa contas de aplicativos que usam BYOEPS ou EPS gerenciado.
- single-account landing zone (SALZ): suas contas AMS usam BYOEPS ou EPS gerenciado.

BYOEPS, reduz sua AWS fatura pelo custo do Trend Micro Deep Security. Você continua incorrendo em custos com o EPS porque o EPS gerenciado pelo AMS ainda é necessário para proteger as EC2 instâncias criadas e mantidas pelo AMS que são necessárias para o gerenciamento de acesso (bastiões e hosts de gerenciamento). Para calcular o impacto total do custo, você deve contabilizar o custo das licenças da sua nova ferramenta e o custo do gerenciamento do EPS nos níveis de serviço necessários.

O uso do BYOEPS altera as funções e responsabilidades do AMS pelo gerenciamento de segurança:

- R significa parte responsável que faz o trabalho para realizar a tarefa.
- C significa consultado; uma parte cujas opiniões são solicitadas, normalmente como especialistas no assunto; e com quem há comunicação bilateral.
- I significa informado; uma parte que é informada sobre o progresso, geralmente apenas após a conclusão da tarefa ou do resultado final.

Gerenciamento de segurança	Cliente	AWS Managed Services
Manutenção de licenças válidas de EPS gerenciado para EC2 instâncias do AMS Shared Services	R	C
Configurar o EPS gerenciado para EC2 instâncias do AMS Shared Services	eu	R
Atualize o EPS gerenciado para EC2 instâncias do AMS Shared Services	eu	R
Monitoramento de malware em EC2 instâncias do AMS Shared Services	eu	R
Manutenção e atualização de assinaturas de vírus para EC2	eu	R

Gerenciamento de segurança	Cliente	AWS Managed Services
instâncias do AMS Shared Services		
Correção de instâncias infectadas com malware para EC2 instâncias do AMS Shared Services	C	R

Ao usar o BYOEPS, você perde um dos controles de segurança oferecidos pelo AMS. Você ainda tem o gerenciamento de segurança fornecido por meio de ferramentas como Amazon GuardDuty, Amazon Macie e controles de processo, como análises das configurações do IAM. O uso do BYOEPS não afeta as certificações e atestados de conformidade da AMS. No entanto, muitas estruturas e certificações de segurança têm requisitos de proteção contra malware e código malicioso. Para ajudar a manter sua conta segura e em conformidade, avalie seus controles planejados para garantir que eles atendam aos requisitos de segurança das certificações de conformidade da sua carga de trabalho.

Ative o BYOEPS para sua conta

O processo para ativar o BYOEPS contém três estágios e usa vários. RFCs Analise as informações a seguir para saber mais sobre os três estágios necessários para ativar o BYOEPS. Em seguida, coordene com seu CSDM para ativar o BYOEPS em sua conta.

Tópicos

- [Etapa 1: Pré-requisitos](#)
- [Etapa 2: habilitar o BYOEPS em sua conta](#)
- [Etapa 3: migração de instâncias](#)

Etapa 1: Pré-requisitos

- O perfil padrão da EC2 instância da Amazon é `customer-mc-ec2-instance-profile`. Se você usar um perfil de EC2 instância da Amazon diferente além do perfil padrão, permita a `ssm:GetParameter` ação do `/ams/end-point-security` recurso em seu perfil de EC2 instância.

Se você não conseguir atualizar perfis de EC2 instância, envie uma RFC que especifique os perfis de instância que você precisa atualizar.

- Entenda o escopo dessa mudança.

As implantações por meio de um tipo de alteração automatizada (CT) do AMS permitem que você especifique a AMI usada na criação.

Para usar o BYOEPS com contas que usam EPS gerenciado pelo AMS, você deve trabalhar com o AMS para desinstalar os agentes da Trend Micro dessas EC2 instâncias e atualizar o código AMS (por exemplo, scripts de inicialização) nessas instâncias. Essas ações podem exigir uma reinicialização, portanto, é uma prática recomendada executá-las como parte de uma janela de manutenção. Entre em contato com seu CSDM para identificar uma janela de manutenção para realizar essa atividade e criar um plano de migração. Para o plano de migração, considere as seguintes questões:

1. Quantas instâncias você precisa migrar? Divida o número total de instâncias em lotes menores e incrementais.
 2. Como você dividirá as instâncias em lotes? Por exemplo, você pode dividir por grupos de recursos e criar uma lista para compartilhar com a equipe de operações do AMS.
 3. Quanto tempo cada lote levará? Quanto tempo total é necessário? Considere que talvez você queira instalar suas ferramentas EPS preferidas na mesma janela de manutenção. Quanto tempo isso vai levar?
- Seu CSDM compartilha o plano de migração com a equipe de operações do AMS. Se sua frota de instâncias estiver acima de 50, trabalhe com seu CSDM para criar um evento planejado usando o processo de gerenciamento de eventos planejados (PEM). Para obter mais informações, consulte [Gerenciamento de eventos planejados no AWS Managed Services](#).

As operações do AMS coordenam com seu CSDM e aconselham como enviar RFCs de acordo com suas janelas de manutenção, com base no número de instâncias em sua conta.

- Atualize as automações ou processos de execução de EC2 instâncias usando o personalizado ou o AMS AMIs para usar o AMS AMIs lançado após dezembro de 2020.

Etapa 2: habilitar o BYOEPS em sua conta

Quando você usa o BYOEPS em sua conta, as responsabilidades que o AMS tem pelo gerenciamento de segurança mudam. Consulte sua equipe de segurança e plataforma de nuvem antes de ativar o BYOEPS.

Para solicitar BYOEPS para sua conta, envie um RFC de atualização “MOO” (Gerenciamento | Outro | Outro | Atualização) com ct-0xdawir96cy7k, com os seguintes detalhes:

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

O AMS implanta atualizações do armazenamento de parâmetros na conta e atualiza o [perfil da instância Amazon EC2 IAM](#).

 Note

- Contas com novas instâncias lançadas que usam o AMS mais recente AMIs podem ignorar a instalação do agente da Trend Micro. AMIs anteriores a dezembro de 2020 não oferecem suporte ao recurso BYOEPS. Atualize as automações que usam o antigo AMIs para usar o AMS mais recente AMIs com suporte ao recurso BYOEPS.
- Para tratamento de EC2 instâncias existentes, consulte Etapa 3: migrações de instâncias

Etapa 3: migração de instâncias

Use uma das opções a seguir para migrar suas instâncias, dependendo do seu caso de uso. Se você não tiver certeza de qual opção escolher, entre em contato com sua CA ou CSDM.

Contas com EC2 instâncias que usam EPS gerenciado pelo AMS

Durante a janela de manutenção, de acordo com o planejamento da Etapa 1, as seguintes ações são executadas em cada instância que precisa ser integrada ao BYOEPS:

- Executado pelo AMS: atualize o código AMS (scripts de inicialização, módulos etc.) para as versões mais recentes. Isso é necessário porque os scripts de inicialização antigos do AMS não têm suporte ao recurso BYOEPS e reinstalam o agente da Trend Micro em cada inicialização. Além disso, desinstale o Trend Micro Agent.
- Executado por você: Instale e configure sua ferramenta EPS preferida.

 Important

O Trend Micro Agent fornece proteção contra malware. Certifique-se de instalar um substituto adequado para proteger suas instâncias.

Para fazer essas alterações, envie RFCs com o tipo de alteração `ct-2iz9nvw8zlhst`, [Trend Micro DSM](#) | [Remove Trend Micro](#) EPS Agent (revisão obrigatória), em lotes.

Contas sem EC2 instâncias que usam EPS gerenciado pelo AMS

Contas com novas instâncias lançadas que usam o AMS mais recente AMIs podem ignorar a instalação do agente da Trend Micro. AMIs anteriores a dezembro de 2020 não oferecem suporte ao recurso BYOEPS. Atualize as automações que usam o antigo AMIs para usar o AMS mais recente AMIs com suporte ao recurso BYOEPS.

Adicione seu agente nas EC2 instâncias

Você pode usar o AMS Patterns para implantar agentes de ferramentas como, CrowdStrike ou Qualys, enviar uma solicitação de serviço para obter assistência.

Recebendo notificações do AMS

As comunicações entre você e o AMS ocorrem por vários motivos:

- Um RFC criado pelo AMS que requer sua aprovação
- Um caso de AMS criado para investigar uma RFC que você criou que falhou
- Eventos criados por alertas de monitoramento
- Notificações do serviço de patches que informam você sobre futuras correções
- Solicitações de serviço e relatórios de incidentes
- Relatórios mensais de CRM
- Anúncios ocasionais importantes da AWS (seu CSDM entra em contato com você se alguma ação de sua parte for necessária)

Todas essas notificações são enviadas para as informações de contato padrão (o e-mail da conta raiz) que você forneceu ao AMS quando foi integrado. Como é difícil manter e-mails individuais atualizados, recomendamos que você use um e-mail de grupo que possa ser atualizado por você. Todas as notificações enviadas a você também são recebidas pelas operações do AMS e analisadas antes de dar uma resposta.

O serviço de notificação do AMS fornece duas maneiras adicionais de configurar contatos para notificações:

- Marque seus recursos com tags de contato (o valor chave da tag sendo informações de contato) e forneça o nome da chave da tag ao seu CSDM. Os alarmes sobre esses recursos serão enviados aos contatos fornecidos no Valor-chave, além do contato da conta criado na integração. Isso é especialmente útil para proprietários de aplicativos. Para obter mais informações, consulte [Notificação de alerta baseada em tag](#).
- (Obrigatório na integração) Envie para seu CSDM listas nomeadas de contatos para notificações não baseadas em recursos. Por exemplo, você pode ter uma lista chamada "SecurityContacts" e outra chamada "OperationsContacts", e assim por diante. O AMS adiciona a lista ao serviço de notificação e os alarmes que se aplicam ao contexto dessa lista são enviados para esses contatos. Isso é especialmente útil para questões organizacionais.

Esse recurso avançado de roteamento de alertas está ativo para a maioria dos CloudWatch alarmes essenciais, como falha de EC2 instância da Amazon, utilização da capacidade de volume do Amazon Elastic Block Store (Amazon EBS) — uso raiz, uso do NonRoot Amazon EBS, alta utilização de memória, alto uso de swap e alta utilização da CPU para a Amazon. EC2

Além disso, ao registrar uma solicitação de serviço ou relatório de incidente, você tem a opção de adicionar "E-mails CC" (altamente recomendado) e esses endereços de e-mail recebem notificações sobre a solicitação de serviço ou o incidente.

Important

Enquanto os endereços de e-mail CC fornecidos nas solicitações de serviço e nos relatórios de incidentes recebem notificações de comunicações por e-mail, outras notificações, como notificações de patches, aparecem na sua lista de solicitações de serviço (um e-mail também é enviado para o contato padrão), sem uma notificação explícita de que você tem uma comunicação aguardando sua atenção. É por isso que é altamente recomendável adicionar um e-mail CC sempre que possível e configurar o e-mail de contato padrão como um grupo do qual todos que usam o AMS são membros.

Além disso, você pode solicitar notificações especiais para alterações novas AMIs, de estado de RFC e de configuração em sua conta do AMS. Esses serviços de notificação opcionais são discutidos a seguir.

Notificações AMI do AMS com SNS

O AMS fornece um serviço de notificação da AMI. Você pode usá-lo para assinar um tópico do Amazon Simple Notification Service (SNS) que notifica você quando as atualizações da AMI do AMS forem lançadas. Você pode optar por receber notificações somente para o AMS AMIs que você usa, ou você pode se inscrever para receber notificações de atualização para todos os AMS AMIs. Para obter mais informações sobre tópicos do SNS, consulte [O que é o Amazon Simple Notification Service?](#)

Sempre que AMIs são lançados, enviamos notificações aos assinantes do tópico correspondente; esta seção descreve como assinar as notificações da AMI do AMS.

Exemplo de mensagem

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

Possíveis tópicos da AMI do AMS para se inscrever:

- TUDO: Use `customer-ams-all-amis`. A assinatura deste tópico notifica você quando qualquer um dos AMS AMIs é atualizado.
- AMS AWS Linux AMIs: Para Amazon Linux, use `customer-ams-amazon1` `customer-ams-amazon1-security-enhanced` e. Para Amazon Linux 2, use `customer-ams-amazon2` `customer-ams-amazon2-security-enhanced` e.
- AMS SUSE Linux AMIs: Use `customer-ams-sles12` ou `customer-ams-sles15`.
- AMS AWS RedHat AMIs: Use `customer-ams-rhel8`, `customer-ams-rhel8-security-enhanced`, `customer-ams-rhel7`, `customer-ams-rhel7-security-enhanced`.
- AMS AWS CentOS AMIs: Use `customer-ams-centos7`, `customer-ams-centos7-security-enhanced`.
- AMS Ubuntu AMIs: Use `customer-ams-ubuntu18`.
- AMS AWS Windows AMIs: Use `customer-ams-windows2019`, `customer-ams-windows2019-security-enhanced`, `customer-ams-windows2016`, `customer-ams-windows2016-security-enhanced`, `customer-ams-windows2012`, `customer-ams-windows2012r2`, `customer-ams-windows2012r2-security-enhanced`, `customer-ams-windows2022`.

Para assinar as novas notificações de AMI do AMS usando o console do Amazon SNS:

1. Abra o console do Amazon SNS no [Painel](#).
2. No canto superior direito, mude para a região da AWS da AMIs qual você está se inscrevendo.
3. No painel de navegação esquerdo, escolha Assinaturas e, em seguida, escolha Criar assinatura.
4. Forneça as informações a seguir:
 - a. ARN do tópico: `arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}` onde REGION é a região selecionada da AWS (onde a notificação do SNS foi criada) e AMS_AMI_NAME é a AMI sobre a qual você deseja receber notificações. Exemplos:
 - Para assinar notificações do novo AMS Amazon Linux AMIs na região us-east-1 da AWS, use este tópico ARN = `arn:aws:sns:us-east-1:287847593866:customer-ams-amazon1`

- Para assinar notificações do novo AMS Window Server 2016 AMIs na região us-west-2 da AWS, use este tópico ARN = `arn:aws:sns:us-west-2:287847593866:customer-ams-windows2016`
 - b. Em Protocol (Protocolo), escolha Email.
 - c. Em Endpoint, insira um endereço de e-mail que possa ser usado para receber notificações. Recomendamos uma lista de distribuição em vez do e-mail de um indivíduo.
5. Selecione Criar assinatura.
 6. Ao receber um e-mail de confirmação com o assunto “Notificação da AWS — Confirmação da assinatura”, abra o e-mail e escolha Confirmar assinatura para concluir sua assinatura.

 Note

Você não está limitado ao e-mail para o Protocolo. Para obter informações sobre outros protocolos aceitáveis e como usá-los, consulte [inscrever-se](#).

Para cancelar a assinatura de novas notificações de AMI do AMS usando o console do AWS SNS:

1. Abra o console do Amazon SNS no [Painel](#).
2. Na barra de navegação, mude para a região da AWS de sua escolha. Você deve usar a região da AWS na qual deseja receber notificações para a região correspondente AMIs.
3. No painel de navegação, escolha Assinaturas, selecione a assinatura e escolha Ações -> Excluir assinaturas.
4. Quando a confirmação for solicitada, escolha Excluir.

Para assinar as notificações da nova AMI do AMS usando o Deployment | Inestion | Stack from CloudFormation Template | Create (ct-36cn2avfrjrj9v):

1. Para assinar AmazonLinuxSubscription, crie e salve um arquivo JSON de parâmetros de execução; este exemplo o chama de CreateSubscribeAmiParams .json:

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "AmazonLinuxSubscription": {
      "Type" : "AWS::SNS::Subscription",
```



```

        "Properties": {
            "TopicArn": "arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}",
            "Protocol": "email",
            "Endpoint": "username@yourdomain.com"
        }
    }
}

```

2. Crie e salve o arquivo JSON de parâmetros RFC com o conteúdo a seguir; este exemplo o chama de CreateSubscribeAmiRfc arquivo.json:

```

{
  "ChangeTypeId": "ct-36cn2avfrj9v",
  "ChangeTypeVersion": "1.0",
  "Title": "cfn-ingest-subscribe-ami"
}

```

3. Crie o RFC, especificando o CreateSubscribeAmiRfc arquivo e o CreateSubscribeAmiParams arquivo:

```

aws amscm create-rfc --cli-input-json file://CreateSubscribeAmiRfc.json --
execution-parameters file://CreateSubscribeAmiParams.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 ver exemplos de criação AMIs, consulte [Criar AMI](#).

Para obter informações sobre o consumo AMIs programático, consulte [EC2 stack: creating](#).

Notificações de serviço

O AMS envia solicitações de serviço externas, ou notificações de serviço, quando você precisa agir ou estar ciente de algo que possa afetar sua conta ou seus recursos, incluindo:

- Impacto na infraestrutura: o AMS envia uma notificação de serviço quando há um serviço subjacente da AWS impactando sua infraestrutura e você precisa agir antes de uma determinada data, ou você pode ter uma interrupção.

- **EC2 Problemas de hardware:** o AMS envia notificações de serviço sobre problemas de EC2 hardware que exigem que você reinicialize uma EC2 instância antes de uma determinada data ou informando que o AMS reinicializará a instância para você. Esse é um aviso importante porque a reinicialização pode causar uma interrupção e você deve responder com uma data aceitável ou criar uma RFC com ct-09qbhy7kvtxqw para reinicializar a instância sozinho. Uma notificação de serviço como essa fecha automaticamente em cinco dias se você não responder.

Notificações de alteração de estado do RFC

O AMS oferece notificações para alterações de estado de RFC por e-mail e CloudWatch eventos:

- **E-mails por meio do console AMS:** há uma opção na segunda página do assistente Criar RFC, na qual você pode adicionar até cinco endereços de e-mail para ser notificado quando o estado do RFC mudar.
- **CloudWatch Eventos:** você pode configurar regras e alvos diferentes para que CloudWatch os Eventos recebam notificações para cada alteração de estado de RFC.

Notificações por e-mail

Você pode adicionar endereços de e-mail para receber alterações de estado de RFC em uma RFC criada no console do AMS ou usando a API/CLI do AMS.

No console AMS, use a opção Notificações por e-mail, na segunda página do assistente Criar RFC:

Na API/CLI do AMS, adicione uma linha como essa à seção de parâmetros de RFC do seu RFC (não adicione a linha à seção de parâmetros de execução):

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

O comportamento das notificações varia de acordo com o tipo de agendamento de RFC:

- **Agendado para RFCs receber notificações por e-mail sobre:** Enviado, Programado, Concluído InProgress, Rejeitado, Cancelado, Rejeitado Automaticamente ou Cancelado Automaticamente.
- **RFCs Receba o mais rápido possível uma notificação por e-mail sobre:** Enviado InProgress, Concluído, Rejeitado, Cancelado ou Cancelado AutoRejected Automaticamente.

 Note

- As notificações por e-mail são enviadas deste endereço: `no-reply@managedservices.amazonaws.com`.
- Os caracteres especiais e URLs o título do seu RFC são redigidos nos e-mails que enviamos. Isso é uma medida de segurança.

CloudWatch Notificações de eventos

O AMS oferece notificações push para as alterações do estado da RFC por meio de CloudWatch eventos. Para receber essas notificações:

1. Crie um tópico e uma assinatura para os quais as notificações serão enviadas. Você pode nomear o tópico como quiser; para obter informações sobre como fazer isso, consulte [Tópico e assinatura do SNS: criação](#).
2. Envie uma RFC com a seção Gerenciamento | Outros | Outros | Crie o tipo de alteração e inclua o tópico e a assinatura do SNS na solicitação de avisos de alteração de estado da RFC.

Ao enviar a solicitação Gerenciamento | Outros | Outros RFC para esse recurso, você pode especificar sobre quais mudanças de estado de RFC você está interessado em ser notificado e quais tipos de alteração, além de definir outros filtros. Por exemplo, talvez você queira solicitar a notificação somente quando os tipos de alteração do Admin Access forem `EventType = RfcSubmitted` e `EventType = RfcUpdated`.

Este é um modelo de notificações de CloudWatch eventos que você pode receber (com todos os valores possíveis):

```
{
  "source ": "aws.managedservices",
  "detail-type": "AMS RFC State Change",
  "detail": {
    "ActionState": "null | AwsActionPending | AwsOperatorAssigned | CustomerActionPending | NotApplicable | NoActionPending",
    "ActualExecutionTimeRange": {
      "StartTime": "null | Actual Start Time",
      "EndTime": "null | Actual End Time"
    }
  },
}
```

```

    "AutomationStatus": "Automated | Manual",
    "AwsAccountId": "AWS Account ID",
    "AwsApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending
| Rejected | Approved",
    "ChangeTypeId": "Change_Type_ID",
    "ChangeTypeVersion": "Change_Type_Version",
    "CreatedTime": "Created_Time",
    "CustomerApprovalStatus": "null | SubmissionPending | NotRequired |
ApprovalPending | Rejected | Approved",
    "EventType": "RfcActionStateUpdated | RfcApproved | RfcAutoRejected |
RfcCanceled | RfcCompleted | RfcCreated | RfcInProgress | RfcRejected | RfcSubmitted |
RfcUpdated",
    "LastModifiedTime": "Last_Updated_Time",
    "LastSubmittedTime": "null | Last_Submitted_Time",
    "RequestedExecutionTimeRange": {
        "StartTime": "null | Expected_Start_Time",
        "EndTime": "null | Expected_End_Time"
    },
    "RfcId": "RFC_ID",
    "Status": "Editing | PendingApproval | Scheduled | Rejected | Canceled |
ExecutionLock | InProgress | Success | Failure",
    "Title": "Title"
}
}

```

As alterações de estado do RFC suportadas (EventType), conforme aparecem na notificação real de CloudWatch eventos, são:

- RfcActionStateUpdated (sem opção de console AMS): O RFC em um dos estados, descrito posteriormente, foi alterado.
- RfcApproved (sem opção de console AMS): O RFC foi aprovado na validação do operador and/or AMS do sistema e foi aprovado para conclusão.
- RfcAutoRejected (Rejeitado automaticamente): O RFC falhou na validação do sistema ou do operador AMS e foi rejeitado.
- RfcCanceled (Cancelado ou cancelado automaticamente): O RFC foi cancelado pelo remetente ou por um operador do AMS.
- RfcCompleted (Concluído): Os parâmetros de execução do RFC foram concluídos, inclusive UserData.
- RfcCreated (sem opção de console AMS): O RFC foi criado com sucesso (o JSON e os parâmetros enviados eram válidos).

- **RfcInProgress (InProgress):** A execução do RFC ainda está em andamento.
- **RfcRejected (Rejeitado):** A validação do sistema com falha de RFC ou do operador AMS foi rejeitada.
- **RfcSubmitted (Enviado):** O RFC foi enviado e está passando por validação do sistema.
- **RfcUpdated (sem opção de console AMS):** O RFC foi atualizado manualmente por um operador do AMS.

Além disso, você pode enviar notificações de CloudWatch Eventos (CWE) para qualquer um dos destinos suportados e criar seus próprios sistemas com base nessas notificações automatizadas:

- EC2 Instâncias da Amazon
- AWS Lambda funções
- Fluxos no Amazon Kinesis Data Streams
- Streams de entrega no Amazon Data Firehose
- Grupos de registros no Amazon CloudWatch Logs
- Tarefas do Amazon ECS
- Run Command do Systems Manager
- Automação do Systems Manager
- AWS Batch empregos
- Máquinas de estado do Step Functions
- Oleodutos em CodePipeline
- CodeBuild projetos
- Modelos de avaliação do Amazon Inspector
- Tópicos do Amazon SNS
- Filas do Amazon SQS
- Destinos integrados: chamada de EC2 CreateSnapshot API, chamada de EC2 RebootInstances EC2 StopInstances API, chamada de API e chamada de EC2 TerminateInstances API.
- O barramento de eventos padrão de outra conta da AWS

Note

Enviamos notificações de CloudWatch eventos para mudanças de estado do RFC, com base no melhor esforço.

Configurando DNS público e privado

Durante a integração, o AMS configura um serviço DNS privado para comunicações entre seus recursos gerenciados e o AMS.

Você pode usar o AMS Route 53 para gerenciar os nomes DNS internos dos recursos do seu aplicativo (servidores web, servidores de aplicativos, bancos de dados etc.) sem expor essas informações à Internet pública. Isso adiciona uma camada adicional de segurança e também permite que você faça o failover de um recurso primário para um secundário (geralmente chamado de “inversão”) mapeando o nome DNS para um endereço IP diferente.

Depois de criar recursos DNS privados usando Implantação | Componentes avançados da pilha | DNS (privado) | Criar (ct-0c38gftq56zj6) ou Implantação | Componentes avançados da pilha | DNS (público) | Criar (ct-0vzsr2nyraedl), você pode usar o Gerenciamento | Componentes avançados da pilha | DNS (privado) | Atualização (ct-1d55pi44ff21u) e Gerenciamento | Componentes avançados de pilha | DNS (público) | Atualização (ct-1hzofpphabs3i), para configurar conjuntos de registros adicionais ou atualizar conjuntos de registros existentes. CTs Para contas multi-account landing zone (MALZ), os recursos de DNS criados na conta do aplicativo VPCs podem ser compartilhados com a conta de serviços compartilhados VPC para manter o DNS centralizado usando o AMS AD.

MALZ

O gráfico a seguir ilustra uma possível configuração de DNS para o Multi-Account Landing Zone AMS. Ele ilustra uma configuração de DNS híbrida entre o AMS e uma rede típica de clientes. Um registro de nome canônico (CNAME) no servidor DNS da rede do cliente encaminha para o AMS AD DNS na conta de serviços compartilhados com um encaminhamento condicional que tem o CNAME do FQDN do AMS encaminhado para o registro A.

SALZ

O gráfico a seguir ilustra uma possível configuração de DNS para a single-account landing zone (SALZ). Ele mostra uma configuração de DNS híbrida entre o AMS e uma rede típica de

clientes. Um CNAME no servidor DNS da rede do cliente encaminha para o AMS AD DNS com um encaminhamento condicional que tem o CNAME do FQDN do AMS encaminhado para o registro A.

SALZ Route53 DNS

O gráfico a seguir ilustra uma possível configuração de DNS para a single-account landing zone (SALZ). Ele mostra uma configuração de DNS híbrida entre o AMS e uma rede típica de clientes. Um CNAME no servidor DNS da rede do cliente encaminha para o AMS AD DNS com um encaminhamento condicional que tem o CNAME do FQDN do AMS encaminhado para o registro A. Isso também aproveita o Route53 para tráfego de rede de saída, para que qualquer aplicativo na conta possa ter resolução de DNS na conta com a maior disponibilidade.

Caminhos de resolução habilitados para Route53:

- Instância tentando resolver o nome MAD do AMS --> VPC +2 (AmazonProvidedRoute53/DNS) --> Encaminhadores condicionais avaliados -> Regra do encaminhador condicional MAD do Route53 correspondida --> Resolvedor de saída do Route53 --> AD DNS gerenciado
- Instância que tenta resolver o nome local do cliente --> VPC +2 (AmazonProvidedRoute53/DNS) --> Encaminhadores condicionais avaliados -> Regra do encaminhador condicional local do Route53 correspondida --> Resolvedor de saída do Route53 --> DNS local do cliente
- Instância tentando resolver o nome da Internet --> VPC +2 (AmazonProvidedRoute53/DNS) --> Encaminhadores condicionais avaliados -> Nenhum encaminhador correspondente --> Serviço DNS da Internet

Para obter mais informações, consulte Como [usar o DNS com sua VPC e Trabalhar com zonas hospedadas privadas](#).

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.

Implantação de recursos do IAM no AMS Advanced

O AMS implanta recursos do IAM em seu aplicativo de zona de aterrissagem com várias contas (MALZ) e contas de zona de pouso com uma única conta (SALZ) de duas maneiras:

- Provisionamento automatizado do IAM: esse recurso no AMS permite que você envie, crie, atualize ou exclua tipos de alteração para o provisionamento de funções ou políticas do IAM, sem a revisão do operador, e com as verificações de validação do IAM e do AMS executadas automaticamente.

Esse recurso deve ser habilitado explicitamente com o Gerenciamento | Conta gerenciada | Provisionamento automatizado de IAM do AMS com permissões de leitura e gravação | [Ativar \(revisão necessária\) tipo de alteração \(ct-1706xvbk6j9hf\)](#). Para saber mais, consulte [Provisionamento automatizado de IAM \(AMS\)](#). Depois que o provisionamento automatizado do IAM do AMS for ativado, você terá acesso aos tipos de alteração Criar, Atualizar e Excluir para gerenciar seus recursos do IAM.

- Revise o tipo de alteração do IAM necessário: esse tipo de alteração, Implantação | Componentes avançados da pilha | Identity and Access Management (IAM) | [Criar entidade ou política \(revisão obrigatória\) \(ct-3dpg8mdd9jn1r\)](#), exige uma análise do operador do AMS, que às vezes pode levar alguns dias para ser concluída se forem necessários esclarecimentos.

Note

Seja qual for o método usado, uma função do IAM é provisionada para a conta ou contas relevantes e, depois que a função for provisionada, você deverá integrar a função na sua solução de federação.

Provisionamento automatizado de IAM (AMS)

AWS Managed Services (AMS) suporta validação e provisionamento automatizados para recursos do IAM, incluindo funções e políticas usando solicitações avançadas de mudança (RFCs) e novos tipos de alteração () do AMS. CTs Anteriormente, essas solicitações passavam por um processo semiautomático que às vezes resultava em longos tempos de espera. Agora, você pode usar o AMS Automated IAM Provisioning para provisionar recursos do IAM e obter os resultados com muito mais rapidez.

Como funciona o provisionamento automatizado de IAM no AMS

O provisionamento automatizado do IAM depende de verificações automatizadas de tempo de execução do IAM para validar as alterações nos recursos do IAM. Essas verificações automatizadas, realizadas quando os tipos de alteração Create, Update ou Delete são executados, evitam que recursos do IAM que são excessivamente permissivos ou com padrões inseguros sejam implantados em sua conta. Isso permite que você combine o nível de rigor nas avaliações do IAM com a experiência de sua equipe. Recomendamos que as equipes que são iniciantes em serviços em nuvem e precisam de verificações manuais para todas as alterações de recursos do IAM usem o tipo de alteração existente exigido pela revisão: Implantação | Componentes avançados da pilha | Identity and Access Management (IAM) | [Create entity or policy \(review required\)](#), (ct-3dpd8mdd9jn1r). Equipes com AWS experiência e controle de seus ambientes podem usar o provisionamento automatizado de IAM para acelerar suas implantações. Você pode usar esse recurso para realizar a validação por meio de verificações automatizadas de tempo de execução ou para realizar a validação e o provisionamento de recursos do IAM após a validação bem-sucedida.

Important

AWS Managed Services implementou proativamente uma lista de [verificações de tempo de execução](#) de validação que impedem a criação de recursos ou políticas do IAM com determinadas permissões e condições. Para obter uma descrição desses privilégios e condições, consulte [Implantação de recursos do IAM no AMS](#) Advanced. Os tipos de alteração automatizados [ct-1n9gfnog5x7fl](#), [ct-1e0xmuy1diafq](#) e [ct-17cj84y7632o6](#) [permitem que usuários com proficiência no gerenciamento de recursos do IAM provisionem funções e políticas do IAM que permitem ações além dos privilégios](#) de somente leitura. [Além disso, você pode usar as funções criadas por meio dos tipos de alteração automatizada ct-1n9gfnog5x7fl, ct-1e0xmuy1diafq e ct-17cj84y7632o6 para criar os novos recursos.](#) No entanto, os recursos não podem seguir o padrão de nomenclatura do AMS e não fazem parte da pilha padrão do AMS. O AMS fornece o suporte operacional e de segurança desses recursos específicos com base no melhor esforço.

Embora os processos manuais e automatizados tenham como objetivo manter nossos padrões de segurança, é importante observar que existem diferenças nas verificações entre os dois. O provisionamento automatizado permite maior flexibilidade na criação e atualização de funções e políticas; portanto, elas não são as mesmas. É recomendável que sua organização analise cuidadosamente as [verificações de tempo de execução de validação](#) listadas no Guia do Usuário do AMS para garantir que elas estejam alinhadas às expectativas e aos requisitos da sua organização.

Fluxo de validação

Fluxo de validação e provisionamento

Note

Esse recurso é adequado para equipes com experiência AWS e recursos do IAM, e não o recomendamos para equipes iniciantes AWS. O processo de validação automatizado foi projetado para detectar a maioria dos erros e é útil para que as equipes obtenham análises rápidas das alterações no IAM, quando entenderem as permissões de que precisam. Para usar os novos tipos de alteração com segurança e eficácia, recomendamos que você tenha um bom entendimento do AWS IAM e das [verificações de tempo de execução](#) oferecidas pelos tipos de alteração para determinar se eles são adequados para sua equipe.

Integração ao provisionamento automatizado de IAM do AMS no AMS

Para usar os novos tipos de alteração, primeiro ative o provisionamento automatizado do IAM pelo AMS enviando uma RFC usando o seguinte tipo de alteração: Gerenciamento | Conta gerenciada | Provisionamento automatizado do IAM com permissões de leitura e gravação | [Ativar](#) (revisão obrigatória) (ct-1706xvvk6j9hf). AWS exige que sua organização passe por um processo de gerenciamento de riscos de segurança do cliente (CSRM) para garantir que o uso desses tipos de mudança esteja alinhado com suas políticas organizacionais. A equipe de AWS operações trabalha com você para obter aprovação explícita do contato da equipe de segurança na forma de aceitação de riscos como parte da revisão necessária. Para saber mais, consulte o processo de [gerenciamento de risco do cliente \(CSRM\) da RFC](#).

Depois que a RFC para ativar o recurso de provisionamento automatizado de IAM do AMS com permissões de leitura e gravação for bem-sucedida, o AMS habilita os tipos de alteração do provisionamento automatizado do IAM do AMS na conta usada para enviar a RFC habilitada. Para confirmar se uma conta tem o AMS Automated IAM Provisioning ativado, verifique a função no console do IAM. `AWSTrustedArns`

Como parte da integração, o AMS provisiona o IAM Access Analyzer na mesma região da AWS da conta para aproveitar seu recurso de visualização prévia de acesso. O IAM Access Analyzer ajuda a identificar recursos em sua organização e contas que são compartilhados com uma entidade externa,

valida as políticas do IAM em relação à gramática e às melhores práticas e gera políticas do IAM com base na atividade de acesso em seus registros. AWS CloudTrail Para saber mais, consulte [Usando AWS Identity and Access Management Access Analyzer](#).

Uma vez integrado, o `AWSManagedServicesIAMProvisionAdminRole` é implantado nas contas habilitadas. Se você optar por usar essa função por meio da federação SAML, deverá integrar a função à sua solução de federação.

Como parte da integração, você pode solicitar a atualização `IAMProvision AdminRole` da política de confiança `AWSManaged` dos Serviços para conceder outro ARN de função do IAM para assumir essa função usando `AWS Security Token Service`.

Usando o provisionamento automatizado de IAM do AMS no AMS

Você pode criar RFCs com os seguintes tipos de alteração do AMS Automated IAM Provisioning.

Note

- Somente o provisionamento de funções e políticas é suportado.

Ao atualizar as funções, o Update CT substitui a lista existente de nomes de recursos da Amazon de políticas gerenciadas e o documento de política “assumir função” pela lista fornecida de política gerenciada ARNs e documento de política de “assumir função”. ARNs Em uma atualização parcial; por exemplo, adicionar ou remover um ARN na lista existente de políticas gerenciadas ARNs, não é permitido adicionar ou remover declarações de política individuais ao documento de política “assumir função”. Da mesma forma, ao atualizar as políticas, o Update CT substitui o documento de política existente e não permite adicionar ou remover declarações de políticas individuais no documento de política existente.

- Quando a opção “somente validar” é selecionada, as verificações em tempo de execução são realizadas sem provisionar nenhuma entidade ou política do IAM. Independentemente de qualquer descoberta, o status da RFC é “sucesso”. O status “sucesso” indica uma validação bem-sucedida em relação à entidade ou política do IAM fornecida.

- Implantação | Advanced Stack Components | Identity and Access Management (IAM) | [Criar entidade ou política \(permissões de leitura e gravação\) \(ct-1n9gfnog5x7fl\)](#): uma nova entidade ou política do IAM é validada e provisionada automaticamente.

- Gerenciamento | Advanced Stack Components | Identity and Access Management (IAM) | [Atualizar entidade ou política \(permissões de leitura e gravação\) \(ct-1e0xmuy1diafq\)](#): uma entidade ou política existente do IAM é atualizada e validada automaticamente.
- Gerenciamento | Advanced Stack Components | Identity and Access Management (IAM) | [Excluir entidade ou política \(permissões de leitura e gravação\) \(ct-17cj84y7632o6\)](#): uma entidade ou política do IAM existente que é provisionada usando a entidade de criação automática ou o tipo de alteração de política é excluída.

Você só pode chamar os três anteriores CTs usando uma função IAM dedicada: `AWSManagedServicesIAMProvisionAdminRole`. Essa função está disponível somente nas contas que foram integradas ao recurso usando Gerenciamento | Conta gerenciada | Permissões de leitura e gravação do AMS Automated IAM Provisioning | [Ativar \(revisão necessária\) \(ct-1706xvvk6j9hf\)](#).

 Important

Os tipos de alteração Criar, Atualizar e Excluir estão sempre visíveis em sua conta, mas não estão ativados por padrão. Se você tentar enviar uma RFC usando um desses tipos de alteração sem primeiro ativar o recurso de provisionamento automatizado do IAM do AMS, um erro “não autorizado” será exibido.

Limitações:

- O Create CT pode permitir que você crie uma função ou política do IAM com permissão para criar AWS recursos. No entanto, AWS os recursos criados por essas funções e políticas não são gerenciados pelo AMS. É uma prática recomendada seguir seu controle organizacional para limitar a criação de tais funções ou políticas.
- O Update CT não pode modificar as funções e políticas do IAM criadas com o CFN Ingest, o Direct Change Mode, o Developer Mode ou, em alguns casos, por meio do manual ou automático do AMS Advanced existente. CTs
- O Delete CT não pode excluir funções ou políticas existentes que não foram criadas com o AMS Automated IAM Provisioning Create CT.
- O recurso AMS Automated IAM Provisioning com permissões de leitura e gravação não é compatível com as funções do Modo de Alteração Direta. Isso significa que você não pode

provisionar ou atualizar funções e políticas do IAM com permissões de leitura e gravação usando essas funções.

- O provisionamento automatizado de IAM do AMS com permissões de leitura e gravação Os tipos de alteração Criar, atualizar e excluir não são compatíveis com o conector. ServiceNow

Verificações de tempo de execução do provisionamento automatizado de IAM do AMS no AMS

O provisionamento automatizado do IAM aproveita as verificações e executa AWS Identity and Access Management Access Analyzer verificações e validações adicionais em relação à política de limites do AMS. O AMS definiu as verificações e validações adicionais com base nas melhores práticas do IAM, na experiência de operar a carga de trabalho do cliente na nuvem e na experiência coletiva de avaliação manual do AMS IAM.

Você pode visualizar os resultados da verificação em tempo de execução da política na saída da solicitação de alteração (RFC). As descobertas incluem o identificador do recurso, a localização na and/or política de função que gerou as descobertas e uma mensagem descrevendo a verificação de que a entidade ou o recurso do IAM não foram aprovados. Essas descobertas ajudam você a criar políticas que sejam funcionais e estejam em conformidade com as melhores práticas de segurança.

Note

O provisionamento automatizado do IAM tenta ser específico sobre o local dentro da definição de entidade ou política que não passa na verificação. Dependendo do tipo, o local pode incluir o nome ou o ARN do recurso ou o índice em uma matriz. Por exemplo, uma declaração para ajudá-lo a ajustar a entidade ou política para obter um resultado bem-sucedido.

Para uma experiência tranquila de provisionamento automatizado de IAM do AMS, é uma prática recomendada usar a opção “somente validar” para executar as verificações de validação até que não haja nenhuma descoberta das verificações de validação relatadas nas saídas da RFC. Quando as verificações de validação não relatarem nenhuma descoberta, escolha Criar cópia no console AMS para criar rapidamente uma cópia da RFC existente. Quando você estiver pronto para provisionar, na seção Parâmetros, alterne o valor Validar somente de Sim para Não e continue.

Estas são as verificações em tempo de execução que o AMS Automated IAM Provisioning executa para garantir que seus recursos do IAM estejam seguros:

 Note

Para provisionar políticas do IAM que contêm ações negadas por esses tipos de alteração automatizada, você deve seguir o processo de gerenciamento de riscos de segurança do cliente (CSRM) da RFC. Use o seguinte tipo de alteração: Implantação | Componentes avançados da pilha | Identity and Access Management (IAM) | Criar entidade ou política (revisão obrigatória) (ct-3dpd8mdd9jn1r).

- Verificação e validação da política do IAM Access Analyzer: consulte também a [referência de verificação de política do Access Analyzer](#) e a validação da política [do IAM Access Analyzer](#).
- Verificações da política de limite de permissões do AMS: ações em um conjunto de serviços que são negadas por padrão. Para obter mais informações, consulte Verificação [automatizada do limite de permissão do IAM Provisioning](#).
- Verificações da política de limite de permissões definidas pelo cliente: ações restritas adicionais em um conjunto de serviços que são negados. Para obter mais informações, consulte Verificação [automatizada do limite de permissão do IAM Provisioning](#).
- Verificações personalizadas definidas pela AMS: verificações que identificam várias políticas ou padrões de acesso inseguros e excessivamente permissivos em uma entidade ou política do IAM solicitada e negam a solicitação se uma for encontrada. Para obter informações, consulte [Elementos da política AWS JSON: Principal](#).

Descoberta	Descrição
A função pode ser acessada de uma conta externa que esteja fora da sua zona de confiança.	Essa descoberta se refere a um principal listado na política de confiança da função que está fora da sua zona de confiança. Uma zona de confiança é definida como a conta na qual a função está sendo criada ou a AWS organização à qual a conta pertence. Uma entidade que não pertence à conta ou à mesma AWS organização é uma entidade externa. Para resolver a descoberta, revise o ID da conta principal ARNs e certifique-se de que ela

Descoberta	Descrição
	pertence a você e é uma conta integrada do AMS.
A função pode ser acessada por uma entidade externa de propriedade de uma conta <i>External_Account_ID</i> que não pertence à conta de propriedade do cliente do AMS. <i>Account_ID</i>	Essa descoberta é gerada se a política de confiança da função incluir um ARN principal que tenha um ID de conta que não seja de sua propriedade e uma conta integrada do AMS. Para resolver essa descoberta, remova qualquer princípio desse tipo da política de confiança da função.
O ID de usuário canônico não é um princípio aceito na política de confiança do IAM.	Os princípios canônicos não IDs são compatíveis com a política de confiança do IAM. Para resolver a descoberta, remova qualquer princípio desse tipo da política de confiança da função.
A função pode ser acessada por uma identidade externa da Web que esteja fora da sua zona de confiança.	Essa descoberta é gerada se a política de confiança da função permitir um provedor externo de identidade da Web (IdP) diferente do SAML IdP. Para resolver essa descoberta, revise a política de confiança da função e remova as declarações que permitem a <code>sts:AssumeRoleWithWebIdentity</code> operação.
A função pode ser acessada por meio da federação SAML; no entanto, o provedor de identidade SAML (IdP) fornecido não existe.	Essa descoberta é gerada se a política de confiança da função contiver SAML IdP que não existe em sua conta. Para resolver, certifique-se de que todo o IdP SAML listado exista em sua conta.

Descoberta	Descrição
A política contém ações privilegiadas equivalentes ao acesso de administrador ou usuário avançado. Considere reduzir o escopo da permissão a um serviço, ação ou recurso específico. Se elementos de política avançada, como NotAction ou NotResource forem usados, certifique-se de que eles não estejam concedendo mais acesso do que o pretendido, especialmente nas declarações Permitir.	É uma boa prática de segurança AWS Identity and Access Management conceder somente as permissões necessárias para realizar uma tarefa ao definir permissões com políticas do IAM. Faça isso definindo as ações que podem ser tomadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Essa descoberta é gerada quando a automação detecta que a política concede amplas permissões e não segue o princípio do menor privilégio. Para resolver a descoberta, revise e reduza as permissões.
A declaração contém ações privilegiadas para <i>Service_Name</i> . Considere excluir essas ações com uma declaração de negação. Consulte a referência da política de limites na documentação do AMS para obter uma lista de ações privilegiadas.	A AMS identificou certas ações de um determinado serviço como arriscadas e exigem uma análise e aceitação adicionais dos riscos pela equipe de segurança do cliente. Essa descoberta é gerada quando a automação detecta a política fornecida que concede tais permissões. Para resolver essa descoberta, negue essas ações em sua política. Para obter uma lista de ações, consulte a política de limites do AMS. Para obter detalhes sobre a política de limites do AMS, consulte Verificação automatizada do limite de permissão do AMS Automated IAM Provisioning.

Descoberta	Descrição
A declaração concede acesso a tipos de alteração de RFC privilegiados: ct-1n9gfnog5x7fl, ct-1e0xmuy1diafq e ct-17cj84y7632o6 para serviço. <i>Service_Name</i> Considere definir o escopo das permissões para tipos de alteração específicos ou excluir esses tipos de alteração com uma declaração de negação.	Essa descoberta é gerada se a política conceder permissões para realizar ações relacionadas à RFC usando tipos de alteração do Automated IAM Provisioning (). CTs Eles CTs estão sujeitos à aceitação de riscos e só devem ser usados por meio de funções integradas. Então, você não pode conceder permissão a eles CTs. Para resolver essa descoberta, negue ações de RFC usando essas CTs.
A declaração contém ações privilegiadas que não têm como escopo seus recursos de serviço. <i>Service_Name</i> Considere definir o escopo das ações para recursos específicos ou excluir recursos com prefixos de namespace do AMS. Se forem usados curingas, assegure-se de que eles restrinjam o escopo aos seus recursos.	Essa descoberta é gerada se a política conceder ações privilegiadas que não têm como escopo os recursos do determinado serviço. Os curingas geralmente criam políticas excessivamente permissivas que trazem um amplo conjunto de recursos ou ações para o escopo da permissão. Para resolver a descoberta, reduza o escopo das permissões para os recursos que você possui ou exclua os recursos que estão no namespace do AMS. Para obter uma lista dos prefixos de namespace do AMS, consulte a política de limites na documentação do AMS. Observe que nem todos os prefixos se aplicam a todos os serviços. Para obter detalhes sobre a política de limites do AMS, consulte Verificação automatizada do limite de permissão do AMS Automated IAM Provisioning.

Descoberta	Descrição
ID de conta ou nome de recurso da Amazon (ARN) inválido.	Essa descoberta é gerada se qualquer ARN ou ID de conta especificado na política ou na política de confiança da função for inválido. Para analisar os recursos válidos do ARN de recursos para serviços, consulte a Referência de autorização de serviço . Verifique se o ID da conta é um número de 12 dígitos e se a conta está ativa em AWS.
O uso do caractere curinga (*) para o ID da conta no ARN é restrito.	Essa descoberta é gerada se um curinga (*) for especificado no campo ID da conta de um ARN. Um curinga em um campo de ID da conta corresponde a qualquer conta e potencialmente concede permissão não intencional aos recursos. Para resolver isso, substitua o curinga por um ID de conta específico.
Conta de recurso especificada que não pertence à mesma conta <i>Account_ID</i> proprietária do cliente do AMS.	Essa descoberta é gerada se um ID de conta especificado em um ARN de recurso não pertencer a você e não for gerenciado pelo AMS. Para resolver isso, certifique-se de que todos os recursos (conforme especificado pelo ARN na política) pertençam às suas contas gerenciadas pelo AMS.
O nome da função está no namespace restrito do AMS.	Essa descoberta é gerada se você tentar criar uma função com um nome que comece com um prefixo reservado do AMS. Para resolver isso, use um nome para a função que seja específico para seu caso de uso. Para obter uma lista dos prefixos reservados do AMS, consulte Prefixos reservados do AMS .

Descoberta	Descrição
O nome da política está no namespace restrito do AMS.	Essa descoberta é gerada se você tentar criar uma política com um nome que comece com um prefixo reservado do AMS. Para resolver isso, use um nome para a política que seja específico para seu caso de uso. Para obter uma lista dos prefixos reservados do AMS, consulte Prefixos reservados do AMS .
O ID do recurso no ARN está no namespace restrito do AMS.	Essa descoberta é gerada se você tentar criar uma política que conceda permissão aos recursos nomeados que estão no namespace do AMS. Para resolver isso, assegure-se de definir o escopo das permissões para seus recursos ou negar permissões para recursos que estão no namespace AMS. Para obter mais informações sobre namespaces do AMS, consulte Espaços de nomes restritos do AMS .
Caso de variável de política inválido. Atualize a variável para <i>Variable_Names</i> .	Essa descoberta é gerada se você tentar criar uma política que contenha uma variável de política global do IAM no caso incorreto. Para resolver isso, use as maiúsculas e minúsculas corretas para variáveis globais em sua política. Para obter uma lista de variáveis globais, consulte chaves de contexto de condição AWS global . Para obter mais informações sobre as variáveis de política, consulte Elementos de política do IAM: Variáveis e tags

Descoberta	Descrição
A declaração contém ações privilegiadas que não têm como escopo suas chaves KMS. Considere definir o escopo dessas permissões para chaves específicas ou excluir as chaves de propriedade do AMS.	Essa descoberta será gerada se a política contiver permissões que não tenham como escopo as chaves KMS específicas de sua propriedade. Para resolver isso, defina o escopo da permissão para chaves específicas ou exclua as chaves que são de propriedade do AMS. As chaves de propriedade do AMS têm conjuntos de aliases específicos. Para obter uma lista de aliases de chave de propriedade do AMS, consulte Verificação automatizada do limite de permissão do AMS Automated IAM Provisioning.
A declaração contém ações privilegiadas que não têm como escopo os aliases de suas chaves KMS. Considere definir o escopo dessas permissões para suas chaves ou aliases, ou excluir aliases de chave de propriedade da AMS.	Essa descoberta será gerada se a política contiver permissões que não tenham como escopo um alias de chaves KMS específico que você possui. Para resolver isso, defina o escopo da permissão para chaves específicas ou exclua as chaves que são de propriedade do AMS. As chaves de propriedade do AMS têm conjuntos de aliases específicos. Para obter uma lista de aliases de chave de propriedade do AMS, consulte Verificação automatizada do limite de permissão do AMS Automated IAM Provisioning.

Descoberta	Descrição
A declaração contém ações privilegiadas que não têm um escopo adequado para suas chaves KMS usando o <code>kms:ResourceAliases condition</code>. Considere usar nomes de alias específicos junto com o operador de conjunto apropriado para a chave de condição. Se forem usados curingas nos nomes de alias, assegure-se de que eles restrinjam o escopo a um conjunto limitado de suas chaves KMS.	Essa descoberta é gerada se você estiver definindo o escopo das permissões para suas chaves KMS usando condições e não usando o <code>kms:ResourceAliases</code> escopo de aliases para suas chaves KMS. Ou, se a chave de <code>kms:ResourceAliases</code> condição tiver um valor que também inclua aliases de chaves KMS de propriedade do AMS. Para resolver isso, atualize a condição para restringir a permissão somente para aliases de suas chaves KMS ou excluir aliases para chaves KMS de propriedade do AMS. Para obter uma lista de aliases de chave de propriedade do AMS, consulte Verificação automatizada do limite de permissão do AMS Automated IAM Provisioning.
A função deve ter <code>customer_deny_policy</code> anexada. Inclua o ARN da política na lista de políticas gerenciadas. ARNs	Essa descoberta é gerada se a função que você está criando não tiver o <code>customer_deny_policy</code> anexo a ela. Para resolver isso, inclua o <code>customer_deny_policy</code> na ARNs lista de políticas gerenciadas.
A política AWS gerenciada é excessivamente permissiva ou concede permissões restritas pela política de limites do AMS.	Essa descoberta é gerada se o <code>ManagedPolicyArns</code> valor da função contiver alguma política gerenciada pelo AMS que forneça acesso total ou em nível de administrador ao serviço relevante. Para resolver isso, revise o uso da política AWS gerenciada e use uma política que forneça permissão de redução de escopo ou defina sua própria política que siga o princípio do menor privilégio.

Descoberta	Descrição
A política gerenciada pelo cliente está em um namespace restrito do AMS.	Essa descoberta é gerada se alguma política gerenciada pelo cliente com nome prefixado no AWS namespace for anexada à função. Para resolver isso, remova a política da ManagedPolicyArnlista da função.
A <code>customer_deny_policy</code> não pode ser separada da função. Inclua o ARN da política na lista de políticas gerenciadas. ARNs	Essa descoberta é gerada se o <code>customer_deny_policy</code> for separado da função durante uma atualização. Para resolver isso, adicione o <code>customer_deny_policy</code> ao <code>ManagedPolicyArns</code> campo da função e tente novamente.
As políticas gerenciadas pelo cliente foram provisionadas fora do serviço AMS Change Management ou sem validação prévia.	Essa descoberta é gerada se uma ou mais políticas existentes gerenciadas pelo cliente ARNs estiverem vinculadas a uma função e as políticas não forem provisionadas por meio do serviço AMS Change Management (por meio de uma RFC). Por exemplo, o Modo Desenvolvedor ou o Modo de Alteração Direta permitem que os clientes provisionem políticas do IAM sem um RFC. Para resolver isso, remova a política gerenciada pelo cliente ARNs da <code>ManagedPolicyArns</code> lista da função.
A contagem de políticas gerenciadas fornecidas ARNs excede a cota da política anexada por função.	Essa descoberta é gerada se o número total de políticas gerenciadas anexadas à função exceder a cota de política por função. Para obter mais informações sobre cotas do IAM, consulte cotas do IAM e AWS STS, requisitos de nome e limites de caracteres . Use essas informações para reduzir o número de políticas que você atribui à função.

Descoberta	Descrição
O tamanho da política de confiança ({trust_policy}) excede a cota de tamanho da política de assumir funções de {size}.	Essa descoberta é gerada se o tamanho do documento de política de assumir função exceder a cota de tamanho da política. Para obter mais informações sobre cotas do IAM, consulte cotas do IAM e AWS STS, requisitos de nome e limites de caracteres.
A declaração contém todas as ações mutativas do Amazon S3. Considere definir o escopo dessas permissões somente para as ações necessárias. Se forem usados curingas, certifique-se de que eles abrangem um conjunto limitado de ações mutativas.	Essa descoberta é gerada se a política dada conceder a todas as permissões mutativas do Amazon Simple Storage Service, independentemente de um ou mais recursos. Para resolver isso, inclua somente as ações mutativas necessárias do Amazon S3 em seus buckets.
A declaração contém ações privilegiadas que não são permitidas em nenhum bucket no Amazon S3. Considere adicionar uma declaração negando essas ações.	Essa descoberta é gerada se a política conceder ações privilegiadas em qualquer bucket. Para obter uma lista de ações privilegiadas, consulte Verificação automatizada do limite de permissão do AMS Automated IAM Provisioning Para resolver essa descoberta, remover ou negar essas ações em sua política.
A declaração contém ações privilegiadas que não têm como escopo seus buckets no Amazon S3. Considere incluir seus buckets ou excluir buckets com prefixos de namespace do AMS. Se forem usados curingas, certifique-se de que eles correspondam aos buckets em seus namespaces.	Essa descoberta é gerada se a política conceder ao Amazon S3 ações que não têm como escopo somente seus buckets. Isso geralmente ocorre quando caracteres curingas são usados ao especificar recursos do bucket. Para resolver isso, especifique os nomes dos buckets ou ARNs se você possui ou exclui os buckets que têm prefixos de namespace AMS.

Descoberta	Descrição
A declaração contém ações privilegiadas que não têm como escopo seus buckets no Amazon S3. Considere evitar o uso de curingas (*) que abrangem todos os compartimentos da conta.	Essa descoberta é gerada se a política conceder ao Amazon S3 ações que não têm como escopo o seu bucket. Isso geralmente ocorre quando caracteres curingas são usados ao especificar recursos do bucket. Para resolver isso, especifique os nomes dos buckets ou ARNs se você possui ou exclui os buckets que têm prefixos de namespace AMS.
A declaração contém um caractere curinga de recursos que tem como escopo todos os buckets do Amazon S3, incluindo buckets inexistentes e buckets que você não possui. Considere definir o escopo das permissões usando uma condição e uma chave de <code>s3:ResourceAccount</code> condição.	Essa descoberta é gerada se a política conceder permissão aos compartimentos especificados usando curingas. O uso de curingas geralmente coloca baldes inexistentes ou não proprietários no escopo. Para resolver isso, use a condição e a chave de <code>aws:ResourceAccount</code> condição para definir o escopo da permissão para buckets somente na conta atual. Para obter mais detalhes, consulte Limitar o acesso aos buckets do Amazon S3 pertencentes a contas específicas. AWS
A declaração contém um elemento de <code>NotResource</code> política, que pode ter como escopo um grande número de compartimentos, incluindo compartimentos inexistentes e compartimentos que você não possui. Considere definir o escopo das permissões usando uma condição e uma chave de <code>s3:ResourceAccount</code> condição.	Essa descoberta é gerada se a política utilizar o elemento de <code>NotResources</code> política para especificar os recursos do bucket. O uso do <code>NotResource</code> elemento pode abranger um grande número de compartimentos, incluindo compartimentos inexistentes ou não proprietários. Para resolver isso, use condições e a chave de <code>aws:ResourceAccount</code> condição para definir o escopo da permissão para buckets somente na conta atual.

Descoberta	Descrição
A declaração contém a ação do Amazon S3 para buckets <i>Bucket_Name</i> que não existem, não são de propriedade da conta <i>Account_ID</i> ou o nome contém um curinga que pode ter como escopo um grande número de buckets, incluindo buckets inexistentes e buckets que você não possui. Considere definir o escopo das permissões usando uma condição e a chave de <code>s3:ResourceAccount</code> condição	Essa descoberta é gerada se a política conceder permissão a compartimentos que não existem, não são de sua propriedade ou têm curingas nos nomes dos compartimentos que abrangem um grande número de compartimentos e o acesso não tem como escopo somente a conta atual. Para resolver isso, use a condição e a chave de <code>aws:ResourceAccount</code> condição para definir o escopo da permissão para buckets somente na conta atual.
A declaração contém a ação do Amazon S3 para buckets <i>Bucket_Name</i> que não existem, não são de propriedade da conta <i>Account_ID</i>, ou o nome contém um curinga que pode ter como escopo um grande número de buckets, incluindo buckets inexistentes e buckets que você não possui. O acesso não é restrito por uso <code>s3:ResourceAccount</code> ou conta de recurso especificada na condição de não pertencer a você.	Essa descoberta é gerada se a política conceder permissão a compartimentos que não existem, não são de sua propriedade ou têm curingas nos nomes dos compartimentos que abrangem um grande número de compartimentos e o acesso é limitado somente a uma conta específica. No entanto, a conta especificada na chave de <code>aws:ResourceAccount</code> condição não pertence a você e é gerenciada pelo AMS. Para resolver isso, atualize a chave de <code>aws:ResourceAccount</code> condição e defina a ID de conta apropriada que você possui e é gerenciada pelo AMS.

Descoberta	Descrição
A declaração contém ações privilegiadas que não têm como escopo suas instâncias da Amazon. EC2 Considere definir o escopo das ações para uma instância específica ARNs ou excluir instâncias que tenham a chave de tag de nome com valor nos prefixos de namespace do AMS. Se forem usados curingas, verifique se eles correspondem aos namespaces que você possui.	Essa descoberta é gerada se a política conceder ações privilegiadas contra EC2 instâncias da Amazon que o AMS possui. As instâncias do AMS são marcadas com a chave Name tag com valores no namespace AMS. Para resolver isso, especifique seus recursos ou exclua instâncias do AMS com uma condição que tenha a <code>aws:ResourceTag/Name</code> chave que exclui valores no namespace do AMS usando o operador <code>StringNotLike</code>
A declaração contém ações privilegiadas que não têm como escopo seus recursos no repositório de AWS Systems Manager parâmetros. Considere especificar ARNs seus parâmetros ou excluir parâmetros com prefixos de namespace do AMS. Se forem usados curingas, certifique-se de que eles definem apenas seus parâmetros.	Essa descoberta é gerada se a política conceder permissões a parâmetros que você não possui. Geralmente, isso ocorre quando curingas são usados ou parâmetros com prefixos de namespace AMS são listados em recursos em uma declaração de política. Para resolver isso, especifique os parâmetros que estão dentro do seu namespace ou exclua os parâmetros do AMS com uma instrução de negação.
A declaração contém ações privilegiadas contra recursos em AWS Systems Manager. Considere definir o escopo das permissões para somente ler ações ou ações em relação aos seus recursos.	Essa descoberta é gerada se a política conceder permissões diferentes do armazenamento de parâmetros ou ações somente de leitura em relação aos recursos do Systems Manager. Para resolver essa descoberta, reduza as permissões para ações somente para leitura ou somente para armazenamento de parâmetros.

Descoberta	Descrição
A declaração contém ações privilegiadas que não têm como escopo {message} <i>Service_Name</i> que você possui. Considere definir o escopo dessas permissões para tipos de recursos específicos, conforme apropriado, ou excluir recursos de propriedade do AMS. Se forem usados curingas, verifique se eles correspondem <i>Resources</i> .	Essa descoberta é gerada se a política permitir ações privilegiadas que não são concedidas contra seus recursos, especialmente para recursos nomeados. Para resolver essa descoberta, revise sua lista de recursos e veja se eles abrangem apenas os recursos que estão em seu namespace. Como alternativa, exclua os recursos que estão no namespace AMS.
A declaração contém ações de marcação de {<i>Service_Name</i> } que não têm como escopo valores específicos para a chave da tag Name. Considere definir o escopo dessas ações definindo a chave de <code>aws:RequestTag/Name</code> e condição com valores em seu namespace ou restrinja essas ações definindo a chave de <code>aws:RequestTag/Name</code> condição com o <code>StringNotLike</code> operador com valores nos prefixos de namespace do AMS.	Essa descoberta é gerada se a política conceder permissão de marcação para determinado serviço e a permissão não tiver como escopo chaves/valores de tag específicos. Para definir qual chave ou valor pode ser usado em ações de tag, por exemplo, ao fazer uma solicitação para realizar as ações, use a <code>aws:RequestTag/tag key</code> condição. Portanto, para resolver isso, use essa chave de condição para restringir a chave ou os valores no seu namespace. Ou negue a <code>Name tag key</code> (<code>aws:RequestTag/Name</code>) com valores no namespace AMS.
Erro interno ao validar a política de confiança da função do IAM.	Essa descoberta é gerada quando a automação de CT encontra um erro ao realizar a validação na política de confiança da função do IAM por meio do serviço IAM Access Analyzer. Para resolver isso, reenvie o RFC. Se o erro persistir, entre em contato com o AMS Operations para solucionar o erro.

Descoberta	Descrição
Erro interno ao validar a política gerenciada pelo cliente.	Essa descoberta é gerada quando a automação de CT encontra um erro ao realizar a ovalidação na política gerenciada pelo cliente por meio do serviço IAM Access Analyzer. Para resolver isso, reenvie o RFC. Se o erro persistir , entre em contato com o AMS Operations para solucionar o erro.
Analizador de acesso não encontrado em <i>Região da AWS</i> . Não é possível realizar a verificação prévia de acesso à política de confiança da função.	Essa descoberta é gerada quando o recurso IAM Access Analyzer não é encontrado no Região da AWS. Entre em contato com o AMS Operations para solucionar problemas e criar o recurso IAM Access Analyzer na região da AWS.
Política de confiança inválida para a função <i>Role_Name</i>	Essa descoberta é gerada quando a função do IAM é fornecida com uma política de confiança inválida. Para resolver, revise a política de confiança para verificar se ela é válida.
O IAM Access Analyzer encontrou um erro interno. Falha ao criar uma visualização prévia de acesso para a função <i>Role_Name</i>	Essa descoberta é gerada quando a automação encontra um erro ao criar uma visualização prévia de acesso para uma função por meio do IAM Access Analyzer. Para resolver isso, reenvie o RFC. Se o erro persistir , entre em contato com o AMS Operations para solucionar o erro.
Falha ao criar uma visualização prévia de acesso para a política de confiança da função <i>Role_Name</i>	Essa descoberta é gerada quando a automação encontra um erro ao criar uma visualização prévia de acesso para uma função por meio do IAM Access Analyzer. Para resolver isso, reenvie o RFC. Se o erro persistir , entre em contato com o AMS Operations para solucionar o erro.

Descoberta	Descrição
Erro interno ao validar o SAML IdP listado.	Essa descoberta é gerada quando a automação encontra um erro ao validar o SAML fornecido IdPs listado na política de confiança da função. Para resolver isso, reenvie o RFC. Se o erro persistir, entre em contato com o AMS Operations para solucionar o erro.
Erro interno ao validar permissões em relação AWS Key Management Service ao.	Essa descoberta é gerada quando a automação encontra um erro ao validar as AWS KMS principais permissões na política fornecida. Para resolver isso, reenvie o RFC. Se o erro persistir, entre em contato com o AMS Operations para solucionar o erro.
Erro interno ao validar a política ARNs gerenciada listada.	Essa descoberta é gerada quando a automação encontra um erro ao validar a política gerenciada listada. ARNs Para resolver isso, reenvie o RFC. Se o erro persistir, entre em contato com o AMS Operations para solucionar o erro.
Erro interno ao validar o customer_deny_policy anexo padrão.	Essa descoberta é gerada quando a automação encontra um erro ao validar se o customer_deny_policy está vinculado à função. Para resolver isso, reenvie o RFC. Se o erro persistir, entre em contato com o AMS Operations para solucionar o erro.
Erro interno ao validar alertas de política gerenciada para a função <i>Role_Name</i>	Essa descoberta é gerada quando a automação encontra um erro ao validar a política gerenciada ARNs para a função. Para resolver isso, reenvie o RFC. Se o erro persistir, entre em contato com o AMS Operations para solucionar o erro.

Descoberta	Descrição
Erro interno de validação em <i>Policy_name</i> relação à política de limites definida pelo cliente <code>AWSManagedServicesIAMProvisionCustomerBoundaryPolicy</code>	Essa descoberta é gerada quando a automação encontra um erro ao validar a política que contém sua lista de negação personalizada. Para resolver isso, reenvie o RFC. Se o erro persistir, entre em contato com o AMS Operations para solucionar o erro.
A política de limites definida pelo cliente <code>AWSManagedServicesIAMProvisionCustomerBoundaryPolicy</code> existe na conta. No entanto, a política contém declarações de permissão que concedem permissões. A política deve conter apenas declarações de negação.	Essa descoberta é gerada quando a política que contém sua lista de negação personalizada inclui uma declaração que concede permissão. Embora a lista de negação personalizada exista em sua conta como uma política gerenciada pelo IAM, ela não pode ser usada para gerenciamento de permissões. A política deve conter apenas declarações de negação que indiquem que você deseja que o AMS Automated IAM Provisioning valide e negue as ações em suas políticas do IAM que o AMS Automated IAM Provisioning cria.
A declaração contém ações privilegiadas definidas por sua organização para <i>Service_Name</i>. Considere excluir essas ações com uma declaração de negação. Consulte a política mencionada em sua conta para ver a lista restrita de ações.	Essa descoberta é gerada quando a automação detecta qualquer ação em sua política que você definiu na lista de negação personalizada. Para resolver a descoberta, revise sua declaração de política e remova todas as ações definidas em sua lista de negação personalizada ou adicione uma declaração de negação que negue essas ações.
A função deve ter sido <i>POLICY_ARN</i> anexada. Inclua o ARN da política na lista de políticas gerenciadas. ARNs	Essa descoberta é gerada se a função que você está criando não estiver <i>POLICY_ARN</i> associada a ela. Para resolver isso, inclua o <i>POLICY_ARN</i> no <code>ManagedPolicyArns</code> campo da função e tente novamente.

Descoberta	Descrição
Eles não POLICY_ARN podem ser separados da função. Inclua o ARN da política na lista de políticas gerenciadas. ARNs	Essa descoberta é gerada se o POLICY_ARN for separado da função durante uma atualização. Para resolver isso, adicione o POLICY_ARN ao ManagedPolicyArns campo da função e tente novamente.

Verificação automatizada do limite de permissão do AMS Automated IAM Provisioning

As verificações de limites de permissão do AMS ajudam você a aderir à política de limite de permissão padrão fornecida pelo AMS. Essa política é uma lista de ações negadas pelo AMS Automated IAM Provisioning. As políticas de provisionamento que contêm essas ações restritas exigem aceitação explícita adicional do risco. Faça o download da política aqui: [boundary-policy.zip](#).

Use verificações de política de limite de permissão definidas pelo cliente para personalizar ações de negação além dos padrões da política de limite de permissão do AMS. Ao integrar o aprovisionamento automatizado de IAM do AMS usando o seguinte tipo de alteração: Gerenciamento | Conta gerenciada | Provisionamento automatizado do IAM do AMS com permissões de leitura e gravação | [Ativar \(revisão necessária\) \(ct-1706xvvk6j9hf\)](#), você pode incluir uma lista de ações de negação personalizadas que especificam ações restritas adicionais.

Você pode atualizar a lista de ações de negação usando o tipo de alteração: Gerenciamento | Conta gerenciada | Provisionamento automatizado de IAM com permissões de leitura e gravação | [Atualizar lista de negação personalizada](#) (ct-2r9xvd3sdsic0). Você deve usar a função dedicada do IAM `AWSManagedServicesIAMProvisionAdminRole` para executar esse tipo de alteração.

Note

- Você deve fornecer uma lista abrangente de ações de negação para cada atualização. A lista anterior é substituída pela nova lista.
- A lista de ações de negação deve conter somente ações a serem negadas. Não há suporte para ações de permissão.
- A lista de ações de negação reside na conta como uma política gerenciada do IAM chamada `AWSManagedServicesIAMProvisionCustomerBoundaryPolicy`. A política não deve ser vinculada a nenhuma função.

- O termo limite de permissão usado para denotar ações negadas no AMS Automated IAM Provisioning tem um significado contextual diferente em comparação com o limite de permissão do IAM. O limite de permissão do IAM define a permissão máxima que uma política pode conceder em tempo de execução a uma entidade do IAM. Para obter mais informações sobre o limite de permissão do IAM, consulte [Tipos de política](#) no Guia do AWS Identity and Access Management usuário. O limite de permissão no AMS Automated IAM Provisioning impede que você provisione uma política do IAM que contenha um determinado conjunto de permissões, por exemplo, uma lista de ações negadas.

Solução de problemas e erros do AMS Automated IAM Provisioning

Há três maneiras pelas quais você pode ter problemas ao usar o AMS Automated IAM Provisioning:

- Erros de RFC: podem ocorrer por vários motivos; por exemplo, entrada incorreta. Para obter mais informações, consulte [Solução de problemas de erros de RFC no AMS](#).
- Erros de SSM: podem ocorrer por vários motivos; por exemplo, formatação incorreta. Para obter mais informações, consulte [Solução de problemas de automação do Systems Manager](#).
- Conclusões da verificação de validação: elas ocorrem quando uma das muitas verificações de validação executadas pelo Automated IAM Provisioning encontra um problema. Para obter uma lista de verificações de validação e ações recomendadas para corrigir, consulte [Verificações de tempo de execução do provisionamento automatizado de IAM do AMS no AMS](#).

Definindo permissões no AMS com funções e perfis do IAM

O AMS usa AWS Identity and Access Management (IAM) para gerenciar usuários, credenciais de segurança, como chaves de acesso, e permissões que controlam quais AWS recursos os usuários e aplicativos podem acessar. O AMS fornece uma função de usuário padrão do IAM e um perfil de EC2 instância padrão da Amazon (que inclui uma declaração permitindo que o recurso acesse a função de usuário padrão do IAM).

Solicitar uma nova função de usuário ou perfil de instância do IAM

O AMS usa uma função do IAM para definir permissões de usuário por meio do seu serviço de federação e um perfil de instância do IAM como um contêiner para essa função do IAM.

Você pode solicitar uma função personalizada do IAM com os componentes Deployment | Advanced stack | Identity and Access Management (IAM) | Criar entidade ou política (revisão obrigatória) tipo de alteração (ct-3dpd8mdd9jn1r) ou um perfil de instância do IAM com o tipo de alteração Management | Applications | IAM | Create Management | Applications | Perfil da instância do IAM | Criar (revisão obrigatória) tipo de alteração (ct-0ixp4r) ch2tiu04). Veja as descrições de cada um nesta seção.

Note

O AMS tem uma política de IAM `customer_deny_policy` que bloqueia namespaces e ações perigosas. Essa política é anexada a todas as funções de clientes do AMS por padrão e raramente é um problema para os usuários. Suas solicitações de usuário e função do IAM não incluem essa política, mas a inclusão automática delas `customer_deny_policy` nas solicitações de funções do IAM ajuda o AMS a implantar novos perfis de instância do IAM mais rapidamente. Você pode solicitar a exclusão da `customer_deny_policy` política. No entanto, essa solicitação passará por uma análise de segurança pesada e provavelmente será recusada por motivos de segurança.

Restrinja as permissões com declarações de política de função do IAM

O AMS usa uma função do IAM para definir permissões de usuário por meio do seu serviço de federação.

Zona de destino de conta única AMS: consulte [SALZ: Funções de usuário padrão do IAM](#).

Zona de destino de várias contas AMS: consulte [MALZ: Funções de usuário padrão do IAM](#).

Uma função do IAM é uma entidade do IAM que define um conjunto de permissões para fazer solicitações AWS de serviço. As funções do IAM não estão associadas a um usuário ou grupo específico. Em vez disso, entidades confiáveis assumem funções, como usuários, aplicativos ou AWS serviços do IAM, como a Amazon EC2. Para obter mais informações, consulte [Perfis do IAM](#).

Você pode definir o escopo da política desejada para um usuário que assume a função de usuário do AMS IAM usando a operação da API AWS Security Token Service (STS) [AssumeRole](#) transmitindo uma política IAM mais restritiva no campo de `Policy` solicitação.

Exemplos de declarações de política que você pode usar para restringir o acesso ao CT são fornecidos a seguir.

Usando seus grupos configurados do Active Directory (AD) e a operação da API do AWS Security Token Service (STS) [AssumeRole](#), você pode definir permissões para determinados usuários ou grupos, incluindo restringir o acesso a determinados tipos de alteração (CTs). Você pode usar as declarações de política mostradas abaixo para restringir o acesso ao CT de várias maneiras.

Declaração de tipo de alteração do AMS no perfil padrão da instância do IAM que permite acesso a todas as chamadas de API do AMS (amscm e amsskms) e a todos os tipos de alteração:

```
{
  "Sid": "AWSManagedServicesFullAccess",
  "Effect": "Allow",
  "Action": [
    "amscm:*",
    "amsskms:*"
  ],
  "Resource": [
    "*"
  ]
}
```

1. Declaração para permitir o acesso e todas as ações para apenas dois itens especificados CTs, em que “Ação” são as operações da API AMS (amscm/amsskms) e “Recurso” representa o tipo de alteração existente IDs e o número da versão:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "amscm:*",
      "Resource": [
        "arn:aws:amscm:*:*:changetype/ct-ID1:1.0",
        "arn:aws:amscm:*:*:changetype/ct-ID2:1.0"
      ]
    }
  ]
}
```

2. Declaração para permitir o acesso para CreateRfc UpdateRfc, e SubmitRfc em apenas duas especificadas CTs:
3. Declaração para permitir o acesso a CreateRfc UpdateRfc, e SubmitRfc sobre todos os disponíveis CTs:
4. Declaração para negar o acesso a todas as ações na TC restrita e permitir outras CTs:

Restrinja as permissões com perfis de instância EC2 do Amazon IAM

Um perfil de instância do IAM é um contêiner para uma função do IAM que você pode usar para passar informações da função para uma EC2 instância da Amazon quando a instância é iniciada.

Atualmente, há um perfil de instância padrão do AWS Managed Services (AMS) que concede permissões aos aplicativos em execução na instância, não aos usuários que fazem login na instância. `customer-mc-ec2-instance-profile` Talvez você queira modificar o perfil de instância padrão ou criar um novo, se quiser dar a uma instância acesso a algo, sem conceder acesso a outras instâncias também. Você pode solicitar um novo perfil de instância do IAM com Management | Applications | IAM instance profile | Create change type (ct-0ixp4ch2tiu04). Ao enviar a RFC, você pode criar seu próprio perfil de instância e incluí-lo como o. InstanceProfileDescription ou pode simplesmente informar ao AMS (usando o mesmo campo) quais alterações você deseja. Como se trata de uma tomografia computadorizada manual, a AMS deve aprovar a alteração e entrará em contato com você sobre ela.

Se você não estiver familiarizado com as políticas do Amazon IAM, consulte [Visão geral das políticas do IAM](#) para obter informações importantes. Também há uma boa postagem no blog, [Desmistificando as permissões em nível de recursos da EC2 Amazon](#). Observe que o AMS atualmente não oferece suporte ao controle de acesso baseado em recursos, mas oferece suporte a controles em nível de recurso usando políticas de função do IAM (para obter uma explicação da diferença, consulte [AWS Serviços](#) que funcionam com o IAM).

Zona de aterrissagem AMS de conta única:

Para ver uma tabela de permissões que o perfil padrão da instância do AMS IAM concede, acesse o [Perfil da instância EC2 do IAM](#).

Regra de declaração do AD FS e configurações de SAML

ActiveDirectory Regra de declaração do Federation Services (AD FS) e configurações de SAML para AWS Managed Services (AMS)

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](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 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-FQDN]/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 da AWS CLI](#)
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. Baixe o 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 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 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

\$ sudo pip install boot

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

Restringir com ACL de rede

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 zona de aterrissagem multicontas gerenciada pelo 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 do Multi-Account Landing Zone, ou seja, conta de gerenciamento, rede, serviços compartilhados, registro e segurança.
- NACLs são compatíveis com contas do Multi-Account Landing Zone Application, desde que sejam usadas apenas como uma lista de “Negar” e tenham “Permitir tudo” para permitir 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 zona de destino de várias contas do AMS para segregar o tráfego de rede entre elas. VPCs

AMS em Outposts

[AWS Outposts](#) é uma solução de hardware gerenciada que estende as zonas de aterrissagem gerenciadas pelo AMS até os data centers dos clientes. Com o suporte do AMS ativado AWS Outposts, os clientes que buscam a experiência em nuvem, a economia de custos e a plataforma padronizada oferecida pela AMS não estão mais limitados a hospedar recursos internos Regiões da AWS. Com o AMS ativado AWS Outposts, os clientes com requisitos locais agora podem se modernizar e aproveitar os serviços de correção AWS, backup, provisionamento, gerenciamento de incidentes, continuidade de negócios e otimização de custos oferecidos pelo AMS.

Depois que um AWS Outposts for ativado em sua conta AMS Multi-Account Landing Zone ou Single-Account Landing Zone, você pode seguir os processos existentes de gerenciamento de alterações do AMS para provisionar e gerenciar AWS recursos. A infraestrutura hospedada pelo AMS pode ser gerenciada especificando sua AWS Outposts sub-rede específica. AWS Outposts os ciclos de vida podem ser gerenciados diretamente no AWS Outposts console usando a função de serviços de AWS Outposts autopvisionamento.

Para obter informações sobre a função, consulte [AWS Outposts](#).

AWS Outposts gerenciamento operacional e de instalação

O AWS Outposts processo de integração ao AMS on é composto por:

1. Planejamento de Outposts
2. Validação do pedido
3. Integração de Outposts ao AMS
4. Gerenciamento de ciclo de vida

AWS Outposts planejamento

Durante o AWS Outposts planejamento, você identifica o AMS em casos de AWS Outposts uso e envolve as principais partes interessadas, incluindo sua equipe de contas e AWS Outposts representantes da AMS, para alinhar a estratégia de capacidade.

1. Depois que os casos de uso que exigem a ativação do AMS forem AWS Outposts identificados, envolva sua equipe de contas do AMS para discutir o planejamento de capacidade.
2. Depois que seus requisitos de AWS Outposts capacidade forem determinados, sua equipe de contas do AMS envolve a equipe de AWS Outposts serviço para discutir o plano de AWS Outposts integração, as funções e as responsabilidades. Durante esse período, um AWS Outposts único ponto de contato (SPOC) é atribuído a você. O AWS Outposts SPOC auxilia na finalização AWS Outposts dos requisitos de dimensionamento.

AWS Outposts validação do pedido

Durante a validação do pedido, você cria um AWS Outposts site e solicita a capacidade necessária diretamente no AWS Outposts console ou por meio do representante da sua AWS Outposts conta.

Depois que você, a equipe da conta do AMS e a AWS Outposts equipe estiverem alinhadas, você poderá solicitar a função de serviço AWS Outposts autopvisionada usando o ID do tipo de alteração ct-3qe6io8t6jtny, para criar seu site e fazer o pedido diretamente no console. AWS Outposts AWS Outposts

Como alternativa, você pode trabalhar por meio do AWS Outposts SPOC para criar sites e pedidos do Outpost. Seu AWS Outposts SPOC continua fornecendo atualizações de status para você e para a equipe da conta do AMS durante a validação e AWS Outposts instalação do site e do pedido.

AWS Outposts integração ao AMS

Depois que sua AWS Outposts unidade for ativada em sua VPC gerenciada pelo AMS, você poderá solicitar a criação de monitores para rastrear a disponibilidade, a capacidade, as exceções e a conectividade de rede do seu hardware Outposts. Ao seguir as etapas de implantação de monitoramento descritas a seguir, seu AWS Outposts hardware é monitorado ativamente pelo AMS.

1. Depois de instalado e ativado, você pode solicitar um monitoramento AWS Outposts específico enviando o seguinte modelo com um RFC usando o tipo de alteração Management | Other | Other | Create (ct-1e1xtak34nx76). AWS Outposts As operações do AMS garantem que a AWS Outposts sub-rede seja rastreada nas ferramentas internas do AMS.

- AWS Outposts ID
- CIDR da sub-rede
- AWS Outposts Alarmes recomendados:
 - InstanceFamilyCapacityAvailabilityAlert
 - InstanceTypeCapacityAvailabilityAlert
 - EBSVolumeTypeCapacityAvailabilityAlert
 - CapacityExceptionsAlert
 - Direct Connect ConnectionAlert
- Para cada um dos alertas acima, especifique os seguintes parâmetros:
 - Estatística (“Média” é recomendada). Outras opções incluem soma, máximo, mínimo, contagem de amostras e p90)
 - O período (“5 minutos” é recomendado). Outras opções incluem 10 e 30 segundos, 1, 5 e 15 minutos, 1 e 6 horas e 1 dia)
 - O tipo de limite (“Estático”) é recomendado. “Anomalia” também são opções.)
 - Condição (“Sempre que a contagem de chamadas for maior que”, “igual a”, “menor que” também são opções.)
 - O valor da condição (“ 25% ”) é configurado por padrão. Outro número inteiro positivo é permitido.)
 - Tópico de notificação (tópicos de operações do AMS) são atribuídos automaticamente. No entanto, qualquer outro tópico, ou personalizado, também pode ser adicionado.)

2. Suporte de monitoramento e operações

- As operações do AMS monitoram AWS Outposts métricas de desconexão de rede ou falhas de componentes. As operações do AMS fornecem serviços de primeira resposta para AWS Outposts problemas e escalam, se necessário, para suporte ou EC2 suporte Premium.
 - As operações do AMS estão disponíveis para resolver problemas relacionados à sua AWS Outposts unidade.
3. Quando as verificações do status da EC2 instância ou do sistema falham, as operações do AMS seguem os processos existentes para colocar a instância novamente on-line. Se a reinicialização falhar ou a AWS Outposts capacidade for insuficiente, um membro da equipe de operações do AMS notificará você diretamente para determinar as próximas etapas.

AWS Outposts gerenciamento do ciclo de vida

Depois AWS Outposts de ser integrado à sua conta do AMS, você é notificado se ocorrer alguma disponibilidade, capacidade ou exceção de rede. Você pode descomissionar AWS Outposts diretamente pelo AWS Outposts console ou pelo AWS Outposts SPOC.

Você pode gerenciar AWS Outposts diretamente no AWS Outposts console usando a função de serviço de provisionamento AWS Outposts de autoatendimento ou o modo de desenvolvedor. Você também pode solicitar AWS Outposts por meio de seu CSDM, ou ponto AWS Outposts único de contato (SPOC).

A alta disponibilidade do on AWS Outposts pode ser alcançada com a implantação de dois ou mais. AWS Outposts A configuração de duas ou mais AWS Outposts habilita a opção de zona de multidisponibilidade para suas instâncias do Amazon Relational Database Service.

Provisionamento de recursos gerenciados pelo AMS em AWS Outposts

Os AWS recursos de provisionamento hospedados em AWS Outposts (por exemplo, Amazon, Amazon EMR, EC2 Amazon EKS, Amazon ECS, Amazon EBS e Amazon S3) em contas AMS (contas Single-Account Landing Zone, Multi-Account Landing Zone e Accelerate) estão sujeitos aos mesmos níveis de suporte do AMS que os recursos em. Regiões da AWS Você pode usar o gerenciamento de alterações do AMS, os serviços de provisionamento de autoatendimento ou o modo de desenvolvedor para criar e modificar os recursos criados no. AWS Outposts

Atualmente, todos os tipos de instância (m5/M5d, C5/C5d, R5/R5d, I3en, G4dn), Amazon Elastic Block Store, Amazon Elastic Container Service, Amazon Elastic Kubernetes Service, Amazon EMR, Amazon Relational Database Service, Application Load Balancers e o proxy App Mesh Envoy estão

disponíveis diretamente ligado. DBs AWS Outposts Esses recursos são elegíveis para o mesmo suporte de operações do AMS que os recursos nas regiões existentes.

Limitações do AMS em AWS Outposts

- O suporte operacional para recursos AWS Outposts hospedados depende da conectividade de rede consistente. AWS Outposts a desconexão da rede impede que as operações do AMS solucionem quaisquer incidentes ou problemas que ocorram na unidade desconectada. AWS Outposts Para o AMS sobre contingências de nível de AWS Outposts serviço, consulte os [Acordos AWS de Nível de Serviço atualizados \(SLAs\)](#).
- Amazon Relational Database Service:
 - O tipo de alteração de criação do RDS (ct-2z60dyvto9g6c), por padrão, habilita o Multi-AZ e requer um grupo de sub-redes de banco de dados. Os grupos de sub-redes de banco de dados exigem duas sub-redes em duas zonas de disponibilidade (AZ) separadas. Se você tiver apenas um AWS Outposts, criar um grupo de sub-redes de banco de dados é um problema, pois AWS Outposts eles são atribuídos apenas a uma única AZ. Para contornar essa limitação, siga estas instruções:
 1. Solicite um grupo de sub-redes de banco de dados por meio de um RFC com um Management | Other | Other CT e especifique a sub-rede no. AWS Outposts
 2. Crie um modelo de CFN personalizado para implantar o RDS e especifique o grupo de sub-redes criado na etapa anterior. AWS Outposts Para saber mais sobre como fazer isso, consulte [Recursos personalizados](#).
 3. Solicite que o AMS implante o modelo CFN contendo a instância do RDS de destino por meio do AMS CFN ingest CT (ct-36cn2avfrj9v).
 4. Observe que, atualmente, o RDS for AWS Outposts não fornece métricas e registros devido a uma limitação do Serviço RDS.
 - Workload ingest (WIGs): o Linux WIGs só funciona se a WIGs EC2 pré-instância estiver em uma sub-rede. AWS Outposts O motivo é porque o Linux WIGs cria um WIGs nó na sub-rede da primeira EC2 instância usando m4.large, por padrão. Como AWS Outposts não tem esse tipo de instância, não WIGs é capaz de iniciar seu nó de trabalho. A solução alternativa para isso é criar a EC2 instância inicial em uma AWS Outposts sub-rede e, em seguida, a instância de destino pode ser criada em. AWS Outposts Além disso, atualmente, somente os tipos de EC2 instância baseados em Nitro, incluindo C5, C5d, M5, M5d, R5, R5d, G4 e I3en, são suportados no. AWS Outposts

- Amazon Elastic Block Store (EBS): Criar volume CT do EBS (ct-16xg8qguovg2w) não funciona, pois os volumes são criados em vez de não AWS Outposts fornecermos o número de recurso da Amazon (ARN) AWS como parâmetro de entrada para o CT. AWS Outposts
- Conectividade de rede: a conectividade de rede é de sua responsabilidade pela AWS Outposts equipe.
- Brownfield e aquisição de conta: AWS Outposts ativados em contas que não sejam do AMS não podem ser transferidos para o AMS, devido à natureza do AWS Outposts faturamento e dos requisitos de suporte corporativo.

AMS sobre AWS Outposts conformidade

AMS sobre AWS Outposts atestado de conformidade

AWS Outposts o plano de controle foi atestado de acordo com a HIPAA, compatível com PCI e ISO. No entanto, o AMS no plano de AWS Outposts controle não foi atestado. AWS Outposts Por esse motivo, os clientes são incentivados a buscar o atestado de conformidade AMS sobre AWS Outposts meio ambiente.

Para controlar a criação de recursos na unidade Outpost, os clientes são incentivados a segregar o acesso do desenvolvedor ao Outpost, para evitar o excesso de acesso do desenvolvedor nas contas gerenciadas padrão do AMS.

Cargas de trabalho gerenciadas pelo AMS que exigem conformidade com o FedRAMP

Acima de tudo, as contas de gerenciamento do AMS devem primeiro ser avaliadas quanto à conformidade regulatória, pois os dados do plano de controle fluiriam das contas de gerenciamento do AMS AWS Outposts para as contas de gerenciamento do AMS.

Se a certificação FedRAMP for necessária e a estrutura da conta AMS estiver em conformidade, é recomendável que você utilize um fornecedor de datacenter que já tenha a certificação exigida e possua todo o dispositivo de link de serviço (ou que já criptografe os dados de saída).

Por fim, uma proteção adicional de dados pode ser implementada trabalhando com sua equipe de conta para implantar um SCP que restringe os dados AWS Outposts e impede a criação de quaisquer recursos regionais na conta que hospeda o Outpost.

Impacto na conformidade existente das contas AMS

A utilização de uma conta AWS Outposts não precisa ser testada novamente quanto à conformidade, desde que nenhum dado regulamentado esteja sendo consumido e a conta

esteja separada logicamente. As contas de gerenciamento do AMS podem gerenciar contas não regulamentadas e regulamentadas, desde que os fluxos de dados de entrada/saída entre contas cruzadas authentication/authorization e de entrada/saída sejam separados. VPCs Portanto, mesmo que a conta Outpost não compatível e as contas de aplicativos compatíveis existentes estejam na mesma organização (incluindo serviços compartilhados, rede, registro, serviços principais e de segurança do AMS), a conta do aplicativo de conformidade ainda mantém a conformidade, pois os dados são separados logicamente.

AMS ativado AWS Outposts FAQs

Em quais casos de uso se qualificam para o suporte do AMS? AWS Outposts

O AMS on AWS Outposts pode ser utilizado por empresas que precisam de um modelo operacional de nuvem comprovado, com cargas de trabalho que exijam baixa latência (por exemplo, gerenciamento de robôs de fábrica e migração de mainframe), computação de ponta (por exemplo, estações de trabalho remotas e simplificação de dados de borda) e grandes cargas de transferência de dados.

Por que devo usar esse recurso?

O AMS fornece monitoramento de AWS Outposts hardware e primeira resposta a qualquer problema AWS Outposts de hardware. Além disso, os seguintes recursos de suporte para todos os recursos gerenciados hospedados em AWS Outposts:

- Registro, monitoramento, grades de proteção e gerenciamento de eventos
- Gerenciamento de continuidade
- Gerenciamento de segurança e acesso
- Gerenciamento de patches
- Gerenciamento de alterações
- Gerenciamento de provisionamento automatizado e de autoatendimento
- Gerenciamento de incidentes e problemas
- Relatórios (os relatórios AWS Outposts de hardware não serão inicialmente suportados com o AMS ativado AWS Outposts)
- Gerenciamento de solicitações de serviço
- Modo de desenvolvedor
- Enterprise Support

Como faço para usar esse recurso?

AWS Outposts planejamento: durante o AWS Outposts planejamento, você identificou o AMS em casos de AWS Outposts uso e envolverá as principais partes interessadas, incluindo a equipe de contas e AWS Outposts representantes da AMS, para alinhar a estratégia de capacidade.

Validação do pedido: durante a validação do pedido, você cria um AWS Outposts site e solicita a capacidade necessária diretamente no AWS Outposts console ou por meio do representante da sua AWS Outposts conta.

AWS Outposts integração ao AMS: Depois que sua AWS Outposts unidade for ativada em sua VPC gerenciada pelo AMS, você poderá solicitar a integração à AWS Outposts sua conta do AMS enviando uma solicitação de alteração (RFC) usando o modelo no Guia do usuário do AMS (). [AWS Outposts](#) As operações do AMS então criam uma sub-rede e monitoram seu Outpost usando as entradas fornecidas no RFC.

Gerenciamento do ciclo de vida: depois AWS Outposts de integrado à sua conta do AMS, você é notificado sobre qualquer disponibilidade, capacidade ou exceções de rede. Você pode descomissionar AWS Outposts diretamente pelo AWS Outposts console ou pelo seu ponto AWS Outposts único de contato (SPOC).

Quais são as limitações do AMS AWS Outposts?

Os casos de uso de residência de dados (por exemplo, leis de localização de dados específicas de cada país etc.) ainda não foram validados para o AMS on. AWS Outposts

AWS Outposts ativados em contas que não sejam do AMS não podem ser transferidos para o AMS, devido à natureza do AWS Outposts faturamento e aos requisitos do Enterprise Support.

AWS Outposts o plano de controle foi atestado de acordo com a HIPAA, compatível com PCI e ISO. No entanto, o AMS no plano de AWS Outposts controle não foi atestado. AWS Outposts Por esse motivo, os clientes são incentivados a buscar o atestado de conformidade AMS sobre AWS Outposts meio ambiente.

Posso optar por não usar esse recurso?

O provisionamento AWS Outposts em seu ambiente AMS é opcional. Depois de implantado em sua conta do AMS, AWS Outposts pode ser desprovisionado por meio do AWS Outposts console a qualquer momento, se não for mais necessário.

Como o AMS on AWS Outposts será cobrado?

O aumento das AWS Outposts taxas do AMS será aplicado no nível do Grupo B.

Como o Acordo de Nível de Serviço do AMS mudará para se acomodar AWS Outposts?

O gerenciamento de incidentes dependerá da AWS Outposts disponibilidade. AWS Outposts a disponibilidade está sujeita à disponibilidade da rede do cliente, que é de responsabilidade do cliente. AWS Outposts a disponibilidade também está sujeita ao tempo de atividade do AWS Outposts hardware, que depende dos contratos AWS Outposts de nível de serviço.

Consulte também [AWS Outposts FAQs](#).

Usando tags no AMS

Tópicos

- [Etiquetagem automática da infraestrutura AMS](#)
- [Tags recomendadas pelo AMS](#)
- [Marcar notas de atualização em massa](#)

Fornecer etiquetas pode ser de grande valor. Para obter informações detalhadas, leia Como [marcar seus recursos da Amazon EC2](#).

RFCs que criam instâncias, como um bucket do Amazon S3 ou um AWS Elastic Load Balancer (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 mensagem Management | Advanced stack components | Amazon S3 storage | Update CT. Amazon EC2, Amazon EFS, Amazon 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.

Ao usar o console AMS, você deve habilitar a visualização 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 Amazon EC2 stack não oferece um parâmetro para nomear a instância da Amazon EC2. 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 da Amazon será exibida no EC2 console da Amazon sem um atributo de nome.

Há restrições de tag? Sim:

- As tags diferenciam letras maiúsculas de minúsculas.
- O comprimento máximo da chave é 128 caracteres Unicode.
- O número máximo de tags que você pode atribuir a um recurso é 50.
- O número máximo de tags por recurso é 50.
- O prefixo reservado é `aws :`.
- Os nomes e valores de tags gerados pela AWS recebem automaticamente o prefixo `aws :`, que não pode ser atribuído por você. Nomes de tags definidas pelo usuário têm o prefixo `user :` no relatório de alocação de custos.
- Use cada chave somente uma vez para cada recurso. Se você tentar usar a mesma chave duas vezes no mesmo recurso, sua solicitação será rejeitada.
- Os caracteres permitidos são letras Unicode, espaço em branco, números e os seguintes caracteres especiais: `+ - = . _ : /`

Quais tipos AWS de recursos oferecem suporte a tags? Consulte [Agora Organize seus AWS recursos usando até 50 tags por recurso](#).

Etiquetagem automática da infraestrutura AMS

O AMS pode marcar todos os recursos criados pelo AMS para fins de gerenciamento, em suas contas de zona de pouso com várias contas (MALZ) e zona de destino de conta única (SALZ) por meio de uma solicitação de alteração (RFC) com o Deployment | Advanced stack components | Tag | Create (revisão obrigatória) tipo de alteração (ct-0176f0n99vcps). Isso pode ajudá-lo a identificar recursos criados pelo AMS para fins de gerenciamento.

O AMS pode identificar automaticamente os recursos criados pelo AMS com base nos padrões de nomenclatura e verificar se o recurso tem as seguintes chaves e valores de tag - "AppName", "AppId", "AMSResource" e "". EnvironmentType Se a chave de tag não existir ou o valor estiver vazio, essas chaves de tag poderão ser criadas automaticamente pelo AMS com o valor de tag "". AMSInfrastructure

Você pode personalizar as tags desejadas nos recursos criados pela AMS com base nos padrões de marcação da sua organização. Você pode incluir suas próprias chaves e valores de tag ao enviar a solicitação ao AMS. Siga estes padrões de nomenclatura de AWS tags: Melhores [práticas de marcação](#)

 Note

Para contas MALZ, a marcação personalizada da infraestrutura do AMS é suportada somente nas contas do aplicativo. Atualmente, a marcação personalizada nas contas principais não é suportada.

Se o nome da chave de tag que você fornecer em sua RFC já existir no recurso, o valor da tag será substituído pelo novo valor da tag que você forneceu na RFC.

O comprimento total dos pares chave-valor da tag não deve exceder 256 caracteres.

Inclua as seguintes informações em sua RFC com o tipo de alteração Deployment | Advanced stack components | Tag | Create (revisão necessária) (ct-0176f0n99vcps) para marcar recursos criados pelo AMS.

1. Lista de contas de zonas de pouso com várias contas ou de zonas de destino com uma única conta nas quais você gostaria de marcar recursos criados pela AMS para fins de gerenciamento.
2. Nome e valor da chave de tag obrigatórios (se necessário). Por padrão, o AMS pode marcar com o nome da chave de tag como "EnvironmentType" e o valor da tag como "". AMSInfrastructure [Se você precisar de um nome de chave e valor de tag personalizados, siga os padrões de nomenclatura de AWS tag: Melhores práticas de marcação](#)

Atualmente, esses recursos são suportados pela marcação de infraestrutura do AMS:

```
API Gateway
Amazon CloudFront
Amazon DynamoDB
Amazon EBS
Amazon EC2
Amazon OpenSearch Service
Amazon Quantum Ledger Database (QLDB)
Amazon Redshift
Amazon RDS
Amazon S3 (specific buckets only*)
```

```

Amazon Simple Queue Service (SQS)
Amazon Simple Notification Service (SNS)
Amazon VPC AWS Certificate Manager AWS CloudFormation AWS CloudTrail AWS CodeBuild
AWS CodePipeline AWS Elastic Beanstalk AWS Lambda AWS Secrets Manager AWS Service
Catalog AWS Systems Manager AWS WAF Regional
Elastic Load Balancing

```

* “arn:aws:s3: ::awsms-a*-patch-data-*”, “arn:aws:s3: ::ams-a*-log-management-*”, “arn:aws:s3: ::cf-templates-*”, “arn:aws:s3: ::mc-a*”, “arn:aws:s3: :ams-a*-backup-reports-*”, “arn:aws:s3: ::ams-a*- -*”, “arn:aws:s3: ::ams-a*- -*”, “arn:aws:s3: ::ams-a*- -*”, “arn:aws:s3: ::ams-a*-release-assets-assets-s-*”, “arn:aws:s3::: -*”, “arn:aws:s3::: *” patch-data-customer-reports patch-data-raw patch-data-reporting ams-cfn-drift-remediation ams-reporting-data-a

Tags recomendadas pelo AMS

O AMS recomenda as seguintes tags nos recursos compatíveis. As etiquetas com estrela (*) são altamente recomendadas.

Note

Você pode usar tags para agendar a aplicação de patches. Para obter informações, consulte [AMS Advanced Patch Orchestrator: um modelo de patch baseado em tags](#).

Prefixos reservados do AMS

Os atributos dos recursos do AMS devem estar em conformidade com determinados padrões; por exemplo, nomes de perfis de instâncias do IAM, BackupVault nomes, nomes de tags e assim por diante, não devem começar com prefixos reservados do AMS. Esses prefixos reservados são:

```

*/aws_reserved/*
ams - *
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role

```

```

CloudTrail*
Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion

```

Tags recomendadas pelo AMS

Chave de tag	Valores com suporte	Observações
AppName*	Irrestrito.	Identifique os aplicativos que residirão no recurso ou exigirão acesso a ele. Isso facilita o rastreamento e a comunicação entre o AMS e você.
AppId*		
EnvironmentType *		Faça a distinção entre infraestrutura de desenvolvimento, teste e produção como ambiente para o recurso.
OwnerTeamEmail *	Endereço de e-mail da lista de distribuição	Identifique o endereço de e-mail da lista de distribuição da equipe responsáv

Chave de tag	Valores com suporte	Observações
		el pelo recurso. O e-mail não deve ser pessoal; deve ser um e-mail anônimo, como uma lista de distribuição.
ComplianceFramework	Sem restrições	Identifique quais controles e políticas devem ser aplicados ao recurso.
CostCenter		Identifique o centro de custo ou a unidade de negócios associada a um recurso (normalmente para alocação e rastreamento de custos).
Customer		Usado por clientes do AMS que têm recursos de vários clientes (subclientes do AMS). Agrupar recursos no ambiente gerenciado no cliente específico que eles estão atendendo. Identifique um cliente específico em um determinado grupo de recursos ou serviços.
DataClassification		Identifique o nível específico de confidencialidade de dados suportado por um recurso. Identifique quais controles e políticas devem ser aplicados ao recurso.
HoursOfOperation		Identifique a data ou a hora em que um recurso deve ser iniciado, interrompido, excluído ou rotacionado.
OwnerTeam		Identifique a equipe responsável pelo recurso. Facilita a comunicação com a equipe responsável pelo recurso.

Chave de tag	Valores com suporte	Observações
Patch Group	Você tem duas opções: - Você pode enviar uma solicitação de serviço com as informações descritas no AMS Advanced Patch Orchestrator: um modelo de patch baseado em tags, que o AMS cria com base nos recursos especificados e, usando as informações fornecidas, uma tag para você. Patch Group - Se você já criou uma Patch Group tag em seus recursos, os valores suportados são irrestritos.	Quais recursos incluir em uma janela de manutenção automatizada de patches.
ProjectId	Sem restrições	Identifique os projetos que o recurso apoia.

Chave de tag	Valores com suporte	Observações
SupportPriority	Uma das seis siglas possíveis para Confidencialidade, Integridade ou Disponibilidade; a ordem da sigla é a prioridade. Por exemplo, I.C.A. significaria que o pedido é Integridade, Confidencialidade e Disponibilidade. Outros valores aceitáveis são C.I.A., C.A.I., I.A.C., A.C.I. e A.I.C.	Identifique qual tipo de suporte deve ser prioritário: confidencialidade, integridade ou disponibilidade.

Marcar notas de atualização em massa

Essas notas devem ser usadas com os exemplos de alteração do tipo de alteração [Tag | Bulk Update e Tag | Bulk Update \(revisão obrigatória\)](#).

Notas sobre tags de atualização em massa:

- Serviços suportados:
 - Para [Tag | Atualização em massa \(revisão obrigatória\)](#): Tudo.
 - Para [Tag | Atualização em massa](#):
 - ajuste de escala automático
 - Amazon EC2
 - Elastic Load Balancing
 - Amazon RDS
 - Buckets do Amazon S3
- Para gerar o arquivo de valores separados por vírgula (CSV), faça login em Resource Groups > Tag Editor no AWS console, encontre os recursos que você deseja marcar e exporte-os para um arquivo CSV. Para obter mais informações, consulte [Exportar resultados para CSV](#).

OBSERVAÇÃO: recomendamos usar uma URL pré-assinada do S3 para fornecer a localização do objeto CSV.

- Deve haver colunas com os cabeçalhos Serviço, Tipo e Identificador. Essas colunas são obrigatórias.
- Renomeie o identificador da coluna para ID.
- Os valores das colunas Serviço, Tipo e Identificador (alterados para ID) são fornecidos pelo Editor de Tags em Resource Groups.
- Se um recurso a ser marcado não estiver disponível no Editor de tags, use o Amazon Resource Name (ARN) do recurso para a coluna Identifier (alterado para ID) e mantenha Service and Type em branco.
- Os cabeçalhos das colunas das tags a serem adicionadas ou modificadas devem ter o formato Tag: **TagKey**.
- Os cabeçalhos das colunas das tags a serem excluídas devem ter o formato Untag: **TagKey**.
- Cada linha é para que um recurso seja marcado ou desmarcado.
- Se uma tag for adicionada a um recurso, especifique o valor da tag na **TagKey** coluna Tag: apropriada.
- Se uma tag precisar ser excluída de um recurso, especifique True na **TagKey** coluna Untag: apropriada.
- Se um Tag: **TagKey** ou Untag: não **TagKey** for aplicável a um recurso, adicione um traço (-) à respectiva coluna ou deixe-a em branco.

NOTA: O Untag substitui o Tag - isso ocorre porque, ao contrário do Tag, o Untag precisa ser adicionado manualmente ao arquivo CSV, então presumimos que a intenção era remover, não modificar, a tag.

- Todas as colunas adicionais que não se encaixam nos critérios são ignoradas.

Important

A exportação do Tag Editor preenche uma matriz de todas as tags em relação a todos os recursos. As tags ausentes são preenchidas com o valor “não marcado”. A reutilização desse CSV de exportação como entrada para a RFC resulta na criação de todas as tags anteriormente ausentes, com valores literais de “não marcadas”.

 Note

Para obter informações sobre como exportar tags para um arquivo CSV, consulte [Encontrar recursos para marcar -> Exportar resultados para CSV](#).

Agendador de recursos do AWS Managed Services

Use o AWS Managed Services (AMS) Resource Scheduler para programar o início e a parada automáticos de AutoScaling grupos, EC2 instâncias da Amazon e instâncias do RDS em sua conta. Isso ajuda a reduzir os custos de infraestrutura quando os recursos não devem funcionar 24 horas por dia, 7 dias por semana. A solução foi criada com base no [Instance Scheduler on AWS](#), mas contém recursos adicionais e personalizações específicas para as necessidades do AMS.

 Note

Por padrão, o AMS Resource Scheduler não interage com recursos que não fazem parte de uma AWS CloudFormation pilha. O recurso deve fazer parte de uma pilha que começa com “stack-”, “sc-” ou “SC-”. Para agendar os recursos que não fazem parte de uma CloudFormation pilha, você pode atualizar o parâmetro da pilha do Resource Scheduler para `ScheduleNonStackResources Yes`

O Agendador de Recursos do AMS usa períodos e programações:

- Os períodos definem os horários em que o Resource Scheduler é executado, como horário de início, horário de término e dias do mês.
- As programações contêm seus períodos definidos, juntamente com configurações adicionais, como janela de manutenção do SSM, fuso horário, configuração de hibernação e assim por diante; e especificam quando os recursos devem ser executados, de acordo com as regras de período configuradas.

Você pode configurar esses períodos e cronogramas usando os tipos de alteração automatizada () CTs do AMS Resource Scheduler.

Para obter detalhes completos sobre as configurações disponíveis para o AMS Resource Scheduler, consulte a documentação correspondente do AWS Instance Scheduler em Componentes da [solução](#). Para uma visão arquitetônica da solução, consulte a documentação correspondente do AWS Instance Scheduler em [Architecture overview.html](#).

Implantando o Agendador de Recursos do AMS

Para implantar o AMS Resource Scheduler, use o tipo de alteração automática (CT): Deployment | AMS Resource Scheduler | Solution | Deploy (ct-0ywnhc8e5k9z5) para gerar uma RFC que, em seguida, implanta a solução em sua conta. Depois que a RFC é executada, uma CloudFormation pilha contendo recursos do AMS Resource Scheduler com configuração padrão é automaticamente provisionada em sua conta. Para obter mais informações sobre os tipos de alteração do Agendador de Recursos, consulte [Agendador de Recursos do AMS](#).

Note

Para descobrir se o AMS Resource Scheduler já está implantado em sua conta, verifique o console AWS Lambda dessa conta e procure a função Scheduler. AMSResource

Depois que o Agendador de Recursos do AMS for provisionado em sua conta, recomendamos que você revise a configuração padrão e, se necessário, personalize configurações como chave de tag, fuso horário, serviços agendados e assim por diante, com base em suas preferências. Para obter detalhes sobre as personalizações recomendadas [Personalizando o Agendador de Recursos do AMS](#), consulte a seguir.

Para fazer as configurações personalizadas ou apenas confirmar a configuração do Resource Scheduler,

Personalizando o Agendador de Recursos do AMS

Recomendamos que você personalize as seguintes propriedades do Agendador de Recursos do AMS usando a atualização dos tipos de alteração do Agendador de Recursos do AMS, consulte Agendador de [Recursos do AMS](#).

- Nome da tag: o nome da tag que o Resource Scheduler usará para associar agendamentos de instâncias a recursos. O valor padrão é Programação.

- **Serviços agendados:** uma lista de serviços separados por vírgulas que o Resource Scheduler pode gerenciar. O valor padrão é “ec2, rds, autoscaling”. Os valores válidos são “ec2”, “rds” e “autoscaling”
- **Fuso horário padrão:** especifique o fuso horário padrão para o Agendador de Recursos usar. O valor padrão é UTC.
- **Use a CMK:** uma lista separada por vírgulas da Chave Gerenciada pelo Cliente (CMK) do Amazon KMS para a ARNs qual o Resource Scheduler pode receber permissões.
- **Uso LicenseManager:** Uma lista separada por vírgulas do Gerenciador de AWS Licenças ARNs para esse Agendador de Recursos pode receber permissões.

Note

O AMS pode, de tempos em tempos, lançar recursos e correções para manter o AMS Resource Scheduler atualizado em sua conta. Quando isso acontece, qualquer personalização feita no Agendador de Recursos do AMS é preservada.

Usando o Agendador de Recursos do AMS

Para configurar o Agendador de Recursos do AMS após a implantação da solução, use o Agendador de Recursos automatizado CTs para criar, excluir, atualizar e descrever (obter detalhes sobre) os períodos do Agendador de Recursos do AMS (os horários em que o Agendador de Recursos é executado) e programações (os períodos configurados e outras opções). Para obter um exemplo do uso dos tipos de alteração do Agendador de Recursos do AMS, consulte [Agendador de Recursos do AMS](#).

Para selecionar recursos a serem gerenciados pelo AMS Resource Scheduler, após a implantação e a criação do cronograma, você usa o AMS Tag Create CTs para marcar grupos de Auto Scaling, pilhas do Amazon RDS e recursos EC2 da Amazon com a chave de tag que você forneceu durante a implantação, e o cronograma definido como o valor da tag. Depois que os recursos são marcados, os recursos são programados para início ou término de acordo com sua programação definida do Agendador de Recursos.

Não há custo adicional para usar o AMS Resource Scheduler. No entanto, a solução usa vários Serviços da AWS e você é cobrado por esses recursos à medida que eles são usados. Para obter mais detalhes, consulte [Visão geral da arquitetura](#).

Para optar por não participar do AMS Resource Scheduler:

- Para cancelamento ou desativação temporária: envie um RFC usando o Gerenciamento automatizado | Agendador de Recursos do AMS | Estado | Desativar o tipo de alteração (ct-14v49adibs4db)
- Para remoção permanente: Envie um RFC de gerenciamento | Outro | Outro | Atualização (revisão necessária) (ct-0xdawir96cy7k) solicitando a remoção do sistema de automação de lançamentos do Resource Scheduler

Estimador de custos do AMS Resource Scheduler

Para monitorar a economia de custos, o AMS Resource Scheduler apresenta um componente que calcula de hora em hora a economia estimada de custos dos recursos da Amazon EC2 e do RDS que são gerenciados pelo programador. Esses dados de economia de custos são então publicados como uma CloudWatch métrica (AMS/ResourceScheduler) para ajudá-lo a rastreá-los. O estimador de economia de custos estima apenas as economias nas horas de operação da instância. Ele não contabiliza nenhum outro custo, como os custos de transferência de dados associados a um recurso.

O estimador de economia de custos é ativado com o Resource Scheduler. Ele é executado de hora em hora e recupera dados de custo e uso de AWS Cost Explorer. A partir desses dados, ele calcula o custo médio por hora para cada tipo de instância e, em seguida, projeta o custo por um dia inteiro se estivesse sendo executado sem ser programado. A economia de custos é a diferença entre o custo projetado e o custo real reportado pelo Cost Explorer para um determinado dia.

Por exemplo, se a instância A estiver configurada com o Resource Scheduler para ser executada das 9h às 17h, são oito horas em um determinado dia. O Cost Explorer relata o custo como \$1 e o uso como 8. O custo médio por hora é, portanto, de \$0,125. Se a instância não fosse agendada com o Resource Scheduler, a instância seria executada 24 horas nesse dia. Nesse caso, o custo teria sido $24 \times 0,125 = \$3$. O Resource Scheduler ajudou você a obter uma economia de custos de \$2.

Para que o estimador de economia de custos recupere o custo e o uso somente dos recursos gerenciados pelo Resource Scheduler a partir do Cost Explorer, a chave de tag que o Resource Scheduler usa para direcionar recursos precisa ser ativada como a tag de alocação de custos no Painel de cobrança. Se a conta pertencer a uma organização, a chave da tag precisará ser ativada na conta de gerenciamento da organização. Para obter informações sobre como fazer isso, consulte [Ativando tags de alocação de custos definidas pelo usuário e tags de alocação pelo usuário](#) de custos definidas pelo usuário

Depois que a chave de tag é ativada como etiqueta de alocação de custos, o AWS faturamento começa a rastrear o custo e o uso dos recursos gerenciados pelo Resource Scheduler e, depois que os dados são disponibilizados, o estimador de economia de custos começa a calcular a economia e publicar os dados no namespace métrico em `AMS/ResourceScheduler` CloudWatch.

Dicas para estimadores de custos

O Cost Savings Estimator não aceita descontos como instâncias reservadas, planos de economia etc. em consideração em seu cálculo. O Estimator pega os custos de uso do Cost Explorer e calcula o custo médio por hora dos recursos. Para obter mais detalhes, consulte [Entendendo seus conjuntos de dados de AWS custo: uma folha de dicas](#).

Para que o estimador de economia de custos recupere o custo e o uso somente dos recursos gerenciados pelo Resource Scheduler a partir do Cost Explorer, a chave de tag que o Resource Scheduler usa para direcionar recursos precisa ser ativada como a tag de alocação de custos no painel de faturamento. Se a conta pertencer a uma organização, a chave da tag precisará ser ativada na conta de gerenciamento da organização. Para obter informações sobre como fazer isso, consulte Tags de [alocação de custos definidas pelo usuário](#). Se a etiqueta de alocação de custos não for ativada, o estimador não poderá calcular a economia e publicar a métrica, mesmo que ela esteja ativada.

Melhores práticas do AMS Resource Scheduler

Programação de instâncias da Amazon EC2

- O comportamento de desligamento da instância deve ser definido como `stop` e não `comotermiante`. Isso é predefinido `stop` para instâncias criadas com o tipo de alteração automática AMS Amazon EC2 Create (`ct-14027q0sjyt1h`) e pode ser definido para instâncias da EC2 Amazon criadas com ingestão, definindo a propriedade como `AWS CloudFormation InstanceInitiatedShutdownBehavior stop`. Se as instâncias tiverem o comportamento de encerramento definido como `comotermiante`, elas terminarão quando o Agendador de Recursos as interromper e o agendador não conseguirá reiniciá-las.
- EC2 As instâncias da Amazon que fazem parte de um grupo de Auto Scaling não são processadas individualmente pelo AMS Resource Scheduler, mesmo que estejam marcadas.
- Se o volume raiz da instância de destino for criptografado com uma chave mestra de cliente (CMK) do KMS, uma `kms:CreateGrant` permissão adicional precisará ser adicionada à sua função do IAM do Resource Scheduler para que o agendador possa iniciar essas instâncias. Essa permissão não é adicionada à função por padrão para melhorar a segurança. Se você

precisar dessa permissão, envie uma RFC com o tipo de alteração Management | AMS Resource Scheduler | Solution | Update e especifique uma lista separada por vírgulas ARNs do KMS. CMKs

Agendamento de grupos de Auto Scaling

- O AMS Resource Scheduler inicia ou interrompe o escalonamento automático de grupos de Auto Scaling, não de instâncias individuais no grupo. Ou seja, o programador restaura o tamanho do grupo Auto Scaling (início) ou define o tamanho como 0 (parada).
- AutoScaling Grupo de tags com a tag especificada e não com as instâncias dentro do grupo.
- Durante a parada, o AMS Resource Scheduler armazena os valores de capacidade mínima, desejada e máxima do grupo Auto Scaling e define a capacidade mínima e desejada como 0. Durante o início, o programador restaura o tamanho do grupo do Auto Scaling como estava durante a parada. Portanto, as instâncias do grupo Auto Scaling devem usar uma configuração de capacidade apropriada para que o encerramento e a reinicialização das instâncias não afetem nenhum aplicativo executado no grupo do Auto Scaling.
- Se o grupo do Auto Scaling for modificado (a capacidade mínima ou máxima) durante um período de execução, o programador armazenará o novo tamanho do grupo do Auto Scaling e o usará ao restaurar o grupo no final de um cronograma de parada.

Programação de instâncias do Amazon RDS

- O agendador pode tirar um snapshot antes de interromper as instâncias do RDS (não se aplica ao cluster de banco de dados Aurora). Esse recurso é ativado por padrão com o parâmetro de CloudFormation modelo Create RDS Instance Snapshot definido como verdadeiro. O snapshot é mantido até a próxima vez em que a instância do Amazon RDS for interrompida e um novo snapshot for criado.

O Scheduler pode usar instâncias do start/stop Amazon RDS que fazem parte de um cluster ou banco de dados Aurora do Amazon RDS ou em uma configuração de várias zonas de disponibilidade (Multi-AZ). No entanto, verifique a limitação do Amazon RDS quando o programador não conseguir interromper a instância do Amazon RDS, especialmente as instâncias Multi-AZ. Para programar o Aurora Cluster para iniciar ou parar, use o parâmetro do modelo Schedule Aurora Clusters (o padrão é true). O cluster Aurora (não as instâncias individuais dentro do cluster) deve ser marcado com a chave de tag definida durante a configuração inicial e o nome da programação como o valor da tag para programar esse cluster.

Cada instância do Amazon RDS tem uma janela de manutenção semanal durante a qual todas as alterações do sistema são aplicadas. Durante a janela de manutenção, o Amazon RDS iniciará automaticamente instâncias que foram interrompidas por mais de sete dias para aplicar a manutenção. Observe que o Amazon RDS não interromperá a instância após a conclusão do evento de manutenção.

O programador permite especificar se deseja adicionar a janela de manutenção preferencial de uma instância do Amazon RDS como um período de execução à sua programação. A solução iniciará a instância no início da janela de manutenção e interromperá a instância no final da janela de manutenção se nenhum outro período de execução especificar que a instância deve ser executada e se o evento de manutenção for concluído.

Se o evento de manutenção não for concluído até o final da janela de manutenção, a instância será executada até o intervalo de agendamento após a conclusão do evento de manutenção.

Note

O Agendador não valida se um recurso foi iniciado ou interrompido. Ele faz a chamada da API e segue em frente. Se a chamada da API falhar, ela registrará o erro para investigação.

AWS Systems Manager no AMS Advanced

Um AWS Systems Manager documento (documento SSM) define as ações que o Systems Manager executa em seus AWS recursos. O Systems Manager inclui mais de uma dúzia de documentos pré-configurados que você pode usar especificando parâmetros em tempo de execução. Os documentos usam notação de JavaScript objeto (JSON) ou YAML e incluem etapas e parâmetros que você especifica.

O AWS Managed Services (AMS) é um editor confiável para documentos SSM. Os documentos SSM de propriedade do AMS são compartilhados somente com contas AMS integradas, sempre começam com um prefixo reservado (AWSManagedServices-*) e aparecem no console do Systems Manager, como propriedade de. AWS O processo do AMS para desenvolvimento e publicação de documentos SSM segue as AWS melhores práticas e exige várias revisões por pares durante todo o ciclo de vida do documento. Para obter mais informações sobre as AWS melhores práticas para compartilhar documentos SSM, consulte [Melhores práticas para documentos SSM compartilhados](#).

Documentos SSM do AMS Advanced disponíveis

Os documentos SSM do AMS Advanced estão disponíveis exclusivamente para clientes do AMS Advanced e são usados para automatizar o fluxo de trabalho operacional para operar sua conta.

Para ver os documentos do AMS Advanced SSM disponíveis no Console de gerenciamento da AWS:

1. [Abra o console do Systems Manager no AWS Systems Manager console.](#)
2. Escolha Compartilhado comigo.
3. Na barra de pesquisa, filtre pelo prefixo do nome do documento, depois Igual e defina o valor como Serviços-. AWSManaged

Para obter instruções de AWS CLI, consulte Como [usar documentos SSM compartilhados](#).

Versões do documento AMS Advanced SSM

Os documentos SSM oferecem suporte ao controle de versão. Os documentos SSM do AMS Advanced não podem ser modificados na conta do cliente e não podem ser compartilhados novamente. Eles são gerenciados e mantidos centralmente pelo AMS Advanced para operar a conta.

Os números de versão são incrementados com cada atualização de documento em um documento específico Região da AWS. À medida que novas regiões são disponibilizadas, o mesmo conteúdo de documento em duas regiões pode ter números de versão diferentes; isso é normal e não significa que o comportamento delas será diferente. Se você quiser comparar dois documentos SSM do AMS Advanced, recomendamos comparar seus hashes com a CLI AWS :

```
aws ssm describe-document \  
--name AWSManagedServices-DOCUMENTNAME \  
--output text --query "Document.Hash"
```

Dois documentos SSM são idênticos se seus hashes corresponderem.

Preços do Systems Manager no AMS

Não há custo associado ao acesso a documentos SSM do AMS Advanced. O custo do tempo de execução varia de acordo com o tipo de documento SSM, suas etapas e a duração do tempo de execução. Para obter mais informações, consulte os [AWS Systems Manager preços](#).

Contas AMS externas

O AMS oferece assistência de desembarque para contas de zona de pouso com uma única conta e contas de zonas de pouso com várias contas.

O AMS não compartilha nada AMIs de você durante a desativação para evitar impacto em nenhuma de suas dependências. Se quiser remover o AMS AMIs da sua conta, você pode usar a `cancel-image-launch-permission` API para ocultar informações específicas AMIs. Por exemplo, você pode usar o script abaixo para ocultar todos os AMS AMIs que foram compartilhados com sua conta anteriormente:

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

Você deve ter a AWS CLI v2 instalada para que o script seja executado sem erros. Para ver as etapas de instalação da AWS CLI, consulte [Instalando ou atualizando a versão mais recente da AWS CLI](#). Para obter detalhes sobre o `cancel-image-launch-permission` comando, consulte [cancel-image-launch-permission](#).

Note

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.

Tópicos

- [Externamente das contas de landing zone de conta única do AMS](#)
- [Extraia as contas multicontas da landing zone do AMS](#)

Externamente das contas de landing zone de conta única do AMS

O AMS oferece assistência de desembarque dentro de 30 dias antes do término do AMS.

Você deve solicitar assistência de desembarque pelo menos 7 dias antes que essa assistência possa ser fornecida. A assistência de desembarque pode ser oferecida de duas formas:

- Transferência de controle: o AMS transfere o controle da conta de volta para você junto com as credenciais de acesso para todos os aplicativos gerenciados pelo AMS, ou
- Encerramento de recursos para encerramento da conta: o AMS exclui todos os dados em seu ambiente gerenciado pelo AMS e desprovisiona quaisquer recursos ativos na conta. Ao enviar a solicitação de desembarque, os clientes podem solicitar que o AMS:
 - Exclua ou retenha os objetos de dados (incluindo registros) que estão armazenados nos buckets do Amazon S3
 - Remova ou retenha os buckets do Amazon S3
 - Remover ou reter pontos de AWS Backup restauração

Important

Quaisquer outras solicitações específicas (sujeitas à plausibilidade) devem ser comunicadas à AMS antes da inicialização da saída.

Pré-requisitos opcionais (se necessário):

Note

Antes da solicitação de desembarque, os clientes podem solicitar assistência do AMS para transferir seus dados no formato existente usando AWS Snowball Edge ou qualquer outra mídia com a qual tenha AWS interface.

Além dos backups de dados, os seguintes dados do cliente podem ser fornecidos como parte da assistência de desembarque:

- Dados armazenados em serviços de armazenamento, incluindo registros
- Esquemas de tipo de alteração específicos do cliente
- CloudFormation modelos para esquemas de tipo de alteração

Se as atividades de desembarque não forem concluídas após o encerramento do AMS, entregamos os controles da (s) conta (s) para permitir que você conclua qualquer atividade pendente.

Função	O que foi removido	Impacto	Ações necessárias
Monitoramento, registro em log, alertas	Monitoramento AMS removido MMS (Sistema de Monitoramento Gerenciado) não inscrito O marcador de recursos e o gerenciador de alarmes foram removidos Os CloudWatch alertas básicos permanecem nos recursos existentes GuardDuty e Macie: A propriedade reverte para você	O AMS não tem mais acesso ou visibilidade de seus recursos e ambiente.	As contingências para serviços removidos e não assinados são de sua propriedade.
Gerenciamento de backups	A automação do AMS Backup foi removida, embora o AWS Backup serviço permaneça disponível para uso. Os cofres e dados de backup são retidos, a menos que a exclusão seja solicitada.	O AMS não monitora mais as tarefas de backup nem executa ações de restauração durante incidentes. Os alarmes e alertas estão desativados. A exclusão da função de backup do IAM e das chaves do KMS	Os planos de backup do AMS devem ser reconfigurados. Toda a propriedade de monitoramento e remediação retorna para você.

Função	O que foi removido	Impacto	Ações necessárias
		torna seus backups do AMS inoperáveis.	
Automações AMS para gerenciamento de serviços	Os runbooks de automação de AWS SSM organizados pela AMS, as funções Amazon Simple Notification Service (SNS) e Lambda não estão mais disponíveis. AWS	Sem acesso AMS às suas contas. Toda a automação está desativada.	Toda a automação, incluindo funções SSM, SNS e Lambda, precisa ser recriada, se necessário.
Compliance	A visibilidade e o monitoramento do AMS para todos GuardDuty e AWS Config as regras foram removidas, embora essas regras permaneçam nas contas.	Todo monitoramento, emissão de relatórios e correções da Amazon GuardDuty and AWS Config Rules não são mais gerenciados pelo AMS.	Monitoramento e remediação de todas as ferramentas de segurança e conformidade a serem assumidas por você.
Agentes na instância	O acesso ao Agendador de Recursos, ao Marcador de Recursos ou à configuração automática de instâncias para instalar os agentes necessários em suas EC2 instâncias é removido.	CloudWatch e os agentes SSM nas instâncias permanecem em vigor com as configurações existentes, no entanto, o AMS não ajuda mais com essas configurações.	Você gerencia a marcação e as configurações do agente SSM CloudWatch e na instância.

Função	O que foi removido	Impacto	Ações necessárias
Infraestrutura de patches e relatórios	O AMS não gerencia mais as atividades de pré e pós-aplicação de patches, e o acesso e a visibilidade a esses serviços são removidos.	O AMS não cria mais um instantâneo da instância antes da aplicação do patch, não instala e monitora mais a instalação do patch e não notifica mais você sobre o resultado. Relatórios e buckets de “auditoria” do S3 são deixados em suas contas conforme sua solicitação. O AMS não gera mais relatórios de métricas de serviço.	Você mantém as linhas de base e os instantâneos do Patch criados no passado. Além disso, a configuração das janelas de manutenção de patches permanece, mas os patches não são mais instalados ou corrigidos pelo AMS. Todos os relatórios sobre métricas operacionais de infraestrutura agora são de sua responsabilidade.
Gerenciamento de processos	Todas as contas são removidas do gerenciamento de serviços fornecido para incidentes, incluindo solicitações de serviço, gerenciamento de problemas e mudanças.	Todas as interrupções de serviço anteriormente corrigidas pelo AMS por meio de incidentes e solicitações de serviço e mudanças no ambiente, bem como investigações de causa raiz, são gerenciadas por mais tempo pelo AMS.	Você recupera a propriedade total de todo o gerenciamento de processos.

Extraia as contas multicontas da landing zone do AMS

Há dois tipos de AWS contas que você pode excluir da landing zone multiconta do AMS Advanced:

- Contas de aplicativos
- Contas principais

Para desativar todas as contas da sua landing zone multiconta do AMS, você deve desativar todas as contas do Aplicativo antes de desativar as contas principais.

Para assumir e continuar operando cargas de trabalho em contas externas de aplicativos ou contas principais, certifique-se de revisar esta documentação com sua equipe de contas do AMS. Esta documentação descreve as mudanças que o AMS realiza durante o processo externo.

Tarefas a serem concluídas para operação contínua de contas externas

As tarefas a seguir são necessárias para a operação contínua das contas que você retirou da landing zone de várias contas do AMS:

- Ative o modo Desenvolvedor: para obter mais permissões para suas contas, ative o modo Desenvolvedor antes de desvincular as contas de aplicativos do AMS. Ao ativar o modo Desenvolvedor, você pode fazer as alterações necessárias com mais facilidade para se preparar para a desativação. Não tente remover ou modificar os recursos da infraestrutura do AMS. Se você excluir recursos de infraestrutura do AMS, talvez o AMS não consiga desvincular sua conta com sucesso. Para obter informações sobre como ativar o modo Desenvolvedor, consulte [Introdução ao modo AMS Advanced Developer](#).

Se você não conseguir concluir as alterações necessárias para se preparar para a desativação depois de ativar o modo Desenvolvedor, entre em contato com a equipe da sua conta do AMS para discutir seus requisitos.

- Escolha um método alternativo para acesso à EC2 pilha: depois de retirar as contas de aplicativos do AMS, você não poderá usar RFCs para acessar os recursos da pilha. [Mudanças de desembarque](#) Revise e escolha um método de acesso alternativo para manter o acesso às suas pilhas. Para obter mais informações, consulte [Alternativas de acesso](#).

Contas externas do aplicativo AMS

Para remover contas de aplicativos do seu ambiente de landing zone com várias contas, conclua as seguintes etapas para cada conta:

1. Verifique se não há nenhuma abertura RFCs na conta. Para obter mais informações, consulte [Crie, clone, atualize, encontre e cancele RFCs](#).
2. Verifique se você pode acessar o endereço de e-mail do usuário principal ou raiz da conta.
3. Na conta do aplicativo, envie um RFC com a conta do [aplicativo | Confirme o tipo de alteração de desligamento \(ct-2wlfo2jxj2rkj\)](#). No RFC, especifique a conta do aplicativo a ser desativada.
4. Na conta de gerenciamento, envie um RFC com o tipo de alteração Conta de [gerenciamento | Conta de aplicativo externo \(ct-0vdiy51oyrhbm\)](#). No RFC, especifique a conta do aplicativo a ser desativada. Além disso, indique se você deseja excluir ou reter o anexo do Transit Gateway na landing zone.
5. Para garantir que o faturamento do AMS seja interrompido, notifique seu CSDM de que você desembarcou a conta.

O seguinte ocorre após a desativação da conta do aplicativo:

- Todos os componentes são desassociados dos serviços do AMS, mas seus recursos criados permanecem na conta. Você pode optar por manter ou fechar a conta externa do AMS.
- As contas principais e outras contas de aplicativo restantes funcionam normalmente após a desativação de uma conta de aplicativo.
- O faturamento do AMS é interrompido, mas o AWS faturamento não é interrompido até que você feche a conta. Para obter mais informações, consulte [O que você precisa saber antes de fechar sua conta](#).
- Se uma conta for fechada, ela ficará visível em sua organização no suspended estado por 90 dias. Depois de 90 dias, a conta fechada é removida permanentemente e não é mais visível em sua organização.
- Depois que a conta for encerrada, você ainda poderá entrar e registrar um caso de suporte ou contato Suporte por 90 dias.
- Após 90 dias, qualquer conteúdo que permaneça na conta será excluído permanentemente e os AWS serviços restantes serão encerrados.

Perguntas frequentes sobre a desativação da conta do aplicativo

P: Posso usar minhas funções federadas do IAM para continuar acessando uma conta de aplicativo que eu removi da minha landing zone multiconta do AMS?

Sim. As [funções padrão criadas pelo AMS AWS Identity and Access Management \(IAM\)](#) permanecem disponíveis na conta após a desativação do AMS. No entanto, essas funções e políticas foram projetadas para uso com o gerenciamento de acesso do AMS. Para fornecer o acesso necessário aos seus usuários, talvez seja necessário implantar seus próprios recursos do IAM.

P: Como faço para obter acesso total a uma conta do aplicativo que eu removi da minha landing zone com várias contas do AMS?

As contas de aplicativos externos são movidas para a Unidade Organizacional (OU) obsoleta na estrutura da conta. AWS Organizations Essa mudança elimina as restrições de acesso ao SCP que anteriormente bloqueavam o acesso do usuário root. Para obter informações sobre como redefinir as credenciais do usuário raiz, consulte [Redefinir uma senha de usuário raiz perdida ou esquecida](#).

P: Quais alterações são feitas durante a desativação da conta do aplicativo?

Para obter informações sobre as ações que o AMS executa quando o serviço exclui contas, consulte [Mudanças de desembarque](#).

P: Posso desativar uma conta de aplicativo sem desconectá-la do gateway de trânsito?

Sim. Use o tipo de alteração [Conta de gerenciamento | Conta de aplicativo externo](#) (ct-0vdiy51oyrhbm) para enviar a RFC e especifique o parâmetro como. DeleteTransitGatewayAttachment False

P: Quanto tempo é necessário para desativar uma conta do aplicativo?

Ao usar o tipo [de alteração da Conta de gerenciamento | Conta de aplicativo externo](#) (ct-0vdiy51oyrhbm), conclua em 1 hora. RFCs

P: É obrigatório que eu feche a conta externa?

Não. O encerramento da conta após a desativação do AMS não é obrigatório. Durante o processo de desligamento, o AMS remove o acesso e o gerenciamento de sua AWS conta, mas sua conta e seus recursos dentro da conta permanecem. É importante observar que, após a desativação do AMS, você é o único responsável por gerenciar e manter sua AWS conta e seus recursos.

O AMS não é responsável por quaisquer problemas, incidentes ou interrupções no serviço que possam ocorrer em sua conta após a conclusão do processo de desligamento. Para obter mais informações, consulte [Como faço para fechar minha AWS conta?](#) .

P: Se eu enviar uma solicitação de encerramento de conta, todos os recursos existentes serão excluídos imediatamente?

Não. O encerramento da conta não encerra seus recursos. Os recursos na conta são encerrados automaticamente 90 dias após a solicitação de encerramento. O faturamento do AMS é interrompido, mas o faturamento por AWS recursos não para até você fechar a conta. Para obter mais informações, consulte [O que você precisa saber antes de fechar sua conta.](#)

P: Posso agendar a desativação de uma conta do aplicativo?

Sim. Você pode RFCs programar o para ser executado em um horário específico. No entanto, a [conta do aplicativo | Confirmar desativação da](#) RFC deve ser concluída antes que você possa agendar a [conta de gerenciamento | RFC da conta de aplicativo externa](#). Para obter mais informações, consulte [Programação de RFC](#).

Desativação da conta do aplicativo RACI

- R: Parte responsável. A parte responsável por concluir a tarefa listada.
- R: Parte responsável. A parte que aprova a tarefa concluída.
- C: Parte consultada. Uma parte cujas opiniões são solicitadas, normalmente como especialistas no assunto, e com quem há comunicação bilateral.
- I: Parte informada. Uma parte que é informada sobre o progresso, geralmente somente após a conclusão da tarefa ou do resultado final.

Atividades	Cliente	AWS Managed Services (AMS)
Pré-requisitos		
Verifique o acesso ao endereço de e-mail raiz para cada ID de AWS conta que será removida	R	C

Atividades	Cliente	AWS Managed Services (AMS)
Analise a documentação do AMS sobre as ações recomendadas do cliente e prepare as contas para a desativação do AMS	R	C
Se necessário, envie um RFC para ativar o modo Desenvolvedor para preparar contas para desativação do AMS	R	eu
Se necessário, escolha um método alternativo para acesso à EC2 pilha.	R	eu
Desembarque		
Enviar RFCs para confirmar e solicitar a exclusão das contas do Aplicativo	R	eu
Remova os componentes do AMS das contas de aplicativos	eu	R
Notifique o AMS CSDM sobre contas removidas para interromper o faturamento do AMS	R	eu
Pós-desembarque		
Redefina a senha da conta de usuário raiz e verifique o acesso root em contas externas	R	C
Feche a conta ou siga as orientações do AMS sobre as ações recomendadas do cliente na documentação de desligamento do AMS para continuar operando as contas.	R	C

Contas principais externas

Para desativar contas principais do landing zone com várias contas, conclua as seguintes etapas:

1. Verifique se todas as contas do aplicativo na landing zone foram removidas do AMS.
2. Verifique se você não tem contas abertas RFCs . Para obter mais informações, consulte [Crie, clone, atualize, encontre e cancele RFCs](#).

3. Verifique se você pode acessar o endereço de e-mail do usuário principal ou raiz de todas as contas principais. Para obter mais informações, consulte [Contas de várias contas da Landing Zone](#).
4. Verifique se você pode acessar o número de telefone do usuário principal ou raiz da conta de gerenciamento. Use a função `AWSTrustedArns` do IAM para atualizar o número de telefone. Para obter mais informações, consulte [Como faço para atualizar meu número de telefone associado à minha AWS conta?](#).
5. Faça login na sua conta de gerenciamento da zona de pouso do AMS e envie uma solicitação de serviço do AMS. Na solicitação de serviço, especifique desembarcar toda a sua landing zone.

O seguinte ocorre após a desativação das contas principais:

- Todos os componentes estão desassociados dos serviços do AMS, mas alguns AWS recursos permanecem na conta. Você pode optar por manter ou fechar as contas principais externas do AMS.
- O faturamento do AMS é interrompido, mas o AWS faturamento não é interrompido até que você feche a conta. Para obter mais informações, consulte [O que você precisa saber antes de fechar sua conta](#).
- Se uma conta for fechada, ela ficará visível em sua organização no suspended estado por 90 dias. Após 90 dias, a conta fechada do membro será removida permanentemente e não estará mais visível em sua organização.
- Depois que a conta for encerrada, você ainda poderá entrar e registrar um caso de suporte ou contato Suporte por 90 dias.
- Depois que a conta for fechada por 90 dias, qualquer conteúdo que permaneça na conta será excluído permanentemente e os AWS serviços restantes serão encerrados.

Perguntas frequentes sobre a desativação da conta principal

P: Posso usar minhas funções federadas do IAM para continuar acessando as contas principais externas?

Sim. As [funções padrão criadas pelo AMS AWS Identity and Access Management \(IAM\)](#) permanecem disponíveis na conta externa. No entanto, essas funções e políticas foram projetadas para uso com o gerenciamento de acesso do AMS. Para fornecer o acesso necessário aos seus usuários, talvez seja necessário implantar seus próprios recursos do IAM.

P: Como faço para obter acesso total à conta MALZ de gerenciamento, serviços compartilhados, rede ou outra [conta MALZ](#) que não seja do aplicativo após sair da landing zone de várias contas do AMS?

Após a desativação, siga as instruções em [Redefinir uma senha de usuário raiz perdida ou esquecida](#) para usar as credenciais do usuário principal (raiz) para acessar contas principais que não sejam a conta de gerenciamento. Ao contrário de outros tipos de conta, a conta de gerenciamento mantém um dispositivo de autenticação multifator (MFA) inacessível que está associado ao usuário raiz para evitar o uso. Para recuperar o acesso root, você deve seguir o processo de recuperação do [dispositivo de MFA perdido](#).

P: Quais mudanças são feitas durante a desativação da conta principal?

Para obter informações sobre as ações que o AMS executa quando o serviço exclui contas, consulte [Mudanças de desembarque](#).

P: Quanto tempo leva para ser concluída a desativação da conta principal?

O processo de desativação da conta principal normalmente leva até 30 dias para ser concluído. No entanto, para garantir que todas as etapas necessárias sejam concluídas corretamente, você deve iniciar a solicitação de desligamento pelo menos 7 dias antes do início do desligamento. Para facilitar uma transição fácil, planeje com antecedência e envie sua solicitação de saída com antecedência.

P: Como faço para gerenciar componentes compartilhados após a desativação do AMS?

O AMS Managed Active Directory e outros componentes de infraestrutura de serviços compartilhados foram projetados para acesso do operador do AMS. Talvez seja necessário atualizar os grupos de segurança, a política de controle de AWS Organizations serviços (SCP EC2) da Amazon Elastic Compute Cloud (Amazon) ou fazer outras alterações para manter o acesso total a esses componentes.

P: Posso fechar contas principais externas?

Por padrão, as contas de aplicativos têm várias dependências nas contas MALZ Core, como AWS Organizations associação, conectividade de rede de gateway de trânsito e resolução de DNS por meio do AMS Managed Active Directory. Depois de resolver essas dependências, você pode descomissionar e fechar a conta Core externa. Para obter mais informações, consulte [Contas de várias contas da Landing Zone](#).

Desativação da conta principal RACI

- R: Parte responsável. A parte responsável por concluir a tarefa listada.
- R: Parte responsável. A parte que aprova a tarefa concluída.
- C: Parte consultada. Uma parte cujas opiniões são solicitadas, normalmente como especialistas no assunto, e com quem há comunicação bilateral.
- I: Parte informada. Uma parte que é informada sobre o progresso, geralmente somente após a conclusão da tarefa ou do resultado final.

Atividades	Cliente	AWS Managed Services (AMS)
Pré-requisitos		
Verifique o acesso ao endereço de e-mail raiz para cada ID de conta da AWS que será removida	R	C
Verifique o acesso e atualize o número de telefone do usuário raiz da conta de gerenciamento	R	C
Análise a documentação do AMS sobre as ações recomendadas do cliente e prepare as contas para a desativação do AMS	R	C
Desembarque		
Envie uma solicitação de serviço para solicitar o desembarque da landing zone	R	eu
Componentes AMS externos das contas principais	eu	R
Pós-desembarque		
Redefina a senha da conta de usuário raiz e verifique o acesso root em contas externas	R	C

Atividades	Cliente	AWS Managed Services (AMS)
Feche as contas ou siga as orientações da AMS sobre as ações recomendadas do cliente na documentação de desligamento da AMS para continuar operando as contas.	R	C

Mudanças de desembarque

A tabela a seguir descreve as ações que o AMS toma para desembarcar na landing zone de várias contas, os impactos potenciais e as ações recomendadas.

Componen e	Account type (Tipo de conta)	Ações tomadas para desembarcar	Impactos potenciais	Ação recomendada pelo cliente
Gerenciarr ento de acesso	Contas de aplicativ os	Após a desativação, o acesso à pilha RFCs para just-in-time acesso com limite de tempo não pode mais ser enviado às EC2 pilhas de acesso por meio de hosts do AMS Bastion O AMS não gerencia mais componentes relacionados ao acesso em nenhuma pilha de EC2 recursos existente (agente aberto do PBIS, scripts de junção de domínio)	Não é possível usar o AMS Bastions por meio do RFS para acessar instâncias EC2 EC2 instâncias iniciadas a partir de dados que não sejam do AMS AMIs não estão associadas ao domínio gerenciado do Active Directory Se não forem removidos, os	Use métodos alternativos para acessar a EC2 instância (consulte Alternativas de acesso) Remova os scripts de inicialização do AMS das pilhas de EC2 recursos existentes (consulte Desativar scripts de EC2 inicialização do AMS)

Componen e	Account type (Tipo de conta)	Ações tomadas para desembarcar	Impactos potenciais	Ação recomendada pelo cliente
			scripts de inicializ ação do AMS nas pilhas de recursos existentes podem produzir erros devido à falta de dependências do AMS e impedir a adesão a um domínio diferente.	
Gerenciarr ento de acesso (continua ção)	Contas principai s	Se você migrou do PBIS Open para o PBIS Enterprise (AD Bridge), o AMS não renova mais o licenciamento após a desativação da conta principal	Se a licença do PBIS Enterpris e puder expirar, as credenciais do Active Directory não serão válidas para as pilhas de instâncias existentes baseadas em Linux EC2	Se você migrou para o PBIS Enterprise (AD Bridge), decida se deseja manter o licenciamento ou descomissionar (consulte) PBIS Open/Enterprise (Ponte AD)

Componen e	Account type (Tipo de conta)	Ações tomadas para desembarcar	Impactos potenciais	Ação recomendada pelo cliente
Registro, monitoramento e Incident/Event gerenciamento	Aplicativos e contas principais	Os componentes do AMS a Alertas do monitoramento de linha de base no AMS serem implantados são removidos Os CloudWatch alarmes existentes da Amazon implantados permanecem, mas não criam mais incidentes de AMS AWS Config as autorizações de agregação do AMS e da conta de segurança MALZ Core são removidas AWS Config as regras permanecem implantadas e a Amazon GuardDuty permanece habilitada, mas não cria mais incidentes de AMS	Recursos recém-criados não têm monitoramento de linha de base e alarmes do AMS aplicados Alarmes métricos de infraestrutura e eventos de segurança não geram mais incidentes de AMS AWS Config não está mais agregado em uma conta central	Defina, capture e analise métricas de operações para visualizar os eventos da carga de trabalho e tomar as medidas apropriadas. Implemente qualquer fluxo de trabalho de alerta necessário para continuar aplicando o monitoramento operacional e os alarmes necessários em novos recursos e para receber alertas de segurança da AWS Config Amazon GuardDuty.

Componen e	Account type (Tipo de conta)	Ações tomadas para desembarcar	Impactos potenciais	Ação recomendada pelo cliente
Gerenciarr ento de continuid ade (backup e restauraç ão)	Contas de aplicativ os	O AMS não monitora mais as tarefas de backup nem executa solicitações de backup e restauração Os cofres de backup padrão do AMS, a chave de criptografia de backup e a função de backup permanecem	Falhas na operação de backup podem não ser notadas	Monitore e revise as configurações do plano de backup

Componere	Account type (Tipo de conta)	Ações tomadas para desembarcar	Impactos potenciais	Ação recomendada pelo cliente
Gerenciamento de patches	Aplicativos e contas principais	O AMS não monitora mais as operações de aplicação de patches para uma execução bem-sucedida nem executa correções manuais O AMS não atualiza mais os componentes da infraestrutura do AMS As linhas de base do patch fornecidas pelo AMS são mantidas Os runbooks de automação de AWS Systems Manager patches fornecidos pelo AMS não são compartilhados e não estão mais disponíveis para uso	Falhas na operação de correção podem não ser notadas As configurações de patch existentes que dependem dos runbooks do Systems Manager Automation fornecidos pelo AMS devem ser reconfiguradas para continuar em ininterruptas.	Revise e reconfigure as configurações de patches conforme necessário

Componen e	Account type (Tipo de conta)	Ações tomadas para desembarcar	Impactos potenciais	Ação recomendada pelo cliente
Gerenciarr ento de rede	Contas de aplicativ os	Se especificado, o anexo do gateway de trânsito na conta externa do aplicativo será removido	A conta de aplicativ o externo não pode mais usar um gateway de trânsito para acessar serviços compartil hados, como o Active Directory gerenciado ou outras contas de aplicativos	Especifique DeleteTra nsitGatew ayAttachment como False manter a conectividade do gateway de trânsito

Componere	Account type (Tipo de conta)	Ações tomadas para desembarcar	Impactos potenciais	Ação recomendada pelo cliente
Gerenciamento de segurança	Contas de aplicativos	A conta é separada do console central do Trend Micro DSM. Além disso, os agentes de endpoint não encaminham mais alertas por meio do processo de incidentes do AMS Os agentes da Trend Micro permanecem instalados, mas não são mais gerenciados ou atualizados pelo AMS As personalizações de AMI fornecidas pela AMI que implantam o agente da Trend Micro não são mais mantidas ou atualizadas pelo AMS	EC2 detecções de malware em endpoints de instância podem não ser notadas O agente Trend micro não é implantado em EC2 instâncias que são iniciadas de forma não fornecida pelo AMS AMIs	Considere as opções para continuar ou descontinuar a Trend Micro (consulte Trend Micro Deep Security)

Componen e	Account type (Tipo de conta)	Ações tomadas para desembarcar	Impactos potenciais	Ação recomendada pelo cliente
Gerenciarr ento de segurança (continua ção)	Contas principai s	A infraestrutura do Trend Micro DSM é mantida nas contas de Serviços Compartilhados, mas não é mais mantida ou atualizada pelo AMS O Trend Micro DSM não encaminha mais alertas por meio do processo de incidentes do AMS	EC2 detecções de malware em endpoints de instância podem passar despercebidas EC2 a proteção de endpoints da instância pode ser afetada se a infraestrutura não for mantida (atualizações de definições, licenciamento etc.)	Decida se deseja continuar ou descontinuar a Trend Micro (consulte Trend Micro Deep Security)
Gerenciarr ento de alteraçõe s	Aplicativ os e contas principai s	O console RFC e a API do AMS foram removidos As políticas de controle de serviço personalizadas do AMS (SCPs) que contêm restrições de acesso no nível da conta são desanexadas durante a desativação da conta do aplicativo e excluídas durante a desativação da conta principal	Você deve usar uma AWS API nativa para criar novos recursos, alterar recursos existente s ou atualizar CloudFormation pilhas existentes As restrições de acesso não são mais impostas no nível da conta por meio do AMS fornecido SCPs	Certifique-se de que as funções de usuário forneçam acesso suficiente para usar AWS os serviços Crie SCPs para fornecer restriçõe s de permissão em nível de conta

Componen e	Account type (Tipo de conta)	Ações tomadas para desembarcar	Impactos potenciais	Ação recomendada pelo cliente
Imagens e automaçõe s do AMS OS para gerenciam ento de serviços	Aplicativ os e contas principai s	O AMS não fornece mais suporte para personali zações e scripts de lançamento incluídos no AMS fornecido EC2 AMIs Os AMS fornecidos EC2 AMIs permanece m disponíveis em suas contas externas Os runbooks do Systems Manager Automation fornecidos pelo AMS não são compartilhados e não estão mais disponíveis para uso	Após a desativaç ão, o AMS forneceu o AMIs sinal de CloudFormation envio cfn FAILURE devido à falta de dependências nos componentes do AMS Os processos operacionais que dependem dos runbooks do Systems Manager Automation fornecidos pelo AMS podem falhar	Revise e atualize todos os processos operacionais ou de compilação que dependam do AMS fornecido AMIs ou dos runbooks do Systems Manager Automation
infraestr utura de serviços compartil hados	Contas principai s	O acesso ao AMS foi removido e o AMS não gerencia mais component es compartilhados, incluindo o AMS Managed Active Directory AWS Transit Gateway,, e AWS Organizations	Perda de gerenciam ento da infraestr utura compartilhada	Redefina o acesso do administrador ao AMS Managed Active Directory e assuma o gerenciam ento dos component es de serviços compartilhados

Componen e	Account type (Tipo de conta)	Ações tomadas para desembarcar	Impactos potenciais	Ação recomendada pelo cliente
Relatório s	Aplicativ os e contas principai s	O AMS não coleta mais detalhes da conta ou do nível do recurso para gerar relatórios agregados	Perda de informaçõ es sobre métricas operacionais e comerciais (cobertur a de backup e patches, gerenciam ento de mudanças e atividade de incidentes)	Substitua qualquer relatório de dados agregado necessário em todas as contas por sua própria solução
Equipe de contas e central de atendimen to do AMS	Aplicativ os e contas principai s	A equipe de contas do AMS (CSDM, CA) e a central de serviços de operações do AMS não oferecem mais suporte às contas externas	Perda de suporte operacional com experiência na arquitetura de landing zone de várias contas projetada pela AMS e componentes relacionados	Certifique-se de que haja pessoal sufficient e e familiaridade com a estrutura e os recursos da conta para apoiar as operações no ambiente

Alternativas de acesso

A seguir estão os métodos alternativos para manter o acesso à sua EC2 pilha depois de desativar as contas do AMS:

- Use o Gerenciador de Sessões para acessar EC2 instâncias com permissões elevadas sem exigir bastiões ou acesso à rede de entrada. Para obter mais informações, consulte [AWS Systems Manager Session Manager](#).

- Reunir EC2 instâncias a um domínio diferente do Active Directory com novas credenciais de domínio. Se você usa Directory Service, consulte [Unir uma EC2 instância ao seu AWS Managed Microsoft AD diretório](#).
- Use contas de usuário locais que você criou por meio de um dos outros métodos de acesso ou por meio do [AWS Systems Manager Run Command](#).

Desativar scripts de EC2 inicialização do AMS

Sistemas operacionais Linux

Use o gerenciador de pacotes da sua distribuição para desinstalar o `ams-modules` pacote. Por exemplo, para uso do Amazon Linux 2 `yum remove ams-modules`.

Sistemas operacionais do Windows

Para desativar os scripts de EC2 inicialização no Windows, conclua as seguintes etapas:

1. Windows Server 2008/2012/2012r2/2016/2019:

Desative ou remova a tarefa agendada do Managed Services Startup do Agendador de Tarefas. Para listar as tarefas agendadas, execute o `Get-ScheduledTask -TaskName '*Ec2*'` comando.

Windows Server 2022:

Remova a [tarefa EC2 Launch v2](#). Essa tarefa é executada `Initialize-AMSBoot` em `postReady` estágio em `C:\AmazonProgramData\EC2 Launch\config\agent-config.yml` na instância. Veja a seguir um trecho de um exemplo: `agent-config.yml`

```
{
  "task": "executeScript",
  "inputs": [
    {
      "frequency": "always",
      "type": "powershell",
      "runAs": "localSystem"
    }
  ]
}
```

2. (Opcional) Remova o seguinte conteúdo do arquivo:

```
C:\Program Files\WindowsPowerShell\Modules\AWSManagedServices.*  
C:\Windows\System32\WindowsPowerShell\v1.0\Modules  
\AWSManagedServices.Build.Utilities\*
```

PBIS Open/Enterprise (Ponte AD)

Para determinar se você usa a edição PBIS Open ou PBIS Enterprise (AD Bridge), execute o seguinte comando em uma instância EC2 gerenciada do Linux:

```
yum info | grep pbis
```

Veja a seguir um exemplo de saída que mostra o PBIS Enterprise (AD Bridge):

```
Name      : pbis-enterprise  
From repo : pbise  
Name      : pbis-enterprise-devel  
Repo      : pbise  
Description : The pbis-enterprise-devel package includes the development
```

PBIS Aberto

O PBIS Open é um produto obsoleto que BeyondTrust não oferece mais suporte. Para obter mais informações, consulte a documentação do [BeyondTrust pbis-open](#).

Ponte AD (PBIS Enterprise)

Você pode executar uma das seguintes ações:

- Renove o licenciamento e continue operando o AD Bridge. Entre em contato BeyondTrust para discutir o licenciamento e o suporte.
- Interrompa o uso do AD Bridge. Execute o comando Shell a seguir para remover o pacote PBIS-Enterprise das instâncias gerenciadas do Linux. Para obter mais informações, consulte a BeyondTrust documentação [Sair de um domínio e desinstalar o AD Bridge Agent](#).

```
$ sudo /opt/pbis/bin/uninstall.sh purge
```

Sair do domínio do Active Directory gerenciado pelo AMS sem remover o agente PBIS

Você tem a opção de deixar o Active Directory gerenciado pelo AMS sem remover o agente PBIS. Use uma das soluções a seguir, dependendo do seu sistema operacional:

Linux operating systems

Use o PBIS do AD gerenciado pelo AMS para executar o seguinte comando shell para desassociar-se de uma instância Linux. EC2 Para obter mais informações, consulte a documentação do [BeyondTrust pbis-open](#) ou do [BeyondTrust AD Bridge](#), dependendo da versão usada.

```
$ sudo /opt/pbis/bin/domainjoin-cli leave
```

Talvez você veja uma mensagem de erro semelhante à seguinte:

```
Error: LW_ERROR_KRB5_REALM_CANT_RESOLVE [code 0x0000a3e1]
Cannot resolve network address for KDC in requested realm
```

Se esse erro ocorrer, execute os seguintes comandos para excluir o registro do provedor AD e reiniciar lwsmd os serviços:

```
$ /opt/pbis/bin/regshell dir '[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin]'
```

Use a saída do ID do diretório que você recebeu do comando anterior (por exemplo, **A123EXAMPLE.AMAZONAWS.COM**) para executar os seguintes comandos:

```
$ /opt/pbis/bin/regshell delete_tree \
'[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin\DIRECTORYID]'

$ /etc/pbis/redhat/lwsmd restart

$ /opt/pbis/bin/lwsm restart lwreg
```

Windows operating systems

```
# Collect hostname and domain name using:
```

```
Test-ComputerSecureChannel -verbose

# Disjoin computer from the domain:

netdom remove hostname /domain:domain name /force
```

Note

Certifique-se de desativar ou remover a tarefa agendada do Managed Services Startup, conforme mencionado em [Desativar scripts de EC2 inicialização do AMS](#).

Trend Micro Deep Security

Use uma das seguintes opções para continuar ou interromper o uso do Trend Micro Deep Security:

Continuar o uso

- (Se desativar todo o MALZ) Após a desativação da conta Core, reconecte as contas externas do Aplicativo ao Trend Micro Deep Security Manager (DSM) existente e mantenha o licenciamento na conta de Serviços compartilhados. Para obter mais informações, consulte [Adicionar contas AWS na nuvem](#) e [Verificar as informações da sua licença](#).
 1. Faça login na conta de serviços compartilhados e navegue até o console do Secrets Manager.
 2. Recupere as credenciais de administrador do console DSM que estão armazenadas no caminho. `/ams/eps/`
 3. Faça login no console DSM em <https://dsm.sentinel.int>.
 4. Escolha Usar função entre contas e, em seguida, insira `arn:aws:iam::ACCOUNTID:role/mc_eps_cross_account_role`. Substitua ACCOUNTID pelo ID da conta do aplicativo externo.
 5. Escolha Próximo.
 6. Aguarde alguns minutos para que o DSM processe a descoberta da conta e mostre que a sincronização foi bem-sucedida.
- Reconecte contas externas do aplicativo a uma nova instalação do Trend Micro DSM. Para obter mais informações, consulte [Ativar e proteger agentes](#) e [Ativar o agente](#).
- Reconecte contas externas do aplicativo ao Trend Micro Cloud One. Para obter mais informações, consulte [Migrar do Deep Security para o Workload Security](#) e [Migrar de um](#) DSM local.

Interromper o uso

- Desinstale o Trend Micro Deep Security Agents das contas externas do aplicativo. Para obter mais informações, consulte [Desinstalar o Deep Security](#).

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 AMS](#) e 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 criação 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 gerenciam ento de eventos				el pelos serviços provision ados de autoatendimento (SSP)	el pelos recursos provision ados usando a função IAM de desenvolvedor fora do sistema AMS CM	
Gerenciam ento de continuidade	Responsabilidade do AMS de executar o plano de backup selecionado pelo cliente			Cliente responsável pelos serviços provision ados de autoatendimento (SSP)	Cliente responsável pelos recursos provision ados 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 padroniza do 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 rehostar 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 rehostar 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 [CreateRfc](#) seção 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-rtc` CLI ou usando o console AMS. Crie páginas RFC. Para obter um tutorial sobre como criar um RFC, consulte [Crie 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, consulte [Solução 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 [AssumeRoleWithWebIdentity](#) AWS 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 `AWSManagedServicesAdminRole` usada pelos administradores de segurança e `AWSManagedServicesChangeManagementRole` 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 `ActionState` muda 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 `ActionState` automaticamente `AwsActionPending` para indicar que um operador precisa revisar e aprovar a RFC.

- Quando um operador começa a revisar ativamente sua RFC, ela `ActionState` muda para `AwsOperatorAssigned`
- Quando o operador aprova sua RFC, o status da RFC muda para Programado e o muda `ActionState` automaticamente 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 `ActionState` automaticamente `AwsActionPending` para indicar que um operador precisa ser designado para a revisão da RFC.
- Quando um operador começa a executar ativamente o RFC, ele muda `ActionState` para `AwsOperatorAssigned`.
- Depois de concluído, o Operador fecha o RFC. Isso muda automaticamente o `ActionState` para `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 `ActionState` definido como `AwsActionPending`
- Quando um RFC é criado, o `ActionState` é automaticamente definido como `NoActionPending`
- Quando um RFC é enviado, o `ActionState` é automaticamente definido como `AwsActionPending`
- Quando uma RFC é rejeitada, cancelada ou concluída com o status de Êxito ou Falha, ela `ActionState` é 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 para `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 `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 normalmente 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-34sxf053yuzah) 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 \(ct-3king0u4l33zf\)](#)

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-3king0u4l33zf) 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 aRequestedStartTime, a RFC é considerada programada e RequestedEndTime é preenchida usando o ExecutionDurationInMinutes valor.
- apenas umRequestedEndTime, nós jogamos um InvalidArgumentException.
- ambos RequestedStartTime eRequestedEndTime, 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: [ApproveRfc](#) marca 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: [RejectRfc](#) marca 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 [UpdateRestrictedExecutionTimes](#) API 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 [ListRestrictedExecutionTimes](#) da 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 RestrictedExecutionTimesOverrideId com 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 \(recrutar\) 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 RFCs para 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-01tm873rsebx9 |
+-----+-----+-----+-----+
```

2. Encontre a versão mais atual do CT:

ChangeTypeIdChangeTypeVersion: 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-sdhopv000000000000",
  "Name":             "MyElbInstance",
  "TimeoutInMinutes": 60,
  "Parameters": {
    "ELBSubnetIds":      ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold": 4,
    "ELBHealthCheckInterval": 5,
    "ELBHealthCheckTarget": "HTTP:80/",
    "ELBHealthCheckTimeout": 60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":         false
  }
}
```

- Envie o modelo RFC JSON para um arquivo em sua pasta atual chamado `CreateElbRfc.json`:

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

- 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 `AwsOperatorAssigned`significar que um operador está examinando a RFC no momento, o que `AwsActionPending`significa que um operador de AMS deve realizar algo antes que a execução da RFC possa continuar ou `CustomerActionPending`que 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 [ListRfcSummaries](#) operação 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, “20170101T000000Z”)			no campo Valores. A condição Between deve ter exatamente 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, “20170101T000000Z”)	Antes, depois, entre	Nenhum	A condição Antes ou Depois aceita somente um valor no campo Valores. A condição Between deve ter exatamente dois valores no campo Valores, onde o primeiro valor deve representar uma data que ocorre antes do segundo valor
AutomationStatusId	Manual, automatizado	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, “20170101T000000Z”)	Antes, depois, entre	Nenhum	A condição Antes ou Depois aceita somente um valor no campo Valores. A condição Between deve ter exatamente 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, “20170101T000000Z”)	Antes, depois, entre	Nenhum	A condição Antes ou Depois aceita somente um valor no campo Valores. A condição Between deve ter exatamente 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, “20170101T000000Z”)	Antes, depois, entre	Nenhum	A condição Antes ou Depois aceita somente um valor no campo Valores. A condição Between deve ter exatamente 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, “20170101T000000Z”)	Antes, depois, entre	Nenhum	A condição Antes ou Depois aceita somente um valor no campo Valores. A condição Between deve ter exatamente 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, “20170101T000000Z”)	Antes, depois, entre	Nenhum	A condição Antes ou Depois aceita somente um valor no campo Valores. A condição Between deve ter exatamente 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 PendingApproval, 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 suportadas. 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-123h45t6uz7j1|
|Management| Monitoring & Notification |SQS   |Update |ct-123h45t6uz7j1|
+-----+-----+-----+-----+-----+-----+

```

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 `AdvancedFilters`, 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 RFCs de 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 (.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, `AwsApprovalId` e `CustomerApprovalId` que 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, consulte [Automatizado 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
<code>AwsApprovalId: Required</code>	O sistema de mudança de tipo do AMS,	Nenhuma ação é necessária. Essa condição é típica de automação CTs.
<code>AwsApprovalId: NotRequiredIfSubmitter</code>	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 application
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-sft6rv000000000000",
    "type": "string",
    "enum": ["stm-sft6rv000000000000"]
  },
  "Name": {
    "description": "A name for the stack or stack component
;
    this becomes the Stack Name.",
    "type": "string",
    "minLength": 1,
    "maxLength": 255
  },
  "Tags": {
    "description": "Up to seven tags (key/value pairs) to
categorize the resource.",
    "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 “propriedades adicionais” permitem que você saiba quais parâmetros 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, selecione um cartão e clique 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`, e `operation`, 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-abc123xyz7890)	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 sam1 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 sam1 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, consulte [Entenda 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 ao **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 (como Create/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 (consulte [Funções 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 Appld 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 <code>aws:TagsKey</code> 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 <code>aws:TagsKey</code> 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 `AWSTManagedServicesCloudFormationAdminRole`, 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 `AmsStackTransform` com sucesso, 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. 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 de 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 em [Pré-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 (AWSManagedServicesDevelopmentRolepara 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 (AWSManagedServicesDevelopmentRolepara 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 peloAWSManagedServicesDevelopmentRole.

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 CloudTrail 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: • <code>ds:AuthorizeApplication</code> • <code>ds:CreateAlias</code> • <code>ds:CreateIdentityPoolDirectory</code> • <code>ds>DeleteDirectory</code> • <code>ds:DescribeDirectories</code> • <code>ds:GetAuthorizedApplicationDetails</code> • <code>ds:ListAuthorizedApplications</code> • <code>ds:UnauthorizeApplication</code> 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: <code>DhcpOptions GatewaySubnet,VPC,, VPN</code> e. Não é possível acessar ou modificar EC2 recursos da Amazon que tenham uma tag prefixada com <code>AMS,, mcManagementHostASG , and/or sentinel</code>.

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 (<code>AWSManagedServicesDevelopmentRole</code> para MALZ, <code>customer_developer_role</code> 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:AWSManagedServicesDevelopmentRolePermissionsBoundary , SALZ:ams-app-infra-permissions-boundary) 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 comAMS.

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 éDecodeAuthorizationMessage .
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: • <code>lakeformation:DescribeResource</code> • <code>lakeformation:GetDataLakeSettings</code> • <code>lakeformation:DeregisterResource</code> • <code>lakeformation:RegisterResource</code> • <code>lakeformation:UpdateResource</code> • <code>lakeformation:PutDataLakeSettings</code>
Amazon Elastic Inference	Você só pode chamar a ação da API Elastic Inference. <code>elastic-inference:Connect</code> Essa permissão está incluída no <code>customer_sagemaker_admin_policy</code> que está anexado ao <code>customer_sagemaker_admin_role</code>. 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

Desenvolvedor `AWSManagedServicesDevelopmentRole`, 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 Lambda](#) qualquer 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_alex_console_role`. A também `customer_alex_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_alex_gateway_installer_user` e `customer_alex_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` 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 executam 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 autopvisionado | 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` e `customer_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. 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_role`, `customer_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 autopvisionada, 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 autopvisionada:
 - 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-3dpg8mdd9jn1r) 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 autopvisionado | 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 `SSPScustomer-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-36cn2avfrjrj9v) 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 seja `Customer_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 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 autopvisionada 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 precisa 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_role`, `customer_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, consulte [Use 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, consulte [Use 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, consulte [Use 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, consulte [Use 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_role` `customer_codedeploy_service_role`, CodeBuild, em sua conta CodeDeploy e CodePipeline serviços. Se forem necessárias permissões adicionais do IAM para o `customer_codebuild_service_role`, envie uma solicitação de serviço do AMS.

 Note

Você também pode adicionar esses serviços separadamente; para obter informações [Use o AMS SSP para provisionar AWS CodeBuild em sua conta AMS](#), consulte [Use o AMS SSP para provisionar AWS CodeDeploy em sua conta AMS](#), e [Use 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: GenerateDataKey` `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 autopvisionado | 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-0fpjlx808sh2` (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:Encrypt, kms:Decrypt, kms:ReEncrypt, kms:GenerateDataKey, kms:GenerateDataKeyWithoutPlaintext, 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. `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 fornecidacustomer_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_role` `customer_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 microserviços 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. O AWS Systems Manager 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 autopvisionado | 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
<code>aws: assertAwsResource</code> Propriedade —	Afirmar um estado AWS de recurso ou estado de evento	Somente EC2 instâncias

Ação	Descrição	Limitação
<code>aws:aws:branch</code> —	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
<code>aws:ExecuteScript</code> —	Executar um script	Único script que não faz nenhuma chamada de API para nenhum serviço
<code>aws:pause</code> —	Pausar uma automação	Sem limitação
AWS: RunCommand —	Executar um comando em uma instância gerenciada	Usando somente o documento fornecido pelo System Manager - AWS- RunShellScript e AWS- RunPowerShellScript
<code>aws:sleep</code> —	Atrasar uma automação	Sem limitação
<code>leis: waitForAws ResourceProperty</code> —	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`.

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/Export capabilities 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-117rmp64d5mvp`: 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 autopvisionados). 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 comunicam 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](#).

Encontrando os dados de que você precisa (SKMS), AMS

Encontrar os dados de que você precisa ao usar suas contas do AWS Managed Services (AMS) exige o sistema de gerenciamento de conhecimento do serviço AMS, ou SKMS. BRAÇOS.

SKMS significa sistema de gerenciamento de conhecimento de serviços e se refere a todas as informações relacionadas ao serviço AWS Managed Services (AMS) para um cliente. O AMS tem uma API SKMS para encontrar dados.

Tópicos

- [O que é gerenciamento de conhecimento de serviços?](#)
- [Encontrando a VPC no AMS IDs](#)
- [Encontrando sub-rede IDs no AMS](#)
- [Encontre AMI IDs, AMS](#)
- [Encontre o grupo de segurança \(SG\) IDs, AMS](#)
- [Encontre entidades do IAM no AMS](#)
- [Encontre uma pilha IDs no AMS](#)
- [Encontre endereços IP IDs ou de instância no AMS](#)
- [Encontre nomes de recursos da Amazon \(ARNs\) no AMS](#)
- [Encontre recursos por ARN no AMS](#)
- [Encontre as configurações da conta AMS](#)

O que é gerenciamento de conhecimento de serviços?

O gerenciamento do conhecimento do serviço é o armazenamento de todas as informações em sua conta do AMS. As informações a seguir são obtidas do sistema de gerenciamento de conhecimento de serviços (SKMS) do AMS, por meio da API AMS SKMS ou do console do AMS:

- VPCs
- Sub-redes gerenciadas
- Pilhas e componentes de pilha, incluindo EC2 instâncias da Amazon e outros recursos
- Imagens de máquinas da Amazon (AMIs)

Você pode usar as informações do SKMS para entender a infraestrutura sob gerenciamento e como entrada para o gerenciamento de mudanças e solicitações de serviço para criar, alterar ou remover a infraestrutura.

 Note

Todas as chamadas da API AMS SKMS são gravadas em AWS CloudTrail.

Acesse o SKMS por meio da API AMS SKMS, que fornece operações para descobrir informações sobre um ambiente (VPCs e sub-redes) e os recursos do aplicativo (pilhas, instâncias da Amazon e imagens de EC2 instâncias ou AMIs) que podem ser implantados lá.

VPCs e as imagens da instância são configuradas em uma conta, com as permissões de acesso necessárias, durante a integração. Depois de estabelecidas, você pode usar o sistema de gerenciamento de mudanças para preenchê-las VPCs com pilhas de trabalho.

Encontrando a VPC no AMS IDs

Uma nuvem privada virtual (VPC) tem uma ou mais sub-redes. No AMS, sua VPC está em um Região da AWS e você tem sub-redes públicas e privadas.

Consulte também [Encontrando sub-rede IDs no AMS](#).

Alguns CTs exigem VpcId o. Para encontrar um ID de VPC, você pode usar o console do AMS ou a API/CLI.

Console AMS:

No painel de navegação, selecione VPCs e a VPC relevante. A página de detalhes da VPC da VPC selecionada é aberta com informações, incluindo o ID da VPC.

API ListVpcSummaries ou CLI do AMS SKMS:

 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.

1. Nos exemplos a seguir, o primeiro comando solicita uma lista de resumos de todos VPCs na conta. O segundo comando solicita a lista de VPCs, com um filtro de consulta para listar somente aqueles VPCs criados em 2016 e gerar o nome `CreatedTime VpcId`, e.

Note

Você pode obter a CLI do AMS SKMS por meio da página Recursos do desenvolvedor no console do AMS.

```
aws amsskms list-vpc-summaries --output table
```

```
-----
|                               |
|               ListVPCSummaries               |
|-----+-----+
|                               |
|               VPCSummaries                   |
|+-----+-----+
| CreatedTime | 2016-01-15T18:50:11Z |
| VpcId       | vpc-01234567890abcdef |
| LastModifiedTime | 2016-01-15T18:50:11Z |
| Name        | 952444781316-initial-vpc |
|+-----+-----+
|                               |
```

Visibility	
Id	PrivateAndPublic
Name	PrivateAndPublic

2. Desta vez com uma consulta:

```
aws amsskms list-VPC-summaries --query "VPCSummaries[?
starts_with(@.CreatedTime,to_string(`2016`))].[CreatedTime, VpcId, Name]" --output
table
```

ListVPCSummaries		
2016-01-15T18:50:11Z	vpc-01234567890abcdef	952444781316-initial-VPC

Encontrando sub-rede IDs no AMS

Vários recursos exigem que você especifique uma sub-rede, ou uma lista de sub-redes, no momento da configuração. Para encontrar sub-redes, você pode usar o console AMS ou o AMS SKMS API/CLI. Note that the AMS SKMS API/CLI é privado e deve ser instalado antes que você possa usá-lo.

Console AMS:

1. No painel de navegação, selecione VPCse a VPC relevante. A página de detalhes da VPC da VPC selecionada é aberta com uma tabela de sub-redes. Clique em uma ID de sub-rede para abrir a página de detalhes e encontrar a ID.

API ListSubnetSummaries ou CLI do AMS SKMS:

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 encontrar as sub-redes da sua VPC, você pode pesquisar com o `list-subnet-summaries` comando, conforme mostrado.

 Note

Se você estiver procurando por sub-redes que não estejam em uma conta AMS, tente. `aws ec2 describe-subnets --region us-west-2`

1. A API/CLI `ListSubnetSummaries` operação do SKMS:

Uma lista simples:

```
aws amsskms list-subnet-summaries
```

Saída para uma tabela:

```
aws amsskms list-subnet-summaries --output table
```

2. A `ListSubnetSummaries` operação da API SKMS tem parâmetros para restringir os resultados com base na visibilidade. Além disso, você pode [filtrar](#) os resultados com base no nome. Se você estiver usando a CLI, também poderá usar a `--query` opção de restringir a saída ou pesquisar uma parte de um valor. Por exemplo, para encontrar todas as sub-redes de uma VPC específica, você pode usar este comando:


```
aws amsskms list-subnet-summaries --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

O que retorna algo assim:

```
-----
|                               ListSubnetSummaries                               |
+-----+-----+-----+-----+
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
+-----+-----+-----+-----+
```

[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](#)

- Se você tiver vários VPCs, inclua um filtro de VPC no comando e execute o comando para cada VPC. Por exemplo:

```
list-subnet-summaries --filter Attribute=VpcId,Value=vpc-xxxxxxx --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

- Na AWS, use [describe-sub-nets](#).

[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](#)

Nomes de sub-rede

Suas sub-redes AMS são criadas automaticamente após a entrada ser coletada de você e adicionada ao sistema. O AMS usa uma fórmula para criar seus nomes de sub-rede: A **ACCOUNT_ID** - **SUBNET-TYPE** - **AZ** - **IDENTIFIER**. O tipo de sub-rede seria dmzshared-services, oucustomer-application. Se você tiver mais de uma sub-rede de aplicativo de cliente, um identificador opcional poderá ser adicionado ao nome da sub-rede, após o ID da conta, para indicar que a sub-rede é uma sub-rede “adicional” ou “reservada”.

Encontre AMI IDs, AMS

Uma Amazon Machine Image, ou AMI, é um modelo para EC2 instâncias da Amazon, criado a partir de uma EC2 instância da Amazon. AWS fornece atualizações AMIs (com patches, por exemplo) todo mês; no entanto, o AWS Managed Services (AMS) exige AMIs que tenham sido modificadas para uso do AMS. O AMS lança novidades AMIs que você pode usar logo após o Patch Tuesday de cada mês.

Amazon Machine Images (AMIs) são modelos de configuração de instâncias usados para criar EC2 instâncias na AWS. O AMS exige que o específico AMIs seja usado para recursos gerenciados pelo AMS. Os tipos de alteração para criar EC2 instâncias e grupos de EC2 Auto Scaling exigem que você especifique uma AMI para o AMS usar como base para as instâncias que o tipo de alteração cria. O AMS recomenda que você sempre selecione a AMI mais recente disponível para você.

Para saber mais AWS AMIs, consulte [AWS AMI Design](#).

Ao criar um Amazon EC2 stack ou um grupo Amazon EC2 Auto Scaling para sua conta AMS, você deve especificar uma AMI até. Amild Você está limitado a AMIs começar com “cliente-” e recomendamos que você sempre escolha a AMI mais recente.

Para encontrar a AMI mais recente para sua conta, você pode pesquisar com um comando da CLI do AMS SKMS ou usar a página de detalhes do console do AMS para ver a VPC relevante:

- Use o console AMS: AMIs Os disponíveis estão listados na página AMI no console AMS. Selecione AMIs com nomes que comecem com “cliente-”.
- Use a API/CLI ListAmis operação AMS SKMS.

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`

Aqui está um exemplo de CLI com uma query opção que restringe os resultados ao cliente: AMIs

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

Este exemplo usa a filter opção com a query opção de encontrar o Windows AMIs que começa com “cliente”:

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

- [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](#)

Encontre o grupo de segurança (SG) IDs, AMS

A EC2 criação e OpenSearch criação de domínios da Amazon CTs exigem um ID de grupo de segurança. Isso estará no formuláriosg-02ce123456e7893c7. Sua conta tem pelo menos dois grupos de segurança padrão; consulte[Grupos de segurança](#). Além disso, você pode ter grupos de segurança criados para fins específicos. Para descobrir seus grupos de segurança:

- Console AWS: use o console EC2 ou VPC para visualizar todos os grupos de segurança da VPC selecionada.
- API/CLI (quando conectado à sua conta AMS):

Liste seus grupos de segurança:

```
aws ec2 describe-security-groups
```

Encontre entidades do IAM no AMS

Sua conta tem funções e políticas padrão do IAM; veja os [Função de usuário do IAM no AMS](#) perfis de instância padrão do IAM; veja [EC2 Perfil de instância do IAM](#) com as políticas padrão. Para descobrir suas funções e políticas do IAM:

- Console: use o console do IAM para ver todas as políticas e funções do IAM para sua conta.
- API/CLI (quando conectado à sua conta AMS):

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`

Liste suas funções:

```
aws --profile saml iam list-roles
```

Liste suas políticas:

```
aws --profile saml iam list-role-policies --role-name ROLE_NAME
```

Encontre uma pilha IDs no AMS

Para encontrar um Stack ID, você pode usar o EC2 console Amazon, o console AMS ou a API/CLI do AMS SKMS.

Console AMS:

- No painel de navegação RFCs, selecione e clique no RFC que criou a pilha. Use a opção de filtro na parte superior para reduzir a lista. A página de detalhes do RFC é aberta e inclui a saída da execução com o ID da pilha.
- Como alternativa, você pode selecionar Pilhas no painel de navegação para abrir a página da lista de pilhas e, em seguida, percorrer a lista de pilhas até a pilha na qual você está interessado. Esse método é mais útil se você souber o assunto da pilha que está procurando.

EC2 Console Amazon:

No painel de navegação, selecione Instâncias ou Balanceadores de Carga ou Grupos de Auto Scaling.

API ListStackSummaries ou CLI do AMS SKMS:

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 ver uma lista de pilhas na conta atual, execute a ListStackSummaries operação da API SKMS (CLI:). `list-stack-summaries` Para obter informações completas sobre uma instância de pilha específica `StackId`, execute `GetStack` by.

- Nos exemplos a seguir, o primeiro comando solicita uma lista de resumos de todas as instâncias de pilha na conta. O segundo comando solicita a lista de instâncias de pilha, com um filtro de consulta para listar somente aquelas de um modelo de pilha específico e gerar o `VpcId` nome e `StackId`

```
aws amsskms list-stack-summaries --output table
```

```

-----
|                                     ListStackSummaries                                     |
|                                     StackSummaries                                     |
+-----+-----+-----+-----+
| VpcId | StackId | StackTemplateId | Name |
+-----+-----+-----+-----+
| vpc-0123abcd | stack-1fb7fe2212345678 | stm-sdhopvbb123456789 | Test ELB |
| vpc-0123abcd | stack-8323cc0e12345678 | stm-s2b72beb123456789 | S3 store |
| vpc-0123abcd | stack-2309fa0712345678 | stm-sdhopvbb123456789 | ELB |
| vpc-0123abcd | stack-5e61a70512345678 | stm-sdpabqbb123456789 | PatchSim |
| vpc-0123abcd | stack-bd0e080d12345678 | stm-s2b72beb123456789 | CLI demo |
+-----+-----+-----+-----+

```

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](#)

Note

Para obter informações sobre como usar IDs a instância para acesso, consulte também [Acessando instâncias usando bastiões](#).

Encontre endereços IP IDs ou de instância no AMS

- 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

O AMS CLI deve estar instalado 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-s6xvs0000000000000",
    "CreatedTime": "1486584508416",
    "Name": "Amazon"
  }
}
```


}

Encontre nomes de recursos da Amazon (ARNs) no AMS

Um Amazon Resource Name (ARN) é uma string que identifica exclusivamente um AWS recurso, como EC2 instâncias, buckets S3, contas, funções Lambda e assim por diante. AWS requer um ARN quando você deseja especificar um recurso de forma inequívoca em todos eles AWS, como nas políticas do IAM, nas tags do Amazon Relational Database Service (Amazon RDS) e nas chamadas de API. ARNs são construídos a partir de identificadores que especificam o serviço, a região, a conta e outras informações. Há três formatos de ARN:

```
arn:aws:service:region:account-id:resource-id
arn:aws:service:region:account-id:resource-type/resource-id
arn:aws:service:region:account-id:resource-type:resource-id
```

Note

O formato exato de um ARN depende do serviço e do tipo de recurso. [Para saber mais ARNs, consulte Amazon Resource Names \(ARNs\) e Namespaces AWS de serviços e formatos ARN.](#)

Para exemplos do formato ARN por recurso, consulte a tabela de [tipos de recursos](#) de Referência AWS de Autorização de Serviço.

Encontrar o ARN de um objeto da AWS pode ser difícil. Aqui estão três maneiras de experimentar:

- Console de serviços da AWS: acesse o console de serviços relevante da AWS, localize o recurso e encontre o ARN nos detalhes do recurso.
- AWS API/CLI (você deve primeiro instalar a AWS CLI): procure o serviço relevante na [Referência de Comandos da CLI](#) da AWS e, dependendo do serviço da AWS, procure a operação relevante, como, ou describeget, e assim por diante. Por exemplo, para todas as funções, políticas e usuários do IAM, você pode obter o ARN na saída da CLI com:

```
aws iam get-role --role-name EMR_DefaultRole
```

- Crie o ARN com base no formato relevante: encontre o formato ARN para o recurso, consultando a página [Ações, recursos e chaves de condição para serviços da AWS](#), localizando o serviço

relevante e, em seguida, a ação relevante e detalhando o formato ARN do recurso. Depois de ter o formato, substitua as variáveis pelas configurações relevantes.

Você mesmo pode criar o ARN seguindo o formato apropriado (os formatos mudam por serviço e tipo de recurso) e preenchendo as informações. Aqui estão alguns exemplos de ARN:

- Um Conta da AWS ARN tem a seguinte sintaxe:

```
arn:aws:iam::ACCOUNT-ID:root
```

- Um ARN do S3 tem uma hierarquia plana de buckets e objetos associados:

```
arn:aws:s3:::ams-bucket
```

- Um EC2 ARN tem subtipos de recursos, como imagem, grupos de segurança, instância e assim por diante. Esse exemplo inclui o ID da instância no final:

```
arn:aws:ec2:us-east-1:123456789012:instance/i-012abcd34efghi56
```

- Um ARN do Lambda tem o nome da função para a parte resource-id, e talvez seja necessário incluir o número da versão no final, conforme mostrado neste exemplo:

```
arn:aws:lambda:us-east-1:123456789012:function:api-function:1
```

O AWS Key Management Service serviço fornece as seguintes informações: [Encontrar o ID da chave e o ARN da chave](#).

[Para encontrar o ARN de uma tabela do DynamoDB, use a CLI da tabela descritiva do DynamoDB](#).

Para quem não conhece a descoberta AWS ARNs, consulte [AWS ARN Explained: Amazon Resource Name Guide](#).

Encontre recursos por ARN no AMS

Os Amazon Resource Names (ARNs) identificam AWS recursos de forma exclusiva. [Para saber mais sobre ARNs os formatos ARN, consulte Amazon Resource Names \(ARNs\) e Namespaces de AWS serviços e formatos ARN](#).

 Note

Para obter detalhes sobre um recurso de seu ARN, você deve ter acesso à conta que criou o recurso.

Não há um caminho direto AWS para pesquisar todos os detalhes do recurso a partir do ARN do recurso, porque os serviços têm vários tipos de recursos com várias informações relacionadas. Se você tiver o ARN de um recurso, poderá determinar:

- O AWS serviço relacionado (o terceiro segmento do ARN) informa qual console da AWS você deve consultar para encontrar o recurso
- O ID do recurso (o sexto ou sétimo segmento do ARN) confirma que você encontrou o recurso certo

Ou você pode procurar os comandos da AWS CLI disponíveis para esse serviço na [Referência de Comandos da AWS CLI](#) para obter informações sobre como obter detalhes sobre o recurso.

Por exemplo, a partir do seguinte ARN, você pode determinar se o serviço é `lambda`, a conta é `123456789012`, o tipo de recurso é `function` e o nome da função é `TestFunction`

```
arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

A partir disso, você pode revisar a [documentação da AWS CLI do serviço Lambda](#) para saber como mais detalhes podem ser recuperados com vários comandos, como `get-function` e `get-function-configuration`

Por exemplo, você pode usar os comandos a seguir para obter mais informações sobre uma função Lambda se tiver seu nome ou ARN:

```
aws lambda get-function-configuration --function-name TestFunction
```

```
aws lambda get-function-configuration --function-name arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

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 Backup](#) serviço 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](#).

Gerenciamento de acesso no AMS

Saiba como acessar recursos usando SSH ou protocolo de desktop remoto (RDP) e como usar os bastiões.

O sistema de gerenciamento de acesso do AWS Managed Services (AMS) é configurado durante a integração. Somente usuários com a função de usuário do AMS IAM, federados por meio do AMS, podem acessar os recursos do AMS na conta.

Além da confiança federada, descrita a seguir, os grupos de segurança do AMS são um elemento importante no acesso a aplicativos públicos e privados. Para obter informações sobre grupos de segurança do AMS e como alterá-los, consulte [Grupos de segurança](#).

Tópicos

- [O que é gerenciamento de acesso?](#)
- [Como e quando usar a conta de usuário raiz no AMS](#)
- [Console AMS Advanced e EC2 acesso à Amazon](#)
- [Acessando o console AWS de gerenciamento e o console AMS](#)
- [Acessando instâncias usando bastiões](#)

O que é gerenciamento de acesso?

O gerenciamento de acesso é a forma como o AMS protege seus recursos, permitindo somente acesso autorizado e autenticado. O AMS usa uma função de usuário e um perfil de instância padrão do IAM, bem como autenticação multifatorial, grupos de segurança, nomes de bastiões compatíveis com DNS e muito mais para manter seus recursos protegidos.

O AMS se concentra em três tipos de acesso que exigem gerenciamento:

- **Acesso ao console:** aproveitando a federação, os usuários no Active Directory da conta podem acessar o console usando o single sign-on (SSO). Se você tiver a autenticação multifator configurada para essas contas, poderá continuar exigindo o MFA para obter acesso ao console.
- **Acesso à instância com RDP ou SSH:** aproveitando a confiança do Active Directory, os usuários do Active Directory existente da conta podem solicitar acesso a uma instância e, em seguida, autenticar-se com êxito em um bastião e na instância usando suas credenciais corporativas existentes. Se você tiver a autenticação multifator configurada para essas contas, poderá continuar

exigindo o MFA para solicitar acesso a uma instância. O AMS usa uma solução própria de MFA para restringir o acesso dos engenheiros do AMS às instâncias.

- Acesso ao aplicativo: varia de acordo com o caso de uso.

Tópicos

- [Por que e quando o AMS acessa sua conta](#)

Por que e quando o AMS acessa sua conta

O AWS Managed Services (AMS) gerencia sua infraestrutura da AWS e, às vezes, por motivos específicos, operadores e administradores do AMS acessam sua conta. Esses eventos de acesso estão documentados em seus registros AWS CloudTrail (CloudTrail).

Por que, quando e como o AMS acessa sua conta são explicados nos tópicos a seguir.

Acionadores de acesso à conta do cliente do AMS

A atividade de acesso à conta do cliente do AMS é impulsionada por gatilhos. Os gatilhos atuais são os AWS tickets criados em nosso sistema de gerenciamento de problemas em resposta aos alarmes e eventos da Amazon CloudWatch (CloudWatch) e aos relatórios de incidentes ou solicitações de serviço que você envia. Várias chamadas de serviço e atividades em nível de host podem ser realizadas para cada acesso.

A justificativa do acesso, os acionadores e o iniciador do gatilho estão listados na tabela a seguir.

Acionadores de acesso

Acesso	Iniciador	Trigger
Aplicação de patches	AMS	Problema de patch
Implantações de infraestrutura	AMS	Problema de implantação
Investigação interna de problemas	AMS	Problema (um problema que foi identificado como sistêmico)
Investigação e remediação de alertas	AMS	Itens de trabalho operacionais (SSM OpsItems) do AWS Systems Manager

Acesso	Iniciador	Trigger
Execução manual de RFC	Você	Problema de solicitação de mudança (RFC). (O não automatizado RFCs pode exigir acesso do AMS aos seus recursos)
Investigação e remediação de incidentes	Você	Caso de suporte de entrada (um incidente ou solicitação de serviço que você envia)
Atendimento da solicitação de serviço de entrada	Você	

Funções do IAM para acesso à conta do cliente do AMS

Quando acionado, o AMS acessa contas de clientes usando funções AWS Identity and Access Management (IAM). Como todas as atividades em sua conta, as funções e seu uso estão logados CloudTrail.

Important

Não modifique nem exclua essas funções.

Funções do IAM para acesso do AMS às contas de clientes

Função	Tipo de conta (SALZ, MALZ Management, MALZ Application, etc.)	Descrição
ams-service-admin	SAL, MALZ	Acesso automatizado ao serviço AMS e implantações automatizadas de infraestrutura, por exemplo, patch, backup, remediação automatizada.

Função	Tipo de conta (SALZ, MALZ Management, MALZ Applicati on, etc.)	Descrição
ams-application-infra-read-somente	SALZ, aplicativo MALZ, aplicativ o de ferramentas MALZ	Acesso somente para leitura do operador
ams-application-infra-operations		Acesso do operador para incidents/service solicitações
ams-application-infra-admin		Acesso de administrador do AD
ams-primary-read-only	Gestão do MALZ	Acesso somente para leitura do operador
ams-primary-operations		Acesso do operador para incidents/service solicitações
ams-primary-admin		Acesso de administrador do AD
ams-logging-read-only	Registro em MALZ	Acesso somente para leitura do operador
ams-logging-operations		Acesso do operador para incidents/service solicitações
ams-logging-admin		Acesso de administrador do AD
ams-networking-read-only	Rede MALZ	Acesso somente para leitura do operador
ams-networking-operations		Acesso do operador para incidents/service solicitações
ams-networking-admin		Acesso de administrador do AD
ams-shared-services-read-somente	Serviços compartilhados MALZ	Acesso somente para leitura do operador

Função	Tipo de conta (SALZ, MALZ Management, MALZ Applicati on, etc.)	Descrição
ams-shared-services- operations		Acesso do operador para incidents/service solicitações
ams-shared-services- admin		Acesso de administrador do AD
ams-security-read-only	Segurança MALZ	Acesso somente para leitura do operador
ams-security-operations		Acesso do operador para incidents/service solicitações
ams-security-admin		Acesso de administrador do AD
ams-access-security- analyst	SALZ, aplicativo MALZ, aplicativ o de ferrament as MALZ, MALZ Core	Acesso de segurança do AMS
ams-access-security- analyst-somente leitura		Segurança do AMS, acesso somente para leitura
Sentinel_ _Role_ 0 MBhe AdminUser PXHaz RQadu PVc CDc	SAL	[BreakGlassRole] Usado para quebrar o vidro nas contas dos clientes
Sentinel_ _Role_ S0 0 PowerUser wZuPu ROOI IazDb RI9	SAL, MALZ	Acesso de usuários avançados às contas de clientes para execução de RFC
Sentinel_ ReadOnlyUser _role_PD4L6RW9RD0L NLKD5 JOo		ReadOnly acesso às contas de clientes para execução de RFC
função ams_admin_		Acesso de administrador às contas de clientes para execução de RFC

Função	Tipo de conta (SALZ, MALZ Management, MALZ Applicati on, etc.)	Descrição
AWSManagedServices _Provisioning_Cust omerStacksRole		Usado para lançar e atualizar pilhas de CFN em nome dos clientes por meio do Ingest CloudFormation
função_ssm_automat ion_customer_ssm_		Função passada pelas execuções de CT para a SSM Automation para execução do runbook
função_ams_ssm_a utomation_role	SALZ, aplicativ o MALZ, MALZ Core	Função passada pelos serviços AMS para a SSM Automation para execução do runbook
ams_ssm_iam_deploy ment_role	Aplicação MALZ	Função usada pelo catálogo do IAM
ams_ssm_shared_svc s_intermediary_role	Serviços compartilhados MALZ	Função usada pelo aplicativo ams_ssm_a utomation_role para executar documentos SSM específicos na conta do Shared Services
AmsOpsCenterRole		Usado para criar e atualizar OpsItems contas de clientes
AMSOpsItemAutoExec utionRole	SAL, MALZ	Usado para obter documentos SSM, descrever tags de recursos OpsItems, atualizar e iniciar a automação
customer-mc-ecPerfil de 2 instâncias		Perfil padrão da EC2 instância do cliente (função)

Solicitando acesso à instância

Para acessar um recurso, você deve primeiro enviar uma solicitação de alteração (RFC) para esse acesso. Há dois tipos de acesso que você pode solicitar: administrador (permissões de leitura/

gravação) e somente leitura (acesso de usuário padrão). O acesso dura oito horas, por padrão. Essas informações são obrigatórias:

- ID da pilha, ou conjunto de pilha IDs, da instância ou instâncias que você deseja acessar.
- O nome de domínio totalmente qualificado do seu domínio confiável da AMS.
- O nome de usuário do Active Directory da pessoa que deseja acessar.
- O ID da VPC onde estão as pilhas às quais você deseja acessar.

Depois de receber o acesso, você pode atualizar a solicitação conforme necessário.

Para ver exemplos de como solicitar acesso, consulte [Stack Admin Access | Grant](#) ou [Stack Read-only Access | Grant](#).

Como e quando usar a conta de usuário raiz no AMS

O [usuário root](#) é o superusuário em sua AWS conta. O AMS monitora o uso do root. Recomendamos que você use root somente para algumas tarefas que exigem isso, por exemplo: alterar as configurações da conta, ativar o acesso AWS Identity and Access Management (IAM) ao faturamento e ao gerenciamento de custos, alterar sua senha raiz e ativar a autenticação multifator (MFA). Consulte [Tarefas que exigem credenciais de usuário root](#) no Guia do AWS Identity and Access Management usuário.

Note

O MFA é ativado durante a integração do AMS Advanced para proibir especificamente o acesso do usuário raiz. O acesso root em contas gerenciadas pelo AMS é diferente de outras AWS contas e é fundamental para a segurança de todo o seu ambiente gerenciado pelo AMS. O MFA configurado é um MFA virtual e é executado usando um dispositivo de propriedade da AMS. Depois que a MFA virtual é configurada com a ajuda da AMS, o token virtual é imediatamente excluído. Isso garante que nem você nem o AMS mantenham a capacidade de fazer login na conta como usuário root. O login root só pode ser reativado em solicitações especiais (explicadas a seguir) e o AMS espera que esses acessos sejam usados somente quando absolutamente necessário. Para obter informações sobre o MFA, consulte [Proteger nova conta com autenticação multifator](#).

O acesso root sempre aciona uma resposta da equipe de segurança e operações do AMS. O AMS monitora as chamadas de API para acesso root e os alarmes são acionados se esse acesso for detectado.

A solicitação de acesso root é um pouco diferente entre os tipos de conta do AMS.

Acesso root com a landing zone de conta única do AMS Advanced:

Se você tiver uma landing zone de conta única, entre em contato com seu gerente de prestação de serviços em nuvem (CSDM) e com os arquitetos de nuvem (CAs) para informá-los sobre o trabalho de acesso raiz necessário. É melhor avisar com vinte e quatro horas de antecedência antes da atividade proposta.

Acesso root com a landing zone multiconta do AMS Advanced:

Para contas de aplicativos, serviços compartilhados, segurança ou rede na zona de destino com várias contas, use o tipo de alteração Management | Other | Other (ct-1e1xtak34nx76). Inclua a data, a hora e a finalidade de usar as credenciais do usuário raiz e agende a RFC para garantir um aviso prévio de vinte e quatro horas antes da atividade proposta. Use sua conta de gerenciamento de landing zone com várias contas para enviar o RFC.

Além disso, entre em contato com seu CSDM com CAs vinte e quatro horas de antecedência, para informá-lo sobre o trabalho de acesso raiz necessário.

Operações do AMS e resposta de segurança ao uso raiz:

O AMS recebe um alarme quando a conta do usuário raiz é usada. Se o uso das credenciais raiz não for programado, eles entrarão em contato com a equipe de segurança do AMS e com a equipe da sua conta para verificar se essa é a atividade esperada. Se não for uma atividade esperada, o AMS trabalha com sua equipe de segurança para investigar o problema.

Console AMS Advanced e EC2 acesso à Amazon

Acessando o console do AMS Advanced.

Acessando suas EC2 instâncias da Amazon.

Enviar solicitação de acesso:

Fazendo login em suas EC2 instâncias do AMS Amazon:

Acessando o console AWS de gerenciamento e o console AMS

Durante a integração, você recebe um login no console de AWS gerenciamento (com privilégios limitados: você pode gravar no console do AMS e em alguns campos na página de informações do cliente). Você pode acessar o console AMS selecionando o link Managed Services no console AWS de gerenciamento. O acesso federado ou as credenciais compartilhadas (nome de usuário/senha) são preparadas conforme acordado com sua equipe de administração de TI. Para criar mais contas ou grupos, envie uma solicitação de serviço ao AMS.

Para obter informações sobre como obter acesso ao console AWS de gerenciamento, consulte [Trabalhando com o console AWS de gerenciamento](#).

Para obter algumas dicas sobre como usar o console AMS, consulte [Usando o console AMS](#).

Acesso temporário ao console AMS

Se você ainda não configurou um provedor de identidade (por exemplo, SAML) para se autenticar no AMS, você pode obter acesso temporário ao console do AMS. Entre em contato com seu CSDM para que uma implantação | Componentes avançados de pilha | Identity and Access Management (IAM) | Crie uma solicitação de alteração de entidade ou política (ct-3dpd8mdd9jn1r) enviada em seu nome com estes valores:

- UserName: um nome para a entidade de usuário do IAM que você está criando
- AccessType: “Acesso ao console”
- UserPermissions: “Acesso temporário ao console AMS para **USERNAME** (a pessoa à qual você deseja ter acesso temporário)”
- Notificações por e-mail: seu endereço de e-mail, para que você possa aprovar a solicitação quando o AMS solicitar que você

Note

Essa RFC para acesso temporário ao console AMS exige uma análise e aceitação da segurança por sua equipe interna de segurança e pela AMS Global Security.

Depois que essa solicitação for concluída e você conseguir fazer login, você deverá aprovar a RFC que foi criada, acompanhar a aprovação e permitir que a equipe do AMS encerre o trabalho. Para aprovar a RFC, localize-a na página de listagem da RFC (haverá um sinalizador de aprovação pendente ao lado dela), selecione-a para abrir a página de detalhes da RFC e escolha Aprovar. Observe que você não poderá usar o AMS até que o RFC seja aprovado.

Quando a RFC é concluída com êxito, as operações do AMS fornecem o novo usuário do IAM e uma senha. Em seguida, siga estas etapas:

1. Acesse o console AWS de gerenciamento e faça login com as credenciais fornecidas. Você será solicitado a criar uma nova senha. Você também deve, ao fazer login, configurar a autenticação multifator (MFA); para saber mais sobre como fazer isso, [consulte Usando a Autenticação Multi-Factor \(MFA\)](#) em. AWS
2. No console AWS de gerenciamento, mude para a função do IAM fornecida (customer_*CustomerCode*_readonly_user_role).
3. Abra o AMS Managed Services Console.

Note

O acesso temporário é padronizado para sessenta dias; no entanto, você pode solicitar uma extensão de trinta dias entrando em contato com seu CSDM.

Acessando instâncias usando bastiões

Todo o acesso aos recursos dentro das contas gerenciadas pelo AMS, tanto para clientes quanto para operadores do AMS, é limitado pelo uso de bastion hosts. Mantemos bastiões do RDP do Linux e do Windows para acesso às contas AMS Advanced da zona de pouso com várias contas (MALZ) e da zona de pouso com conta única (SALZ).

Seus bastiões são acessíveis somente por meio de sua conexão privada (VPN ou Direct Connect) DX. Além do firewall para evitar o tráfego de entrada, os bastiões são regularmente reprovionados (com as credenciais existentes) em um cronograma fixo.

 Note

Para obter informações sobre como mover arquivos para uma EC2 instância, consulte [Transferência de arquivos: PC Windows ou MAC local para Linux Amazon EC2](#).

MALZ

Você acessa as instâncias da sua conta fazendo login em uma instância do Bastion com suas credenciais do Active Directory (AD). A Amazon usa bastiões localizados na rede perimetral VPC (conta de rede), e você usa seus bastiões de clientes, localizados na sub-rede Customer Bastions na conta de serviços compartilhados.

Quando seu ambiente AMS é inicialmente integrado, você tem dois bastiões SSH e dois bastiões RDP, dependendo da sua escolha.

SALZ

Você acessa as instâncias da sua conta fazendo login em uma instância do Bastion com suas credenciais do Active Directory (AD). O AMS usa bastiões localizados nas sub-redes da rede de perímetro, e você usa bastiões localizados em suas sub-redes privadas.

Quando sua conta é inicialmente integrada, você tem dois bastiões RDP e dois SSH, por padrão.

 Note

Como parte da landing zone de conta única, o AMS fornece bastiões RDP (Windows) e SSH (Linux) para acessar suas pilhas; no entanto, você pode escolher se deseja apenas bastiões RDP ou apenas bastiões SSH. Para solicitar que somente o RDP ou somente os bastiões do SSH sejam mantidos, envie uma solicitação de serviço.

Para acessar uma instância, você precisa:

- Acesso concedido à pilha. Para obter acesso concedido a uma pilha, consulte Stack [Admin Access | Grant ou Stack Read-Only Access | Grant](#).
- O ID da pilha que você deseja acessar para ter acesso à instância. Para encontrar um ID de pilha, consulte [Encontre uma pilha IDs no AMS](#).
- O IP da instância que você deseja acessar. Para encontrar um IP de instância, consulte [Encontre endereços IP IDs ou de instância no AMS](#).

- O nome do bastião compatível com DNS ou o IP do bastião. Como usar nomes de bastião compatíveis com DNS e como encontrar um IP de bastião são descritos a seguir.

Nomes de bastiões compatíveis com DNS

O AWS Managed Services (AMS) usa nomes de bastião 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`, `oubob`, 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`

Economizando custos em bastiões de landing zone de conta única (SALZ)

O AMS fornece dois bastiões SSH e dois bastiões RDP na configuração padrão para você se conectar às suas EC2 instâncias da Amazon e também implanta dois bastiões DMZ na configuração padrão para operações de serviço. Os bastiões usam EC2 instâncias grandes da Amazon por padrão. Você tem a opção de alterar as EC2 instâncias da Amazon usadas para bastions para t3.small e economizar custos.

Se você estiver usando instâncias sob demanda, instâncias spot ou um plano de economia, considere esse recurso e economize custos. Se você usa instâncias reservadas, considere se o uso de instâncias t3.small pode reduzir seus custos. Para alterar o tipo de instância, envie uma RFC

com Gerenciamento | Componentes avançados da pilha | Pilha de EC2 instâncias | Redimensionar (ct-15mazjj88xc69) CT da sua conta AMS.

Entre em contato com seu gerente de prestação de serviços em nuvem (CSDM) para perguntas adicionais ou para verificar se você pode se beneficiar desse recurso.

Usando endereços IP 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.

Exemplos de acesso à instância no AMS

Esses exemplos mostram como fazer login em uma instância em sua conta do AMS usando um bastion depois de receber acesso por meio de um RFC. Para obter informações sobre como obter acesso concedido, consulte [Solicitando acesso à instância](#).

 Note

Para obter informações sobre como mover arquivos para uma EC2 instância, consulte [Transferência de arquivos: PC Windows ou MAC local para Linux Amazon EC2](#).

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. [Usando endereços IP bastion](#)

 Note

Uma EC2 instância da Amazon criada por meio de um grupo do Amazon EC2 Auto Scaling terá um endereço IP que entra e sai alternadamente, e você precisa usar o EC2 console da Amazon para encontrar esse endereço IP.

- Nome de usuário (por exemplo `DOMAIN_FQDN\USERNAME`) e Senha: Credenciais da conta. `USERNAME` Deve ser seu nome de usuário do Active Directory.

Observe que um nome de usuário no formato `username@customerdomain.com` pode ser usado, mas pode causar problemas na configuração do PBIS.

- Endereço IP da pilha: encontre isso examinando a saída de execução da RFC que você enviou para iniciar a pilha ou procure o endereço IP da EC2 instância da Amazon no console da Amazon. EC2 Para uma única EC2 instância da Amazon, você também pode usar o comando `AMS SKMS ListStackSummaries` para encontrar o ID da pilha e, em seguida, `GetStack` encontrar o endereço IP da pilha. Para a referência da API AMS SKMS, consulte a guia Relatórios no console do AWS Artifact.

Acesse o endereço IP do bastion, SSH ou RDP, conforme apropriado, e faça login usando um dos procedimentos a seguir.

 Note

Os bastiões RDP permitem apenas duas conexões simultâneas. Portanto, na melhor das hipóteses, apenas 4 administradores podem se conectar às pilhas do Windows ao mesmo

tempo. Se você precisar de mais conexões para o RDP, consulte [Opções do AMS Bastion durante as migrações/integração de aplicativos no guia de integração](#) do AMS.

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, consulte [Nomes 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, consulte [Nomes 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).AMSAccountNumber.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).AMSAccountNumber.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\\\njohn.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, consulte [Nomes 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, consulte [Nomes 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).AMSAccountNumber.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).AMSAccountNumber.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
```

Controle de acesso baseado em equipe ou função em uma conta AMS

Cenário: duas equipes de aplicativos A e B usam uma única conta AMS para seus aplicativos “AA” e “BB”, respectivamente. A equipe A deseja acessar somente os recursos do aplicativo “AA” e a equipe B deseja acessar somente os recursos do aplicativo “BB”. Como faço para configurar isso?

Use suas ferramentas de ITSM para implementar controles de acesso baseados em equipe (TBAC). Por exemplo, você pode usar o aplicativo AMS ServiceNow Connector para integração com o AMS APIs. Entre em contato com seu CSDM para obter orientação de alto nível sobre essa implementação.

Configuração automatizada de instâncias no AMS Advanced

O serviço de configuração automática de instâncias do AMS Advanced é executado diariamente e verifica e atualiza automaticamente o SSM, os CloudWatch agentes e os arquivos de configuração em suas instâncias gerenciadas EC2. As atualizações se aplicam, conforme necessário, a:

- SSM e agentes CloudWatch
- CloudWatch arquivos de configuração

Essas atualizações permitem que o AMS acesse suas EC2 instâncias gerenciadas pelo AMS e configure suas instâncias para emitir [registros](#) e métricas apropriados.

Tópicos

- [Pré-requisitos para configuração automatizada de instâncias](#)
- [Instalação automática do SSM Agent](#)
- [Mudanças automatizadas](#)

Pré-requisitos para configuração automatizada de instâncias

Para clientes do AMS Advanced que implantam instâncias com o Change Management, os seguintes pré-requisitos devem ser atendidos:

- O Agente SSM está instalado e em um estado gerenciado.
- A instância é marcada como uma instância gerenciada. (A `aws:cloudformation:stack-name` tag tem um valor que começa com `stack-ousc-`.)

Se o Agente SSM ainda não estiver instalado na sua instância, você poderá instalá-lo usando o recurso de instalação automática do Agente SSM do AMS. Para obter mais informações, consulte [Instalação automática do SSM Agent](#).

Ou você pode instalar o SSM Agent manualmente. Para obter mais informações, consulte:

- Linux: [instale manualmente o SSM Agent em EC2 instâncias para Linux - AWS Systems Manager](#)
- Windows: [instale manualmente o SSM Agent em EC2 instâncias para Windows Server - AWS Systems Manager](#)

Para obter mais informações sobre o agente SSM, consulte a documentação da AWS [Trabalhando com o agente SSM](#).

Instalação automática do SSM Agent

Para que o AMS gerencie suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2), você deve instalar o AWS Systems Manager SSM Agent em cada instância. Se suas instâncias não tiverem o SSM Agent instalado, você poderá usar o recurso de instalação automática do AMS SSM Agent.

Note

- Esse recurso está disponível somente para EC2 instâncias que não estão em um grupo de Auto Scaling e que executam sistemas operacionais Linux compatíveis com o AMS.
- O recurso de instalação automática do AMS SSM Agent está desativado por padrão. Para habilitá-lo, entre em contato com sua CA ou CSDM.

Pré-requisitos para o uso do SSM Agent

- Certifique-se de que o perfil da instância associado às instâncias de destino tenha uma das seguintes políticas (ou permissões equivalentes, conforme listado nelas):
 - Amazon SSMMANAGED EC2 InstanceDefaultPolicy
 - Amazon SSMMANAGED InstanceCore
- Certifique-se de que não haja uma Política de Controle de Serviços no AWS Organizations nível que negue explicitamente as permissões listadas nas políticas anteriores.

Para obter mais informações, consulte [Configurar permissões de instância obrigatórias para o Systems Manager](#).

- Para bloquear o tráfego de saída, certifique-se de que os seguintes endpoints de interface estejam habilitados na VPC em que as instâncias de destino residem (substitua “região” na URL adequadamente):
 - ssm.<region>.amazonaws.com
 - ssmmessages.<region>.amazonaws.com
 - mensagens ec2. <region>.amazonaws.com

Para obter mais informações, consulte [Melhorar a segurança das EC2 instâncias usando VPC endpoints para Systems Manager](#).

Para dicas gerais sobre como habilitar ou solucionar problemas de disponibilidade de nós gerenciados, consulte [Solução 2: verificar se um perfil de instância do IAM foi especificado para a instância \(somente EC2 instâncias\)](#).

 Note

O AMS interrompe e inicia cada instância como parte do processo de instalação automática. Quando uma instância é interrompida, os dados armazenados nos volumes de armazenamento da instância e os dados armazenados na RAM são perdidos. Para obter mais informações, consulte [O que acontece quando você interrompe uma instância](#).

Solicite a instalação automática do SSM Agent em suas instâncias

Se suas contas estiverem integradas ao AMS Accelerate Patch Add-On, configure uma janela de manutenção de patches (MW) para as instâncias. É necessário um agente SSM em funcionamento para concluir o processo de patch. Se o SSM Agent estiver ausente em uma instância, o AMS tentará instalá-lo automaticamente durante a janela de manutenção do patch.

 Note

O AMS interrompe e inicia cada instância como parte do processo de instalação automática. Quando uma instância é interrompida, os dados armazenados nos volumes de armazenamento da instância e os dados armazenados na RAM são perdidos. Para obter mais informações, consulte [O que acontece quando você interrompe uma instância](#).

Como funciona a instalação automática do SSM Agent

O AMS usa dados EC2 do usuário para executar o script de instalação em suas instâncias. Para adicionar o script de dados do usuário e executá-lo em suas instâncias, o AMS deve parar e iniciar cada instância.

Se sua instância já tiver um script de dados do usuário existente, o AMS concluirá as seguintes etapas durante o processo de instalação automática:

1. Cria um backup do script de dados do usuário existente.
2. Substitui o script de dados do usuário existente pelo script de instalação do SSM Agent.
3. Reinicia a instância para instalar o SSM Agent.
4. Interrompe a instância e restaura o script original.
5. Reinicia a instância com o script original.

Mudanças automatizadas

O serviço de configuração automática de instâncias do AMS Advanced faz alterações, conforme necessário, em suas EC2 instâncias.

O que muda:

- [Atualize automaticamente o código em instâncias Linux](#)
- [Atualize automaticamente o PBIS em instâncias Linux](#)
- [Atualize automaticamente a versão mínima do SSM e CloudWatch dos agentes](#)
- [CloudWatch arquivos de configuração, detalhes da atualização](#)
- [Registros configurados automaticamente](#)

Atualize automaticamente o código em instâncias Linux

O AMS atualiza automaticamente o código da instância em instâncias Linux. Isso ajuda a melhorar completamente a estabilidade operacional e a segurança dos componentes e do ambiente do AMS.

PERGUNTAS FREQUENTES:

O que está incluído no Código de Instância Única (OIC) no Linux?

O OIC inclui o pacote `ams-toolkit` junto com alguns arquivos de configuração e tarefas cron. O AMS exige esses arquivos e pacotes para integração (Active Directory CloudFormation e outras dependências). Pré-configuramos esses arquivos em arquivos fornecidos pelo AMS AMIs ou os instalamos em sua instância durante a ingestão da carga de trabalho.

Quando o AMS atualizará o OIC?

O AMS atualiza o OIC quando lançamos uma nova versão com correções de bugs ou outras melhorias. O fluxo de trabalho para verificar a versão e a atualização do OIC é executado diariamente.

Atualize automaticamente o PBIS em instâncias Linux

O AMS usa o módulo Power Broker Identity Service (PBIS) para unir instâncias Linux ao Active Directory gerenciado pelo AMS.

O AMS atualiza automaticamente o PBIS em instâncias Linux.

PERGUNTAS FREQUENTES:

Quando o AMS atualizará o PBIS?

O AMS ativa a atualização do PBIS na reinicialização. Se houver uma nova versão do PBIS disponível, o AMS tentará instalar a nova versão durante a próxima reinicialização da instância.

A atualização do PBIS pode ser desativada?

Você pode desativar a atualização do PBIS nos níveis da instância ou da conta:

- Nível da conta: crie um parâmetro no armazenamento de parâmetros SSM: Nome: `/ams/skip-pbis-update`, Valor: `true` (qualquer caso).

Note

O perfil da instância deve ter permissões para ler os parâmetros do SSM. Se o sinalizador estiver ausente, o comportamento padrão é executar a atualização.

- Nível da instância:
 - Com base em tags: adicione a seguinte tag à instância: Key: `skip_pbis_update`, Value: `true` (qualquer caso).
 - Arquivo de configuração: adicione o seguinte sinalizador ao `/opt/aws/ams/etc/ams.conf.d/state.ini` arquivo: `skip_pbis_update = true`.

 Note

A tag tem uma prioridade maior do que o parâmetro SSM. Você pode desativar a atualização do PBIS no nível da conta por meio do parâmetro, mas transformá-la para uma única (ou várias) instância (s) adicionando uma `tagKey:skip_pbis_update,Value: false`.

Para configurar qualquer uma das opções descritas, siga o processo padrão de gerenciamento de alterações em seu ambiente AMS.

Atualize automaticamente a versão mínima do SSM e CloudWatch dos agentes

A versão mínima do AMS Advanced (do SSM ou dos CloudWatch agentes) é a versão que foi testada pela equipe de serviço do AMS e pré-aprovada para seu sistema operacional. Tentamos ser proativos e executar a versão mais recente estável e compatível, então o número da versão muda com o tempo. Você pode encontrar a versão mínima atual enviando uma solicitação de serviço para o AMS.

- Gerenciamento de agentes SSM

O Amazon SSM Agent é responsável por executar comandos remotos na instância. A automação da configuração da instância garante que o agente SSM esteja executando a versão mínima.

- Gerenciamento de agentes do Cloudwatch

O Amazon CloudWatch Agent é responsável por emitir registros e métricas do sistema operacional. A configuração automatizada da instância executa o seguinte:

- Se necessário, desativa o agente de CloudWatch log antigo e migra a configuração para o novo agente unificado CloudWatch
- Se sua instância estiver executando o Agente de CloudWatch Log legado, a configuração automática da instância desativa o serviço de agente de CloudWatch Log legado e migra sua configuração para o agente unificado CloudWatch .
- Personaliza sua CloudWatch configuração para emitir registros e métricas apropriados.

Arquivos e diretórios afetados:

- Windows
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\

- %ProgramData%\ Amazon\AmazonCloudWatchAgent\ Configs\
- Linux
 - /opt/aws/amazon-cloudwatch-agent/etc/
 - /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/
 - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

CloudWatch arquivos de configuração, detalhes da atualização

Lemos suas CloudWatch configurações personalizadas (somente JSON) dos seguintes CloudWatch diretórios (consulte os [diretórios recomendados](#)) e as mesclamos com a configuração padrão do AMS: CloudWatch

- CloudWatch Arquivos
 - Na instância:
 - Windows
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\ Configs\
 - %ProgramFiles%\ ModulesWindowsPowerShell\ AWSManaged Services.Logging.Utilities\ Files\ Config.json
 - Linux
 - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json
 - No Amazon S3:
 - Windows:
 - [https://ams-configuration-artifacts- *REGION_NAME* .s3. *REGION_NAME*.amazonaws. com/ configurations/cloudwatch/latest/windows-cloudwatch-config.json](https://ams-configuration-artifacts-<i>REGION_NAME</i>.s3.<i>REGION_NAME</i>.amazonaws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json)
 - Linux
 - [https://ams-configuration-artifacts- *REGION_NAME* .s3. *REGION_NAME*.amazonaws. com/ configurations/cloudwatch/latest/linux-cloudwatch-config.json](https://ams-configuration-artifacts-<i>REGION_NAME</i>.s3.<i>REGION_NAME</i>.amazonaws.com/configurations/cloudwatch/latest/linux-cloudwatch-config.json)

Registros configurados automaticamente

Configuramos sua instância para gravar os seguintes registros.

- **Windows:**

- SSMAgentRegistro da Amazon
- AmazonCloudWatchAgentLog
- SSMErrrorRegistro da Amazon
- AmazonCloudFormationLog
- ApplicationEventLog
- EC2ConfigServiceEventLog
- MicrosoftWindowsAppLockerEXEAndDLLEventRegistro
- MicrosoftWindowsAppLockerMSIAndScriptEventLog
- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog
- Linux
 - /var/log/amazon/ssm/amazon-ssm-agent.log
 - /var/log/amazon/ssm/errors.log
 - /var/log/audit/audit.log
 - /var/log/cloud-init-output.log
 - /var/log/cloud-init.log
 - /var/log/cron
 - /var/log/dpkg.log
 - /var/log/maillog
 - /var/log/messages
 - /var/log/secure
 - /var/log/spooler
 - /var/log/syslog
 - /var/log/yum.log
 - /var/log/zypper.log

Monitoramento e gerenciamento de eventos no AMS

Tópicos

- [O que é monitoramento?](#)
- [O que o sistema de monitoramento AMS monitora?](#)
- [Como funciona o monitoramento](#)
- [Visualizando a configuração de monitoramento de uma conta AMS](#)
- [Alterando a configuração de monitoramento de uma conta AMS](#)
- [Notificações de incidentes com reconhecimento de aplicativos no AMS](#)
- [Usando OpsCenter no AMS](#)
- [Notificações de alerta do AMS](#)
- [Criação de CloudWatch alarmes adicionais no AMS](#)
- [Criação de CloudWatch métricas e alarmes personalizados no AMS](#)
- [Usando o CloudWatch Application Insights para servidores do .Net e SQL no AMS](#)
- [Usando as regras EventBridge gerenciadas da Amazon no AMS](#)
- [Remediador confiável no AMS](#)

O sistema de monitoramento do AWS Managed Services (AMS) monitora seus recursos do AMS em busca de falhas, degradação do desempenho e problemas de segurança. O sistema de monitoramento do AMS depende de serviços da AWS, como Amazon CloudWatch (CloudWatch), Amazon GuardDuty, Amazon Macie e AWS Health. Além do sistema de monitoramento, o AMS também implanta TrendMicro DeepSecurity para proteção contra malware em instâncias do Amazon Elastic Compute Cloud (Amazon EC2). Para obter informações sobre os padrões de segurança de endpoints (EPS), consulte [Segurança de terminais \(EPS\)](#).

O monitoramento do AMS oferece os seguintes benefícios:

- Uma linha de base de monitoramento para que você tenha um nível padrão de proteção, mesmo que não configure nenhum outro monitoramento para suas contas gerenciadas. Para mais informações, consulte [Alertas do monitoramento de linha de base no AMS](#).
- Alertas de investigação para determinar a ação apropriada. Por exemplo, se GuardDuty encontrar uma atividade indicando tentativas de força bruta contra uma EC2 instância da Amazon, o AMS analisa os registros de fluxo da VPC para entender a origem e o contexto da atividade.

- Correção de alertas, quando possível, para evitar ou reduzir o impacto em seus aplicativos. Por exemplo, se você estiver usando uma EC2 instância autônoma da Amazon e ela falhar na verificação de integridade do sistema, o AMS tentará recuperar a instância interrompendo-a e reiniciando-a. Para obter mais informações, consulte [Remediação automática de alertas pelo AMS](#).
- Transparência no uso de alertas ativos e previamente resolvidos OpsCenter. Por exemplo, se você tiver uma alta utilização inesperada da CPU em uma EC2 instância da Amazon, você pode solicitar acesso ao console do AWS Systems Manager (inclui acesso ao OpsCenter console) e visualizá-los OpsItem diretamente no OpsCenter console.

O que é monitoramento?

O sistema de monitoramento AMS monitora seus AWS recursos em busca de falhas, degradação do desempenho e problemas de segurança. Como uma conta gerenciada, o AMS configura e implanta alarmes para os AWS recursos aplicáveis, os monitora e executa a correção quando aplicável.

O sistema de monitoramento AMS gera alertas com base na configuração de monitoramento em sua conta. A configuração de monitoramento de uma conta se refere a todos os parâmetros de recursos na conta que criam um alerta; para obter informações sobre os parâmetros do recurso, consulte [Alertas do monitoramento de linha de base no AMS](#). A configuração de monitoramento de uma conta inclui definições de CloudWatch alarme e regras de CloudWatch eventos que geram o alerta (alarme ou evento).

A configuração básica de monitoramento é o conjunto de definições de alarme ([Alertas do monitoramento de linha de base no AMS](#)) selecionadas pelo AMS para monitorar recursos em sua conta gerenciada. A configuração de monitoramento de uma conta pode ser diferente da configuração básica, como resultado das alterações solicitadas por você.

Uma notificação de falhas iminentes, contínuas, recorrentes ou potenciais, degradação do desempenho ou problemas de segurança gerados pelo monitoramento básico configurado em uma conta é chamada de alerta. Exemplos de alertas são um CloudWatch alarme da Amazon, um CloudWatch evento da Amazon, um evento ou uma descoberta do serviço da AWS, como a Amazon GuardDuty, e um evento, ou um alerta, do Trend Micro Deep Security.

Os alertas de serviços da AWS relacionados à segurança, como Amazon, GuardDuty Amazon Macie ou Trend Micro Deep Security, são chamados de alertas de segurança para diferenciá-los de outros tipos de alertas.

O monitoramento do AMS oferece os seguintes benefícios:

- A capacidade de personalizar os alarmes de recursos básicos para atender às suas necessidades.
- Remediação automática de alertas, quando possível, para evitar ou reduzir o impacto em seus aplicativos. Por exemplo, se você estiver usando uma EC2 instância autônoma da Amazon e ela falhar na verificação de integridade do sistema, o AMS tentará recuperar a instância interrompendo-a e reiniciando-a. Para obter mais informações, consulte [Remediação automática de alertas pelo AMS](#).
- Transparência no uso de alertas ativos e previamente resolvidos OpsCenter. Por exemplo, se você tiver uma alta utilização inesperada da CPU em uma EC2 instância da Amazon, poderá solicitar acesso ao AWS Systems Manager console (o que inclui acesso ao OpsCenter console) e OpsItem visualizá-lo diretamente no OpsCenter console.
- Investigando alertas para determinar as ações apropriadas.
- Alertas gerados com base na configuração da sua conta e AWS dos serviços suportados. A configuração de monitoramento de uma conta se refere a todos os parâmetros de recursos na conta que criam um alerta. A configuração de monitoramento de uma conta inclui definições de CloudWatch alarme e EventBridge (anteriormente conhecidas como CloudWatch Eventos) que geram o alerta (alarme ou evento). Para obter mais informações sobre parâmetros de recursos, consulte [Alertas do monitoramento de linha de base no AMS](#).
- Notificação de falhas iminentes, contínuas, recorrentes ou potenciais; degradação do desempenho; ou problemas de segurança gerados pelo monitoramento básico configurado em uma conta (conhecido como alerta). Exemplos de alertas incluem um CloudWatch alarme, um evento ou uma descoberta de um serviço da AWS, como GuardDuty ou AWS Health.

O que o sistema de monitoramento AMS monitora?

De acordo com o modelo de responsabilidade de serviços compartilhados do AWS Managed Services (AMS), o sistema de monitoramento do AMS monitora sua infraestrutura da AWS. Para obter detalhes sobre o monitoramento básico no AMS, incluindo os recursos da AWS monitorados e o tipo de alertas para cada recurso, consulte [Alertas do monitoramento de linha de base no AMS](#). Para EC2 instâncias da Amazon, o AMS monitora o sistema operacional e fornece monitoramento básico com base nas métricas do sistema operacional, como utilização da CPU e uso do volume raiz.

Recomendamos complementar o monitoramento do AMS com monitoramento adicional usando serviços da AWS personalizados para seu aplicativo. [Para obter orientação sobre o monitoramento da disponibilidade, consulte a seção “Monitoramento e alarme” neste whitepaper Pilar de confiabilidade](#). Você pode configurar seu próprio monitoramento para atender às suas necessidades

operacionais; como fazer isso é discutido em [Criação de CloudWatch alarmes adicionais no AMS](#) e [Criação de CloudWatch métricas e alarmes personalizados no AMS](#).

Monitoramento proativo da confiança do Active Directory no AMS na zona de destino com uma única conta

O AMS single-account landing zone (SALZ) monitora o status das relações de confiança unidirecionais entre o Managed Active Directory (AD) em sua conta gerenciada do AMS e o domínio de sua empresa. A confiança unidirecional com o AD gerenciado é fundamental para solicitações de acesso e solicitações de logon de instância. Com esse novo monitoramento, o AMS agora responde proativamente às questões relacionadas à confiança e reduz o tempo médio para detectar incidentes relacionados ao acesso.

Esse recurso é habilitado automaticamente em suas contas do AWS Managed Services (AMS).

Há um pequeno impacto nos custos. O recurso usa quatro CloudWatch métricas da AWS e dois CloudWatch alarmes da AWS para uma confiança.

Como funciona o monitoramento

Veja os gráficos a seguir sobre a arquitetura de monitoramento no AWS Managed Services (AMS).

O diagrama a seguir fornece uma visão geral de alto nível do fluxo de trabalho de monitoramento da zona de pouso com várias contas do AMS e da zona de pouso com uma única conta do AMS.

- **Geração:** no momento da integração da conta, o AMS configura o monitoramento básico (uma combinação de alarmes CloudWatch (CW) e regras de eventos do CW) para todos os seus recursos criados em uma conta gerenciada. A configuração de monitoramento de linha de base gera um alerta quando um alarme CW é acionado ou um evento CW é gerado.
- **Agregação:**
 - **Zona de aterrissagem de várias contas:** os alertas são gerados por seus recursos nas contas do aplicativo e da unidade organizacional principal e enviados ao sistema de monitoramento do AMS, direcionando-os por meio da conta de segurança.
 - **Zona de aterrissagem de conta única:** todos os alertas gerados por seus recursos são enviados ao sistema de monitoramento do AMS, direcionando-os para um tópico do SNS na conta.
 - **Você também pode configurar como o AMS agrupa os EC2 alertas.** O AMS agrupa todos os alertas relacionados à mesma EC2 instância em um único incidente ou cria um incidente

por alerta, dependendo da sua preferência. Você pode alterar essa configuração a qualquer momento trabalhando com seu Cloud Service Delivery Manager ou Cloud Architect. Isso funciona da mesma forma se você estiver usando a Zona de Aterrissagem de Várias Contas ou a Zona de Aterrissagem de Conta Única.

- **Processamento:** O AMS analisa os alertas e os processa com base em seu potencial de impacto. Os alertas são processados conforme descrito a seguir.
- **Alertas com impacto conhecido no cliente:** eles levam à criação de um novo relatório de incidentes e o AMS segue o processo de gerenciamento de incidentes; para obter informações sobre o gerenciamento de incidentes, consulte [Resposta ao incidente do AMS](#).

Exemplo de alerta: uma EC2 instância da Amazon falha em uma verificação de integridade do sistema, o AMS tenta recuperar a instância interrompendo-a e reiniciando-a.

- **Alertas com impacto incerto no cliente:** para esses tipos de alertas, o AMS envia um relatório de incidentes, em muitos casos solicitando que você verifique o impacto antes que o AMS tome medidas. No entanto, se as verificações relacionadas à infraestrutura forem aprovadas, o AMS não enviará um relatório de incidentes para você.

Por exemplo: um alerta de mais de 85% de utilização da CPU por mais de 10 minutos em uma EC2 instância da Amazon não pode ser imediatamente classificado como um incidente, pois esse comportamento pode ser esperado com base no uso. Neste exemplo, o AMS Automation executa verificações relacionadas à infraestrutura no recurso. Se essas verificações forem aprovadas, o AMS não enviará uma notificação de alerta, mesmo que o uso da CPU ultrapasse 99%. Se a automação detectar que as verificações relacionadas à infraestrutura estão falhando no recurso, o AMS enviará uma notificação de alerta e verificará se a mitigação é necessária. As notificações de alerta são discutidas em detalhes nesta seção. O AMS oferece opções de mitigação na notificação. Quando você responde à notificação confirmando que o alerta é um incidente, o AMS cria um novo relatório de incidente e o processo de gerenciamento de incidentes do AMS começa. As notificações de serviço que recebem uma resposta de “sem impacto no cliente”, ou nenhuma resposta por três dias, são marcadas como resolvidas e o alerta correspondente é marcado como resolvido.

- **Alertas sem impacto no cliente:** se, após a avaliação, o AMS determinar que o alerta não tem impacto no cliente, o alerta será encerrado.

Por exemplo, AWS Health notifica sobre uma EC2 instância que precisa ser substituída, mas essa instância já foi encerrada.

EC2 notificações agrupadas por instâncias

Você pode configurar o monitoramento do AMS para agrupar alertas da mesma EC2 instância em um único incidente. Seu Cloud Service Delivery Manager ou Cloud Architect pode configurar isso para você. Há quatro parâmetros que você pode configurar para cada conta gerenciada pelo AMS.

1. Escopo: escolha em toda a conta ou com base em tags.

- Para especificar uma configuração que se aplique a todas as EC2 instâncias dessa conta, escolha scope = account-wide.
- Para especificar uma configuração que se aplique somente às EC2 instâncias dessa conta com uma tag específica, escolha scope = tag-based.

2. Regra de agrupamento: escolha clássica ou instância.

- Para configurar o agrupamento em nível de instância para cada recurso em sua conta, escolha escopo = toda a conta e regra de agrupamento = instância.
- Para configurar recursos específicos em sua conta para usar o agrupamento em nível de instância, marque essas instâncias e escolha escopo = baseado em tag e regra de agrupamento = nível de instância.
- Para não usar o agrupamento de instâncias para alertas em sua conta, escolha regra de agrupamento = clássico.

3. Opção de engajamento: escolha nenhuma, somente relatório ou padrão.

- Para que o AMS não crie incidentes ou execute automações para alarmes desses recursos enquanto a configuração estiver ativa, escolha nenhum.
- Para que o AMS não crie incidentes ou execute automações para alarmes desses recursos enquanto a configuração estiver ativa, e não execute a correção automática de documentos do Systems Manager, mas inclua registros desses eventos em seus relatórios, escolha somente relatório. Isso pode ser útil se você quiser reduzir o volume de casos de suporte a incidentes com os quais interage e se alguns incidentes de alguns recursos não exigirem atenção imediata, por exemplo, aqueles em uma conta que não seja de produção.
- Para que o AMS processe seus alertas, execute automações e crie casos de incidentes quando necessário, escolha padrão.

4. Resolver depois: escolha 24 horas, 48 horas ou 72 horas. Por fim, configure quando os casos de incidentes são encerrados automaticamente. Se a hora da correspondência do último caso atingir o valor de Resolver após configurado, o incidente será encerrado.

Notificação de alerta

Como parte do processamento do alerta, com base na análise de impacto, o AWS Managed Services (AMS) cria um incidente e inicia o processo de gerenciamento de incidentes para remediação, quando o impacto pode ser determinado. Se o impacto não puder ser determinado, o AMS enviará uma notificação de alerta para o endereço de e-mail associado à sua conta por meio de uma notificação de serviço. Em alguns cenários, essa notificação de alerta não é enviada. Por exemplo, se as verificações relacionadas à infraestrutura estiverem passando por um alerta de alta utilização da CPU, uma notificação de alerta não será enviada para você. Para obter mais informações, consulte o diagrama da arquitetura de monitoramento do AMS para o processo de tratamento de alertas em [Como funciona o monitoramento](#).

Notificação de alerta baseada em tag

Use tags para enviar notificações de alerta de seus recursos para diferentes endereços de e-mail. É uma prática recomendada usar notificações de alerta baseadas em tags, pois as notificações enviadas para um único endereço de e-mail podem causar confusão quando várias equipes de desenvolvedores usam a mesma conta. As notificações de alerta baseadas em tags não são afetadas pelas [EC2 notificações agrupadas por instâncias](#) configurações escolhidas.

Com as notificações de alerta baseadas em tags, você pode:

- Envie alertas para um endereço de e-mail específico: Marque os recursos que têm alertas que devem ser enviados para um endereço de e-mail específico com `okey = OwnerTeamEmail,value = EMAIL_ADDRESS`.
- Enviar alertas para vários endereços de e-mail: para usar vários endereços de e-mail, especifique uma lista de valores separados por vírgula. Por exemplo, `key = OwnerTeamEmail, value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...`. O número total de caracteres para o campo de valor não pode exceder 260.
- Use uma chave de tag personalizada: para usar uma chave de tag personalizada, forneça o nome da chave de tag personalizada ao seu CSDM em um e-mail que autorize explicitamente a ativação de notificações automáticas para a comunicação baseada em tags. É uma prática recomendada usar a mesma estratégia de marcação para tags de contato em todas as suas instâncias e recursos.

 Note

O valor chave *OwnerTeamEmail* não precisa estar em camel case. No entanto, as tags diferenciam maiúsculas de minúsculas e é uma prática recomendada usar o formato recomendado.

O endereço de e-mail deve ser especificado por completo, com o “sinal de arroba” (@) para separar a parte local do domínio. Exemplos de endereços de e-mail inválidos:

Team.AppATabc.xyz ou *john.doe*. Para obter orientação geral sobre sua estratégia de marcação, consulte Recursos de [marcação AWS](#). Não adicione informações de identificação pessoal (PII) em suas tags. Use listas de distribuição ou aliases sempre que possível.

A notificação de alerta baseada em tags é compatível com recursos dos seguintes serviços da Amazon: Elastic Block Store (EBS) EC2, Elastic Load Balancing (ELB), Application Load Balancer (ALB), Network Load Balancer, Relational Database Service (RDS), Elastic File System (EFS) e VPN. OpenSearch FSx Site-to-Site

Visualizando a configuração de monitoramento de uma conta AMS

Há duas partes principais na configuração de monitoramento de uma conta que você pode visualizar:

- CloudWatch Alarmes: Você pode ver todos os alarmes CW na conta acessando o CloudWatch console e selecionando diferentes serviços de interesse.
- CloudWatch Eventos:
 - Zona de destino de várias contas: CloudWatch os eventos monitorados na conta podem ser encontrados filtrando todas as regras de eventos do CW com a string. "ams -"
 - Zona de destino de conta única: CloudWatch os eventos monitorados na conta podem ser encontrados filtrando todas as regras de eventos do CW com a string. "mc -"

Alterando a configuração de monitoramento de uma conta AMS

Você pode alterar sua configuração básica de monitoramento dos EC2 recursos da Amazon. Para ver os alertas que podem ser configurados, consulte [Alertas do monitoramento de linha de base no AMS](#). Você pode alterar a definição do alarme, o destino do alarme ou cancelar a notificação de alarme dos monitores de linha de base para que os alertas atendam aos requisitos operacionais do seu aplicativo. Você pode solicitar qualquer uma ou todas as alterações mencionadas anteriormente

enviando um CT de Gerenciamento | Outro | Outro | Atualize o CT (ct-0xdawir96cy7k) com os seguintes detalhes.

- Instância IDs [opcional, se não for mencionada, todas as instâncias na conta estão dentro do escopo]
- CloudWatch nome da métrica, por exemplo, utilização da CPU/swap free/ IOwait
- Alvo - ID de e-mail/número de telefone para SMS/tópico SNS

Para saber mais sobre os tipos de mudanças que você pode solicitar na configuração básica de monitoramento, consulte a [CloudWatch documentação da Amazon](#).

Notificações de incidentes com reconhecimento de aplicativos no AMS

Use notificações de incidentes automatizadas com reconhecimento de aplicativos para personalizar sua experiência de comunicação para casos de suporte que o AMS cria em seu nome. Quando você usa esse recurso, o AMS recupera preferências personalizadas de carga de trabalho [AWS Service Catalog AppRegistry](#) para enriquecer suas comunicações sobre incidentes do AMS com metadados sobre seus aplicativos e para personalizar a gravidade dos casos de suporte criados pelo AMS em seu nome. Para usar esse recurso, primeiro você deve provisionar AWS Service Catalog AppRegistry em sua conta do AMS.

Para saber mais sobre os padrões de monitoramento do AMS, consulte [Monitoramento e gerenciamento de eventos no AMS](#)

Provisione AppRegistry sua conta AMS e crie aplicativos

O AppRegistry serviço está disponível no modo Self-Service Provisioning (SSP) para sua conta AMS. Para obter instruções sobre como solicitar acesso, consulte [Usar o AMS SSP para provisionar AWS Service Catalog AppRegistry em sua conta do AMS](#).

Após o provisionamento AppRegistry, use um dos métodos a seguir para criar aplicativos:

1. AWS console: Para saber mais sobre a criação de um aplicativo AppRegistry por meio do console da AWS, consulte [Criação de aplicativos](#) no Guia AWS Service Catalog AppRegistry do administrador.

2. CloudFormation: você pode definir seu AppRegistry aplicativo da mesma forma que define qualquer outro recurso. Para obter mais informações, consulte [AWS Service Catalog AppRegistry resource type reference](#) no Guia do usuário do CloudFormation .

Crie tags para permitir o enriquecimento de casos

Você deve marcar seus aplicativos antes que o AMS possa acessar os metadados do aplicativo. A tabela a seguir lista a tag necessária.

Chave de tag	Valor da tag
gerenciado por ams	true

Personalize a gravidade do caso de suporte do AMS para seus aplicativos

Você pode personalizar a gravidade dos casos de suporte criados pelo AMS especificando a importância do seu aplicativo para sua organização. Essa configuração é controlada por um grupo de atributos associado ao seu aplicativo em AppRegistry. O nome do grupo de atributos deve corresponder ao seguinte padrão:

```
AMS.<ApplicationName>.CommunicationOptions
```

No padrão anterior, o `ApplicationName` deve corresponder ao nome usado AppRegistry quando você criou o aplicativo.

Exemplo de conteúdo:

```
{
  "SchemaVersion": "1.0",
  "Criticality": "low"
}
```

SchemaVersion

Isso determina a versão do esquema que você está usando e o subconjunto de recursos disponíveis para uso.

Versão do esquema	Recurso
1,0	Gravidade personalizada do caso de suporte com base no valor de criticidade

Criticidade

A criticidade desse aplicativo determina a gravidade dos casos de suporte criados pelos sistemas automatizados da AMS.

Valores válidos:

```
low|normal|high|urgent|critical
```

Para obter mais informações sobre os níveis de gravidade, consulte [SeverityLevel](#) Referência AWS Support da API.

Obrigatório: Sim

Revise as permissões necessárias

Para usar esse recurso, o AMS requer acesso às seguintes AWS Identity and Access Management permissões:

- objetivo: ListRoleTags
- objetivo: ListUserTags
- API de marcação de grupos de recursos: GetResources
- catálogo de serviços - registro de aplicativos: GetApplication
- catálogo de serviços - registro de aplicativos: ListAssociatedAttributeGroups
- catálogo de serviços - registro de aplicativos: GetAttributeGroup

Important

Certifique-se de que não haja uma política do IAM ou uma política de controle de serviços (SCP) que negue as ações anteriores.

As chamadas de API são feitas pela `ams-access-admin` função. Veja a seguir um exemplo do que você pode ver:

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

Usando OpsCenter no AMS

A equipe de operações do AWS Managed Services (AMS) usa [AWS Systems Manager OpsCenter](#) para diagnosticar e remediar muitos alertas relacionados aos seus recursos.

O uso OpsCenter reduz o tempo médio de resolução (MTTR), ao mesmo tempo em que fornece uma visão transparente das filas operacionais das equipes de operações do AMS.

Com OpsCenter, o AMS fornece uma visão transparente dos itens de trabalho operacionais, também conhecidos como [OpsItems](#), ativamente trabalhados pelas equipes do AMS, além de soluções automatizadas.

Para saber mais sobre OpsCenter e OpsItems, consulte [AWS Systems Manager OpsCenter](#).

Para obter informações sobre como obter acesso ao console AWS de gerenciamento, consulte Como [trabalhar com o AWS Management Console](#). No Console de Gerenciamento da AWS, você pode navegar até o Console do AWS Systems Manager e OpsCenter, para saber mais, consulte [Gerenciador de AWS Systems Manager sessões](#). OpsCenter também fornece uma API que você pode usar; para obter informações, consulte [Saiba mais sobre OpsCenter](#).

OpsCenter é um recurso com preço de aproximadamente 1000 dólares OpsItems que custa menos de \$10. Para obter mais informações, consulte [Definição de preço do AWS Systems Manager](#).

Notificações de alerta do AMS

Como parte do processamento do alerta, com base na análise de impacto, o AWS Managed Services (AMS) cria um incidente e inicia o processo de gerenciamento de incidentes para remediação, quando o impacto pode ser determinado. Caso o impacto não possa ser determinado, o AMS envia uma notificação de alerta para o endereço de e-mail associado à sua conta por meio de uma notificação de serviço; consulte o diagrama da arquitetura de monitoramento do AMS para ver o processo de tratamento de alertas em [Como funciona o monitoramento](#).

Recebendo alertas gerados pelo AMS

O AWS Managed Services (AMS) permite que você receba notificações de alerta diretamente para EC2 os recursos da Amazon para reduzir os atrasos na comunicação. Para receber EC2 alertas da Amazon diretamente, inscreva seu alvo (e-mail preferencial) no tópico Direct-Customer-Alerts do Amazon SNS usando o tipo de alteração Gerenciamento | Monitoramento e notificação | SNS | Subscribe (ct-3rc19u1k017wu).

Note

Nem todos os alertas de linha de base são enviados para o tópico Alertas diretos do cliente por padrão. Para ver todos os alertas gerados pelo sistema de monitoramento AMS, assine o tópico Amazon SNS para o sistema de monitoramento AMS. Na solicitação, solicite o “Tópico de monitoramento do AMS”, especifique um canal de assinatura para receber os alertas (Lambda, Amazon SQS, HTTP/S, e-mail ou SMS) e especifique os endpoints (por exemplo, endereços de e-mail, se você escolher o protocolo de e-mail) que receberão os alertas. O tópico de monitoramento do AMS recebe alertas que são usados pelos serviços compartilhados do AMS, portanto, pode ser ruidoso.

Para saber mais, consulte a seção [Inscrever-se](#) na referência da API de assinatura do Amazon Simple Notification Service.

Para obter uma lista dos alertas básicos fornecidos pelo AMS, consulte [Alertas do monitoramento de linha de base no AMS](#).

Notificações de alerta baseadas em tags no AMS

Use tags para enviar notificações de alerta de seus recursos para diferentes endereços de e-mail. É uma prática recomendada usar notificações de alerta baseadas em tags, pois as notificações enviadas para um único endereço de e-mail podem causar confusão quando várias equipes de desenvolvedores usam a mesma conta.

Important

As notificações de alerta baseadas em tags só funcionam para notificações relacionadas à Amazon EC2, Amazon EBS, Elastic Load Balancing, Network Load Balancer, Application Load Balancer, Amazon RDS, Amazon Redshift e. OpenSearch

Não adicione informações de identificação pessoal (PII) em suas tags.

Enviar alertas para um endereço de e-mail específico

Marque os recursos que têm alertas que devem ser enviados para um endereço de e-mail específico com `okey = OwnerTeamEmail,value = EMAIL_ADDRESS`.

Envie alertas para vários endereços de e-mail

Para usar vários endereços de e-mail, especifique uma lista de valores separados por vírgula.

Por exemplo, `key = OwnerTeamEmail,value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, . . .`. O número total de caracteres para o campo de valor não pode exceder 260.

Use uma chave de tag personalizada

Para usar uma chave de tag personalizada, forneça o nome da chave de tag personalizada ao seu CSDM em um e-mail fornecendo consentimento para ativar a notificação automática para a comunicação baseada em tag. É uma prática recomendada usar a mesma estratégia de marcação para tags de contato em todas as suas instâncias e recursos.

O endereço de e-mail deve ser especificado por completo, com o “sinal de arroba” (@) para separar a parte local do domínio. Exemplos de endereços de e-mail inválidos: `Team.AppATabc.xyz` ou `john.doe`. Para obter orientação geral sobre sua estratégia de marcação, consulte [Uso de tags](#). Para marcar um recurso existente, envie uma RFC com o tipo de alteração Deployment | Advanced stack components | Tag | Create (auto) (ct-3cx7we852p3af).

Note

O valor chave `OwnerTeamEmail` não precisa estar em camel case. No entanto, as tags diferenciam maiúsculas de minúsculas e é uma prática recomendada usar o formato recomendado.

Remediação automática de alertas pelo AMS

Após a verificação, o AWS Managed Services (AMS) corrige automaticamente determinados alertas de acordo com condições e processos específicos descritos nesta seção.

Nome do alerta	Descrição	Limites	Ação
Canal seguro quebrado	O alarme Broken Secure Channel é acionado nas EC2 instâncias do Windows quando a instância perde a conexão com o controlador de domínio AD.	O limite está acima do valor definido 10 vezes nos últimos 15 minutos.	A correção automática do AMS valida se a instância está on-line no SSM, o nome do host não está duplicado e se o objeto de computador do AD está alinhado com a pilha. CloudFormation A correção repara a conexão segura do canal para restaurar o acesso à instância.
Falha ao verificar status	Possíveis falhas de hardware ou um estado de falha da instância.	O sistema detectou um status de falha pelo menos uma vez nos últimos 15 minutos.	A remediação automática do AMS primeiro valida se a instância está acessível. Se a instância estiver inacessível, ela será interrompida e reiniciada. O stop and start permite que a instância migre para um novo hardware subjacente. Para obter mais informações, consulte a seção a seguir "Automação de remediação de falhas na verificação de EC2 status".
AMSLinuxDiskUsage	Acione quando o uso do disco de 1 ponto de montagem (espaço	O limite está acima do valor definido 6 vezes nos últimos 30 minutos.	A remediação automática do AMS primeiro exclui os arquivos temporários

Nome do alerta	Descrição	Limites	Ação
	designado em um volume) na sua EC2 instância estiver sendo preenchido.		os. Se isso não liberar espaço em disco suficiente, ele estende o volume para evitar tempo de inatividade se o volume ficar cheio.
AMSWindow sDiskUsage	Quando o uso do disco de 1 ponto de montagem (espaço designado em um volume) na sua EC2 instância está se esgotando.	O limite está acima do valor definido 6 vezes nos últimos 30 minutos.	A remediação automática do AMS primeiro exclui os arquivos temporários. Se isso não liberar espaço em disco suficiente, ele estende o volume para evitar tempo de inatividade se o volume ficar cheio.

Nome do alerta	Descrição	Limites	Ação
RDS-EVENT-0089	A instância de banco de dados consumiu mais de 90% do armazenamento alocado.	O armazenamento é mais de 90% alocado.	A remediação automática do AMS primeiro valida se o banco de dados está em um estado modificável e disponível ou com armazenamento cheio. Em seguida, ele tenta aumentar o armazenamento alocado, o IOPS e a taxa de transferência de armazenamento por meio de um conjunto de alterações. CloudFormation Se o desvio da pilha já for detectado, ele retornará à API do RDS para evitar o tempo de inatividade. Esse recurso pode ser desativado adicionando a seguinte tag à instância de banco de dados do RDS: "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Nome do alerta	Descrição	Limites	Ação
RDS-EVENT-0007	O armazenamento alocado para a instância de banco de dados foi esgotado. Para resolver, aloque armazenamento adicional.	O armazenamento é 100% alocado.	A remediação automática do AMS primeiro valida se o banco de dados está em um estado modificável e disponível ou com armazenamento cheio. Em seguida, ele tenta aumentar o armazenamento alocado, o IOPS e a taxa de transferência de armazenamento por meio de um conjunto de alterações. CloudFormation Se o desvio da pilha já for detectado, ele retornará à API do RDS para evitar o tempo de inatividade. Esse recurso pode ser desativado adicionando a seguinte tag à instância de banco de dados do RDS: "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Nome do alerta	Descrição	Limites	Ação
RDS-EVENT-0224	O armazenamento alocado solicitado atinge ou excede o limite máximo de armazenamento configurado.	O limite máximo de armazenamento para a instância de banco de dados foi esgotado ou é maior ou igual ao armazenamento alocado solicitado.	A remediação automática do AMS primeiro valida se a quantidade solicitada de armazenamento do RDS ultrapassará o limite máximo de armazenamento. Se confirmado, o AMS tenta aumentar o limite máximo de armazenamento em 30% com um CloudFormation conjunto de alterações ou uma API direta do RDS se os recursos não forem provisionados. CloudFormation Esse recurso pode ser desativado adicionando a seguinte tag à instância de banco de dados do RDS: "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Nome do alerta	Descrição	Limites	Ação
Capacidade de armazenamento RDS	Restam menos de 1 GB no armazenamento alocado para a instância de banco de dados.	O armazenamento é alocado em 99%.	A remediação automática do AMS primeiro valida se o banco de dados está em um estado modificável e disponível ou com armazenamento cheio. Em seguida, ele tenta aumentar o armazenamento alocado, o IOPS e a taxa de transferência de armazenamento por meio de um conjunto de alterações. CloudFormation Se o desvio da pilha já for detectado, ele retornará à API do RDS para evitar o tempo de inatividade. Esse recurso pode ser desativado adicionando a seguinte tag à instância de banco de dados do RDS: "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Amazon EC2 Broken Secure Channel: nota de automação de remediação

Antes que a remediação automática do AWS Managed Services (AMS) realize a correção dos problemas EC2 do Amazon Windows Broken Secure Channel, a automação realiza as seguintes verificações prévias e cria um relatório de incidentes para investigação adicional:

- Valida se o status do SSM da EC2 instância Amazon é “Online”.
- Valida se a EC2 instância da Amazon faz parte de um grupo de Auto Scaling e se todas as instâncias do grupo Auto Scaling têm o mesmo nome de host.
- Verifica se a EC2 instância da Amazon faz parte da CloudFormation pilha usada para provisioná-la. Se a instância tiver sido removida da CloudFormation pilha, a automação verifica se a Unidade Organizacional (OU) do Active Directory associada ainda está fazendo referência à pilha.

Após a aprovação das validações acima, a automação prossegue para corrigir o canal Broken Secure.

Etapas de remediação:

- A correção automática tenta reparar o canal seguro entre a EC2 instância e o domínio AD, restaurando o acesso à instância.
- Após a remediação, a automação verifica se o canal seguro foi estabelecido. Se não for bem-sucedido, o AMS cria um incidente e envolve as operações do AMS para investigar.

EC2 falha na verificação de status: notas de automação de remediação

Como a remediação automática do AMS funciona com problemas de falha na verificação de EC2 status:

- Se sua EC2 instância da Amazon estiver inacessível, ela deverá ser interrompida e iniciada novamente para que possa ser migrada para um novo hardware e recuperada.
- Se a raiz do problema estiver no sistema operacional (dispositivos ausentes no fstab, corrupção do kernel etc.), a automação não conseguirá recuperar sua instância.
- Se sua instância pertencer a um grupo de Auto Scaling, a automação não tomará nenhuma ação — a ação de AutoScalingGroup escalabilidade substitui a instância.
- Se sua instância tiver a recuperação EC2 automática ativada, a correção não será executada.

EC2 automação de remediação de uso de volume

Como a remediação automática do AWS Managed Services (AMS) funciona com problemas de uso EC2 de volume:

- A automação primeiro valida se a expansão do volume é necessária e se ela pode ser executada. Se a expansão for considerada apropriada, a automação pode aumentar a capacidade do volume. Esse processo automatizado equilibra a necessidade de crescimento com uma expansão controlada e limitada.
- Antes de estender um volume, a automação executa tarefas de limpeza (Windows: Disk Cleaner, Linux: Logrotate + Simple Service Manager Agent Log, remoção do log) na instância para tentar liberar espaço.

Note

As tarefas de limpeza não são executadas em instâncias da família EC2 “T” devido à dependência de créditos de CPU para funcionalidade contínua.

- No Linux, a automação só suporta a extensão de sistemas de arquivos do tipo EXT2 EXT3, EXT4 e XFS.
- No Windows, a automação só oferece suporte ao New Technology File System (NTFS) e ao Resilient File System (ReFS).
- A automação não estende os volumes que fazem parte do Logical Volume Manager (LVM) ou de uma matriz RAID.
- A automação não amplia os volumes de armazenamento de instâncias.
- A automação não age se o volume afetado já for maior que 2 TiB.
- A expansão por meio da automação é limitada a um máximo de três vezes por semana e cinco vezes no total durante a vida útil do sistema.
- A automação não expande o volume se a expansão anterior ocorreu nas últimas seis horas.

Quando essas regras impedem a automação de agir, o AMS entra em contato com você por meio de uma solicitação de serviço de saída para determinar as próximas ações a serem tomadas.

Automação de remediação de eventos de baixo armazenamento do Amazon RDS

Como a remediação automática do AWS Managed Services (AMS) funciona com problemas de eventos de baixo armazenamento do Amazon RDS:

- Antes de tentar estender o armazenamento da instância do Amazon RDS, a automação executa várias verificações para garantir que a instância do Amazon RDS esteja em um estado modificável e disponível, ou com armazenamento cheio.
- Quando o desvio da CloudFormation pilha é detectado, a remediação ocorre por meio da API do Amazon RDS.
- A ação de remediação não é executada nos seguintes cenários:
 - O status da instância do Amazon RDS não é “disponível” ou “com armazenamento cheio”.
 - O armazenamento da instância do Amazon RDS não é modificável no momento (como quando o armazenamento foi modificado nas últimas seis horas).
 - A instância do Amazon RDS tem armazenamento com escalabilidade automática habilitado.
 - A instância do Amazon RDS não é um recurso dentro de uma CloudFormation pilha.
- A remediação é limitada a uma expansão por seis horas e não mais do que três expansões em um período contínuo de quatorze dias.
- Quando esses cenários ocorrem, o AMS entra em contato com você com um incidente de saída para determinar as próximas ações.

Criação de CloudWatch alarmes adicionais no AMS

Você pode criar novos CloudWatch alarmes usando o tipo de alteração AWS Managed Services (AMS) Deployment | Monitoring and notification CloudWatch | | Create alarmes.

Important

O AMS não monitora CloudWatch os alarmes criados por você.

Usando CloudWatch métricas e alarmes personalizados para EC2 instâncias da Amazon (funciona somente para implantações mutáveis que não dependem de implantações atualizadas em grupos do AMIs Auto Scaling):

1. Produza seu script de monitoramento de aplicativos e sua métrica personalizada. Para obter mais informações e acesso a exemplos de scripts, consulte [Monitoramento de memória e métricas de disco para instâncias EC2 Linux da Amazon](#). Os scripts de CloudWatch monitoramento da Amazon para EC2 instâncias Linux da Amazon demonstram como produzir e consumir métricas CloudWatch personalizadas da Amazon. Esses scripts Perl de amostra formam um exemplo

- totalmente funcional que relata métricas de utilização de memória, swap e espaço em disco para uma instância do Linux.
2. Faça o upload do seu script de monitoramento. Para carregar o script de monitoramento para seu grupo de Auto Scaling ou configuração de EC2 instância da Amazon, você pode usá-lo UserData ao configurar seu grupo de Auto Scaling ou instância da EC2 Amazon, ou, se seu aplicativo foi implantado CodeDeploy com, você pode modificar a configuração com um Deployment | Applications | application | Deploy CT (CodeDeploy ct-2edc3sd1sqmrb).
 3. Publique sua métrica personalizada em CloudWatch (na primeira vez que você publica um ponto de dados para uma nova métrica personalizada, ela é criada), consulte [Publicação de métricas personalizadas](#).
 4. Crie o CloudWatch alarme, consulte [Criar um CloudWatch alarme para uma instância](#).

 Important

Os dados de monitoramento devem ser enviados para esse caminho [infra/INSTANCE_ID/YOUR_CUSTOM_METRIC]

Para modificar ou excluir um CloudWatch alarme, envie uma RFC com o campo Management | Other | Other | Create Change type (ct-1e1xtak34nx76) com os parâmetros necessários para concluir a ação, conforme descrito na referência da API da Amazon. CloudWatch [PutMetricAlarm](#)

Você pode usar o stream do CloudWatch evento. O AMS está integrado CloudWatch e você pode solicitar que qualquer chamada de API da AWS acione um CloudWatch evento.

Para fazer isso, envie um relatório Gerenciamento | Outro | Outro | Atualize o CT (ct-0xdawir96cy7k) com as chamadas de API nas quais você está interessado. Um operador de AMS conversará com você para reunir os requisitos. Para saber mais, consulte a [CloudWatch documentação da Amazon](#).

Para ter acesso ao stream do CloudWatch evento, envie um tópico Gerenciamento | Outro | Outro | Atualize o CT (ct-0xdawir96cy7k) para adicionar uma pessoa ao tópico de notificação do SNS. Um operador de AMS conversará com você para reunir os requisitos.

Criação de CloudWatch métricas e alarmes personalizados no AMS

Você pode armazenar suas métricas de negócios e aplicativos na Amazon CloudWatch. Você pode visualizar gráficos e definir alarmes com base nessas métricas, assim como você pode ver as métricas que CloudWatch já estão armazenadas para seus recursos do AWS Managed Services (AMS). Para saber mais sobre isso CloudWatch, consulte [Amazon CloudWatch Concepts](#).

O Amazon SNS permite que os aplicativos enviem mensagens urgentes para vários assinantes por meio de um mecanismo “push” contra o AMS Managed Monitoring System ou MMS, tópico do Amazon SNS (SNS) no qual os alarmes são publicados; nesse caso, MMS e suas filas SQS. Você pode usar CloudWatch para criar métricas personalizadas e, por meio de um tópico do SNS, fazer com que o AMS o avise adequadamente. Para isso, siga estas etapas.

Note

Esse processo não funciona para implantações imutáveis que dependem de implantações atualizadas em grupos de AMLs Auto Scaling, ele é adequado para implantações de aplicativos mutáveis (não ASG).

Configurar uma métrica personalizada dentro das limitações do AMS Advanced é uma tarefa complexa. Para obter um exemplo de CloudWatch, consulte [Exemplo: Contar ocorrências de um termo](#).

1. Produza seu script de monitoramento de aplicativos e sua métrica personalizada (como o exemplo de contagem de ocorrências). Para obter mais informações e acesso a exemplos de scripts, consulte [Monitoramento de memória e métricas de disco para instâncias EC2 Linux da Amazon](#).
2. Faça o upload do seu script de monitoramento. Para carregar o script de monitoramento para seu grupo de Auto Scaling ou configuração de EC2 instância da Amazon, você pode usá-lo UserData ao configurar seu grupo de Auto Scaling ou instância da EC2 Amazon, ou, se seu aplicativo foi implantado CodeDeploy com, você pode modificar a configuração com um Deployment | Applications | application | Deploy CT (CodeDeploy ct-2edc3sd1sqmrb).
3. Publique sua métrica personalizada em CloudWatch (na primeira vez que você publica um ponto de dados para uma nova métrica personalizada, ela é criada), consulte [Publicar métricas personalizadas](#).

4. Para integrar sua métrica de cliente ao seu sistema de monitoramento de aplicativos, solicite que o AMS crie um tópico de SNS para a métrica enviando uma RFC com a seção Implantação | Monitoramento e notificação | SNS | Criar tipo de alteração (ct-3dfnglm4ombbs).
5. Crie o CloudWatch alarme, consulte [Criação de CloudWatch alarmes na Amazon](#).

 Important

Os dados de monitoramento devem ser enviados para esse caminho [infra/*INSTANCE_ID/YOUR_CUSTOM_METRIC*].

Usando o CloudWatch Application Insights para servidores do .Net e SQL no AMS

Você pode usar o Amazon CloudWatch Application Insights para configurar os monitores dos seus recursos de aplicativos do AWS Managed Services (AMS) para analisar continuamente os dados em busca de sinais de problemas com seus aplicativos e reduzir o tempo médio de reparo (MTTR) ao solucionar problemas do aplicativo. Para obter detalhes sobre o CloudWatch Application Insights, consulte [CloudWatch Application Insights para .NET e SQL Server](#).

 Important

O AMS não monitora problemas do CloudWatch Application Insights porque eles são para códigos de aplicativos controlados por você.

Para usar o CloudWatch Application Insights, envie uma RFC com os componentes Deployment | Advanced stack components | Identity and Access Management (IAM) | Crie o tipo de alteração de entidade ou política (revisão obrigatória) (ct-3dpd8mdd9jn1r) com uma solicitação para criar uma função do IAM que forneça permissão para configurar o Application Insights. CloudWatch Há duas opções para receber os problemas identificados: por meio de um tópico do SNS ou com um alvo nas regras do CloudWatch evento. No RFC, especifique o que você deseja. Se você planeja usar regras de CloudWatch eventos, especifique também a definição da regra na RFC. Depois de configurar o CloudWatch Application Insights, você recebe um aviso de possíveis problemas, incluindo insights que apontam para uma possível causa raiz.

Para saber como você pode assumir a função, consulte o Guia de integração do AMS [Federe seu Active Directory com as funções do AMS IAM](#).

Usando as regras EventBridge gerenciadas da Amazon no AMS

O AMS Advanced usa o Amazon EventBridge Managed Rules. Uma regra gerenciada é um tipo exclusivo de regra diretamente vinculada ao AMS. Essas regras combinam os eventos recebidos e os enviam aos alvos para processamento. As regras gerenciadas são predefinidas pelo AMS e incluem padrões de eventos exigidos pelo serviço para gerenciar contas de clientes e, a menos que definido de outra forma, somente o serviço proprietário pode utilizar essas regras gerenciadas.

As regras gerenciadas do AMS estão vinculadas ao principal `events.managedservices.amazonaws.com` de serviço. Essas regras gerenciadas são gerenciadas por meio da função [AWSServiceRoleForManagedServices_Eventsvinculada ao serviço](#). Para excluir essas regras, é necessária uma confirmação especial do cliente. Para obter mais informações, consulte [Excluindo regras gerenciadas para o AMS](#).

Para obter mais informações sobre regras, consulte [Regras](#) no Guia do EventBridge usuário da Amazon.

Amazon EventBridge Managed Rules implantadas pelo AMS

Regras EventBridge gerenciadas da Amazon

Nome da regra	Descrição	Definição
AMSAdvancedCoreRule	Essa regra encaminha os Amazon CloudWatch Alarms para o AMS Monitoring. Os CloudWatch eventos da Amazon	<pre>{ { "source": ["aws.cloudwatch"], "detail-type": ["CloudWatch Alarm State Change"], } }</pre>

Nome da regra	Descrição	Definição
	monitoram os CloudWatch alarmes.	

Criação de regras gerenciadas para AMS

Você não precisa criar manualmente as Amazon EventBridge Managed Rules. Quando você se integra ao AMS no AWS Management Console AWS CLI, no ou na AWS API, o AMS os cria para você.

Editando regras gerenciadas para AMS

O AMS não permite que você edite as regras gerenciadas. O nome e o padrão de evento para cada regra gerenciada são predefinidos pelo AMS.

Excluindo regras gerenciadas para AMS

Você não precisa excluir manualmente as regras gerenciadas. Quando você se desconecta do AMS no AWS Management Console, no ou na AWS API AWS CLI, o AMS limpa os recursos e exclui todas as regras gerenciadas de propriedade do AMS para você.

Caso o AMS não remova as regras gerenciadas durante a desativação, você também pode usar o EventBridge console da Amazon AWS CLI ou a AWS API para excluir manualmente as regras gerenciadas. Para fazer isso, você deve primeiro sair do AMS e realizar uma exclusão forçada das Regras Gerenciadas.

Remediador confiável no AMS

O Trusted Remediator é uma solução do AWS Managed Services que automatiza a remediação e as recomendações. [AWS Trusted Advisor](#)[AWS Compute Optimizer](#) O Trusted Remediator cria recomendações quando Trusted Advisor e o Compute Optimizer indicam oportunidades para você reduzir custos, melhorar a disponibilidade do sistema, otimizar o desempenho ou fechar lacunas de segurança. Contas da AWS Com o Trusted Remediator, você pode abordar essas recomendações de segurança, desempenho, otimização de custos, tolerância a falhas e limite

de serviço de uma forma segura e padronizada que usa as melhores práticas estabelecidas. O Trusted Remediator permite que você configure uma solução de remediação e seja executada automaticamente de acordo com um cronograma criado por você, simplificando o processo de remediação. Essa abordagem simplificada aborda os problemas de forma consistente, eficiente e sem intervenção manual.

Principais benefícios do Trusted Remediator

A seguir estão os principais benefícios do Trusted Remediator:

- **Segurança, desempenho e otimização de custos aprimorados:** o Trusted Remediator ajuda você a aprimorar a postura geral de segurança de suas contas, otimizar a utilização de recursos e reduzir os custos operacionais.
- **Configuração e configuração de autoatendimento:** você pode configurar o Trusted Remediator de acordo com seus requisitos e preferências.
- **Trusted Advisor Verificações automatizadas e correção de AWS Compute Optimizer recomendações:** após a configuração, o Trusted Remediator executa automaticamente as ações de remediação para as verificações selecionadas. Essa automação elimina a necessidade de intervenção manual.
- **Implementação das melhores práticas:** as ações de remediação são baseadas nas melhores práticas estabelecidas, portanto, os problemas são tratados de forma padronizada e eficaz.
- **Execução programada:** você pode escolher o cronograma de remediação que se alinha aos seus fluxos de trabalho day-to-day operacionais.

O Trusted Remediator permite que você resolva proativamente os problemas identificados em seus AWS ambientes, ajudando você a aderir às melhores práticas e a manter uma infraestrutura de nuvem segura, de alto desempenho e econômica.

Como funciona o Trusted Remediator

A seguir está uma ilustração do fluxo de trabalho do Trusted Remediator:

O Trusted Remediator avalia as recomendações Trusted Advisor e o Compute Optimizer para você e cria em. Contas da AWS AWS Systems Manager [OpsItems](#) OpsCenter Em seguida, você pode usar os documentos de automação do Trusted Remediator para corrigir o problema de OpsItems forma automática ou manual. A seguir estão os detalhes de cada tipo de remediação:

- Remediação automatizada: o Trusted Remediator executa o documento de automação e monitora a execução. Após a conclusão do documento de automação, o Trusted Remediator resolve o OpsItem.
- Remediação manual: o Trusted Remediator cria o OpsItem para você revisar. Depois de revisar, você pode criar um RFC automatizado, [Trusted Remediator | Finding | Remediate](#), alterar o tipo para remediar o recurso. Para obter informações sobre as etapas de remediação manual, consulte [Execute correções manuais no Trusted Remediator](#).

Os registros de remediação são armazenados em um bucket do Amazon S3. Você pode usar os dados no bucket do S3 para criar QuickSight painéis personalizados para relatórios. O AMS também fornece relatórios mediante solicitação para o Trusted Remediator. Para receber esses relatórios, entre em contato com seu CSDM.

Termos-chave para Trusted Remediator

A seguir estão os termos que são úteis para conhecer quando você usa o Trusted Remediator no AMS:

- AWS Trusted Advisor e AWS Compute Optimizer: Serviços de otimização de nuvem fornecidos pela AWS. Trusted Advisor e o Compute Optimizer inspecionam AWS seu ambiente e fornecem recomendações com base nas melhores práticas nas seis categorias a seguir:
 - Otimização de custo
 - Desempenho
 - Segurança
 - Tolerância a falhas
 - Excelência operacional
 - Limites do serviço

Para obter mais informações, consulte [AWS Trusted Advisor](#) e [AWS Compute Optimizer](#).

- Trusted Remediator: uma solução de remediação do AMS para [Trusted Advisor](#) verificações e [AWS Compute Optimizer](#) recomendações. O Trusted Remediator ajuda você a corrigir com segurança as Trusted Advisor verificações e as recomendações do Compute Optimizer com as melhores práticas conhecidas para melhorar a segurança, o desempenho e reduzir custos. O Trusted Remediator é fácil de instalar e configurar. Você configura uma vez e o Trusted Remediator executa as correções de acordo com sua programação preferida (diária ou semanal).

- **AWS Systems Manager Documento SSM:** um arquivo JSON ou YAML que define as ações que são AWS Systems Manager executadas em seus recursos. AWS O documento SSM serve como uma especificação declarativa para automatizar tarefas operacionais em vários AWS recursos e instâncias.
- **AWS Systems Manager OpsCenter OpsItem:** um recurso de gerenciamento de problemas operacionais na nuvem que ajuda você a rastrear e resolver problemas operacionais em seu AWS ambiente. OpsItems forneça uma visão centralizada e um sistema de gerenciamento para dados operacionais e problemas em todos Serviços da AWS os recursos. Cada um OpsItem representa um problema operacional, como um potencial risco de segurança, um problema de desempenho ou um incidente operacional.
- **Configuração:** Uma configuração é um conjunto de atributos armazenados em [AWS AppConfig, uma capacidade de AWS Systems Manager](#). O aplicativo Trusted Remediator AWS AppConfig ajuda a configurar remediações no nível da conta.
- **Modo de execução:** o modo de execução é um atributo de configuração que determina como executar a correção para cada resultado da Trusted Advisor verificação. Há quatro modos de execução suportados: automatizado, manual, condicional e inativo.
- **Substituição de recursos:** esse recurso usa tags de recursos para substituir uma configuração para recursos específicos.
- **Registro do item de remediação:** um arquivo de log no bucket de log de remediação do Trusted Remediator S3. O registro do item de remediação é criado quando a remediação OpsItems é criada. Esse arquivo de log contém remediação de execução manual OpsItems e remediação de execução automatizada. OpsItems Use esse arquivo de log para rastrear todos os itens de remediação.
- **Registro de execução de remediação automatizada:** um arquivo de log no bucket de log de remediação do Trusted Remediator S3. O registro automatizado de execução de remediação é criado quando a execução automatizada de um documento SSM é concluída. Esse registro contém detalhes da execução do SSM para remediação OpsItems automática da execução. Use esse arquivo de log para rastrear remediações automatizadas.

Comece a usar o Trusted Remediator no AMS

O Trusted Remediator está disponível no AMS sem custo adicional. O Trusted Remediator oferece suporte a configurações de conta única e de várias contas.

Integrado ao Trusted Remediator

Para integrar suas contas do AMS ao Trusted Remediator, envie um e-mail para seus arquitetos de nuvem ou gerentes de entrega de serviços em nuvem (CSDMs). No e-mail, inclua as seguintes informações:

- Contas da AWS: O número de identificação da conta de doze dígitos. Todas as contas que você deseja integrar ao Trusted Remediator devem pertencer ao mesmo cliente do AMS Advanced.
- Conta de administrador delegado: a conta que é usada para verificar a configuração Trusted Advisor de uma ou várias contas do Compute Optimizer.
- Contas de membros: são as contas vinculadas à conta de administrador delegado. Essas contas herdam as configurações da conta de administrador delegado. Você pode ter uma conta de membro ou várias contas de membros.

Note

As contas dos membros herdam as configurações da conta do administrador delegado. Se você precisar de configurações diferentes para contas específicas, integre várias contas de administrador delegado com suas configurações preferidas. Planeje a estrutura da conta e as configurações com seus arquitetos de nuvem antes de embarcar.

- Região da AWS: Região da AWS Onde seus recursos estão localizados. Para obter uma lista de Regiões da AWS, consulte [Serviços da AWS por região](#).
- Cronograma e horário de remediação: seu cronograma de remediação preferido (diário ou semanal). O Trusted Remediator reúne as Trusted Advisor verificações e inicia a remediação no horário programado. Por exemplo, você pode definir o cronograma de remediação para 1h da manhã de domingo de cada semana, horário padrão do leste da Austrália.
- E-mail de notificação: o Trusted Remediator usa o e-mail de notificação para notificá-lo diariamente se houver remediações. O assunto do e-mail de notificação é “Resumo da remediação do Trusted Remediator” e o conteúdo fornece informações sobre as remediações do Trusted Remediator executadas nas últimas 24 horas.

Note

Analise seus aplicativos e recursos após cada remediação programada. Para obter suporte adicional, entre em contato com a AMS.

Depois de enviar sua solicitação de integração com os detalhes necessários para sua CA ou CSDM, o AMS integra suas contas ao Trusted Remediator. O Trusted Remediator usa AWS AppConfig um recurso de AWS Systems Manager, para definir a configuração das Trusted Advisor verificações. Essas configurações são um conjunto de atributos armazenados em AWS AppConfig. Para evitar cobranças não autorizadas em seus recursos, todas as Trusted Advisor verificações suportadas são definidas como Inativas quando as contas são integradas ao Trusted Remediator. Essas configurações ajudam você a corrigir automaticamente Trusted Advisor verificações específicas ou a avaliar e corrigir manualmente as verificações restantes. As configurações são altamente personalizáveis, permitindo que você aplique configurações para cada verificação. Trusted Advisor Para obter mais informações, consulte [Configurar Trusted Advisor a correção de cheques no Trusted Remediator](#).

Configure o Trusted Remediator em seu Contas da AWS

Quando a integração estiver concluída, sua CA ou CDSM notificará você e as configurações padrão serão criadas em seu administrador delegado. Conta da AWS A configuração é AWS AppConfig armazenada no aplicativo Trusted Remediator. Você pode usar o RFC [Management | Trusted Remediator | Remediation configuration | Update](#) para solicitar atualizações de configuração. Para obter mais informações, consulte [Configurar Trusted Advisor a correção de cheques no Trusted Remediator](#).

Para visualizar as configurações padrão do Trusted Remediator, conclua as seguintes etapas:

1. Abra o AWS Systems Manager console em <https://console.aws.amazon.com/systems-manager/>.

Note

Verifique se você está na conta de administrador delegado.

2. Escolha Gerenciamento de aplicativos, AppConfig.
3. Selecione Trusted Remediator na lista de aplicativos.

Veja a seguir um exemplo do AWS AppConfig console mostrando as configurações do Trusted Remediator:

Escolha as verificações e recomendações a serem corrigidas

Por padrão, o modo de execução de remediação é inativo para todas as Trusted Advisor verificações e recomendações do Compute Optimizer em sua configuração. Isso evita a remediação não autorizada e protege os recursos. O AMS fornece documentos de automação SSM selecionados para remediação de Trusted Advisor cheques.

Para selecionar as verificações que você deseja corrigir com o Trusted Remediator, conclua as seguintes etapas:

1. Analise a lista de [recomendações suportadas Trusted Advisor e do Compute Optimizer ou o nome dos documentos de automação SSM associados](#) para decidir quais verificações e recomendações você deseja corrigir com o Trusted Remediator.
2. Envie uma solicitação [de gerenciamento | Trusted Remediator | Configuração de remediação | Atualização](#) para atualizar a configuração das verificações selecionadas Trusted Advisor . Para obter instruções sobre como selecionar cheques, consulte [Configurar Trusted Advisor a correção de cheques no Trusted Remediator](#).

Acompanhe suas remediações no Trusted Remediator

Depois de atualizar sua configuração em nível de conta, o Trusted Remediator cria OpsItems para cada remediação. O Trusted Remediator executa o documento SSM para remediação automatizada de OpsItems acordo com seu cronograma de remediação. Para obter instruções sobre como visualizar todas as correções no OpsCenter console OpsItems do Systems Manager, consulte [Rastreie as remediações no Trusted Remediator](#).

Execute correções manuais no Trusted Remediator

Você pode corrigir manualmente as Trusted Advisor verificações usando um RFC automatizado. Quando você escolhe a remediação manual, o Trusted Remediator cria uma execução manual. OpsItem Para obter mais informações, consulte [Execute correções manuais no Trusted Remediator](#).

Recomendações do Compute Optimizer suportadas pelo Trusted Remediator

A tabela a seguir lista as recomendações suportadas do Compute Optimizer, os documentos de automação do SSM, os parâmetros pré-configurados e o resultado esperado dos documentos de automação. Analise o resultado esperado para ajudá-lo a entender os possíveis riscos com base nos

requisitos de sua empresa antes de habilitar um documento de automação de SSM para remediação de cheques.

Certifique-se de que a regra de configuração correspondente para cada verificação do Compute Optimizer esteja presente nas verificações suportadas para as quais você deseja habilitar a correção. Para obter mais informações, consulte [Aceitar AWS Compute Optimizer Trusted Advisor cheques](#).

Opção de otimização	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados

Redimensionamento

Recomendações de EC2 instâncias da Amazon	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation Tipo de EC2 instância da Amazon atualizado de acordo com as recomendações do Compute Optimizer. As opções mais ideais são escolhidas mantendo os mesmos parâmetros da plataforma (arquitetura, hipervisor, interface de rede, tipo de virtualização etc.), se a opção existir.	• MinimumDaysSinceLastChange: o parâmetro para especificar o número mínimo de dias desde a última alteração do tipo de instância. O padrão são 7 dias. Sem restrições • Criar AMIBefore redimensionamento: para criar a AMI da instância como backup antes do redimensionamento, defina como "Verdadeiro". Para não criar um backup, defina como 'False'. O padrão é 'Verdadeiro'. Sem restrições
Recomendações de volume do Amazon EBS	AWSManagedServices-ModifyEBSVolume O volume do Amazon EBS é modificado de acordo com as recomendações do Compute Optimizer. A modificação pode incluir tipo de volume, tamanho, IOPS, geração de volume (gp2, gp3 etc.).	• CreateSnapshot: para criar um instantâneo antes de modificar o volume, defina como "Verdadeiro". Para não criar um instantâneo, defina como 'False'. O padrão é "Verdadeiro". Sem restrições

Opção de otimização	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
		• VolumeType: O tipo de volume desejado. Se nenhum tipo for especificado, o tipo existente será mantido. Sem restrições • VolumeSize: o tamanho desejado do volume, em GiB. O tamanho do volume de destino deve ser maior ou igual ao tamanho existente do volume. Se nenhum tamanho for especificado, o tamanho existente será mantido. Sem restrições • Iops: o número solicitado de I/O operações por segundo (IOPS). Esse parâmetro só é válido para volumes io1, io2 e gp3. Sem restrições • Taxa de transferência: a taxa de transferência para provisionar um volume, com um máximo de 1000 MiB/s. Esse parâmetro é válido somente para volumes gp3. Sem restrições • RemediateStackDrift: Para iniciar a correção do desvio, se algum desvio for causado pela modificação do volume, defina como “Verdadeiro”. Para não tentar

Opção de otimização	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
		remediar o desvio, defina como 'False'. O padrão é 'Verdadeiro'. Sem restrições
Recomendações da função Lambda	AWSManagedServices-TrustedRemediatorOptimizeLambdaMemory AWS Lambda memória de função otimizada de acordo com as recomendações do Compute Optimizer.	RecommendedMemorySize : tamanho de memória personalizado, se diferente das opções recomendadas. Sem restrições

Recursos ociosos

Volume inativo do Amazon EBS	AWSManagedServices-DeleteUnusedEBSVolume O volume Amazon EBS não anexado será excluído.	• CreateSnapshot: para criar um instantâneo antes de excluir o volume, defina como “Verdadeiro”. Para não criar um instantâneo, defina como 'False'. O padrão é “Verdadeiro”. Sem restrições • MinimumUnattachedDays: Mínimo de dias não vinculados do volume do Amazon EBS a serem excluídos, até 62 dias. O padrão é 7. Sem restrições

Opção de otimização	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Instância inativa da Amazon EC2	AWSManagedServices-StopEC2 instâncias A EC2 instância inativa da Amazon será interrompida.	ForceStopWithInstanceStore: para forçar a interrupção de instância usando o armazenamento de instâncias, defina como "Verdadeiro". Para não forçar a parada, defina como 'False'. O valor padrão 'False' impede que a instância pare. Sem restrições
Instância inativa do Amazon RDS	AWSManagedServices-StopIdle RDSInstance Pare uma instância inativa do Amazon RDS. Os mecanismos suportados são: MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL. Este documento não se aplica ao Aurora MySQL e ao Aurora PostgreSQL. A instância será interrompida por até 7 dias e reiniciada automaticamente.	Não são permitidos parâmetros pré-configurados. Sem restrições

Trusted Advisor verificações suportadas pelo Trusted Remediator

A tabela a seguir lista as Trusted Advisor verificações suportadas, os documentos de automação do SSM, os parâmetros pré-configurados e o resultado esperado dos documentos de automação. Analise o resultado esperado para ajudá-lo a entender os possíveis riscos com base nos requisitos de sua empresa antes de habilitar um documento de automação de SSM para remediação de cheques.

Certifique-se de que a regra de configuração correspondente para cada Trusted Advisor verificação esteja presente para as verificações suportadas para as quais você deseja habilitar a correção.

Para obter mais informações, consulte [Exibir AWS Trusted Advisor verificações fornecidas por AWS](#)

[Config](#). Se uma verificação tiver AWS Security Hub CSPM controles correspondentes, verifique se o controle do Security Hub está ativado. Para obter mais informações, consulte [Habilitando controles no Security Hub](#). Para obter informações sobre o gerenciamento de parâmetros pré-configurados, consulte [Configure Trusted Advisor check remediation no Trusted Remediator](#).

Trusted Advisor verificações de otimização de custos suportadas pelo Trusted Remediator

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Z4 AUBRNSmz Endereços de IP elástico não associados	AWSManagedServices-TrustedRemediatorReleaseElasticIP Libera um endereço IP elástico que não está associado a nenhum recurso.	Não são permitidos parâmetros pré-configurados. Sem restrições
c18d2gz150 - Instâncias da Amazon paradas EC2	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime - EC2 As instâncias da Amazon interrompidas por vários dias são encerradas.	• Criar AMIBefore encerramento: Para criar a AMI da instância como backup antes de encerrar a EC2 instância da Amazon, escolhatrue. Para não criar um backup antes de encerrar, escolhafalse. O padrão é true. • AllowedDays: o número de dias em que a instância está parada antes de ser encerrada. O padrão é 30. Sem restrições
c18d2gz128 Repositório do Amazon ECR sem política de	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy Cria uma política de ciclo de vida para o repositório especificado se	ImageAgeLimit: O limite máximo de idade em dias (1-365) para “qualquer” imagem no repositório Amazon ECR.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
ciclo de vida configurada	uma política de ciclo de vida ainda não existir.	Sem restrições
DAvU99Dc4C Volumes subutilizados do Amazon EBS	AWSManagedServices-DeleteUnusedEBSVolume Exclui volumes subutilizados do Amazon EBS se os volumes estiverem desvinculados nos últimos 7 dias. Um snapshot do Amazon EBS é criado por padrão.	• CreateSnapshot: Se configurada como <code>true</code>, a automação cria um snapshot do volume do Amazon EBS antes de ser excluído. A configuração padrão é <code>true</code>. Os valores válidos são <code>true</code> e <code>false</code> (com distinção entre maiúsculas e minúsculas). • MinimumUnattachedDays: Mínimo de dias não vinculados do volume do EBS a serem excluídos, até 62 dias. Se definido como <code>0</code>, o documento SSM não verifica o período não anexado e exclui o volume se o volume estiver atualmente desconectado. O padrão é <code>value is 7</code>. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
oi M8 LMh88u Balanceadores de carga obsoletos	AWSManagedServices-DeleteIdleClassicLoadBalancer Exclui um Classic Load Balancer ocioso se ele não for usado e nenhuma instância estiver registrada.	IdleLoadBalancerDays: o número de dias em que o Classic Load Balancer tem 0 conexões solicitadas antes de considerá-lo ocioso. O padrão é sete dias. Se a execução automática estiver ativada, a automação excluirá os Classic Load Balancers ociosos se não houver instâncias de back-end ativas. Para todos os Classic Load Balancers ociosos que têm instâncias de back-end ativas, mas não têm instâncias de back-end saudáveis, a remediação automática não é usada. OpsItems e a correção manual é criada.
TI39HalfU8 Amazon RDS Idle DB Instances	AWSManagedServices-StopIdleRDSInstance A instância de banco de dados Amazon RDS que esteve em um estado ocioso nos últimos sete dias foi interrompida.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
COr6dfpM05 AWS Lambda funções superprovisionadas para o tamanho da memória	AWSManagedServices-ResizeLambdaMemory AWS Lambda o tamanho da memória da função é redimensionado para o tamanho de memória recomendado fornecido pelo Trusted Advisor.	RecommendedMemorySize: a alocação de memória recomendada para a função Lambda. O intervalo de valores está entre 128 e 10240. Se o tamanho da função Lambda foi modificado antes da execução da automação, as configurações podem ser substituídas por essa automação pelo valor recomendado por. Trusted Advisor
QCH7dWOUx1 Instâncias Amazon EC2 de baixa utilização	AWSManagedServices-StopEC2Instance (documento SSM padrão para o modo de execução automática e manual). EC2 As instâncias da Amazon com baixa utilização são interrompidas.	ForceStopWithInstanceStore: defina como <code>true</code> forçar a parada de instâncias usando o armazenamento de instâncias. Caso contrário, defina como <code>false</code> . O valor padrão de <code>false</code> impede que a instância pare. Os valores válidos são verdadeiros ou falsos (diferencia maiúsculas de minúsculas). Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
QCH7dWOUx1 Instâncias Amazon EC2 de baixa utilização	AWSManagedServices-ResizeInstanceByOneLevel A EC2 instância da Amazon é redimensionada por um tipo de instância abaixo do mesmo tipo de família de instâncias. A instância é interrompida e iniciada durante a operação de redimensionamento e retorna ao estado inicial após a conclusão da execução do documento SSM. Essa automação não dá suporte ao redimensionamento de instâncias que estão em um grupo de Auto Scaling.	• MinimumDaysSinceLastChange: número mínimo de dias desde a última alteração do tipo de instância. Se o tipo de instância foi modificado dentro de um tempo especificado, o tipo de instância não será alterado. Use 0 para pular essa validação. O padrão é 7. • Criar AMIBefore redimensionamento: para criar a AMI da instância como backup antes do redimensionamento, escolha <code>true</code> Para não criar um backup, escolha <code>false</code>. O padrão é <code>false</code>. Os valores válidos são <code>true</code> e <code>false</code> (com distinção entre maiúsculas e minúsculas). • ResizeIfStopped: para continuar com a alteração do tamanho da instância, mesmo que a instância esteja em um estado interrompido, escolha <code>true</code>. Para não redimensionar automaticamente a instância se estiver em um estado interrompido, escolha <code>false</code>. Os valores válidos são <code>true</code> e <code>false</code> (com distinção entre maiúsculas e minúsculas). Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
QCH7dWOUx1 Instâncias Amazon EC2 de baixa utilização	AWSManagedServices-TerminateInstance As EC2 instâncias Amazon de baixa utilização são encerradas se não fizerem parte de um grupo de Auto Scaling e a proteção contra rescisão não está ativada. Uma AMI é criada por padrão.	Criar AMI Before encerramento: defina essa opção para <code>true</code> ou <code>false</code> para criar uma AMI de instância como backup antes de encerrar a EC2 instância. O padrão é <code>true</code> . Os valores válidos são <code>true</code> e <code>false</code> (com distinção entre maiúsculas e minúsculas). Sem restrições
G31sq1e9u Clusters subutilizados do Amazon Redshift	AWSManagedServices-PauseRedshiftCluster O cluster do Amazon Redshift está pausado.	Não são permitidos parâmetros pré-configurados. Sem restrições
c1cj39rr6v Configuração de cancelamento de upload em várias partes incompleta do Amazon S3	AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload O bucket do Amazon S3 é configurado com uma regra de ciclo de vida para abortar carregamentos de várias partes que permanecem incompletos após determinados dias.	DaysAfterInitiation: o número de dias após os quais o Amazon S3 interrompe um upload incompleto de várias partes. O padrão é definido para 7 dias. Sem restrições
c1z7kmr00n Recomendações EC2 de otimização de custos da Amazon para instâncias	Use as recomendações de EC2 instâncias da Amazon e a EC2 instância inativa da Amazon de Recomendações do Compute Optimizer suportadas pelo Trusted Remediator .	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
c1z7kmr02n Recomendações de otimização de custos do Amazon EBS para volumes	Use as recomendações de volume do Amazon EBS e deixe o volume ocioso do Amazon EBS de. Recomendações do Compute Optimizer suportadas pelo Trusted Remediator	Não são permitidos parâmetros pré-configurados. Sem restrições
c1z7kmr03n Recomendações de otimização de custos do Amazon RDS para instâncias de banco de dados	Use a instância inativa do Amazon RDS de. Recomendações do Compute Optimizer suportadas pelo Trusted Remediator	Não são permitidos parâmetros pré-configurados. Sem restrições
c1z7kmr05n AWS Lambda recomendações de otimização de custos para funções	Use as recomendações da função Lambda de. Recomendações do Compute Optimizer suportadas pelo Trusted Remediator	Não são permitidos parâmetros pré-configurados. Sem restrições

Trusted Advisor verificações de segurança suportadas pelo Trusted Remediator

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
12Fnkpl8Y5 Exposed Access Keys	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey	Não são permitidos parâmetros pré-configurados.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
	A chave de acesso do IAM exposta está desativada.	Os aplicativos configurados com uma chave de acesso do IAM exposta não podem ser autenticados.
Hs4Ma3G127 - O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados AWS Security Hub CSPM Verificação correspondente: 1 APIGateway.	AWSManagedServices-TrustedR emediatorEnableAPIGateWayExecutionLogging O registro de execução é ativado no estágio da API.	LogLevel: Nível de registro para ativar o registro de execução, ERROR - O registro é ativado somente para erros. INFO - O registro está ativado para todos os eventos. Você deve conceder permissão ao API Gateway para ler e gravar registros da sua conta CloudWatch para ativar o registro de execução. Consulte Configurar o CloudWatch registro para REST APIs no API Gateway para obter detalhes.
Hs4Ma3G129 - Os estágios da API REST API Gateway devem ter o rastreamento ativado AWS X-Ray AWS Security Hub CSPM Verificação correspondente: 3 APIGateway.	AWSManagedServices-EnableAPIGatewayXRayTracing O rastreamento X-Ray está ativado no estágio da API.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G202 - Os dados do cache da API REST do API Gateway devem ser criptografados em repouso AWS Security Hub CSPM Verificação correspondente: 5 APIGateway.	AWSManagedServices-EnableAPIGatewayCacheEncryption Ative a criptografia em repouso para os dados de cache da API REST do API Gateway se o estágio da API REST API Gateway tiver o cache ativado.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma 3G177 - AWS Security Hub CSPM Verificação correspondente: grupos de escalonamento automático associados a um balanceador de carga devem usar verificações de integridade do balanceador de carga .1 AutoScaling	AWSManagedServices-TrustedRoleEnableAutoScalingGroupELBHealthCheck As verificações de saúde do Elastic Load Balancing estão habilitadas para o Auto Scaling Group.	HealthCheckGracePeriod: a quantidade de tempo, em segundos, que o Auto Scaling espera antes de verificar o status de saúde de uma instância do Amazon Elastic Compute Cloud que entrou em serviço. A ativação das verificações de integridade do Elastic Load Balancing pode resultar na substituição de uma instância em execução se algum dos load balancers do Elastic Load Balancing vinculados ao grupo Auto Scaling relatar que ela não está íntegra. Para obter mais informações, consulte Anexar um balanceador de carga do Elastic Load Balancing ao seu grupo de Auto Scaling

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G245 - as CloudFormation pilhas devem ser integradas ao Amazon Simple Notification Service AWS Security Hub CSPM Verificação correspondente: 1 CloudFormation.	AWSManagedServices-EnableCFNStackNotification Associe uma CloudFormation pilha a um tópico do Amazon SNS para notificação.	NotificaçãoARNs: Os tópicos ARNs do Amazon SNS a serem associados às pilhas selecionadas CloudFormation . Para ativar a correção automática, o parâmetro NotificationARNs pré-configurado deve ser fornecido.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G210 - CloudFront as distribuições devem ter o registro ativado AWS Security Hub CSPM Verificação correspondente: 2 CloudFront.	AWSManagedServices-EnableCloudFrontDistributionLogging O registro está habilitado para CloudFront distribuições da Amazon.	• BucketName: o nome do bucket do Amazon S3 em que você deseja armazenar os registros de acesso. • S3KeyPrefix: O prefixo da localização no bucket do S3 para os registros de distribuição da CloudFront Amazon. • IncludeCookies: indica se os cookies devem ser incluídos nos registros de acesso. Para ativar a correção automática, os seguintes parâmetros pré-configurados devem ser fornecidos: • BucketName • S3KeyPrefix • IncludeCookies Para essas restrições de remediação, consulte Como faço para ativar o registro em log para minha distribuição? CloudFront

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G109 - a validação do arquivo de CloudTrail log deve ser ativada AWS Security Hub CSPM Verificação correspondente: CloudTrail.4	AWSManagedServices-TrustedR emediatorEnableCloudTrailLogValidation Permite a validação do registro de CloudTrail trilhas.	Não são permitidos parâmetros pré-configurados. Sem restrições
Hs4Ma3G108 - as CloudTrail trilhas devem ser integradas ao Amazon Logs CloudWatch AWS Security Hub CSPM Verificação correspondente: 5 CloudTrail.	AWSManagedServices-IntegrateCloudTrailWithCloudWatch AWS CloudTrail é integrado ao CloudWatch Logs.	- CloudWatchLogsLogGroupName: nome do grupo de CloudWatch registros de registros para o qual CloudTrail os registros são entregues. Você deve usar um grupo de logs que exista em sua conta. - CloudWatchLogsRoleName: nome da função do IAM que o endpoint de CloudWatch registros deve assumir para gravar no grupo de registros de um usuário. Você deve usar uma função que exista em sua conta. Para ativar a correção automática, os seguintes parâmetros pré-configurados devem ser fornecidos: - CloudWatchLogsLogGroupName - CloudWatchLogsRoleName

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G217 - os ambientes do CodeBuild projeto devem ter uma configuração de registro AWS AWS Security Hub CSPM Verificação correspondente: CodeBuild.4	AWSManagedServices-TrustedR emediatorEnableCodeBuildLog gingConfig Ativa o registro para o CodeBuild projeto.	Não são permitidos parâmetros pré-configurados. Sem restrições
Hs4Ma3G306 - Os clusters de banco de dados Neptune devem ter a proteção de exclusão ativada AWS Security Hub CSPM Verificação correspondente: DocumentDB.3	AWSManagedServices-TrustedR emediatorDisablePublicAcces sOnDocumentDBSnapshot Remove o acesso público do snapshot manual do cluster do Amazon DocumentDB.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G308 - Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada AWS Security Hub CSPM Verificação correspondente: DocumentDB.5	AWSManagedServices-TrustedRolemediatorEnableDocumentDBClusterDeletionProtection Permite a proteção contra exclusão do cluster Amazon DocumentDB.	Não são permitidos parâmetros pré-configurados. Sem restrições
Hs4Ma3G323 - As tabelas do DynamoDB devem ter a proteção contra exclusão ativada AWS Security Hub CSPM Verificação correspondente: DynamoDB.6	AWSManagedServices-TrustedRolemediatorEnableDynamoDBTableDeletionProtection Ativa a proteção contra exclusão de tabelas do DynamoDB que não sejam do AMS.	Não são permitidos parâmetros pré-configurados. Sem restrições
EPS02jt06w - Snapshots públicos do Amazon EBS	AWSManagedServices-TrustedRolemediatorDisablePublicAccessOnEBSSnapshot O acesso público ao snapshot do Amazon EBS está desativado.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G118 - Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou saída AWS Security Hub CSPM Verificação correspondente: 2 EC2.	AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG Todas as regras de entrada e saída no grupo de segurança padrão são removidas.	Não são permitidos parâmetros pré-configurados. Sem restrições
Hs4Ma3G117 - Os volumes EBS anexados devem ser criptografados em repouso AWS Security Hub CSPM Verificação correspondente: 3 EC2.	AWSManagedServices-EncryptInstanceVolume O volume do Amazon EBS anexado na instância é criptografado.	• KMSKeyID: ID da AWS KMS chave ou ARN para criptografar o volume. • DeleteStaleNonEncryptedSnapshotBackups: um sinalizador que decide se o backup instantâneo dos volumes antigos não criptografados deve ser excluído. A instância é reiniciada como parte da correção e a reversão é possível se DeleteStaleNonEncryptedSnapshotBackups estiver configurada para false ajudar na restauração.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G120 - EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado AWS Security Hub CSPM Verificação correspondente: EC2.4	AWSManagedServices-TerminateInstance(documento SSM padrão para o modo de execução automática e manual) EC2 As instâncias da Amazon interrompidas por 30 dias são encerradas.	Criar AMIBefore rescisão:. Para criar a AMI da instância como backup antes de encerrar a EC2 instância, escolhatrue. Para não criar um backup antes de encerrar, escolhafalse. O padrão é true. Sem restrições
Hs4Ma3G120 - EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado AWS Security Hub CSPM Verificação correspondente: EC2.4	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime - EC2 As instâncias da Amazon paradas por um número de dias definido no Security Hub (o valor padrão é 30) são encerradas.	Criar AMIBefore encerramento: Para criar a AMI da instância como backup antes de encerrar a EC2 instância, escolhatrue. Para não criar um backup antes de encerrar, escolhafalse. O padrão é true. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G12 1 - A criptografia padrão do EBS deve estar ativada AWS Security Hub CSPM Verificação correspondente: 7 EC2.	AWSManagedServices-EncryptEBSByDefault A criptografia do Amazon EBS, por padrão, está habilitada para o Região da AWS	Não são permitidos parâmetros pré-configurados. A criptografia por padrão é uma configuração específica da região. Se você habilitá-lo para uma região, não poderá desativá-lo para volumes ou snapshots individuais nessa região.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G124 - As instâncias da EC2 Amazon devem usar o Instance Metadata Service versão 2 () IMDSv2 AWS Security Hub CSPM Verificação correspondente: 8 EC2.	AWSManagedServices-TrustedRoleMediatorHabilitar EC2 instância IMDSv2 EC2 As instâncias da Amazon usam o Instance Metadata Service versão 2 (IMDSv2).	• IMDSv1MetricCheckPeriod: o número de dias (42-455) para analisar as métricas de IMDSv1 uso CloudWatch. Se a EC2 instância da Amazon foi criada dentro do período de tempo especificado, a análise começa a partir da data de criação da instância. • HttpPutResponseHopLimit: o número máximo de saltos de rede permitidos para o token de metadados da instância. Esse valor pode ser configurado entre 2 saltos 1 e saltos. Um limite de salto 1 restringe o acesso por token a processos executados diretamente na instância, enquanto um limite de salto de 2 permite o acesso de contêineres em execução na instância. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G207 - as EC2 sub-redes não devem atribuir automaticamente endereços IP públicos AWS Security Hub CSPM Cheque correspondente: EC2.15	AWSManagedServices-UpdateAutoAssignPublicIpv4 endereços As sub-redes VPC são configuradas para não atribuir automaticamente endereços IP públicos.	Não são permitidos parâmetros pré-configurados. Sem restrições
Hs4Ma3G209 - As listas de controle de acesso à rede não utilizadas são removidas AWS Security Hub CSPM Verificação correspondente: EC2.16	AWSManagedServices-DeleteUnusedNACL Excluir ACL de rede não utilizada	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G215 - Grupos de segurança não utilizados da Amazon devem ser removidos EC2 AWS Security Hub CSPM Verificação correspondente: EC2.22	AWSManagedServices-DeleteSecurityGroups Exclua grupos de segurança não utilizados.	Não são permitidos parâmetros pré-configurados. Sem restrições
Hs4Ma3G247 - O Amazon Transit EC2 Gateway não deve aceitar automaticamente solicitações de anexos de VPC AWS Security Hub CSPM Cheque correspondente: EC2.23	AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach- Desativa a aceitação automática de solicitações de anexos de VPC para o Amazon Transit EC2 Gateway não AMS especificado.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G235 - Os repositórios privados do ECR devem ter a imutabilidade da tag configurada AWS Security Hub CSPM Verificação correspondente: ECR.2	AWSManagedServices-TrustedRemediatorSetImageTagImmutability Define as configurações de mutabilidade da tag de imagem como IMMUTABLE para o repositório especificado.	Não são permitidos parâmetros pré-configurados. Sem restrições
Hs4Ma3G216 - Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada AWS Security Hub CSPM Verificação correspondente: ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy O repositório ECR tem uma política de ciclo de vida configurada.	LifecyclePolicyText: o texto da política do repositório JSON a ser aplicado ao repositório. Para ativar a correção automática, os seguintes parâmetros pré-configurados devem ser fornecidos: LifecyclePolicyText

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G32 5 - Os clusters EKS devem ter o registro de auditoria ativado AWS Security Hub CSPM Verificação correspondente: EKS.8	AWSManagedServices-TrustedRemediatorEnableEKSAuditLog O registro de auditoria está habilitado para o cluster EKS.	Não são permitidos parâmetros pré-configurados. Sem restrições
Hs4Ma3G183 - O balanceador de carga do aplicativo deve ser configurado para descartar cabeçalhos HTTP AWS Security Hub CSPM Verificação correspondente: ELB.4	AWSConfigRemediation-DropInvalidHeadersForALB O Application Load Balancer está configurado para campos de cabeçalho inválidos.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G184 - O registro de balanceadores de carga de aplicativos e balanceadores de carga clássicos deve estar ativado AWS Security Hub CSPM Verificação correspondente: ELB.5	AWSManagedServices-EnableELBLogging (documento SSM padrão para o modo de execução automática e manual) O registro em log do Application Load Balancer e do Classic Load Balancer está ativado.	• BucketName: o nome do bucket (não o ARN). Certifique-se de que a política de bucket esteja configurada corretamente para registro em log. • S3KeyPrefix: O prefixo da localização no bucket do Amazon S3 para os registros do Elastic Load Balancing. Para ativar a correção automática, os seguintes parâmetros pré-configurados devem ser fornecidos: • BucketName • S3KeyPrefix O bucket do Amazon S3 deve ter uma política de bucket que conceda permissão ao Elastic Load Balancing para gravar os registros de acesso no bucket.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G184 - O registro de balanceadores de carga de aplicativos e balanceadores de carga clássicos deve estar ativado AWS Security Hub CSPM Verificação correspondente: ELB.5	AWSManagedServices-EnableELBLoggingV2 O registro em log do Application Load Balancer e do Classic Load Balancer está ativado.	• TargetBucketTagKey: o nome da tag (com distinção entre maiúsculas e minúsculas) usada para identificar o bucket de destino do Amazon S3. Use isso junto com TargetBucketTagValue para marcar o bucket que servirá como bucket de destino para o registro de acesso. • TargetBucketTagValue: o valor da tag (com distinção entre maiúsculas e minúsculas) usado para identificar o bucket de destino do Amazon S3. Use isso junto com TargetBucketTagKey para marcar o bucket que servirá como bucket de destino para o registro de acesso. • S3BucketPrefix: O prefixo (hierarquia lógica) do bucket Amazon S3. O prefixo especificado não pode incluir a string <code>AWSLogs</code>. Para mais informações, consulte Organizar objetos usando prefixos. Para ativar a correção automática, os seguintes parâmetros pré-configurados devem ser fornecidos: • TargetBucketTagKey • TargetBucketTagValue • S3BucketPrefix

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
		O bucket do Amazon S3 deve ter uma política de bucket que conceda permissão ao Elastic Load Balancing para gravar os registros de acesso no bucket.
Hs4Ma3G326 - A configuração de bloqueio de acesso público do Amazon EMR deve estar ativada AWS Security Hub CSPM Verificação correspondente: EMR.2	AWSManagedServices-TrustedRoleMediatorEnableEMRBlockPublicAccess As configurações de bloqueio de acesso público do Amazon EMR estão ativadas para a conta.	Não são permitidos parâmetros pré-configurados. Sem restrições
Hs4Ma3G135 - as AWS KMS chaves não devem ser excluídas acidentalmente AWS Security Hub CSPM Verificação correspondente: KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS a exclusão da chave foi cancelada.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G299 - Os snapshots manuais do cluster do Amazon DocumentDB não devem ser públicos AWS Security Hub CSPM Cheque correspondente: Netuno.4	AWSManagedServices-TrustedRolemediatorEnableNeptuneDBClusterDeletionProtection Permite a proteção contra exclusão do cluster Amazon Neptune.	Não são permitidos parâmetros pré-configurados. Sem restrições
Hs4Ma3G319 - Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada AWS Security Hub CSPM Cheque correspondente: 9 NetworkFirewall.	AWSManagedServices-TrustedRolemediatorEnableNetworkFirewallDeletionProtection- Ativa a proteção de exclusão para o AWS Network Firewall.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G223 - os OpenSearch domínios devem criptografar os dados enviados entre os nós AWS Security Hub CSPM Verificação correspondente: 3 OpenSearch.	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption A criptografia de nó a nó está habilitada para o domínio.	Não são permitidos parâmetros pré-configurados. Depois que a node-to-node criptografia estiver ativada, você não poderá desativar a configuração. Em vez disso, tire um instantâneo manual do domínio criptografado, crie outro domínio, migre seus dados e exclua o domínio antigo.
Hs4Ma3G222 - o registro de erros de OpenSearch domínio nos registros deve estar ativado CloudWatch AWS Security Hub CSPM Verificação correspondente: Opensearch.4	AWSManagedServices-EnableOpenSearchLogging O registro de erros está ativado para o OpenSearch domínio.	CloudWatchLogGroupArn: o ARN de um grupo de CloudWatch logs do Amazon Logs. Para habilitar a remediação automática, o seguinte parâmetro pré-configurado deve ser fornecido: CloudWatchLogGroupArn A política CloudWatch de recursos da Amazon deve ser configurada com permissões. Para obter mais informações, consulte Habilitar registros de auditoria no Guia do usuário do Amazon OpenSearch Service

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G221 - OpenSearch os domínios devem ter o registro de auditoria ativado AWS Security Hub CSPM Verificação correspondente: Opensearch.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch os domínios são configurados com o registro de auditoria ativado.	CloudWatchLogGroupArn: o ARN do grupo de CloudWatch registros no qual publicar registros. Para habilitar a correção automática, o seguinte parâmetro pré-configurado deve ser fornecido: CloudWatchLogGroupArn A política CloudWatch de recursos da Amazon deve ser configurada com permissões. Para obter mais informações, consulte Habilitar registros de auditoria no Guia do usuário do Amazon OpenSearch Service
Hs4Ma3G220 - As conexões com OpenSearch domínios devem ser criptografadas usando TLS 1.2 AWS Security Hub CSPM Verificação correspondente: Opensearch.8	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 A política TLS está definida como `policy-min-TLS-1-2-2019-07` e somente conexões criptografadas por HTTPS (TLS) são permitidas.	Não são permitidos parâmetros pré-configurados. Conexões com OpenSearch domínios são necessárias para usar o TLS 1.2. A criptografia de dados em trânsito pode afetar o desempenho. Teste seus aplicativos com esse recurso para entender o perfil de desempenho e o impacto do TLS.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G194 - O snapshot do Amazon RDS deve ser privado AWS Security Hub CSPM Verificação correspondente: RDS.1	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 O acesso público ao snapshot do Amazon RDS está desativado.	Não são permitidos parâmetros pré-configurados. Sem restrições
Hs4Ma3G192 - As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela configuração PubliclyAccessible AWS AWS Security Hub CSPM Verificação correspondente: RDS.2	AWSManagedServices-TrustedResourceMediatorDisablePublicAccessOnRDSInstance Desative o acesso público na instância de banco de dados do RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G189 - O monitoramento aprimorado é configurado para instâncias de banco de dados Amazon RDS AWS Security Hub CSPM Verificação correspondente: RDS.6	AWSManagedServices-TrustedR emediatorEnableRDSEnhancedM onitoring Habilite o monitoramento aprimorado para instâncias de banco de dados Amazon RDS	• MonitoringInterval: o intervalo, em segundos, entre os pontos em que as métricas de monitoramento aprimorado são coletadas para a instância de banco de dados. Os intervalos válidos são 0, 1, 5, 10, 15, 30 e 60. Para desabilitar a coleta de métricas de monitoramento avançado, especifique 0. • MonitoringRoleName: o nome da função do IAM que permite que o Amazon RDS envie métricas de monitoramento aprimoradas para o Amazon CloudWatch Logs. Se uma função não for especificada, a função <code>rds-monitoring-rol</code> e padrão será usada ou criada, caso não exista. Se o monitoramento aprimorado for ativado antes da execução da automação, as configurações poderão ser substituídas por essa automação com os <code>MonitoringRoleName</code> valores <code>MonitoringInterval</code> e configurados nos parâmetros pré-configurados.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G190 - Os clusters do Amazon RDS devem ter a proteção de exclusão ativada AWS Security Hub CSPM Verificação correspondente: RDS.7	AWSManagedServices-TrustedR emediatorEnableRDSDeletionP rotection A proteção contra exclusão está habilitada para clusters do Amazon RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições
Hs4Ma3G198 - As instâncias de banco de dados do Amazon RDS devem ter a proteção de exclusão ativada AWS Security Hub CSPM Verificação correspondente: RDS.8	AWSManagedServices-TrustedR emediatorEnableRDSDeletionP rotection A proteção contra exclusão está habilitada para instâncias do Amazon RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G199 - As instâncias de banco de dados do RDS devem publicar registros nos registros CloudWatch AWS Security Hub CSPM Verificação correspondente: RDS.9	AWSManagedServices-TrustedR emediatorEnableRDSLogExports As exportações de log do RDS estão habilitadas para a instância de banco de dados RDS ou o cluster de banco de dados RDS.	Não são permitidos parâmetros pré-configurados. A função AWSServiceRoleForRDS vinculada ao serviço é necessária.
Hs4Ma3G160 - A autenticação do IAM deve ser configurada para instâncias do RDS AWS Security Hub CSPM Verificação correspondente: RDS.10	AWSManagedServices-UpdateRD SIAMDatabaseAuthentication AWS Identity and Access Management a autenticação está habilitada para a instância do RDS.	ApplyImmediately: indica se as modificações nessa solicitação e quaisquer modificações pendentes são aplicadas de forma assíncrona o mais rápido possível. Para aplicar a alteração imediatamente, escolha <code>true</code> Para programar a alteração para a próxima janela de manutenção, escolha <code>false</code>. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G161 - A autenticação do IAM deve ser configurada para clusters RDS AWS Security Hub CSPM Verificação correspondente: RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication A autenticação do IAM está habilitada para o cluster RDS.	ApplyImmediately: indica se as modificações nessa solicitação e quaisquer modificações pendentes são aplicadas de forma assíncrona o mais rápido possível. Para aplicar a alteração imediatamente, escolha <code>true</code>. Para programar a alteração para a próxima janela de manutenção, escolha <code>false</code>. Sem restrições
Hs4Ma3G162 - As atualizações automáticas de versões secundárias do RDS devem ser habilitadas AWS Security Hub CSPM Verificação correspondente: RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade A configuração automática de upgrade de versões secundárias para o Amazon RDS está habilitada.	Não são permitidos parâmetros pré-configurados. A instância do Amazon RDS deve estar no <code>available</code> estado para que essa remediação ocorra.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G163 - Os clusters de banco de dados RDS devem ser configurados para copiar tags para instantâneos AWS Security Hub CSPM Verificação correspondente: RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagstosnapshot a configuração para clusters do Amazon RDS está ativada.	Não são permitidos parâmetros pré-configurados. As instâncias do Amazon RDS devem estar disponíveis para que essa correção ocorra.
Hs4Ma3G164 - As instâncias de banco de dados do RDS devem ser configuradas para copiar tags para instantâneos AWS Security Hub CSPM Verificação correspondente: RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagsToSnapshot a configuração do Amazon RDS está ativada.	Não são permitidos parâmetros pré-configurados. As instâncias do Amazon RDS devem estar disponíveis para que essa correção ocorra.
RsS93 HQwa1 Snapshots públicos do Amazon RDS	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 O acesso público ao snapshot do Amazon RDS está desativado.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G103 - Os clusters do Amazon Redshift devem proibir o acesso público AWS Security Hub CSPM Verificação correspondente: Redshift.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster O acesso público no cluster do Amazon Redshift está desativado.	Não são permitidos parâmetros pré-configurados. A desativação do acesso público bloqueia todos os clientes provenientes da Internet. E o cluster do Amazon Redshift fica no estado de modificação por alguns minutos, enquanto a remediação desativa o acesso público ao cluster.
Hs4Ma3G106 - Os clusters do Amazon Redshift devem ter o registro de auditoria ativado AWS Security Hub CSPM Verificação correspondente: Redshift.4	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterAuditLogging O registro de auditoria é ativado no seu cluster do Amazon Redshift durante a janela de manutenção.	Não são permitidos parâmetros pré-configurados. Para habilitar a correção automática, os seguintes parâmetros pré-configurados devem ser fornecidos. BucketName: O balde deve estar no mesmo Região da AWS. O cluster deve ter permissões de leitura e colocação de objetos. Se o registro em cluster do Redshift estiver ativado antes da execução da automação, as configurações de registro poderão ser substituídas por essa automação com os S3KeyPrefix valores BucketName e configurados nos parâmetros pré-configurados.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G105 - O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas AWS Security Hub CSPM Verificação correspondente: Redshift.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade- As principais atualizações da versão são aplicadas automaticamente ao cluster durante a janela de manutenção. Não há tempo de inatividade imediato para o cluster do Amazon Redshift, mas seu cluster do Amazon Redshift pode ter tempo de inatividade durante a janela de manutenção se for atualizado para uma versão principal.	Não são permitidos parâmetros pré-configurados. Sem restrições
Hs4Ma3G104 - Os clusters do Amazon Redshift devem usar roteamento de VPC aprimorado AWS Security Hub CSPM Verificação correspondente: Redshift.7	AWSManagedServices-TrustedRedshiftClusterEnhancedVPCRouting O roteamento aprimorado de VPC está habilitado para clusters do Amazon Redshift.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G173 - A configuração de acesso público do bloco S3 deve ser ativada no nível do bucket AWS Security Hub CSPM Verificação correspondente: S3.8	AWSManagedServices-TrustedRoleBlockS3BucketPublicAccess Os blocos de acesso público no nível do bucket são aplicados ao bucket do Amazon S3.	Não são permitidos parâmetros pré-configurados. Essa correção pode afetar a disponibilidade dos objetos do S3. Para obter informações sobre como o Amazon S3 avalia o acesso, consulte Bloqueio do acesso público ao seu armazenamento do Amazon S3.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G230 - O registro de acesso ao servidor de bucket S3 deve estar ativado AWS Security Hub CSPM Verificação correspondente: S3.9	AWSManagedServices-EnableBucketAccessLogging(documento SSM padrão para o modo de execução automática e manual) O registro de acesso ao servidor Amazon S3 está ativado.	• TargetBucket: o nome do bucket do S3 para armazenar registros de acesso ao servidor. • TargetObjectKeyFormat: formato de chave do Amazon S3 para objetos de log (os valores diferenciam maiúsculas de minúsculas). Para usar o formato simples das chaves do S3 para objetos de log, escolha <code>SimplePrefix</code>. Para usar a chave S3 particionada para objetos de log e usar <code>EventTime</code> para o prefixo particionado, escolha <code>PartitionedPrefixEventTime</code>. Para usar a chave S3 particionada para objetos de log e usar <code>DeliveryTime</code> para o prefixo particionado, escolha <code>PartitionedPrefixDeliveryTime</code>. Os valores válidos são <code>SimplePrefix</code>, <code>PartitionedPrefixEventTime</code> e <code>PartitionedPrefixDeliveryTime</code>. Para habilitar a remediação automática, o seguinte parâmetro pré-configurado deve ser fornecido: TargetBucket O bucket de destino deve estar no mesmo bucket Região da AWS e Conta da AWS no bucket de origem, com as permissões corretas para

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
		entrega de registros. Para obter mais informações, consulte Habilitar registro em log de acesso ao servidor do Amazon S3 .

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G230 — O registro de acesso ao servidor bucket S3 deve estar habilitado AWS Security Hub CSPM Verificação correspondente: S3.9	AWSManagedServices-TrustedRoleMediatorEnableBucketAccess LoggingV2 - O registro do bucket do Amazon S3 está ativado.	• TargetBucketTagKey: o nome da tag (com distinção entre maiúsculas e minúsculas) para identificar o bucket de destino. Use isso e TargetBucketTagValue para marcar o bucket a ser usado como o bucket de destino para o registro de acesso. • TargetBucketTagValue: o valor da tag (com distinção entre maiúsculas e minúsculas) para identificar o bucket de destino, use-o e TargetBucketTagKey para marcar o bucket a ser usado como o bucket de destino para o registro de acesso. • TargetObjectKeyFormat: Formato de chave do Amazon S3 para objetos de log (os valores diferenciam maiúsculas de minúsculas): Para usar o formato simples das chaves do S3 para objetos de log, escolha. SimplePrefix Para usar a chave S3 particionada para objetos de log e usar EventTime para o prefixo particionado, escolha. PartitionedPrefixEventTime Para usar a chave S3 particionada para objetos de log e usar DeliveryTime para o prefixo particionado, escolha. PartitionedPrefixDeliveryTime O padrão é PartitionedPrefixEventTime.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
		Para habilitar a correção automática, os seguintes parâmetros devem ser fornecidos: TargetBucketTagKey e TargetBucketTagValue. O bucket de destino deve estar na mesma região da AWS e Conta da AWS no bucket de origem, com as permissões corretas para entrega de registros. Para obter mais informações, consulte Habilitar registro em log de acesso ao servidor do Amazon S3.
Pfx0 RwgBli Permissões do bucket do Amazon S3	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess Bloqueio de acesso público	Não são permitidos parâmetros pré-configurados. Essa verificação consiste em vários critérios de alerta. Essa automação corrige problemas de acesso público. A correção de outros problemas de configuração sinalizados por Trusted Advisor não é suportada. Essa remediação oferece suporte à remediação de buckets S3 AWS service (Serviço da AWS) criados (por exemplo, cf-templates-000000000000).

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G272 - Os usuários não devem ter acesso root às instâncias do notebook SageMaker AWS Security Hub CSPM Verificação correspondente: 3 SageMaker.	AWSManagedServices-TrustedRolemediatorDisableSageMakerNotebookInstanceRootAccess O acesso root para usuários está desativado para a instância do SageMaker notebook.	Não são permitidos parâmetros pré-configurados. Essa remediação causa interrupção se a instância do SageMaker notebook estiver no InService estado.
Hs4Ma3G179 - Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS AWS Security Hub CSPM Verificação correspondente: SNS.1	AWSManagedServices-EnableSNSEncryptionAtRest O tópico do SNS é configurado com criptografia do lado do servidor.	KmsKeyId: o ID de uma chave mestra de cliente AWS gerenciada (CMK) para o Amazon SNS ou de uma CMK personalizada a ser usada para criptografia do lado do servidor (SSE). O padrão está definido como <code>alias/aws/sns</code>. Se uma AWS KMS chave personalizada for usada, ela deverá ser configurada com as permissões corretas. Para obter mais informações, consulte Habilitando a criptografia do lado do servidor (SSE) para um tópico do Amazon SNS

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G158 - Documentos SSM não devem ser públicos AWS Security Hub CSPM Verificação correspondente: SSM.4	AWSManagedServices-TrustedResourceMediatorDisableSSMDocPublicSharing- Desativa o compartilhamento público do documento SSM.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Hs4Ma3G136 - As filas do Amazon SQS devem ser criptografadas em repouso AWS Security Hub CSPM Verificação correspondente: SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest As mensagens no Amazon SQS são criptografadas.	• <code>SqsManagedSseEnabled</code>: Defina como <code>true</code> para habilitar a criptografia de filas do lado do servidor usando chaves de criptografia de propriedade do Amazon SQS, defina como <code>false</code> para habilitar a criptografia de filas do lado do servidor usando uma chave. AWS KMS • <code>KMSKeyID</code>: O ID ou alias de uma chave mestra de cliente (CMK) AWS gerenciada para o Amazon SQS ou de uma CMK personalizada a ser usada para criptografia do lado do servidor para a fila. Se não for fornecido, <code>alias/aws/sqs</code> é usado. • <code>KmsDataKeyReusePeriodSeconds</code>: o período de tempo, em segundos, durante o qual o Amazon SQS pode reutilizar uma chave de dados para criptografar ou descriptografar mensagens antes de ligar novamente. AWS KMS Um número inteiro que representa segundos, entre 60 segundos (1 minuto) e 86.400 segundos (24 horas). Essa configuração será ignorada se <code>SqsManagedSseEnabled</code> estiver definida como <code>true</code>.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
		Anônimo SendMessage e ReceiveMessage as solicitações para a fila criptografada são rejeitadas. Todas as solicitações para filas com SSE habilitada devem usar HTTPS e o Signature versão 4.

Trusted Advisor verificações de tolerância a falhas suportadas pelo Trusted Remediator

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
c18d2gz138 Recuperação do Amazon DynamoDB Point-in-time	AWSManagedServices-TrustedRemediatorEnableDDBPITR Permite point-in-time a recuperação de tabelas do DynamoDB.	Não são permitidos parâmetros pré-configurados. Sem restrições
R365s2qddf Versionamento em bucket do Amazon S3	AWSManagedServices-TrustedRemediatorEnableBucketVersioning O versionamento do bucket do Amazon S3 está ativado.	Não são permitidos parâmetros pré-configurados. Essa correção não oferece suporte à correção de buckets S3 AWS service (Serviço da AWS) criados (por exemplo, cf-templates-000000000000000000000000).
BueAdJ7nRP Registro em bucket do Amazon S3	AWSManagedServices-EnableBucketAccessLogging O registro do bucket do Amazon S3 está ativado.	- TargetBucket: o nome do bucket do S3 para armazenar os registros de acesso ao servidor. - TargetObjectKeyFormat: Formato de chave Amazon S3 para objetos

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
		de log, para usar o formato simples para chaves S3 para objetos de log, escolha. <code>SimplePrefix</code> Para usar a chave S3 particionada para objetos de log e usar <code>EventTime</code> para o prefixo particionado, escolha. <code>PartitionedPrefixEventTime</code> Para usar a chave S3 particionada para objetos de log e usar <code>DeliveryTime</code> para o prefixo particionado, escolha. <code>PartitionedPrefixDeliveryTime</code> O padrão é <code>PartitionedPrefixEventTime</code>. Os valores válidos são <code>SimplePrefix</code>, <code>PartitionedPrefixEventTime</code> e <code>PartitionedPrefixDeliveryTime</code> (com distinção entre maiúsculas e minúsculas). Para ativar a correção automática, os seguintes parâmetros pré-configurados devem ser fornecidos: • <code>TargetBucket</code> O bucket de destino deve estar no mesmo bucket Região da AWS e Conta da AWS no bucket de origem, com as permissões corretas para entrega de registros. Para obter

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
		mais informações, consulte Habilitar registro em log de acesso ao servidor do Amazon S3 .
F2ik5r6dep Amazon RDS Multi-AZ	AWSManagedServices-TrustedR emediatorEnableRDSMultiAZ A implantação da Zona de Multidisponibilidade está ativada.	Não são permitidos parâmetros pré-configurados. Há uma possível degradação do desempenho durante essa alteração.
H7 IgTzj TYb Snapshots do Amazon EBS	AWSManagedServices-TrustedR emediatorCreateEBSSnapshot A Amazon EBSsnapshots é criada.	Não são permitidos parâmetros pré-configurados. Sem restrições
em QPADk ZvH Backups do RDS	AWSManagedServices-EnableRDS BackupRetention A retenção de backup do Amazon RDS está habilitada para o banco de dados.	- BackupRetentionPeriod: o número de dias (1 a 35) para reter backups automatizados. - ApplyImmediately: indica se a alteração na retenção de backup do RDS e quaisquer modificações pendentes são aplicadas de forma assíncrona assim que possível. Escolha true aplicar a alteração imediatamente ou false programar a alteração para a próxima janela de manutenção. Se o ApplyImmediately parâmetro for definido comotru, as alterações pendentes no banco de dados serão aplicadas junto com a configuração RDSBackup de retenção.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
c1qf5bt013 As instâncias de banco de dados do Amazon RDS têm o escalonamento automático de armazenamento desativado	AWSManagedServices-TrustedR emediatorEnableRDSInstanceS torageAutoScaling- O escalonamento automático de armazenamento está habilitado para a instância de banco de dados Amazon RDS.	MaxAllocatedStorageIncrease Percentage: A porcentagem de aumento da corrente Allocated Storage, para definir MaxAllocatedStorage o. O padrão está definido como 26. Você deve definir o limite máximo de armazenamento para pelo menos 10% a mais do que o armazenamento alocado atualmente. É uma prática recomendada definir o limite máximo de armazenamento para pelo menos 26% a mais. Para obter detalhes, consulte Gerenciando a capacidade automaticamente com o escalonamento automático de armazenamento do Amazon Relational Database Service. Sem restrições
7q GXs KIUw Classic Load Balancer Connection Draining	AWSManagedServices-TrustedR emediatorEnableCLBConnectionDraining A drenagem da conexão está ativada para o Classic Load Balancer.	ConnectionDrainingTimeout: o tempo máximo, em segundos, para manter as conexões existentes abertas antes de cancelar o registro das instâncias. O padrão é definido como 300 segundos. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
c18d2gz106 Amazon EBS não incluído no plano AWS Backup	AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan O Amazon EBS está incluído no AWS Backup plano.	A remediação marca o volume do Amazon EBS com o seguinte par de tags. O par de tags deve corresponder aos critérios de seleção de recursos baseados em tags para AWS Backup. • TagKey • TagValue Sem restrições
c18d2gz107 Tabela do Amazon DynamoDB não incluída no plano AWS Backup	AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlan A tabela do Amazon DynamoDB está incluída no plano. AWS Backup	A remediação marca o Amazon DynamoDB com o seguinte par de tags. O par de tags deve corresponder aos critérios de seleção de recursos baseados em tags para AWS Backup. • TagKey • TagValue Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
c18d2gz117 Amazon EFS não incluído no AWS Backup plano	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan O Amazon EFS está incluído no AWS Backup plano.	A remediação marca o Amazon EFS com o seguinte par de tags. O par de tags deve corresponder aos critérios de seleção de recursos baseados em tags para AWS Backup. • TagKey • TagValue Sem restrições
c18d2gz105 Balanceamento de carga cruzada dos Network Load Balancers	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing O balanceamento de carga entre zonas está ativado no Network Load Balancer.	Não são permitidos parâmetros pré-configurados. Sem restrições
c1qf5bt026 O synchronous_commit parâmetro Amazon RDS está desativado	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter synchronous_commit O parâmetro está ativado para o Amazon RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições
c1qf5bt030 O innodb_flush_log_at_trx_commit parâmetro Amazon RDS não é 1	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter innodb_flush_log_at_trx_commit O parâmetro está definido como 1 para Amazon RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
c1qf5bt031 O sync_binlog parâmetro Amazon RDS está desativado	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter sync_binlog O parâmetro está ativado para o Amazon RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições
c1qf5bt036 A configuração de innodb_default_row_format parâmetros do Amazon RDS não é segura	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter innodb_default_row_format O parâmetro está definido como DYNAMIC para Amazon RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições
c18d2gz144 Monitoramento EC2 detalhado da Amazon não ativado	AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring O monitoramento detalhado está habilitado para a Amazon EC2.	Não são permitidos parâmetros pré-configurados. Sem restrições

Trusted Advisor verificações de desempenho suportadas pelo Trusted Remediator

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
COr6dfpM06 AWS Lambda funções subprovis ionadas para	AWSManagedServices-ResizeLambdaMemory O tamanho da memória das funções Lambda é redimensionado para o	RecommendedMemorySize: a alocação de memória recomendada para a função Lambda. O intervalo de valores está entre 128 e 10240.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
o tamanho da memória	tamanho de memória recomendado fornecido por. Trusted Advisor	Se o tamanho da função Lambda for modificado antes da execução da automação, essa automação poderá substituir as configurações pelo valor recomendado por. Trusted Advisor

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
ZRxQIPsb6c Instâncias Amazon EC2 de alta utilização	<code>AWSManagedServices-ResizeInstanceByOneLevel</code> As EC2 instâncias da Amazon são redimensionadas por um tipo de instância no mesmo tipo de família de instâncias. As instâncias são interrompidas e iniciadas durante a operação de redimensionamento e retornam ao estado inicial após a conclusão da execução. Essa automação não dá suporte ao redimensionamento de instâncias que estão em um grupo de Auto Scaling.	• <code>MinimumDaysSinceLastChange</code>: o número mínimo de dias desde a última alteração do tipo de instância. Se o tipo de instância foi modificado dentro do tempo especificado, o tipo de instância não será alterado. Use 0 para pular essa validação. O padrão é 7. • <code>Criar AMIBefore redimensionamento</code>: para criar a AMI da instância como backup antes do redimensionamento, escolha <code>true</code> Para não criar um backup, escolha <code>false</code>. O padrão é <code>false</code>. Os valores válidos são <code>true</code> e <code>false</code> (com distinção entre maiúsculas e minúsculas). • <code>ResizeIfStopped</code>: para continuar com a alteração do tamanho da instância, mesmo que a instância esteja em um estado interrompido, escolha <code>true</code>. Para não redimensionar automaticamente a instância se estiver em um estado interrompido, escolha <code>false</code>. Os valores válidos são <code>true</code> e <code>false</code> (com distinção entre maiúsculas e minúsculas). Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
c1qf5bt021 innodb_change_buffering Parâmetro do Amazon RDS usando menos do que o valor ideal	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter O valor do innodb_change_buffering parâmetro é definido como NONE para o Amazon RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições
c1qf5bt025 O autovacuum parâmetro Amazon RDS está desativado	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter autovacuum O parâmetro está ativado para o Amazon RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições
c1qf5bt028 O enable_indexonlyscan parâmetro Amazon RDS está desativado	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter enable_indexonlyscan O parâmetro está ativado para o Amazon RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições
c1qf5bt029 O enable_indexscan parâmetro Amazon RDS está desativado	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter enable_indexscan O parâmetro está ativado para o Amazon RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
c1qf5bt032 O <code>innodb_stats_persistent</code> parâmetro Amazon RDS está desativado	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter <code>innodb_stats_persistent</code> O parâmetro está ativado para o Amazon RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições
c1qf5bt037 O <code>general_logging</code> parâmetro Amazon RDS está ativado	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter <code>general_logging</code> O parâmetro está desativado para o Amazon RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições

Trusted Advisor verificações de limites de serviço suportadas pelo Trusted Remediator

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
Ln7RR0L7j9 EC2-Endereço IP elástico da VPC	AWSManagedServices-UpdateVpcElasticIPQuota É solicitado um novo limite para endereços IP elásticos EC2 -VPC. Por padrão, o limite é aumentado em 3.	Incremento: o número para aumentar a cota atual. O padrão é 3. Se essa automação for executada várias vezes antes da Trusted Advisor verificação ser atualizada com o OK status, talvez haja um aumento maior no limite.
Km7QQ0L7J9 Gateways da Internet da VPC	AWSManagedServices-IncreaseServiceQuota- É solicitado um novo limite para gateways de	Incremento: o número para aumentar a cota atual. O padrão é 3.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
JI7pp0I7j9 VPC	Internet VPC. Por padrão, o limite é aumentado em três. AWSManagedServices-Increase ServiceQuota Um novo limite para VPC é solicitado. Por padrão, o limite é aumentado em 3.	Se essa automação for executada várias vezes antes da Trusted Advisor verificação ser atualizada com o OK status, talvez haja um aumento maior no limite. Incremento: o número para aumentar a cota atual. O padrão é 3. Se essa automação for executada várias vezes antes da Trusted Advisor verificação ser atualizada com o OK status, talvez haja um aumento maior no limite.
Fw7hh0I7j9 Grupos de Auto Scaling	AWSManagedServices-Increase ServiceQuota É solicitado um novo limite para grupos de Auto Scaling. Por padrão, o limite é aumentado em 3.	Incremento: o número para aumentar a cota atual. O padrão é 3. Se essa automação for executada várias vezes antes da Trusted Advisor verificação ser atualizada com o OK status, talvez haja um aumento maior no limite.
3 Njm0 DJQO9 Grupos de opção do RDS	AWSManagedServices-Increase ServiceQuota Um novo limite para grupos de opções do Amazon RDS é solicitado. Por padrão, o limite é aumentado em 3.	Incremento: o número para aumentar a cota atual. O padrão é 3. Se essa automação for executada várias vezes antes da Trusted Advisor verificação ser atualizada com o OK status, talvez haja um aumento maior no limite.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
EM8b3yLRTr Balanceadores de carga da aplicação do ELB	AWSManagedServices-IncreaseServiceQuota É solicitado um novo limite para os balanceadores de carga de aplicativos ELB. Por padrão, o limite é aumentado em 3.	Incremento: o número para aumentar a cota atual. O padrão é 3. Se essa automação for executada várias vezes antes da Trusted Advisor verificação ser atualizada com o OK status, talvez haja um aumento maior no limite.
8 WiQ K YSt25 Balanceadores de carga da rede do ELB	AWSManagedServices-IncreaseServiceQuota É solicitado um novo limite para os balanceadores de carga de rede ELB. Por padrão, o limite é aumentado em 3.	Incremento: o número para aumentar a cota atual. O padrão é 3. Se essa automação for executada várias vezes antes da Trusted Advisor verificação ser atualizada com o OK status, talvez haja um aumento maior no limite.

Trusted Advisor verificações de excelência operacional suportadas pelo Trusted Remediator

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
c18d2gz125 O Amazon API Gateway não está registrando em log os logs de execução	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging O registro de execução é ativado no estágio da API.	Não são permitidos parâmetros pré-configurados. Você deve conceder permissão ao API Gateway para ler e gravar registros da sua conta CloudWatch para ativar o registro de execução. Consulte Configurar o CloudWatch

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
		h registro para REST APIs no API Gateway para obter detalhes.
c18d2gz168 A proteção contra exclusão do Elastic Load Balancing não está habilitada para balanceadores de carga	AWSManagedServices-TrustedRolemediatorEnableELBDeletionProtection- A proteção contra exclusão está ativada para o Elastic Load Balancer.	Não são permitidos parâmetros pré-configurados. Sem restrições
c1qf5bt012 O Amazon RDS Performance Insights está desativado	AWSManagedServices-TrustedRolemediatorEnableRDSPerformanceInsights O Performance Insights está ativado para o Amazon RDS.	• PerformanceInsightsRetentionPeriod: o número de dias para reter os dados do Performance Insights. Valores válidos: 7 ou mês * 31, em que mês é um número de meses de 1 a 23. Exemplos: 93 (3 meses* 31), 341 (11 meses* 31), 589 (19 meses* 31) ou 731. • PerformanceInsightsKMSKeyId : O ID da AWS KMS chave para criptografia dos dados do Performance Insights. Se você não especificar um valor para PerformanceInsights KMSKeyId, o Amazon RDS usará sua AWS KMS chave padrão. Sem restrições

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
c1fd6b9614 Logs de acesso do Amazon S3 habilitados	AWSManagedServices-TrustedRoleMediatorEnableBucketAccessLoggingV2 O registro de acesso ao bucket do Amazon S3 está ativado.	- TargetBucketTagValue: o valor da tag (com distinção entre maiúsculas e minúsculas) para identificar o bucket de destino, use-o e TargetBucketTagKey para marcar o bucket a ser usado como o bucket de destino para o registro de acesso. - TargetObjectKeyFormat: formato de chave do Amazon S3 para objetos de log (os valores diferenciam maiúsculas de minúsculas). Para usar o formato simples das chaves do S3 para objetos de log, escolha SimplePrefix . Para usar a chave S3 particionada para objetos de log e usar EventTime para o prefixo particionado, escolha. PartitionedPrefixEventTime Para usar a chave S3 particionada para objetos de log e usar DeliveryTime para o prefixo particionado, escolha. PartitionedPrefixDeliveryTime Os valores válidos são SimplePrefix , PartitionedPrefixEventTime e PartitionedPrefixDeliveryTime . Para habilitar a correção automática, o seguinte parâmetro pré-configurado deve ser fornecido: e.

Verifique o ID e o nome	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
		TargetBucketTagKeyTargetBucketTagValue O bucket de destino deve estar no mesmo bucket Região da AWS e Conta da AWS no bucket de origem, com as permissões corretas para entrega de registros. Para obter mais informações, consulte Habilitar registro em log de acesso ao servidor do Amazon S3.

Configurar Trusted Advisor a correção de cheques no Trusted Remediator

As configurações são armazenadas AWS AppConfig como parte do aplicativo Trusted Remediator. Cada categoria de Trusted Advisor verificação tem um perfil de configuração separado. Para obter mais informações sobre Trusted Advisor categorias, consulte [Exibir categorias de verificação](#).

Você pode solicitar a configuração de remediações por recurso ou por Trusted Advisor verificação. Você pode aplicar exceções usando tags de recursos.

Note

A correção das Trusted Advisor descobertas está atualmente configurada usando AWS AppConfig, e esse recurso é totalmente suportado atualmente. A AMS prevê que isso mudará no futuro. É uma prática recomendada evitar criar automações que dependam de AWS AppConfig, pois esse método está sujeito a alterações. Lembre-se de que talvez seja necessário atualizar ou modificar as automações criadas com base na AWS AppConfig implementação atual no futuro para fins de compatibilidade.

O sinalizador de recurso Compute Optimizer EC2 -> instances tem parâmetros extras:

- allow-upscale Para permitir o aumento da escala de instâncias subprovisionadas e não otimizadas. EC2 O valor padrão é "false".

- `min-savings-opportunity-percentage` A oportunidade mínima de porcentagem de economia para remediação automatizada. O valor padrão é 10%

Configurações padrão de remediação

As configurações para Trusted Advisor verificações individuais são armazenadas como AWS AppConfig sinalizadores. O nome da bandeira corresponde ao nome do cheque. Cada configuração de verificação contém os seguintes atributos:

- modo de execução: determina como o Trusted Remediator executa a remediação padrão:
 - Automatizado: o Trusted Remediator corrige automaticamente os recursos criando um OpsItem, executando o documento SSM e resolvendo-o após a OpsItem execução bem-sucedida.
 - Manual: Um OpsItem é criado, mas o documento SSM não é executado automaticamente. Você revisa OpsItem e executa a remediação usando o RFC automatizado. Para obter mais informações, consulte [Trabalhe com remediações no Trusted Remediator](#).
 - Condicional: a remediação está desativada por padrão. Você pode habilitá-lo para recursos específicos usando tags. Para obter mais informações, consulte as seções a seguir [Personalize a remediação com tags de recursos](#) [Personalize a remediação com tags de substituição de recursos](#) e.
 - Inativo: a remediação não ocorre e nenhuma OpsItem é criada. Você não pode substituir o modo de execução da Trusted Advisor verificação que está definida como inativa.
- parâmetros preconfigurados: insira valores para os parâmetros do documento SSM que são necessários para remediação automatizada, no formato de, separados por uma vírgula (`Parameter=Value,`). Consulte [Trusted Advisor verificações suportadas pelo Trusted Remediator](#) os parâmetros pré-configurados compatíveis para o documento SSM associado para cada verificação.
- `alternative-automation-document`: esse atributo ajuda a substituir o documento de automação existente por outro documento compatível (se disponível para a verificação específica). Por padrão, esse atributo não está selecionado.

Note

O `alternative-automation-document` atributo não é compatível com documentos de automação personalizados. Você pode usar os documentos de automação do Trusted

Remediator compatíveis existentes listados em [Trusted Advisor verificações suportadas pelo Trusted Remediator](#).

Por exemplo, para verificar Qch7DwouX1, há três documentos SSM associados: AWSManagedServices-StopEC2Instance, AWSManagedServices-ResizeInstanceByOneLevel, e AWSManagedServices-TerminateInstance. O valor de `alternative-automation-document` pode ser AWSManagedServices-ResizeInstanceByOneLevel ou AWSManagedServices-TerminateInstance (AWSManagedServices-StopEC2Instance é o documento SSM padrão a ser corrigido Qch7DwouX1).

O valor de cada atributo deve corresponder às restrições desse atributo.

Tip

Antes de aplicar as configurações padrão para suas Trusted Advisor verificações, é uma prática recomendada considerar o uso dos recursos de marcação de recursos e substituição de recursos descritos nas seções a seguir. As configurações padrão se aplicam a todos os recursos da conta, o que pode não ser desejável em todos os casos.

A seguir está um exemplo de captura de tela do console com o modo de execução definido como Manual e os atributos que correspondem às suas restrições.

Personalize a remediação com tags de recursos

Os `manual-for-tagged-only` e `automated-for-tagged-only` na configuração de verificação permitem que você especifique tags de recursos sobre como você deseja corrigir verificações individuais. É uma prática recomendada usar esse método quando você precisa aplicar um comportamento consistente de remediação a um grupo de recursos que compartilham a mesma tag ou tags. A seguir estão as descrições dessas tags:

- `automated-for-tagged-only`: especifique as tags de recursos (um ou mais pares de tags, separadas por vírgula) para que as verificações sejam corrigidas automaticamente, independentemente do modo de execução padrão.

- **manual-for-tagged-only**: especifique tags de recursos (um ou mais pares de tags, separados por vírgula) para correções que devem ser executadas manualmente, independentemente do modo de execução padrão.

Por exemplo, se você quiser habilitar a remediação automatizada para todos os recursos que não são de produção e impor a correção manual para os recursos de produção, você pode definir sua configuração da seguinte forma:

```
"execution-mode": "Conditional",  
"automated-for-tagged-only": "Environment=Non-Production",  
"manual-for-tagged-only": "Environment=Production",
```

Com as configurações anteriores definidas em seus recursos, verifique se o comportamento da correção é o seguinte:

- Os recursos marcados com 'Environment=Non-Production' são corrigidos automaticamente.
- Recursos marcados com 'Environment=Production' requerem intervenção manual para remediação.
- Recursos sem a tag 'Ambiente' seguem o modo de execução padrão ('Conditional', neste caso). Portanto, nenhuma ação é tomada com os recursos restantes).

Para obter suporte adicional com suas configurações, entre em contato com seu Cloud Architect.

Personalize a remediação com tags de substituição de recursos

As tags de substituição de recursos permitem que você personalize o comportamento de remediação de recursos individuais, independentemente de suas tags. Ao adicionar uma tag específica a um recurso, você substitui o modo de execução padrão desse recurso e a Trusted Advisor verificação. A tag de substituição de recursos tem precedência sobre a configuração padrão e as configurações de marcação de recursos. Portanto, se você definir o modo de execução padrão como Automatizado, Manual ou Condicional para um recurso usando a tag de substituição de recursos, ele substituirá o modo de execução padrão e todas as configurações de marcação de recursos.

Para substituir o modo de execução de um recurso, conclua as seguintes etapas:

1. Identifique os recursos para os quais você deseja substituir a configuração de remediação.

2. Determine o Trusted Advisor ID do cheque que você deseja substituir. Você pode encontrar a verificação IDs de Trusted Advisor check-ins compatíveis [Trusted Advisor verificações suportadas pelo Trusted Remediator](#).
3. Adicione uma tag aos recursos com a chave e o valor a seguir usando o tipo de alteração [Tag | Update](#) ou [Tag | Bulk Update](#):
 - Chave de tag: **TR-*Trusted Advisor check ID*-Execution-Mode** (diferencia maiúsculas de minúsculas)

No exemplo de chave de tag anterior, Trusted Advisor check ID substitua pelo identificador exclusivo da Trusted Advisor verificação que você deseja substituir.

- Valor da tag: use um dos seguintes valores para o valor da tag:
 - Automatizado: o Trusted Remediator corrige automaticamente o recurso para essa Trusted Advisor verificação.
 - Manual: Um OpsItem é criado para o recurso, mas a correção não é executada automaticamente. Você revisa e executa a remediação usando o automatizado. Para obter mais informações, consulte [Trabalhe com remediações no Trusted Remediator](#).
 - Inativo: a correção e a OpsItem criação não são realizadas para esse recurso e para a verificação especificada Trusted Advisor .

Por exemplo, para corrigir automaticamente um volume do Amazon EBS com o ID do Trusted Advisor cheque, DAvU99Dc4C adicione uma tag ao volume do EBS. A chave da tag é TR-DAvU99Dc4C-Execution-Mode e o valor da tag éAutomated.

Veja a seguir um exemplo do console mostrando a seção Tags:

Fluxo de trabalho de decisão do modo execução

Há vários níveis para configurar o modo de execução para seus recursos e cada Trusted Advisor verificação. O diagrama a seguir mostra como o Trusted Remediator decide qual modo de execução usar com base em suas configurações:

Configurar tutoriais de remediação

Os tutoriais a seguir fornecem exemplos de criação de remediações comuns no Trusted Remediator.

Corrija todos os recursos manualmente

Este exemplo configura a remediação manual para todos os volumes do Amazon EBS com o ID de Trusted Advisor verificação DAv U99Dc4C (volumes subutilizados do Amazon EBS).

Configure a remediação manual para volumes do Amazon EBS com o ID de verificação U99Dc4C DAv

1. Use a Configuração de Remediação|Atualização, altere o tipo para solicitar a atualização da configuração.
2. Insira os seguintes parâmetros:
 - CheckIds: DAv U99Dc4C
 - ExecutionMode: Manual

Note

Várias verificações podem ser configuradas em uma única solicitação. Para verificações que exigem a mesma configuração, inclua várias verificações IDs no CheckIdsparâmetro. Para verificações que exigem uma configuração diferente, crie um novo RemediationConfigurationobjeto.

3. Envie o RFC.

Corrija todos os recursos automaticamente, exceto os recursos selecionados

Este exemplo configura a remediação automática para todos os volumes do Amazon EBS com o ID de Trusted Advisor verificação DAv U99Dc4C (volumes subutilizados do Amazon EBS), com exceção dos volumes especificados que não serão corrigidos (designados como inativos).

Configure a remediação automática para volumes do Amazon EBS com o ID de verificação DAv U99Dc4C, com exceção dos recursos inativos selecionados

1. Substitua a remediação automatizada para volumes selecionados do Amazon EBS:

Use o tipo de alteração [Tag | Update](#) ou [Tag | Bulk Update](#) para aplicar a seguinte tag aos volumes a serem excluídos da remediação automática:

- Chave: Modo de execução TR- DAv U99Dc4C
 - Valor: Inativo
2. Use o tipo de alteração Configuração de remediação|Atualização para solicitar a atualização da configuração.
 3. Insira os seguintes parâmetros:
 - CheckIds: DAv U99Dc4C
 - ExecutionMode: Automatizado
 4. Envie o RFC.

Corrija recursos marcados automaticamente

Este exemplo configura a remediação automática para todos os volumes do Amazon EBS com a tag `Stage=NonProd` com o ID de Trusted Advisor verificação DAv U99Dc4C (volumes subutilizados do Amazon EBS). Todos os outros recursos sem essa tag não são corrigidos.

Configure a remediação automática para volumes do Amazon EBS com a tag **Stage=NonProd** para ID de verificação U99Dc4C DAv

1. Use a [Configuração de Remediação | Atualizar](#), alterar o tipo para solicitar a atualização da configuração.
2. Insira os seguintes parâmetros:
 - CheckIds: DAv U99Dc4C
 - ExecutionMode: Condicional
 - AutomatedForTaggedOnly: {"Palco": "NonProd"}

Note

O valor especificado para o AutomatedForTaggedOnly parâmetro substitui o valor configurado anteriormente. Para manter as tags existentes, inclua-as no novo valor.

3. Envie o RFC.

Redefinir a configuração para o padrão

Este exemplo remove a `automated-for-tagged-only` configuração existente para a verificação Hs4Ma3G104. Para remover a configuração de tag aplicada anteriormente, defina o valor do `AutomatedForTaggedOnly` parâmetro como `{}`.

Redefina a configuração para o padrão para verificar Hs4Ma3G104

1. Use o tipo de alteração [Configuração de remediação | Atualizar](#) para solicitar a atualização da configuração.
2. Insira os seguintes parâmetros:
 - `CheckIds`: Hs4Ma3G104
 - `ExecutionMode`: insira o valor usado atualmente
 - `AutomatedForTaggedOnly`: `{}`
3. Envie o RFC.

Trabalhe com remediações no Trusted Remediator

Rastreie as remediações no Trusted Remediator

Para rastrear OpsItems as remediações, conclua as seguintes etapas:

1. Abra o AWS Systems Manager console em <https://console.aws.amazon.com/systems-manager/>.
2. Escolha Gerenciamento de operações, OpsCenter.
3. (Opcional) Filtre a lista por `Source=Trusted Remediator` para incluir somente Trusted OpsItems Remediator na lista.

Veja a seguir um exemplo da OpsCenter tela filtrada pelo `Source=Trusted Remediator`:

Note

Além OpsItems de visualizar a partir do OpsCenter, você pode visualizar os registros de remediação no bucket do AMS S3. Para obter mais informações, consulte [Registros de remediação no Trusted Remediator](#).

Execute correções manuais no Trusted Remediator

O Trusted Remediator cria OpsItems para verificações configuradas para remediação manual. Você deve revisar essas verificações e iniciar o processo de remediação manualmente.

Para corrigir manualmente o OpsItem, conclua as seguintes etapas:

1. Abra o AWS Systems Manager console em <https://console.aws.amazon.com/systems-manager/>.
2. Escolha Gerenciamento de operações, OpsCenter.
3. (Opcional) Filtre a lista por Source=Trusted Remediator para incluir somente Trusted OpsItems Remediator na lista.
4. Escolha o OpsItem que você deseja revisar.
5. Revise os dados operacionais do OpsItem. Os dados operacionais incluem os seguintes itens:
 - trustedAdvisorCheckCategoria: A categoria da ID do Trusted Advisor cheque. Por exemplo, tolerância a falhas
 - trustedAdvisorCheckID: O ID exclusivo do Trusted Advisor cheque.
 - trustedAdvisorCheckMetadados: os metadados do recurso, incluindo o ID do recurso.
 - trustedAdvisorCheckNome: O nome do Trusted Advisor cheque.
 - trustedAdvisorCheckStatus: O status da Trusted Advisor verificação detectada para o recurso.
 - trustedAdvisorCheckManualRemediation: os dados personalizados que fornecem detalhes de referência para remediação manual.
 - ManualExecutionInput: um objeto que define parâmetros para os quais você pode modificar valores ao executar a correção manual.
 - DocumentName: O nome do runbook (documento SSM).
 - CustomizableParameters: nomes de parâmetros que você pode modificar.
 - DefaultInput: um objeto que define nomes e valores de parâmetros a serem usados para remediação manual. Os valores são preenchidos com base em parâmetros pré-configurados.
6. Para corrigir manualmente o OpsItem, conclua as seguintes etapas:
 - a. Use o [Trusted Remediator | Finding | Corrija o tipo de alteração ct-1c7ch8z5phrjp](#)
 - b. Use os valores para os seguintes parâmetros.
 - DocumentName: Deve ser AWSManagedServices-RemediateTrustedRemediatorFinding.

- Região: A Região da AWS, no formato us-east-1.
- Parâmetros: insira os parâmetros de remediação manual:
 - OpsItemId: A ID do item de operações.
 - RemediationDocumentName: o nome do documento de automação do SSM a ser usado. O documento deve estar associado ao Item de Operações. Se vários documentos estiverem associados ao Item de Operações, eles DocumentName devem ser especificados.
 - RemediationParameters: Um key/value mapa de parâmetros para a execução da automação, no formato: `{\"ParameterName1\": [\"ParameterValue1\"], \"ParameterName2\": [\"ParameterValue2\"]}`. Você só pode usar parâmetros que estão presentes no Item de Operações trustedAdvisorCheckManualRemediation CustomizableParameters. Se não forem especificados, os parâmetros e valores serão recuperados do Item de Operações.
- c. Escolha 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.
- d. Monitore o progresso da execução do RFC.
- e. Depois que a execução for concluída, o OpsItem será resolvido. Se o RFC falhar, siga as etapas em [Solucionar problemas de remediações no Trusted Remediator](#). Para obter suporte adicional para solução de problemas, entre em contato com a AMS.

Solucionar problemas de remediações no Trusted Remediator

Para obter ajuda com correções manuais e falhas de remediação, entre em contato com a AMS.

Para ver o status e os resultados da remediação, conclua as seguintes etapas:

1. Abra o AWS Systems Manager console em <https://console.aws.amazon.com/systems-manager/>.
2. Escolha Gerenciamento de operações, OpsCenter.
3. (Opcional) Filtre a lista por Source=Trusted Remediator para incluir somente Trusted OpsItems Remediator na lista.
4. Escolha o OpsItem que você deseja revisar.
5. Na seção Execuções de automação, revise o nome e o status do documento e os resultados.
6. Analise as seguintes falhas comuns de automação. Se seus problemas não estiverem listados aqui, entre em contato com seu CSDM para obter ajuda.

Erros comuns de remediação

Nenhuma execução está listada em Execuções de automação

Nenhuma execução associada ao OpsItem pode indicar que a execução falhou ao iniciar devido a valores de parâmetros incorretos.

Etapas de solução de problemas

1. Nos dados operacionais, revise o valor da `trustedAdvisorCheckAutoRemediation` propriedade.
2. Verifique se os valores `DocumentName` dos parâmetros estão corretos. Para obter os valores corretos, consulte [Configurar Trusted Advisor a correção de cheques no Trusted Remediator](#) os detalhes sobre como configurar os parâmetros do SSM. Para analisar os parâmetros de verificação compatíveis, consulte [Trusted Advisor verificações suportadas pelo Trusted Remediator](#)
3. Verifique se os valores no documento SSM correspondem aos padrões permitidos. Para visualizar os detalhes dos parâmetros no conteúdo do documento, selecione o nome do documento na seção Runbooks.
4. Depois de revisar e corrigir os parâmetros, corrija manualmente o OpsItem. Para as etapas de remediação, consulte [Execute correções manuais no Trusted Remediator](#).
5. Para evitar que esse erro ocorra novamente, certifique-se de configurar a correção com os valores de parâmetros corretos em sua configuração. Para obter mais informações, consulte [Configurar Trusted Advisor a correção de cheques no Trusted Remediator](#).

Execuções com falha em execuções de automação

Os documentos de remediação contêm várias etapas que interagem com a Serviços da AWS execução de várias ações. APIs Para identificar uma causa específica para a falha, conclua as seguintes etapas:

Etapas de solução de problemas

1. Para visualizar as etapas de execução individuais, escolha o link ID de execução na seção Execuções de automação. Veja a seguir um exemplo do console do Systems Manager mostrando as etapas de execução de uma automação selecionada:
2. Escolha a etapa com o status Falha. Veja a seguir exemplos de mensagens de erro:

- NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist

Esse erro indica que o nome incorreto do bucket foi especificado nos parâmetros pré-configurados da configuração de remediação.

Para resolver esse erro, [execute manualmente a automação](#) usando o nome correto do bucket. Para evitar que esse problema ocorra novamente, [atualize a configuração de remediação](#) com o nome correto do bucket.

- DB instance my-db-instance-1 is not in available status for modification.

Esse erro indica que a automação não pôde fazer as alterações esperadas porque a instância de banco de dados estava em um estado inválido.

Para resolver esse erro, [execute manualmente a automação](#).

Registros de remediação no Trusted Remediator

O Trusted Remediator cria registros no formato JSON e os carrega no Amazon Simple Storage Service. Os arquivos de log são enviados para um bucket do S3 criado pelo AMS e nomeado. `ams-trusted-remediator-{your-account-id}-logs` O AMS cria o bucket do S3 na conta do administrador delegado. Você pode importar os arquivos de log QuickSight para gerar relatórios de remediação personalizados.

Registro de itens de remediação

O Trusted Remediator cria o Remediation item log quando uma remediação OpsItem é criada. Esse registro contém remediação manual OpsItem e remediação automatizada. OpsItem Você pode usar o Remediation item log para acompanhar a visão geral de todas as remediações.

Localização do log do item de remediação para recomendações do Compute Optimizer

`s3://ams-trusted-remediator-delegated-administrator-account-id-logs/compute_optimizer_remediation_items/remediation creation time in yyyy-mm-dd format/10 digits epoch time or unix timestamp-Trusted Advisor check ID-Resource ID.json`

Localização do registro do item de remediação para verificações Trusted Advisor

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs/
remediation_items/*remediation creation time in yyyy-mm-dd format/10 digits*
epoch time or unix timestamp-Trusted Advisor check ID- Resource ID.json

URL do arquivo de amostra de registro do item de remediação

s3:///ams-trusted-remediator-*111122223333*-logs/
remediation_items/*2023-02-06/1675660464-DAvU99Dc4C-*
vol-00bd8965660b4c16d.json

Formato de registro de itens de remediação do Compute Optimizer

```
{
  "AccountID": "Account_ID",
  "ComputeOptimizerCheckID": "Compute Optimizer check ID",
  "ComputeOptimizerCheckName": "Compute Optimizer check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

Trusted Advisor Formato de registro do item de remediação

```
{
  "TrustedAdvisorCheckID": Trusted Advisor check ID,
  "TrustedAdvisorCheckName": Trusted Advisor check name,
  "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
  "ResourceID": Resource ID,
  "RemediationTime": Remediation creation time,
  "ExecutionMode": Automated or Manual,
  "OpsItemID": OpsItem ID
}
```

Conteúdo de amostra do formato de registro do item de remediação do Compute Optimizer

```
{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
}
```



```

"RemediationTime": 1755044783,
"ExecutionMode": "Manual",
"OpsItemID": "oi-b8888b38fe78"
}

```

Trusted Advisor Exemplo de conteúdo do formato de registro do item de remediação

```

{
  "TrustedAdvisorCheckID": "DAvU99Dc4C",
  "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
  "TrustedAdvisorCheckResultTime": 1675614749,
  "ResourceID": "vol-00bd8965660b4c16d",
  "RemediationTime": 1675660464,
  "OpsItemID": "oi-cca5df7af718"
}

```

Registro de execução de remediação automatizado, Compute Optimizer e Trusted Advisor

O Trusted Remediator cria o Automated remediation execution log quando uma execução automatizada de documentos SSM é concluída. Esse registro contém detalhes da execução do SSM somente para remediação OpsItem automatizada. Você pode usar esse arquivo de log para rastrear remediações automatizadas.

Compute Optimizer Localização automatizada do registro de remediação

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs//
remediation_executions/*remediation creation time in yyyy-mm-dd format/10*
digits epoch time or unix timestamp-Compute Optimizer recommendation
ID.json

Trusted Advisor Localização automatizada do registro de remediação

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs//
remediation_executions/*remediation creation time in yyyy-mm-dd format/10*
digits epoch time or unix timestamp-Trusted Advisor check ID-Resource
ID.json

Exemplo de localização do log de remediação automatizado do Compute Optimizer

```
s3://ams-trusted-remediator-111122223333-logs/  
remediation_executions/2025-06-26/1750908858-123456789012-compute-  
optimizer-ec2-i-1235173471d2cd789.json
```

Trusted Advisor Exemplo de localização automatizada do registro de remediação

```
s3://ams-trusted-remediator-111122223333-logs/  
remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-  
vol-00bd8965660b4c16d.json
```

Exemplo de conteúdo do formato de registro de remediação automatizado

```
{  
  "OpsItemID": "oi-767c77e05301",  
  "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",  
  "SSMExecutionStatus": "Success"}
```

Melhores práticas no Trusted Remediator

A seguir estão as melhores práticas para ajudá-lo a usar o Trusted Remediator:

- Se você não tiver certeza sobre os resultados da correção, comece com o modo de execução manual. Às vezes, aplicar a execução automatizada para remediações desde o início pode causar resultados inesperados.
- Faça uma análise semanal das remediações e obtenha informações sobre OpsItems os resultados do Trusted Remediator.
- As contas dos membros herdam as configurações da conta do administrador delegado. Portanto, é importante estruturar as contas de uma forma que ajude você a gerenciar várias contas com as mesmas configurações. Você pode isentar recursos da configuração padrão usando tags.

Remediador confiável FAQs

A seguir estão as perguntas mais frequentes sobre o Trusted Remediator:

O que é Trusted Remediator e como ele me beneficia?

Quando uma não conformidade é identificada Trusted Advisor ou uma recomendação é emitida pelo Compute Optimizer, o Trusted Remediator responde de acordo com suas preferências especificadas,

seja aplicando correções, buscando aprovação por meio de correções manuais ou relatando as correções durante sua próxima Análise Empresarial Mensal (MBR). A remediação acontece no horário ou no cronograma de remediação de sua preferência. O Trusted Remediator oferece a capacidade de autoatendimento e de Trusted Advisor realizar verificações com a flexibilidade de configurar e corrigir verificações individualmente ou em massa. Com uma biblioteca de documentos de remediação testados, o AMS constantemente aumenta suas contas aplicando verificações de segurança e seguindo as AWS melhores práticas. Você só será notificado se especificar isso em sua configuração. Os usuários do AMS podem optar pelo Trusted Remediator sem custo adicional.

Como o Trusted Remediator se relaciona e trabalha com outros Serviços da AWS?

Você tem acesso a Trusted Advisor verificações e recomendações do Compute Optimizer como parte do seu plano atual de Enterprise Support. O Trusted Remediator se integra ao Trusted Advisor Compute Optimizer para aproveitar os recursos existentes de automação do AMS. Especificamente, o AMS usa documentos de AWS Systems Manager automação (runbooks) para remediações automatizadas. AWS AppConfig é usado para configurar os fluxos de trabalho de remediação. Você pode ver todas as remediações atuais e passadas por meio do Systems Manager OpsCenter. Os registros de remediação são armazenados em um bucket do Amazon S3. Você pode usar os registros para importar e criar painéis de relatórios personalizados no QuickSight.

Quem configura as remediações?

Você é o proprietário das configurações da sua conta. Gerenciar suas configurações é de sua responsabilidade. Você também pode entrar em contato com o AMS para obter alterações na configuração, suporte e remediações manuais, além de solucionar falhas de remediação.

Como faço para instalar documentos de automação SSM?

Os documentos de automação do SSM são compartilhados automaticamente com contas AMS integradas.

Os recursos de propriedade da AMS também serão corrigidos?

Os recursos de propriedade da AMS não são sinalizados pelo Trusted Remediator. O Trusted Remediator se concentra apenas em seus recursos.

Em Regiões da AWS que o Trusted Remediator está disponível e quem pode usá-lo?

O Trusted Remediator está disponível para clientes do AMS Advanced. Para obter uma lista atual das regiões de suporte, consulte [Serviços da AWS por região](#).

O Trusted Remediator causará desvio de recursos?

Como os documentos de automação do SSM atualizam diretamente os recursos por meio da AWS API, pode ocorrer desvio de recursos. Você pode usar tags para segregar recursos criados por meio de seus pacotes existentes CI/CD . Você pode configurar o Trusted Remediator para ignorar os recursos marcados e, ao mesmo tempo, remediar seus outros recursos.

Como faço para pausar ou parar o Trusted Remediator?

Use o [Gerenciamento | Trusted Remediator | State | Ativar ou desativar](#) o tipo de alteração para interromper o serviço Trusted Remediator. Use o mesmo tipo de alteração para reativar o Trusted Remediator.

Como posso corrigir verificações que não são suportadas pelo Trusted Remediator?

Você pode continuar entrando em contato com o AMS por meio do Operations On Demand (OOD) para verificar verificações não suportadas. O AMS ajuda você a corrigir essas verificações. Para obter mais informações, consulte [Operations On Demand](#).

Quais recursos o Trusted Remediator implanta em suas contas?

O Trusted Remediator implanta os seguintes recursos na conta de administrador delegado do Trusted Remediator:

- Um bucket do Amazon S3 nomeado `ams-trusted-remediator-{your-account-id}-logs`. O Trusted Remediator cria o formato JSON quando uma remediação OpsItem é criada e carrega os arquivos de log `Remediation item log` nesse bucket.
- Um AWS AppConfig aplicativo para manter as configurações de remediação para Trusted Advisor verificações suportadas e recomendações do Compute Optimizer.

O Trusted Remediator não implanta recursos na conta de membro do Trusted Remediator.

Gerenciamento de logs

Tópicos

- [O que é gerenciamento de registros?](#)
- [Como funciona o registro do AMS](#)
- [Acessar os logs no](#)
- [Personalizando sua configuração de log](#)

O gerenciamento de registros do AMS coleta, agrega e controla a retenção dos registros da conta gerenciada. AWS o gerenciamento de registros agrega registros de EC2 instâncias e AWS recursos da Amazon implantados em sua conta CloudWatch no Logs. A lista completa dos serviços dos quais os registros são agregados atualmente pode ser encontrada em [Registros de serviços agregados do AMS](#).

O que é gerenciamento de registros?

O gerenciamento de registros é o processo de lidar com eventos de log gerados por instâncias, aplicativos e serviços da AWS. Esse recurso define como o AMS processa, armazena e gira os eventos de log gerados em sua conta gerenciada da AWS. Os registros de infraestrutura são usados durante a resolução de incidentes e para apoiar as auditorias do sistema.

Como funciona o registro do AMS

O gerenciamento de registros do AMS single-account landing zone (SALZ) usa uma variedade de agentes e ferramentas pré-instalados que são implementados quando instâncias e aplicativos são integrados ou provisionados.

O registro é configurado durante o processo de integração da conta e quando uma pilha é lançada.

Os registros do AMS multi-account landing zone (MALZ) produzidos por instâncias e serviços da AWS estão disponíveis em CloudWatch Logs ou Amazon Simple Storage Service (Amazon S3), dentro de cada conta gerenciada pelo AMS. O landing zone de várias contas do AMS fornece uma conta de registro central que atua como um local central de agregação para alguns registros produzidos por contas de aplicativos individuais.

As tabelas nas [Acessar os logs no](#) subseções descrevem quais registros estão disponíveis em contas individuais e quais estão disponíveis na conta de registro central.

Acessar os logs no

Para acessar seus registros, verifique se você tem uma das funções necessárias do IAM e está em sua conta do AMS. Em seguida, navegue até o diretório mostrado.

Multi-Account Landing Zone (MALZ)

Fornece cinco funções padrão do IAM, cada uma das quais permite acesso a todos os registros da sua conta (todos são prefaciados com `AWSManagedServices`):

- `AdminRole`
- `CaseRole`
- `ChangeManagementRole`
- `ReadOnlyRole`
- `SecurityOpsRole`

O acesso a essas funções é configurado por meio de federação, com cada função sendo mapeada para um grupo dentro do seu domínio do Active Directory.

Para saber mais sobre essas funções, consulte [Função de usuário do IAM no AMS](#).

Single-Account Landing Zone (SALZ)

O padrão `Customer_ReadOnly_Role` para a landing zone de conta única do AMS permite que você acesse todos os registros da sua conta. O acesso aos registros é controlado usando funções do AWS Identity and Access Management (IAM) mapeadas para grupos do Active Directory.

Registros de serviços agregados do AMS

Cada AWS serviço é registrado no CloudWatch Logs ou em um local específico em um bucket do Amazon S3.

Note

A menos que especificamente declarado, todos os locais de registro são locais da conta que gerou os registros e não são agregados à conta central do Logging.

Para encontrar os nomes padrão das CloudTrail trilhas do AMS nas contas SALZ e MALZ, acesse o AWS Console CloudTrail e, em seguida, até a página Trails e pesquise por AMS. Como os recursos do AMS têm tags, você pode encontrar as trilhas dessa forma. Exemplo de CloudTrail tag AMS:

```
Environment    AMSInfrastructure
```

Para acessar seus registros, verifique se você tem uma das funções necessárias do IAM e está em sua conta do AMS. Em seguida, navegue até o diretório mostrado.

Multi-Account Landing Zone

Registros de serviços agregados da landing zone com várias contas do AMS

	Nome do serviço	Detalhes dos logs	Localização do registro
1	Amazon Aurora	Registros gerais, lentos de consultas e erros.	CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/{ <i>log_name</i> }
2	AWS CloudFormation (CFN)	Somente registro de chamadas de API.	AWS CloudFormation As chamadas de API são documentadas por meio de CloudTrail, que envia seus registros para o CloudWatch LogGroup e depois sincroniza os registros em um bucket do S3. Por padrão, os registros são retidos por 14 dias no CloudWatch LogGroup e são retidos indefinidamente no bucket do S3.

	Nome do serviço	Detalhes dos logs	Localização do registro
			CloudWatch LogGroup:/CloudTrail/Registros da zona de pouso Bucket S3 [na conta de registro central]: aws-landing-zone-logs-ams-a {} -log-management-<i>{account_ID } region</i> Caminho:AWSLogs/<i>{account_ID }</i>/CloudTrail/
3	Amazon CloudFront (CloudFront)	Registro de solicitações do usuário. CloudFront o registro deve ser ativado explicitamente. Para mais informações, consulte Habilitando o registro para serviços compatíveis .	Bucket S3: ams-a {} -log-management- <i>{account_ID } region</i> Caminho: RedShift AWS/ {} <i>CloudFront distribution ID</i>
4	Amazon CloudWatch (CloudWatch)	Somente registro de chamadas de API.	CloudWatch LogGroup:/CloudTrail/Registros da zona de pouso Bucket S3 [na conta de registro central]: aws-landing-zone-logs -<i>{account_ID } - {region}</i> Caminho:AWSLogs/<i>{account_ID }</i>/CloudTrail/
5	Amazon Elastic Block Store (Amazon EBS)	Nenhum registro é produzido pelo serviço EBS.	Não aplicável

	Nome do serviço	Detalhes dos logs	Localização do registro
6	Nuvem de computação elástica da Amazon (Amazon EC2)	Registros do sistema e do aplicativo. Para obter informações, consulte Amazon Elastic Compute Cloud (Amazon EC2) — registros em nível de sistema o.	CloudWatch Registros:/{ <i>instance ID</i> }
7	Amazon Elastic File System (Amazon EFS)	Somente registro de chamadas de API.	CloudWatch LogGroup:/CloudTrail/Registros da zona de pouso Bucket S3 [na conta de registro central]: aws-landing-zone-logs - {<i>account_ID</i>} - {<i>region</i>} Caminho:AWSLogs/{<i>account_ID</i>}/CloudTrail/

	Nome do serviço	Detalhes dos logs	Localização do registro
8	Elastic Load Balancing (ELB)	Entradas de registro de acesso e erro. Os balanceadores de carga elásticos registram todas as solicitações enviadas a eles, incluindo solicitações que não são roteadas para instâncias de back-end. Por exemplo, se um cliente enviar uma solicitação malformada ou se não houver instâncias íntegras para responder, a solicitação ainda será registrada. Para obter mais informações sobre as entradas de log do Elastic Load Balancing, consulte - Balanceadores de carga clássicos: entradas de registro de acesso. - Balanceadores de carga de aplicativos: entradas de registro de acesso. - Balanceadores de carga de rede: entradas de registro de acesso.	Registros de chamadas da API: CloudWatch LogGroup:/CloudTrail/Registros da zona de pouso Bucket S3 [na conta de registro central]: aws-landing-zone-logs - {account_ID} - {region} Caminho:AWSLogs/{account_ID}/CloudTrail/ Logs de acesso: Balde S3: mc-a {account_ID} - logs {region} Caminho: aws/elbaccess

	Nome do serviço	Detalhes dos logs	Localização do registro
9	Amazon OpenSearch Service (OpenSearch Serviço)	Registros de erros de serviço. Você deve habilitar explicitamente o OpenSearch registro. Para obter mais informações, consulte Habilitando o registro para serviços compatíveis	CloudWatch LogGroup:/CloudTrail/Registros da zona de pouso Bucket S3 [na conta de registro central]: aws-landing-zone-logs - <i>{account_ID}</i> - <i>{region}</i> Caminho:AWSLogs/ <i>{account_ID}</i> /CloudTrail/
10	Amazon ElastiCache	Somente registro de chamadas de API.	CloudWatch LogGroup://CloudTrail/Registros da zona de pouso
11	Amazon GuardDuty		Bucket S3 [na conta de registro central]: aws-landing-zone-logs - <i>{account_ID}</i> - <i>{region}</i>
12	Amazon Inspector		Caminho:AWSLogs/ <i>{account_ID}</i> /CloudTrail/
13	Amazon Macie		
14	Amazon Redshift	Registros de conexão, usuário e atividade. Por padrão, o registro em log é ativado quando você cria seu cluster do Redshift invocando o Create Redshift cluster CT (ct-1malj7snzxrkr). Para obter informações, consulte Registro de auditoria do banco de dados .	Bucket S3: ams-a {} -log-management- <i>{account_ID}</i> <i>region</i> Caminho: /AWS/ {} RedShift <i>CloudFront Distribution ID</i>

	Nome do serviço	Detalhes dos logs	Localização do registro
15	Amazon Relational Database Service (RDS)	Registros específicos para o tipo de banco de dados. Você deve habilitar explicitamente o registro do RDS. Para obter mais informações, consulte Habilitando o registro para serviços compatíveis Você só pode acessar os registros do MSSQL por meio de um procedimento armazenado; para obter informações, consulte Arquivamento de arquivos de log.	CloudWatch LogGroup: /aws/rds/ (<i>instance</i>ou<i>cluster</i>)/ {}/{ <i>database_name</i> <i>log_name</i>
16	Amazon S3 (S3)	Registros de acesso ao bucket. Cada registro de registro de acesso fornece detalhes sobre uma única solicitação de acesso, como solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e código de erro (se houver). As informações de log de acesso podem ser úteis em auditorias de segurança e acesso. Isso também pode ajudá-lo a conhecer sua base de clientes e entender a conta do Amazon S3. Para obter mais informações sobre as entradas do S3 Access Log, consulte S3 Server Access Log Format.	Compartimento S3: mc-a {<i>account_ID</i> } -log-management- { <i>region</i> Caminho: /aws/s3access/ { <i>bucket_name</i> Bucket S3 [na conta de registro central]: aws-landing-zone-s3-access-logs- { } - { <i>account_ID</i> <i>region</i> Caminho: /

	Nome do serviço	Detalhes dos logs	Localização do registro
17	Amazon Simple Email Service (SES)	Chamadas de serviço da API SES.	CloudWatch LogGroup:/CloudTrail/Registros da zona de pouso Bucket S3 [na conta de registro central]: aws-landing-zone-logs - {account_ID} - {region} Caminho:AWSLogs/{account_ID}/CloudTrail/
18	Amazon Virtual Private Cloud (VPC)	Dados de fluxo da VPC (informações sobre o tráfego IP que entra e sai das interfaces de rede da VPC).	CloudWatch LogGroup: /aws/vpcflow/ { VPC_ID
19	ajuste de escala automático	Somente registro de chamadas de API.	CloudWatch LogGroup:/CloudTrail/Registros da zona de pouso Bucket S3 [na conta de registro central]: aws-landing-zone-logs - {account_ID} - {region} Caminho:AWSLogs/{account_ID}/CloudTrail/
20	AWS Certificate Manager		
21	AWS CodeDeploy	Registros de implantação específicos da instância.	Por instância

	Nome do serviço	Detalhes dos logs	Localização do registro
22	AWS Config	Chamadas de serviço da API AWS Config.	CloudWatch LogGroup:/CloudTrail/Registros da zona de pouso Bucket S3 [na conta de registro central]: aws-landing-zone-logs - {account_ID} - {region} Caminho:AWSLogs/{ account_ID }/CloudTrail/
		Alterações na configuração dos recursos, conforme monitorado pelo AWS Config.	Bucket S3 [na conta de registro central]: aws-landing-zone-logs - {account_ID} - {region} Caminho:AWSLogs/{ account_ID }/Config/
23	AWS Database Migration Service	Registros de migração do banco de dados. Para obter informações, consulte Introdução ao gerenciamento de logs no AWS Database Migration Service .	console de migração de banco de dados
24	AWS Direct Connect (DX)	Somente registro de chamadas de API.	CloudWatch LogGroup:/CloudTrail/Registros da zona de pouso
25	AWS Glacier		Bucket S3 [na conta de registro central]: aws-landing-zone-logs - {account_ID} - {region}
26	AWS IAM (IAM)		
27	AWS Key Management Service		Caminho:AWSLogs/{ account_ID }/CloudTrail/

	Nome do serviço	Detalhes dos logs	Localização do registro
28	Console de gerenciamento da AWS (console ou console da AWS)		
29	AWS Simple Notification Service (SNS)		
30	AWS Simple Queueing Service (SQS)		

Single-Account Landing Zone

Registros de serviços agregados da landing zone de conta única do AMS

	Nome do serviço	Detalhes dos logs	Localização do registro
1	Amazon Aurora	Registros gerais, lentos de consultas e erros.	CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/{ <i>log_name</i> }
2	Amazon CloudFormation (CloudFormation ou CFN)	Somente registro de chamadas de API.	CloudFormation As chamadas de API são documentadas por meio de CloudTrail, que envia seus registros para o CloudWatch LogGroup e depois sincroniza os registros em um bucket do S3. CloudWatch LogGroup: /aws/ams/cloudtrail

	Nome do serviço	Detalhes dos logs	Localização do registro
3	Amazon CloudFront (CloudFront)	Registro de solicitações do usuário. Você deve habilitar explicitamente o CloudFront registro. Para obter mais informações, consulte Habilitando o registro para serviços compatíveis	Bucket S3: ams-a {} -log-management- {<i>account_ID</i> } <i>region</i> Bucket S3: ams-a {} -log-management- {<i>account_ID</i> } <i>region</i> Caminho: RedShift AWS/ {} <i>CloudFront_distribution_ID</i>
4	Amazon CloudWatch (CloudWatch)	Somente registro de chamadas de API.	CloudWatch LogGroup: /aws/ams/cloudtrail
5	Amazon Elastic Block Store (EBS)	Nenhum registro é produzido pelo serviço EBS.	Não aplicável
6	Nuvem de computação elástica Amazon () EC2	Registros do sistema e do aplicativo. Para obter informações, consulte Amazon Elastic Compute Cloud (Amazon EC2) — registros em nível de sistema o.	CloudWatch Registros: / { <i>instance_ID</i> }
7	Amazon Elastic File System (Amazon EFS)	Somente registro de chamadas de API.	CloudWatch LogGroup: /aws/ams/cloudtrail

	Nome do serviço	Detalhes dos logs	Localização do registro
8	Elastic Load Balancing (ELB)	Entradas de registro de acesso e erro. Os balanceadores de carga elásticos registram todas as solicitações enviadas a eles, incluindo solicitações que não são roteadas para instâncias de back-end. Por exemplo, se um cliente enviar uma solicitação malformada ou se não houver instâncias íntegras para responder , a solicitação ainda será registrada. Para obter mais informações sobre as entradas de log do Elastic Load Balancer, consulte • Balanceadores de carga clássicos: entradas de registro de acesso. • Balanceadores de carga de aplicativos: entradas de registro de acesso. • Balanceadores de carga de rede: entradas de registro de acesso.	CloudWatch LogGroup: /aws/ams/cloudtrail Bal de S3: mc-a {<i>account_ID</i>} - logs- {} <i>region</i> Caminho: aws/elbaccess

	Nome do serviço	Detalhes dos logs	Localização do registro
9	Amazon OpenSearch Service (OpenSearch Serviço)	Registros de erros de serviço. Você deve habilitar explicitamente o OpenSearch registro. Para obter mais informações, consulte Habilitando o registro para serviços compatíveis	CloudWatch LogGroup: /aws/ams/cloudtrail
10	Amazon ElastiCache	Somente registro de chamadas de API.	CloudWatch LogGroup: /aws/ams/cloudtrail
11	Amazon GuardDuty		
12	Amazon Inspector		
13	Amazon Macie		
14	Amazon Redshift	Registros de conexão, usuário e atividade. Por padrão, o registro em log é ativado quando você cria seu cluster do Redshift invocando o Create Redshift cluster CT (ct-1malj7snzxrkr). Para obter informações, consulte Registro de auditoria do banco de dados .	Bucket S3: ams-a {} -log-management- { <i>account_ID</i> } <i>region</i> Caminho: /AWS/ {} RedShift <i>CloudFront_Distribution_ID</i>

	Nome do serviço	Detalhes dos logs	Localização do registro
15	Amazon Relational Database Service (RDS)	Registros específicos para o tipo de banco de dados. O registro do RDS deve ser ativado explicitamente. Para obter mais informações, consulte Habilitando o registro para serviços compatíveis Você só pode acessar os registros do MSSQL por meio de um procedimento armazenado; para obter informações, consulte Arquivamento de arquivos de log.	CloudWatch LogGroup: /aws/rds/(instance cluster)/{nome do banco de dados}/{nome do log}

	Nome do serviço	Detalhes dos logs	Localização do registro
16	Amazon S3 (S3)	Registros de acesso ao bucket. Cada registro de registro de acesso fornece detalhes sobre uma única solicitação de acesso, como: solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e código de erro (se houver). As informações do registro de acesso podem ser úteis em auditorias de segurança e acesso; elas também podem ajudar você a conhecer sua base de clientes e entender sua fatura do Amazon S3. Para obter mais informações sobre as entradas do log de acesso do S3, consulte Formato do log de acesso do servidor do S3.	Compartimento S3: mc-a {<i>account_ID</i>} -log-management- {<i>region</i>} Caminho: /aws/s3access/ {<i>bucket_name</i>}
17	Amazon Simple Email Service (SES)	Chamadas de serviço da API SES.	CloudWatch LogGroup: /aws/ams/cloudtrail Bucket S3: ams-a { } -log-management- {<i>account_ID</i>} <i>region</i> Caminho: AWS/CloudTrail/AWSLogs/{<i>account_ID</i>}CloudTrail/{<i>region</i>}
18	Amazon Virtual Private Cloud (VPC)	Dados de fluxo da VPC (informações sobre o tráfego IP que entra e sai das interfaces de rede da VPC).	CloudWatch LogGroup: /aws/vpcflow/ {vpc_id}

	Nome do serviço	Detalhes dos logs	Localização do registro
19	ajuste de escala automático	Somente registro de chamadas de API.	CloudWatch LogGroup: /aws/ams/cloudtrail
20	AWS Certificate Manager		
21	AWS CodeDeploy	Registros de implantação específicos da instância.	Por exemplo
22	AWS Config	Chamadas de serviço da API AWS Config.	CloudWatch LogGroup: /aws/ams/cloudtrail Bucket S3: ams-a {} -log-management- {<i>account_ID</i> } <i>region</i> Caminho: AWS/CloudTrail/AWSLogs/{<i>account_ID</i> }CloudTrail/{<i>region</i>}
23	AWS Database Migration Service	Registros de migração do banco de dados. Para obter informações, consulte Introdução ao gerenciamento de logs no AWS Database Migration Service.	console de migração de banco de dados
24	AWS Direct Connect (DX)	Somente registro de chamadas de API.	CloudWatch LogGroup: /aws/ams/cloudtrail
25	AWS Glacier		
26	AWS IAM (IAM)		

	Nome do serviço	Detalhes dos logs	Localização do registro
27	AWS Key Management Service		
28	Console de gerenciamento da AWS (console ou console da AWS)		
29	AWS Simple Notification Service (SNS)		
30	AWS Simple Queueing Service (SQS)		

Registros de serviços compartilhados do AMS

A tabela a seguir descreve os registros e a localização dos registros dos Serviços Compartilhados do AMS em sua conta.

Para acessar seus registros, verifique se você tem uma das funções necessárias do IAM e está em sua conta do AMS. Em seguida, navegue até o diretório mostrado.

Registro de serviços compartilhados na landing zone de conta única do AMS

	Nome do serviço compartilhado	Detalhes dos logs	Localização do registro
1	Bastion hosts	Informações sobre usuários que acessam o bastion host.	Basthões do Linux: CloudWatch Registros:/{id da instância}/var/log/secure

	Nome do serviço compartilhado	Detalhes dos logs	Localização do registro
			CloudWatch Registros:/{id da instância}/var/log/audit/audit.log Bastões do Windows: CloudWatch Registros:/{id da instância}/SecurityEventLog
2	Anfitriões de gerenciamento	Saída de scripts, que auxiliam nas ações automatizadas de gerenciamento de acesso dentro da conta.	CloudWatch Registros:/{id da instância}/ApplicationEventLog
4	Hospedeiros EPS (DSM)	Informações sobre a inscrição de instâncias na plataforma Deep Security Management.	CloudWatch Registros:/{id da instância}/var/log/DSM.log
5	Serviços de diretório	Informações sobre login da conta, gerenciamento da conta, rastreamento detalhado, acesso a objetos, alteração de política e uso de privilégios no diretório da conta. Você deve habilitar explicitamente o log dos Serviços de Diretório. Para mais informações, consulte Habilitando o registro para serviços compatíveis.	CloudWatch Registros: /aws/directoryservice/ {id do diretório} - {nome dns do diretório}

	Nome do serviço compartilhado	Detalhes dos logs	Localização do registro
6	Lambdas	Saída de vários lambdas, que auxiliam nas ações operacionais automatizadas dentro da conta.	CloudWatch Registros: /aws/lambda/{nome lambda}

Registro de serviços compartilhados na landing zone de várias contas do AMS

	Nome do serviço compartilhado	Detalhes dos logs	Localização do registro
1	Bastões	Saída de logins de instância e falhas de autenticação.	CloudWatch Registros do Linux Bastions:/{ <i>instance_ID</i> }/var/log/secure.log CloudWatch Registros do Windows Bastions:/{ <i>instance_ID</i> }/SecurityEventLog
2	Anfitriões de gerenciamento	Saída de scriptsy, que auxilia nas ações automatizadas de gerenciamento de acesso dentro da conta.	CloudWatch Registros:/{ <i>instance_ID</i> }/ApplicationEventLog
3	Hospedeiros EPS (DSM)	Informações sobre a inscrição de instâncias na plataforma Deep Security Management.	CloudWatch Registros:/{ <i>instance_ID</i> }/var/log/DSM.log
4	Serviços de diretório	Informações sobre login da conta, gerenciamento da conta, rastreamento detalhado, acesso a objetos, alteração de política e uso de privilégios no diretório da conta.	CloudWatch Registros: /aws/directoryservice/{ } - { } <i>directory_ID</i> <i>directory_DNS_name</i>

	Nome do serviço compartilhado	Detalhes dos logs	Localização do registro
		Você deve habilitar explicitamente o log dos Serviços de Diretório. Para mais informações, consulte Habilitando o registro para serviços compatíveis .	
5	Lambdas	Saída de vários lambdas, que auxiliam nas ações operacionais automatizadas dentro da conta.	CloudWatch Registros: /aws/lambda/ <code>{ } <i>Lambda_name</i></code>

Amazon Elastic Compute Cloud (Amazon EC2) — registros em nível de sistema

Os registros de instâncias são coletados por um agente de CloudWatch registros em execução na instância e podem ser acessados por meio de um grupo de CloudWatch registros com o mesmo nome da instância. Por exemplo, se o ID da instância for i-0123456789abcdef0 e o nome do arquivo de log for `/var/log/messages`, the Log Group would be i-0123456789abcdef0 and the Log Stream `/var/log/messages`

Consulte também [Registros de serviços agregados do AMS](#).

Para acessar seus registros, verifique se você tem uma das funções necessárias do IAM e está em sua conta do AMS. Em seguida, navegue até o diretório mostrado.

Note

Os registros a seguir são coletados por padrão.

Amazon Linux/Red Hat Linux/CentOS Linux/Ubuntu/SUSE Linux

Arquivo de log//Fluxo de log

```
/var/log/amazon/ssm/amazon-ssm-agent.log
/var/log/amazon/ssm/errors.log
/var/log/audit/audit.log
/var/log/cloud-init-output.log
/var/log/cfn-init.log
/var/log/cfn-init-cmd.log
/var/log/cloud-init.log (Amazon Linux 1 / Amazon Linux 2 only)
/var/log/cron
/var/log/dnf.log
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
/var/log/yum.log
/var/log/aws/ams/bootstrap.log
/var/log/aws/ams/build.log
/var/log/syslog
/var/log/dpkg.log
/var/log/auth.log
/var/log/zypper.log
```

Note

Para obter informações sobre como acessar registros para o Amazon Linux 2023, consulte [Por que o diretório /var/log não tem registros na minha instância do EC2 Amazon Linux 2023?](#)

Windows

Arquivo de log//Fluxo de log

```
SecurityEventLog
SystemEventLog
AmazonSSMAgentLog
MicrosoftWindowsAppLockerMSIAndScriptEventLog
MicrosoftWindowsAppLockerEXEAndDLLEventLog
AmazonCloudWatchAgentLog
EC2ConfigServiceEventLog (Windows Server 2012 R2 Only)
ApplicationEventLog
AmazonCloudFormationLog
MicrosoftWindowsGroupPolicyOperationalEventLog
```

Integração com o Splunk

O AMS oferece suporte a serviços de análise de log de clientes baseados no AWS Lambda, como o Splunk.

O AMS utiliza o complemento Splunk para Amazon Web Services, que permite que os dados da AWS sejam transmitidos para o Splunk. Consulte os [requisitos de hardware e software](#).

Consulte esta postagem do blog do Splunk [Como transmitir CloudWatch registros da AWS para o Splunk \(dica: é mais fácil do que você pensa\)](#). Como o streaming de CloudWatch logs está habilitado por padrão para clientes do AMS, o AMS configura a função AWS Lambda para você, embora você precise configurar a entrada do Splunk HTTP Event Collector (HEC) e enviar uma solicitação ao AMS para obter a funcionalidade adicional.

Veja como as configurações de entrada de dados podem parecer:

Personalizando sua configuração de log

Você pode alterar a retenção de dados de log para CloudWatch registros e pode habilitar o registro para serviços adicionais da AWS.

Alterando a retenção de CloudWatch registros

Você pode alterar a configuração de retenção de dados de registro para CloudWatch registros. Por padrão, os logs são mantidos indefinidamente e nunca expiram. Você pode ajustar a política de retenção para cada grupo de logs, mantendo a retenção indefinida ou escolhendo um período de retenção entre 10 anos e um dia. Para ver o período mínimo de retenção permitido no AMS, consulte o documento de Normas Técnicas do AMS disponível por meio do AWS Artifact. Para acessar o AWS Artifact, entre em contato com seu CSDM para obter instruções ou acesse Getting [Started with AWS](#) Artifact.

O recurso de retenção de CloudWatch registros de registros exclui os eventos de registro em um stream com base na política de retenção. Ele não exclui fluxos de registros nem grupos de registros. Para obter informações gerais, consulte o Guia do usuário do Amazon CloudWatch Logs [O que é o Amazon CloudWatch Logs?](#).

Para obter informações sobre como personalizar um período de retenção de registros e saber mais, consulte [Retenção de dados de registros de alterações em CloudWatch registros](#).

Habilitando o registro para serviços compatíveis

Alguns serviços não têm o registro ativado por padrão e exigem ativação explícita.

Para ativar o registro em log para CloudFront OpenSearch, Amazon RDS e Route53, envie um RFC com Management | Other | Other | Create change type (ct-1e1xtak34nx76) com os seguintes valores, substituindo-os conforme apropriado: *variables*

Subject: Enable logging for *SERVICE_NAME*
Description: Service ARN: *SERVICE_ARN*

Gerenciamento de segurança

O gerenciamento de segurança do AWS Managed Services (AMS) é o processo pelo qual o AMS identifica os ativos de uma organização e implementa políticas e procedimentos para proteger esses ativos.

Note

O AMS agora tem um tipo de alteração (CT), Implantação | Componentes avançados de pilha | Certificado ACM com adicional SANs | Create (ct-3l14e139i5p50), que você pode usar para enviar uma solicitação de um certificado. AWS Certificate Manager Para mais informações, consulte [AWS::CertificateManager::Certificate](#). Esta CT prevê a criação de um nome alternativo de assunto adicional (SAN).

Para entender melhor a AWS segurança geral, consulte [Melhores práticas de segurança, identidade e conformidade](#).

O AMS classifica os riscos de segurança da seguinte forma:

- Riscos conhecidos detectados pelo antimalware, que o processo de mitigação de malware trata.
- Eventos de segurança, incluindo violações de acesso, que o processo de gerenciamento de eventos de segurança trata.

Tópicos

- [Proteção de dados no AMS](#)
- [Gerenciamento de identidade e acesso](#)
- [Resposta a incidentes de segurança no AMS](#)
- [Revisões de segurança de solicitações de alteração no AMS Advanced](#)

Proteção de dados no AMS

O AMS monitora continuamente suas contas gerenciadas utilizando AWS serviços nativos, como Amazon GuardDuty, Amazon Macie (opcionalmente) e outras ferramentas e processos proprietários

internos. Depois que um alarme é acionado, o AMS assume a responsabilidade pela triagem inicial e pela resposta ao alarme. Nossos processos de resposta são baseados nos padrões do NIST. O AMS testa regularmente seus processos de resposta usando a Simulação de Resposta a Incidentes de Segurança com você para alinhar seu fluxo de trabalho aos programas existentes de resposta de segurança do cliente.

Quando o AMS detecta qualquer violação ou ameaça iminente de violação de suas políticas de AWS segurança, coletamos informações, incluindo recursos afetados e quaisquer alterações relacionadas à configuração. O AMS fornece follow-the-sun suporte 24 horas por dia, 7 dias por semana, 365 dias por ano, com operadores dedicados revisando e investigando ativamente painéis de monitoramento, fila de incidentes e solicitações de serviço em todas as suas contas gerenciadas. O AMS investiga as descobertas com nossos especialistas em segurança para analisar a atividade e notificá-lo por meio dos contatos de escalonamento de segurança listados em sua conta.

Com base em nossas descobertas, a AMS interage com você de forma proativa. Se você acredita que a atividade não é autorizada ou suspeita, a AMS trabalha com você para investigar, corrigir ou conter o problema. Existem certos tipos de descobertas geradas por GuardDuty que exigem que você confirme o impacto antes que o AMS possa realizar qualquer ação. Por exemplo, o tipo de GuardDuty descoberta `UnauthorizedAccess:IAMUser/ConsoleLogin` indica que um de seus usuários fez login em um local incomum; o AMS notifica você e solicita que você revise a descoberta para confirmar se esse comportamento é legítimo.

Amazon Macie

O AWS Managed Services recomenda que você use o Macie para detectar uma lista grande e abrangente de dados confidenciais, como informações pessoais de saúde (PHI), informações de identificação pessoal (PII) e dados financeiros.

O Macie pode ser configurado para ser executado periodicamente em qualquer bucket do Amazon S3, automatizando a avaliação de qualquer objeto novo ou modificado dentro de um bucket ao longo do tempo. À medida que as descobertas de segurança forem geradas, o AMS notificará você e trabalhará com você para remediar, conforme necessário.

Para obter mais informações, consulte [Análise das descobertas do Amazon Macie](#).

Segurança do Amazon Macie

O Macie é um serviço de segurança intelligence/AI artificial que ajuda você a evitar a perda de dados descobrindo, classificando e protegendo automaticamente dados confidenciais armazenados

na AWS. O Macie usa o aprendizado de máquina para reconhecer dados confidenciais, como informações de identificação pessoal (PII) ou propriedade intelectual, atribui um valor comercial e fornece visibilidade de onde esses dados são armazenados e como estão sendo usados em sua organização. O Macie monitora continuamente a atividade de acesso aos dados em busca de anomalias e emite alertas quando detecta o risco de acesso não autorizado ou vazamento inadvertido de dados. O serviço Macie oferece suporte ao Amazon S3 AWS CloudTrail e às fontes de dados.

O AMS monitora continuamente os alertas do Macie e, se alertado, toma medidas rápidas para proteger seus recursos e sua conta. Com a adição do Macie à lista de serviços que o AMS suporta, agora também somos responsáveis por habilitar e configurar o Macie em todas as suas contas, de acordo com suas instruções. Você pode ver os alertas do Macie e nossas ações à medida que elas se desenrolam no console da AWS ou nas integrações compatíveis. Durante a integração da conta, você pode indicar as contas que você usa para armazenar PII. Para todas as novas contas com PII, recomendamos o uso do Macie. Para contas existentes com PII, entre em contato conosco e nós a ativaremos em sua conta. Como resultado, você pode ter uma camada adicional de proteção disponível e aproveitar todos os benefícios do Macie em seu ambiente da AWS gerenciado pelo AMS.

AMS Macie FAQs

- Por que eu preciso do Macie quando todas as contas do AMS têm o Trend Micro e GuardDuty estão ativadas?

O Macie ajuda você a proteger seus dados no Amazon S3, ajudando você a classificar quais dados você tem, o valor que os dados têm para a empresa e o comportamento associado ao acesso a esses dados. GuardDuty A Amazon oferece ampla proteção de suas contas, cargas de trabalho e dados da AWS, ajudando a identificar ameaças como reconhecimento de agentes de ameaças, problemas de instâncias e atividades problemáticas da conta. Ambos os serviços incorporam análise do comportamento do usuário, aprendizado de máquina e detecção de anomalias para detectar ameaças em suas respectivas categorias. A Trend Micro não se concentra em identificar PII e ameaças provenientes delas.

- Como faço para ativar o Macie na minha conta AMS?

Se você PII/PHI armazenou em suas contas ou planeja armazená-las, entre em contato com seu CSDM ou faça uma solicitação de serviço para habilitar o Macie para suas contas novas ou existentes gerenciadas pelo AMS.

- Quais são as implicações de custo de ativar o Macie na minha conta do AMS?

Os preços do Macie funcionam para o AMS de forma semelhante a outros serviços, como o Amazon Elastic Compute Cloud (Amazon EC2). Você paga pelo Amazon Macie com base no uso e um aumento do AMS com base no seu. SLAs As taxas do Macie são baseadas no uso, consulte os preços do [Amazon Macie](#), medidos com base AWS CloudTrail em eventos e no armazenamento do Amazon S3. Observe que as cobranças do Macie tendem a diminuir a partir do segundo mês após sua ativação, pois a cobrança é baseada nos dados incrementais adicionados aos buckets do Amazon S3.

Para saber mais sobre Macie, consulte [Amazon Macie](#).

GuardDuty

GuardDuty é um serviço contínuo de monitoramento de segurança que usa feeds de inteligência de ameaças, como listas de endereços IP e domínios maliciosos, e aprendizado de máquina para identificar atividades inesperadas, potencialmente não autorizadas e maliciosas em seu ambiente da AWS. Isso pode incluir problemas como escalonamento de privilégios, uso de credenciais expostas ou comunicação com endereços IP ou domínios maliciosos. GuardDuty também monitora o comportamento de acesso à conta da Amazon Web Services em busca de sinais de comprometimento, como implantações de infraestrutura não autorizadas, como instâncias implantadas em uma região que nunca foi usada, ou chamadas de API incomuns, como uma alteração na política de senha para reduzir a força da senha. Para obter mais informações, consulte o [Guia GuardDuty do usuário](#).

Para visualizar e analisar suas GuardDuty descobertas, use o procedimento a seguir.

1. Abra o [console de GuardDuty](#).
2. Escolha Descobertas e, em seguida, escolha uma descoberta específica para ver os detalhes. Os detalhes de cada descoberta diferem dependendo do tipo de descoberta, dos recursos envolvidos e da natureza da atividade.

Para obter mais informações sobre os campos de busca disponíveis, consulte [os detalhes da GuardDuty descoberta](#).

GuardDuty segurança

A Amazon GuardDuty oferece detecção de ameaças que permite monitorar e proteger continuamente suas contas e cargas de trabalho da AWS. A Amazon GuardDuty analisa fluxos

contínuos de metadados gerados a partir de sua conta e atividade de rede encontrados em Eventos, registros de fluxo do AWS CloudTrail Amazon VPC e registros do Sistema de Nomes de Domínio (DNS). Ele também usa inteligência de ameaças integrada, como endereços IP maliciosos conhecidos, detecção de anomalias e aprendizado de máquina para identificar ameaças com mais precisão. GuardDuty é um serviço AMS monitorado. Para saber mais sobre o GuardDuty monitoramento da Amazon, consulte [GuardDuty monitoramento](#). Para saber mais sobre isso GuardDuty, consulte [Amazon GuardDuty](#).

Todas as novas contas do AMS foram GuardDuty ativadas por padrão. O AMS é configurado GuardDuty durante a integração da conta. Você pode enviar solicitações de alteração para modificar as configurações a qualquer momento. GuardDuty os preços funcionam para o AMS de forma semelhante a outros serviços, como o Amazon Elastic Compute Cloud (Amazon EC2). Você paga GuardDuty com base no uso e um aumento do AMS com base no seu SLAs. GuardDuty as taxas são baseadas no uso ([Amazon GuardDuty Pricing](#)), medidas com base nos AWS CloudTrail eventos e no volume do seu registro de fluxo do Amazon VPC.

GuardDuty Para o AMS, as seguintes categorias primárias de detecção estão habilitadas:

- Reconhecimento -- Atividade que sugere reconhecimento por um agente de ameaça, como atividade incomum de API, escaneamento de portas intra-VPC, padrões incomuns de solicitações de login com falha ou sondagem de porta desbloqueada de um IP incorreto conhecido.
- Problema na instância: atividade problemática na instância, como mineração de criptomoedas, malware usando algoritmos de geração de domínio (DGA), atividade de negação de serviço de saída, volume anormalmente alto de tráfego de rede, protocolos de rede incomuns, comunicação de instância de saída com um IP malicioso conhecido, EC2 credenciais temporárias da Amazon usadas por um endereço IP externo e exfiltração de dados usando DNS.
- Atividade da conta — Os padrões comuns indicativos da atividade da conta incluem chamadas de API de uma geolocalização incomum ou proxy anônimo, tentativas de desativar o registro em AWS CloudTrail log, lançamentos incomuns de instâncias ou infraestruturas, implantações de infraestrutura em uma região incomum da AWS e chamadas de API de endereços IP maliciosos conhecidos.

O AMS usa GuardDuty em suas contas gerenciadas para monitorar continuamente descobertas e alertas GuardDuty e, se alertadas, as operações do AMS tomam medidas proativas para proteger seus recursos e sua conta. Você pode ver GuardDuty as descobertas e nossas ações à medida que elas se desenrolam no console da AWS ou nas integrações suportadas.

GuardDuty funciona com o Trend Micro Deep Security Manager em sua conta. O Trend Micro Deep Security Manager fornece serviços de detecção e prevenção de intrusões baseados em host. Os serviços de Web Reputation da Trend Micro têm alguma sobreposição GuardDuty na capacidade de detectar quando um host está tentando se comunicar com um host ou serviço web conhecido por ser uma ameaça. No entanto, GuardDuty fornece categorias adicionais de detecção de ameaças e faz isso monitorando o tráfego da rede, um método que é complementar à detecção baseada em host da Trend Micro. A detecção de ameaças baseada em rede permite maior segurança ao não permitir que os controles falhem se o host estiver exibindo um comportamento problemático. O AMS recomenda o uso GuardDuty em todas as suas contas do AMS.

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.

GuardDuty monitoramento

GuardDuty informa você sobre o status do seu ambiente da AWS, produzindo [descobertas de segurança](#) que o AMS captura e sobre as quais pode alertar.

A Amazon GuardDuty monitora a segurança do seu ambiente da AWS analisando e processando registros de fluxo de VPC, registros de AWS CloudTrail eventos e registros do Sistema de Nomes de Domínio. Você pode expandir esse escopo de monitoramento configurando GuardDuty para também usar suas próprias listas de IPs confiáveis e personalizadas e listas de ameaças.

- As listas de IP confiáveis consistem em endereços IP que você permitiu para comunicação segura com sua infraestrutura e aplicativos da AWS. GuardDuty não gera descobertas para endereços IP em listas de IP confiáveis. Você pode ter somente uma lista de IPs confiáveis enviada por vez por conta da AWS e por região.
- As listas de ameaças consistem em endereços IP maliciosos conhecidos. GuardDuty gera descobertas com base em listas de ameaças. Você pode ter no máximo seis listas de ameaças enviadas por vez por conta da AWS e por região.

Para implementar GuardDuty, use o AMS CT Deployment | Monitoring and notification | GuardDuty IP set | Create (ct-08avsj2e9mc7g) para criar um conjunto de endereços IP aprovados. Você também pode usar o AMS CT Deployment | Monitoring and notification | GuardDuty Threat Intel Set | Create (ct-25v6r7t8gvkq5) para criar um conjunto de endereços IP negados.

Para obter uma lista dos serviços que o AMS monitora, consulte [O que o sistema de monitoramento AMS monitora?](#).

Firewall DNS do Amazon Route 53 Resolver

O Amazon Route 53 Resolver responde recursivamente às consultas de DNS de AWS recursos para registros públicos, nomes DNS específicos do Amazon VPC e zonas hospedadas privadas do Amazon Route 53, e está disponível por padrão em todos. VPCs Com o Firewall DNS do Route 53 Resolver, você pode filtrar e regular o tráfego DNS de saída para sua nuvem privada virtual (VPC). Para fazer isso, você cria coleções reutilizáveis de regras de filtragem em grupos de regras do Firewall DNS, associa os grupos de regras à sua VPC e monitora a atividade em logs e métricas do Firewall DNS. Com base na atividade, você pode ajustar o comportamento do Firewall DNS adequadamente. Para obter mais informações, consulte [Usando o firewall DNS para filtrar o tráfego DNS de saída](#).

Para visualizar e gerenciar sua configuração do Route 53 Resolver DNS Firewall, use o procedimento a seguir:

1. Faça login no Console de gerenciamento da AWS e abra o console da Amazon VPC em. <https://console.aws.amazon.com/vpc/>
2. Em Firewall DNS, escolha Grupos de regras.
3. Revise, edite ou exclua sua configuração existente ou crie um novo grupo de regras. Para obter mais informações, consulte [Como o Route 53 Resolver DNS Firewall funciona](#).

Amazon Route 53 Resolver DNS Firewall: monitoramento e segurança

O Amazon Route 53 DNS Firewall usa os conceitos de associação de regras, ação de regras e prioridade de avaliação de regras. Uma lista de domínios é um conjunto reutilizável de especificações de domínios que você usa em uma regra do DNS Firewall, dentro de um grupo de regras. Quando você associa um grupo de regras a uma VPC, o DNS Firewall compara suas consultas de DNS com as listas de domínios usadas nas regras. Se o Firewall do DNS encontrar uma correspondência, ele processará a consulta de DNS de acordo com a ação da regra correspondente. Para obter mais informações sobre regras e grupos de regras, consulte [Regras e grupos de regras do Firewall DNS](#).

As listas de domínios se enquadram em duas categorias principais:

- Listas de domínios gerenciados, que AWS criam e mantêm para você.
- Suas próprias listas de domínios, que você cria e mantém.

Os grupos de regras são avaliados com base em seu índice de prioridade de associação.

Por padrão, o AMS implanta uma configuração de linha de base que consiste na seguinte regra e grupo de regras:

- Um grupo de regras chamado `DefaultSecurityMonitoringRule`. O grupo de regras tem a maior prioridade de associação disponível no momento da criação para cada VPC existente em cada uma habilitada. Região da AWS
- Uma regra nomeada `DefaultSecurityMonitoringRule` com prioridade 1 dentro do grupo de `DefaultSecurityMonitoringRule` regras, usando a lista de domínios `AWSManagedDomainsAggregateThreatList` gerenciados com a ação ALERT.

Se você tiver uma configuração existente, a configuração básica será implantada com menor prioridade do que a configuração existente. Sua configuração existente é a padrão. Você usa a configuração básica do AMS como uma solução abrangente se sua configuração existente não fornecer uma instrução de maior prioridade sobre como lidar com a resolução de consultas. Para alterar ou remover a configuração da linha de base, faça o seguinte:

- Entre em contato com seu Cloud Service Delivery Manager (CSDM) ou Cloud Architect (CA).
- Crie uma solicitação de mudança (RFC) usando [Gerenciamento | Outro | Outro | Crie CT \(ct-1e1xtak34nx76\)](#).
- Crie uma solicitação de serviço.

Se sua conta for operada no modo Desenvolvedor ou no modo Alteração Direta, você mesmo poderá realizar as alterações.

AWS Certificate Manager certificado (ACM)

O AMS tem um certificado CT, Deployment | Advanced stack components | ACM com SANs | Create adicional (ct-3l14e139i5p50), que você pode usar para enviar uma solicitação de um certificado do AWS Certificate Manager, com até cinco nomes alternativos de assunto (SAN) adicionais (como example.com, example.net e example.org). Para obter detalhes, consulte [O que é AWS Certificate Manager?](#) e [característica do certificado ACM](#).

 Note

Essa configuração de tempo limite não diz respeito apenas à execução, mas também à validação do certificado ACM por meio da validação por e-mail. Sem sua validação, o RFC falha.

Criptografia de dados no AMS

O AMS usa vários AWS serviços para criptografia de dados, principalmente Amazon Simple Storage Service, AWS Key Management Service (AWS KMS), Amazon Elastic Block Store, Amazon Relational Database Service Amazon Redshift,,, Amazon ElastiCache AWS Lambda, e Amazon OpenSearch Service.

Amazon S3

O Amazon S3 oferece várias opções de criptografia de objetos que protegem os dados em trânsito e em repouso. A criptografia no lado do servidor criptografa o objeto antes de salvá-lo em discos em seus datacenters e os descriptografa ao fazer download dos objetos. Contanto que você autentique sua solicitação e tenha permissões de acesso, não há diferença na forma de acesso aos objetos criptografados ou não criptografados. Para obter mais informações, consulte [Proteção de dados no Amazon S3](#).

Amazon EBS

Com a criptografia do Amazon EBS, você não precisa criar, manter e proteger sua própria infraestrutura de gerenciamento de chaves. A criptografia do Amazon EBS usa AWS KMS chaves ao criar volumes e snapshots criptografados. As operações de criptografia ocorrem nos servidores que hospedam as EC2 instâncias da Amazon. Isso é feito para garantir que tanto a instância data-at-rest data-in-transit quanto o armazenamento conectado do Amazon EBS estejam seguros. É possível anexar volumes criptografados e não criptografados a uma instância simultaneamente. Para obter mais informações, consulte [Criptografia do Amazon EBS](#).

Amazon RDS

O Amazon RDS pode criptografar suas instâncias de banco de dados do Amazon RDS. Os dados criptografados em repouso incluem o armazenamento subjacente para instâncias de banco de dados, seus backups automatizados, réplicas de leitura e instantâneos. As instâncias de banco de dados criptografadas do Amazon RDS usam o algoritmo de criptografia AES-256 padrão do

setor para criptografar seus dados no servidor que hospeda suas instâncias de banco de dados do Amazon RDS. Após a criptografia dos seus dados, o Amazon RDS lida com a autenticação do acesso e a decodificação dos seus dados de forma transparente com um mínimo impacto sobre o desempenho. Você não precisa modificar suas aplicações cliente de banco de dados para usar a criptografia. Para ter mais informações, consulte [Criptografar recursos do Amazon RDS](#).

Amazon Simple Queue Service

Além da opção padrão de criptografia do lado do servidor (SSE) gerenciada pelo Amazon SQS, a SSE gerenciada pelo Amazon SQS (SSE-SQS) permite que você crie uma criptografia gerenciada personalizada do lado do servidor que usa chaves de criptografia gerenciadas pelo Amazon SQS para proteger dados confidenciais enviados por filas de mensagens. A criptografia no lado do servidor (SSE) permite que você transmita dados sigilosos em filas criptografadas. A SSE protege o conteúdo de mensagens em filas usando chaves de criptografia gerenciadas pelo Amazon SQS (SSE-SQS) ou chaves gerenciadas em (SSE-KMS). AWS KMS Para obter informações sobre como gerenciar o SSE usando o Console de gerenciamento da AWS, consulte [Criptografia em repouso](#).

Criptografia de dados em repouso

OpenSearch Os domínios de serviço oferecem criptografia de dados em repouso, um recurso de segurança que ajuda a impedir o acesso não autorizado aos seus dados. O recurso usa AWS Key Management Service (AWS KMS) para armazenar e gerenciar suas chaves de criptografia e o algoritmo Advanced Encryption Standard com chaves de 256 bits (AES-256) para realizar a criptografia. Para obter mais informações, consulte [Criptografia de dados em repouso para o Amazon OpenSearch Service](#).

Gerenciamento de chaves

AWS KMS é um serviço gerenciado que facilita a criação e o controle das chaves mestras do cliente (CMKs), as chaves de criptografia usadas para criptografar seus dados. AWS KMS CMKs são protegidos por módulos de segurança de hardware (HSMs) validados pelo Programa de Validação de Módulos Criptográficos FIPS 140-2, exceto nas regiões da China (Pequim) e China (Ningxia). Para obter mais informações, consulte [O que é o AWS Key Management Service?](#)

Gerenciamento de identidade e acesso

AWS Identity and Access Management (IAM) é um serviço web que ajuda você a controlar com segurança o acesso aos AWS recursos. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) a usar os recursos. Durante a integração do AMS, você é

responsável por criar funções de administrador do IAM entre contas em cada uma das suas contas gerenciadas.

Proteções IAM da Multi-Account Landing Zone (MALZ)

O AMS Multi-Account Landing Zone (MALZ) exige a confiança do Active Directory (AD) como objetivo principal do projeto de gerenciamento de acesso ao AMS para permitir que cada organização (tanto a AMS quanto o cliente) gerencie os ciclos de vida de suas próprias identidades. Isso evita a necessidade de ter credenciais no diretório um do outro. A confiança unidirecional é configurada para que o Active Directory gerenciado dentro do AD Conta da AWS confie no AD gerenciado ou de propriedade do cliente para autenticar os usuários. Como a confiança é apenas uma forma, isso não significa que o AD gerenciado seja confiável para o Active Directory do cliente.

Nessa configuração, o diretório de clientes que gerencia as identidades dos usuários é conhecido como Floresta de Usuários, e o AD gerenciado ao qual as EC2 instâncias da Amazon estão anexadas é conhecido como Floresta de Recursos. Esse é um padrão de design da Microsoft comumente utilizado para autenticação do Windows; para obter mais informações, [consulte Modelos de design florestal](#).

Esse modelo permite que ambas as organizações automatizem seus respectivos ciclos de vida e permite que você e o AMS revoguem rapidamente o acesso se um funcionário deixar a organização. Sem esse modelo, se ambas as organizações usassem um diretório comum (ou criassem users/groups nos diretórios uma da outra), ambas precisariam incluir fluxos de trabalho adicionais e sincronizações de usuários para contabilizar a entrada e saída dos funcionários. Isso introduz riscos, pois esse processo tem latência e pode estar sujeito a erros.

Pré-requisitos de acesso ao MALZ

Integração com o MALZ Identity Provider para acesso ao console AWS/AMS, CLI, SDK.

Confiança unidirecional para EC2 instâncias da Amazon em sua conta AMS.

Autenticação com identidades

O AMS usa funções do IAM, que é um tipo de identidade do IAM. Uma função do IAM é muito semelhante à de um usuário, pois é uma identidade com políticas de permissão que determinam o que a identidade pode ou não fazer AWS. No entanto, uma função não tem credenciais associadas e, em vez de ser associada exclusivamente a uma pessoa, a função deve ser assumida por

qualquer pessoa que precise dela. Um usuário do IAM pode assumir uma função para conseguir temporariamente permissões diferentes para uma tarefa específica.

As funções de acesso são controladas pela associação interna ao grupo, que é administrada e revisada periodicamente pelo Operations Management.

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 `AMSCustomer_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 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

Role (Função)	Política ou políticas
	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 AWSSupport Exemplo de acesso Essa política fornece acesso a todas as operações e recursos de suporte.

Role (Função)	Política ou políticas
	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
	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
AWSManagedServicesAdminRole	AMSS3Política
	ReadOnlyAccess
	AWSSupportAcesso
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy

Role (Função)	Política ou políticas
	AMSCChangeManagementPolicy
	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/hashtes compartilhado pelo AMS por meio de AWS Secrets Manager (por exemplo, senhas de infraestrutura para auditoria).

Permissões para criar um segredo password/hashtes 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 [ReadOnlyAccess](#) para 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": [
        "*"
      ]
    }
  ]
}
```

Registro e monitoramento de eventos de segurança no

O AMS monitora continuamente o ambiente gerenciado em busca de ameaças à segurança. Eventos de segurança podem ser detectados pelo AMS ou por você. O AMS atualiza regularmente seu processo de automação, com base no Guia de Tratamento de Incidentes de Segurança de Computadores do Instituto Nacional de Padrões e Tecnologia (NIST), para detectar melhor as ameaças à segurança.

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 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)

Configuração	Padrão
Ativação de vários computadores com o mesmo nome de host	É permitido
Alertas para atualizações pendentes são gerados	Depois de sete dias
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

Configuração	Padrão
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

Configuração	Padrão	Observações
	Todos os Day/All dias (24 horas)	os vírus suspeitos. Ativação IntelliTrap e spyware/grayware proteção. O spyware e o Grayware acionam o Anti-Malware 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

Processo de mitigação de malware

O AMS usa o Deep Security Platform (sistema antimalware) da Trend Micro para detectar e responder ao malware em suas instâncias gerenciadas pelo AMS. Por padrão, o agente de detecção da Trend Micro é executado em todas as EC2 instâncias da Amazon, incluindo aquelas nos serviços compartilhados e sub-redes privadas, para sistemas operacionais Windows e Linux. O sistema antimalware é conectado ao monitoramento do AMS para que um evento seja gerado sempre que um malware for detectado. Se houver impacto no cliente, o evento será encaminhado para o processo de gerenciamento de incidentes (para obter detalhes, consulte [Resposta ao incidente do AMS](#)). Enquanto o AMS avalia o impacto, você é notificado e são feitas tentativas para mitigar o impacto.

As definições de antimalware da Trend Micro são atualizadas automaticamente quando a Trend Micro publica atualizações.

Durante a integração do aplicativo, você indica a ação que deseja que o AMS execute quando um malware é encontrado em uma instância:

- Verifique se o arquivo em quarentena está na lista de permissões, removendo-o da quarentena e liberando-o de volta para o sistema de arquivos.
- Exclua o arquivo em quarentena, removendo-o da instância.
- Suspenda a instância e substitua-a. A instância suspensa fica então disponível para você montar para pesquisa forense.

Após a integração do aplicativo:

- Quando o sistema antimalware descobre um malware em uma instância, o AMS coloca o malware automaticamente em quarentena. Isso desencadeia um evento e uma investigação de acompanhamento.
- O AMS notifica você sobre o evento por meio de uma notificação de serviço e começa a seguir a ação de mitigação padrão que você selecionou.
- Se você não tiver escolhido uma ação padrão, o AMS perguntará qual ação tomar. Depois de receber suas instruções, o AMS executa a ação selecionada e notifica você. O AMS notifica você novamente após a conclusão da ação, incluindo os detalhes necessários para a análise forense, se aplicável.

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.

Verificações completas de malware do sistema

O Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) exige escaneamentos completos de malware do sistema, que são ativados em sua VPC gerenciada pelo AMS por padrão. As varreduras completas do sistema estão programadas para ocorrer às 2h (no fuso horário definido no servidor) porque elas usam muita CPU. As verificações completas do sistema são adicionais às verificações regulares de malware que não usam muita CPU.

Há um novo tipo de alteração de gerenciamento (CT), Desativar escaneamentos de malware, que permite desativar escaneamentos completos de malware do sistema. Você pode encontrar o CT em Gerenciamento | Segurança do host | Verificação completa do sistema | Desativar classificação, alterar ID ct-1pybwg08h8qsz. Para reativar as digitalizações, use o Gerenciamento | Outros | Outros | Atualizar CT. Desativar os escaneamentos completos do sistema não desativa seus escaneamentos regulares de malware.

Segurança do Amazon Inspector

O serviço Amazon Inspector monitora a segurança de suas pilhas gerenciadas pelo AMS. O Amazon Inspector é um serviço automatizado de avaliação de segurança que ajuda a identificar lacunas na segurança e conformidade da infraestrutura implantada. AWS As avaliações de segurança do Amazon Inspector permitem que você avalie automaticamente as pilhas quanto à exposição, vulnerabilidades e desvios das melhores práticas, verificando a acessibilidade e vulnerabilidades não intencionais da rede em suas instâncias da Amazon. EC2 Depois de executar uma avaliação, o Amazon Inspector fornece uma lista detalhada das descobertas de segurança, priorizadas de acordo

com seu nível de severidade. As avaliações do Amazon Inspector são oferecidas como pacotes de regras predefinidos mapeados de acordo com as melhores práticas e definições de segurança comuns. Essas regras são atualizadas regularmente por pesquisadores AWS de segurança. Para obter mais informações sobre o Amazon Inspector, acesse Amazon [Inspector](#).

AMS Amazon Inspector FAQs

- O Amazon Inspector está instalado em minhas contas AMS por padrão?

Não. O Amazon Inspector não faz parte da compilação padrão da AML ou da ingestão de carga de trabalho.

- Como faço para acessar e instalar o Amazon Inspector?

Envie um RFC (Gerenciamento | Outro | Outro | Criar) para solicitar acesso e instalação da conta ao Inspector e a equipe de operações do AMS modificará a função ReadOnly Cliente_ para fornecer acesso ao console do Amazon Inspector (sem acesso ao SSM).

- O agente do Amazon Inspector precisa ser instalado em todas as EC2 instâncias da Amazon que eu quero avaliar?

Não, as avaliações do Amazon Inspector com o pacote de regras de acessibilidade de rede podem ser executadas sem um agente para qualquer instância da Amazon. EC2 O agente é necessário para pacotes de regras de avaliação do host. Para obter mais informações sobre a instalação do agente, consulte [Instalando agentes do Amazon Inspector](#).

- Há algum custo adicional para esse serviço?

Sim. Os preços do Amazon Inspector podem ser encontrados no site de preços do [Amazon Inspector](#).

- Quais são as descobertas do Amazon Inspector?

As descobertas são possíveis problemas de segurança descobertos durante a avaliação do Amazon Inspector do alvo de avaliação selecionado. As descobertas são exibidas no console do Amazon Inspector ou na API e contêm uma descrição detalhada dos problemas de segurança e recomendações para resolvê-los.

- Os relatórios da avaliação do Amazon Inspector estão disponíveis?

Sim. Um relatório de avaliação é um documento que explica o que foi testado em uma execução de avaliação e os resultados da avaliação. Os resultados de sua avaliação são formatados em relatórios padrão, que podem ser gerados para compartilhar resultados com sua equipe

para ações de remediação, para enriquecer os dados de auditoria de conformidade ou para armazenamento para referência futura. Um relatório de avaliação do Amazon Inspector pode ser gerado para uma execução de avaliação depois de concluída com sucesso.

- Posso usar tags para identificar as pilhas com as quais eu quero executar relatórios do Amazon Inspector?

Sim.

- As equipes de operações do AMS terão acesso aos resultados da avaliação do Amazon Inspector?

Sim. Qualquer pessoa com acesso ao console do Amazon Inspector na AWS pode visualizar descobertas e relatórios de avaliação.

- As equipes de operações do AMS recomendarão ou tomarão medidas com base nas conclusões dos relatórios do Amazon Inspector?

Não. Se você quiser que as alterações sejam feitas com base nas descobertas do relatório do Amazon Inspector, você deve solicitar alterações por meio de um RFC (Gerenciamento | Outro | Outro | Atualização).

- O AMS será notificado quando eu executar um relatório do Amazon Inspector?

Quando você solicita o acesso ao Amazon Inspector, o operador do AMS que executa o RFC notifica seu CSDM sobre a solicitação.

Para obter mais informações, consulte [Amazon Inspector FAQs](#).

Resposta ao incidente do AMS

O AMS usa as melhores práticas tradicionais de gerenciamento de incidentes de gerenciamento de serviços de TI (ITSM) para restaurar o serviço, quando necessário, o mais rápido possível.

Fornecemos follow-the-sun suporte 24 horas por dia, 7 dias por semana, 365 dias por ano, por meio de vários centros de operações em todo o mundo, com operadores dedicados monitorando ativamente painéis e filas de incidentes.

Nossos engenheiros de operações usam ferramentas internas de rastreamento de incidentes para identificar, registrar, categorizar, priorizar, diagnosticar, resolver e fechar incidentes e fornecer atualizações sobre todas essas atividades por meio do console do AMS ou da API. Suporte Nossos operadores, muitos dos quais passaram algum tempo no AWS Premium Support em vários perfis

e funções de tecnologia, utilizam uma variedade de Suporte ferramentas internas para ajudar em todas essas atividades. Esses operadores estão profundamente familiarizados com as infraestruturas suportadas pelo AMS e têm habilidades técnicas de nível especializado para resolver todos os problemas de suporte identificados. Nos raros casos em que nossos operadores precisam de assistência, as equipes de Suporte e AWS Serviço Premium estão disponíveis para ajudar conforme necessário.

Nos casos em que incidentes de alta prioridade estão afetando suas cargas de trabalho críticas, a AMS recomendará uma restauração da infraestrutura. Muitas vezes, há uma compensação entre solucionar um problema ou restaurar a partir de um backup em boas condições, e os riscos e impactos do tempo de inatividade do serviço para o cliente são os fatores decisivos. Se você tiver tempo para se dedicar à solução de problemas, o AMS o ajudará, mas se a urgência de restaurar for alta, podemos iniciar uma restauração imediatamente.

Note

Dados efêmeros que não fazem parte do modelo de pilha ou da restauração de dados são perdidos. O AMS usa esforços razoáveis para realizar a restauração da infraestrutura enquanto as ofertas AWS de serviços não estão disponíveis. A restauração da infraestrutura é concluída quando as ofertas AWS de serviços estão disponíveis.

Se você não autorizar uma restauração de infraestrutura conforme recomendado pelo AMS, não terá direito a um crédito de serviço pelo compromisso de serviço do AMS pelo tempo de resolução de incidentes.

Validação de conformidade

O AMS implanta e gerencia uma biblioteca de AWS Config regras e ações de remediação para se proteger contra configurações incorretas que podem reduzir a segurança e a integridade operacional de suas contas.

Por exemplo, quando um bucket do Amazon S3 é criado, AWS Config pode avaliar o bucket do Amazon S3 em relação a uma regra que exige que os buckets do Amazon S3 neguem o acesso público de leitura. Se a política de bucket do Amazon S3 ou a lista de controle de acesso ao bucket (ACL) permitirem acesso público de leitura, AWS Config sinalizará o bucket e a regra como não compatíveis. Eles Regras do AWS Config marcam os recursos como compatíveis, não compatíveis ou não aplicáveis, com base no resultado de sua avaliação. Para obter mais informações sobre o AWS Config serviço, consulte o [Guia do AWS Config desenvolvedor](#).

Você pode usar o AWS Config console, a AWS CLI ou a AWS Config API para ver as regras implantadas em sua conta e o estado de conformidade de suas regras e recursos. Para obter mais informações, consulte a AWS Config documentação: [Exibindo a conformidade da configuração](#).

 Note

Informações adicionais sobre esse tópico estão disponíveis acessando os relatórios do AWS Artifact. Para obter mais informações, consulte [Fazer download dos relatórios no AWS Artifact](#). Para acessar o AWS Artifact, você pode entrar em contato com seu CSDM para obter instruções ou acessar Getting [Started with AWS](#) Artifact. Essas informações não estão incluídas neste guia do usuário porque contêm conteúdo de segurança confidencial.

Zona de destino de várias contas visualizando o status de conformidade de seu Regras do AWS Config

A landing zone multiconta do AMS utiliza o serviço AWS Config agregador para criar uma visão centralizada da conformidade em todas as suas contas. Isso significa que você pode ver o status de conformidade de Regras do AWS Config todo o seu ambiente de landing zone com várias contas do AMS no AWS Config agregador em sua conta de segurança.

Veja a seguir uma amostra do AWS Config agregador que mostra o status de conformidade central de todas as contas. Regras do AWS Config

Para obter mais informações, consulte a documentação da AWS para o [Config](#) Agregador.

- Como o AMS usa as regras do AWS Config?

O AMS cria Regras do AWS Config para dar visibilidade à configuração de seus AWS recursos em relação às condições especificadas nas regras. Se uma regra não estiver em conformidade, você poderá solicitar uma alteração e a equipe de operações do AMS trabalhará com você para tomar medidas corretivas.

- Nesse caso, você verá as seguintes alterações aparecerem em suas contas do AMS:
 - Regras do AWS Config em AWS Config > Regras
 - As regras do Custom Config com suas funções Lambda existem em sua conta
 - Config Agregador na conta de segurança e Config Authorization em todas as contas (somente na zona de destino de várias contas)

A seguir está uma amostra Regras do AWS Config e seus resultados da avaliação de conformidade são mostrados abaixo:

Para saber mais sobre o AWS Config, consulte:

- AWS Config: [O que é o Config?](#)
- Regras do AWS Config: [avaliação](#) de recursos com regras
- Regras do AWS Config: Verificação [dinâmica de conformidade: AWS Config Rules — Verificação dinâmica de conformidade](#) para recursos na nuvem
- AWS Config Aggregator: agregação de dados multiconta e [multirregional](#)

Restrições da política de controle de serviços de landing zone multicontas do 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.

Resiliência

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte [infraestrutura AWS global](#).

Segurança da infraestrutura

Note

Informações adicionais sobre esse tópico estão disponíveis acessando os relatórios do AWS Artifact. Para obter mais informações, consulte [Fazer download dos relatórios no AWS Artifact](#). Para acessar o AWS Artifact, você pode entrar em contato com seu CSDM para obter instruções ou acessar Getting [Started with AWS](#) Artifact. Essas informações não estão incluídas neste guia do usuário porque contêm conteúdo de segurança confidencial.

Controle de segurança para sistemas end-of-support operacionais

Os sistemas operacionais que estão fora do período de suporte geral do fabricante do sistema operacional "end-of-support" ou EOS e não recebem atualizações de segurança têm um risco de segurança maior.

AWS oferece alguns serviços para ajudar no manuseio do sistema operacional end-of-support. Para obter informações sobre o Windows end-of-support, consulte [Programa de End-of-Support migração para Windows Server](#).

Note

Informações adicionais sobre esse tópico estão disponíveis acessando os relatórios do AWS Artifact. Para obter mais informações, consulte [Fazer download dos relatórios no AWS Artifact](#). Para acessar o AWS Artifact, você pode entrar em contato com seu CSDM para obter instruções ou acessar Getting [Started with AWS](#) Artifact. Essas informações não estão incluídas neste guia do usuário porque contêm conteúdo de segurança confidencial.

Usar grupos de segurança

Um grupo de segurança atua como um firewall virtual que controla o tráfego de uma ou mais instâncias. Os grupos de segurança do AMS permitem que você defina regras de tráfego de entrada e de saída em nível de instância. Você pode criar um grupo de segurança e especificar recursos em sua conta AMS, EC2 instâncias Amazon, instâncias de banco de dados Amazon RDS, Load Balancers, instâncias de replicação do Deep Security Manager (DSM), destinos de montagem do

EFS e ElastiCache clusters, para associar ao grupo de segurança. Uma vez associado, o tráfego de ou para essas instâncias é limitado pelas regras definidas no grupo de segurança.

Para entender melhor a segurança geral da AWS, consulte [Melhores práticas de segurança, identidade e conformidade](#) e [Grupos de EC2 segurança da Amazon para instâncias Linux](#).

O AMS agora tem um conjunto de tipos de alterações para criar e gerenciar grupos de segurança:

- Implantação | Componentes avançados da pilha | Grupo de segurança | Criar (ct-10xx2g2d7hc90)
- Gerenciamento | Componentes avançados da pilha | Grupo de segurança | Excluir (ct-3cp96z7r065e4)
- Gerenciamento | Componentes avançados da pilha | Grupo de segurança | Atualização (ct-3memthlcmvc1b)

Para ver exemplos, consulte [Grupos de segurança](#).

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)

Tipo	Protocolo	Intervalo de portas	Origem
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:			
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:			

Tipo	Protocolo	Intervalo de portas	Origem
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-10xx2g2d7hc90).

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-2019s9y3nfm14]

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](#).

Biblioteca de controles preventivos e de detetive do AMS

O AWS Managed Services (AMS) fornece uma seleção de políticas comprovadas library/catalog de controle de serviços (SCPs) ConfigRules que podem ser utilizadas para melhorar sua postura de segurança e mitigar as lacunas de conformidade em suas contas do AMS.

Tópicos

- [Regras selecionadas SCPs e de configuração](#)
- [Notificação personalizada para regras de Config](#)

Regras selecionadas SCPs e de configuração

Regras selecionadas SCPs e de configuração para o AMS Advanced.

- Políticas de controle de serviço (SCPs): As fornecidas SCPs são adicionais às padrão do AMS.

Você pode usar esses controles de biblioteca em conjunto com os padrões para atender aos requisitos de segurança específicos.

- Regras de configuração: [como medida básica, o AMS recomenda aplicar pacotes de conformidade \(consulte Pacotes de conformidade no AWS Config guia\), além das regras de configuração padrão do AMS \(consulte Artefatos do AMS para ver as regras padrão\)](#). Os pacotes de conformidade cobrem a maioria dos requisitos de conformidade e a AWS os atualiza regularmente.

As regras listadas aqui podem ser usadas para cobrir lacunas específicas de casos de uso que não são cobertas pelos pacotes de conformidade

Note

À medida que as regras padrão e os pacotes de conformidade do AMS são atualizados com o tempo, você pode ver duplicatas dessas regras.

O AMS recomenda fazer uma limpeza periódica das regras de configuração duplicadas em geral.

Para o AMS Advanced, o Config Rules não deve usar remediações automáticas (consulte Correção de [recursos não compatíveis da AWS pelo AWS Config Rules](#)) para evitar alterações. out-of-band

SCP-AMS-001: Restringir a criação de EBS

Evite a criação de volumes do EBS se você não tiver a criptografia ativada.

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:CreateVolume",
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-002: Restringir o lançamento EC2

Evite a execução de uma EC2 instância se o volume do EBS não estiver criptografado. Isso inclui negar uma EC2 inicialização não criptografada AMIs porque esse SCP também se aplica aos volumes raiz.

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:RunInstances",
  "Resource": "arn:aws:ec2:*:*:volume/*",
  "Effect": "Deny"
}
```

SCP-ADV-001: Restringir envios de RFC

Restrinja o envio automático de funções padrão do AMS, RFCs como Criar VPC ou Excluir VPC. Isso é útil se você quiser aplicar permissões mais granulares às suas funções federadas.

Por exemplo, talvez você queira que o padrão seja `AWSSManagedServicesChangeManagement` Role capaz de enviar a maioria das informações disponíveis, RFCs exceto aquelas que permitem a criação e exclusão de uma VPC, a criação de sub-redes adicionais, a desativação de uma conta de aplicativo, a atualização ou a exclusão de provedores de identidade SAML:

SCP-AMS-003: Restringir EC2 ou criar RDS no AMS

Evite a criação de instâncias da Amazon EC2 e do RDS que não tenham tags específicas e, ao mesmo tempo, permita que a AMS Backup IAM função padrão do AMS faça isso. Isso é necessário para recuperação de desastres ou DR.

```
{
  "Sid": "DenyRunInstanceWithNoOrganizationTag",
  "Effect": "Deny",
  "Action": [
    "ec2:RunInstances",
    "rds:CreateDBInstance"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:rds:*:*:db:*"
  ],
  "Condition": {
    "Null": {
      "aws:RequestTag/organization": "true"
    },
    "StringNotLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam:*:<Account_Number>:role/ams-backup-iam-role"
      ]
    }
  }
}
```

SCP-AMS-004: Restringir os carregamentos do S3

Evite o upload de objetos S3 não criptografados.

```
{
  "Sid": "DenyUnencryptedS3Uploads",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "StringNotLike": {
      "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"]
    },
    "Null": {
      "s3:x-amz-server-side-encryption": "false"
    }
  }
}
```

SCP-AMS-005: Restrinja o acesso à API e ao console

Impeça o acesso ao console e à API da AWS para solicitações provenientes de endereços IP inválidos conhecidos como incorretos, conforme determinado cliente InfoSec.

SCP-AMS-006: Impedir que a entidade IAM remova a conta do membro da organização

Impeça que uma AWS Identity and Access Management entidade remova contas de membros da organização.

```
{
  "Effect": "Deny",
  "Action": ["organizations:LeaveOrganization"],
  "Resource": ["*"]
}
```

SCP-AMS-007: Evite compartilhar recursos com contas fora de sua organização

Evite compartilhar recursos com contas externas fora da sua AWS organização

```
{
  "Effect": "Deny",
  "Action": [
```

```

    "ram:*"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "Bool": {
      "ram:AllowsExternalPrincipals": "true"
    }
  }
},
{
  "Effect": "Deny",
  "Action": [
    "ram:CreateResourceShare",
    "ram:UpdateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "Bool": {
      "ram:RequestedAllowsExternalPrincipals": "true"
    }
  }
}
}

```

SCP-AMS-008: Impedir o compartilhamento com organizações ou unidades organizacionais () OUs

Evite compartilhar recursos com uma conta and/or OU que esteja em uma organização.

```

{
  "Effect": "Deny",
  "Action": [
    "ram:CreateResourceShare",
    "ram:AssociateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringLike": {
      "ram:Principal": [
        "arn:aws:organizations::*:account/o-${OrganizationId}/${AccountId}",
        "arn:aws:organizations::*:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}"
      ]
    }
  }
}

```

```
}
```

SCP-AMS-009: Impedir que usuários aceitem convites de compartilhamento de recursos

Impeça que as contas dos membros aceitem convites AWS RAM para participar de compartilhamentos de recursos. Essa API não suporta nenhuma condição e impede compartilhamentos somente de contas externas.

```
{
  "Effect": "Deny",
  "Action": ["ram:AcceptResourceShareInvitation"],
  "Resource": ["*"]
}
```

SCP-AMS-010: Impedir ações de ativação e desativação da região da conta

Evite ativar ou desativar novas AWS regiões para suas AWS contas.

```
{
  "Effect": "Deny",
  "Action": [
    "account:EnableRegion",
    "account:DisableRegion"
  ],
  "Resource": "*"
}
```

SCP-AMS-011: Evitar ações de modificação do faturamento

Evite modificações na configuração de cobrança e pagamento.

```
{
  "Effect": "Deny",
  "Action": [
    "aws-portal:ModifyBilling",
    "aws-portal:ModifyAccount",
    "aws-portal:ModifyPaymentMethods"
  ],
  "Resource": "*"
}
```

SCP-AMS-012: Impedir a exclusão ou modificação de dados específicos CloudTrails

Evite modificações em AWS CloudTrail trilhas específicas.

```
{
  "Effect": "Deny",
  "Action": [
    "cloudtrail:DeleteEventDataStore",
    "cloudtrail:DeleteTrail",
    "cloudtrail:PutEventSelectors",
    "cloudtrail:PutInsightSelectors",
    "cloudtrail:UpdateEventDataStore",
    "cloudtrail:UpdateTrail",
    "cloudtrail:StopLogging"
  ],
  "Resource": [
    "arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}"
  ]
}
```

SCP-AMS-013: Impedir a desativação da criptografia padrão do EBS

Evite a desativação da criptografia padrão do Amazon EBS.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

SCP-AMS-014: Impedir a criação de VPC e sub-rede padrão

Evite a criação de uma Amazon VPC e sub-redes padrão.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateDefaultSubnet",
    "ec2:CreateDefaultVpc"
  ],
}
```

```
"Resource": "*"
}
```

SCP-AMS-015: Impedir a desativação e modificação GuardDuty

Impeça que GuardDuty a Amazon seja modificada ou desativada.

```
{
  "Effect": "Deny",
  "Action": [
    "guardduty:AcceptInvitation",
    "guardduty:ArchiveFindings",
    "guardduty:CreateDetector",
    "guardduty:CreateFilter",
    "guardduty:CreateIPSet",
    "guardduty:CreateMembers",
    "guardduty:CreatePublishingDestination",
    "guardduty:CreateSampleFindings",
    "guardduty:CreateThreatIntelSet",
    "guardduty:DeclineInvitations",
    "guardduty>DeleteDetector",
    "guardduty>DeleteFilter",
    "guardduty>DeleteInvitations",
    "guardduty>DeleteIPSet",
    "guardduty>DeleteMembers",
    "guardduty>DeletePublishingDestination",
    "guardduty>DeleteThreatIntelSet",
    "guardduty:DisableOrganizationAdminAccount",
    "guardduty:DisassociateFromMasterAccount",
    "guardduty:DisassociateMembers",
    "guardduty:InviteMembers",
    "guardduty:StartMonitoringMembers",
    "guardduty:StopMonitoringMembers",
    "guardduty:TagResource",
    "guardduty:UnarchiveFindings",
    "guardduty:UntagResource",
    "guardduty:UpdateDetector",
    "guardduty:UpdateFilter",
    "guardduty:UpdateFindingsFeedback",
    "guardduty:UpdateIPSet",
    "guardduty:UpdateMalwareScanSettings",
    "guardduty:UpdateMemberDetectors",
    "guardduty:UpdateOrganizationConfiguration",
    "guardduty:UpdatePublishingDestination",
  ]
}
```

```
"guardduty:UpdateThreatIntelSet"
],
"Resource": "*"
}
```

SCP-AMS-016: Impedir a atividade do usuário root

Impeça que o usuário root execute qualquer ação.

```
{
  "Action": "*",
  "Resource": "*",
  "Effect": "Deny",
  "Condition": {
    "StringLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::*:root"
      ]
    }
  }
}
```

SCP-AMS-017: Impedir a criação de chaves de acesso para o usuário root

Impeça a criação de chaves de acesso para o usuário root.

```
{
  "Effect": "Deny",
  "Action": "iam:CreateAccessKey",
  "Resource": "arn:aws:iam::*:root"
}
```

SCP-AMS-018: Impedir a desativação do bloqueio de acesso público da conta S3

Evite desativar um bloqueio de acesso público da conta Amazon S3. Isso evita que qualquer bucket na conta se torne público.

```
{
  "Effect": "Deny",
  "Action": "s3:PutAccountPublicAccessBlock",
  "Resource": "*"
}
```



```
}
```

SCP-AMS-019: Evite a desativação do AWS Config ou a modificação das regras do Config

Evite desativar ou modificar regras. AWS Config

```
{
  "Effect": "Deny",
  "Action": [
    "config:DeleteConfigRule",
    "config:DeleteConfigurationRecorder",
    "config:DeleteDeliveryChannel",
    "config:DeleteEvaluationResults",
    "config:StopConfigurationRecorder"
  ],
  "Resource": "*"
}
```

SCP-AMS-020: Impeça todas as ações do IAM

Evite todas as ações do IAM.

```
{
  "Effect": "Deny",
  "Action": [
    "iam:*"
  ],
  "Resource": "*"
}
```

SCP-AMS-021: Impedir a exclusão de grupos e fluxos de registros CloudWatch

Evite excluir grupos e streams do Amazon CloudWatch Logs.

```
{
  "Effect": "Deny",
  "Action": [
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream"
  ],
  "Resource": "*"
}
```

```
}
```

SCP-AMS-022: Impedir a exclusão do Glacier

Evite a exclusão do Amazon Glacier.

```
{
  "Effect": "Deny",
  "Action": [
    "glacier:DeleteArchive",
    "glacier:DeleteVault"
  ],
  "Resource": "*"
}
```

SCP-AMS-023: Impedir a exclusão do IAM Access Analyzer

Evite a exclusão do IAM Access Analyzer.

```
{
  "Action": [
    "access-analyzer:DeleteAnalyzer"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-024: Evitar modificações no Security Hub

Impedir a exclusão do AWS Security Hub CSPM

```
{
  "Action": [
    "securityhub:DeleteInvitations",
    "securityhub:DisableSecurityHub",
    "securityhub:DisassociateFromMasterAccount",
    "securityhub:DeleteMembers",
    "securityhub:DisassociateMembers"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

```
}
```

SCP-AMS-025: Impedir a exclusão no Directory Service

Evite a exclusão de recursos em Directory Service.

```
{
  "Action": [
    "ds:DeleteDirectory",
    "ds:DeleteLogSubscription",
    "ds:DeleteSnapshot",
    "ds:DeleteTrust",
    "ds:DeregisterCertificate",
    "ds:DeregisterEventTopic",
    "ds:DisableLDAPS",
    "ds:DisableRadius",
    "ds:DisableSso",
    "ds:UnshareDirectory"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-026: Impedir o uso do serviço negado

Evite o uso de serviços negados.

Note

Substitua *service1* e *service2* por seus nomes de serviço. Exemplo *access-analyzer* ou *IAM*.

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"]
}
```

SCP-AMS-027: Impedir o uso de serviços negados em regiões específicas

Evite o uso de serviços da lista negada em regiões específicas AWS .

Note

Substitua *service1* e *service2* por seus nomes de serviço. Exemplo *access-analyzer* ou *IAM*.

Substitua *region1* e *region2* por seus nomes de serviço. Exemplo *us-west-2* ou *use-east-1*.

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"],
  "Condition": {
    "StringEquals": {
      "aws:RequestedRegion": [
        "region1",
        "region2"
      ]
    }
  }
}
```

SCP-AMS-028: Impedir que as etiquetas sejam modificadas, exceto por diretores autorizados

Evite modificações de tags por qualquer usuário, exceto os diretores autorizados. Use etiquetas de autorização para autorizar diretores. As etiquetas de autorização devem estar associadas aos recursos e aos diretores. user/role A só é considerado autorizado se a tag no recurso e no principal corresponder. Para obter mais informações, consulte os seguintes recursos:

- [Protegendo tags de recursos usadas para autorização usando uma política de controle de serviço no AWS Organizations](#)
- [Impedir que as etiquetas sejam modificadas, exceto por diretores autorizados](#)

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
```

```

"Resource": [
  "*"
],
"Condition": {
  "StringNotEquals": {
    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-project}",
    "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
  },
  "Null": {
    "ec2:ResourceTag/access-project": false
  }
}
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:RequestTag/access-project": "${aws:PrincipalTag/access-project}",
      "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
    },
    "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
        "access-project"
      ]
    }
  }
}
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {

```

```

    "StringNotEquals": {
      "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
    },
    "Null": {
      "aws:PrincipalTag/access-project": true
    }
  }
}

```

SCP-AMS-029: Impedir que os usuários excluam os registros de fluxo da Amazon VPC

Evite a exclusão dos registros de fluxo da Amazon VPC.

```

{
  "Action": [
    "ec2:DeleteFlowLogs",
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream",
    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:PutLifecycleConfiguration",
    "firehose:DeleteDeliveryStream"
  ],
  "Resource": "*",
  "Effect": "Deny"
}

```

SCP-AMS-030: Impedir o compartilhamento da sub-rede VPC com uma conta que não seja uma conta de rede

Evite compartilhar sub-redes da Amazon VPC com contas que não sejam a conta da rede.

Note

NETWORK_ACCOUNT_ID Substitua pelo ID da sua conta de rede.

```

{
  "Effect": "Deny",
  "Action": [
    "ram:AssociateResourceShare",

```

```

    "ram:CreateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "ram:Principal": "NETWORK_ACCOUNT_ID"
    },
    "StringEquals": {
      "ram:RequestedResourceType": "ec2:Subnet"
    }
  }
}

```

SCP-AMS-031: Evite a execução de instâncias com tipos de instância proibidos

Evite o lançamento de tipos de EC2 instância proibidos da Amazon.

Note

instance_type2 Substitua *instance_type1* e pelos tipos de instância que você deseja restringir, como *t2.micro* ou uma string curinga, como **.nano*.

```

{
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "ForAnyValue:StringLike": {
      "ec2:InstanceType": [
        "instance_type1",
        "instance_type2"
      ]
    }
  }
}

```

SCP-AMS-032: Impeça o lançamento de instâncias sem IMDSv2

Evite EC2 instâncias da Amazon sem IMDSv2.

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*"
  }
]
```

SCP-AMS-033: Evitar modificações na função específica do IAM

Evite modificações em funções específicas do IAM.

```
{
```



```

"Action": [
  "iam:AttachRolePolicy",
  "iam>DeleteRole",
  "iam>DeleteRolePermissionsBoundary",
  "iam>DeleteRolePolicy",
  "iam:DetachRolePolicy",
  "iam:PutRolePermissionsBoundary",
  "iam:PutRolePolicy",
  "iam:TagRole",
  "iam:UntagRole",
  "iam:UpdateAssumeRolePolicy",
  "iam:UpdateRole",
  "iam:UpdateRoleDescription"
],
"Resource": [
  "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
],
"Effect": "Deny"
}

```

SCP-AMS-034: Evitar AssumeRolePolicy modificações em funções específicas do IAM

Evite modificações nas quatro AssumeRolePolicy funções específicas do IAM.

```

{
  "Action": [
    "iam:UpdateAssumeRolePolicy"
  ],
  "Resource": [
    "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
  "Effect": "Deny"
}

```

ConfigRule: Etiquetas obrigatórias

Verifique se EC2 as instâncias têm as tags personalizadas que você solicitou. Além disso InfoSec, isso também é útil para seu gerenciamento de custos

```

ConfigRuleName: required-tags
Description: >-
  A Config rule that checks whether EC2 instances have the required tags.

```

```
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
InputParameters:
  tag1Key: COST_CENTER
  tag2Key: APP_ID
Source:
  Owner: AWS
  SourceIdentifier: REQUIRED_TAGS
```

ConfigRule: Tecla de acesso girada

Verifique se as chaves de acesso estão sendo giradas dentro do período de tempo especificado. Geralmente, isso é definido para ser de 90 dias de acordo com os requisitos de conformidade típicos.

```
ConfigRuleName: access-keys-rotated
Description: >-
  A config rule that checks whether the active access keys are rotated
  within the number of days specified in maxAccessKeyAge. The rule is
  NON_COMPLIANT if the access keys have not been rotated for more than
  maxAccessKeyAge number of days.
InputParameters:
  maxAccessKeyAge: '90'
Source:
  Owner: AWS
  SourceIdentifier: ACCESS_KEYS_ROTATED
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: chave de acesso raiz do IAM no AMS

Verifique se a chave de acesso raiz não está presente em uma conta. Para contas AMS Advanced, espera-se que isso seja compatível. out-of-the-box

```
ConfigRuleName: iam-root-access-key-check
Description: >-
  A config rule that checks whether the root user access key is available. The
  rule is COMPLIANT if the user access key does not exist.
Source:
  Owner: AWS
  SourceIdentifier: IAM_ROOT_ACCESS_KEY_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: SSM gerenciado EC2

Verifique se você EC2s está sendo gerenciado pelo SSM Systems Manager.

```
ConfigRuleName: ec2-instance-managed-by-systems-manager
Description: >-
  A Config rule that checks whether the EC2 instances in the
  account are managed by AWS Systems Manager.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
    - 'AWS::SSM::ManagedInstanceInventory'
Source:
  Owner: AWS
  SourceIdentifier: EC2_INSTANCE_MANAGED_BY_SSM
```

ConfigRule: Usuário do IAM não utilizado no AMS

Verifique as credenciais de usuário do IAM que não foram usadas por um período especificado. Assim como a verificação de rotação de chaves, o padrão é de 90 dias de acordo com os requisitos de conformidade típicos.

```
ConfigRuleName: iam-user-unused-credentials-check
Description: >-
  A config rule that checks whether IAM users have passwords
  or active access keys that have not been used within the
  specified number of days provided.
InputParameters:
  maxCredentialUsageAge: '90'
Source:
  Owner: AWS
SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: registro de buckets do S3

Verifique se o registro foi ativado para buckets do S3 na conta.

```
ConfigRuleName: s3-bucket-logging-enabled
Description: >-
  A Config rule that checks whether logging is enabled for S3 buckets.
Scope:
```

```
ComplianceResourceTypes:
  - 'AWS::S3::Bucket'
Source:
  Owner: AWS
SourceIdentifier: S3_BUCKET_LOGGING_ENABLED
```

ConfigRule: controle de versão do bucket S3

Verifique se o controle de versão e a exclusão de MFA (opcional) estão habilitados em todos os buckets do S3

```
ConfigRuleName: s3-bucket-versioning-enabled
Description: >-
  A Config rule that checks whether versioning is enabled for S3
  buckets. Optionally, the rule checks if MFA delete is enabled for S3 buckets.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::Bucket'
  Source:
    Owner: AWS
SourceIdentifier: S3_BUCKET_VERSIONING_ENABLED
```

ConfigRule: acesso público S3

Verifique se as configurações de acesso público (ACL pública, política pública, compartimentos públicos) estão restritas em toda a conta

```
ConfigRuleName: s3-account-level-public-access-blocks
Description: >-
  A Config rule that checks whether the required public access block
  settings are configured from account level. The rule is only
  NON_COMPLIANT when the fields set below do not match the corresponding
  fields in the configuration item.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::AccountPublicAccessBlock'
InputParameters:
  IgnorePublicAcls: 'True'
  BlockPublicPolicy: 'True'
  BlockPublicAcls: 'True'
  RestrictPublicBuckets: 'True'
Source:
```

Owner: AWS

SourceIdentifier: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

ConfigRule: Descobertas não arquivadas GuardDuty

Verifique se há GuardDuty descobertas não arquivadas que sejam mais antigas do que a duração especificada. A duração padrão é de 30 dias para descobertas de baixo nível, 7 dias para sev médio e 1 dia para descobertas de alto nível.

ConfigRuleName: guardduty-non-archived-findings

Description: >-

A Config rule that checks whether the Amazon GuardDuty has findings that are non archived. The rule is NON_COMPLIANT if GuardDuty has non archived low/medium/high severity findings older than the specified number.

InputParameters:

daysLowSev: '30'

daysMediumSev: '7'

daysHighSev: '1'

Source:

Owner: AWS

SourceIdentifier: GUARDDUTY_NON_ARCHIVED_FINDINGS

MaximumExecutionFrequency: TwentyFour_Hours

ConfigRule: exclusão da CMK

Verifique se há chaves mestras AWS Key Management Service personalizadas (CMKs) que estão programadas (também conhecidas como pendentes) para exclusão. Isso é crucial, pois o desconhecimento da exclusão da CMK pode fazer com que os dados sejam irrecuperáveis.

ConfigRuleName: kms-cmk-not-scheduled-for-deletion

Description: >-

A config rule that checks whether customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). The rule is NON_COMPLIANT if CMKs are scheduled for deletion.

Source:

Owner: AWS

SourceIdentifier: KMS_CMK_NOT_SCHEDULED_FOR_DELETION

MaximumExecutionFrequency: TwentyFour_Hours

ConfigRule: Rotação CMK

Verifique se a rotação automática está ativada para cada CMK na conta

```
ConfigRuleName: cmk-backing-key-rotation-enabled
Description: >-
  A config rule that checks that key rotation is enabled for each customer
  master key (CMK). The rule is COMPLIANT, if the key rotation is enabled
  for specific key object. The rule is not applicable to CMKs that have
  imported key material.
Source:
  Owner: AWS
SourceIdentifier: CMK_BACKING_KEY_ROTATION_ENABLED
MaximumExecutionFrequency: TwentyFour_Hours
```

Notificação personalizada para regras de Config

Pode haver ocorrências de regras de configuração críticas não compatíveis que exijam uma maior conscientização diretamente com sua equipe e com a equipe de liderança. InfoSec Para esses cenários, o AMS recomenda que você configure uma notificação personalizada baseada em eventos de não conformidade.

Por exemplo:

```
ConfigRuleName: required-tags
Description: >-
  A Config rule that checks whether EC2 instances have the mandated tags.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
InputParameters:
  tag1Key: COST_CENTER
  tag2Key: APP_ID
Source:
  Owner: AWS
SourceIdentifier: REQUIRED_TAGS
NotificationEventRule:
  Type: 'AWS::Events::Rule'
Properties:
  Name: CWEventForrequired-tags
  Description: >-
    SNS Notification for Non-Compliant Events of Config Rule:
    required-tags
  State: ENABLED
  EventPattern:
    detail-type:
      - Config Rules Compliance Change
```

```

    source:
      - aws.config
    detail:
      newEvaluationResult:
        complianceType:
          - NON_COMPLIANT
      configRuleARN:
        - 'Fn::GetAtt':
            - RequiredEC2Tags
            - Arn
    Targets:
      - Id: RemediationNotification
      Arn:
        Ref: SnsTopic
      InputTransformer:
        InputTemplate: >-
          "EC2 Instance <Instance_ID> is non-compliant. Please add required tags:
COST_CENTER, APP_ID, Name, and Backup."
        InputPathsMap:
          instance_id: $.detail.resourceId
    SnsTopic:
      Type: 'AWS::SNS::Topic'
      Properties:
        Subscription:
          - Endpoint: Cloud_Ops_Leaders@customer.com
            Protocol: email
          TopicName: noncompliant-instance-notification
    SnsTopicPolicy:
      Type: 'AWS::SNS::TopicPolicy'
      Properties:
        PolicyDocument:
          Statement:
            - Sid: __default_statement_ID
              Effect: Allow
              Principal:
                AWS: '*'
              Action:
                - 'SNS:GetTopicAttributes'
                - 'SNS:SetTopicAttributes'
                - 'SNS:AddPermission'
                - 'SNS:RemovePermission'
                - 'SNS:DeleteTopic'
                - 'SNS:Subscribe'
                - 'SNS:ListSubscriptionsByTopic'

```

```

    - 'SNS:Publish'
    - 'SNS:Receive'
  Resource:
    Ref: SnsTopic
  Condition:
    StringEquals:
      'AWS:SourceOwner':
        Ref: 'AWS::AccountId'
- Sid: TrustCWEToPublishEventsToMyTopic
  Effect: Allow
  Principal:
    Service: events.amazonaws.com
  Action: 'sns:Publish'
  Resource:
    Ref: SnsTopic
Topics:
  - Ref: SnsTopic

```

Função vinculada ao serviço de EventBridge regras da Amazon para o AMS Advanced

O AMS Advanced usa a função vinculada ao serviço (SLR) chamada `AWSServiceRoleForManagedServices_Events`— Essa função confia em um dos diretores do serviço AWS Managed Services (`events.managedservices.amazonaws.com`) para assumir a função para você. O serviço usa a função para criar uma regra EventBridge gerenciada. Essa regra é a infraestrutura necessária em sua AWS conta para fornecer informações de alteração do estado de alarme de sua conta para a AWS Managed Services.

Permissões para EventBridge SLR para AMS Advanced

O perfil vinculado ao serviço `AWSServiceRoleForManagedServices_Events` confia nos seguintes serviços para aceitar o perfil:

- `events.managedservices.amazonaws.com`

Anexada a essa função está a política `AWSManagedServices_EventsServiceRolePolicy` AWS gerenciada (consulte a [política gerenciada da AWS: `AWSManagedServices\_EventsServiceRolePolicy`](#)). O serviço usa a função para fornecer informações de alteração do estado do alarme da sua conta para o AWS Managed Services. Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte [Permissões de função vinculadas ao serviço](#) no Guia do usuário do AWS Identity and Access Management.

Você pode baixar o JSON `AWSManagedServices_EventsServiceRolePolicy` neste ZIP: [EventsServiceRolePolicy.zip](#).

Criando uma EventBridge SLR para o AMS Advanced

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você se integra ao AMS no AWS Management Console, no ou na AWS API AWS CLI, o AMS Advanced cria a função vinculada ao serviço para você.

Important

Essa função vinculada ao serviço pode aparecer em sua conta se você estava usando o serviço AMS Advanced antes de 7 de fevereiro de 2023, quando ele começou a oferecer suporte a funções vinculadas ao serviço e, em seguida, o AMS Accelerate criou a `AWSServiceRoleForManagedServices_Events` função em sua conta. Para saber mais, consulte [Uma nova função apareceu na minha conta do IAM](#).

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você pode usar esse mesmo processo para recriar a função na sua conta. Quando você se integra ao AMS, o AMS Advanced cria a função vinculada ao serviço para você novamente.

Editando uma EventBridge SLR para AMS Advanced

O AMS Advanced não permite que você edite a função `AWSServiceRoleForManagedServices_Events` vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte [Editar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Excluindo uma EventBridge SLR para o AMS Advanced

Você não precisa excluir manualmente a função `AWSServiceRoleForManagedServices_Events`. Quando você sai do AMS no AWS Management Console AWS CLI ou na AWS API, o AMS Advanced limpa os recursos e exclui a função vinculada ao serviço para você.

Você também pode usar o console do IAM AWS CLI ou a AWS API para excluir manualmente a função vinculada ao serviço. Para isso, primeiro você deve limpar manualmente os recursos de sua função vinculada ao serviço e depois excluí-la manualmente.

 Note

Se o serviço AMS Advanced estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir recursos do AMS Advanced usados pela função vinculada ao `AWSServiceRoleForManagedServices_Events` serviço

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função `AWSServiceRoleForManagedServices_Events` vinculada ao serviço.

Para obter mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Práticas recomendadas de segurança

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.

Configurações não padrão de EPS da landing zone multiconta do 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.

Guardrails AMS

Uma grade de proteção é uma regra de alto nível que fornece governança contínua para seu ambiente geral de 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.

Políticas de controle de serviços MALZ

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.

Resposta a incidentes de segurança no AMS

A segurança é a principal prioridade no AWS Managed Services (AMS). O AMS implanta recursos e controles em suas contas para gerenciá-las. AWS tem um modelo de responsabilidade compartilhada: AWS gerencia a segurança da nuvem e você é responsável pela segurança na nuvem. O AMS protege seus dados e ativos e ajuda a manter sua AWS infraestrutura segura usando controles de segurança e monitoramento ativo para problemas de segurança. Esses recursos ajudam você a estabelecer uma linha de base de segurança para aplicativos executados na AWS nuvem. A AMS colabora com você por meio do Security Incident Response para avaliar o efeito e, em seguida, realizar a contenção e as remediações com base nas recomendações de melhores práticas.

Quando ocorre um desvio da linha de base, como por uma configuração incorreta ou uma alteração em fatores externos, você precisa responder e investigar. Para fazer isso com sucesso, você precisa entender os conceitos básicos de Resposta a Incidentes de Segurança em seu ambiente AMS. Você também deve entender os requisitos para preparar, educar e treinar equipes de nuvem antes que ocorram problemas de segurança. É importante conhecer os controles e os recursos que você pode usar, preparar planos de resposta para problemas comuns de segurança, como comprometimento da conta do usuário ou uso indevido de contas privilegiadas, e identificar métodos de remediação que usam a automação para melhorar a velocidade e a consistência da resposta. Além disso, você precisa entender seus requisitos regulatórios e de conformidade relacionados à criação de um programa de resposta a incidentes de segurança para atender a esses requisitos.

A resposta a incidentes de segurança pode ser complexa, mas, ao implementar uma abordagem iterativa, você pode simplificar o processo e permitir que a equipe de resposta a incidentes mantenha as partes interessadas dos ativos satisfeitas, fornecendo detecção e resposta precoces e contínuas. Neste guia, fornecemos a metodologia que o AMS usa para resposta a incidentes, a matriz de

responsabilidade do AMS (RACI), como você pode se preparar para um evento de segurança, como engajar o AMS durante incidentes de segurança e alguns dos runbooks de resposta a incidentes que o AMS usa.

Como funciona o AMS Security Incident Response

O AWS Managed Services se alinha ao [Guia de Tratamento de Incidentes de Segurança de Computadores do NIST 800-61 para resposta a incidentes de segurança](#). Ao nos alinharmos a esse padrão do setor, fornecemos uma abordagem consistente para o gerenciamento de eventos de segurança e aderimos às melhores práticas para proteger e responder a incidentes de segurança em sua nuvem.

Ciclo de vida de resposta a incidentes

Quando a detecção identifica e gera um alerta de segurança, ou você solicita assistência de segurança, a equipe de operações do AWS Managed Services garante que haja uma investigação oportuna, executa automações para realizar a coleta, triagens e análises de dados, informa sobre a análise, realiza a investigação e quaisquer atividades de contenção e, em seguida, publica a análise do evento.

As atividades de coleta, triagem, análise e contenção de dados realizadas durante a resposta ao incidente variam de acordo com o tipo de evento de segurança que está sendo investigado. Exemplos de fluxos de trabalho do Security Incident Response para cenários selecionados estão no final deste documento.

Durante incidentes, o AMS determina dinamicamente o curso de ação correto, o que pode resultar em etapas documentadas sendo reordenadas ou ignoradas, conforme apropriado, para garantir que o resultado correto ocorra.

Preparar

À medida que o cenário de ameaças evolui, o AMS continua expandindo os recursos de detecção e resposta. À medida que novas detecções são adicionadas, o AMS incorpora os alertas dessas novas detecções na plataforma de detecção e resposta. Os agentes de segurança da AMS são treinados para investigar e fazer parceria com você durante todo o ciclo de vida do Security Incident Response.

Por causa dessa abordagem de parceria, é importante que suas equipes de segurança e aplicativos estejam preparadas para interagir com o AMS para lidar com eventos de segurança à medida

que esses eventos ocorrerem. Esta documentação explica o que esperar durante um evento de segurança e ajuda você a se preparar para uma resposta rápida quando ocorrer um incidente de segurança.

Esta documentação usa a definição do NIST 800-61 de um evento como qualquer ocorrência observável em um sistema ou rede e um incidente como uma violação ou ameaça iminente de violação de políticas, políticas de uso aceitável ou práticas de segurança padrão.

Lista de verificação de preparação

Faça a seguinte lista de verificação com seu gerente de entrega de soluções de nuvem (CSDM) e arquiteto de nuvem AMS (CA):

- Entenda quais cargas de trabalho estão sendo executadas em quais contas.
- Entenda quais equipes internas são responsáveis pelas várias cargas de trabalho e marque-as adequadamente nas cargas de trabalho.
- Mantenha os detalhes de contato internos de outras equipes que possam ser necessárias durante uma investigação de evento de segurança e para decisões de contenção.
- Confirme se os contatos de segurança estão atualizados e adicionados a todas as AWS contas gerenciadas. Os contatos são gerenciados por conta.
- Saiba como enviar um incidente de segurança para o AMS e esteja familiarizado com a gravidade e os tempos de resposta esperados.
- Certifique-se de que, quando as notificações de segurança forem recebidas, elas sejam encaminhadas para as pessoas e sistemas apropriados, como pagers ou seu centro de operações de segurança.
- Entenda quais fontes de registro estão disponíveis para você, onde elas estão armazenadas em suas contas e quem tem acesso a elas.
- Entenda como usar o CloudWatch Insights para consultar registros durante investigações.
- Entenda as opções de contenção disponíveis para você por recurso (IAM, EC2, S3 e assim por diante) e as consequências na disponibilidade de sua carga de trabalho quando em contenção.

Detectar

Durante o gerenciamento de suas AWS contas, o AMS monitora anomalias no comportamento do usuário, atividades da conta e possíveis eventos de segurança usando dados coletados de fontes

e controles de detecção, incluindo, mas não se limitando a, CloudWatch Amazon, GuardDuty VPC Flow Logs, Amazon Macie e feeds internos de inteligência de ameaças AWS Config da Amazon.

O AMS usa AWS serviços nativos e outras tecnologias de detecção para responder aos eventos de segurança criados por:

- Configure tipos de descoberta de conformidade
- GuardDuty Tipos de localização
- Tipos de descoberta de Macie
- Eventos de firewall DNS do Amazon Route 53 Resolver
- Eventos de segurança do AMS (alarmes de vigilância na nuvem)

Descobertas adicionais são adicionadas à medida que os serviços, produtos e ecossistemas de ameaças evoluem.

Relate eventos de segurança ao AMS

Levante um incidente por meio do Suporte Centro ou Portal de Suporte do AMS para notificar o AMS sobre um incidente de segurança ou solicitar investigações.

Analisar

Depois que um evento de segurança é identificado e relatado, a próxima etapa é analisar se o evento relatado é um falso positivo ou um incidente real. O AMS usa automação e técnicas de investigação manual para lidar com eventos de segurança. A análise inclui a investigação de registros de diferentes fontes de detecção, como registros de tráfego de rede, registros de host, CloudTrail eventos, registros AWS de serviços e assim por diante. A análise também busca padrões que mostram um comportamento anômalo por correlação.

Sua parceria é necessária para entender o contexto específico do ambiente da conta e estabelecer o que é normal para sua conta e suas cargas de trabalho. Isso ajuda o AMS a identificar uma anomalia mais rapidamente e a uma resposta acelerada a incidentes.

Gerencie as comunicações do AMS sobre eventos de segurança

O AMS mantém você informado durante a investigação, envolvendo seus contatos de segurança por meio de um ticket de incidente. Seu gerente de prestação de serviços em nuvem (CSDM) e o arquiteto de nuvem (CA) do AMS são os pontos de contato a serem contatados para qualquer comunicação durante uma investigação de segurança ativa.

A comunicação inclui a notificação automática quando um alerta de segurança é gerado, a comunicação após a análise do evento, o estabelecimento de pontes de chamadas e a entrega contínua de artefatos, como arquivos de log, captura instantânea dos recursos infectados e obtenção dos resultados da investigação durante o evento de segurança.

Os campos padrão incluídos nas notificações de alerta de segurança do AMS estão listados abaixo. Esses campos fornecem informações para que você possa encaminhar eventos para as equipes apropriadas em sua organização para remediação.

- Tipo de descoberta
- Identificador de localização (quando relevante)
- Encontrando a severidade
- Descrição da descoberta
- Localizando a data e a hora de criação
- AWS ID da conta
- Região (quando relevante)
- AWS Recursos (IAMuser/role/policy, S3 EC2, EKS)

Campos adicionais são fornecidos dependendo do tipo de descoberta, por exemplo, as descobertas do EKS incluem detalhes do pod, do contêiner e do cluster.

Contenção

A abordagem da AMS à contenção é uma parceria com você. Você entende seus negócios e os impactos na carga de trabalho que podem ocorrer com atividades de contenção, como isolamento de rede, desprovisionamento de usuários ou funções do IAM, reconstrução de instâncias e assim por diante.

Uma parte essencial da contenção é a tomada de decisões. Por exemplo, desligue um sistema, isole um recurso da rede ou desative o acesso ou encerre sessões. Essas decisões são mais fáceis de tomar se houver estratégias e procedimentos predeterminados para conter o incidente. O AMS fornece a estratégia de contenção e, em seguida, implementa a solução depois de considerar o risco envolvido na implementação das ações de contenção.

Há diferentes opções de contenção, dependendo dos recursos em análise. A AMS espera que vários tipos de contenção sejam implantados simultaneamente durante uma investigação de incidente. Alguns desses exemplos incluem:

- Aplique regras de proteção para bloquear tráfego não autorizado (grupo de segurança, NACL, regras WAF, regras de SCP, negação de listagem, configuração da ação de assinatura para quarentena ou bloqueio)
- Isolamento de recursos
- Isolamento de rede
- Desabilitando usuários, funções e políticas do IAM
- Modificando/reduzindo o usuário e o privilégio de função do IAM
- Encerrando/Suspendo/ Excluindo recursos computacionais
- Restringindo o acesso público ao recurso afetado
- Chaves de acesso, chaves de API e senhas rotativas
- Limpando credenciais divulgadas e informações confidenciais

A AMS incentiva você a considerar o tipo de estratégia de contenção para cada tipo de incidente importante que esteja dentro de seu apetite pelo risco, com critérios claramente documentados para ajudar na tomada de decisões no caso de um incidente. Os critérios para determinar a estratégia apropriada incluem:

- Potenciais danos aos recursos.
- Preservação de evidências
- Indisponibilidade de serviços (por exemplo, conectividade de rede e serviços fornecidos para entidades externas).
- Tempo e recursos necessários para implementar a estratégia.
- Eficácia da estratégia (por exemplo, contenção parcial, contenção total)
- Permanência da solução (por exemplo, decisões de porta unidirecional versus decisões de porta bidirecional)
- Duração da solução (por exemplo, solução alternativa de emergência a ser removida em quatro horas, solução temporária a ser removida em duas semanas, solução permanente).
- Aplique controles de segurança que você possa ativar para reduzir o risco e ter tempo para definir e implementar uma contenção mais eficaz.

A velocidade da contenção é fundamental. A AMS recomenda uma abordagem em etapas para obter uma contenção eficiente e eficaz, elaborando estratégias de abordagens de curto e longo prazo.

Use este guia para considerar sua estratégia de contenção que envolve técnicas diferentes com base no tipo de recurso.

- Estratégia de contenção
 - O AMS pode identificar o escopo do incidente de segurança?
 - Em caso afirmativo, realize a identificação de todos os recursos afetados (usuários, sistemas e recursos).
 - Em caso negativo, realize a investigação simultaneamente à execução da próxima etapa nos recursos previamente identificados.
 - O recurso pode ser isolado?
 - Em caso afirmativo, prossiga com o isolamento dos recursos afetados.
 - Em caso negativo, colabore com os responsáveis pelos sistemas e gerentes para determinar as ações necessárias para a contenção do problema.
 - Todos os recursos afetados estão isolados dos recursos que não foram afetados?
 - Em caso afirmativo, prossiga para a próxima etapa.
 - Se não, continue isolando os recursos afetados até que a contenção de curto prazo seja realizada para evitar que o incidente se agrave ainda mais.
- Backup do sistema
 - Foram criadas cópias de backup dos sistemas afetados para análises posteriores?
 - As cópias para análises forenses estão devidamente criptografadas e armazenadas em um local seguro?
 - Em caso afirmativo, prossiga para a próxima etapa.
 - Em caso negativo, criptografe as imagens para análises forenses e, em seguida, armazene-as em um local seguro para evitar uso acidental, danos e adulterações.

Erradicação

Depois que um incidente for contido, a erradicação pode ser necessária para eliminar completamente as fontes de ameaça e proteger o sistema antes de prosseguir para o próximo estágio de recuperação. As etapas de erradicação podem incluir a exclusão de malware e a remoção de contas de usuário comprometidas, além de identificar e mitigar todas as vulnerabilidades que foram exploradas. Durante a erradicação, é importante identificar todas as contas, recursos e instâncias afetados no ambiente para que possam ser corrigidos.

É uma prática recomendada que a erradicação e a recuperação sejam feitas em uma abordagem em fases para que as etapas de remediação sejam priorizadas. Para incidentes de grande escala, a recuperação pode levar meses. A intenção das fases iniciais deve ser aumentar a segurança geral com mudanças de alto valor relativamente rápidas (dias ou semanas) para evitar futuros incidentes. As fases posteriores devem se concentrar em mudanças de longo prazo (por exemplo, mudanças na infraestrutura) e no trabalho contínuo para manter a empresa o mais segura possível.

Para alguns incidentes, a erradicação não é necessária ou é realizada durante a recuperação.

Considere o seguinte:

- O sistema pode ser recriado e depois reforçado com patches ou outras contramedidas para evitar ou reduzir o risco de ataques?
- Todos os malwares e outros artefatos deixados pelos atacantes são removidos e os sistemas afetados são protegidos contra novos ataques?

Recuperar

A AMS faz parceria com você para restaurar a operação normal dos sistemas, confirmar se os sistemas estão funcionando normalmente e (conforme aplicável) corrigir vulnerabilidades para evitar incidentes semelhantes.

Considere o seguinte:

- O (s) sistema (s) afetado (s) está (m) corrigido (s) e protegido (s) contra o ataque recente e possíveis ataques futuros?
- Em que dia e horário são viáveis para restaurar a produção dos sistemas afetados?
- Quais ferramentas você usará para testar, monitorar e verificar se os sistemas que você restaura para produção não são vulneráveis às técnicas iniciais de ataque?

Relatório pós-incidente

Após o evento, o AMS executa um processo de análise de investigação para todos os incidentes de segurança. Além disso, o AMS inicia um processo de correção de erro (COE) para tratar de incidentes de segurança causados por um sistema ou por uma falha processual que, plausivelmente, pode ser melhorada. A AMS faz parceria com você para melhorar continuamente a experiência de investigação de segurança. O processo de COE ajuda a AMS a identificar os fatores que contribuem

para eventos que afetam o cliente e conecta essas causas aos itens de ações futuras que podem evitar que eventos semelhantes se repitam ou ajudar a mitigar a duração ou o nível de impacto.

O processo de análise da investigação de incidentes de segurança aborda os seguintes itens para identificar oportunidades de melhoria:

- Qual foi o tempo decorrido desde o início do incidente até a descoberta do incidente, a avaliação inicial do impacto e cada estágio do processo de tratamento do incidente (por exemplo, contenção, recuperação)?
- Quanto tempo a equipe de resposta a incidentes levou para responder ao relatório inicial do incidente?
- Quanto tempo demorou para fazer uma análise de impacto inicial?
- Isso era evitável e como? Existe uma ferramenta ou processo que poderia ter evitado isso?
- Poderíamos ter detectado isso mais cedo e como?
- O que poderia ter acelerado a investigação?
- Os procedimentos documentados de resposta a incidentes foram seguidos? Eles eram adequados?
- O compartilhamento de informações com outras partes interessadas foi feito em tempo hábil? Como ele poderia ser melhorado?
- A colaboração com outras equipes (AWS segurança, equipes de contas, equipe de AWS desenvolvimento e equipe de segurança do cliente) foi eficaz? Se não, o que poderia ser melhorado?
- Quais etapas de preparação estavam faltando que poderiam ter ajudado, matrizes de escalonamento, RACIs, modelos de responsabilidade compartilhada e assim por diante? É necessário atualizar algum Runbook?
- Qual foi a diferença entre a avaliação de impacto inicial e a avaliação de impacto final? O que podemos fazer para melhorar a precisão das avaliações anteriores na resposta ao incidente?
- Quais são os itens de ação das lições aprendidas?

Runbooks de resposta a incidentes de segurança no AMS

Esta seção contém dois runbooks:

- [Resposta à atividade do usuário root](#)

- [Resposta a eventos de malware](#)

Resposta à atividade do usuário root

O [usuário root](#) é o superusuário em sua AWS conta. Observe que o AMS monitora o uso do root. É uma prática recomendada usar o usuário root somente para as poucas tarefas que o exigem, como alterar as configurações da conta, ativar o acesso AWS Identity and Access Management (IAM) ao faturamento e ao gerenciamento de custos, alterar sua senha raiz e ativar a autenticação multifator (MFA). Para obter mais informações, consulte [Tarefas que exigem credenciais de usuário root](#).

Para obter mais informações sobre como informar o AMS sobre o uso raiz planejado, consulte [Quando e como usar a conta raiz no AMS](#).

Quando a atividade do usuário root é detectada, ou tentativas malsucedidas de login que podem indicar um ataque de força bruta ou atividade na conta após um login bem-sucedido, um evento é gerado e um incidente é enviado aos seus contatos de segurança definidos.

O AWS Managed Services Operations investiga atividades não planejadas do usuário raiz, realiza coleta, triagem e análise de dados e realiza atividades de contenção sob sua orientação, seguidas pela análise pós-evento.

Se você tiver o modelo operacional AMS Advanced, receberá comunicações adicionais dos engenheiros do AMS CSDM e do AMS Ops que confirmam a atividade não planejada do usuário raiz devido à responsabilidade do AMS de proteger as credenciais do usuário raiz. O AMS investiga a atividade do usuário raiz até que você confirme um caminho a seguir.

Preparar

Avise o AMS sobre qualquer uso planejado do usuário raiz enviando uma solicitação de serviço do AMS com dados e horários do evento planejado para evitar atividades desnecessárias de resposta a incidentes.

Conduza periodicamente GameDays com a AMS para validar os processos de resposta a incidentes de clientes da AMS, se as pessoas e os sistemas estão atualizados e crie uma memória muscular com indivíduos responsáveis para obter uma resposta mais rápida a incidentes.

Fase A: Detectar

O AMS monitora a atividade raiz nas contas por meio de fontes de detecção, incluindo GuardDuty o monitoramento do AMS.

Se você tiver o AMS Accelerate, o modelo operacional responde ao incidente solicitando investigação de atividade inesperada do usuário raiz. Quando isso ocorre, o AMS Operations inicia o runbook de contas comprometidas.

Se você tiver o AMS Advanced, o modelo operacional responde ao incidente ou informa o CSDM sobre qualquer atividade planejada do usuário raiz para encerrar uma investigação ativa de comprometimento de conta.

Fase B: Analisar

O AMS realiza uma investigação completa dos eventos do usuário raiz quando é determinado que a atividade não está autorizada. Usando as automações e a equipe de resposta de segurança do AMS, os registros e eventos são analisados em busca de anomalias e comportamentos inesperados dos usuários root. Os registros são fornecidos para ajudar a determinar se a atividade é desconhecida, se é um evento autorizado do usuário root ou se requer uma investigação mais aprofundada.

Alguns exemplos das informações fornecidas durante a investigação para apoiar as verificações internas incluem:

- Informações da conta: em qual conta a conta raiz foi usada?
- Endereço de e-mail do usuário raiz: cada usuário raiz está associado a um endereço de e-mail da sua organização
- Detalhes da autenticação: de onde e quando o usuário root acessou seu ambiente?
- Registros de atividades: o que o usuário fez quando estava logado como root? Esses registros estão na forma de CloudWatch eventos. Entender como ler esses registros ajuda na investigação.

É uma prática recomendada que você esteja preparado para receber as informações de análise e ter um plano de como alcançar pontos de contato autorizados para contas em sua organização. Como os usuários raiz não são nomeados como indivíduos, determinar quem tem acesso ao endereço de e-mail raiz usado para a conta em sua organização ajuda a encaminhar rapidamente as perguntas internamente.

Fase C: Conter e erradicar

A AMS faz parceria com suas equipes de segurança para realizar a contenção sob a orientação de seus contatos autorizados de Segurança do Cliente. As opções de contenção incluem:

- Rotação de credenciais e chaves apropriadas.

- Encerramento de sessões ativas em contas e recursos.
- Erradicando os recursos criados.

Durante as atividades de contenção, o AMS trabalha em estreita colaboração com sua equipe de segurança para garantir que qualquer interrupção em suas cargas de trabalho seja minimizada e que as credenciais raiz sejam protegidas adequadamente.

Depois que o plano de contenção for concluído, você trabalha com a equipe de operações do AMS para quaisquer ações de recuperação, conforme necessário.

Relatório pós-incidente

Conforme necessário, a AMS inicia o processo de revisão da investigação para identificar as lições aprendidas. Como parte da conclusão de um COE, a AMS comunica todas as descobertas relevantes aos clientes afetados para ajudá-los a melhorar seu processo de resposta a incidentes.

O AMS documenta todos os detalhes finais da investigação, coleta métricas apropriadas e, em seguida, relata o incidente a qualquer equipe interna do AMS que precise de informações, incluindo seu CSDM e CA designados.

Resposta a eventos de malware

As EC2 instâncias da Amazon são usadas para hospedar uma variedade de cargas de trabalho, incluindo software de terceiros e software desenvolvido sob medida, implantado por equipes de aplicativos dentro das organizações. O AMS fornece e incentiva você a implantar suas cargas de trabalho em imagens que são corrigidas e mantidas continuamente pelo AMS.

Durante a operação das instâncias, o AMS monitora anomalias no comportamento ou na atividade por meio de uma variedade de controles de detecção de segurança, incluindo Amazon, Endpoint Protection GuardDuty, Network Traffic e feeds internos da Amazon Threat Intelligence.

Os clientes do AMS com o modelo operacional AMS Advanced têm automaticamente o cliente de monitoramento de segurança de terminais (EPS) instalado nos recursos provisionados. Isso garante que os recursos sejam monitorados e suportados 24 horas por dia, 7 dias por semana, incluindo a criação de um incidente de segurança quando um evento é detectado.

O AMS também monitora as descobertas de GuardDuty malware. Eles estão disponíveis no AMS Advanced e no AMS Accelerate, se habilitados. Consulte [Proteção contra malware na Amazon GuardDuty](#) para obter mais informações.

 Note

Se você optou por [Traga seu próprio EPS](#), o processo de resposta a incidentes é diferente do descrito nesta página. Para obter mais informações, consulte a documentação referenciada.

Quando um malware é detectado, um incidente é criado e você é notificado sobre o evento. Essa notificação é seguida por todas as atividades de remediação que ocorreram. O AMS Operations investiga, realiza coleta, triagem e análise de dados e, em seguida, realiza atividades de contenção sob sua direção, seguidas pela análise pós-evento.

Fase A: Detectar

O AMS monitora eventos em instâncias com GuardDuty monitoramento de soluções de segurança de terminais. O AMS determina as atividades apropriadas de enriquecimento e triagem para ajudá-lo a tomar decisões de contenção ou aceitação de riscos com base no tipo de descoberta ou alerta.

A coleta de dados é realizada com base no tipo de descoberta. A coleta de dados envolve a consulta de várias fontes de dados dentro e fora da conta afetada para criar uma imagem da atividade observada ou das configurações preocupantes.

O AMS realiza a correlação da descoberta com quaisquer outros alarmes e alertas ou telemetria de quaisquer contas afetadas ou plataformas de inteligência de ameaças da AMS.

Fase B: Analisar

Depois que os dados são coletados, eles são analisados para identificar qualquer atividade ou indicador de preocupação. Durante essa fase da investigação, a AMS faz parceria com você para integrar o conhecimento comercial e de domínio das instâncias e cargas de trabalho para ajudar a entender o que é esperado e o que está fora do comum.

Alguns exemplos das informações fornecidas durante a investigação para apoiar as verificações internas incluem:

- Informações da conta: em qual conta a atividade do malware foi observada?
- Detalhes da instância: quais instâncias estão envolvidas nos eventos de malware?
- Data e hora do evento: quando o alerta foi acionado?
- Informações sobre a carga de trabalho: o que está sendo executado na instância?

- Detalhes do malware, se relevante: famílias de malware e informações de código aberto sobre o malware.
- Detalhes de usuários ou funções: quais usuários ou funções são afetados e envolvidos na atividade?
- Registros de atividades: quais atividades são registradas na instância? Eles estão na forma de CloudWatch eventos e eventos do sistema da instância. Entender como ler esses registros ajudará você na investigação.
- Atividade de rede: quais endpoints estão se conectando à instância, a que a instância está se conectando e qual é a análise de tráfego?

É uma prática recomendada estar preparado para receber informações de investigação e ter um plano sobre como entrar em contato com os pontos de contato apropriados para contas, instâncias e cargas de trabalho em sua organização. Compreender a topologia da rede e a conexão esperada pode ajudar a acelerar a análise de impacto. O conhecimento dos testes de penetração planejados no ambiente e das implantações recentes realizadas pelos proprietários de aplicativos também podem acelerar a investigação.

Se você determinar que a atividade foi planejada e autorizada, o incidente será atualizado e a investigação será encerrada. Se o comprometimento for confirmado, você e a AMS determinarão o plano de contenção apropriado.

Fase C: Conter e erradicar

A AMS faz parceria com você para determinar as atividades de contenção apropriadas com base nos dados coletados e nas informações conhecidas. As opções de contenção incluem, mas não estão limitadas a:

- Preservando dados por meio de instantâneos
- Modificação das regras de rede para limitar o tráfego de entrada ou saída de instâncias
- Modificando as políticas de usuário e função do SCP, do IAM para limitar o acesso
- Encerramento, suspensão ou desativação de instâncias
- Encerrando todas as conexões persistentes
- Rotação de credenciais/chaves apropriadas

Se você optar por realizar atividades de erradicação contra a instância, o AMS o ajudará a conseguir isso. As opções incluem, mas não estão limitadas a:

- Removendo qualquer software indesejado
- Reconstruindo a instância a partir de uma imagem limpa e totalmente corrigida e reimplantando aplicativos e configurações
- Restaurando a instância a partir de um backup anterior
- Implantar aplicativos e serviços em outra instância da sua conta que possa ser adequada para hospedar as cargas de trabalho.

É importante determinar como o malware foi entregue e executado na instância antes da restauração do serviço para garantir que quaisquer controles adicionais sejam aplicados para evitar a recorrência do malware na instância. O AMS fornece insights ou informações adicionais aos seus parceiros ou equipes forenses, conforme necessário, para apoiar a perícia.

Neste ponto, você trabalha com o AMS Operations para as atividades de recuperação. O AMS trabalha em estreita colaboração com você para minimizar a interrupção das cargas de trabalho e proteger as instâncias.

Relatório pós-incidente

Conforme necessário, a AMS inicia o processo de revisão da investigação para identificar as lições aprendidas. Como parte da conclusão de um COE, o AMS comunica descobertas relevantes para ajudá-lo a melhorar seu processo de resposta a incidentes.

O AMS documenta os detalhes finais da investigação, coleta métricas apropriadas e relata o incidente às equipes internas do AMS que precisam de informações, incluindo seu CSDM e CA designados.

Revisões de segurança de solicitações de alteração no AMS Advanced

O processo de revisão da solicitação de alteração do AWS Managed Services garante que o AMS realize uma análise de segurança das alterações solicitadas à medida que elas são implementadas em seu nome em sua conta.

[Padrões técnicos avançados do AMS](#) define os critérios, configurações e processos mínimos de segurança para estabelecer a segurança básica de suas contas. Quando o AMS implementa as mudanças solicitadas, seguimos esses padrões.

O AMS avalia todas as solicitações de alteração 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 um processo de revisão de segurança. Durante esse processo, o risco relevante é destacado pela AMS e revisado e aprovado por seu aprovador de riscos autorizado para equilibrar as necessidades comerciais e de segurança.

Processo de gerenciamento de riscos de segurança do cliente

O processo de Gerenciamento Avançado de Riscos de Segurança do Cliente (CSRM) da AMS ajuda a identificar e comunicar claramente os riscos aos proprietários certos. Esse processo minimiza os riscos de segurança em seu ambiente e reduz a sobrecarga operacional contínua dos riscos identificados.

Por padrão, quando alguém da sua organização solicita que o AMS implemente uma alteração em seu ambiente gerenciado, o AMS analisa a alteração para determinar se a solicitação está fora dos padrões técnicos, o que pode alterar a postura de segurança da sua conta. Se houver um risco de segurança alto ou muito alto, a revisão da alteração será aceita ou rejeitada pela equipe de segurança autorizada. As alterações solicitadas também são avaliadas quanto aos efeitos adversos na capacidade da AMS de operar a conta. Se a revisão encontrar possíveis impactos adversos, revisões e aprovações adicionais serão necessárias dentro da AMS.

Você pode optar por não participar do fluxo de trabalho baseado em aprovação no processo de CSRM para riscos altos ou muito altos. Para alterar a opção CSRM para contas específicas de CSRM padrão para Somente notificação, trabalhe com seus gerentes de entrega de serviços em nuvem para criar uma aceitação de risco única. Se você optar por continuar com a opção Somente notificação, o AMS implementará as alterações solicitadas, independentemente da categoria de risco. Além disso, o AMS envia uma notificação de risco para seus aprovadores de risco autorizados em vez de buscar aprovação antes da implementação da mudança. Fale com seus arquitetos de nuvem ou gerentes de entrega de serviços em nuvem para obter mais informações sobre o processo de CSRM do AMS, como alterar a opção de CSRM padrão ao integrar novas contas do AMS ou como atualizar as contas existentes.

Note

O AMS recomenda fortemente que você use a opção padrão de CSRM padrão em todas as suas contas.

Padrões técnicos avançados do AMS

A seguir estão as categorias de padrões técnicos avançados do AMS:

ID	Categoria
AMS-STD-001	Configuração de marcação
AMS-STD-002	AWS Identity and Access Management
AMS-STD-003	Segurança de rede
AMS-STD-004	Teste de penetração
AMS-STD-005	Amazon GuardDuty
AMS-STD-006	Segurança do host
AMS-STD-007	Registro em log
AMS-STD-008	ESTOU LOUCO
AMS-STD-009	Diversos

Controles padrão no AMS Advanced

A seguir estão os controles padrão no AMS:

AMS-STD-001 - Configuração de marcação

A seguir está o controle padrão para 001 - Configuração de marcação.

1. Todos os AWS recursos exigidos pela equipe do AMS para fins operacionais e de gerenciamento devem ter o seguinte par de valores-chave.
 - Appld= AMSInfrastructure
 - Meio ambiente = AMSInfrastructure
 - AppName = AMSInfrastructure
 - AMSResource=Verdadeiro

2. Todas as tags exigidas pela equipe do AMS, exceto as listadas anteriormente, devem ter prefixos conforme mencionado na lista de prefixos do AMS (consulte a Nota).
3. Os valores de tag exigidos pela equipe do AMS (AppId, Ambiente e AppName) podem ser alterados em qualquer um dos recursos criados por você com base em suas solicitações de alteração.
4. Qualquer tag nas pilhas exigida pelo AMS não deve ser excluída com base em suas solicitações de alteração.
5. Você não pode usar a convenção de nomenclatura de tags do AMS para sua infraestrutura, conforme mencionado no ponto 2.
6. Você pode criar etiquetas personalizadas nos recursos exigidos pelo AMS (normalmente para casos de uso de faturamento e relatórios de custos). As tags personalizadas são mantidas se os recursos forem atualizados pela atualização da pilha e não pela atualização do modelo.

 Note

Lista de prefixos AMS

1. ams-*
2. AWSManagedServiços*
3. /ams/ *
4. mão*
5. MÃO*
6. Amigos*
7. mc*
8. MC*
9. Mc*
- 10sentinela*
- 11Sentinela*
- 12Serviços_gerenciados*
- 13Novo AMS*
- 14AWS_*
- 15era*
- 16.VPC_*

17.CloudTrail*
 18.Cloudtrail*
 19/aws_reserved/
 20.JINGERIR*
 21.EPSDB*
 22.MÃES*
 23.TemplateId*
 24.StackSet-mão*
 25.StackSet-Zona de aterrissagem da AWS
 26.IAMPolicy*
 27.cliente-mc-*
 28.Raiz*
 29.LandingZone*
 30.StateMachine*
 31.codedeploy_service_role
 32.host de gerenciamento
 33.sentinel.int.
 34.eps
 35.UnhealthyInServiceBastion
 36.ms-

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

ID	Padrão técnico
1.0	Duração do tempo limite
1.1	O tempo limite padrão de uma sessão de usuário federado é de uma hora e pode ser aumentado para até quatro horas.

ID	Padrão técnico
1.2	O tempo padrão de acesso à pilha é de 12 horas.
2.0	AWS Uso da conta raiz
2.1	Se houver uso da conta raiz por qualquer motivo, a Amazon GuardDuty deverá ser configurada para gerar descobertas relevantes.
2.2	Para contas de zona de destino de conta única (SALZ) e conta de gerenciamento de zona de destino com várias contas (MALZ) (anteriormente conhecida como Master/Billing conta), a conta de usuário raiz deve ter o MFA virtual ativado e o soft token do MFA é descartado durante a integração da conta, para que nem o AMS nem os clientes possam fazer login como root. O processo padrão de perda da senha AWS raiz deve ser seguido em conjunto com o AMS Cloud Service Delivery Manager (CSDM). Essa configuração deve permanecer durante o ciclo de vida das contas gerenciadas pelo AMS.
2.3	Você não deve criar chaves de acesso para a conta raiz.
3.0	Criação e modificação de usuários
3.1	O IAM users/roles com acesso programático e com permissões somente de leitura pode ser criado sem nenhuma política de tempo limitado. No entanto, a permissão para permitir a leitura de objetos (por exemplo, S3:GetObject) em todos os buckets do Amazon Simple Storage Service na conta não é permitida.

ID	Padrão técnico
3.1.1	Usuários humanos do IAM para acesso ao console e com permissões somente de leitura podem ser criados com a política de limite de tempo (até 180 dias), enquanto a política com limite removal/renewal/extension de tempo resultará na notificação de risco. No entanto, a permissão para permitir a leitura de objetos (por exemplo, S3:GetObject) em todos os buckets do S3 na conta não é permitida.
3.2	Os usuários e funções do IAM para acesso programático e de console com quaisquer permissões que alterem a infraestrutura (gravação e gerenciamento de permissões) na conta do cliente não devem ser criados sem a aceitação do risco. Existem exceções para permissões de gravação em nível de objeto do S3, que são permitidas sem aceitação de riscos, desde que os buckets específicos estejam no escopo e nas operações de marcação em tags não relacionadas ao AMS.
3.3	Usuários do IAM com acesso programático, nomeados <code>customer_servicenow_user</code> e <code>customer_servicenow_logging_user</code> necessários para ServiceNow integração na conta do aplicativo SALZ ou MALZ e nas contas*principais*, podem ser criados sem nenhuma política de tempo limitado.

ID	Padrão técnico
3.4	Os usuários do IAM com acesso programático, uso <code>customer_cloud_endure_policy</code> e <code>customer_cloud_endure_deny_policy</code> (com acesso somente leitura) necessários para CloudEndure integração nas contas SALZ e MALZ podem ser criados, mas precisam de uma política de tempo limitado para o período da migração planejada. O limite de tempo pode ser de um período máximo de 180 dias sem qualquer RA. O SCP também está autorizado a alterar as contas MALZ para permitir que essas políticas funcionem pelo período exigido. Você define janelas de migração apropriadas para suas necessidades e ajusta conforme necessário.
4,0	Políticas, ações e APIs
4.1	Todos os seus usuários e funções do IAM nas contas do SALZ devem ter a Política de Negação do Cliente (CDP) padrão anexada para proteger a infraestrutura do AMS contra danos acidentais ou intencionais.
4.2	O AMS SCPs deve estar habilitado em todas as contas gerenciadas pelo AMS no MALZ.
4.3	Identities capazes de realizar ações administrativas em chaves KMS, como, e <code>PutKeyPolicy</code> <code>ScheduleKeyDeletion</code> , devem ser restritas somente aos operadores e diretores de automação do AMS.

ID	Padrão técnico
4.4	Uma política não deve fornecer acesso ao administrador com uma declaração equivalente a “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*” sem aceitação de risco.
4.5	A política do IAM não deve incluir nenhuma ação que inclua a ação Permitir S3: *** em nenhum bucket sem aceitação de risco.
4.6	As chamadas de API contra políticas de chaves do KMS para chaves de infraestrutura do AMS nas políticas de IAM do cliente não devem ser permitidas.
4.7	Ações que ignoram o processo de gerenciamento de alterações (RFC) não devem ser permitidas, como iniciar ou interromper a instância, criar um bucket do S3 ou instância do RDS e assim por diante.
4.8	Ações que fazem alterações nos registros DNS da infraestrutura do AMS no Amazon Route 53 não devem ser permitidas.
4.9	Usuários humanos do IAM com acesso ao console criado após seguirem o devido processo legal não devem ter nenhuma política anexada diretamente, exceto a política de confiança, a política de assumir funções e a política de limite de tempo.
4.10	Perfis de EC2 instância da Amazon com acesso de leitura a um segredo ou namespace específico AWS Secrets Manager na mesma conta podem ser criados.

ID	Padrão técnico
4.11	As permissões do AWS Managed Services Change Management (AMSCM) ou do AWS Managed Services Service Knowledge Management System (AMSSKMS) podem ser adicionadas a qualquer função (capacidade de abertura). SR/Incident/RFC
4.12	A política do IAM não deve incluir nenhuma ação que inclua a ação Permitir registros: DeleteLogGroup e registros: DeleteLogStream em qualquer grupo de CloudWatch registros do AMS Amazon.
4.13	As permissões para criar chaves multirregionais não devem ser permitidas.
4.14	Para fornecer acesso ao bucket do S3 ARNs que ainda não foi criado em suas contas, use a chave de condição do S3 específica do serviço <code>s3:ResourceAccount</code> para especificar o número da conta.
4.15	Você pode ter acesso de visualização, criação, lista e exclusão ao seu painel personalizado, mas somente acessar e listar nos CloudWatch painéis da Amazon.
4.15.1	Você pode visualizar, criar, listar e excluir o acesso ao painel personalizado da lente de armazenamento do S3.
4.16	Permissões completas relacionadas ao SQL Workbench podem ser concedidas roles/users para trabalhar nos bancos de dados do Amazon Redshift.

ID	Padrão técnico
4.17	Qualquer AWS CloudShell permissão pode ser concedida às funções do cliente como alternativa à CLI.
4.18	Uma função do IAM com um AWS service (Serviço da AWS) diretor confiável também deve estar em conformidade com os padrões técnicos do IAM.
4.19	As funções vinculadas ao serviço (SLRs) não estão sujeitas aos padrões técnicos do AMS IAM, pois são criadas e mantidas pela equipe de serviço do IAM.
4.20	As políticas do IAM não devem permitir acesso de leitura irrestrito aos objetos de bucket do Amazon S3 (por exemplo, Amazon S3GetObject:) em todos os buckets de uma conta: • Nas contas do modo Desenvolvedor: as violações resultam em uma notificação de risco • Em contas do modo não desenvolvedor: violações exigem aceitação de risco
4.21	Todas as permissões do IAM para o tipo de recurso “savingsplan” podem ser concedidas aos clientes.

ID	Padrão técnico
4.22	Os engenheiros do AMS não têm permissão para copiar ou mover dados do cliente (arquivos, objetos do S3, bancos de dados) manualmente em nenhum dos serviços de armazenamento de dados, como Amazon S3, Amazon Relational Database Service, Amazon DynamoDB, etc., nem no sistema de arquivos do sistema operacional.
4.23	A política de SCP não deve ser modificada para permitir qualquer acesso adicional em qualquer conta gerenciada do AMS.
4,24	Quaisquer alterações na política do SCP que possam prejudicar a infraestrutura ou os recursos de gerenciamento do AMS não devem ser permitidas. (Observação: os recursos do AMS têm a tag <code>AppId= AMSInfrastructure</code> e seguem o AMS Protected Namespace).
4,25	O recurso AMS Automated IAM Provisioning deve ser ativado em suas contas como um recurso opcional.
4.26	As funções ou os usuários assumidos por humanos do AMS não devem ter acesso ao conteúdo do cliente no S3, RDS, DynamoDB, Redshift, ElastiCache, EFS e FSx. Além disso, qualquer acesso a um novo e conhecido APIs lançado por terceiros Serviços da AWS que conceda acesso ao conteúdo do cliente deve ser explicitamente negado nas funções de operador.
5.0	Federação

ID	Padrão técnico
5.1	A autenticação deve ser configurada usando a federação na conta gerenciada do AMS.
5.2	Só deve haver confiança de saída unidirecional do AMS AD para seu Active Directory (o AMS AD confia no AD local).
5.3	Seus repositórios de identidade usados para se autenticar no AMS não devem existir nas contas de aplicativos gerenciados pelo AMS.
6.0	Políticas de contas cruzadas
6.1	As funções do IAM, as políticas de confiança entre contas do AMS que pertencem ao mesmo cliente, de acordo com os registros do cliente, podem ser configuradas.
6.2	As políticas de confiança das funções do IAM entre contas AMS e não AMS devem ser configuradas somente se a conta não AMS pertencer ao mesmo cliente do AMS (confirmando que elas estão na mesma AWS Organizations conta ou combinando o domínio de e-mail com o nome da empresa do cliente).
6.3	As políticas de confiança das funções do IAM entre contas do AMS e contas de terceiros não devem ser configuradas sem a aceitação do risco.
6.4	Políticas entre contas para acessar qualquer cliente gerenciado CMKs entre contas AMS do mesmo cliente podem ser configuradas.

ID	Padrão técnico
6.5	Políticas entre contas para acessar qualquer chave KMS em uma conta não AMS por meio de uma conta AMS podem ser configuradas.
6.6	As políticas entre contas para acessar qualquer chave KMS em uma conta AMS por uma conta de terceiros não devem ser permitidas sem a aceitação do risco.
6.6.1	As políticas entre contas para acessar qualquer chave KMS em uma conta AMS por uma conta não AMS só podem ser configuradas se a conta não AMS pertencer ao mesmo cliente do AMS.
6.7	Políticas entre contas para acessar quaisquer dados ou recursos do bucket do S3 em que os dados possam ser armazenados (como Amazon RDS, Amazon DynamoDB ou Amazon Redshift) entre contas AMS do mesmo cliente podem ser configuradas.
6.8	Políticas entre contas para acessar quaisquer dados ou recursos do bucket do S3 em que os dados possam ser armazenados (como Amazon RDS, Amazon DynamoDB ou Amazon Redshift) em uma conta não AMS a partir de uma conta AMS com acesso somente leitura podem ser configuradas.

ID	Padrão técnico
6.9	Políticas entre contas para acessar quaisquer dados ou recursos de bucket do S3 em que os dados possam ser armazenados (como Amazon RDS, Amazon DynamoDB ou Amazon Redshift) com permissões de gravação do AMS para uma conta que não seja do AMS (ou de uma conta que não seja do AMS para AMS) devem ser configuradas somente se a conta não AMS pertencer ao mesmo cliente do AMS (confirmando que eles estão na mesma conta ou combinando com o domínio de e-mail) com AWS Organizations o nome da empresa do cliente).
6.10	Políticas entre contas para acessar quaisquer dados ou recursos do bucket do S3 em que os dados possam ser armazenados (como Amazon RDS, Amazon DynamoDB ou Amazon Redshift) em uma conta de terceiros a partir de uma conta AMS com acesso somente leitura podem ser configuradas.
6.11	Políticas entre contas para acessar quaisquer dados ou recursos do bucket do S3 em que os dados possam ser armazenados (como Amazon RDS, Amazon DynamoDB ou Amazon Redshift) em uma conta de terceiros a partir de uma conta AMS com acesso de gravação não devem ser configuradas.

ID	Padrão técnico
6.12	Políticas entre contas de contas de terceiros para acessar um bucket S3 de um cliente do AMS ou recursos nos quais os dados podem ser armazenados (como Amazon RDS, Amazon DynamoDB ou Amazon Redshift) não devem ser configuradas sem a aceitação do risco.
7.0	User Groups (Grupos de usuários)
7.1	Grupos do IAM com permissões somente de leitura e não mutativas são permitidos.
8.0	Políticas baseadas em recurso
8.1	Os recursos de infraestrutura do AMS devem ser protegidos do gerenciamento por identidade e não autorizadas por meio da anexação de políticas baseadas em recursos.
8.2	Seus recursos devem ser configurados com políticas baseadas em recursos com privilégios mínimos, a menos que você especifique explicitamente uma política diferente.
9.0	Serviços provisionados de autoatendimento (SSPS)
9.1	A função ou política padrão do IAM do AMS (incluindo perfil de instância, SSPS, padrão) não deve ser modificada com ou sem qualquer aceitação de risco. Exceções são permitidas (sem aceitação de risco) para políticas de confiança. A marcação da função, política ou alterações do usuário também é permitida nas funções SSP padrão.

ID	Padrão técnico
9.3	A política SSPS para a função de console do Systems Manager Automation não pode ser anexada a nenhuma função personalizada além da função padrão. Outras políticas de SSPS só devem ser anexadas a funções personalizadas do IAM depois de garantir que a vinculação da política a uma função personalizada não forneça permissões adicionais fora do design pretendido para o serviço SSPS padrão.

AMS-STD-003 - Segurança de rede

A seguir está o controle padrão para 003 - Network Security:

ID	Padrão técnico
	Redes
1,0	Todas as EC2 instâncias devem ser acessadas por SSH ou RDP somente por meio de hosts Bastion, do intervalo VPC CIDR do Bastion Host ou do mesmo intervalo de CIDR VPC da instância.
2,0	O IP elástico em EC2 instâncias é permitido
3.0	O plano de controle AMS e, por extensão, no plano de dados TLS 1.2+ devem ser usados.
4,0	Todo o tráfego de saída deve passar usando a conta IGW ou TGW.
5,0	Um grupo de segurança não deve ter origem como 0.0.0.0/0 na regra de entrada se não

ID	Padrão técnico
	estiver conectado a um balanceador de carga conforme 9.0
6.0	O bucket ou os objetos do S3 não devem ser tornados públicos sem a aceitação do risco.
7.0	O acesso ao gerenciamento de servidores nas portas SSH/22 ou SSH/2222 (não SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 ou 1604, LDAP/389 ou 636 e RPC/135, NETBIOS/137-139 não deve ser permitido de fora da VM VPC por meio de grupos de segurança.
8.0	O acesso ao gerenciamento de banco de dados em portas (MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433) ou em portas personalizadas não deve ser permitido do público, não roteado para VPC sobre DX, VPC-peer ou VPN por meio de um grupo de segurança. IPs
8.1	Qualquer recurso em que os dados do cliente possam ser armazenados não deve ser exposto diretamente à Internet pública.
9.0	O acesso direto a aplicativos pela porta HTTP/80, HTTPS/8443 e HTTPS/443 da Internet é permitido somente para balanceadores de carga, mas não para nenhum recurso de computação diretamente, por exemplo, instâncias, contêineres etc. EC2 ECS/EKS/Fargate

ID	Padrão técnico
10.0	O acesso de aplicativos pelas portas HTTP/80 e HTTPS/443 a partir do intervalo de IP privado do cliente pode ser permitido.
11.0	Quaisquer alterações nos grupos de segurança que controlam o acesso à infraestrutura do AMS não devem ser permitidas sem a aceitação do risco.
12.0	A segurança do AMS se refere aos padrões toda vez que é solicitado que um grupo de segurança seja anexado a uma instância.
13.0	O acesso ao bastião do cliente nas portas 3389 e 22 deve ser permitido somente a partir de intervalos de IP privados que são roteados para a VPC via DX, VPC-peer ou VPN.
14.0	A associação entre contas de zonas hospedadas privadas com contas VPCs de AMS para contas não AMS (ou não AMS para AMS) deve ser configurada somente se a conta não AMS pertencer ao mesmo cliente AMS (confirmando que elas estão na mesma conta da AWS Organization ou combinando o domínio de e-mail com o nome da empresa do cliente) usando ferramentas internas.
15.0	Conexões de emparelhamento de VPC entre contas que pertencem ao mesmo cliente podem ser permitidas.

ID	Padrão técnico
16,0	A base do AMS AMIs pode ser compartilhada com contas que não sejam da AMS, desde que ambas sejam de propriedade do mesmo cliente (confirmando que estão na mesma AWS Organizations conta ou combinando o domínio do e-mail com o nome da empresa do cliente) usando ferramentas internas.
17.0	A porta FTP 21 não deve ser configurada em nenhum grupo de segurança sem a aceitação do risco.
18,0	A conectividade de rede entre contas via gateway de trânsito é permitida, desde que todas as contas sejam de propriedade do cliente.
19,0	Não é permitido transformar uma sub-rede privada em pública
20.0	Conexões de emparelhamento de VPC com contas de terceiros (não pertencentes ao cliente) não devem ser permitidas.
21,0	A vinculação do Transit Gateway a uma conta de terceiros (não pertencente ao cliente) não deve ser permitida.
22,0	Qualquer tráfego de rede necessário para que o AMS forneça os serviços aos clientes não deve ser bloqueado no ponto de saída da rede do cliente.

ID	Padrão técnico
23,0	O compartilhamento de regras do resolvidor com Conta da AWS pertencentes ao mesmo cliente é permitido com uma notificação de risco
19,0	ICMP
19.1	A solicitação de ICMP recebida da infraestrutura EC2 do cliente para a Amazon exigirá uma notificação de risco.
19.2	Solicitações de entrada do público IPs roteadas para a Amazon VPC via DX, VPC-peer ou VPN via grupo de segurança são permitidas.
19.3	Solicitações de entrada de um público IPs não roteado para a Amazon VPC via DX, VPC-peer ou VPN via grupo de segurança exigiram uma aceitação de risco.
19,4	A solicitação ICMP de saída da Amazon EC2 para qualquer destino é permitida.
20,0	Compartilhamento de grupos de segurança
20.1	Se um grupo de segurança atender a esse padrão de segurança, ele poderá ser compartilhado VPCs na mesma conta e entre contas na mesma organização.

ID	Padrão técnico
20.2	Se um grupo de segurança não atender a esse padrão e uma aceitação de risco tiver sido exigida anteriormente para esse grupo de segurança, o uso do recurso de compartilhamento de grupos de segurança entre VPCs a mesma conta ou entre contas na mesma organização não será permitido sem a aceitação do risco para essa nova VPC ou conta.

AMS-STD-004 - Teste de penetração

O seguinte é o controle padrão para 004 - Teste de Penetração

1. O AMS não oferece suporte à infraestrutura de pentest. É responsabilidade do cliente. Por exemplo, o Kali não é uma distribuição Linux compatível com AMS.
2. Os clientes precisam aderir aos [testes de penetração](#).
3. O AMS deve ser pré-notificado com 24 horas de antecedência, caso o cliente deseje realizar testes de penetração de infraestrutura nas contas.
4. A AMS provisionará a infraestrutura de pentesting do cliente de acordo com os requisitos do cliente explicitamente declarados na solicitação de mudança ou solicitação de serviço do cliente.
5. O gerenciamento de identidade da infraestrutura de testes do cliente é de responsabilidade do cliente.

AMS-STD-005 - GuardDuty

O seguinte é o controle padrão para 005 - GuardDuty

1. GuardDuty deve estar habilitado em todas as contas de clientes em todos os momentos.
2. GuardDuty As descobertas da Customer Managed Application Account (CMA) no MALZ não resultarão em alarmes para a equipe de operações.
3. GuardDuty os alertas devem ser armazenados na mesma conta ou em qualquer outra conta gerenciada da mesma organização.

4. O recurso de lista de IP confiável do não GuardDuty deve ser usado. Em vez disso, o arquivamento automático pode ser usado como alternativa, o que é útil para fins de auditoria.
5. GuardDuty a delegação de administrador não deve ser habilitada no MALZ, pois o administrador delegado seria capaz de realizar ações de alto privilégio, como desativá-las GuardDuty em outras contas sem aceitar riscos.
6. GuardDuty Os filtros de arquivamento automático devem usar o escopo mínimo para obter o máximo retorno. Por exemplo, se o AMS ver vários imprevisíveis IPs em diferentes blocos CIDR e houver um ASN corporativo apropriado para uso, use o ASN. No entanto, se você puder reduzir o escopo para intervalos específicos ou endereços /32, defina o escopo para aqueles.

AMS-STD-006 - Segurança do host

A seguir está o controle padrão para 006 - Host Security

- Um agente antivírus deve estar sempre em execução em todas as EC2 instâncias. (por exemplo, Trend Micro DSM).
- O módulo antimalware deve estar ativado.
- O agente EPS deve incluir todos os diretórios e arquivos para digitalização.
- Os arquivos colocados em quarentena pela solução antivírus podem ser compartilhados com você sob demanda.
- Uma solução de segurança de terminais de terceiros não deve ser instalada.
- A frequência de atualização da assinatura de antivírus deve ser definida para pelo menos uma vez por dia.
- A frequência de varredura programada deve ser definida para pelo menos uma vez por mês.
- A verificação em tempo real (ao acessar) deve estar sempre ativada e em execução.
- O AMS não deve executar nenhum script personalizado que não seja de propriedade ou de autoria do AMS em suas instâncias. (Observação: você pode fazer isso usando o acesso de administrador da pilha por meio da CT de acesso de administrador da pilha ou usando a [AWS Systems Manager automação \(AMS SSPS\)](#).
- A Autenticação em Nível de Rede (NLA) não deve ser desativada no host Windows.
- O sistema operacional do host deve estar atualizado com os patches de segurança mais recentes de acordo com o ciclo de patch configurado.
- Uma conta gerenciada do AMS não deve ter uma instância não gerenciada na conta.
- A criação de contas de administrador local em sua instância pelo AMS não deve ser permitida.

- O par de chaves EC2 ativado não deve ser criado.
- Você não deve usar sistemas operacionais declarados como Fim da Vida Útil (EOL) e que não haja mais suporte de segurança fornecido pelo fornecedor ou por terceiros.

AMS-STD-007 - Registro

O seguinte é o controle padrão para 007 - Logging

ID	Padrão técnico
1.0	Tipos de registro
1.1	Registros do sistema operacional: todos os hosts devem registrar eventos mínimos de autenticação do host, eventos de acesso para todos os usos de privilégios elevados e eventos de acesso para todas as alterações no acesso e na configuração de privilégios, incluindo sucesso e falha.
1.2	AWS CloudTrail: o registro CloudTrail de eventos de gerenciamento deve ser ativado e configurado para entregar os registros a um bucket do S3.
1.3	Registros de fluxo de VPC: todos os registros de tráfego de rede devem ser registrados por meio de registros de fluxo de VPC.
1.4	Registro de acesso ao servidor Amazon S3: os buckets S3 obrigatórios do AMS que armazenam registros devem ter o registro de acesso ao servidor ativado.
1.5	AWS Config Snapshots: AWS Config devem registrar as alterações de configuração de todos os recursos suportados em todas as regiões e entregar os arquivos de instantâneos

ID	Padrão técnico
	de configuração aos buckets do S3 pelo menos uma vez por dia.
1.6	Registros do Endpoint Protection System (EPS): o registro da solução EPS deve estar ativado e configurado para entregar os registros a um grupo de CloudWatch registros de registros.
1,7	Registros de aplicativos: os clientes têm o poder de ativar o login em seus aplicativos e armazená-los no grupo de registros de CloudWatch registros ou em um bucket do S3.
1.8	Registro em nível de objeto do S3: os clientes têm o poder de ativar o registro em nível de objeto em seus buckets do S3.
1.9	Registro de serviços: os clientes têm o poder de habilitar e encaminhar registros para serviços SSPS como qualquer serviço principal .
1.10	Registros do Elastic Load Balancing (Classic/ Application Load Balancer/NetworkLoad Balancer): as entradas de registro de acesso e erro devem ser armazenadas nos buckets S3 gerenciados pelo AMS 2.0.
2.0	Controle de acesso
2.1	Você não deve ter acesso de gravação ou exclusão nos buckets do S3 exigidos pelo AMS que armazenam registros e grupos de CloudWatch registros;.

ID	Padrão técnico
2.2	Você deve ter acesso somente para leitura a todos os registros em suas contas.
2.3	Os buckets S3 exigidos pela AMS que armazenam registros não devem permitir usuários de contas de terceiros como princípios nas políticas do bucket.
2.4	Os registros dos grupos de CloudWatch registros do Logs não devem ser excluídos sem a aprovação explícita do seu contato de segurança autorizado.
3.0	Retenção de registros
3.1	Os grupos de registros de CloudWatch registros exigidos pela AMS devem ter um período mínimo de retenção de 90 dias nos registros.
3.2	Os buckets S3 exigidos pela AMS que armazenam os registros devem ter um período mínimo de retenção de 18 meses nos registros.
3.3	AWS Backup os instantâneos devem estar disponíveis com retenção mínima de 31 dias nos recursos suportados.
4,0	Criptografia
4.1	A criptografia deve estar habilitada em todos os buckets do S3 exigidos pelas equipes do AMS que armazenam registros.
4.2	Qualquer encaminhamento de registros de contas de clientes para qualquer outra conta deve ser criptografado.

ID	Padrão técnico
5.0	Integridade
5.1	O mecanismo de integridade do arquivo de log deve estar ativado. A “validação do arquivo de log” deve ser configurada nas AWS CloudTrail trilhas exigidas pelas equipes do AMS.
6.0	Encaminhamento de registros
6.1	Qualquer registro pode ser encaminhado de uma conta AMS para outra conta AMS do mesmo cliente.
6.2	Qualquer registro pode ser encaminhado do AMS para uma conta não AMS somente se a conta não AMS for de propriedade do mesmo cliente do AMS.
6.3	Quaisquer registros de uma conta de cliente não devem ser encaminhados para uma conta de terceiros (que não seja de propriedade do cliente).

AMS-STD-008 - AMS-MAD

O seguinte é o controle padrão para 008 - AMS-MAD

ID	Padrão técnico
1.0	Gerenciamento de acesso
1.1	Somente usuários privilegiados do AMS com logins interativos e tarefas de automação devem ter permissão para fazer login no host de gerenciamento para administrar o AD gerenciado nas contas dos clientes.

ID	Padrão técnico
1.2	Os administradores do AD só devem ter privilégios de administrador delegado (Grupo de Administradores Delegados do AMS).
1.3	Os engenheiros que fazem login nos ambientes AD do cliente (host de gerenciamento ou instâncias) devem ter acesso com limite de tempo.
1.4	Os clientes têm acesso somente de leitura aos objetos do AD usando o Remote Server Administrator Tools em uma EC2 instância.
1.5	Os direitos administrativos para o usuário ou grupo do Active Directory não devem ser permitidos.
1.6	AWS O compartilhamento de diretórios com pessoas Conta da AWS pertencentes ao mesmo cliente é permitido com uma notificação de risco.
2.0	Contas de serviço
2.1	As contas de serviço gerenciadas em grupo (gMSA) devem ser usadas sempre que suportadas pelos aplicativos, em vez da conta de serviço padrão.
2.2	Todas as outras contas de serviço devem ser criadas após o processo de aceitação do risco.

ID	Padrão técnico
2.3	Os grupos de segurança do AD não devem ser reutilizados, a menos que sejam explicitamente solicitados pelo cliente. Novos grupos do AD devem ser criados. Objetos de computador que solicitam acesso à conta de serviço devem ser adicionados ao novo grupo de segurança.
2.4	Qualquer conta de serviço gMSA deve ser adicionada à Unidade Organizacional (OU) “Conta de Serviço Gerenciada”.
2,5	Qualquer conta de serviço que não seja GMSA deve ser adicionada na OU “Usuários → Contas de serviço”.
3.0	Objetos de política de grupo (GPO)
3.1	Qualquer configuração no GPO “Configurações do Windows > Configurações de segurança” não deve ser modificada se reduzir a postura de segurança da conta de alguma forma em relação ao estado atual.
3.2	No MALZ, RFCs enviado de uma conta de aplicativo solicitando a criação de um GPO, o GPO deve estar vinculado à OU que corresponde à conta do aplicativo. Qualquer GPOs coisa que afete todas as contas deve ser da conta do Shared Service.
3.3	O tempo limite padrão da sessão RDP Idle deve ser definido como 15 minutos para todos os servidores no domínio do Active Directory.
4,0	Confiança do Active Direc

ID	Padrão técnico
4.1	A confiança de saída unidirecional (diretório o hospedado em AMS para diretório de clientes) é IPs permitida se os encaminhadores condicionais forem roteados para a VPC via DX, VPC-peer ou VPN.
5.0	Outros
5.1	O mecanismo de integridade do arquivo de log deve estar ativado. A “validação do arquivo de log” deve ser configurada nas AWS CloudTrail trilhas exigidas pelas equipes do AMS.
6.0	Encaminhamento de registros
6.1	Usuários, grupos, objetos de computador, UO ou outras entidades do cliente não devem usar a convenção de nomenclatura do AMS de acordo com a convenção de nomenclatura do AMS.
6.2	Tudo isso OUs deve ser gerenciado pelo AMS.

AMS-STD-009 - Diversos

O seguinte é o controle padrão para 009 - Diversos

- Se a criptografia estiver ativada em um recurso, objeto, banco de dados ou sistema de arquivos, ela não deverá ser desativada.

Alterações que introduzem riscos de segurança altos ou muito altos em seu ambiente

As alterações a seguir introduzem riscos de segurança altos ou muito altos em seu ambiente:

AWS Identity and Access Management

- High_Risk-IAM-001: Crie chaves de acesso para a conta root
- High_Risk-IAM-002: modificação da política de SCP para permitir acesso adicional
- High_Risk-IAM-003: Modificação da política de SCP que pode quebrar a infraestrutura do AMS
- High_Risk-IAM-004: Criação de um role/user com permissões de mutação de infraestrutura (gravação, gerenciamento de permissões ou marcação) na conta do cliente
- High_Risk-IAM-005: as funções do IAM confiam nas políticas entre contas do AMS e contas de terceiros (não pertencentes ao cliente)
- High_Risk-IAM-006: políticas entre contas para acessar qualquer chave KMS de uma conta AMS por uma conta de terceiros)
- High_Risk-IAM-007: políticas entre contas de terceiros para acessar um bucket S3 de um cliente AMS ou recursos nos quais os dados podem ser armazenados (como Amazon RDS, Amazon DynamoDB ou Amazon Redshift)
- High_Risk-IAM-008: atribua as permissões do IAM com qualquer permissão de mutação de infraestrutura na conta do cliente
- High_Risk-IAM-009: Permitir a listagem e a leitura de todos os buckets S3 na conta
- High_Risk-IAM-010: Provisionamento automatizado de IAM com permissões read/write

Segurança de rede

- High_Risk-Net-001: portas abertas de gerenciamento de sistema operacional SSH/22 ou SSH/2222 (não SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/ CITRIX/1494 ou 1604, LDAP/389 ou 636 e NETBIOS/137-139 da Internet
- High_Risk-Net-002: Abra as portas de gerenciamento de banco de dados MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433 ou qualquer porta de gerenciamento do cliente a partir da Internet
- High_Risk-Net-003: abra as portas do aplicativo HTTP/80, HTTPS/8443 e HTTPS/443 diretamente em qualquer recurso computacional. Por exemplo, EC2 instâncias, ECS/EKS/Fargate contêineres etc. da Internet
- High_Risk-Net-004: Qualquer alteração nos grupos de segurança que controlam o acesso à infraestrutura do AMS
- High_Risk-Net-006: emparelhamento de VPC com a conta de terceiros (não de propriedade do cliente)
- High_Risk-Net-007: Adicionando o firewall do cliente como ponto de saída para todo o tráfego do AMS

- High_Risk-Net-008: A conexão do Transit Gateway com a conta de terceiros não é permitida
- High_Risk-S3-001: Provisione ou habilite o acesso público no bucket do S3

Registro em log

- High_Risk-log-001: Desativar. CloudTrail (É necessária a aprovação do gerente do site de operações)
- High_risk-log-002: desative os registros de fluxo da VPC. (É necessária a aprovação do gerente do site de operações)
- High_risk-log-003: encaminhamento de registros por meio de qualquer método (notificação de evento do S3, extração do agente SIEM, envio do agente do SIEM etc.) de uma conta gerenciada do AMS para uma conta de terceiros (não pertencente ao cliente)
- High_Risk-log-004: Use uma trilha não AMS para CloudTrail

Segurança do host

- High_Risk-Host-001: Desative o End Point Security na conta por qualquer motivo. (É necessária a aprovação do gerente do site de operações)
- High_risk-host-002: desative a aplicação de patches em um recurso ou no nível da conta.
- High_risk-host-003: implantação de uma instância não gerenciada na conta. EC2
- High_Risk-Host-004: Executando um script personalizado fornecido pelo cliente.
- High_risk-host-005: criação de contas de administrador local em instâncias.
- High_Risk-Host-006: exclusões de escaneamento de tipo de arquivo/extensão do Trend Micro EPS ou desativação da proteção contra malware em endpoints.

Note

A aceitação do risco não é necessária para exclusões antimalware do EPS ou regras de GuardDuty supressão relacionadas a testes de penetração, escaneamentos de vulnerabilidade ou problemas de desempenho que afetam events/known o serviço, garantindo ações proativas. Uma notificação de risco é suficiente nessas situações.

- High_Risk-Host-007: Criar para KeyPair EC2
- High_Risk-Host-008: Desative a segurança do endpoint no EC2
- High_Risk-Host-009: Contas usando o sistema operacional End of Life (EOL)

Diversos

- High_Risk-ENC-001: Desative a criptografia em qualquer recurso se ela estiver ativada

Active Directory gerenciado

- High_Risk-AD-001: Forneça direitos de administrador ao usuário ou grupo do Active Director
- High_Risk-AD-002: Políticas de GPO capazes de reduzir a postura de segurança da conta

Gerenciamento de continuidade no AMS Advanced

Como parte do gerenciamento de continuidade, o AWS Managed Services (AMS) fornece acesso automatizado a AWS Backup um serviço nativo com AWS. Isso facilita o acesso a um serviço compatível com Amazon EBS, Amazon, EC2 Amazon RDS, Amazon EFS e muito mais.

Para saber mais, consulte [AWS Backup: Como funciona](#).

Tópicos

- [O que é gerenciamento de continuidade?](#)
- [Como funciona o gerenciamento de continuidade](#)
- [Resposta de recuperação de desast](#)
- [planejamento de recuperação de desastres](#)

O que é gerenciamento de continuidade?

O gerenciamento de continuidade é o processo que o AMS usa para fornecer backups e instantâneos para sua conta.

O AMS fornece acesso aos AWS Backup tipos de alteração que você usa para criar e gerenciar tarefas e planos de backup.

Como funciona o gerenciamento de continuidade

O AMS usa [AWS Backup](#) para gerenciamento de continuidade.

Ao começar a trabalhar com o AWS Backup AMS:

1. Execute um backup sob demanda
2. Crie um plano de backup (opcional, o AMS fornece planos de backup padrão)
3. Use o AMS padrão como cofres de backup (opcional)
4. Gerencie (execute, refine, exclua e assim por diante) seus planos de backup e pontos de recuperação

Planos de backup do AMS

Um plano de backup é uma expressão de política que define quando e como você deseja fazer backup de recursos compatíveis da AWS, como bancos de dados do RDS, volumes do EBS, tabelas do DynamoDB e sistemas de arquivos EFS. As políticas de agendamento e retenção são gerenciadas por meio de planos de backup personalizados, que você pode criar usando um tipo de alteração (CT) com o AMS Advanced ou usando AWS Backup com o AMS Accelerate. Atribua recursos aos seus planos de backup usando tags e AWS Backup automaticamente faz backup e retém backups dos recursos atribuídos de acordo com o plano de backup definido. Você poderá criar vários planos de backup se tiver cargas de trabalho com diferentes requisitos de backup.

Um plano de backup pode ter até seis regras de backup que definem um cronograma e um período de retenção, entre outros detalhes. O agendamento de backup determina quando AWS Backup inicia uma tarefa de backup e com que frequência um backup é criado. Você pode escolher uma frequência horária, diária, semanal ou mensal. A configuração de dias de exclusão determina quantos dias o instantâneo é armazenado antes de ser excluído automaticamente.

Note

AMS Advanced: Se você for migrado do sistema de backup antigo do AMS, o AMS criará um plano de backup padrão para compatibilidade com versões anteriores. O par chave-valor nesse cenário é Backup:True. Para oferecer suporte à compatibilidade com versões anteriores, o valor aqui não diferencia maiúsculas de minúsculas, então Backup:True ou Backup:True são todas tags válidas. Todos os outros pares de chave-valor diferenciam maiúsculas de minúsculas.

AWS Backup pode operar no nível do volume do EBS ou no nível da EC2 instância da Amazon, mas não faça as duas coisas ao mesmo tempo, pois isso pode levar a uma condição de corrida em que os backups podem entrar em conflito.

Planos de backup padrão, landing zone com várias contas

Durante a nova RFC de criação de conta, o AMS garante que haja um plano de backup padrão abrangente no nível da conta para proteger suas cargas de trabalho. Os valores dos campos obrigatórios são definidos por padrão, conforme mostrado na seção a seguir:

Plano de backup padrão do AMS

default-backup-plan

Chave TAG: Backup

Valor da TAG: True

```

RuleForDailyBackups schedule expression: cron(30 23 ? * *) (a daily backup for 23:30
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(30 23 ? * 7 *) (a weekly backup for
23:30 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(30 23 * ? *) (a monthly backup for
23:30 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(30 23 1 1 ? *) (a yearly backup for
23:30 UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years

```

Plano de backup padrão do AMS	Horário de início do cluster	Retenção
backup de hora em hora	N/D	N/D
backup diário	diariamente às 23:30 UTC	7 dias
backup semanal	semanalmente às 23:30 UTC, somente no sábado	4 semanas
backup mensal	mensalmente às 23:30 UTC, no dia 1 do mês	26 semanas
backup anual	23:30 UTC, no dia 1 do mês	2 anos

Plano de backup padrão aprimorado do AMS

Esse plano é um modelo das AWS Backup melhores práticas de proteção contra ataques de ransomware. Ele implementa uma estratégia de backup diária, semanal, mensal e anual. AWS Backup o [backup contínuo](#) é ativado com retenção máxima (31 dias) [dos recursos suportados](#).

ams-enhanced-default-backup-plano

Chave TAG: backup-orchestrator-enhanced

Valor da TAG: true

```
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForDailyBackups continuous backup: true
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Plano de backup aprimorado do AMS	Horário de início do cluster	Retenção
backup de hora em hora	N/D	N/D
backup diário	diariamente 4:00 UTC	31 dias
backup semanal	Sábado, 2:00 UTC	6 semanas
backup mensal	1º dia do mês, 2:00 UTC	26 semanas
backup anual	1º de janeiro, 2:00 UTC	2 anos

Plano de backup AMS sensível a dados

Esse plano é um modelo das melhores práticas de backup do AWS para proteção contra ataques de ransomware em aplicativos sensíveis a dados. Ele implementa uma estratégia de backup por hora, diária, semanal, mensal e anual. O backup [contínuo do AWS Backup](#) é habilitado com retenção máxima (31 dias) nos [recursos suportados](#).

ams-data-sensitive-backup-plano

Chave TAG: backup-orchestrator-data-sensitive

Valor da TAG: true

```

RuleForHourlyBackups schedule expression: cron(0 * ? * * *) (an hourly backup at the
hour mark)
RuleForHourlyBackups delete after days: 7 days
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years

```

Plano de backup AMS sensível a dados	Horário de início do cluster	Retenção
backup de hora em hora	na marca da hora	7 dias
backup diário	diariamente 4:00 UTC	31 dias
backup semanal	Sábado, 2:00 UTC	6 semanas
backup mensal	1º dia do mês, 2:00 UTC	26 semanas
backup anual	1º de janeiro, 2:00 UTC	2 anos

Cofres de backup do AMS

AWS Backup organiza os instantâneos em unidades lógicas de armazenamento chamadas cofres.

Você pode controlar as notificações do cofre de backup em nível individual do cofre usando tags. Você pode desativar as notificações de um cofre específico adicionando a tag `AMSNotificationOptOut` e definindo o valor `True` em um cofre específico. Para continuar recebendo notificações do cofre, remova a tag.

Para ver uma lista dos seus backups do AMS, abra o [AWS Backup console](#). No painel de navegação, escolha Cofres de backup e selecione um dos cofres de backup do AMS nas tabelas

a seguir. Na seção Backups, veja a lista de todos os backups no cofre de backup. Selecione um backup para editar, excluir ou restaurar.

Cofres para planos de backup do AMS

Nome do AMS Vault	Descrição
ams-automated-backups	Esse cofre recebe todos os pontos de recuperação obtidos pelo AWS Backup plano default-backup-plan padrão do AMS Advanced.
ams-automated-enhanced-backups	Esse cofre recebe todos os pontos de recuperação obtidos pelo AWS Backup plano ams-enhanced-default-backup padrão avançado do AMS Advanced.
ams-automated-data-sensitive-backups	Esse cofre recebe todos os pontos de recuperação obtidos pelo plano e AWS Backup plano ams-data-sensitive-backup AMS Advanced.
ams-manual-backups	Esse é o local padrão para todos os backups dos planos de backup Start Backup Job RFC (ct-2hhud2lx01tq7), se nenhum nome de cofre for definido.
ams-custom-backups	Esse é o local padrão para os instantâneos que o AMS tira antes de aplicar patches em uma instância usando o Patch Orchestrator ou as atividades mensais de patch. Eles são removidos automaticamente de acordo com a política padrão do ciclo de vida do patch do AMS de 60 dias.

Tipos de alteração de backup do AMS

O AMS fornece vários CTs para você criar e usar planos de backup.

 Important

Não edite seus planos de backup padrão do AMS, pois suas alterações podem ser perdidas. Em vez disso, crie novos planos para suas configurações personalizadas.

- [Plano de backup: Criar](#)
- [Backup Job: Iniciar](#)
- [Trabalho de Backup: Parar](#)
- [Ponto de recuperação: Excluir](#)
- [DynamoDB | Crie a partir do Backup](#)
- [Volume do EBS: criar a partir do backup](#)
- [Amazon Elastic File System \(EFS\): crie a partir do backup](#)

Monitoramento e relatórios de backup do AMS

 Important

O monitoramento e a emissão de relatórios de backup do AMS só estão disponíveis nas regiões suportadas pelo AMS. São 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), UE (Paris), Ásia-Pacífico (Mumbai), Ásia-Pacífico (Seul), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Sydney), Ásia-Pacífico (Sydney), Ásia-Pacífico (Sydney) Tóquio).

O AMS gera relatórios diários de autoatendimento, bem como relatórios mensais sobre a cobertura dos recursos e o status do trabalho de backup. Os relatórios mensais são compartilhados em Monthly Business Reviews (MBRs). Para saber mais sobre relatórios diários de backup, consulte Relatório de [diário de backup](#).

Os especialistas em AMS monitoram todas as suas tarefas de backup que são configuradas usando AWS Backup. Em caso de falhas de backup, o AMS investiga a falha e notifica você com a causa raiz e as opções de remediação, se disponíveis. Para evitar ruídos de alerta, durante eventos que causam um grande número de falhas de backup em suas contas, o AMS faz uma recomendação coletiva, por meio de seu CSDM, em vez de notificá-lo sobre cada falha individual.

Observe que o AMS não monitora nenhum backup configurado usando o recurso de backup independente de um AWS serviço.

Resposta de recuperação de desast

Além das opções descritas nas seções a seguir, é bom que você saiba quais etapas devem ser tomadas para iniciar uma recuperação de desastres (DR) com o AMS.

Se você enfrentar um desastre e precisar iniciar uma recuperação, siga estas diretrizes gerais:

1. Abra um incidente de alta prioridade com a categoria Disponibilidade. O AMS abrirá uma ponte de conferência e convidará sua equipe a participar.
2. Conheça a lista de recursos que você precisa recuperar.
3. Conheça a landing zone (LZ) de destino para a qual você precisa se recuperar (por exemplo, a mesma conta, uma AZ diferente ou uma conta diferente e uma região diferente).
4. Envie solicitações de recuperação para cada recurso na landing zone de destino. Siga seu plano de DR existente ou veja as opções na seção a seguir (por exemplo [Proteção contra desastres EC2 com instantâneos do EBS no AMS](#), ou [Proteção contra desastres EC2 com Elastic Disaster Recovery no AMS](#)).
5. Restaure a funcionalidade do aplicativo e use a assistência do AMS para solucionar problemas relacionados à infraestrutura.

O AMS pode ajudá-lo a se preparar para esse evento e a criar um plano de DR para sua organização para cobrir essas questões. Para obter mais detalhes, entre em contato com seu gerente de prestação de serviços em nuvem (CSDM) ou arquiteto de nuvem (CA).

planejamento de recuperação de desastres

A recuperação de desastres (DR) é um serviço essencial para a continuidade e conformidade dos negócios corporativos. O AMS faz parceria com você para ajudá-lo a planejar, implementar e manter sua estratégia de DR no AMS.

O AMS landing zone (LZ), com várias contas e conta única, fornece alta disponibilidade nativa, multi-AZ e de alta disponibilidade para componentes de infraestrutura do AMS que atendem à maioria dos cenários de proteção contra desastres. No entanto, dependendo da cobertura geográfica da sua empresa, você pode precisar de proteção regional. Para disponibilidade entre regiões e DR, outra

conta AMS é necessária em uma região diferente (isso vale tanto para a landing zone com várias contas quanto para a landing zone com uma única conta).

O AMS se alinha à orientação de DR da AWS, conforme descrito neste blog, [Recupere rapidamente sistemas de missão crítica em um desastre](#) e oferece suporte às quatro opções a seguir:

- Vários sites (ou altamente disponíveis)
- Espera quente
- Luz piloto
- Backup e restauração

Essas opções e o suporte do AMS para elas são descritos nas seções a seguir.

Vários sites ou de alta disponibilidade (HA)

A solução de alta disponibilidade geralmente é fornecida pela funcionalidade integrada do aplicativo, como clustering ou replicação síncrona. Os usuários são direcionados tanto para o Prod quanto para os HA/DR nós. O DNS aponta diretamente para os nós ou por meio de um balanceador de carga elástico (ELB).

Seu arquiteto de nuvem (CA) do AMS trabalhará com você como parte de seu planejamento Well-Architected-Review e de DR.

O HA DR utiliza serviços e recursos AWS de aplicativos e nativos, conforme ilustrado no gráfico a seguir:

O site de DR pode estar no mesmo local ou em um local diferente Região da AWS.

Note

Uma região diferente (entre regiões) terá um ambiente diferente do Active Directory.

Etapas de DR (failover): Failover automático, nenhuma etapa manual é necessária. Em caso de falha na LZ primária, os usuários serão automaticamente redirecionados para o nó. DR/HA Isso é obtido tanto pelo DNS quanto pela configuração do aplicativo.

Métricas HA DR:

- Objetivo de ponto de recuperação (RPO): <5 min
- Objetivo de tempo de recuperação e (RTO): <5 min
- Manutenção: Alta (mudanças síncronas são necessárias em ambos os ambientes, como configuração de aplicativos, aplicação de patches, SG ou ALB, certificados etc.).
- Custo: Alto

Standby passivo

O termo “espera quente” é usado para descrever um cenário de recuperação de desastres (DR) no qual uma versão reduzida do ambiente está sendo executada na nuvem.

A replicação de dados é feita pela camada de aplicativo, geralmente de forma assíncrona, para uma instância on-line, enquanto o restante das instâncias (por exemplo, camada de aplicativo e Web) pode ser desativada para reduzir o custo. Os usuários são direcionados somente para o site de produção. Outros AWS recursos, como o elastic load balancer (ELB), também podem ser pré-provisionados no site de DR.

Seu arquiteto de nuvem (CA) do AMS trabalhará com você como parte de seu planejamento Well-Architected-Review e de DR.

O Warm Standby DR utiliza serviços e recursos AWS de aplicativos e nativos, conforme ilustrado no gráfico a seguir:

O site de DR pode ser igual ou diferente Região da AWS.

Note

Uma região diferente (entre regiões) terá um ambiente diferente do Active Directory.

Etapas de DR (failover):

1. Freie a replicação de dados e torne a instância de dados no site de DR a principal
2. Atualize a configuração do aplicativo conforme necessário (novo IP, nome do servidor etc.)
3. Redirecione o DNS para o site de DR (ELB)

4. Dependências do AD, se necessário (contas de serviço SPNs, GPOs, etc.)

Métricas HA DR:

- Objetivo de ponto de recuperação (RPO): <1 hora
- Objetivo de tempo de recuperação e (RTO): <1 hora (depende do número de instâncias e da orquestração)
- Manutenção: alta (mudanças síncronas são necessárias em ambos os ambientes, como configuração de aplicativos, aplicação de patches, grupos de segurança (SG) ou balanceador de carga de aplicativos (ALB), certificados etc.).
- Custo: Médio

Luz piloto

Nessa abordagem de recuperação de desastres (DR), você replica parte do seu ambiente Prod para um conjunto limitado de serviços principais. Uma pequena parte da sua infraestrutura está sempre em execução, sincronizando simultaneamente dados mutáveis (como bancos de dados ou documentos), enquanto outras partes da sua infraestrutura são desligadas e usadas somente durante o teste. Ao contrário de uma abordagem de backup e recuperação, você deve garantir que seus elementos principais mais críticos já estejam configurados e funcionando na zona de pouso do DR (a luz piloto).

Seu arquiteto de nuvem do AMS trabalhará com você como parte de seu planejamento Well-Architected-Review e de DR.

O Pilot Light DR utiliza serviços e recursos AWS de aplicativos e nativos, conforme ilustrado no gráfico a seguir:

O site de DR pode ser igual ou diferente Região da AWS.

Note

Uma região diferente (entre regiões) terá um ambiente diferente do Active Directory.

Etapas de DR (failover):

1. Freie a replicação de dados e torne a instância de dados no site de DR a principal
2. Inicie as instâncias e a infraestrutura desativadas
3. Atualize a configuração do aplicativo conforme necessário (novo IP, nome do servidor etc.)
4. Adicione as instâncias ao ELB conforme necessário
5. Redirecione o DNS para o site de DR (ELB)
6. Dependências do AD, se necessário (contas de serviço SPNs, GPOs, etc.)

Métricas de DR do Pilot Light:

- Objetivo de ponto de recuperação (RPO): <1 hora
- Objetivo de tempo de recuperação e (RTO): aproximadamente 1 hora (depende do número de instâncias e da orquestração)
- Manutenção: Média
- Custo: Médio

Backup e restauração

Essa abordagem de recuperação de desastres (DR) simples e de baixo custo faz backup de seus dados e aplicativos de qualquer lugar na landing zone de DR para uso durante a recuperação de um desastre.

Seu arquiteto de nuvem do AMS trabalha com você como parte de seu planejamento de Backup e DR.

O Backup and Restore DR utiliza ferramentas e processos automatizados do AMS, conforme ilustrado no gráfico a seguir:

Dois métodos de backup e replicação podem ser usados:

- Snapshot do EBS (objetivo de ponto de recuperação (RPO) > 1 hora), conhecido como “EBS”
- AWS Elastic Disaster Recovery (Recovery Point Objective (RPO) ~ 0,25 horas), conhecido como “DRS”

O site de DR pode estar no mesmo local ou em outra Região da AWS.

 Note

Uma região diferente (entre regiões) tem um ambiente diferente do Active Directory.

Etapas de DR (failover):

1. Restaure as instâncias a partir de instantâneos (processo em duas etapas com a instância de espaço reservado primeiro)
2. Atualizar a configuração do aplicativo (novo IP, nome do servidor etc.)
3. Configure outra infraestrutura conforme necessário (SG, ELB e assim por diante)
4. Redirecione o DNS para o site de DR (ELB)
5. Atualize ou restaure dependências do AD, se necessário (contas de serviço, nomes principais de serviço (SPNs), objetos de política de grupo (GPOs) e assim por diante)

Métricas de DR de backup e restauração:

- Objetivo de ponto de recuperação (RPO): >1 hora ou ~0,25 horas (depende da solução selecionada - EBS ou DRE)
- Objetivo de tempo de recuperação e (RTO): aproximadamente 1 hora (depende do número de instâncias e da orquestração)
- Manutenção: Alta (mudanças síncronas são necessárias em ambos os ambientes, como configuração de aplicativos, patches, grupos de segurança ou balanceadores de carga de aplicativos, certificados e assim por diante).
- Custo: Médio

Proteção contra desastres EC2 com instantâneos do EBS no AMS

Pré-requisitos:

- Zona de pouso do AMS Prod (fonte)
- Zona de pouso do AMS DR (alvo de DR)
- Os snapshots do EBS estão habilitados para EC2 instâncias (AWS Backup)

Solução de replicação de instantâneos:

- Cross AZ: Não aplicável - os snapshots do EBS estão altamente disponíveis na região por design
- Entre regiões: AWS Backup

O diagrama a seguir representa o processo de EC2 restauração dos snapshots do EBS no AMS:

EC2 Etapas de DR no AMS:

1. Crie um RFC para compartilhar os snapshots do EBS com a conta de destino (necessário para DR entre regiões).

: Gerenciamento, componentes avançados de pilha, EBS Snapshot, compartilhamento

2. Crie uma pilha EC2 AMS de espaço reservado na sub-rede de destino (sub-rede do site de DR). A recomendação é usar a ingestão de CFN para criar a pilha, pois o cliente pode combinar as etapas de atribuição de grupos de segurança e outras (como adicionar a instância a um ELB) na mesma pilha.

Tipo de alteração: implantação, ingestão, empilhamento a partir do CloudFormation modelo, criação

3. Eleve um RFC para realizar a restauração do volume da EC2 pilha.

Tipo de alteração: gerenciamento, componentes avançados da pilha, pilha de EC2 instâncias, volumes de restauração.

O CT restaura os volumes dos instantâneos compartilhados na etapa 1 e se conecta à instância de espaço reservado criada na etapa 2.

Funcionalidade de CT de restauração de volume:

- Encerrar a instância de espaço reservado
- Restaure volumes a partir dos instantâneos
- Troque os volumes
- Inicie a instância
- Sair do domínio antigo
- Alterar o nome do host

- Reinicializar. Os scripts de bootstrap do AMS unem a instância ao domínio de destino (DR) na inicialização

Entrada CT de restauração de volume:

- InstanceId (ID da instância de espaço reservado)
- RootDeviceSnapshotId, o snapshot do EBS para o volume raiz restaurado
- KMSKeyId, o identificador da chave KMS, ou ARN, para criptografar todos os volumes restaurados na instância EC2
- DeviceNames, até 25 (opcional)
- SnapshotIds, até 25 (opcional). Lista de instantâneos dos volumes a serem restaurados

Proteção contra desastres EC2 com Elastic Disaster Recovery no AMS

Pré-requisitos:

- Zona de pouso do AMS Prod (fonte)
- Zona de pouso do AMS DR (alvo de DR)
- Você deve primeiro inicializar o serviço Elastic Disaster Recovery para tudo em Regiões da AWS que planeja usá-lo.

Crie uma função do IAM em sua landing zone (LZ) de DR para acessar o console do Elastic Disaster Recovery.

- Importante: um documento SSM é criado como uma ação pós-lançamento no DRS. Essa ação deve estar ativada em todos os seus servidores nas PostLaunch configurações.
- a instância de destino (espaço reservado) deve ter uma chave de tag: "AWSDRS", value:"AllowLaunchingIntoThisInstance". A instância de espaço reservado deve estar no estado interrompido. Caso contrário, o AMS não poderá selecionar a instância de espaço reservado nas configurações de execução e o Elastic Disaster Recovery não poderá restaurar sobre a instância de espaço reservado.

Para obter um diagrama do processo de configuração e restauração do Elastic Disaster Recovery EC2 no AMS, consulte [Arquitetura geral AWS Elastic Disaster Recovery \(AWS DRS\)](#).

EC2 Etapas de DR com Elastic Disaster Recovery no AMS:

1. Crie uma pilha EC2 AMS de espaço reservado na sub-rede de destino (sub-rede do site de DR) com as tags adequadas. Para obter mais informações, consulte a seção anterior. Recomendamos usar a ingestão de CFN para criar a pilha, pois você pode combinar as etapas de atribuição de grupos de segurança e marcação da instância, do volume do EBS e outros (como adicionar a instância a um ELB) na mesma pilha.

Tipo de alteração: implantação, ingestão, empilhamento a partir do CloudFormation modelo, criação

2. Pare a instância de espaço reservado.

Tipo de alteração: gerenciamento, componentes avançados da pilha, EC2 instância, parada

3. Se não for feito na etapa 1, marque a instância de espaço reservado e seu volume do EBS com a chave: "AWSDRS", valor: ""AllowLaunchingIntoThisInstance".

Tipo de alteração: Gerenciamento, Componentes avançados da pilha, Tag, Atualização.

4. Use a instância de espaço reservado da etapa 1 como destino em Iniciar na ID da instância, Configurações de inicialização do DRS para o servidor de origem. Inicie o treinamento de recuperação de instâncias a partir do console do Elastic Disaster Recovery para o servidor de origem.

Note

Os volumes da instância de espaço reservado são retidos na conta. Para excluir esses volumes, envie um item Gerenciamento | Componentes avançados da pilha | Volume do EBS | Excluir tipo de alteração (ct-3e3h8u0sp5z80) ao final da operação de recuperação de desastres.

Fluxo de trabalho do Elastic Disaster Recovery

- A instância de destino (espaço reservado) precisa estar no estado interrompido
- Troque os volumes e exclua o volume raiz de origem (espaço reservado)
- Inicie a instância
- Execute as ações de pós-lançamento para concluir os seguintes itens:
 - Ative o agente SSM.
 - Troque os volumes e exclua o volume raiz de origem (espaço reservado).

- Inicie a instância
- Execute o documento PostLaunchScript SSM. Este documento faz o seguinte:
 1. Sai do domínio antigo.
 2. Muda o nome do host.
 3. Reinicializar. Os scripts de bootstrap do AMS unem a instância ao domínio de destino (DR) durante a inicialização.

Gerenciamento de patches no AMS

Tópicos

- [AMS Patch Orchestrator: um modelo de patch baseado em tags](#)
- [Usando o Patch Orchestrator](#)
- [Aplicação de patches sob demanda](#)
- [Correção padrão do AMS](#)
- [Compromissos de serviços de correção](#)

No AMS, o gerenciamento de patches é um serviço que ajuda você a manter as atualizações do fornecedor do sistema operacional em suas instâncias do Amazon Elastic Compute Cloud EC2 (Amazon). Você tem a liberdade de personalizar a frequência e o processo de correção de suas EC2 instâncias da Amazon.

Você configura o gerenciamento de patches durante a integração e pode atualizá-lo usando o processo RFC. As pilhas criadas usando o sistema de gerenciamento de alterações e um modelo compatível com patches (para Amazon, grupo Auto EC2 Scaling, pilha HA de um ou dois níveis) são automaticamente inscritas no gerenciamento de patches.

O AMS fornece um recurso, o Patch Orchestrator — correção baseada em tags, para configurar a correção.

Para obter definições de termos de patches, consulte [Termos-chave do AMS](#).

Important

- Não é possível que as pilhas ou as instâncias constituintes de uma pilha optem por não receber o gerenciamento de patches, se o modelo AMS a partir do qual a pilha é criada for compatível com o gerenciamento de patches. Atualmente, a aplicação de patches é compatível com os seguintes modelos de pilha:
 - Amazon EC2 stack | Create e Amazon EC2 stack | Create (com volumes adicionais)
 - EC2 Instância da Amazon lançada com CloudFormation ingestão
 - Grupo Auto Scaling | Criar (as EC2 instâncias da Amazon no grupo estão corrigidas)
 - Pilha de uma camada de alta disponibilidade | Criar e alta disponibilidade de pilha de duas camadas | Criar

- Se houver um incidente contínuo que afete uma pilha, os operadores do AMS podem reagendar ou cancelar a aplicação de patches programada.
- Por padrão, todas as instâncias dentro de uma pilha específica compatível com patches são corrigidas no local. Para corrigir grupos do Auto Scaling com uma substituição do Amazon Machine Image (AMI) usando a latest/patched AMS AMI, envie uma solicitação de serviço. AMIs As atualizações são compartilhadas nas contas todos os meses.

Important

Você pode especificar repositórios de patches alternativos para nós gerenciados. Embora o AMS implemente as configurações de patch solicitadas, você é responsável por selecionar e validar a segurança dos repositórios escolhidos. Você também deve aceitar quaisquer riscos decorrentes do uso desses repositórios, como riscos da cadeia de suprimentos.

A seguir estão as melhores práticas para a segurança do seu processo de gerenciamento de patches:

- Use somente fontes de repositório confiáveis e verificadas
- Use como padrão os repositórios padrão do fornecedor do sistema operacional quando possível
- Audite regularmente as configurações personalizadas do repositório

Tip

O AMS recomenda que você habilite backups para instâncias que tenham aplicativos ou serviços valiosos. Para obter informações sobre como habilitar backups, consulte [Gerenciamento de continuidade no AMS Advanced](#).

AMS Patch Orchestrator: um modelo de patch baseado em tags

Se você foi integrado ao novo modelo de patches baseado em tags do AMS Patch Orchestrator, você pode usar tags para aplicar sua configuração de patch a um conjunto preciso de recursos, chamado grupo de patches, que varia de uma instância a todas as suas instâncias. Para obter

informações sobre tags AMS, consulte [Usando tags](#). As instruções sobre como configurar as tags do Patch Orchestrator são fornecidas na seção a seguir.

Os patches são instalados durante as janelas de patch que você define com o [SSM Patch Window | Create](#). Cada janela de patch é uma janela de manutenção do AWS Systems Manager que é executada em um cronograma de sua escolha, tem uma duração configurada e se aplica a um grupo de patches. Instâncias que não fazem parte de uma janela de patch explícita são corrigidas durante a janela de manutenção padrão que você define ao se integrar ao Patch Orchestrator.

 Important

Se várias janelas de manutenção de patches estiverem programadas para serem executadas ao mesmo tempo, elas deverão ter menos de 1001 instâncias sendo processadas a qualquer momento. Essa é uma limitação do AWS Systems Manager. O AMS recomenda pelo menos uma hora a cada cinquenta instâncias.

Por padrão, todos os patches do sistema operacional (SO) fornecidos pelo fornecedor são instalados durante uma janela de manutenção ou um patch sob demanda. Isso é chamado de linha de base do patch padrão. Se quiser restringir quais patches estão instalados, você pode definir uma linha de base de patch personalizada com uma das linhas de base de patches criadas CTs (por OSes), consulte Subcategoria de [patches](#). Por exemplo, você pode usar uma linha de base de patch personalizada para que somente atualizações de segurança críticas e importantes sejam instaladas para um ou mais grupos de patches.

Depois que os patches são instalados em uma instância, a instância é reinicializada. As notificações de patch são enviadas antes e depois da correção, e um lembrete adicional é enviado dentro de 96 horas antes do início programado. Além disso, o AMS aplica atualizações às ferramentas de gerenciamento de infraestrutura (como o agente AWS SSM) durante a janela de manutenção selecionada.

 Important

O AMS está descontinuando os relatórios mensais de conformidade de patches de instâncias com patches ausentes e não enviará relatórios mensais. Essa alteração foi feita com base nos relatórios operacionais de autoatendimento lançados recentemente, que são atualizados a cada 24 horas e estão disponíveis sob demanda e fornecem os dados mais recentes e

granulares. Para saber mais sobre os relatórios, consulte Relatórios de autoatendimento.
Para saber mais sobre os relatórios, consulte [Relatórios de autoatendimento](#).

Para obter mais informações sobre as notificações, consulte [Notificações de patch](#).

Usando o Patch Orchestrator

Ative o AMS Patch Orchestrator para sua conta enviando uma solicitação de serviço que inclua os seguintes detalhes:

- Categoria: Outros
- Assunto: Integração ao Patch Orchestrator
- E-mails CC: os endereços de e-mail CC recebem notificações quando o status dessa RFC de integração é alterado
- Detalhes: cole as informações a seguir no e-mail e forneça seus valores. Observe que isso ThirdTagKey é opcional. Para recomendações e exemplos, consulte a tabela a seguir.

```
Default maintenance window Schedule:  
Default Maintenance Window Schedule TimeZone:  
Default Maintenance Window Duration:  
Default Maintenance Window Cutoff:  
Default Patch Backup Retention In Days:  
Default Maintenance Window Notification Emails:  
First Tag Key:  
Second Tag Key:  
Third Tag Key:
```

A tabela a seguir descreve o formato e as recomendações para os valores fornecidos.

Configurações de patches baseadas em tags do Patch Orchestrator

Nome do parâmetro	Informações	Recomendação ou exemplo
Programação da janela de manutenção padrão	O cronograma da janela de manutenção padrão na forma de uma expressão cron ou de taxa. Por exemplo:	Recomendamos que a janela funcione pelo menos uma vez por mês em um dia útil consistente.

Nome do parâmetro	Informações	Recomendação ou exemplo
	• <code>cron(0 3 ? * 6L *)</code>: 03:00 da manhã na última sexta-feira de cada mês • <code>rate(7 days)</code>: A cada sete dias Para obter mais informações sobre a criação de expressões cron e links para recursos de expressão cron e de taxa, consulte Expressões cron e de taxa para janelas de manutenção.	
Fuso horário de programação da janela de manutenção padrão	O fuso horário no qual a janela de manutenção padrão é executada se baseia, no formato Internet Assigned Numbers Authority (IANA).	Por exemplo: • America/Los_Angeles • Etc/UTC
Duração padrão da janela de manutenção	A duração da janela de manutenção padrão em horas.	Pelo menos 1 hora a cada 50 instâncias, mais 2 horas para o limite.
Limite padrão da janela de manutenção	O número de horas antes do final da janela de manutenção padrão em que nenhum novo comando de patch é iniciado. Esse intervalo existe para permitir que a correção seja concluída antes que a janela termine.	Pelo menos 2 horas.

Nome do parâmetro	Informações	Recomendação ou exemplo
Retenção de backup de patches padrão em dias (opcional)	O tempo padrão em dias para manter os pontos de restauração do EBS criados antes da aplicação de patches nas instâncias.	Recomendamos manter o padrão, que é 60.
E-mails de notificação da janela de manutenção padrão	De um a cinco endereços de e-mail ou listas de distribuição para receber notificações sobre o status de correção da janela de manutenção padrão.	Recomendamos usar listas de distribuição em grupo em vez de e-mails individuais.
Primeira chave de tag	A primeira chave de tag a ser usada para criar seus valores de tag do Patch Group.	Por exemplo, Appld. Especifique null se você já tiver definido seus próprios grupos de patches com uma tag de grupo de patches.
Segunda chave de tag	A segunda chave de tag a ser usada para criar seus valores de tag do Patch Group.	Por exemplo, Meio Ambiente. Especifique null se você já tiver definido seus próprios grupos de patches com uma tag de grupo de patches.
Terceira chave de tag (opcional)	A terceira chave de tag opcional a ser usada para criar seus valores de tag do Patch Group.	Por exemplo, Grupo.

Depois de se integrar ao novo modelo de serviço de patches do Patch Orchestrator, todas as instâncias com tags apropriadas em sua conta pertencem a um grupo de patches com uma tag de grupo de patches. O Patch Orchestrator usa sua tag de Grupo de Patch existente ou uma tag criada pelo AMS que consiste em dois ou três valores de tag concatenados que você especificou durante a integração do Patch Orchestrator. Por exemplo, *{Tag Value 1} - {Tag Value 2} - {Tag Value 3}*. O AMS atualiza essas tags de grupo de patches aplicadas pelo AMS a cada 12 horas. Se

necessário, você pode atualizar os valores da tag do seu Grupo de Patch com os tipos de alteração [Tag | Atualizar \(Revisão obrigatória\)](#) ou [Tag | Atualizar \(Revisão obrigatória\)](#).

Por exemplo, se sua EC2 instância da Amazon tiver os seguintes pares de tag chave-valor:

- AppId:MyApplication
- Environment:Production
- Group:1

Durante a integração, você especificou as seguintes chaves de tag:

- First Tag Key = AppId
- Second Tag Key = Environment
- Third Tag Key = Group

O AMS cria a seguinte tag de grupo de patches e a aplica às suas instâncias: Patch Group:MyApplication-Production-1.

 Note

Os alertas de falha de patch não são criados para instâncias que têm sistemas operacionais incompatíveis ou que são interrompidas durante a janela de manutenção.

Pré-requisitos do Patch Orchestrator

O fluxo de trabalho do Patch Orchestrator tem como alvo EC2 as instâncias da Amazon que são corrigidas pela versão mais recente do documento de automação do System Manager: `AWSManagedServices-PatchInstanceFromMaintenanceWindow`

Como parte do fluxo de trabalho do documento, o documento de comando run “AWS-RunPatchBaseline” é executado em cada uma das EC2 instâncias da Amazon a partir dos membros do grupo de patches. Para saber mais, consulte [Sobre o documento SSM AWS-. RunPatchBaseline](#)

Requisitos:

- EC2 Instância da Amazon implantada a partir da Amazon Machine Image (AMI) fornecida pela AMS ou em uma AMI por meio da instância migrada do parceiro de migração “Stack from migration partner” CT (ct-257p9zjk14ija).
- Conexão de saída à Internet ativada. Para firewall/proxy soluções, o requisito é permitir que o Windows atualize o repositório and/or Linux, endpoints espelhados, endpoints, configurações de proxy do AWS System Manager e configuração de proxy de metadados. Para obter mais informações, consulte [Configurar o agente SSM para usar um proxy](#) e [Usar um proxy HTTP](#)
- Função do IAM que corresponde ao acesso mínimo permissivo para o serviço SSM da função do customer-mc-ec2-instance-profile IAM.
- Recomendamos 10 GB de espaço disponível na partição raiz. Para o sistema operacional Linux, pelo menos 2 GB disponíveis na /var partição.
- Autoridade de certificação válida e ativa para downloads de atualizações.
- Windows Server Update Services (WSUS) - Registro incluindo, mas não limitado a: DisableWindowsUpdateAccess, NoWindowsUpdate; As atualizações automáticas não devem prejudicar a operação do processo do Windows Update.

Validação:

- Para instâncias do sistema operacional Linux usando o gerenciador de pacotes yum, você pode validar a disponibilidade de atualizações executando `#yum check-update`
- Para Linux OS RedHat 5.7 e mais recente, 6.1 e mais recente e 7.0 e mais recente; EC2 instâncias da Amazon migraram para sua conta AMS por meio da CT “Stack from migration partner migrated instance” (ct-257p9zjk14ija), você precisa validar o status do gerenciador de assinaturas para verificar o desempenho da atualização.
- No sistema operacional Windows, habilite o Windows Server Update Services (WSUS). Nenhuma política local deve bloquear a capacidade do WSUS de verificar ou instalar atualizações. Depois de fazer login como administrador, você pode validá-lo executando uma verificação das atualizações disponíveis no console do Windows Update Service. As versões do sistema operacional Windows Server, incluindo 2012R2, 2016 e 2019, têm configurações padrão do Windows Update para baixar e instalar. Você pode definir as configurações desejadas antes da digitalização. Em versões posteriores do sistema operacional, essa operação pode acionar a instalação; configure o comportamento desejado com antecedência.
- Solicite a validação da equipe de operações do AMS enviando uma solicitação de serviço: “Documento de AWSManagedServices-CheckPatchingPrerequisites automação a ser executado na EC2 instância da Amazon para avaliação da prontidão do patch”.

 Note

Os alertas de falha de patch não são criados para instâncias que têm sistemas operacionais incompatíveis ou que são interrompidas durante a janela de manutenção.

Janelas de patch

Instâncias em um grupo de patches específico são corrigidas durante uma ou mais janelas de patch. As janelas de patch são executadas em um cronograma definido como uma expressão cron ou rate e têm uma duração configurável destinada a manter as interrupções relacionadas ao patch dentro de um intervalo de tempo escolhido. O AMS recomenda criar várias janelas de patch que cubram coletivamente todas as suas instâncias, de acordo com as rotinas de correção específicas da sua organização e para usar a janela de manutenção padrão como alternativa. As janelas de patch são criadas com o tipo de alteração RFC Deployment | Patching | SSM patch window | Create (ct-0el2j07llrxs7). Todas as instâncias que não fazem parte de uma janela de patch são corrigidas durante a janela de manutenção padrão criada durante a integração.

Normalmente, uma janela de patch não precisa ser atualizada para incluir novas instâncias. Normalmente, isso é feito modificando as tags da instância. Por exemplo, considere a seguinte sequência de eventos:

1. Duas instâncias estão marcadas

`comAppId:MyApplication,Environment:Production,Group:1.`

Isso produz uma tag nessas instâncias, supondo que First Tag Key = AppId, Second Tag Key = Environment, Third Tag Key = Group e uma janela de patch para o grupo de patches MyApplication -Production-1 seja criada.

2. Mais três instâncias são criadas e marcadas

`comAppId:MyApplication,Environment:Production,Group:1.`

Isso produz uma tag para o Patch Group: MyApplication -Production-1.

Nenhuma alteração na janela de patch é necessária porque ela coleta todas as cinco instâncias no momento da próxima execução programada.

Para uma discussão mais detalhada e uma explicação sobre como usar esse tipo de alteração, consulte [Janela de patch do SSM | Criar](#).

Notificações de patch

Important

A partir de 1º de fevereiro de 2025, os clientes do AMS não receberão mais notificações sobre janelas de manutenção de patches vazias em suas contas gerenciadas.

Os endereços de e-mail inscritos (até cinco) recebem um e-mail semelhante ao seguinte pouco antes do início da janela de manutenção do patch:

Dear Customer,
The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* was started at:
2020-02-21T12:02:18.196Z.

Details:

Maintenance Window AccountId: *YOUR_ACCOUNT_ID*
Maintenance Window Region: *YOUR_ACCOUNT_REGION*
Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*
Maintenance Window Name: *THE_MAINTENANCE_WINDOW_NAME*
Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH_GROUP_NAME*

Maintenance Window Patch Group: *PATCH_GROUP_NAME*
Maintenance Window ExecutionId: *THE_EXECUTION_ID*

Targets:

InstanceId	InstanceName	StackId
-----	-----	-----
<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>

A follow-up message with a detailed report is sent as soon as the maintenance window is over.

Please raise a service request if you have any inquiries about AMS Patch Orchestrator by following this URL:

<https://console.aws.amazon.com/managedservices/servicerequest/new>

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

Ao final da atividade do patch, os endereços de e-mail inscritos recebem um e-mail semelhante ao seguinte:

```
Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME ended at:
  2020-02-21T12:03:20.058Z, with status: SUCCESS.
Details:
  Maintenance Window AccountId: YOUR_ACCOUNT_ID
  Maintenance Window Region:    YOUR_ACCOUNT_REGION
  Maintenance Window Id:        THE_MAINTENANCE_WINDOW_ID
  Maintenance Window Name:      THE_MAINTENANCE_WINDOW_NAME
  Maintenance Window Description: MaintenanceWindow for patching patch
  Group PATCH_GROUP_NAME
  Maintenance Window Patch Group: PATCH_GROUP_NAME
  Maintenance Window ExecutionId: THE_EXECUTION_ID
Targets:
  RfcId                InstanceId                InstanceName                StackId
  Status
  -----
  THE_RFC_ID          THE_INSTANCE_ID          THE_INSTANCE_NAME THE_STACK_NAME
STATUS

You can view the current Patch Compliance of your Amazon EC2 Instances by following
this URL:
https://console.aws.amazon.com/systems-manager/compliance?region=YOUR\_ACCOUNT\_REGION

Please raise an Incident if an issue is impacting one of your production applications
by following this URL:
https://console.aws.amazon.com/managedservices/incident/new

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team
```

A cada 96 horas, o sistema de patches do AMS identifica todas as próximas janelas de manutenção gerenciada de patches dentro dessas 96 horas e envia uma notificação de lembrete para todos os endereços de e-mail inscritos que se enquadrem nessa janela de 96 horas. Isso pode ser apenas uma hora antes da janela ou as 96 horas completas. Por exemplo:

Dear Customer,

The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* will start at:
2020-05-06T16:35:36.523Z.

Details:

Maintenance Window AccountId: *YOUR_ACCOUNT_ID*
 Maintenance Window Region: *YOUR_ACCOUNT_REGION*
 Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*
 Maintenance Window Name: *THE_MAINTENANCE_WINDOW_NAME*
 Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH_GROUP_NAME*

Maintenance Window Patch Group: *PATCH_GROUP_NAME*
 Maintenance Window Next Start Time: 2020-05-06T16:35:36.523Z
 Maintenance Window Schedule: rate(24 hours)
 Maintenance Window Timezone: *THE_TIMEZONE*

At this time, these are the instances in the "*PATCH_GROUP_NAME*" Patch Group:

InstanceId	InstanceName	StackId	InstanceState

<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped
<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped
<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped

A notification message is sent as soon as the maintenance window starts.

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

If you would like to disable this maintenance window or you have inquiries about the AMS Patch Orchestrator click on the following URL:

<https://console.aws.amazon.com/managedservices/servicerequest/new>

If you would like to delete this maintenance window, you can run the CT with id "ct-0q0bic0ywqk6c" against the stack id "stack-rctyznutkyj4tkkzq".

Kind Regards,

Amazon Web Services
 Amazon Managed Services
 Patch Team

Linhas de base de patch

Por padrão, todos os patches do sistema operacional (SO) fornecidos pelo fornecedor são instalados usando a linha de base de patches padrão da AMS. Se quiser restringir quais patches estão instalados, você pode, opcionalmente, criar uma linha de base de patch usando o tipo de alteração RFC Deployment | Patching | SSM patch baseline | Create **OS** (o CT ID varia de acordo com o sistema operacional).

Para obter informações sobre como usar esses tipos de alteração, consulte a [subcategoria Patching](#).

Tags reservadas do Patch Orchestrator

O Patch Orchestrator também gera as seguintes tags que não podem ser modificadas:

- **AMSPatchGrupo** — Essa tag é usada para a geração do valor da tag Patch Group. Você não deve modificar o AMSPatch Grupo. Você pode modificar a tag “Grupo de patches” se quiser usar um valor personalizado de “Grupo de patches”. O Patch Orchestrator continua gerando um valor para o AMSPatch Grupo com base nas chaves de tag fornecidas durante a integração, mas não modificará o valor da tag “Grupo de Patches” se ele tiver sido definido como um valor personalizado por você. Para parar de usar um valor personalizado de “Grupo de patches”, você pode definir o valor de “Grupo de patches” para corresponder ao valor da tag do AMSPatch grupo.
- **AMSDefaultPatchGroup**— Essa tag indica se uma instância faz parte da janela de manutenção padrão, com um valor verdadeiro ou falso. Se o Patch Group de uma instância não estiver atribuído a uma janela de manutenção, esse valor será definido como True.

Aplicação de patches sob demanda

O AMS tem um tipo de alteração que funciona com sua linha de base de patches, para permitir que você execute um patch em instâncias sob demanda. Essa pode ser a linha de base padrão que você definiu na integração ou a linha de base do patch do Patch Orchestrator Systems Manager que você definiu com o tipo de alteração da linha de base do patch (o CT ID varia de acordo com o sistema operacional).

Você pode usar o tipo de alteração de patch sob demanda com ou sem o Patch Orchestrator.

Para obter informações sobre como usar esse tipo de alteração, consulte [On Demand Patching | Run](#).

 Note

Você não pode usar instâncias que fazem parte de um grupo de Auto Scaling em um tipo de alteração de patch sob demanda.

Correção padrão do AMS

O AMS oferece suporte a clientes existentes usando o modelo de patch padrão do AMS, mas esse modelo não está disponível para novos clientes e está sendo retirado em favor do AMS Patch Orchestrator.

O conteúdo típico do patch padrão do AMS inclui atualizações do fornecedor para sistemas operacionais suportados e software pré-instalado com sistemas operacionais compatíveis (por exemplo, IIS e Apache Server).

Durante a integração do AMS, você especifica os requisitos, a política, a frequência e as janelas de patch preferenciais. Essas configurações significam que você pode evitar colocar os aplicativos off-line de uma só vez para aplicar patches na infraestrutura, para que você possa controlar qual infraestrutura será corrigida e quando.

 Note

O processo de correção descrito neste tópico se aplica somente às suas pilhas. A infraestrutura do AMS é corrigida durante um processo separado. 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 configura a janela de patch do AMS na integração ou aprova ou rejeita a notificação mensal do serviço de patch.

O AMS examina regularmente as EC2 instâncias gerenciadas da Amazon em busca de atualizações disponíveis por meio da funcionalidade de atualização do sistema operacional. Também fornecemos atualizações regulares para a base do AMS Amazon Machine Images (AMIs) suportada em nosso ambiente.

Depois de validadas, as versões do AMS AMI são compartilhadas com todas as contas do AMS. Você pode visualizar as versões disponíveis da AWS AMI usando a chamada de EC2 API da

[Describelmages](#) Amazon ou usando o EC2 console da Amazon. Para encontrar o AMS disponível AMIs, consulte [Encontre AMI IDs, AMS](#).

O AMS executa cronogramas de patches ad hoc somente quando solicitado por você. Anteriormente, o AMS enviava uma notificação; atualmente, uma notificação não é enviada.

 Note

Por padrão, o AMS usa o Systems Manager para aplicar patches fazendo com que o gerenciador de pacotes (Linux) ou o serviço System Update (Windows) consulte seu repositório padrão para ver quais novos pacotes estão disponíveis. Se, durante o curso de suas day-to-day operações, você instalou um pacote em um host Linux usando o gerenciador de pacotes padrão, esse gerenciador de pacotes também selecionará novos pacotes para esse software quando estiverem disponíveis. Nesse caso, talvez você queira realizar uma ação de correção (descrita nesta seção) para optar por não participar dessa instância.

Sistemas operacionais compatíveis

Sistemas operacionais compatíveis (x86-64)

- Amazon Linux 2023
- Amazon Linux 2 (data prevista de término do suporte ao AMS em 30 de junho de 2026)
- Oracle Linux 9.x, 8.x
- Red Hat Enterprise Linux (RHEL) 9.x, 8.x
- Servidor SUSE Linux Enterprise 15 SP6
- SUSE Linux Enterprise Server para SAP 15 SP3 e versões posteriores
- Microsoft Windows Server 2022, 2019, 2016
- Ubuntu 20.04, 22.04, 24.04

Sistemas operacionais compatíveis (ARM64)

- Amazon Linux 2023
- Amazon Linux 2 (data prevista de término do suporte ao AMS em 30 de junho de 2026)

Patches compatíveis

O AWS Managed Services oferece suporte à aplicação de patches principalmente no nível do sistema operacional. Os patches instalados podem diferir de acordo com o sistema operacional.

Important

Todas as atualizações são baixadas dos repositórios remotos do serviço de linha de base de patches do Systems Manager configurados na instância e descritos posteriormente neste tópico. A instância deve ser capaz de se conectar aos repositórios para que a correção possa ser executada.

Para desativar o serviço de linha de base de patches para repositórios que entregam pacotes que você mesmo deseja manter, execute o comando a seguir para desativar o repositório:

```
yum-config-manager DASHDASHdisable REPOSITORY_NAME
```

Recupere a lista dos repositórios atualmente configurados com o seguinte comando:

```
yum repolist
```

- Repositórios pré-configurados do Amazon Linux (geralmente quatro):

ID do repositório	Nome do repositório
amzn-main/mais recente	Base principal da AMZN
atualizações do amzn/últimas	Base de atualizações da AMZN
pele/x86_64	Pacotes extras para Enterprise Linux 6 - x86_64
pbis	Atualizações dos pacotes PBIS

- Repositórios pré-configurados do Red Hat Enterprise Linux (cinco para o Red Hat Enterprise Linux 7 e cinco para o Red Hat Enterprise Linux 6):

ID do repositório	Nome do repositório
Região RHUI- -7/x86_64 client-config-server	Conjunto de configuração do cliente Red Hat Update Infrastructure 2.0
Região RHUI- /7Server/x86_64 rhel-server-releases	Servidor Red Hat Enterprise Linux 7
Região RHUI- /7Server/x86_64 rhel-server-releases	Servidor Red Hat Enterprise Linux 7 RH Comum () RPMs
pele/x86_64	Pacotes extras para Enterprise Linux 7 - x86_64
pbis	Atualizações dos pacotes PBIS

ID do repositório	Nome do repositório
Região de Rhui- -6 client-config-server	Red Hat Update Infrastructure 2.0
Região de Rhui- rhel-server-releases	Servidor Linux Empresarial Red Hat (6RPMs)
Região de Rhui- rhel-server-rh-common	Red Hat Enterprise Linux Server 6 RH Comum () RPMs
repelir	Pacotes extras para Enterprise Linux 6 - x86_64
pbis	Atualizações dos pacotes PBIS

- Repositórios pré-configurados do CentOS 7 (geralmente cinco):

ID do repositório	Nome do repositório
base/7/x86_64	CentOS-7 - Base
atualizações/7/x86_64	CentOS-7 - Atualizações

ID do repositório	Nome do repositório
extras/7/x86_64	CentOS-7 - Extras
pele/x86_64	Pacotes extras para Enterprise Linux 7 - x86_64
pbis	Atualizações dos pacotes PBIS

- Para o Microsoft Windows Server, todas as atualizações são detectadas e instaladas usando o Windows Update Agent, que está configurado para usar o catálogo do Windows Update (isso não inclui atualizações do Microsoft Update).

Nos sistemas operacionais Microsoft Windows, o Patch Manager usa o arquivo cab wsusscn2.cab da Microsoft como fonte das atualizações de segurança disponíveis do sistema operacional. Esse arquivo contém informações sobre as atualizações de segurança que o Microsoft publica. O Patch Manager baixa esse arquivo regularmente da Microsoft e o usa para atualizar o conjunto de patches disponíveis para instâncias do Windows. O arquivo contém apenas atualizações que a Microsoft identifica como relacionada à segurança. Quando as informações no arquivo são processadas, o Patch Manager remove também atualizações que foram substituídas por atualizações posteriores. Portanto, apenas a atualização mais recente é exibida e disponibilizada para instalação. Por exemplo, se KB4 012214 substituir KB3135456, somente KB4 012214 será disponibilizado como uma atualização no Patch Manager.

Para ler mais sobre o arquivo wsusscn2.cab, consulte o artigo da Microsoft [Usando o WUA para verificar atualizações off-line](#).

Patching e design de infraestrutura

O AMS emprega diferentes métodos de correção, dependendo do design da sua infraestrutura: mutável ou imutável (para obter definições detalhadas, consulte). [Termos-chave do AMS](#)

Com infraestruturas mutáveis, a correção é feita usando uma metodologia tradicional local de instalação de atualizações diretamente nas EC2 instâncias da Amazon, individualmente, pelos engenheiros de operações da AMS. Esse método de correção é usado para pilhas que não são grupos do Auto Scaling e contêm uma única instância da EC2 Amazon ou algumas instâncias. Nesse cenário, substituir a AMI na qual a instância ou a pilha se baseava destruiria todas as alterações feitas nesse sistema desde que ele foi implantado pela primeira vez, então isso não é feito. As

atualizações são aplicadas ao sistema em execução e você pode enfrentar um tempo de inatividade do sistema (dependendo da configuração da pilha) devido à reinicialização do aplicativo ou do sistema. Isso pode ser mitigado com uma estratégia de Blue/Green atualização. Para obter mais informações, consulte [AWS CodeDeploy Apresenta Blue/Green implantações](#).

Com infraestruturas imutáveis, o método de aplicação de patches é o substituto da AMI. As instâncias imutáveis são atualizadas uniformemente usando uma AMI atualizada que substitui a AMI especificada na configuração do grupo Auto Scaling. Os lançamentos do AMS são atualizados (ou seja, corrigidos) AMIs todos os meses, geralmente na semana do Patch Tuesday. A seção a seguir descreve como isso funciona.

Como funciona a correção padrão do AMS

O AMS usa o serviço Systems Manager Run Command para correções críticas regulares, mensais e conforme necessário, com dois métodos principais de correção, no local e substituição da AMI, dependendo da estratégia de implantação da sua infraestrutura (mutável versus imutável). Esta seção descreve o serviço, os tipos, os métodos e os processos de aplicação de patches do AMS.

O AMS define dois tipos de patch, que são programados de forma diferente:

- Correção crítica: as atualizações são aplicadas o mais rápido possível, após a aceitação do aviso.
- Patches padrão: atualizações regulares do fornecedor do sistema operacional e aplicadas mensalmente.

Os patches são aplicados por meio de patches no local ou substituição da AMI (mediante solicitação).

Escaneamento de atualizações

O AMS usa o [Amazon EC2 Run Command Service](#) para entrar em contato com suas EC2 pilhas da Amazon e implantar os scripts de verificação e correção necessários. O AMS usa o componente nativo de gerenciamento de pacotes já instalado no sistema operacional compatível para realizar todo o comportamento necessário de escaneamento e correção na EC2 pilha da Amazon. Para Red Hat e Amazon Linux, o serviço usa yum. Para Windows, o serviço usa o Windows Update Agent.

As digitalizações são realizadas diariamente usando o [SSM Maintenance Windows](#) e o documento AWS- RunPatchBaseline padrão do AMS. Cada EC2 pilha acessível da Amazon é escaneada, usando os repositórios de atualização para Linux e Windows. O processo de aplicação de patches do AMS detecta todas as pilhas acessíveis da EC2 Amazon e, em seguida, executa as varreduras

em um processo em lote para que a pilha permaneça sempre em bom estado, mesmo que ocorra uma falha durante a execução da verificação. Os resultados da verificação são então salvos para cada EC2 pilha da Amazon.

Para ver os resultados da verificação de uma pilha ou instância, envie uma solicitação de serviço com o ID da pilha ou o ID da instância.

O processo padrão de aplicação de patches do AMS é instalar todos os patches disponíveis, independentemente da classificação ou gravidade do patch (por exemplo, crítico versus padrão). A exceção a isso são os patches que você excluiu explicitamente da pilha (os patches definidos como obrigatórios pelo AMS não devem ser excluídos).

Você recebe uma notificação do serviço de patches 14 dias antes da janela de manutenção proposta. Isso lhe dá tempo para testar os patches propostos e aceitá-los ou rejeitá-los. Se você não responder à notificação do serviço de patches, suas instâncias não serão corrigidas. Quando chega a hora de instalar os patches, o AMS cria uma Solicitação de Alteração (RFC) para cada pilha, e essa RFC aparece na lista de RFC da sua conta.

Janela e aviso de manutenção configurados pelo AMS

Com o patch configurado pelo AMS, cada conta tem uma janela de manutenção mensal, que você define ao integrar sua conta. 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.

A janela de aplicação de patches é diferente. A solicitação de serviço de saída de patch (também conhecida como notificação de serviço) inclui uma janela de patch sugerida.

Note

Para obter informações sobre como responder à notificação do serviço de patches, consulte [Ações que você pode realizar na aplicação de patches padrão do AMS](#)

A notificação do serviço de patches é enviada por e-mail para o endereço de e-mail de contato registrado em sua conta. A notificação inclui um link para o console do AWS Support, onde você pode responder a ela. Você também pode responder à notificação usando a página de solicitação de serviço do AMS. A notificação do serviço inclui:

- Uma lista de atualizações IDs (CSUs, IUs, e OUs) que se aplicam à pilha e as atualizações que você solicitou que foram excluídas da correção (se houver).
- IDs de instâncias que serão afetadas.
- Uma proposta de janela de correção quando as atualizações serão aplicadas. Você pode solicitar uma janela de correção diferente.
- Uma solicitação para que você aceite o patch proposto ou solicite informações adicionais. O AMS dá a você tempo para testar o impacto das atualizações e aprovar ou rejeitar a correção, ou solicitar que atualizações específicas sejam excluídas. Se você precisar de mais tempo para testar e quiser que as atualizações sejam aplicadas após o teste, responda à notificação de serviço e descreva o que você deseja, ou envie uma solicitação de serviço para um novo patch RFC com base nos detalhes do RFC anterior. Se você não responder à notificação do serviço, nenhuma ação de correção será executada e a RFC será cancelada.

Se você aprovar a notificação do serviço, o AMS executará o RFC do patch e aplicará as atualizações dentro da janela de patch acordada, de acordo com o compromisso do serviço.

Quando a correção é concluída, o AMS envia uma correspondência na Solicitação de Serviço, com um resumo do resultado da atividade de correção (ou seja, sucesso ou falha).

Correção de patches no local

A aplicação de patches no local se refere a um método em que o AMS faz login em cada instância da pilha e aplica os patches.

A aplicação de patches no local ocorre em infraestruturas mutáveis usando instâncias da EC2 Amazon que executam um sistema operacional compatível. A aplicação de patches aplica todas as atualizações não excluídas disponíveis até aquele momento. Quando os patches críticos são lançados, há um processo adicional de correção crítica.

Aplicação de patches padrão: no local

A correção padrão ocorre de acordo com o cronograma de patches acordado sugerido na notificação do serviço de patches e inclui atualizações regulares de patches que não são consideradas críticas.

Antes da janela de patch proposta, e com sua resposta afirmativa à notificação, uma RFC de patch é criada e aparece no painel da RFC.

Correção crítica: no local

Quando um fornecedor de sistema operacional lança uma atualização crítica de segurança, o AMS notifica você sobre o patch RFC enviando uma notificação de serviço (para o e-mail de contato da sua conta) para cada pilha, de acordo com o compromisso de serviço do AMS. A notificação de serviço inclui o seguinte para cada atualização:

- Atualize a data de lançamento
- Criticidade da atualização
- Detalhes da atualização (referência de KB, etc.)
- IDs de pilhas afetadas

Você pode testar as atualizações listadas na notificação e aprovar ou rejeitar os patches respondendo à notificação do serviço. Se você aprovar a notificação, precisará fornecer uma janela de patch específica por pilha para instalar as atualizações.

Note

As janelas de patch que estão dentro de 24 horas após a resposta à notificação de serviço podem ser reprogramadas com base na capacidade disponível.

Se você não responder dentro de 10 dias ou se rejeitar o patch proposto, o patch será cancelado.

Se você quiser aplicar as atualizações após o período permitido (fornecido na notificação), envie uma solicitação de serviço para um novo cronograma de patches com base nos detalhes da notificação anterior.

Se você aprovar a notificação de serviço, o AMS aplicará as atualizações dentro da janela de patch especificada, de acordo com o compromisso do serviço.

No caso de várias atualizações, você pode excluir atualizações específicas do patch especificando as atualizações a serem excluídas em sua resposta à notificação do serviço.

O AMS envia uma notificação de serviço para cada pilha sobre o resultado de cada atualização (ou seja, sucesso ou falha).

Atualizações e patches da AMI (usando patches AMIs para grupos de Auto Scaling)

A correção de substituição de AMI é feita em infraestruturas imutáveis por meio da atualização do ID da AMI que está configurado para implantar novas instâncias da Amazon EC2 em um grupo de Auto Scaling.

As Amazon Machine Images (AMIs) são lançadas regularmente para os sistemas operacionais compatíveis. Os fornecedores de sistemas operacionais lançam novos patches periodicamente. O AMS pega a AMI fornecida pela Amazon, a atualiza com os patches mais recentes e, em seguida, adiciona os componentes apropriados para permitir que ela opere no ambiente AMS. Em seguida, ele disponibiliza a nova AMI do AMS para todos os clientes do AMS compartilhando a AMI com as contas. Suas pilhas de grupos do Auto Scaling podem ser atualizadas mensalmente com esses AMS recém-lançados. AMIs O gráfico a seguir ilustra como seus ambientes AMIs são usados no AMS.

Os grupos de Auto Scaling criam suas instâncias com base na AMI configurada para o grupo Auto Scaling. Quando os compartilhamentos do AMS são atualizados AMIs, você tem as seguintes opções, dependendo de como você está gerenciando as atualizações da AMI:

- Se você estiver usando uma ferramenta de implantação de aplicativos (por exemplo UserData, CodeDeploy,, etc.) que personaliza suas instâncias automaticamente após a criação, você pode fazer o seguinte:
 - Responda à notificação do serviço de correção ou envie uma solicitação de serviço para a AMI do AMS mais recente para substituir a AMI de configuração do seu grupo de Auto Scaling atual. Depois que o ID da AMI na configuração dos grupos do Auto Scaling for substituído, o AMS inicia as atualizações contínuas das suas instâncias e as configurações da instância do grupo do Auto Scaling (por exemplo, instalação de aplicativos, scripts de inicialização etc.) são aplicadas automaticamente às novas instâncias criadas com a nova AMI do AMS.
- Se você estiver usando uma custom/golden AMI na configuração dos grupos do Auto Scaling, você pode:
 - Crie uma instância com a nova AMI do AMS, personalize a instância e crie uma nova AMI dourada. Compartilhe a nova AMI dourada com o AMS usando o EC2 console da Amazon e envie uma solicitação de serviço ao AMS para atualizar a configuração dos grupos do Auto Scaling para usar sua nova AMI personalizada.
 - Compartilhe sua AMI dourada existente com o AMS usando o EC2 console da Amazon e envie uma solicitação de serviço para que o AMS atualize sua AMI dourada. Para fazer isso, o AMS cria uma instância da sua AMI dourada, aplica os patches a essa instância, cria uma nova

AMI dourada para você e, em seguida, atualiza a configuração dos grupos do Auto Scaling para usar a nova AMI. A desvantagem aqui é que o AMS não pode testar se sua nova AMI personalizada funciona da maneira que você deseja. Em vez disso, você deve testar a instância criada com a nova AMI e verificar se tudo funciona corretamente antes de criar uma nova AMI dourada, compartilhá-la e solicitar que o AMS atualize seus grupos do Auto Scaling. O AMS não recomenda essa opção.

Patching padrão: atualizações da AMI

Todo mês, o AMS lança novas Amazon Machine Images (AMIs) com melhorias nos serviços e novos patches que se aplicam ao AMIs.

Note

Novos AMS AMIs são gerados após o Patch Tuesday a partir da AWS atualizada AMIs. Em seguida, o AMS os testa antes de disponibilizá-los. Após a AMIs aprovação do novo teste, os compartilhamentos do AMS foram atualizados AMIs para contas gerenciadas.

Patches críticos: atualizações da AMI

Quando necessário, o AMS fornece patches de segurança críticos AMIs atualizados desde a última versão mensal da AMI.

O processo de atualizações críticas de segurança em infraestruturas imutáveis é idêntico ao processo mensal de AMI para infraestruturas imutáveis, exceto que uma nova AMI do AMS é criada fora do cronograma normal (Patch Tuesday), com base no lançamento de novas atualizações críticas. O AMS disponibiliza uma nova AMI com os patches de segurança críticos de acordo com os acordos de nível de serviço (SLAs) definidos para sua conta. Atualizações do AMS de grupos do Auto Scaling somente mediante solicitação. Use uma solicitação de serviço para enviar solicitações de substituição da AMI.

Falhas de patches padrão do AMS

Em caso de falha nas atualizações, o AMS realiza uma análise para entender a causa da falha e comunica o resultado da análise a você. Se a falha for atribuível ao AMS, tentaremos novamente as atualizações se elas estiverem dentro da janela de manutenção. Caso contrário, o AMS cria notificações de serviço para a falha na atualização da instância e aguarda suas instruções.

Para falhas atribuíveis ao seu sistema, você pode enviar uma solicitação de serviço com um novo patch RFC para atualizar as instâncias.

Ações que você pode realizar na aplicação de patches padrão do AMS

Além de testar novas AMIs, há várias ações que você pode tomar para gerenciar a correção de sua infraestrutura:

- Se o teste das atualizações demorou mais do que o permitido pela janela de patch, você pode solicitar que o AMS aplique as atualizações que foram canceladas quando você estiver pronto, enviando uma solicitação de serviço (use os detalhes na notificação de serviço original como base).
- Você pode solicitar que uma atualização importante (IU) ou outra atualização (OU) seja aplicada antes da próxima janela de atualização automática enviando uma solicitação de serviço fornecendo uma lista das atualizações, das instâncias aplicáveis e outros detalhes, conforme apropriado. Como essa tomografia computadorizada não é automatizada, ela leva mais tempo para ser programada e executada. Verifique os objetivos do nível de serviço (SLOs) para saber o momento apropriado. Para obter mais informações, consulte [Objetivos de nível de serviço do AMS \(SLOs\)](#).

Além disso, você pode usar o AMS existente e corrigido AMIs para criar itens personalizados AMIs. Para obter informações, consulte [AMI | Create](#).

Note

Você não pode solicitar uma nova AMI do AMS com base em uma atualização importante ou outra atualização antes da próxima janela de manutenção, pois o processo de lançamento do AMS segue um ritmo uniforme para o benefício de todos os clientes do AMS.

Mudando o que patched/opting sai

Com o patch configurado pelo AMS, em sua resposta à notificação do serviço de patch ou em uma solicitação de serviço, você pode alterar quais recursos são corrigidos. Você pode fazer o seguinte:

- Defina uma lista de patches que devem ser excluídos da correção, por pilha e por sistema operacional.

- Defina uma lista de recursos que devem ser excluídos de determinados patches ou de todos os patches.
- Defina uma lista de recursos que sempre devem ser excluídos de todas as correções.
- Defina uma lista de recursos que devem ser corrigidos em um determinado dia e horário (bom se você não tiver definido uma janela de manutenção).

Para excluir um ou mais patches, envie uma solicitação de serviço ou responda à notificação do serviço de patches usando o modelo fornecido a seguir. Não envie um RFC. Inclua na solicitação o nome ou nomes do patch que você deseja excluir e por quê. Inclua essas informações em uma solicitação de serviço da seguinte forma:

- Nome: O nome do patch. Para patches do Windows, esse é o nome do KB, como KB3145384. Para patches do Linux, esse é o nome do pacote, como openssl-6.6.1p1-25.61.amzn1.x86_64.
- Motivo: Um comentário indicando por que o patch está sendo excluído.
- Tempo de expiração: o date/time momento em que a exclusão expira.

Se um patch excluído já estiver instalado, ele será removido.

A solicitação é analisada por um operador que discutirá o assunto com você se a exclusão desses patches representar um risco significativo de segurança. A data de validade dos patches excluídos também é negociada. Após a data de expiração acordada, a exclusão expira e o patch é instalado em qualquer patch subsequente.

Os patches na lista de exclusão ainda são retornados nos resultados da verificação, se aplicável.

Note

Diferentemente do Windows, os patches do Linux são específicos para cada versão. Essa distinção é importante porque novas versões de um patch excluído não são excluídas automaticamente. É sua responsabilidade notificar o AMS para excluir novas versões de um patch do Linux, se é isso que você deseja fazer.

Modelos de resposta de notificação do serviço de patch

Você deve responder às notificações do serviço de patches, usando o formato especificado, para que os patches sejam executados em suas instâncias. Você deve fazer isso se ainda não tiver definido uma janela de manutenção com o AMS.

Ao responder a uma notificação de serviço, use o formato fornecido.

Se nenhuma janela de manutenção estiver definida, informe-nos quando corrigir o que é mostrado a seguir:

UTC	StartTime	StackId	InstanceId (Optional)
2019-04-01	15:00	stack-123456789012	i-1234566789
2019-04-01	15:00	stack-123456789013	i-1234566784
2019-04-01	15:00	stack-123456789014	i-1234566783
2019-04-01	15:00	stack-123456789015	i-1234566782

Se você tiver uma janela de manutenção definida e quiser que determinados recursos sejam excluídos de determinados patches, use o seguinte formato:

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	<i>PATCH</i>
stack-123456789013	i-1234566784	<i>PATCH</i>
stack-123456789014	i-1234566783	<i>PATCH</i>
stack-123456789015	i-1234566782	<i>PATCH</i>

Se você tiver uma janela de manutenção definida e quiser que determinados recursos sejam sempre excluídos de todas as correções, use o seguinte formato:

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	ALL
stack-123456789015	i-1234566782	ALL

Preparando-se para a aplicação de patches

Para preparar seu ambiente para a aplicação automática de patches, recomendamos o seguinte:

- Certifique-se de ter um inventário completo de todas as instâncias a serem corrigidas.
- Garanta que seus recursos sejam copiados regularmente como parte de sua estratégia de continuidade de negócios. Backups adicionais são criados como parte da sequência de patches

e excluídos automaticamente de acordo com sua política de retenção configurada do Patch Orchestrator (o padrão é 60 dias).

- Certifique-se de que todas as licenças relevantes estejam atualizadas.
- Modifique suas janelas de manutenção de pilhas para escalonar a aplicação de patches para que as pilhas de teste sejam corrigidas antes das pilhas de produção. Dessa forma, quaisquer erros com a correção são encontrados nas pilhas de teste e podem ser identificados antes que as pilhas de produção sejam corrigidas.

Visualizando as configurações do patch

Para descobrir qual é sua configuração atual de patches, você pode fazer o seguinte:

- Envie uma solicitação de serviço ao AMS com a consulta.
- Aguarde uma notificação do serviço de patch. O aviso de patch informa sobre todos os patches a serem aplicados e as instâncias a serem corrigidas, além de sugerir uma janela de patch.

Você pode enviar uma solicitação de serviço para modificar o seguinte:

- Intervalo de verificação: a quantidade de tempo, em minutos, entre as verificações de conformidade realizadas em instâncias dessa pilha.

O padrão é 240 (4 horas).

- NotificationWindow: Com que antecedência (em minutos) de uma alteração programada (patch) a notificação deve ser enviada a você. O padrão é 10080 (7 dias).

Correção padrão do AMS FAQs

Esta seção fornece respostas para algumas perguntas frequentes.

- P: Como faço para optar por não aplicar patches globalmente?

R: Para cancelar globalmente a aplicação de patches, registre uma solicitação de serviço. Observe que você não pode optar por não receber os patches obrigatórios do AMS. Todas as pilhas continuarão sendo verificadas para que possamos relatar as vulnerabilidades.

- P: Como excluo pilhas específicas da aplicação de patches?

R: Para excluir permanentemente pilhas específicas da aplicação de patches, envie uma solicitação de serviço. Para excluir determinadas pilhas de um ciclo de patch específico, responda ao próximo aviso de patch com a lista de pilhas a serem excluídas. Para mais informações, consulte [Mudando o que patched/opting sai](#). Observe que você não pode optar por não receber os patches obrigatórios.

- P: O que acontece se eu não aprovar uma notificação de serviço de patches?

R: Você tem 14 dias para aprovar uma solicitação de serviço de patch padrão e 10 dias para aprovar um aviso de patch crítico. Se você não aprovar a solicitação de serviço dentro do prazo, o compromisso de serviço será anulado e nenhuma correção ocorrerá. No caso de patches obrigatórios, os patches são aplicados independentemente da resposta à solicitação de serviço.

- P: Como excluo a instalação de patches e pacotes específicos?

R: Para excluir permanentemente patches ou pacotes específicos, envie uma solicitação de serviço. Para excluir determinados patches ou pacotes de um determinado ciclo de patches, responda ao próximo aviso de patch com a lista de patches ou pacotes a serem excluídos. Para obter detalhes, consulte [Mudando o que patched/opting sai](#). Observe que você não pode optar por não receber os patches obrigatórios.

- P: O que acontece se um sistema falhar como resultado da aplicação de patches?

R: O AMS monitora cada sistema. O AMS envia uma notificação de serviço para você sobre o resultado de cada atualização (ou seja, sucesso ou falha) por pilha e instância. Se uma falha for detectada, o AMS investiga, trabalha para restaurar a instância e, em seguida, um engenheiro de operações do AMS tenta corrigir manualmente. Para mais informações, consulte [Falhas de patches padrão do AMS](#).

- P: Quais atualizações são gerenciadas pelo AMS?

R: O AMS gerencia as atualizações no nível do sistema operacional sobre as quais o AMS é notificado pelo fornecedor. Para obter mais informações, consulte [Patches compatíveis](#).

- P: Quais atualizações não são gerenciadas pelo AMS?

R: As atualizações no nível do aplicativo não são gerenciadas pelo AMS.

- P: Como os grupos do Auto Scaling são atualizados?

R: Os grupos do Auto Scaling são atualizados com uma substituição da AMI na configuração do grupo do Auto Scaling e realizam uma atualização contínua. Uma atualização contínua observa a HealthyHostThreshold configuração de sua configuração de patches, que determina quantas EC2 instâncias da Amazon em uma pilha devem ser mantidas ativas durante a aplicação de patches. Para obter mais informações, consulte [Atualizações e patches da AMI \(usando patches AMIs para grupos de Auto Scaling\)](#).

- P: Como faço para instalar atualizações fora do ciclo normal?

R: Para atualizações no nível do sistema operacional que você deseja instalar fora do cronograma normal de patches, envie uma solicitação de serviço usando a notificação de patch que você recebeu. Isso pode acontecer se o teste de um patch proposto levar mais de 21 dias (para um patch padrão) ou 14 dias (para um patch crítico). Out-of-banda correção pode ser feita localmente para instâncias autônomas da Amazon EC2.

- P: Como as pilhas ou instâncias recém-implantadas são corrigidas?

R: Ao criar uma nova instância do Amazon EC2 Stack ou um grupo de Auto Scaling, você deve sempre especificar a AMI AMI mais recente, que já terá os patches mais recentes nela. Para infraestruturas mutáveis, a correção em linha deve ser executada assim que a pilha for implantada.

Compromissos de serviços de correção

Com base no tipo de implantação da infraestrutura e na criticidade da atualização, oferecemos compromissos de serviço para atualizações críticas de segurança para infraestruturas mutáveis e imutáveis e atualizações importantes para infraestruturas mutáveis e imutáveis.

Aplicação de patches padrão

Esses são os compromissos de serviço do AMS para patches padrão.

Aplicação de patches padrão, infraestrutura mutável (aplicação de patches no local)

Evento/Ação	Medição do compromisso com o serviço
Atualizações importantes são lançadas em um mês.	O relógio começa
Quatorze dias a partir da criação da notificação de patch padrão, o AMS notifica você sobre a próxima correção planejada por meio de uma notificação de serviço e por e-mail para cada pilha. A notificação do serviço inclui: • Uma lista de atualizações IDs (CSUs e IUs) que são aplicáveis (necessárias e não aplicadas) à pilha e aquelas atualizações excluídas do patch • IDs de pilhas afetadas • A janela de manutenção em que as atualizações serão aplicadas	O relógio para após o envio da notificação de serviço.
Você testa o impacto das atualizações e aprova ou rejeita a RFC. Se você não responder dentro de 14 dias ou rejeitar a correção em sua resposta à notificação do serviço, nenhuma ação será tomada. Se você levar mais de 14 dias para testar e quiser que as atualizações sejam aplicadas	Se você não aprovar ou responder dentro de 14 dias, a alteração pendente será cancelada e o compromisso de serviço para as atualizações não será aplicável.

Evento/Ação	Medição do compromisso com o serviço
após o período de 14 dias, envie uma solicitação de serviço para um novo patch RFC com base nos detalhes do RFC anterior.	
Se você aprovar a notificação de serviço dentro de 14 dias, o AMS aplicará as atualizações. Você pode optar por excluir atualizações específicas de uma RFC especificando as atualizações a serem excluídas em sua resposta à notificação do serviço.	O relógio começa se você aprovar a notificação de serviço dentro de 14 dias após o recebimento. O relógio para após a tentativa de instalação da atualização.
O AMS envia uma notificação de serviço para você sobre o resultado de cada tentativa de atualização. A notificação de serviço inclui os seguintes detalhes: • ID da EC2 instância Amazon • Sucesso/falha na atualização 1: ARN a1, ARN a2... • Sucesso/falha na atualização 2: ARN b1, ARN b2... • Sucesso/falha na atualização N: ARN c1, ARN c2...	Não aplicável.
Em caso de falha nas atualizações, o AMS realiza uma análise para entender a causa da falha e comunica o resultado da análise a você. Se a falha for atribuível ao AMS, o AMS tentará novamente as atualizações se estiver dentro da janela de manutenção, caso contrário, o AMS criará notificações de serviço para a combinação de instância-atualização com falha e aguardará suas instruções em uma janela de manutenção.	Não aplicável.

Evento/Ação	Medição do compromisso com o serviço
Para falhas atribuíveis a você, envie uma solicitação de serviço para um novo patch RFC para atualizar as instâncias.	Não aplicável.

Correção crítica

Esses são compromissos de serviço do AMS para atualizações críticas de segurança.

Atualizações críticas de segurança, infraestrutura mutável

Evento/Ação	Medição do compromisso com o serviço
CSU é lançado.	O relógio começa
O AMS notifica você sobre o patch RFC por meio de uma notificação de serviço (que também envia um e-mail) para cada pilha. A notificação do serviço inclui: • Atualiza a data de lançamento • Criticidade da atualização • Detalhes da atualização: referência de KB e assim por diante • IDs de pilhas afetadas	O relógio para após o envio da notificação do serviço.
Você testa as atualizações listadas na RFC e aprova ou rejeita a RFC em 10 dias, respondendo à notificação de serviço. Você fornece uma janela de manutenção específica (por pilha) para instalar as atualizações. As janelas de manutenção especificadas dentro de 24 horas após a resposta à notificação de serviço podem ser reprogramadas com base na capacidade disponível.	Se você não aprovar ou responder dentro de 14 dias, a alteração pendente será cancelada e o compromisso de serviço para a atualização não será aplicável.

Evento/Ação	Medição do compromisso com o serviço
Se você não responder dentro de 10 dias ou se rejeitar a RFC do patch, a ação pendente será cancelada. Se você quiser aplicar as atualizações após o período de 14 dias, envie uma solicitação de serviço para um novo patch RFC com base nos detalhes do RFC anterior.	
Se você aprovar a notificação de serviço, o AMS aplicará as atualizações. Para várias atualizações, você pode optar por excluir atualizações específicas da alteração especificando as atualizações a serem excluídas em sua resposta à notificação do serviço.	Se a janela de manutenção desejada não estiver dentro do prazo de compromisso de serviço, o compromisso de serviço para a atualização será perdido somente se a RFC não for executada dentro da janela de manutenção desejada.
O AMS envia uma notificação de serviço para você sobre o resultado de cada atualização aplicada. A notificação de serviço inclui os seguintes detalhes: • ID da EC2 instância Amazon • Sucesso da atualização: ARN a1, ARN a2... • Falha na atualização: ARN c1, ARN c2...	Não aplicável.

Evento/Ação	Medição do compromisso com o serviço
Em caso de falha nas atualizações, o AMS realiza uma análise para entender a causa da falha e comunica o resultado da análise a você. Se a falha for atribuível ao AMS, o AMS tentará novamente as atualizações se estiver dentro da janela de manutenção, caso contrário, o AMS criará notificações de serviço para a combinação falhada de instância-atualização e aguardará suas instruções em uma nova janela de manutenção.	Não aplicável.
Para falhas atribuíveis a você, envie uma solicitação de serviço para um novo patch RFC para atualizar as instâncias.	Não aplicável.

Atualizações críticas de segurança, infraestrutura imutável

Evento/Ação	Medição do compromisso com o serviço
CSU é lançado.	O relógio começa
O AMS notifica você do seguinte por meio de uma notificação de serviço: • Atualizar data de lançamento • Criticidade da atualização • Detalhes da atualização (referência de KB e assim por diante) • AMS Amazon Machine Images (AMI) impactadas • Data e hora de lançamento previstas para a nova atualização AMIs	O relógio continua funcionando.
Versões do AMS atualizadas AMIs na conta gerenciada.	O relógio para.

Evento/Ação	Medição do compromisso com o serviço
Se você aprovar a notificação de serviço, o AMS aplicará as atualizações. O AMS notifica você sobre o AMIs compartilhamento em sua conta, por meio de uma notificação de serviço e por e-mail.	Não aplicável.
Se o teste do novo AMIs demorar mais do que o tempo estipulado (uma semana), você poderá enviar uma solicitação de serviço ao AMS para atualizar seus grupos de Auto Scaling com o novo AMI do AMS (no estado em que se encontra). Se você quiser modificar a nova AMI do AMS com suas configurações, use um RFC com Management Other Other Update CT (ct-0xdawir96cy7k) para solicitar que atualizemos seus grupos do Auto Scaling.	Não aplicável.

Relatórios e opções

O AWS Managed Services (AMS) coleta dados de vários serviços nativos da AWS para fornecer relatórios de valor agregado sobre as principais ofertas de AMS.

O AMS oferece dois tipos de relatórios detalhados:

- **Relatórios sob solicitação:** você pode solicitar determinados relatórios ad hoc por meio do Cloud Service Delivery Manager (CSDM). Esses relatórios não têm limite porque talvez você precise solicitá-los várias vezes durante a integração ou em eventos críticos. No entanto, esteja ciente de que esses relatórios não foram projetados para serem fornecidos em um cronograma, como os relatórios semanais. Para entender melhor suas necessidades ou obter mais informações sobre o uso de relatórios de autoatendimento, entre em contato com seu CSDM.
- **Relatórios de autoatendimento:** os relatórios de autoatendimento do AMS permitem que você consulte e analise dados diretamente sempre que precisar. Use relatórios de autoatendimento para acessar relatórios do console AMS e conjuntos de dados de relatórios por meio de buckets do S3 (um bucket por conta). Isso permite que você integre os dados em sua ferramenta de Business Intelligence (BI) favorita para que você possa personalizar relatórios de acordo com suas necessidades.

Tópicos

- [Relatórios sob solicitação](#)
- [Relatórios de autoatendimento](#)

Relatórios sob solicitação

Tópicos

- [Relatórios do AMS Patch](#)
- [Relatórios de backup do AMS](#)
- [Incidentes evitados e monitoramento dos relatórios do Top Talkers](#)
- [Relatório de detalhes de cobranças](#)
- [Relatórios do Trusted Remediator](#)

O AMS coleta dados de vários serviços nativos da AWS para fornecer relatórios de valor agregado sobre as principais ofertas do AMS. Para obter uma cópia desses relatórios, faça uma solicitação ao seu Cloud Service Delivery Manager (CSDM).

Relatórios do AMS Patch

Relatórios disponíveis

- [Relatório resumido de detalhes da instância de patch](#)
- [Relatório de detalhes do patch](#)
- [Relatório de instâncias que perderam os patches](#)
- [Corrigindo o relatório de cobertura do SSM](#)

Relatório resumido de detalhes da instância de patch

O relatório Resumo dos Detalhes da Instância de Patch fornece detalhes da instância coletados para instâncias que estão integradas ao relatório. Esse é um relatório informativo que ajuda a identificar todas as instâncias integradas, o status da conta, os detalhes da instância, a cobertura da janela de manutenção, o tempo de execução da janela de manutenção, os detalhes da pilha e o tipo de plataforma. Esse relatório fornece o seguinte:

1. Dados sobre as instâncias de produção e não produção de uma conta. Observação: o estágio de produção e não produção é derivado do nome da conta e não das tags de instância.
2. Dados sobre a distribuição de instâncias por tipo de plataforma. Observação: o tipo de plataforma 'N/A' é quando não AWS Systems Manager consigo recuperar as informações da plataforma.
3. Dados sobre a distribuição do estado das instâncias e o número de instâncias em execução, paradas ou encerradas.

Nome do campo	Definição
Data e hora do relatório	A data e a hora em que o relatório foi gerado.
ID da conta	ID da conta da AWS à qual o ID da instância pertence
Nome da conta	Nome da conta da AWS

Nome do campo	Definição
Conta de produção	Identificador de contas produtivas e não produtivas do AMS, dependendo se o nome da conta inclui o valor 'PROD', 'NONPROD'. Exemplo: PROD, NONPROD, não disponível
Status da conta	Status da conta AMS. Por exemplo: ATIVO, INATIVO
Compromisso de serviço da conta AMS	PREMIUM, MAIS
Zona de pouso	Sinalizar o tipo de landing zone da conta. Por exemplo: MALZ, NON-MALZ
Restrições de acesso	Regiões às quais o acesso é restrito. Por exemplo: US SOIL
ID da instância	ID da EC2 instância
Nome da instância	Nome da EC2 instância
Tipo de plataforma de instância	Tipo de sistema operacional (SO). Por exemplo: Windows, Linux e assim por diante
Nome da plataforma da instância	Nome do sistema operacional (SO). Por exemplo: MicrosoftWindowsServer 2012R2Standard, RedHatEnterpriseLinuxServer
Stack Name	Nome da pilha que contém a instância
Tipo de pilha	Pilha AMS (infraestrutura AMS dentro da conta do cliente) ou pilha de clientes (infraestrutura gerenciada pelo AMS que dá suporte aos aplicativos do cliente). Exemplos: AMS, CUSTOMER
Nome do grupo do Auto Scaling	Nome do Auto Scaling Group (ASG) que contém a instância

Nome do campo	Definição
Grupo de patches de instância	Nome do grupo de patches usado para agrupar instâncias e aplicar a mesma janela de manutenção. Se o grupo de patches não estiver atribuído, o valor será “Não atribuído”
Tipo de grupo de patches de instância	Tipo de grupo de patches. DEFAULT: grupo de patches padrão com a janela de manutenção padrão, determinada pela <code>AMSDefaultPatchGroup:True</code> tag na instância. CLIENTE: grupo de patches criado pelo cliente. NOT_ASSIGNED: nenhum grupo de patch atribuído
Estado da instância	Estado dentro do ciclo de vida da EC2 instância. Exemplos: ENCERRADO, EM EXECUÇÃO, PARADO, PARADO, ENCERRADO, PENDENTE. Para obter mais informações, consulte Ciclo de vida da instância.
Cobertura da janela de manutenção	Se houver uma janela de manutenção futura nessa instância. Exemplos: COVERED ou NOT_COVERED
Data e hora de execução da janela de manutenção	Na próxima vez, espera-se que a janela de manutenção seja executada. Se for NULL, execução em janela única, ou seja, não recorrente

Relatório de detalhes do patch

O relatório de detalhes do patch do AWS Managed Services (AMS) fornece detalhes do patch e cobertura da janela de manutenção de várias instâncias, incluindo:

1. Dados sobre grupos de patches e seus tipos.
2. Dados sobre janelas de manutenção, duração, limite, datas futuras de execuções da janela de manutenção (cronograma) e instâncias afetadas em cada janela.
3. Dados sobre todos os sistemas operacionais da conta e o número de instâncias em que esse sistema operacional está instalado.

Nome do campo	Definição
Data e hora do relatório	A data e a hora em que o relatório foi gerado.
ID da conta	ID da conta da AWS à qual o ID da instância pertence
Nome da conta	Nome da conta da AWS
ID da instância	ID da EC2 instância
Conta de produção	Identificador de contas produtivas e não produtivas do AMS, dependendo se o nome da conta inclui o valor 'PROD', 'NONPROD'. Se os dados não estiverem disponíveis, o valor será “Não disponível”
Status da conta	Status da conta AMS. Por exemplo: ATIVO, INATIVO
Tipo de plataforma de instância	Tipo de sistema operacional (SO). Por exemplo: Windows, Linux
Nome da plataforma da instância	Nome do sistema operacional (SO). Por exemplo: MicrosoftWindowsServer 2012R2Standard, RedHatEnterpriseLinuxServer

Nome do campo	Definição
Tipo de pilha	Pilha AMS (infraestrutura AMS dentro de uma conta de cliente) ou pilha de clientes (infraestrutura gerenciada pelo AMS que dá suporte aos aplicativos do cliente). Por exemplo: AMS, CUSTOMER
Grupo de patches de instância	Nome do grupo de patches usado para agrupar instâncias e aplicar a mesma janela de manutenção. Se o grupo de patches não estiver atribuído, o valor será “Não atribuído”
Tipo de grupo de patches de instância	Tipo de grupo de patches. DEFAULT: grupo de patches padrão com janela de manutenção padrão, determinado pela <code>AMSDefaultPatchGroup:True</code> tag na instância CLIENTE: grupo de patches criado pelo cliente NÃO ATRIBUÍDO: nenhum grupo de patch atribuído
Estado da instância	Estado dentro do ciclo de vida da EC2 instância. Por exemplo: ENCERRADO, EM EXECUÇÃO, PARADO, PARADO, ENCERRADO, PENDENTE Para obter mais informações, consulte Ciclo de vida da instância.
ID da janela de manutenção	Identificador da janela de manutenção
Estado da janela de manutenção	Os valores possíveis são HABILITADO ou DESATIVADO.
Tipo de janela de manutenção	Tipo de janela de manutenção

Nome do campo	Definição
Janela de manutenção: próxima data de execução	Na próxima vez, espera-se que a janela de manutenção seja executada. Se for NULL, execução em janela única, ou seja, não recorrente
Janela de manutenção da última execução	A última vez em que a janela de manutenção foi executada
Duração da janela de manutenção (horas)	A duração da janela de manutenção em horas
Cobertura da janela de manutenção	A cobertura da janela de manutenção
ID da linha de base do patch	Linha de base do patch atualmente anexada à instância
Status do patch	Status geral de conformidade do patch. Por exemplo: COMPLIANT, NON_COMPLIANT. Se houver pelo menos um patch ausente, a instância será considerada não compatível, caso contrário, compatível.
Compatível - Total	Contagem de patches compatíveis (todas as gravidades)
Não compatível - Total	Contagem de patches não compatíveis (todas as gravidades)
Compatível - Crítico	Contagem de patches compatíveis com severidade “crítica”
Compatível - Alto	Contagem de patches compatíveis com severidade “alta”
Compatível - Médio	Contagem de patches compatíveis com severidade “média”

Nome do campo	Definição
Compatível - Baixo	Contagem de patches compatíveis com severidade “baixa”
Compatível - Informativo	Contagem de patches compatíveis com severidade “informativa”
Compatível - Não especificado	Contagem de patches compatíveis com severidade “não especificada”
Incompatível - Crítico	Contagem de patches não compatíveis com severidade “crítica”
Não compatível - Alto	Contagem de patches não compatíveis com severidade “alta”
Não compatível - Médio	Contagem de patches não compatíveis com severidade “média”
Não compatível - Baixo	Contagem de patches não compatíveis com severidade “baixa”
Incompatível - Informativo	Contagem de patches não compatíveis com severidade “informativa”
Não compatível - Não especificado	Contagem de patches não compatíveis com severidade “não especificada”

Relatório de instâncias que perderam os patches

O relatório AWS Managed Services (AMS) Instances That Missed Patches fornece detalhes sobre instâncias que perderam patches durante a execução da última janela de manutenção, incluindo:

1. Dados sobre patches ausentes no nível da ID do patch.
2. Dados sobre todas as instâncias que têm pelo menos um patch ausente, juntamente com atributos como gravidade do patch, dias sem patch, intervalo e data de lançamento do patch.

Nome do campo	Definição
Data e hora do relatório	A data e a hora em que o relatório foi gerado.
ID da conta	ID da conta da AWS à qual o ID da instância pertence
Nome da conta	Nome da conta da AWS
Conta de produção	Identificador de contas produtivas e não produtivas do AMS, dependendo se o nome da conta inclui o valor 'PROD', 'NONPROD'.
Status da conta	Status da conta AMS. Por exemplo: ATIVO ou INATIVO
Nível de serviço da conta AMS	PREMIUM ou PLUS
ID da instância	ID da EC2 instância
Tipo de plataforma de instância	Tipo de sistema operacional (SO). Por exemplo: Windows
Estado da instância	Estado do ciclo de vida da EC2 instância . Por exemplo: TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING Para obter mais informações, consulte Ciclo de vida da instância .
ID do patch	ID do patch lançado. Por exemplo: KB3172729
Gravidade do patch	Gravidade do patch por editor. Por exemplo: CRÍTICO, IMPORTANTE, MODERADO, BAIXO, NÃO ESPECIFICADO
Classificação de patches	Classificação do patch por editor. Por exemplo: ATUALIZAÇÕES CRÍTICAS, ATUALIZAÇÕES DE SEGURANÇA, UPDATEROLLUPS, ATUALIZAÇÕES, PACOTES DE RECURSOS

Nome do campo	Definição
Data e hora do lançamento do patch (UTC)	Data de lançamento do patch por editor
Estado de instalação do patch	Instale o estado do patch na instância por SSM. Por exemplo: INSTALADO, AUSENTE, NÃO APLICÁVEL
Dias sem correção	Número de dias em que a instância não foi corrigida desde a última verificação de SSM
Intervalo de dias sem correção	Período de dias sem correção. Por exemplo: <30 DIAS, 30-60 DIAS, 60-90 DIAS, 90+ DIAS

Corrigindo o relatório de cobertura do SSM

O relatório AMS Patching SSM Coverage informa se as EC2 instâncias na conta têm ou não o SSM Agent instalado.

Nome do campo	Definição
Nome do cliente	Nome do cliente para situações em que há vários subclientes
Região de recursos	AWS Região em que o recurso está localizado
Nome da conta	O nome da conta
AWS ID da conta	O ID da AWS conta
ID de recurso	ID da EC2 instância
Nome do recurso	Nome da EC2 instância
Bandeira compatível	Indica se o recurso tem o Agente SSM instalado (“Compatível”) ou não (“NÃO COMPATÍVEL”)

Relatórios de backup do AMS

Relatórios disponíveis

- [Relatório de sucesso/falha do Backup Job](#)
- [Relatório resumido do backup](#)
- [Summary/Coverage Relatório de backup](#)

Relatório de sucesso/falha do Backup Job

O Success/Failure relatório Backup Job fornece informações sobre backups executados nas últimas semanas. Para personalizar o relatório, especifique o número de semanas para as quais você deseja recuperar dados. O número padrão de semanas é 12. A tabela a seguir lista os dados incluídos no relatório:

Nome do campo	Definição
ID da conta da AWS	ID da conta da AWS à qual o recurso pertence
Nome da conta	Nome da conta da AWS
ID do Backup Job	O ID da tarefa de Backup
ID do recurso	O ID do recurso de backup
Tipo de recurso	O tipo de recurso que está sendo copiado
Região de recursos	A AWS região do recurso de backup
Estado do backup	O estado do backup. Para obter mais informações, consulte Status da tarefa de backup
ID do ponto de recuperação	O identificador exclusivo do ponto de recuperação
Mensagem de status	Descrição dos erros ou avisos que ocorreram durante a tarefa de backup

Nome do campo	Definição
Tamanho do backup	Tamanho do backup em GB
ARN do ponto de recuperação	O ARN do backup criado
Idade do ponto de recuperação em dias	Número de dias que passaram desde a criação do ponto de recuperação
Menos de 30 dias	Indicador de backups com menos de 30 dias

Relatório resumido do backup

Nome do campo	Definição
Nome do cliente	Nome do cliente para situações em que vários subclientes estão
Mês do backup	Mês do backup
Ano de backup	Ano do backup
Tipo de recurso	O tipo de recurso que está sendo copiado
Nº de recursos	O número de recursos que foram copiados
Nº de pontos de recuperação	Número de instantâneos distintos
Backups com menos de 30 dias	A contagem de backups com menos de 30 dias
Idade máxima do ponto de recuperação	A idade mais antiga do ponto de recuperação em dias
Idade mínima do ponto de recuperação	A idade mais recente do ponto de recuperação em dias

Summary/Coverage Relatório de backup

O Summary/Coverage relatório de Backup lista quantos recursos não estão atualmente protegidos por nenhum AWS Backup plano. Discuta com seu CDSM um plano apropriado para aumentar a cobertura, sempre que possível, e reduzir o risco de perda de dados.

Nome do campo	Definição
Nome do cliente	Nome do cliente para situações em que vários subclientes estão
Região	AWS região em que o recurso está localizado
Nome da conta	O nome da conta
AWS ID da conta	O ID da AWS conta
Tipo de recurso	Tipo de recurso. Os recursos são suportados por AWS Backup (Aurora, DocumentDB, DynamoDB, EBS, EFS, RDS e EC2 S3) FSx
Atributo ARN	ARN do recurso
ID do recurso	ID do recurso
Cobertura	Indica se o recurso está coberto ou não ("COVERED" ou "NOT_COVERED")
Nº de recursos	Número de recursos suportados na conta
cobertura por cento	Porcentagem de recursos suportados com um backup executado nos últimos 30 dias.

Incidentes evitados e monitoramento dos relatórios do Top Talkers

Relatórios disponíveis

- [Relatório de incidentes evitados](#)
- [Monitorando o relatório Top Talkers](#)

Relatório de incidentes evitados

O relatório Incidentes evitados lista os CloudWatch alarmes da Amazon que foram corrigidos automaticamente, evitando um possível incidente. Para saber mais, consulte [Remediação automática](#). A tabela a seguir lista as informações incluídas nesse relatório:

Nome do campo	Definição
horário_de_inicio_utc	Data em que a automação foi executada
customer_name	Nome do cliente da conta
account_name	O nome da conta
AwsAccountId	O ID da conta da AWS
nome_documento	O nome do documento SSM ou da automação executada
duração_em_minutos	A duração da automação em minutos
Região	AWS Região em que o recurso está localizado
id_de_execução de automação	O ID da execução
status de execução_de_automação	O status da execução

Monitorando o relatório Top Talkers

O relatório Monitoring Top Talkers apresenta o número de CloudWatch alertas da Amazon gerados durante um período específico e fornece visualizações dos recursos que geram o maior número de alertas. Esse relatório ajuda você a identificar os recursos que geram o maior número de alertas. Esses recursos podem ser candidatos para realizar a análise de causa raiz para remediar o problema ou modificar os limites de alarme para evitar acionadores desnecessários quando não há um problema real. A tabela a seguir lista as informações incluídas nesse relatório:

Nome do campo	Definição
Nome do cliente	Nome do cliente

Nome do campo	Definição
AccountId	O ID da AWS conta
Categoria de alerta	O tipo de alerta acionado
Descrição	Descrição do alerta
ID do recurso	ID do recurso que acionou o alerta
Nome do recurso	Nome do recurso que acionou o alerta
Região	AWS Região em que o recurso está localizado
Status do incidente	Status mais recente do incidente gerado pelo alarme
Primeira ocorrência	Primeira vez que o alerta foi acionado
Ocorrência recente	A última vez em que o alerta foi acionado
Contagem de alertas	Número de alertas gerados entre a primeira ocorrência e a recente

Relatório de detalhes de cobranças

O relatório AWS Managed Services (AMS) Billing Charges Details fornece detalhes sobre as cobranças de faturamento do AMS com contas vinculadas e os respectivos serviços da AWS, incluindo:

- Taxas de nível de serviço do AMS, porcentagens de aumento, níveis de serviço do AMS no nível da conta e taxas do AMS.
- Contas vinculadas e cobranças AWS de uso

Nome do campo	Definição
Mês de cobrança	O mês e o ano do serviço cobrado

Nome do campo	Definição
ID da conta do pagador	O ID de 12 dígitos que identifica a conta que será responsável pelo pagamento das cobranças do AMS
ID da conta vinculada	O ID de 12 dígitos que identifica a conta AMS que consome serviços que geram despesas
AWS Nome do serviço	O AWS serviço que foi usado
AWS Cobranças	As AWS cobranças pelo nome do AWS serviço listado em Nome do AWS serviço
Plano de preços	O nome do plano de preços associado à conta vinculada
Proporção de elevação	A porcentagem de aumento (como um V.WXYZ decimal) com base no pricing_plan, no SLA e no serviço da AWS
AWS Cobranças ajustadas	AWS uso ajustado para AMS
Cobranças aumentadas da AWS	A porcentagem das cobranças da AWS a serem cobradas pelo AMS; $\text{adjusted\_aws\_charges} * \text{uplift\_percent}$
Gastos do EC2 RDS em instâncias	Gastos em EC2 instâncias do RDS e suas
Taxas do AMS	Total de cobranças do AMS pelo produto; $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$
Taxa mínima proporcional	O valor que cobramos para atender ao mínimo contratual
Taxa mínima	Taxas mínimas do AMS (se aplicável)
Total de cobranças AMS da conta vinculada	Soma de todas as cobranças da linked_account

Nome do campo	Definição
Total de cobranças de AMS da conta do pagador	Soma de todas as cobranças da conta do pagador

Relatórios do Trusted Remediator

Relatórios disponíveis

- [Relatório resumido de remediação do Trusted Remediator](#)
- [Relatório resumido da configuração do Trusted Remediator](#)
- [Trusted Advisor Verifique o relatório resumido](#)

Relatório resumido de remediação do Trusted Remediator

O relatório de status de remediação do Trusted Remediator fornece informações sobre as remediações que ocorreram durante os ciclos de remediação anteriores. O número padrão de semanas é 1. Para personalizar o relatório, especifique o número de semanas com base no seu cronograma de remediação.

Nome do campo	Definição
Data	A data em que os dados foram coletados.
ID da conta	O ID AWS da conta à qual o recurso pertence
Nome da conta	O nome AWS da conta
Verifique a categoria	A categoria de AWS Trusted Advisor cheques
Verifique o nome	O nome do cheque corrigido Trusted Advisor
ID da verificação	O ID do cheque corrigido Trusted Advisor
Modo de execução	O modo de execução que foi configurado para a Trusted Advisor verificação específica

Nome do campo	Definição
OpsItem ID	O ID do OpsItem criado por Trusted Advisor para remediação
OpsItem Status	O status do OpsItem criado por Trusted Advisor no momento do relatório
ID do recurso	O ARN do recurso criado para remediação

Relatório resumido da configuração do Trusted Remediator

O relatório Resumo da Configuração do Trusted Remediator fornece informações sobre as configurações atuais do Trusted Remediator Remediation para cada verificação. Trusted Advisor

Nome do campo	Definição
Data	A data em que os dados foram coletados.
ID da conta	A ID AWS da conta à qual a configuração se aplica
Nome da conta	O nome AWS da conta
Verifique a categoria	A categoria de AWS Trusted Advisor cheques
Verifique o nome	O nome da Trusted Advisor verificação corrigida à qual a configuração se aplica
ID da verificação	O ID da Trusted Advisor verificação corrigida à qual a configuração se aplica
Modo de execução	O modo de execução que foi configurado para a Trusted Advisor verificação específica
Substituir para automatizado	O padrão de tag, se configurado, para substituir o modo de execução para Automatizado

Nome do campo	Definição
Substituir para manual	O padrão de tag, se configurado, para substituir o modo de execução para Manual

Trusted Advisor Verifique o relatório resumido

O relatório de resumo da Trusted Advisor verificação fornece informações sobre as Trusted Advisor verificações atuais. Esse relatório coleta dados após cada cronograma semanal de remediação. O número padrão de semanas é 1. Para personalizar o relatório, especifique o número de semanas com base no seu ciclo de remediação.

Nome do campo	Definição
Data	A data em que os dados foram coletados.
ID da conta	A ID AWS da conta à qual a configuração se aplica
Nome do cliente	O nome AWS da conta
Verifique a categoria	A categoria de AWS Trusted Advisor cheques
Verifique o nome	O nome da Trusted Advisor verificação corrigida à qual a configuração se aplica
ID da verificação	O ID da Trusted Advisor verificação corrigida à qual a configuração se aplica
Status	O status do alerta da verificação. Os status possíveis são ok (verde), aviso (amarelo), erro (vermelho) ou not_available
Recursos sinalizados	O número de AWS recursos que foram sinalizados (listados) pela Trusted Advisor verificação.

Nome do campo	Definição
Recursos ignorados	O número de AWS recursos que foram ignorados Trusted Advisor porque você os marcou como suprimidos.
Recursos em estado crítico	O número de recursos em estado crítico
Recursos em estado de alerta	O número de recursos em estado de alerta

Relatórios de autoatendimento

Os relatórios de autoatendimento (SSR) do AWS Managed Services (AMS) são um recurso que coleta dados de vários AWS serviços nativos e fornece acesso a relatórios sobre as principais ofertas do AMS. O SSR fornece informações que você pode usar para apoiar operações, gerenciamento de configuração, gerenciamento de ativos, gerenciamento de segurança e conformidade.

Use o SSR para acessar os relatórios do console do AMS e os conjuntos de dados de relatórios por meio de buckets do Amazon S3 (um bucket por conta). Você pode conectar os dados à sua ferramenta de business intelligence (BI) favorita para personalizar os relatórios com base em suas necessidades exclusivas. O AMS cria esse bucket do S3 (nome do bucket do S3: (ams-reporting-data-a<Account_ID>)) na sua AWS região principal, e os dados são compartilhados do plano de controle do AMS hospedado na região us-east-1.

Important

Para acessar esse recurso, você deve ter uma das seguintes funções:

- Zona de aterrissagem com várias contas: AWSManagedServicesReadOnlyRole
- Zona de destino de conta única: ReadOnlyCliente_ _Função

Important

Usando teclas personalizadas com AWS Glue

Para criptografar seus AWS Glue metadados com uma chave KMS gerenciada pelo cliente, você deve executar as seguintes etapas adicionais para permitir que o AMS agregue dados da conta:

1. Abra o AWS Key Management Service console em <https://console.aws.amazon.com/kms> e escolha Chaves gerenciadas pelo cliente.
2. Selecione a ID da chave que você planeja usar para criptografar os AWS Glue metadados.
3. Escolha a guia Aliases e, em seguida, escolha Criar alias.
4. Na caixa de texto AmsReportingFlywheelCustomKey, insira e escolha Criar alias.

Tópicos

- [Operações internas de API](#)
- [Relatório de patch \(diário\)](#)
- [Relatório de backup \(diário\)](#)
- [Relatório de incidentes \(semanal\)](#)
- [Relatório de cobrança \(mensal\)](#)
- [Relatórios agregados](#)
- [Painéis de relatórios de autoatendimento do AMS](#)
- [Política de retenção de dados](#)
- [Fora do SSR](#)

Operações internas de API

Se você monitorar as operações da API, poderá ver chamadas para as seguintes operações somente internas:

- `GetDashboardUrl`
- `ListReportsV2`

Operação interna da API: `GetDashboardUrl`

Essa operação aparece nos registros do sistema quando invocada pelo console AMS. Não tem outro caso de uso. Ele não está disponível para seu uso direto.

Retorna o URL do painel incorporado para o relatório correspondente. Esta operação aceita um `dashboardName` retorno de `ListReports`.

Sintaxe da solicitação

```
HTTP/1.1 200
Content-type: application/json
{
  "dashboardName": "string"
}
```

Elementos de solicitação

dashboardName: o nome do QuickSight painel para o qual o URL está sendo solicitado. O nome do painel é retornado na ListReports V2.

Tipo: String

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200. Os dados a seguir são retornados no formato JSON pelo serviço.

url: retorna a QuickSight URL da solicitação dashboardName.

Tipo: String

Erros

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#).

BadRequestException:

A solicitação enviada não é válida. Por exemplo, se a entrada estiver incompleta ou incorreta. Consulte a mensagem de erro anexa para obter detalhes.

Código de status HTTP: 400

NotFoundException:

O recurso solicitado não foi encontrado. Verifique se o URI da solicitação está correto.

Código de status HTTP: 404

TooManyRequestsException:

A solicitação atingiu seu limite de limitação. Tente novamente após o período especificado.

Código de status HTTP: 429

UnauthorizedException:

A solicitação é negada porque o chamador não tem permissões suficientes.

Código de status HTTP: 401

Operação interna da API: ListReports V2

Essa API aparece nos registros do sistema quando invocada pelo console do AMS. Não tem outro caso de uso. Ele não está disponível para seu uso direto.

Retorna uma lista de relatórios operacionais que estão disponíveis para uma conta especificada.

Sintaxe da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
      "dashboard": "string",
      "lastUpdatedTime": "string",
    }
  ],
  "reportsType": "string"
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200. Os dados a seguir são retornados no formato JSON pelo serviço.

reportsList: A lista de relatórios operacionais disponíveis.

Tipo: Matriz de objetos do Dashboard

reportsType: indica se um relatório está agregado em várias contas ou não.

Tipo: String

Erros

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#).

BadRequestException:

A solicitação enviada não é válida. Por exemplo, a entrada está incompleta ou incorreta. Consulte a mensagem de erro anexa para obter detalhes.

Código de status HTTP: 400

NotFoundException:

O recurso solicitado não foi encontrado. Verifique se o URI da solicitação está correto.

Código de status HTTP: 404

TooManyRequestsException:

A solicitação atingiu seu limite de limitação. Tente novamente após o período especificado.

Código de status HTTP: 429

UnauthorizedException:

A solicitação é negada porque o chamador não tem permissões suficientes.

Código de status HTTP: 401

Relatório de patch (diário)

Relatórios disponíveis

-
- [Detalhes do patch](#)
- [Instâncias que perderam os patches](#)

Esse é um relatório informativo que ajuda a identificar todas as instâncias integradas ao Patch Orchestrator (PO), o status da conta, os detalhes da instância, a cobertura da janela de manutenção, o tempo de execução da janela de manutenção, os detalhes da pilha e o tipo de plataforma.

Esse conjunto de dados fornece:

- Dados sobre as instâncias de produção e não produção de uma conta. O estágio de produção e não produção é derivado do nome da conta e não das tags da instância.
- Dados sobre a distribuição de instâncias por tipo de plataforma. O tipo de plataforma 'N/A' ocorre quando o AWS Systems Manager (SSM) não consegue obter as informações da plataforma.
- Dados sobre a distribuição do estado das instâncias, o número de instâncias em execução, paradas ou encerradas.

Nome do campo do console	Nome do campo do conjunto de dados	Definição
Restrições de acesso	restrições_de acesso	Regiões às quais o acesso é restrito
ID da conta	aws_account_id	AWS ID da conta à qual a ID da instância pertence
ID da conta de administrador	aws_admin_account_id	AWS Organizations Conta confiável ativada por você.
Nome da conta	account_name	AWS nome da conta
Status da conta	status da conta	Status da conta AMS
	conta_sla	Compromisso de serviço da conta AMS
Tipo de conta	malz_role	Papel do MALZ
Nome do grupo do Auto Scaling	instance_asg_name	Nome do Auto Scaling Group (ASG) que contém a instância
ID da instância	instance_id	ID da EC2 instância

Nome do campo do console	Nome do campo do conjunto de dados	Definição
Nome da instância	nome_instância	Nome da EC2 instância
Grupo de patches de instância	grupo_patch_instância	Nome do grupo de patches usado para agrupar instâncias e aplicar a mesma janela de manutenção
Tipo de grupo de patches de instância	tipo de grupo_patch_de_instância	Tipo de grupo de patches
Tipo de plataforma de instância	tipo_de_plataforma de instância	Tipo de sistema operacional (OS)
Nome da plataforma da instância	nome_da_plataforma da instância	Nome do sistema operacional (SO)
Estado da instância	estado_instância	Estado dentro do ciclo de vida da EC2 instância
Tags de instância	ec2_tags	As tags associadas ao ID da EC2 instância da Amazon
Zona de pouso	bandeira_mala	Bandeira para conta relacionada a Malz
Cobertura da janela de manutenção	bandeira mw_covered_	Se uma instância tiver pelo menos uma janela de manutenção habilitada com uma data de execução futura, ela será considerada coberta, caso contrário, não coberta
Data e hora de execução da janela de manutenção	Horário de execução mais precoce da janela	Na próxima vez, espera-se que a janela de manutenção seja executada

Nome do campo do console	Nome do campo do conjunto de dados	Definição
Data e hora de execução da janela de manutenção	Horário de execução mais precoce da janela	Na próxima vez, espera-se que a janela de manutenção seja executada
Conta de produção	conta_produto	Identificador de contas produtivas e não produtivas do AMS, dependendo se o nome da conta inclui o valor 'PROD', 'NONPROD'.
Data e hora do relatório	dataset_datetime	A data e a hora em que o relatório foi gerado.
Stack Name	nome_da_pilha da instância	Nome da pilha que contém a instância
Tipo de pilha	tipo de pilha de instância	Pilha AMS (infraestrutura AMS dentro da conta do cliente) ou pilha de clientes (infraestrutura gerenciada pelo AMS que oferece suporte aos aplicativos do cliente)

Detalhes do patch

Esse relatório fornece detalhes do patch e cobertura da janela de manutenção de várias instâncias.

Esse relatório fornece:

- Dados sobre grupos de patches e seus tipos.
- Dados sobre janelas de manutenção, duração, limite, datas futuras de execuções da janela de manutenção (cronograma) e instâncias afetadas em cada janela.
- Dados sobre todos os sistemas operacionais da conta e o número de instâncias em que o sistema operacional está instalado.

Nome do campo	Nome do campo do conjunto de dados	Definição
Data e hora do relatório	dataset_datetime	A data e a hora em que o relatório foi gerado.
ID da conta	aws_account_id	AWS ID da conta à qual a ID da instância pertence
Nome da conta	account_name	AWS nome da conta
Status da conta	status da conta	Status da conta AMS
Compatível - Crítico	compatível_crítico	Contagem de patches compatíveis com severidade “crítica”
Compatível - Alto	compliant_high	Contagem de patches compatíveis com severidade “alta”
Compatível - Médio	médio_compatível	Contagem de patches compatíveis com severidade “média”
Compatível - Baixo	compliant_low	Contagem de patches compatíveis com severidade “baixa”
Compatível - Informativo	informativo compatível	Contagem de patches compatíveis com severidade “informativa”
Compatível - Não especificado	compatível_não especificado	Contagem de patches compatíveis com severidade “não especificada”

Nome do campo	Nome do campo do conjunto de dados	Definição
Compatível - Total	total_compatível	Contagem de patches compatíveis (todas as gravidades)
ID da instância	instance_id	ID da EC2 instância
Nome da instância	nome_instância	Nome da EC2 instância
	conta_sla	Nível de serviço da conta AMS
Tipo de plataforma de instância	tipo_de_plataforma de instância	Tipo de sistema operacional (OS)
Nome da plataforma da instância	nome_da_plataforma da instância	Nome do sistema operacional (SO)
Tipo de grupo de patches de instância	tipo de grupo_patch_de_instância	DEFAULT: grupo de patches padrão com janela de manutenção padrão, determinado pela AMSDefault PatchGroup tag: True na instância CLIENTE: grupo de patches criado pelo cliente NOT_ASSIGNED: nenhum grupo de patch atribuído
Grupo de patches de instância	grupo_patch_instância	Nome do grupo de patches usado para agrupar instâncias e aplicar a mesma janela de manutenção
Estado da instância	estado_instância	Estado dentro do ciclo de vida da EC2 instância

Nome do campo	Nome do campo do conjunto de dados	Definição
Tags de instância	ec2_tags	As tags associadas ao ID da EC2 instância da Amazon
Janela de manutenção da última execução	última janela_de execução	A última vez em que a janela de manutenção foi executada
ID da janela de manutenção	id_da_janela	ID da janela de manutenção
Estado da janela de manutenção	estado_janela	Estado da janela de manutenção
Tipo de janela de manutenção	tipo_janela	Tipo de janela de manutenção
Janela de manutenção: próxima data de execução	janela_seguite execution_time	Na próxima vez, espera-se que a janela de manutenção seja executada
Duração da janela de manutenção (horas)	duração_janela	A duração da janela de manutenção em horas
Cobertura da janela de manutenção	bandeira mw_covered_	Se uma instância tiver pelo menos uma janela de manutenção habilitada com uma data de execução futura, ela será considerada coberta, caso contrário, não coberta
Incompatível - Crítico	não conformidade_crítico	Contagem de patches não compatíveis com severidade “crítica”
Não compatível - Alto	não conformidade_alto	Contagem de patches não compatíveis com severidade “alta”

Nome do campo	Nome do campo do conjunto de dados	Definição
Não compatível - Médio	médio_não compatível	Contagem de patches não compatíveis com severidade “média”
Não compatível - Baixo	não conformidade_baixo	Contagem de patches não compatíveis com severidade “baixa”
Incompatível - Informativo	não compatível_informativo	Contagem de patches não compatíveis com severidade “informativa”
Não compatível - Não especificado	não compatível_não especificado	Contagem de patches não compatíveis com severidade “não especificada”
Não compatível - Total	total_incompatível	Contagem de patches não compatíveis (todas as gravidades)
ID da linha de base do patch	ID da linha de base do patch	Linha de base do patch atualmente anexada à instância
Status do patch	status do patch	Status geral de conformidade do patch. Se houver pelo menos um patch ausente, a instância será considerada não compatível, caso contrário, compatível.

Nome do campo	Nome do campo do conjunto de dados	Definição
Conta de produção	conta_produto	Identificador de contas produtivas e não produtivas do AMS, dependendo se o nome da conta inclui o valor 'PROD', 'NONPROD'.
Tipo de pilha	tipo de pilha de instância	Pilha AMS (infraestrutura AMS dentro da conta do cliente) ou pilha de clientes (infraestrutura gerenciada pelo AMS que oferece suporte aos aplicativos do cliente)
	window_next_exec_aaaa	Parte do ano de window_next_execution_time
	janela_next_exec_mm	Parte do mês de window_next_execution_time
	Window_Next_Exec_D	Parte do dia de window_next_execution_time
	janela_seguinte _Exec_HHMM	Hora:Parte de um minuto do window_next_execution_time

Instâncias que perderam os patches

Esse relatório fornece detalhes sobre instâncias que perderam os patches durante a execução da última janela de manutenção.

Esse relatório fornece:

- Dados sobre patches ausentes no nível da ID do patch.
- Dados sobre todas as instâncias que têm pelo menos um patch ausente e atributos como gravidade do patch, dias sem patch, intervalo e data de lançamento do patch.

Nome do campo	Nome do campo do conjunto de dados	Definição
Data e hora do relatório	dataset_datetime	A data e a hora em que o relatório foi gerado
ID da conta	aws_account_id	AWS ID da conta à qual o ID da instância pertence
Nome da conta	account_name	AWS nome da conta
Nome do cliente: pai	nome_parente do cliente	
Nome do cliente	customer_name	
Conta de produção	conta_produto	Identificador de contas produtivas ou não produtivas da AMS, dependendo se o nome da conta inclui o valor 'PROD' ou 'NONPROD'.
Status da conta	status da conta	Status da conta AMS
Tipo de conta	tipo_de_conta	
	conta_sla	Nível de serviço da conta AMS
ID da instância	instance_id	ID da sua EC2 instância
Nome da instância	nome_instância	Nome da sua EC2 instância
Tipo de plataforma de instância	tipo_de_plataforma de instância	Tipo de sistema operacional (OS)
Estado da instância	estado_instância	Estado dentro do ciclo de vida da EC2 instância
Tags de instância	ec2_tags	As tags associadas ao ID da EC2 instância da Amazon

Nome do campo	Nome do campo do conjunto de dados	Definição
ID do patch	ID do patch	ID do patch lançado
Gravidade do patch	patch_sev	Gravidade do patch por editor
Classificação de patches	classe de patch	Classificação do patch de acordo com o editor do patch
Data e hora do lançamento do patch (UTC)	release_dt_utc	Data de lançamento do patch por editor
Estado de instalação do patch	estado_de_instalação	Instale o estado do patch na instância por SSM
Dias sem correção	dias_não corrigido	Número de dias em que a instância não foi corrigida desde a última verificação de SSM
Intervalo de dias sem correção	day_unpatched_bucket	Período de dias sem correção

Relatório de backup (diário)

O relatório de backup abrange as regiões primária e secundária (quando aplicável). Ele abrange o status dos backups (sucesso/falha) e os dados dos instantâneos tirados.

Esse relatório fornece:

- Status do backup
- Número de instantâneos tirados
- Ponto de recuperação
- Plano de backup e informações do cofre

Nome do campo	Nome do campo do conjunto de dados	Definição
Data e hora do relatório	dataset_datetime	A data e a hora em que o relatório foi gerado.
ID da conta	aws_account_id	ID da conta da AWS à qual o ID da instância pertence
ID da conta de administrador	aws_admin_account_id	AWS Organizations Conta confiável ativada por você.
Nome da conta	account_name	Nome da conta da AWS
SLA da conta	conta_sla	Compromisso de serviço da conta AMS
	bandeira_mala	Bandeira para conta relacionada a Malz
	malz_role	Papel do MALZ
	restrições_de acesso	Regiões às quais o acesso é restrito
Data de início programada do snapshot de backup	iniciar_por_dt_utc	Registro de data e hora em que o snapshot está programado para começar
Data e hora de início real do instantâneo de backup	criação_dt_utc	Registro de data e hora em que o instantâneo realmente começa
Data e hora de conclusão do backup instantâneo	completo_dt_utc	Registro de data e hora em que o instantâneo é concluído
Data e hora de expiração do snapshot de backup	expiração_dt_utc	Registro de data e hora em que o snapshot expira

Nome do campo	Nome do campo do conjunto de dados	Definição
Status do Backup Job	status do trabalho de backup	Estado do instantâneo
Tipo de backup	backup_type	Tipo de backup
ID do trabalho de backup	ID do trabalho de backup	O identificador exclusivo da tarefa de backup
Tamanho do backup em bytes	tamanho_do_backup_em_bytes	O tamanho do backup em bytes
ARN do plano de backup	plano de backup_arn	O plano de backup ARN
ID do plano de backup	ID do plano de backup	Identificador exclusivo do plano de backup
Nome do plano de backup	nome_do_plano_backup	O nome do Plano de Backup
Versão do plano de backup	versão_do_plano_backup	A versão do plano de backup
ID da regra de backup	ID da regra de backup	O id da regra de backup
ARN do cofre de backup	backup_vault_arn	ARN do cofre de backup
Nome do cofre de backup	nome_do_cofre de backup	O nome do cofre de backup
ARN do perfil do IAM	iam_role_arn	A função ARN do IAM
ID da instância	instance_id	ID de instância exclusivo
Estado da instância	estado_instância	Estado da instância
Tags de instância	ec2_tags	As tags associadas ao ID da EC2 instância
Atributo ARN	resource_arn	O nome do recurso da Amazon

Nome do campo	Nome do campo do conjunto de dados	Definição
ID de recurso	id_do_recurso	O identificador exclusivo do recurso
Região de recursos	região_de_recursos	As regiões primária (e secundária, quando aplicável) do recurso.
Tipo de recurso	resource_type	O tipo de recurso
ARN do ponto de recuperação	ponto de recuperação	O ARN do ponto de recuperação
ID do ponto de recuperação	id_ponto_de_recuperação	O identificador exclusivo do ponto de recuperação
Status do ponto de recuperação	status do ponto_de_recuperação	Status do ponto de recuperação
Exclusão do ponto de recuperação após dias	point_recovery_delete_after_days	Exclusão do ponto de recuperação após dias
O ponto de recuperação é transferido para o armazenamento refrigerado após dias	point_recovery_move_to_cold_storage_after_days	Número de dias após a data de conclusão em que o instantâneo de backup é movido para o armazenamento refrigerado
Status da criptografia do ponto de recuperação	O ponto de recuperação está criptografado	Status de criptografia do ponto de recuperação
ARN da chave de criptografia do ponto de recuperação	point_recovery_encryption_key_arn	ARN da chave de criptografia do ponto de recuperação
ID da pilha	stack_id	Identificador exclusivo da pilha Cloudformation

Nome do campo	Nome do campo do conjunto de dados	Definição
Stack Name	stack_name	Stack Name
Tag: Grupo de patches padrão do AMS	tag_ams_default_patch_group	Valor da tag: Grupo de patches padrão do AMS
Tag: ID do aplicativo	tag_app_id	Valor da tag: ID do aplicativo
Tag: Nome do aplicativo	tag_app_name	Valor da tag: Nome do aplicativo
Tag: Backup	tag_backup	Valor da tag: Backup
Tag: Estrutura de conformidade	estrutura de conformidade de tags	Valor da tag: Estrutura de conformidade
Tag: Centro de custos	tag_cost_center	Valor da tag: Centro de custos
Tag: Cliente	tag_cliente	Valor da tag: Cliente
Tag: Classificação de dados	tag_data_classification	Valor da tag: Classificação de dados
Tag: Tipo de ambiente	tipo_do_ambiente_tag	Valor da tag: Tipo de ambiente
Tag: Horário de funcionamento	tag_horas_de_operação	Valor da etiqueta: Horário de funcionamento
Tag: Equipe do proprietário	tag_owner_team	Valor da etiqueta: Equipe proprietária
Tag: E-mail da equipe do proprietário	tag_owner_team_email	Valor da tag: E-mail da equipe proprietária
Etiqueta: Patch Group	tag_patch_group	Valor da tag: Grupo de patches
Tag: Support Priority	tag_support_priority	Valor da tag: Support Priority

Nome do campo	Nome do campo do conjunto de dados	Definição
Estado do volume	estado_volume	Estado do volume

Relatório de incidentes (semanal)

Esse relatório fornece a lista agregada de incidentes, juntamente com sua prioridade, gravidade e status mais recente, incluindo:

- Dados sobre casos de suporte categorizados como incidentes na conta gerenciada
- Informações de incidentes necessárias para visualizar as métricas de incidentes da conta gerenciada
- Dados sobre categorias de incidentes e status de remediação de cada incidente

Tanto a visualização quanto os dados estão disponíveis para o relatório semanal de incidentes.

- A visualização pode ser acessada por meio do console AMS na conta por meio da página Relatórios.
- O conjunto de dados com o esquema a seguir pode ser acessado por meio do bucket do S3 na conta gerenciada.
- Use os campos de data fornecidos para filtrar incidentes com base no mês, trimestre, semana e and/or dia em que o incidente foi criado ou resolvido.

Nome do campo	Nome do campo do conjunto de dados	Definição
Data e hora do relatório	dataset_datetime	A data e a hora em que o relatório foi gerado.
ID da conta	aws_account_id	AWS ID da conta à qual o incidente pertence.
ID da conta de administrador	aws_admin_account_id	AWS Organizations Conta confiável ativada por você.

Nome do campo	Nome do campo do conjunto de dados	Definição
Nome da conta	account_name	AWS nome da conta.
ID do caso	case_id	A identificação do incidente.
Mês criado	mês_criado	O mês em que o incidente foi criado.
Prioridade	priority	A prioridade do incidente.
Gravidade	severidade	A gravidade do incidente.
Status	status	O status do incidente.
Categoria	categoria_yuma	A categoria do incidente.
Dia da Criação	dia_criado	O dia em que o incidente foi criado em YYYY-MM-DD formato.
Semana criada	created_wk	A semana em que o incidente foi criado no formato YYYY-WW. Domingo a sábado é contado como o início e o fim de uma semana. A semana é de 01 a 52. A semana 01 é sempre a semana que contém o primeiro dia do ano. Por exemplo, 2023-12-31 e 2024-01-01 estão na semana 2024-01.
Trimestre criado	created_qtr	O trimestre em que o incidente foi criado no formato YYYY-Q. 01/01 a 31/03/31 é definido como Q1 e assim por diante.

Nome do campo	Nome do campo do conjunto de dados	Definição
Dia resolvido	dia_resolvido	O dia em que o incidente foi resolvido em YYYY-MM-DD formato.
Semana resolvida	resolvido_wk	A semana em que o incidente foi resolvido no formato YYYY-WW. Domingo a sábado é contado como o início e o fim de uma semana. A semana é de 01 a 52. A semana 01 é sempre a semana que contém o primeiro dia do ano. Por exemplo, 2023-12-31 e 2024-01-01 estão na semana 2024-01.
Mês resolvido	mês_resolvido	O mês em que o incidente foi resolvido no formato YYYY-MM.
Trimestre resolvido	resolvido_qtr	O trimestre em que o incidente foi resolvido no formato YYYY-Q. 01/01 a 31/03/31 é definido como Q1 e assim por diante.
Regra de agrupamento criada	regra_de_agrupamento	A regra de agrupamento que se aplica ao incidente. Ou “no_grouping” ou “instance_grouping”.
Instância IDs	id_de_instância	A instância associada ao incidente.

Nome do campo	Nome do campo do conjunto de dados	Definição
Número de alertas	número_de_alertas	O número de alertas associados a esse incidente. Se você tiver o agrupamento ativado, esse número poderá ser maior que 1. Se você não tiver o agrupamento ativado, ele sempre será 1.
Criado em	created_at	A data e hora em que o incidente foi criado.
Alarme ARNs	alarme_avisos	O nome de recurso da Amazon ("arn") dos alarmes associados ao seu incidente.
Alarmes relacionados	alarmes relacionados	Os nomes legíveis por humanos de todos os alarmes associados ao incidente.

Relatório de cobrança (mensal)

Detalhes das cobranças de cobrança

Esse relatório fornece detalhes sobre as cobranças de faturamento do AMS com contas vinculadas e os respectivos serviços da AWS.

Esse relatório fornece:

- Dados sobre cobranças de nível de serviço do AMS, porcentagens de aumento, níveis de serviço do AMS no nível da conta e taxas do AMS.
- Dados sobre contas vinculadas e cobranças de uso da AWS.

⚠ Important

O relatório de cobrança mensal só está disponível em sua Conta Administrativa do Pagador (MPA) ou em sua Conta de Cobrança definida. Essas são as contas para as quais sua fatura mensal do AMS é enviada. Se você não conseguir localizar essas contas, entre em contato com seu Cloud Service Delivery Manager (CSDM) para obter ajuda.

Nome do campo	Nome do campo do conjunto de dados	Definição
Data de cobrança	date	O mês e o ano do serviço cobrado
ID da conta do pagador	payer_account_id	O ID de 12 dígitos que identifica a conta responsável pelo pagamento das cobranças do AMS
ID da conta vinculada	linked_account_id	O ID de 12 dígitos que identifica a conta AMS que consome serviços que gera expansões
AWS Nome do serviço	product_name	O AWS serviço que foi usado
AWS Cobranças	cobranças da AWS	As AWS cobranças pelo nome do AWS serviço em Nome do AWS serviço
Plano de preços	plano_de_preços	O plano de preços associado à conta vinculada
Grupo de serviços AMS	grupos de elevação de níveis	Código do grupo de serviços do AMS que determina a porcentagem de aumento
Proporção de elevação	percentual de elevação	A porcentagem de aumento (como um V.WXYZ decimal)

Nome do campo	Nome do campo do conjunto de dados	Definição
		com base no pricing_plan, no SLA e no serviço AWS
AWS Cobranças ajustadas	utilização_aws_ajustada	AWS uso ajustado para AMS
Taxas elevadas AWS	cobranças elevadas da AWS	A porcentagem de AWS cobranças a serem cobradas pelo AMS; $\text{adjusted\_aws\_charges} * \text{uplift\_percent}$
Gastos do EC2 RDS em instâncias	instâncias_ec2_rds_spend	Gastos em EC2 instâncias do RDS e suas
Cobranças de instância reservada	cobranças de risco	Cobranças de instância reservada
Taxas de instância reservada aumentadas	íris elevada	A porcentagem de cobranças de instâncias reservadas a serem cobradas pelo AMS; $\text{ris\_charges} * \text{uplift\_percent}$
Cobranças do Savings Plan	sp_charges	SavingsPlan taxas de uso
Taxas aumentadas do Savings Plan	uplifted_sp	A porcentagem das cobranças dos planos de poupança a serem cobradas pelo AMS; $\text{sp\_charges} * \text{uplift\_percent}$
Taxas do AMS	ams_charges	Total de cobranças de ams pelo produto; $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$
Taxa mínima proporcional	mínimo_proporcional	O valor que cobramos para atender ao mínimo contratual

Nome do campo	Nome do campo do conjunto de dados	Definição
Total de cobranças AMS da conta vinculada	total da conta vinculada ams_charges	Soma de todas as cobranças da linked_account
Total de cobranças de AMS da conta do pagador	total da conta do pagador ams_charges	Soma de todas as cobranças da conta do pagador
Taxa mínima	taxas_mínimas	Taxas mínimas do AMS (se aplicável)
Desconto em Instância Reservada e Savings Plan	adj_ri_sp_charges	RI/SP discount to be applied against RI/SPencargos (aplicáveis sob certas circunstâncias)

Relatórios agregados

Os relatórios de autoatendimento agregados (SSR) fornecem uma visão dos relatórios de autoatendimento existentes agregados no nível da organização, entre contas. Isso lhe dá visibilidade das principais métricas operacionais, como conformidade de patches, cobertura de backup e incidentes, em todas as contas sob gerenciamento do AMS em sua AWS Organizations.

O SSR agregado está disponível em todas as áreas comerciais em Regiões da AWS que o AWS Managed Services está disponível. Para obter uma lista completa das regiões disponíveis, consulte a [tabela de regiões](#).

Ativar relatórios agregados

Você deve gerenciar o SSR agregado a partir de uma conta de AWS Organizations [gerenciamento](#). A conta de gerenciamento é a AWS conta que você usou para criar sua organização.

Para habilitar o SSR agregado para uma conta AWS Organizations de gerenciamento integrada ao AMS, acesse seu console do AMS e navegue até Relatórios. Selecione Acesso à organização no top-right-hand canto para abrir o painel [AWS Managed Services Console: Organization View](#). Nesse painel, você pode gerenciar a funcionalidade SSR agregada.

AWS Organizations contas de gerenciamento que não estão integradas ao AMS não têm acesso ao console do AMS. Para habilitar o SSR agregado para uma conta AWS Organizations de gerenciamento que não está integrada ao AMS, primeiro autentique-se na sua Conta da AWS, depois navegue até o [AWS console](#) e pesquise Managed Services. Isso abre a página de marketing do AMS. Nesta página, selecione o link Acesso à organização na barra de navegação para abrir o console do AWS Managed Services: Organization View, onde você pode gerenciar a funcionalidade SSR agregada.

Na primeira vez que você acessar o [AWS Managed Services Console: Organization View](#), conclua as seguintes etapas:

1. Se você ainda não tiver configurado AWS Organizations, escolha Ativar AWS Organizations no seu console. Para obter informações adicionais sobre a configuração AWS Organizations, consulte o [Guia AWS Organizations do usuário](#). Você pode pular essa etapa se já estiver usando AWS Organizations.
2. Para ativar o serviço Aggregated Self-Service Reporting, selecione Habilitar acesso confiável no console.
3. (Opcional) Registre um administrador delegado para ter acesso de leitura à visão organizacional.

Visualize relatórios agregados como administrador delegado

Um administrador delegado é a conta que você escolhe para ter acesso de leitura aos relatórios agregados. O administrador delegado deve ser uma conta integrada ao AMS e ser a única conta que tenha acesso de leitura aos relatórios agregados.

Para escolher um administrador delegado, insira o ID da conta na Etapa 3 no console do AWS Managed Services: Organization View. Você só pode ter uma conta de administrador delegado registrada por vez. Observe que a conta do administrador delegado deve ser uma conta gerenciada pelo AMS.

Para atualizar uma conta de administrador delegado, navegue até o [AWS Managed Services Console: Organization View](#) e selecione Remove the Delegated Administrator. O console solicita que você insira uma nova ID de conta para se registrar como administrador delegado.

Leia relatórios agregados

Se você não registrar um administrador delegado e sua conta de AWS Organizations gerenciamento estiver integrada ao AMS, a conta de AWS Organizations gerenciamento terá acesso de leitura

aos relatórios agregados por padrão. Se a conta AWS Organizations de gerenciamento não for gerenciada pelo AMS, você deverá escolher uma conta de administrador delegado para ter acesso de leitura aos relatórios agregados.

A qualquer momento, somente uma única conta integrada ao AMS tem acesso de leitura aos relatórios agregados, seja a conta de AWS Organizations gerenciamento ou o administrador delegado registrado. Todas as outras contas de membros em sua organização (e integradas ao AMS) ainda têm acesso somente aos relatórios de uma única conta para cada conta individual.

[Depois de ativar o SSR agregado, navegue até seus Relatórios.](#) Todos os seus relatórios de autoatendimento existentes estão listados nesta seção, e uma etiqueta azul indica que eles foram agregados. Observe que você deve acessar o console do AMS a partir da conta que escolheu para ter acesso de leitura aos relatórios agregados. Essa é a conta AWS Organizations de gerenciamento ou a conta de administrador delegado.

Depois de ativar o SSR agregado, os relatórios agregados estarão disponíveis a partir do próximo ciclo de relatórios.

Desativar relatórios agregados

Para desativar o SSR agregado, abra o [console do AWS Managed Services: Organization View](#). Selecione Desativar acesso confiável. Depois de desativar o acesso confiável ao SSR agregado, seus relatórios de autoatendimento do AMS deixam de ser agregados no nível da organização, em todas as contas. Observe também que a desativação entra em vigor a partir do próximo ciclo de relatórios.

Depois de desativar o SSR agregado, aguarde até que os relatórios no console do AMS apareçam como relatórios de conta única. Esse atraso ocorre porque a desativação do recurso entra em vigor a partir do próximo ciclo de relatórios.

Painéis de relatórios de autoatendimento do AMS

Os relatórios de autoatendimento do AMS oferecem dois painéis: e. [Painel do Resource Tagger](#)
[Painel de regras de configuração de segurança](#)

Painel do Resource Tagger

O painel do Resource Tagger do AMS fornece informações detalhadas sobre os recursos suportados pelo Resource Tagger, bem como o status atual das tags que o Resource Tagger está configurado para aplicar a esses recursos.

Cobertura do Resource Tagger por tipo de recurso

Esse conjunto de dados consiste em uma lista de recursos que têm tags gerenciadas pelo Resource Tagger.

A cobertura de recursos por tipo de recurso é visualizada como gráficos de quatro linhas que descrevem as seguintes métricas:

- Contagem de recursos: o número total de recursos na região, por tipo de recurso.
- Recursos sem tags gerenciadas: o número total de recursos na região, por tipo de recurso, que exigem tags gerenciadas, mas não são marcados pelo Resource Tagger.
- Recursos não gerenciados: o número total de recursos na região, por tipo de recurso, que não têm tags gerenciadas aplicadas a eles pelo Resource Tagger. Isso geralmente significa que esses recursos não são correspondidos por nenhuma configuração do Resource Tagger ou são explicitamente excluídos das configurações.
- Recursos gerenciados: contrapartida da métrica de recursos não gerenciados (Contagem de recursos - Recursos não gerenciados).

A tabela a seguir lista os dados fornecidos por esse relatório.

Nome do campo	Nome do campo do conjunto de dados	Definição
Data e hora do relatório	dataset_datetime	A data e a hora em que o relatório foi gerado (hora UTC)
Conta da AWS ID	aws_account_id	Conta da AWS ID
ID da conta de administrador	aws_admin_account_id	AWS Organizations Conta confiável ativada por você.
Região	região	Região da AWS
Tipo de recurso	resource_type	Esse campo identifica o tipo de recurso. Somente os tipos de recursos compatíveis com o Resource Tagger estão incluídos.

Nome do campo	Nome do campo do conjunto de dados	Definição
Contagem de recursos	contagem_de_recursos	Número de recursos (do tipo de recurso especificado) implantados nessa região.
ResourcesMissingManagedTags	resource_missing_managed_tags_count	Número de recursos (do tipo de recurso especificado) que exigem tags gerenciadas, de acordo com os perfis de configuração, mas ainda não foram marcados pelo Resource Tagger.
UnmanagedResources	contagem de recursos não gerenciada	Número de recursos (do tipo de recurso especificado) sem tags gerenciadas aplicadas pelo Resource Tagger. Normalmente, esses recursos não correspondem a nenhum bloco de configuração do Resource Tagger ou são explicitamente excluídos dos blocos de configuração.

Conformidade com as regras de configuração do Resource T

Esse conjunto de dados consiste em uma lista de recursos em um Região da AWS, por tipo de recurso, que têm um determinado perfil de configuração aplicado a eles. É visualizado como um gráfico de linhas.

A tabela a seguir lista os dados fornecidos por esse relatório.

Nome do campo	Nome do campo do conjunto de dados	Definição
Data e hora do relatório	dataset_datetime	A data e a hora em que o relatório foi gerado (hora UTC)
Conta da AWS ID	aws_account_id	Conta da AWS ID
ID da conta de administrador	aws_admin_account_id	AWS Organizations Conta confiável ativada por você.
Região	região	Região da AWS
Tipo de recurso	resource_type	Esse campo identifica o tipo de recurso. Somente os tipos de recursos compatíveis com o Resource Tagger estão incluídos.
ID do perfil de configuração	configuration_profile_id	O ID do perfil de configuração do Resource Tagger. Um perfil de configuração é usado para definir políticas e regras usadas para marcar seus recursos.
MatchingResourceCount	contagem_de_recursos	Número de recursos (do tipo de recurso especificado) que correspondem à ID do perfil de configuração do Resource Tagger. Para que um recurso corresponda ao perfil de configuração, o perfil deve estar ativado e o recurso deve corresponder à regra do perfil.

Recursos não compatíveis com o Resource Tagger

Esse conjunto de dados consiste em uma lista de recursos que não estão em conformidade com uma única configuração do Resource Tagger. Esses dados são um resumo diário da conformidade dos recursos, mostrando o estado dos recursos do cliente no momento em que esses relatórios são entregues às contas dos clientes (não há uma visão histórica). Ela é visualizada como uma tabela dinâmica que consiste em recursos que não são compatíveis com uma determinada configuração.

A tabela a seguir lista os dados fornecidos por esse relatório.

Nome do campo	Nome do campo do conjunto de dados	Definição
Data e hora do relatório	dataset_datetime	A data e a hora em que o relatório foi gerado (hora UTC)
Conta da AWS ID	aws_account_id	Conta da AWS ID
ID da conta de administrador	aws_admin_account_id	AWS Organizations Conta confiável ativada por você.
Região	região	Região da AWS
Tipo de recurso	resource_type	Esse campo identifica o tipo de recurso. Somente os tipos de recursos compatíveis com o Resource Tagger estão incluídos.
ID do recurso	ID do recurso	O identificador exclusivo para recursos suportados pelo Resource Tagger.
Estado de cobertura	estado_de_cobertura	Esse campo indica se o recurso está marcado como configurado pelo ID de configuração do Resource Tagger.

Nome do campo	Nome do campo do conjunto de dados	Definição
ID do perfil de configuração	configuration_profile_id	O ID do perfil de configuração do Resource Tagger. Um perfil de configuração é usado para definir políticas e regras usadas para marcar seus recursos.

Painel de regras de configuração de segurança

O painel de regras do Security Config fornece uma visão aprofundada da conformidade de recursos e AWS Config regras das contas do AMS. Você pode filtrar o relatório por severidade da regra para priorizar as descobertas mais importantes. A tabela a seguir lista os dados fornecidos por esse relatório.

Nome do campo	Nome do campo do conjunto de dados	Definição
Conta da AWS ID	Conta da AWS ID	O ID da conta vinculado aos recursos relacionados.
ID da conta de administrador	aws_admin_account_id	AWS Organizations Conta confiável ativada por você.
data e hora do relatório	Data do relatório	A data e a hora em que o relatório foi gerado.
customer_name	Nome do cliente	O nome do cliente.
account_name	Nome da conta	O nome associado ao ID da conta
ID do recurso	ID do recurso	Um identificador para um recurso.

Nome do campo	Nome do campo do conjunto de dados	Definição
região_de_recursos	Região de recursos	O Região da AWS local onde o recurso está localizado.
resource_type	Tipo de recurso	O tipo de recurso AWS service (Serviço da AWS) ou.
nome_do_recurso	Nome do recurso	O nome do recurso.
resource_ams_flag	Sinalizador AMS de recursos	Se o recurso for de propriedade de do AMS, esse sinalizador será definido como TRUE. Se o recurso for de propriedade do cliente, esse sinalizador será definido como FALSE. Se a propriedade não for conhecida, esse sinalizador será definido como DESCONHECIDO.
regra de configuração	Regra do Config	O nome não personalizável da regra de configuração.
config_rule_description	Descrição da regra de configuração	Uma descrição da regra de configuração.
identificador_fonte	Identificador de origem	Um identificador exclusivo para a regra de configuração gerenciada e nenhum identificador para uma regra de configuração personalizada.
sinalizador_de_conformidade	Sinalizador de conformidade	Mostra se os recursos estão em conformidade ou não com as regras de configuração.

Nome do campo	Nome do campo do conjunto de dados	Definição
tipo_regra	Tipo de regra	Indica se a regra é predefinida ou personalizada.
sinizador_exceção	Sinalizador de exceção	O sinalizador de exceção de recurso mostra a aceitação do risco em relação a um recurso não compatível. Se o sinalizador de exceção do recurso for VERDADEIRO para um recurso, o recurso será isento. Se o sinalizador de exceção for NULL, o recurso não será isento.
cal_dt	Data	A data de avaliação da regra.
descrição_da remediação	Descrição da remediação	Uma descrição de como corrigir a conformidade com as regras.
severidade	Gravidade	A severidade da regra de Config indica o impacto da não conformidade.
ação do cliente	Ação do cliente	Ação necessária para remediar essa regra.
recomendação	Recomendação	Uma descrição do que a regra de configuração verifica.
categoria_de remediação	Categoria de remediação	As ações padrão que o AMS executa quando essa regra se torna incompatível.

Política de retenção de dados

O AMS SSR tem uma política de retenção de dados por relatório após o período relatado, os dados são apagados e não estão mais disponíveis.

Nome do relatório	Console SSR de retenção de dados	Bucket SSR S3 de retenção de dados
Resumo dos detalhes da instância (Patch Orchestrator)	2 meses	2 anos
Detalhes do patch	2 meses	2 anos
Instâncias que perderam os patches durante a execução da janela de manutenção	2 meses	2 anos
Detalhes das cobranças de cobrança do AMS	2 anos	2 anos
Relatório diário de backup	1 mês	2 anos
Relatório semanal de incidentes	2 meses	2 anos
Painel de regras de configuração de segurança	3 meses	2 anos
Painel do Resource Tagger	1 ano	2 anos

Fora do SSR

Para sair do serviço SSR, crie uma solicitação de serviço (SR) por meio do console AMS. Depois de enviar o SR, um engenheiro de operações do AMS ajuda você a sair do SSR. No SR, forneça o motivo pelo qual você deseja desembarcar.

Para desativar uma conta e realizar uma limpeza de recursos, crie um SR por meio do console do AMS. Depois de enviar o SR, um engenheiro de operações do AMS ajuda você a excluir o bucket SSR Amazon S3.

Se você desembarcar do AMS, será automaticamente desembarcado do console SSR do AMS. O AMS interrompe automaticamente o envio de dados para sua conta. O AMS exclui seu bucket SSR S3 como parte do processo de desativação.

Relatórios de incidentes, solicitações de serviço e perguntas sobre faturamento no AMS

Tópicos

- [Gerenciamento de incidentes](#)
- [Gerenciamento de solicitações de serviço](#)
- [Perguntas sobre faturamento](#)

Com o AWS Managed Services (AMS), você pode solicitar ajuda com problemas operacionais e solicitações a qualquer momento por meio do console do AMS. Os engenheiros de operações do AMS estão disponíveis para responder aos seus incidentes e solicitações de serviço 24 horas por dia, 7 dias por semana, com tempo de resposta de Acordos de Nível de Serviço (SLAs) e Objetivos de Nível de Serviço (SLOs), dependendo do nível de serviço de sua conta selecionada (Plus, Premium). Os engenheiros de operações do AMS notificam você de forma proativa sobre alertas e perguntas importantes usando os mesmos mecanismos.

Gerenciamento de incidentes

Tópicos

- [O que é gerenciamento de incidentes?](#)
- [Compromissos do serviço de gerenciamento de incid](#)
- [Exemplos de gerenciamento de incidentes](#)

Incidentes são problemas de AWS service (Serviço da AWS) desempenho que afetam seu ambiente gerenciado, conforme determinado pelo AWS Managed Services (AMS) ou por você. Os incidentes identificados pela equipe do AMS são primeiramente recebidos como “eventos”: uma mudança no estado do sistema capturada pelo monitoramento. Se um limite configurado for violado, o evento acionará um alarme, também chamado de alerta. A equipe de operações do AMS determina se o evento não tem impacto, é um incidente (uma interrupção ou degradação do serviço) ou um problema (a causa raiz subjacente de um ou mais incidentes resolvidos).

A equipe do AMS também recebe incidentes identificados por você por meio do Suporte centro ou programaticamente usando a [API do AWS Support](#) com o código do serviço. `sentinel-report-incident`

Depois que seu incidente é recebido pela equipe de operações do AMS, ele é analisado para garantir que o incidente não seja melhor classificado como uma solicitação de serviço. Se ela deve ser classificada como uma solicitação de serviço, ela é imediatamente reclassificada e a equipe de solicitação de serviço do AMS assume o controle e você é notificado. Se o incidente puder ser resolvido pelo operador receptor, serão tomadas medidas para resolvê-lo imediatamente. Os operadores do AMS consultam a documentação interna para obter uma resolução e, se necessário, encaminham o incidente para outros recursos de suporte até que o incidente seja resolvido. Para se manter informado em cada etapa do processo de resolução de incidentes, certifique-se de preencher a opção CC Emails e, se você quiser se conectar por federação, faça login antes de seguir o link no e-mail enviado pelo AMS. Depois de resolvido, a equipe de operações do AMS documenta o incidente e a resolução para uso futuro.

Se a resolução de um incidente exigir mudanças na infraestrutura, talvez seja necessária uma revisão de segurança. As mudanças na infraestrutura que podem exigir uma análise de segurança incluem aquelas relacionadas ao IAM, à política baseada em recursos ou às aprovações de risco. Esses tipos de incidentes exigem que um engenheiro de operações do AMS crie uma RFC antes de fazer a alteração, e sua aprovação para essa RFC é necessária. Por exemplo, se a resolução do incidente exigir a atualização de uma política do IAM, haveria uma análise de segurança do AMS e, em seguida, um engenheiro de operações do AMS criaria um RFC com os componentes Management | Advanced stack | Identity and Access Management (IAM) | Atualizar entidade ou tipo de alteração de política (ct-27tuth19k52b4) e aguardar a aprovação do RFC antes de continuar.

Note

O AMS agora permite a resolução de incidentes que exigem que mudanças na infraestrutura sejam feitas sem a etapa adicional da aprovação da RFC. Se as mudanças necessárias para resolver o incidente NÃO exigirem uma revisão de segurança (a alteração não está relacionada ao IAM, à política baseada em recursos ou às aprovações de risco), o AMS poderá fazer as alterações com base na aprovação recebida no incidente, sem precisar de aprovação separada em uma RFC.

Para obter definições dos termos de gerenciamento de incidentes, consulte [os principais termos do AMS](#).

Para entender o caminho de escalonamento dos incidentes, consulte [Como obter](#) ajuda.

Para obter uma descrição da resposta do AMS aos incidentes, consulte [Resposta a incidentes do AMS](#).

O que é gerenciamento de incidentes?

O gerenciamento de incidentes é o processo que o AMS usa para registrar, agir, comunicar o progresso e fornecer notificação de incidentes ativos.

O objetivo do processo de gerenciamento de incidentes é garantir que a operação normal do seu serviço gerenciado seja restaurada o mais rápido possível, que o impacto nos negócios seja minimizado e que todas as partes envolvidas sejam mantidas informadas.

Exemplos de incidentes incluem (mas não estão restritos a) perda ou degradação da conectividade de rede, um processo ou API que não responde ou uma tarefa agendada que não está sendo executada (por exemplo, falha no backup).

O gráfico a seguir mostra o fluxo de trabalho de um incidente relatado por você ao AMS.

Este gráfico mostra o fluxo de trabalho de um incidente relatado pelo AMS a você.

Prioridade do incidente

Os incidentes criados no centro de suporte, no console ou na API de suporte (SAPI) da AWS têm classificações diferentes dos incidentes criados no console do AMS.

- Baixo: funções não críticas do seu serviço ou aplicativo comercial relacionadas aos recursos da AWS ou do AMS são afetadas.
- Médio: um serviço ou aplicativo comercial relacionado aos recursos do AWS and/or AMS sofre um impacto moderado e está funcionando em um estado degradado.
- Alto: sua empresa é significativamente afetada. Funções críticas do seu aplicativo relacionadas aos recursos do AWS and/or AMS não estão disponíveis. Reservado para as interrupções mais críticas que afetam os sistemas de produção.

Note

O AWS Support Console oferece cinco níveis de prioridade de incidentes que traduzimos para os três níveis do AMS.

Problema versus incidente

Quando a AMS acredita que um incidente revela um defeito maior ou uma configuração incorreta e pode ocorrer novamente, ele é considerado um problema e não apenas um incidente. Nesses casos, a AMS realiza análises do problema e oferece sugestões para resolvê-lo.

Compromissos do serviço de gerenciamento de incid

Compromissos do serviço de gerenciamento de incid

Evento ou ação	Medição do compromisso com o serviço
Caso 1: Um evento com impacto conhecido é gerado. O AMS abre um incidente e informa você. Caso 2: A AMS entra em contato com você para confirmar o impacto do evento. Você confirma que o evento é um incidente. Caso 3: Você percebe um problema e envia um relatório de incidente.	O relógio para resposta a incidentes e a resolução de incidentes começa quando: Caso 1: O AMS cria um incidente. Caso 2: Você confirma que o alerta é um incidente. Caso 3: Você envia um incidente. Os compromissos de serviço dependem da prioridade do incidente criado.
Se você enviar o incidente, o AMS enviará uma resposta para reconhecê-lo. Se o AMS criar o incidente em seu nome, uma resposta separada ao incidente não será enviada.	O tempo para resolução de incidentes continua correndo. O relógio para ver o tempo de resposta ao incidente é interrompido quando o AMS envia a confirmação do incidente.  Note O tempo gasto aguardando suas informações é excluído dos cálculos do tempo de resolução de incidentes. Para incidentes criados pelo AMS, o tempo de resposta inicial é o momento

Evento ou ação	Medição do compromisso com o serviço
	da criação da notificação inicial do incidente para você.
Para os recursos/serviços em questão, o AMS verifica a integridade para verificar se: • O evento detectado pelo AMS ou o incidente enviado pelo cliente se qualifica como um incidente, e • o incidente é priorizado corretamente e Se um incidente que você enviar não for priorizado corretamente, o AMS o priorizará novamente. Se o AMS alterar a prioridade de um incidente, uma notificação será enviada a você junto com o raciocínio por trás da mudança de prioridade. Em certos casos, um problema que você enviou pode não se qualificar como um incidente, dependendo da causa. Nesses casos, o AMS encerra o incidente e envia uma notificação explicando o motivo. Independentemente da categorização do evento, a AMS trabalha com você para ajudar conforme necessário. Para entender as regras de categorização de incidentes, consulte Prioridade do incidente.	Caso a prioridade do incidente mude, o compromisso de serviço para a nova prioridade é aplicável; o relógio continua correndo. Nos casos em que um incidente é encerrado porque não atende à definição de incidente, os compromissos de serviço não são aplicáveis; o relógio para.

Evento ou ação	Medição do compromisso com o serviço
O AMS trabalha no incidente para resolvê-lo dentro do compromisso de serviço. Em certos casos, se o AMS determinar que pilhas ou recursos indisponíveis não podem ser resolvidos em tempo hábil, o AMS oferecerá a restauração da infraestrutura como uma opção de resolução. A restauração da infraestrutura envolve a reimplantação da (s) pilha (s) existente (s), com base nos modelos da (s) pilha (s) afetada (s), e o início de uma restauração de dados com base no último ponto de restauração conhecido (instantâneo do EBS/RDS), a menos que você especifique o contrário. Dados efêmeros em EC2 instâncias individuais serão perdidos. Se você não autorizar uma restauração de infraestrutura conforme recomendado pela AWS, você não estará qualificado para receber um crédito de serviço pelo Compromisso de Serviço de Tempo de Resolução de Incidentes associado.	O relógio para quando: • O AMS restaurou todos os serviços ou recursos indisponíveis relacionados a esse incidente para um estado disponível, ou • uma restauração da infraestrutura é iniciada.
Ocasionalmente, o AMS precisa de esclarecimentos ou atividades de você para manter os esforços de resolução de incidentes em andamento, a menos que você tenha uma ação predefinida e aprovada. Como resultado, há comunicação entre o AMS e você para resolver incidentes	O relógio para quando: O AMS está esperando por uma resposta ou ação sua. O relógio reinicia quando: O AMS recebe sua resposta ou a ação que o AMS exige de você é concluída.

 Note

Para obter uma lista completa dos compromissos de serviço, baixe o [Acordo de Nível de Serviço do AMS](#).

Exemplos de gerenciamento de incidentes

Exemplos de gerenciamento de incidentes.

Tópicos

- [Teste de incidentes](#)
- [Notificação de incidentes](#)
- [Monitoramento e atualização de incidentes](#)
- [Gerenciamento de incidentes com a API do AWS Support](#)
- [Respondendo a incidentes gerados pela AMS](#)

Os exemplos a seguir descrevem o uso do console AMS para enviar um incidente. Depois de enviado, a equipe do AMS trabalha com você para resolver o incidente de acordo com seu Acordo de Nível de Serviço (SLA).

Teste de incidentes

Ao testar os envios de incidentes do AMS, pedimos que você inclua no texto do assunto esta bandeira: AMSTestNoOpsActionRequired. Esse sinalizador permite que o AMS saiba que o envio do incidente é apenas para testes. Quando os engenheiros de operações da AMS virem essa bandeira, eles não responderão de forma alguma ao envio do incidente.

Notificação de incidentes

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 tiver sido 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.

YouTube Vídeo: [Como faço para levantar um incidente no console do AWS Managed Services?](#)

Monitoramento e atualização de incidentes

Você pode atualizar, monitorar e revisar relatórios de incidentes e solicitações de serviço, ambos chamados de casos, usando o console do AMS ou programaticamente usando a Suporte API. Para obter informações sobre como usar a Suporte API, consulte [DescribeCases](#) operação.

Para monitorar um caso, incidente ou solicitação de serviço usando o console do AMS, siga estas etapas.

1. No console do AMS, Relatórios de incidentes ou painel de solicitações de serviço, navegue até um caso e escolha o Assunto para abrir uma página de detalhes com o status atual e as correspondências.

Quando um incidente relatado ou um caso de solicitação de serviço é atualizado pela equipe de operações do AMS, você recebe um e-mail e um link para o incidente no console do AMS para poder responder. Você não pode responder à correspondência do incidente respondendo ao e-mail.

 Important

Você deve ter inserido um endereço de e-mail para receber notificações de mudança de estado para uma solicitação de serviço ou caso de incidente. As notificações só vão para o endereço de e-mail adicionado ao caso quando ele é criado.

O link no e-mail de notificação não funcionará, a menos que você esteja usando um servidor de e-mail na sua rede federada do AMS. No entanto, você pode responder à correspondência acessando o console do AMS e usando a página de detalhes do caso.

2. Se houver muitos casos na lista, você poderá usar a opção Filtro:

- Todos abertos (padrão): use esse filtro para ver todos os casos que não foram resolvidos.
- Não atribuído: use se você acabou de enviar o caso e não recebeu nenhum aviso de que o estado do caso mudou. Observe que os incidentes e os casos de solicitação de serviço são tratados com rapidez diferente, dependendo da prioridade enviada (incidentes) ou do seu contrato de nível de serviço (solicitações de serviço).
- Abrir: use se você recebeu uma notificação de que o caso é uma ação “Amazon pendente”; isso significa que o caso foi atribuído, mas o trabalho ainda não começou.
- Reaberto: use se você recebeu um aviso de que o caso foi reaberto depois de ter sido resolvido.
- Trabalho em andamento: use se você recebeu um aviso de que um operador começou a trabalhar no caso.
- Ação pendente do cliente: use se você tiver recebido uma solicitação de ação do operador de sua parte.
- Ação do cliente concluída: use se você recebeu uma notificação de que sua ação no caso foi processada.
- Resolvidos: use para ver casos que você sabe que foram resolvidos. Os casos resolvidos são mantidos no histórico por doze meses.
- Qualquer status: use esse filtro para ver todos os casos, independentemente do status.

3. Para verificar o status mais recente, atualize a página.

4. Se houver tantas correspondências que nem todas apareçam na página, escolha Carregar mais.
5. Para atualizar o status do caso, escolha Responder, insira a nova correspondência e escolha Enviar.
6. Para encerrar o caso após ele ter sido resolvido de forma satisfatória, escolha Fechar caso.

Não se esqueça de avaliar o serviço por meio da classificação de 1 a 5 estrelas para que a AMS saiba como estamos indo!

Gerenciamento de incidentes com a API do AWS Support

A [API do AWS Support](#) permite que você crie incidentes e adicione correspondência a eles durante as investigações de seus problemas e interações com a equipe do AWS Support. A API do AWS Support modela grande parte do comportamento do [AWS Support Center](#). Para obter mais detalhes sobre como você pode usar esse serviço de suporte da AWS, consulte [Programando um caso de suporte da AWS](#).

Note

Ao usar a API AWS Support, ou SAPI, para incidentes do AMS Advanced, use este código de serviço: `sentinel-report-incident`

Respondendo a incidentes gerados pela AMS

O AMS monitora proativamente seus recursos; para obter mais informações, consulte [Monitoramento e gerenciamento de eventos](#). Às vezes, o AMS identifica e cria um caso de incidente, na maioria das vezes para notificá-lo sobre um incidente. Caso seja necessária uma ação de sua parte para resolver um incidente, o AMS envia uma notificação às informações de contato que você forneceu para a conta. Você responde a esse incidente da mesma forma que responderia a qualquer outro incidente. Normalmente, você responderia a incidentes por meio do console do AMS; em alguns casos, é necessário entrar em contato por e-mail ou telefone.

Note

O AMS envia comunicações para seu endereço de e-mail principal na sua conta da AWS; recomendamos adicionar um alias alternativo de e-mail de contato de Operações para facilitar o processo de gerenciamento de incidentes. Isso é abordado durante o processo de integração do AMS e a documentação de integração relacionada. Se você forneceu

ao AMS contatos não baseados em recursos (sobre os quais você informou seu CSDM) durante a integração, esses contatos serão usados. Por exemplo, você pode fornecer uma lista de contatos chamada "SecurityContacts" CSDMs/CAs para você usar em incidentes ou notificações relacionados à segurança. As etiquetas de contato em você instances/resources são usadas para incidentes gerados pela AMS, se você tiver fornecido seu consentimento ao CSDM para usar as informações da tag.

Para saber mais sobre esse serviço de notificação, consulte [Notificações](#).

Gerenciamento de solicitações de serviço

Tópicos

- [Quando usar uma solicitação de serviço](#)
- [Como funciona o gerenciamento de solicitações de serviço](#)
- [Testando uma solicitação de serviço no AMS](#)
- [Criando uma solicitação de serviço no AMS](#)
- [Monitoramento e atualização de solicitações de serviço no AMS](#)
- [Respondendo a uma solicitação de serviço gerada pelo AMS](#)

Solicitações de serviço são comunicações ao AMS criadas por você para solicitar informações ou conselhos. Um bom exemplo de solicitação de serviço padrão é para orientação ou ajuda na configuração de um serviço AMS, como o Alarm Manager, o Patch Orchestrator e assim por diante. Você também pode receber solicitações de serviço do AMS; elas são chamadas de solicitações de serviço de saída ou notificações de serviço. Para ver uma lista de suas solicitações de serviço e solicitações de serviço de saída (notificações de serviço) enviadas a você pelo AMS, consulte a página Solicitações de serviço do console do AMS.

Para saber mais sobre solicitações de serviço de saída, consulte [Respondendo a uma solicitação de serviço gerada pelo AMS](#).

Você cria uma solicitação de serviço do AWS Managed Services (AMS) usando o console do AMS ou, programaticamente, usando a Suporte API. Para obter detalhes sobre como usar a API, consulte [Suporte API](#). Para AMS, escolha o código sentinel-service-request de serviço.

Depois que sua solicitação de serviço é recebida pela equipe de operações do AMS, ela é priorizada de acordo com seu contrato de nível de serviço. Para se manter informado em cada etapa do

processo de resolução da solicitação de serviço, preencha a opção CC Emails e, se você quiser se conectar por federação, faça login antes de seguir o link no e-mail enviado pelo AMS.

Use a página Criar Solicitação de Serviço do console AMS para realizar as seguintes tarefas:

- Criar e atualizar uma solicitação de serviço
- Obtenha uma lista e informações detalhadas sobre todas as suas solicitações de serviço atuais
- Limite sua busca por solicitações de serviço por datas e identificadores de incidentes, incluindo solicitações que foram resolvidas
- Adicione comunicações e anexos de arquivos às suas solicitações e adicione destinatários de e-mail para correspondência de casos
- Resolver solicitações de serviço
- Classifique as comunicações de solicitação de serviço

Quando usar uma solicitação de serviço

Os exemplos a seguir descrevem uma solicitação de serviço:

- AMS ou orientação AWS geral
- Perguntas relacionadas ao Patch MW
- Perguntas relacionadas ao cronograma de backup
- Perguntas sobre a funcionalidade dos AWS serviços

Veja a seguir exemplos do que não deve ser gerado em uma solicitação de serviço:

- Problemas de acesso
- Falha no patch
- Falha no backup
- Falha de RFC ou RFC que causa interrupção de negócios (incidente de uso para interrupção de negócios)
- Perguntas de RFC ou entrada adicional ou alteração do escopo da RFC (use correspondência bidirecional de RFC)

Como funciona o gerenciamento de solicitações de serviço

As solicitações de serviço são tratadas pela equipe de operações do AMS de plantão.

Depois que sua solicitação de serviço é recebida pela equipe de operações do AMS, ela é analisada para garantir que a solicitação não seja classificada de forma mais adequada como um incidente. Se ele deve ser classificado como um incidente, ele é imediatamente reclassificado, a equipe de gerenciamento de incidentes do AMS assume o controle e você é notificado.

Se a solicitação de serviço puder ser resolvida com o envio de uma RFC, o operador de revisão enviará um e-mail solicitando que você envie a RFC apropriada (os detalhes são fornecidos).

Se o operador do AMS puder resolver a solicitação de serviço, as etapas para fazer isso serão tomadas imediatamente. Por exemplo, se a solicitação de serviço for para consultoria de arquitetura ou outras informações, o operador encaminhará você para os recursos apropriados ou responderá diretamente à pergunta.

Se a análise da sua solicitação de serviço identificar um bug ou uma solicitação de recurso, o AMS enviará uma notificação por meio da solicitação de serviço. Como não há ETA para solicitações de recursos ou correções de bugs, a solicitação de serviço original foi encerrada. Entre em contato com seu CSDM para fazer perguntas de acompanhamento relacionadas à solicitação de serviço original.

Se a solicitação de serviço estiver fora do escopo das operações do AMS, a operadora enviará a solicitação ao seu gerente de prestação de serviços em nuvem para que ele possa se comunicar com você, ou à equipe de AWS operações apropriada, junto com um e-mail para você, sobre quais etapas estão sendo tomadas.

A solicitação de serviço não é resolvida até que você indique que está satisfeito com o resultado.

Note

Recomendamos fornecer um e-mail de contato, nome e número de telefone em todos os casos para facilitar a comunicação.

Testando uma solicitação de serviço no AMS

Ao testar solicitações de serviço do AMS, pedimos que você inclua no texto do assunto esta sinalização: `AMSTestNoOpsActionRequired` para que o AMS saiba que a solicitação de serviço é

apenas para testes. Quando os engenheiros de operações do AMS veem essa bandeira, eles não respondem à solicitação de serviço.

Criando uma solicitação de serviço no AMS

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 à cobrança, crie um caso de solicitação de serviço no Support Center Console.

YouTube Vídeo: [Como e quando levantar solicitações de serviço do AWS Console e quais são seus objetivos de nível de serviço?](#)

Monitoramento e atualização de solicitações de serviço no AMS

Você pode atualizar, monitorar e revisar relatórios de incidentes e solicitações de serviço, ambos chamados de casos, usando o console do AMS ou programaticamente usando a Suporte API. Para obter informações sobre como usar a Suporte API, consulte [DescribeCases](#) operação.

Para monitorar um caso, incidente ou solicitação de serviço usando o console do AMS, siga estas etapas.

1. No console do AMS, Relatórios de incidentes ou painel de solicitações de serviço, navegue até um caso e escolha o Assunto para abrir uma página de detalhes com o status atual e as correspondências.

Quando um incidente relatado ou um caso de solicitação de serviço é atualizado pela equipe de operações do AMS, você recebe um e-mail e um link para o incidente no console do AMS para poder responder. Você não pode responder à correspondência do incidente respondendo ao e-mail.

 Important

Você deve ter inserido um endereço de e-mail para receber notificações de mudança de estado para uma solicitação de serviço ou caso de incidente. As notificações só vão para o endereço de e-mail adicionado ao caso quando ele é criado.

O link no e-mail de notificação não funcionará, a menos que você esteja usando um servidor de e-mail na sua rede federada do AMS. No entanto, você pode responder à correspondência acessando o console do AMS e usando a página de detalhes do caso.

2. Se houver muitos casos na lista, você poderá usar a opção Filtro:
 - Todos abertos (padrão): use esse filtro para ver todos os casos que não foram resolvidos.
 - Não atribuído: use se você acabou de enviar o caso e não recebeu nenhum aviso de que o estado do caso mudou. Observe que os incidentes e os casos de solicitação de serviço são tratados com rapidez diferente, dependendo da prioridade enviada (incidentes) ou do seu contrato de nível de serviço (solicitações de serviço).
 - Abrir: use se você recebeu uma notificação de que o caso é uma ação “Amazon pendente”; isso significa que o caso foi atribuído, mas o trabalho ainda não começou.
 - Reaberto: use se você recebeu um aviso de que o caso foi reaberto depois de ter sido resolvido.
 - Trabalho em andamento: use se você recebeu um aviso de que um operador começou a trabalhar no caso.
 - Ação pendente do cliente: use se você tiver recebido uma solicitação de ação do operador de sua parte.

- Ação do cliente concluída: use se você recebeu uma notificação de que sua ação no caso foi processada.
 - Resolvidos: use para ver casos que você sabe que foram resolvidos. Os casos resolvidos são mantidos no histórico por doze meses.
 - Qualquer status: use esse filtro para ver todos os casos, independentemente do status.
3. Para verificar o status mais recente, atualize a página.
 4. Se houver tantas correspondências que nem todas apareçam na página, escolha Carregar mais.
 5. Para atualizar o status do caso, escolha Responder, insira a nova correspondência e escolha Enviar.
 6. Para encerrar o caso após ele ter sido resolvido de forma satisfatória, escolha Fechar caso.

Não se esqueça de avaliar o serviço por meio da classificação de 1 a 5 estrelas para que a AMS saiba como estamos indo!

Respondendo a uma solicitação de serviço gerada pelo AMS

O gerenciamento de patches do AMS envia solicitações de serviço (também conhecidas como notificação de serviço) para você antes da janela de manutenção definida; para obter mais informações, consulte [Janela de manutenção do AMS](#). [O AMS também envia notificações de serviço para você quando há uma chance de sua infraestrutura ser afetada por um AWS serviço ou quando uma EC2 instância em sua conta precisar ser reinicializada; para obter mais informações, consulte Notificações de serviço.](#)

Note

O AMS envia comunicações para o endereço de e-mail principal da sua AWS conta que você forneceu; recomendamos adicionar um alias alternativo de e-mail de contato de Operações para facilitar o processo de gerenciamento de solicitações ou notificações de serviço. A adição desses e-mails é abordada durante o processo de integração do AMS e a documentação de integração relacionada.

Perguntas sobre faturamento

Para enviar uma pergunta relacionada ao faturamento, conclua as seguintes etapas:

1. Abra o [AWS Support Centro](https://console.aws.amazon.com/support/) em <https://console.aws.amazon.com/support/> casa#/.
2. Escolha Conta e cobrança.
3. Escolha Criar caso.
4. Escolha Conta e cobrança e siga as instruções para enviar seu caso.

Operações sob demanda

Operations on Demand (OOD) é um recurso do AWS Managed Services (AMS) que amplia o escopo padrão do seu plano de operações do AMS fornecendo serviços operacionais que atualmente não são oferecidos nativamente pelos [planos de operações do AMS](#) ou. AWS Depois de selecionada, a oferta do catálogo é fornecida por uma combinação de automação e recursos altamente qualificados de AMS. Não há compromissos de longo prazo ou contratos adicionais, permitindo que você amplie seu AMS existente, suas AWS operações e capacidades conforme necessário. Você concorda em comprar blocos de horas (blocos OOD), 20 horas por bloco, mensalmente.

Você pode selecionar no catálogo de ofertas padronizadas e iniciar um novo contrato de OOD por meio de uma solicitação de serviço. Exemplos de ofertas de OOD incluem assistência na manutenção do Amazon EKS, nas operações e no gerenciamento de AWS Control Tower clusters SAP. Novas ofertas de catálogos são adicionadas regularmente com base na demanda e nos casos de uso operacional que vemos com mais frequência.

O OOD está disponível para os planos de operações do AMS Advanced e do AMS Accelerate e está disponível em todos os [Regiões da AWS](#) lugares onde o AMS está disponível.

O AMS realiza o Gerenciamento de Riscos de Segurança do Cliente (CSRM) enquanto implementa as alterações solicitadas. Para saber mais sobre o processo de CSRM, consulte Revisões de [segurança da solicitação de alteração](#).

Catálogo de ofertas do Operations on Demand

O Operations on Demand (OOD) oferece os serviços descritos na tabela a seguir.

Note

Para obter as definições dos principais termos, consulte a documentação [Key Terms](#) da documentação do AWS Managed Services.

Plano de operações	Título	Descrição	Resultados esperados

AMS Accelerate	Manutenção do cluster Amazon EKS	O AMS libera seus desenvolvedores de contêineres gerenciando a manutenção contínua de suas implantações do Amazon Elastic Kubernetes Service (Amazon EKS). O AMS executa end-to-end os procedimentos necessários para atualizar um cluster abordando os componentes do plano de controle, complementos e nós. O AMS realiza a atualização dos tipos de nós gerenciados, bem como de um conjunto selecionado de complementos do Amazon EKS e do Kubernetes.	As equipes de clientes ajudaram no trabalho operacional subjacente de atualização dos clusters do Amazon EKS.

AMS Accelerate	Construção e venda de AMI	O AMS fornece gerenciamento contínuo da construção e venda de AMI para os clientes. Nossos engenheiros realizam uma versão mensal de atividades de patching emergentes assinadas e sob AMIs demanda AMIs, gerenciam alterações usando runbooks e monitoram compilações de AMI usando o Monitoring. CloudWatch Também fornecemos assistência para solução de problemas e relatórios detalhados para todos os AMIs usados nas contas designadas. Essa oferta exige que os pipelines de criação da AMI sejam implantados por meio do EC2 Image Builder. O AMS não oferece suporte a nenhuma outra automação ou serviço que interaja com o EC2 Image Builder.	A postura de segurança do cliente melhorou e o tempo gasto pelo cliente na construção e venda AMIs foi reduzido.

AMS Accelerate	Execução de mudanças com curadoria	Trabalhe com nossos engenheiros de operações qualificados para traduzir seus requisitos de negócios em solicitações de mudança validadas que possam ser executadas com segurança em seu AWS ambiente. Aproveite nossa abordagem exclusiva de automação e o conhecimento das melhores práticas operacionais (por exemplo, avaliação de impacto, reversões, regra de duas pessoas), seja uma simples mudança em grande escala ou uma ação complexa com impactos posteriores.	Os clientes ajudaram a definir, criar e executar solicitações de alteração personalizadas. As alterações podem ser manuais ou automatizadas (CloudFormation, SSM). Inclui consulta Suporte para orientação de configuração, quando necessário. Não se destina a alterações no código do aplicativo, na instalação/implantação do aplicativo, na migração de dados ou nas alterações na configuração do sistema operacional.

AMS Accelerate	AWS Network Firewall Operações	O AMS colabora com você para integrar seu firewall e implementar e gerenciar as políticas e regras para operações contínuas de firewall. Nossos engenheiros fazem isso aproveitando nossas melhores práticas operacionais e automação para configurar políticas e regras padronizadas e permitindo o monitoramento para detectar alterações feitas fora do processo de automação. O AMS notifica você rapidamente sobre alterações indesejadas e fornece opções para incluí-las, se solicitado, ou restaurar a conta para uma configuração anterior para garantir a estabilidade geral de seus sistemas.	As equipes de clientes ajudaram a reduzir a sobrecarga de gerenciamento detectando rapidamente alterações não intencionais no firewall da rede, resultando em melhor resolução de incidentes e redução do tempo de análise da causa raiz de problemas esperados e inesperados.
AMS Accelerate	AWS Control Tower operações	Operações e gerenciamento contínuos de sua zona de AWS Control Tower, incluindo AWS Transit Gateway e AWS Organizations - fornecendo uma solução abrangente de zona de pouso. Lidamos com vendas de contas, gerenciamento de SCP e OU, correção de desvios, gerenciamento de usuários de SSO e AWS Control Tower atualizações com nossa biblioteca de controles e proteções personalizados.	As equipes de clientes ajudaram em alguns dos trabalhos operacionais subjacentes de gerenciamento AWS Control Tower, AWS Transit Gateway e AWS Organizations.

AMS Accelerate	AWS landing zone Acelere as operações	O AMS fornece operações contínuas de zonas de AWS pouso implantadas por meio do AWS Landing Zone Accelerator (LZA). Nossos engenheiros lidam com alterações nos arquivos de configuração, gerenciamento do ambiente AWS Control Tower (CT) (venda de contas, criação de UO, grades de proteção de CT), gerenciamento de políticas de controle de serviços (SCP), detecção e remediação de desvios de CT, gerenciamento de configuração de rede e atualizações da CT e da estrutura LZA. AWS O LZA fornece um meio de configurar e governar um AWS ambiente seguro com várias contas usando as melhores práticas operacionais e serviços, como. AWS Control Tower	As equipes de clientes ajudaram nas operações e no gerenciamento contínuos da solução AWS Landing Zone Accelerator.

AMS Accelerate	SAP Cluster Assist	Alarme, monitoramento, correção de clusters, backup e remediação de incidentes dedicados para seus clusters SAP. Esse item do catálogo permite que você descarregue parte do trabalho operacional contínuo de sua equipe de operações da SAP para que ela possa se concentrar no gerenciamento de capacidade e no ajuste de desempenho.	As equipes SAP de clientes ou parceiros ajudaram em alguns dos trabalhos operacionais subjacentes. Ainda exige que o cliente forneça outros recursos SAP, como gerenciamento de capacidade, ajuste de desempenho, DBA e administração baseada em SAP.

AMS Accelerate	SQL Server em EC2 operações	O AMS colabora com você para integrar, implementar e gerenciar as operações contínuas de seus bancos de dados SQL Server implantados em instâncias. EC2 Nossos engenheiros utilizam nossas melhores práticas operacionais e automação para liberar suas equipes de banco de dados executando tarefas como backup e aplicação de patches, estendendo o suporte operacional do AMS à aplicação de patches do SQL Server para incluir atualizações contínuas com reconhecimento de cluster, serviços de backup e restauração alinhados à nossa estratégia de defesa contra ransomware e monitorando a adesão aos controles de backup e patches fornecidos pelo cliente.	Os clientes do SQL Server ajudaram a aliviar as operações de patches e backup do banco de dados para melhorar a resiliência e a postura de segurança de suas cargas de trabalho, além de otimizar os custos de licença trazendo suas próprias licenças (BYOL) para o. EC2

AMS Avançado	Manutenção do cluster Amazon EKS	O AMS libera seus desenvolvedores de contêineres ao lidar com a manutenção e a integridade de contínuas de suas implantações do Amazon Elastic Kubernetes Service (Amazon EKS). O AMS executa end-to-end os procedimentos necessários para atualizar um cluster abordando os componentes do plano de controle, complementos e nós. O AMS realiza a atualização dos tipos de nós gerenciados, bem como de um conjunto selecionado de complementos do Amazon EKS e do Kubernetes.	As equipes de clientes ajudaram no trabalho operacional subjacente de atualização dos clusters do Amazon EKS.
AMS Avançado	Execução prioritária de RFC	Capacidade designada de engenheiro de operações da AMS para priorizar a execução de suas solicitações de mudança (RFC). Todos os envios recebem um nível mais alto de resposta e a ordem prioritária pode ser ajustada interagindo diretamente com os engenheiros por meio de uma sala de reuniões do Amazon Chime.	Os clientes recebem um SLO de resposta de 8 horas por RFCs.

AMS Advanced e AMS Accelerate	Atualização do sistema operacional legado	Evite a migração de instâncias atualizando as instâncias para uma versão compatível do sistema operacional. Podemos realizar uma atualização local em suas instâncias selecionadas aproveitando a automação e os recursos de atualização dos fornecedores de software (por exemplo, Microsoft Windows 2008 R2 para Microsoft Windows 2012 R2). Essa abordagem é ideal para aplicativos legados que não podem ser facilmente reinstalados em uma nova instância e fornece proteção adicional contra ameaças de segurança conhecidas e não mitigadas em versões mais antigas do sistema operacional. Os seguintes sistemas operacionais são compatíveis com atualizações no local: • Microsoft Windows 2012 R2 para Microsoft Windows 2016 e superior • Microsoft Windows 2016 a Microsoft Windows 2022 e superior • Red Hat Enterprise Linux 7 para Red Hat Enterprise Linux 8 • Red Hat Enterprise Linux 8 para Red Hat Enterprise Linux 9 • Oracle Linux 7 para Oracle Linux 8	Essa solução é fornecida para aplicativos que não podem mais ser reinstalados em uma nova instância (por exemplo, código-fonte perdido, ISV fora do mercado etc.). Você pode reverter as atualizações com falha de volta ao estado original. Do ponto de vista operacional, a reversão é preferível porque coloca a instância em um estado mais compatível com os patches de segurança mais recentes.

Tópicos

- [Solicitando operações de AMS sob demanda](#)
- [Fazendo alterações nas ofertas do Operations on Demand](#)

Solicitando operações de AMS sob demanda

O AWS Managed Services (AMS) Operations on Demand (OOD) está disponível para todos os Contas da AWS que foram integrados ao AMS. Para aproveitar as vantagens do Operations on Demand, solicite informações adicionais ao seu gerente de prestação de serviços em nuvem (CSDM), arquiteto de soluções (SA), gerente de contas ou arquiteto de nuvem (CA). As ofertas de OOD disponíveis estão listadas na tabela anterior do [catálogo de ofertas do Operations on Demand](#). Depois que o escopo do contrato for concluído, envie uma solicitação de serviço à AMS Operations para iniciar um contrato para o OOD.

Cada solicitação de serviço de OOD deve conter as seguintes informações detalhadas relacionadas ao contrato:

- As ofertas específicas de OOD solicitadas e para cada oferta específica de OOD:
 - O número de blocos (um bloco equivale a 20 horas de tempo de recursos operacionais em um determinado mês civil, a serem cobrados de acordo com a taxa padrão vigente para a oferta de Operações sob Demanda aplicável) a serem alocados à oferta específica de OOD. AWS
 - O ID da conta de cada conta do AWS Managed Services para a qual a oferta específica de OOD está sendo solicitada.

As solicitações de serviço OOD devem ser enviadas por você por meio de:

- A conta do AWS Managed Services que recebe as ofertas aplicáveis de Operations on Demand, ou
- Uma conta do AWS Managed Services que é uma conta AWS Organizations de gerenciamento no modo de todos os recursos, em nome de qualquer uma de suas contas membros que sejam contas do AWS Managed Services.

Depois que a solicitação de serviço OOD é recebida, a AMS Operations analisa e atualiza as contas com sua aprovação, aprovação parcial ou negação.

Depois que a solicitação de serviço de ofertas de OOD for aprovada, você e a AMS se coordenam para iniciar o contrato. Nenhuma oferta de OOD é iniciada até que a solicitação de serviço seja aprovada e a data de início do contrato seja acordada.

O AMS usa uma alocação mensal de assinaturas de blocos OOD. Alocamos o número aprovado de blocos mensalmente, a partir da data de início do contrato, até que você solicite a exclusão por meio de uma nova solicitação de serviço. Os blocos OOD são válidos por um mês civil. Blocos não utilizados, ou partes de blocos, não são acumulados nem transferidos para os próximos meses.

Você recebe uma cobrança mínima de um bloco de OOD por mês, independentemente do número de horas realmente usadas. Qualquer bloco OOD adicional alocado, no qual nenhuma hora tenha sido usada, não será cobrado.

Fazendo alterações nas ofertas do Operations on Demand

Para solicitar alterações nos contratos contínuos das ofertas de Operations on Demand (OOD), envie uma solicitação de serviço contendo as seguintes informações:

- A (s) modificação (ões) solicitada (s), e
- A data solicitada para que as modificações entrem em vigor.

Depois de receber a solicitação de serviço OOD, a AMS Operations analisa a solicitação e atualiza com sua aprovação ou solicita que o CSDM designado trabalhe com você para determinar o escopo e as implicações da modificação. Se for determinado que a modificação exige um esforço de definição de escopo com o CSDM, você deverá enviar uma segunda solicitação de serviço de OOD para iniciar o contrato modificado após a conclusão do exercício de definição de escopo.

Depois de aprovada, a alocação de blocos modificada mais recentemente se torna e continua ativa, substituindo quaisquer alocações de blocos anteriores, a menos que acordado de outra forma entre você e você. AWS

Histórico do documento

A tabela a seguir descreve as mudanças importantes em cada versão do Guia do Usuário Avançado do AMS. Para receber notificações sobre atualizações dessa documentação, é possível inscrever-se em um feed RSS.

- Versão da API: 2019-05-21
- Novo ou atualizado CTs e instruções passo a passo: Histórico do documento de referência do AMS [Advanced Change Type](#).
- Novo AMS AMIs: [Imagens de máquinas AMS Amazon \(AMIs\)](#).

Alteração	Descrição	Data
Tabela atualizada para AWS Identity and Access Management (IAM) nos controles padrão na seção AMS Advanced	Informações atualizadas na tabela sobre políticas do IAM e acesso aos buckets do Amazon S3.	25 de setembro de 2025
Etapa atualizada para consultas relacionadas ao faturamento	Etapa atualizada para criar solicitações de serviço para consultas relacionadas ao faturamento na seção Criação de uma solicitação de serviço no AMS.	25 de setembro de 2025
Informações atualizadas para notificações por e-mail para tipos de alteração	Informações atualizadas e exemplo para adicionar notificações por e-mail para tipos de alteração na seção Configurar notificações por e-mail RFC (console).	25 de setembro de 2025
Tipo de alteração atualizado	Seção atualizada de marcação automática da infraestrutura do AMS com tipo de alteração	25 de setembro de 2025

para marcar recursos criados pelo AMS.

[Perguntas frequentes sobre a VM atualizada Import/Export no AWS Managed Services](#)

Atualizou a RFC usada para solicitar um perfil de instância para permitir que as ferramentas executem comandos a partir da instância.

24 de setembro de 2025

[Solicitação de alteração \(RFC\) atualizada para iniciar uma instância do SUSE Linux Enterprise Server for SAP Applications 15 SP6](#)

Etapa 2 atualizada sobre como iniciar uma nova SP6 instância do SUSE Linux Enterprise Server for SAP Applications 15 com o RFC correto.

22 de setembro de 2025

[Solicitação de alteração atualizada \(RFC\)](#)

Atualizado AWS Elastic Disaster Recovery na seção de perguntas frequentes do AWS Managed Services com o RFC correto para criar as funções do IAM necessárias em sua conta.

22 de setembro de 2025

[Foram adicionadas 4 novas verificações de otimização de Trusted Advisor custos suportadas pelo Trusted Remediator](#)

Foram adicionadas as seguintes verificações de otimização de custos:

- c1z7kmr00n - Recomendações de otimização de custos da Amazon para instâncias EC2
- c1z7kmr02n - Recomendações de otimização de custos do Amazon EBS para volumes
- c1z7kmr03n - Recomendações de otimização de custos do Amazon RDS para instâncias de banco de dados
- c1z7kmr05n - recomendações de otimização de custos para funções AWS Lambda

22 de setembro de 2025

[Nota atualizada para zonas de disponibilidade \(AZs\)](#)

Informações atualizadas sobre grupos de segurança no AMS.

5 de setembro de 2025

[Tipo de alteração atualizado](#)

Amazon atualizada FSx na seção de perguntas frequentes do AWS Managed Services com o tipo de alteração para compartilhar o AD gerenciado com a conta do aplicativo.

5 de setembro de 2025

Tipo de alteração atualizado	Amazon DocumentDB atualizado na seção de perguntas frequentes do AWS Managed Services com o tipo de alteração para usar a exclusão. APIs	5 de setembro de 2025
Tipo de alteração atualizado	A seção de perguntas frequentes do Alexa for Business no AWS Managed Services foi atualizada com o tipo de alteração para dois usuários do IAM com acesso limitado para instalar e operar seu gateway do Alexa for Business.	5 de setembro de 2025
Tipo de alteração atualizado	AppStream Versão 2.0 atualizada na seção de perguntas frequentes do AWS Managed Services com o tipo de alteração para criar e escolher uma função do IAM que estará disponível em todas as instâncias de streaming da frota	5 de setembro de 2025
Tipo de alteração atualizado	Atualizado EventBridge na seção de perguntas frequentes do AWS Managed Services com o tipo de alteração para solicitar uma função de EventBridge serviço antes de usar EventBridge para acionar outros AWS recursos.	5 de setembro de 2025

<u>Suporte atualizado para verificações de Trusted Advisor segurança do Trusted Remediator</u>	Os parâmetros e restrições pré-configurados suportados foram atualizados para verificação Hs4Ma3G108 - as trilhas devem ser integradas ao Amazon Logs CloudTrail CloudWatch	5 de setembro de 2025
<u>Suporte atualizado para verificações de Trusted Advisor segurança do Trusted Remediator</u>	Verificação Trusted Advisor de segurança atualizada para adicionar a versão 2 do Hs4Ma3G184 - O registro em log do Application Load Balancers e do Classic Load Balancers deve estar ativado	5 de setembro de 2025
<u>Verificações de excelência Trusted Advisor operacional atualizadas suportadas pela seção Trusted Remediator</u>	Verificações de excelência Trusted Advisor operacional atualizadas suportadas pela seção Trusted Remediator para adicionar a nova verificação suportada c1fd6b96l4 Amazon S3 Access Logs Enabled.	28 de agosto de 2025
<u>Tipo de alteração atualizado</u>	Altere o tipo da função personalizada do IAM.	25 de agosto de 2025
<u>Atualizado usando o CloudWatch Application Insights para .Net e SQL server na seção AMS</u>	Tipo de alteração revisado para usar o CloudWatch Application Insights.	25 de agosto de 2025
<u>Solicitação de alteração atualizada (RFC)</u>	Solicitação de alteração (RFC) para adicionar mais tags ao bucket do Amazon S3.	25 de agosto de 2025

Solicitação de alteração atualizada (RFC)	Solicitação de alteração (RFC) para marcar todos os recursos criados pelo AMS para fins de gerenciamento.	25 de agosto de 2025
Lambda atualizado na seção de perguntas frequentes do AWS Managed Services	Tipo de alteração revisado para acesso a outros AWS serviços para criar fontes de eventos.	25 de agosto de 2025
Lambda atualizado na seção de perguntas frequentes do AWS Managed Services	Tipo de alteração revisado para provisionar funções Lambda.	25 de agosto de 2025
Seção Criar, alterar ou excluir grupos de segurança atualizada	Tipo de alteração revisado para criar um grupo de segurança fora das pilhas e VPCs	25 de agosto de 2025
Seção Trusted Remediator atualizada para incluir novo conteúdo para o Compute Optimizer	A seção Trusted Remediator foi atualizada para incluir novo conteúdo para AWS Compute Optimizer recomendações suportadas.	18 de agosto de 2025
O link do glossário do TOC foi removido	AWS Glossário.	8 de agosto de 2025
Recomendação precisa do tipo de alteração	Para integrar sua métrica de cliente ao seu sistema de monitoramento de aplicativos, solicite que o AMS crie um tópico do Amazon SNS para a métrica enviando uma RFC com a seção Implantação Monitoramento e notificação SNS Create CT (ct-3dfng lm4ombbs).	8 de agosto de 2025

[Recomendação precisa do tipo de alteração](#)

Para excluir volumes de instância de espaço reservado, envie um item Gerenciamento | Componentes avançados da pilha | Volume do EBS | Excluir tipo de alteração (ct-3e3h8u0sp5z80).

8 de agosto de 2025

[Novos alertas de monitoramento: SecureChannelFailure e Broken Secure Channel](#)

[Alertas do monitoramento de linha de base no AMS](#) [AMS \(correção automática de alertas\)](#).

8 de agosto de 2025

[Novas verificações do Trusted Remediator](#)

[Trusted Advisor verificações de otimização de custos suportadas pelas verificações de Trusted Advisor segurança do Trusted Remediator suportadas pelo Trusted Remediator](#)
Hs4Ma3G120— AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime, Hs4Ma3G230— 2 e c18d2gz150— 2. AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV
AWSManagedServices-TerminateEC InstanceStoppedForPeriodOfTime

8 de agosto de 2025

[Atualização do padrão IAM no ponto 3.2](#)

Linguagem esclarecida e menção removida à marcação.

25 de julho de 2025

Atualização das opções de cancelamento de alertas	A adição de uma tag permite que você opte por não receber mais dois alertas.	25 de julho de 2025
Depreciação do serviço de provisionamento de autoatendimento	O CloudEndure serviço de provisionamento de autoatendimento está sendo descontinuado em favor do. AWS Application Migration Service	25 de julho de 2025
Novo recurso para backups	Personalize as notificações nos cofres de backup com uma nova tag.	25 de julho de 2025
Tabela de controles atualizada	Alguns controles duplicados foram removidos na seção AMS-STD-002 - AWS Identity and Access Management (IAM) da tabela.	26 de junho de 2025
Pré-requisitos atualizados do serviço AWS Transfer Family SSP	Informações adicionadas à seção de pré-requisitos.	26 de junho de 2025
Exemplo de política do IAM atualizado	Exemplo de política do IAM atualizado com mais restrições, conforme recomendado.	26 de junho de 2025
Suporte para AMI atualizada OSes	Adicionou o Ubuntu Linux 24.04 ao Ubuntu Linux 22.04 e alterou todas as referências para SP5 . SP6	26 de junho de 2025
Serviço de provisionamento de autoatendimento, obsoleto MediaStore	Nota de depreciação adicionada para. AWS Elemental MediaStore	26 de junho de 2025

Serviço de provisionamento de autoatendimento, Amazon Inspector Classic obsoleto	Foi adicionada uma nota de descontinuação para o Amazon Inspector Classic.	26 de junho de 2025
Serviço de provisionamento de autoatendimento, Amazon Connect obsoleto	Foi adicionada uma nota de suspensão de uso para o Amazon Connect.	26 de junho de 2025
Seção atualizada para configurações suportadas no AMS	Configurações suportadas atualizadas para sistemas operacionais suportados e sistemas operacionais Supported End of Support (EOS) no AMS.	25 de junho de 2025
Serviço de provisionamento de autoatendimento, obsoleto WorkDocs	Página removida e referências à obsoleta WorkDocs.	19 de junho de 2025
Nota de segurança importante e sobre gerenciamento de patches para repositórios alternativos de patches	Nota de segurança importante e melhores práticas para usar repositórios alternativos de patches no AMS.	10 de junho de 2025
Atualizações de sistemas operacionais compatíveis	Os sistemas operacionais compatíveis com o AMS Advanced são atualizados, alguns adicionados e outros removidos.	22 de maio de 2025
Somente interno APIs	Somente internos APIs que aparecem em alguns registros . CloudWatch	22 de maio de 2025

Atualizações do AMS Trusted Remediator	Como usar um novo parâmetro, <code>preconfigured-parameters</code> , para personalizar as Trusted Advisor verificações no Trusted Remediator.	22 de maio de 2025
Atualizações do SSP Amazon Elastic Container Registry	Mais funções são provisionadas automaticamente quando você integra o serviço Amazon ECR.	8 de maio de 2025
Perguntas frequentes e atualizações do AMS Advanced Trusted Remediator.	Várias atualizações nas Trusted Advisor verificações suportadas, perguntas frequentes sobre o Trusted Remediator (adicionada “Quais recursos o Trusted Remediator implanta em suas contas?”) e muito mais. Veja também as Trusted Advisor verificações suportadas pelo Trusted Remediator .	8 de maio de 2025
Atualização dos controles de segurança do AMS Advanced Standard.	Foram adicionados controles de “Compartilhamento de grupos de segurança”.	8 de maio de 2025
Namespaces protegidos pelo AMS Advanced.	Espaços de nomes protegidos pelo AMS EPSMarketplaceSubscriptionRole e EPS adicionados.	24 de abril de 2025
Localizações de registro do AMS Advanced.	Localizações de registro adicionais adicionadas.	24 de abril de 2025

[Modo de provisionamento de autoatendimento avançado do AMS para atualização dos pré-requisitos AppStream 2.0.](#)

Um pré-requisito para AppStream 2.0 foi adicionado: você deve incluir um nome de bucket do Amazon S3 ao enviar a RFC de provisionamento para o serviço.

24 de abril de 2025

[Novo alerta de remediação automática do AMS Advanced do Amazon RDS.](#)

ID do alerta: - 0224, é acionado quando o armazenamento alocado solicitado atinge ou excede o limite máximo de armazenamento configurado.

27 de março de 2025

[O AMS Advanced AWS fechou o acesso de novos clientes à Amazon CloudSearch, a partir de 25 de julho de 2024.](#)

Os clientes existentes ainda podem usar o serviço, mas não haverá novos recursos.

27 de março de 2025

[O AMS Advanced AWS encerrou o acesso de novos clientes ao AWS CodeCommit, a partir de 25 de julho de 2024.](#)

Os clientes existentes ainda podem usar o serviço, mas não haverá novos recursos.

27 de março de 2025

[O Trusted Remediator já está disponível.](#)

O Trusted Remediator, uma solução do AWS Managed Services que automatiza a correção de AWS Trusted Advisor cheques, já está disponível.

19 de março de 2025

[AMS Advanced Novo alerta RDS de remediações automáticas.](#)

RDS-EVENT-0224 adicionado.

17 de março de 2025

Novo recurso do AMS Advanced: notificações de incidentes.	Você pode usar AppRegistry para criar aplicativos e personalizar as notificações de incidentes para esses aplicativos.	13 de março de 2025
Atualização do AMS para o limite de monitoramento de alarmes do RDS.	O limite do alarme de utilização média da CPU do RDS foi alterado de 75% para 90%.	20 de fevereiro de 2025
Relatórios de autoatendimento atualizados com novas opções de dados para visualização agregada de relatórios	Foram adicionadas opções de dados para incluir o novo Nome do campo:Admin Account ID, Nome do campo do conjunto de dados: aws_admin_account_id e Definição: Trusted AWS Organization account enabled by the customer para os seguintes relatórios de autoatendimento: • Relatório de patch (diário) • Relatório de backup (diário) • Relatório de incidentes (semanal)	28 de janeiro de 2025
Atualização para o AWS Batch SSP	Você pode usar o seguinte RFC para provisionar AWS Batch em sua conta do AMS: Gerenciamento Serviço da AWS Serviço autoprovisionado Adicionar (ct-1w8z66n899dct).	28 de janeiro de 2025

Novo recurso do AMS: relatórios de autoatendimento agregados	Os relatórios de autoatendimento agregados (SSR) fornecem uma visão dos relatórios de autoatendimento existentes agregados no nível da organização, entre contas.	21 de janeiro de 2025
Atualização na seção Forecast SSP	Observação adicionada: 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.	10 de janeiro de 2025
Atualização para a seção de namespaces protegidos por AMS	Foi adicionado um namespace protegido ausente (*mc, *MC e *Mc) à lista de namespaces protegidos pelo AMS.	9 de janeiro de 2025
Atualização para a seção Como o monitoramento funciona	Foram adicionadas informações sobre um novo recurso, configurando notificações de alerta por recurso ou ID da instância, em vez de por incidente.	8 de janeiro de 2025
Atualizado: conteúdo de atualização baseado em tags	Corrigido o erro de digitação no nome da chave e o caminho incorreto do arquivo de configuração corrigido.	6 de janeiro de 2025

[Atualizado: AMS AMI Notes](#)

O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.

21 de novembro de 2024

[Tabela atualizada de ofertas do Operations On Demand](#)

Os seguintes sistemas operacionais são compatíveis com atualizações no local:

11 de novembro de 2024

- Microsoft Windows 2016 a Microsoft Windows 2022 e superior

[Tabela atualizada de ofertas do Operations On Demand](#)

Os seguintes sistemas operacionais são compatíveis com atualizações no local:

1.º de novembro de 2024

- Microsoft Windows 2012 R2 para Microsoft Windows 2016 e superior
- Red Hat Enterprise Linux 7 para Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 8 para Red Hat Enterprise Linux 9
- Oracle Linux 7 para Oracle Linux 8

[Configurações suportadas atualizadas](#)

Os sistemas operacionais Oracle Linux compatíveis foram atualizados para 9.0-9.3, 8.0-8.9, 7.5-7.9.

24 de outubro de 2024

[Imagens atualizadas do AMS Amazon Machine \(AMIs\)](#)

Atualizado com base no Windows AMIs para remover o Windows 2012 e 2012 R2. Atualizado baseado em Linux AMIs para remover várias AMIS que não são mais suportadas e adicionar o seguinte:

24 de outubro de 2024

- Amazon Linux (2ARM64)
- RHEL 9
- Servidor SUSE Linux Enterprise 15 SP5

[Agora você pode incluir vários endereços de e-mail em alertas baseados em tags.](#)

Agora, vários endereços de e-mail são compatíveis com alertas baseados em tags.

20 de setembro de 2024

[Foi adicionada a seção de revisões de segurança da solicitação de alteração.](#)

Foi adicionada uma nova seção que fornece detalhes sobre o processo de revisão de segurança da solicitação de alteração.

17 de setembro de 2024

[Nova seção adicionada.](#)

Uma nova seção descreve como as revisões de segurança de solicitações de alteração ocorrem no AMS Advanced já está disponível.

12 de setembro de 2024

[Novo serviço suportado pelo AMS Advanced.](#)

AWS Resilience Hub agora é compatível com o AMS Advanced.

30 de agosto de 2024

[Novos serviços suportados pelo AMS Advanced.](#)

Cinco novos serviços agora são suportados pelo AMS Advanced:

21 de agosto de 2024

- Amazon Bedrock
- Amazon Kendra
- Amazon Quantum Ledger Database (Amazon QLDB)
- AWS Service Catalog AppRegistry
- Amazon Managed Service para Prometheus

[Uma nova configuração padrão de rede de segurança de terminais já está disponível.](#)

A fonte de atualização agora está incluída nas configurações de rede padrão do EPS.

21 de agosto de 2024

[Atualizado: AMS AMI Notes](#)

O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.

30 de julho de 2024

[O AMS agora oferece suporte ao Amazon Route 53 Resolver DNS Firewall.](#)

O AMS agora oferece suporte ao Amazon Route 53 Resolver DNS Firewall

30 de julho de 2024

[AWS DataSync Atualização do SSPS](#)

AWS DataSync não exige mais o prefixo “datasync-” nos nomes de bucket do Amazon S3.

30 de julho de 2024

[Painel de regras de configuração de segurança](#)

O painel de regras do Security Config agora está disponível nos relatórios de autoatendimento.

24 de julho de 2024

O AMS agora oferece suporte ao Oracle Linux 8.9, RHEL 8.10 e RHEL 9.4.	O AMS agora oferece suporte ao Oracle Linux 8.9, RHEL 8.10 e RHEL 9.4.	5 de julho de 2024
Amazon Bedrock agora disponível no modo de provisionamento de autoatendimento	Agora você pode solicitar o Amazon Bedrock no modo AMS SSP.	27 de junho de 2024
Amazon Route 53 Resolve eventos de firewall DNS no Security Incident Response	O AMS agora monitora os eventos do firewall DNS do Amazon Route 53 Resolver no Security Incident Response	21 de junho de 2024
Foram adicionadas informações adicionais sobre como ativar o recurso Traga seu próprio EPS (BYOEPS) do AMS.	Foram adicionadas informações adicionais sobre como ativar o recurso Traga seu próprio EPS (BYOEPS) do AMS.	5 de junho de 2024
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	23 de maio de 2024
Informações adicionadas sobre o uso de uma função personalizada AWS Amplify no modo de provisionamento de autoatendimento (somente em ambientes MALZ).	Instruções adicionadas sobre como os ambientes MALZ podem usar uma função personalizada AWS Amplify no modo de provisionamento de autoatendimento.	23 de maio de 2024
O Amazon Kendra agora está disponível no modo de provisionamento de autoatendimento.	O Amazon Kendra agora está disponível no modo de provisionamento de autoatendimento.	23 de maio de 2024

O AMS Advanced oferece suporte a sistemas operacionais adicionais.	O AMS Advanced é compatível com Red Hat Enterprise Linux (RHEL) 9.x e Ubuntu 20.04 e 22.04.	25 de abril de 2024
O AMS Advanced oferece suporte à ARM64 arquitetura do Amazon Linux 2.	O AMS Advanced oferece suporte à ARM64 arquitetura do Amazon Linux 2.	25 de abril de 2024
Offboard atualizado a partir da seção de contas da zona de pouso com várias contas (MALZ).	Foram adicionadas informações detalhadas sobre como desativar contas Application e Core da landing zone de várias contas.	11 de abril de 2024
Atualizado: descrição do gerenciamento de solicitações de serviço.	Descrição atualizada do gerenciamento de solicitações de serviço no tópico Descrição do serviço.	21 de março de 2024
Atualizado: seção de compromissos do serviço de gerenciamento de incidentes.	Foi adicionado um link para o Acordo de Nível de Serviço do AMS.	21 de março de 2024
Atualizado: seção Como funciona o gerenciamento de solicitações de serviço.	Foi adicionado um esclarecimento sobre como o AMS lida com solicitações de serviço que contêm uma solicitação de recurso ou um bug.	21 de março de 2024
Atualizado: Obtenha a seção de suporte.	A seção Obter suporte foi atualizada para incluir uma nova seção de perguntas sobre faturamento.	21 de março de 2024

Atualizado: Provisionamento automatizado do IAM pelo AMS	Provisionamento AMS Automated IAM atualizado com informações personalizadas da lista de negação	21 de março de 2024

Atualizações anteriores

A tabela a seguir descreve as mudanças importantes na documentação do guia avançado do AMS antes de março de 2024.

Alteração	Descrição	Link
Fevereiro de 2024		
Sistemas operacionais suportados atualizados	Sistemas operacionais compatíveis atualizados para incluir o SUSE Linux Enterpris e Server 15 SP5.	Consulte Configurações compatíveis
Nota adicionada aos alertas do monitoramento de linha de base no AMS.	Foi adicionada uma nota indicando que o alarme para uso de volume EC2 não raiz está desativado por padrão.	Consulte Alertas do monitoramento de linha de base no AMS
Foi adicionada uma nova seção Roteador de Eventos AMS ao Monitoramento e gerenciamento de eventos.	Foi adicionada uma nova seção discutindo o AMS Advanced Event Router.	Consulte Usando as regras EventBridge gerenciadas da Amazon no AMS
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	Veja AMIs. csv-and-notes02.2024
Fevereiro de 2024		

Alteração	Descrição	Link
Foi adicionada uma nova seção para a função vinculada ao serviço de EventBridge regras da Amazon para o AMS Advanced	Foi adicionada uma nova seção para a função vinculada ao serviço de EventBridge regras da Amazon para o AMS Advanced na seção Segurança da infraestrutura.	Consulte a função vinculada ao serviço de EventBridge regras da Amazon para o AMS Advanced
Seção atualizada do Modo de provisão de autoatendimento	Foi adicionada uma nova seção para o novo Amazon Inspector no modo de provisão de autoatendimento.	Veja o Amazon Inspector Classic (AMS SSPS)
Janeiro de 2024		
Seção atualizada de gerenciamento de eventos planejados (PEM)	Foram adicionados detalhes adicionais e um FAW ao gerenciamento de eventos planejados (PEM).	Consulte Gerenciamento de eventos planejados no AWS Managed Services
Foi adicionada uma nova seção para instalação automática do SSM Agent	Foi adicionada uma nova seção para a instalação automática do SSM Agent na Configuração automatizada de EC2 instâncias.	Consulte Instalação automática do SSM Agent
Adicionado AWS Resilience Hub (AMS SSPS)	Foi adicionado um novo serviço SSPS.	Consulte Use o AMS SSP para provisionar AWS Resilience Hub em sua conta AMS
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	Veja AMIs. csv-and-notes01.2024

Alteração	Descrição	Link
Dezembro de 2023		
Modo de mudança direta atualizado no AMS	Foi adicionada uma nova subseção, Casos de uso do Modo de Alteração Direta, ao modo de Mudança Direta no AMS.	Consulte Modo de mudança direta no AMS
Atualizado AWS Amplify (AMS SSPS)	Perguntas frequentes atualizadas para esclarecer que é necessária uma aceitação de risco para solicitar o Amplify.	Consulte Use o AMS SSP para provisionar AWS Amplify em sua conta AMS
Novo AWS Elastic Disaster Recovery (AMS SSPS)	Adicionado um novo serviço SSPS	Consulte Use o AMS SSP para provisionar AWS Elastic Disaster Recovery em sua conta AMS
Novo Amazon Managed Service para Prometheus (AMS SSPS)	Adicionado um novo serviço SSPS	Consulte Use o AMS SSP para provisionar o Amazon Managed Service para Prometheus em sua conta AMS
Atualizada a seção Como funciona o gerenciamento de continuidade.	Foi adicionada uma nova subseção, monitoramento e relatórios de backup do AMS.	Consulte Como funciona o gerenciamento de continuidade
Novo Amazon DevOps Guru (AMS SSPS)	Adicionado um novo serviço SSPS	Consulte Use o AMS SSP para provisionar o Amazon DocumentDB (com compatibilidade com o MongoDB) em sua conta AMS

Alteração	Descrição	Link
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	Veja AMIs. csv-and-notes0,12.2023
Novembro de 2023		
Amazon CloudWatch Synthetics (AMS SSPS) atualizado	Atualizado FAQs para usar os nomes de função corretos.	Consulte Use o AMS SSP para provisionar Amazon CloudWatch Synthetics em sua conta AMS
Modo de provisionamento de autoatendimento atualizado do Amazon API Gateway	Foi adicionada uma função adicional <code>customer_apigateway_cloudwatch_role</code> à seção API Gateway.	Consulte Use o AMS SSP para provisionar o Amazon API Gateway em sua conta AMS
Adicionou um novo serviço ao modo de provisionamento de autoatendimento	Adicionado AWS Service Catalog AppRegistry à seção do modo de provisionamento de autoatendimento	Consulte Use o AMS SSP para provisionar AWS Service Catalog AppRegistry em sua conta AMS
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	Veja AMIs. csv-and-notes1 de novembro de 2023
Setembro de 2023		

Alteração	Descrição	Link
Adicionou uma nota ao Usando o Patch Orchestrator	A seguinte nota foi adicionada à seção Usando o Patch Orchestrator: “Os alertas de falha de patch não são criados para instâncias que têm sistemas operacionais sem suporte ou que são interrompidas durante a janela de manutenção”	Consulte Gerenciamento de patches no AMS
Criptografia de dados atualizada com serviços adicionais	Serviços adicionados à criptografia de dados no AMS.	Consulte Proteção de dados no AMS
Novo parágrafo adicionado às mensagens de erro do RFC.	Foi adicionado um novo parágrafo para adicionar o link Criar uma solicitação de serviço.	Consulte Solução de problemas de erros de RFC no AMS
Nomes de função do IAM corrigidos.	Corrigido o nome da função do IAM customer_emr_cluster_autoscaling_role.	Consulte Modo de provisionamento de autoatendimento no AMS
Informações de monitoramento de linha de base atualizadas	Foi removida a referência a dois alarmes obsoletos e. RDSRead LatencyAlarm RDSWrite LatencyAlarm	Consulte Alertas do monitoramento de linha de base no AMS
agosto de 2023		
Adicionado: Resposta a incidentes de segurança do AMS	Foi adicionada documentação para usar o AMS Security Incident Response.	Consulte Resposta a incidentes de segurança no AMS
Julho de 2023		

Alteração	Descrição	Link
Adicionado: Provisionamento automatizado do IAM	Foi adicionada documentação para usar o provisionamento automatizado do IAM.	Consulte Provisionamento automatizado de IAM (AMS)
Atualizado: tabela de funções do Access	Foram adicionadas funções ausentes para o AMS Access.	Consulte Funções do IAM para acesso à conta do cliente do AMS
Junho de 2023		
Atualizado: Lista de alertas de RDS monitorados.	Atualizou a lista de alertas do RDS para o monitoramento básico do AMS. 9 novos tipos de alerta do RDS foram adicionados e 3 tipos de alertas do RDS existentes foram removidos.	Consulte Alertas do monitoramento de linha de base no AMS .
Atualizado: tabela de funções do Access	Novas funções para o AMS Security.	Consulte Funções do IAM para acesso à conta do cliente do AMS
Maio de 2023		
Atualizado: Política de data de início do faturamento de serviços.	Definições atualizadas da data de início do faturamento.	Consulte Termos-chave do AMS .
Abril de 2023		

Alteração	Descrição	Link
Atualizado: Relatório mensal de autoatendimento de cobrança.	Observação adicional: os relatórios de cobrança mensal estão disponíveis somente em uma conta do Management Payer (landing zone multicontas do AMS Advanced), mas estão disponíveis para todas as contas vinculadas gerenciadas pelo AMS Accelerate.	Consulte Relatório de cobrança (mensal) .
Atualizado: conteúdo "Patching padrão" removido	O AMS usa o Patch Orchestrator.	Gerenciamento de patches no AMS
Atualizado: O que é AMS?	Alguns tópicos foram transferidos anteriormente para O que é AMS? para fazer parte da descrição do serviço AMS.	Service description (Descrição do serviço)
Atualizado: desembarcando a landing zone de várias contas	Fez vários esclarecimentos.	Extraia as contas multicontas da landing zone do AMS
Atualizado: AWS Transfer Family (AMS SSPS)	Link adicionado para o tutorial de configuração de transferência.	Use o AMS SSP para provisionar AWS Transfer Family em sua conta AMS
Conteúdo atualizado: provisionamento de autoatendimento	Substituído "CodeSuite" por "Serviços de código" de acordo com as normas legais da AWS.	Use o AMS SSP para provisionar serviços do Código AMS em sua conta AMS
Conteúdo atualizado: CloudWatch métricas e alarmes	Link adicionado para Exemplo: Contar ocorrências de um termo .	Criação de CloudWatch métricas e alarmes personalizados no AMS

Alteração	Descrição	Link
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	AMIs. csv-and-notes 04.2023
Março de 2023		
Conteúdo atualizado: desativação do AMS	Esclareceu quais recursos são excluídos quando as contas de landing zone com várias contas são excluídas	Extraia as contas multicontas da landing zone do AMS
Atualizado: AMS AMIs	Foi adicionado um link para o arquivo ZIP da AMI para cada mês na seção Histórico do documento.	Histórico do documento
Atualizado: remediação automática	Suporte LVM removido para automação de EC2 volume.	Remediação automática de alertas pelo AMS
Atualizado: Patch RACI	Várias atualizações e esclarecimentos sobre o RACI para aplicação de patches.	Matriz de responsabilidade da AMS (RACI)
Conteúdo atualizado: provisionamento de autoatendimento	Foi adicionado um bullet de perguntas frequentes. Para iniciar um novo agente AWS Datasync, a ingestão de WIGS não é necessária.	Modo de provisionamento de autoatendimento no AMS
Conteúdo atualizado: provisionamento de autoatendimento	Foi adicionado um bullet de perguntas frequentes. Para iniciar um novo agente AWS Datasync, a ingestão de WIGS não é necessária.	Modo de provisionamento de autoatendimento no AMS

Alteração	Descrição	Link
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	AMIs. csv-and-notes03.2023
Fevereiro de 2023		
Conteúdo atualizado: desativação do AMS	Esclareceu como desativar ambientes de landing zone e contas de aplicativos com várias VPCs contas	Contas AMS externas
Conteúdo atualizado: Finding ARNs	Foi adicionada a CLI <code>describe-table</code> do DynamoDB para encontrar um ARN de tabela do DynamoDB	Encontre nomes de recursos da Amazon (ARNs) no AMS

Alteração	Descrição	Link
Conteúdo atualizado: provisionamento de autoatendimento	A opção AMS "CodeSuit e" foi removida, pois não é um SSPS real. Você ainda pode usar o tipo de alteração Gerenciamento AWS serviço Serviço autoprovisionado Adicionar (revisão obrigatória) (ct-3qe6io8t6jtny) e solicitar os três serviços: e. CodeBuild CodeDeploy CodePipeline Em seguida, o AMS provisionará as seguintes funções do IAM em sua conta: customer_codebuild_service_role customer_codedeploy_service_role , aws_code_pipeline_service_role e. Depois de provisionado em sua conta, você deve integrar a função em sua solução de federação.	Modo de provisionamento de autoatendimento no AMS
Conteúdo atualizado: atualização do Secrets Manager	Funções corrigidas necessárias para a zona de pouso com várias contas (MALZ) versus zona de pouso com uma única conta (SALZ).	Perguntas frequentes sobre compartilhamento de chaves usando o Secrets Manager
Conteúdo atualizado: correção automática de alertas pelo AMS	Foi adicionado suporte para volumes do Logical Volume Manager (LVM).	EC2 automação de remediação de uso de volume

Alteração	Descrição	Link
Conteúdo atualizado: AMS Amazon Machine Images (AMIs)	Foi adicionada a seção Offboarding AMS AMIs com código de amostra para remover AMIs da sua conta.	Imagens de máquinas AMS Amazon (AMIs)
Conteúdo atualizado: função de usuário do IAM	Atualizou a política do IAM: AMSBilling Política.	Função de usuário do IAM no AMS
Novo conteúdo: Não suportado OSes	Foram adicionadas informações sobre quais serviços o AMS fornece para sistemas operacionais não suportados (OSes).	Capacidades para sistemas operacionais não suportados no AMS
Conteúdo atualizado: relatórios sob demanda	Alguns relatórios sob demanda não estão disponíveis no AMS Advanced e foram erroneamente exibidos como disponíveis.	Relatórios sob solicitação
Conteúdo atualizado: desativação de contas AMS	Instruções esclarecidas para desativar as contas do aplicativo MALZ.	Contas externas do aplicativo AMS
Conteúdo atualizado: Secrets Manager	Foram corrigidos os nomes das funções do IAM necessárias para usar o Secrets Manager.	Perguntas frequentes sobre o Secrets Manager in AWS Managed Services
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	AMIs. csv-and-notes 02.2023

Janeiro de 2023

Alteração	Descrição	Link
Novo conteúdo: AWS Device Farm (AMS SSPS)	Foi adicionado um novo serviço SSPS: AWS Device Farm.	Use o AMS SSP para provisionar AWS Device Farm em sua conta AMS
Atualizado: versões compatíveis do Windows	Foi adicionado suporte para o Windows Server 2022.	Imagens de máquinas AMS Amazon (AMIs), Configurações compatíveis, e Notificações AMI do AMS com SNS
Atualizado: gerenciamento de continuidade	As regras do plano de backup padrão do AMS foram atualizadas.	Planos de backup padrão, landing zone com várias contas
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	AMIs. csv-and-notes01.2023
Dezembro de 2022		
Atualizado: Usando bastiões	Link incorreto corrigido.	Acessando instâncias usando bastiões
Atualizado: Agendador de recursos	Fiz várias melhorias e adicionou links ao Agendador de AWS Instâncias para obter mais contexto.	Agendador de recursos do AWS Managed Services

Alteração	Descrição	Link
Atualizado: Windows AMIs e configurações suportadas (para novos Windows AMIs)	Conteúdo atualizado da AMI do AMS adicionado do EC2 Launch (Windows Server 2016 e posterior) ao EC2 Launch (Windows Server 2016 e Windows Server 2019) e adicionado o EC2 LaunchV2 (Windows Server 2022 e posterior). Atualizado com base no Windows do AMIs Microsoft Windows Server (2012, 2012 R2, 2016 e 2019) para o Microsoft Windows Server (2012, 2012 R2, 2016, 2019 e 2022).	Imagens de máquinas AMS Amazon (AMIs) e Service description (Descrição do serviço)
Atualizado: seção Resourced Scheduler	Métodos aprimorados para implantar e personalizar o AMS Resource Scheduler.	Agendador de recursos do AWS Managed Services
Atualizado: Configurando o AMS: DNS público e privado	Atualizado o diagrama da arquitetura do DNS.	Configurando DNS público e privado
Atualizado: arquitetura de rede MALZ	Atualizou o diagrama e adicionou orientações para contas de aplicativos do Accelerate.	Arquitetura de rede MALZ
Atualizado: Configuração: Usando tags	Nova observação: a marcação personalizada só é suportada para contas de aplicativos MALZ, não para contas principais.	Etiquetagem automática da infraestrutura AMS

Alteração	Descrição	Link
Atualizado: Gerenciamento de acesso: usando bastiões	Introdução atualizada para incluir bastiões do RDP.	Economizando custos em bastiões de landing zone de conta única (SALZ)
Atualizado: configurações padrão do AMS: alertas	EC2 Instância adicionada: Uso de volume não raiz à tabela de alertas.	Alertas do monitoramento de linha de base no AMS
Atualizado: Gerenciamento de continuidade	Orientações adicionais sobre backups contínuos.	Como funciona o gerenciamento de continuidade
Atualizado: configuração automatizada da EC2 instância	Foi adicionado suporte para PowerBroker Identity Service (PBIS) e On Instance Code (OIC).	Atualize automaticamente o PBIS em instâncias Linux e Atualize automaticamente o código em instâncias Linux
Atualizado: Provisionamento de autoatendimento para Secrets Manager	Atualizou o CT para adicionar o Secrets Manager à sua conta (abaixo FAQs).	Use o AMS SSP para provisionar AWS Secrets Manager em sua conta AMS
Atualizado: gerenciamento de registros	Atualizou a lista de registros em EC2 nível de sistema.	Amazon Elastic Compute Cloud (Amazon EC2) — registros em nível de sistema
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	AMIs. csv-and-notes1 de dezembro de 2022
Novembro de 2022		
Atualizado: AMS Amazon Machine Images (AMIs)	Versões atualizadas do SUSE Linux suportadas.	Imagens de máquinas AMS Amazon (AMIs)

Alteração	Descrição	Link
Atualizado: contas MALZ	Foi adicionada orientação para excluir uma conta de aplicativo gerenciada pelo cliente.	Contas de aplicativos gerenciadas pelo cliente
Atualizado: Configurando o AMS	Adição do customer-ams-amazon2-security-enhanced .	Notificações AMI do AMS com SNS
Atualizado: Como o monitoramento funciona	Explicação atualizada das notificações de serviço e relatórios de incidentes.	Como funciona o monitoramento
Atualizado: tipos de conta do aplicativo MALZ	Melhorou a explicação dos tipos de conta.	Tipos de conta de aplicativo
Atualizado: modo de desenvolvedor	Foi adicionado um aviso sobre o modo Desenvolvedor.	Antes de começar com o modo AMS Developer
Atualizado: gerenciamento de eventos planejados	Foi adicionada a seção: Tipos de PEM	Gerenciamento de eventos planejados no AWS Managed Services
Atualizado: Amazon Machine Images (AMIs)	Versões atualizadas do SUSE Linux suportadas	Imagens de máquinas AMS Amazon (AMIs)
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	AMIs. csv-and-notes 1 de novembro de 2022
Outubro de 2022		
Novo: Configuração automatizada de instâncias	A nova seção descreve o processo de configuração automatizada de instâncias.	Configuração automatizada de instâncias no AMS Advanced

Alteração	Descrição	Link
Novo: Somente a tomografi a computadorizada manual é aceitável para alguns SSPS	Atualizou mais de 50 serviços de provisionamento de autoatendimento FAQs para usar a CT manual e não a CT automatizada para adicionar SSPS.	Modo de provisionamento de autoatendimento no AMS
Atualização: Configurando o AMS	Foram adicionadas duas políticas aos perfis de instância EC2 do Amazon IAM para MALZ.	EC2 Perfil de instância do IAM
Novo: Biblioteca de regras personalizadas de detetive e prevenção.	Adicionamos um conjunto de exemplos de políticas de controle de serviço (SCPs) e controles preventivos de regras do Config com base no que aprendemos com vários clientes.	Regras selecionadas SCPs e de configuração
Atualização: AWS Backup aviso	Foi adicionado um aviso: “Não edite os planos de backup do AMS, pois suas alterações podem ser perdidas. Em vez disso, crie novos planos de backup usando ct-2hyozbpa0sx0m para suas configurações personalizadas.”	Como funciona o gerenciamento de continuidade
Atualização: AWS Backup cuidado	Foi adicionada uma observação sobre a adição de novas funções do IAM à sua federação.	Implantação de recursos do IAM no AMS Advanced

Alteração	Descrição	Link
Atualização: gerenciamento de monitoramento	Os alertas geram relatórios de incidentes, não solicitações de serviço.	Como funciona o monitoramento
Atualização: traga seu próprio EPS	Aplica-se tanto ao SALZ quanto ao MALZ.	AMS: traga seu próprio EPS
Atualização: Accelerate a conta do aplicativo	Esclareceu que sua conta do Accelerate é uma conta do aplicativo.	Tipos de conta de aplicativo
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	AMIs. csv-and-notes ¹ de outubro de 2022
Setembro de 2022		
Atualizado: exemplos de comandos CLI para encontrar recursos	Foi adicionado um novo exemplo e disse que a --region opção pode ser necessária.	Encontrando os dados de que você precisa (SKMS), AMS
Atualizado: provisionamento de funções do IAM	Agora, as funções do IAM podem ser criadas e gerenciadas com AWSManagedServicesCloudFormationAdminRole o.	Criação de pilhas usando o modo Direct Change
Atualizado: Normas técnicas da AMS	Registro AMS-STD-007: (#20) Requisitos de encaminhamento esclarecidos.	Segurança e conformidade

Alteração	Descrição	Link
Atualizado: como funciona o gerenciamento de continuidade	A redação do Start Backup Job foi revisada para “sob demanda” em vez de “existente”.	Como funciona o gerenciamento de continuidade
Atualizado: Segurança e conformidade	Descrição e orientação atualizadas para o padrão AMS-STD-007 número 20: registros de encaminhamento entre contas.	Segurança e conformidade
Atualizado: casos de uso do gerenciamento de mudanças	Foi removido um link quebrado para o antigo Guia do Usuário do Change Management.	Casos de uso do gerenciamento de mudanças
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	AMIs. csv-and-notes09.2022
11 de agosto de 2022		

Alteração	Descrição	Link
Atualizado: os cabeçalhos dos capítulos para consistência e legibilidade mudaram algumas subseções do tópico para seções mais apropriadas	“Arquitetura de rede MALZ” e “Arquitetura de rede SALZ” são agora, ambas, subseções da seção “Arquitetura de rede” de nível superior, anteriormente a seção “Arquitetura de rede AMS” “Modos de gerenciamento de mudanças” é o novo título de “Gerenciamento de mudanças” “Configurações padrão” agora é uma subseção de “Configurando o AMS” “Regra de declaração do AD FS e configurações de SAML” (anteriormente “regra de declaração dos Serviços de ActiveDirectory Federação (ADFS) e configurações de SAML” agora é uma subseção de “Configurando o AMS” “Gerenciamento de acesso” é o novo título para “Acesso no AMS” e é movido para cima no TOC “Encontrar os dados de que você precisa” é o novo título para “Gerenciamento do conhecimento de serviços”	O que é o AWS Managed Services?

Alteração	Descrição	Link
	“Relatórios e opções” é o novo título para “Relatórios do AMS” e está mais abaixo no TOC “Operações sob demanda” agora é o último tópico do TOC	
Atualizado: Encontrando e ARN, Novo: Encontrando um recurso com um ARN	Ambos os procedimentos foram completamente reescritos para fins de utilidade.	Encontre nomes de recursos da Amazon (ARNs) no AMS e Encontre recursos por ARN no AMS .
Atualizado: Conectando seu CMA ao Transit Gateway	A automação não suporta a adição de rotas aos domínios de rotas principais, e o procedimento precisa ser atualizado.	Conectando seu CMA com o Transit Gateway
Atualizado: preços dos componentes básicos do MALZ	Todos os preços estão em dólares americanos, formatados com cifrões.	Componentes básicos do ambiente AMS
Atualizado: AMS AMI Notes	O arquivo zip inclui notas sobre as imagens mais recentes da máquina AMS Amazon (AMIs) e um arquivo CSV das mais recentes AMIs.	AMIs. csv-and-notes.08.2022
14 de julho de 2022		
Atualizado: Relatórios de autoatendimento	Foram adicionadas instruções para criptografar AWS Glue metadados com chaves KMS.	Relatórios de autoatendimento

Alteração	Descrição	Link
Atualizado: monitoramento de linha de base do AMS	Alerta DeleteRecoveryPoint de backup adicionado.	Alertas do monitoramento de linha de base no AMS
Atualizado: sistemas operacionais compatíveis	Data de fim do suporte adicionada para Amazon Linux 2.	Configurações compatíveis
Atualizado: Provisionamento de autoatendimento	Foi adicionado um pré-requisito para o AWS Transfer SSPS.	Use o AMS SSP para provisionar AWS Transfer Family em sua conta AMS
Atualizado: Relatórios do AMS	Foi adicionada uma observação sobre as regiões de aceitação.	Relatórios e opções
Atualizado: correspondência e anexo do RFC	Tipos de arquivo de texto permitidos esclarecidos; em particular, os arquivos YAML devem terminar em .yaml (não .yml).	Adicionar correspondência e anexos RFC (console)
21 de junho de 2022		
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.	Visão geral dos modos.
Novo alarme	Adicionou um AWS Backup alarme.	Alertas do monitoramento de linha de base no AMS
16 de junho de 2022		

Alteração	Descrição	Link
Novo conteúdo	Gerenciamento de incidentes. Incidentes que não são um risco de segurança agora podem ser resolvidos pelo AMS com sua aprovação no relatório de incidentes e não precisam de uma RFC e aprovação separadas.	Gerenciamento de incidentes
Conteúdo atualizado	MALZ: Diagrama de arquitetura de rede atualizado. Atualizações: o emparelhamento de VPC da conta principal VPC para serviços compartilhados vpc deve ser removido, pois não existe.	Arquitetura da conta de rede
	Serviço provisionado de autoatendimento (SSPS) do Sagemaker. Atualizado com a nova função do IAM adicionada na integração para uso do Sagemaker.	Use o AMS SSP para provisionar o Amazon SageMaker AI em sua conta AMS

Alteração	Descrição	Link
	À lista de notificações AMIs compatíveis com SNS: Foram adicionados customer-ams-sles 12, customer-ams-sles 15, customer-ams-amazon 1 com segurança aprimorada, 8, customer-ams-rhel 8 com segurança aprimorada, 18, 2012, 2019 e customer-ams-rhel 2019 com segurança aprimorada. customer-ams-ubuntu customer-ams-windows customer-ams-windows Removido customer-ams-rhel 6 e customer-ams-rhel 6, com segurança aprimorada AMIs.	Notificações AMI do AMS com SNS
	E-mails de escalonamento removidos.	Obter ajuda no AWS Managed Services
	A lista de tópicos foi movida para os parágrafos iniciais abaixo.	O que é o AWS Managed Services?
	Registros de serviço atualizados com links melhores para registros de balanceamento de carga, também reformata dos.	Registros de serviços agregados do AMS

Alteração	Descrição	Link
Serviço de provisionamento de autoatendimento (SSPS) da EKS. Foram adicionadas as informações sobre como habilitar a criptografia de segredos de envelope em seu cluster.	Use o AMS SSP para provisionar o Amazon EKS AWS Fargate em sua conta AMS	
09 de junho de 2022		
Conteúdo atualizado, Obtendo ajuda	Os e-mails do caminho de escalonamento foram removidos. O AMS fornece métodos de comunicação por meio de relatórios de incidentes, solicitações de serviço RFCs e.	Obter ajuda no AWS Managed Services
12 de maio de 2022		
Novo conteúdo, modelo de assinatura de Operations on Demand (OOD)	O AMS mudou a integração do Operations on Demand do modelo atual de inscrição e renovação para uma alocação de assinaturas e um modelo de aceitação padrão. Ao integrar uma conta AMS, você é automaticamente inscrito no Operations on Demand agora.	Operações sob demanda
14 de abril de 2022		
Novo conteúdo, otimização de custos	O AMS fornece recomendações para otimização de custos.	Otimização de custos no AWS Managed Services

Alteração	Descrição	Link
Conteúdo atualizado, conta Accelerate no MALZ	Um nome de função incorreto (CustomerDefaultAdminRole) foi atualizado para o nome de função correto (AccelerateDefaultAdminRole).	Contas AMS Accelerate Seção “Acessando sua conta do Accelerate”.
Conteúdo atualizado, acesso ao AMS, funções do IAM	Foram adicionadas outras funções do AMS IAM usadas para acessar suas contas.	Por que e quando o AMS acessa sua conta Seção “Funções do IAM para acesso à conta do cliente do AMS”.
Conteúdo atualizado, planos de backup do AMS	Planos de backup gerenciados pelo AMS adicionados.	Planos de backup do AMS e Cofres de backup do AMS
Conteúdo atualizado, AWS Secrets Manager	Atualizou o FAQ.	Use o AMS SSP para provisionar AWS Secrets Manager em sua conta AMS
Conteúdo atualizado, integração do Direct Change Mode (DCM)	O AMS não oferece suporte à integração de clientes do Service Catalog ao DCM.	Introdução ao modo Direct Change
Conteúdo atualizado, descrição do serviço	Esclareceu a seção Serviços Suportados: • Amazon EKS em AWS Fargate -> Amazon Elastic Kubernetes Service em Fargate • Amazon ECS para Fargate -> Amazon Elastic Container Service em Fargate AWS • Amazon Kinesis -> Amazon Kinesis Data Streams	AWS Serviços suportados

Alteração	Descrição	Link
Conteúdo atualizado, desativação de contas MALZ	Atualizado para fazer referência a novos tipos de alteração nas contas de aplicativos de desativação.	Contas externas do aplicativo AMS
Conteúdo atualizado, gerenciamento de incidentes no modo Desenvolvedor	Descrição atualizada do SLA do incidente para: O AMS SLA não se aplica a recursos criados ou atualizados fora do AMS Change Management (incluindo o Modo Desenvolvedor), portanto, os recursos atualizados ou criados no modo Desenvolvedor são automaticamente degradados para P3 e o suporte é o melhor esforço.	Gerenciamento de incidentes no modo AMS Developer
Conteúdo atualizado, integração do DCM	O modelo de RFC para o novo DCM agora inclui um campo para o ARN do seu provedor de SAML.	Introdução ao modo Direct Change
Conteúdo atualizado, DCM para CloudFormation	As instruções para criar e atualizar CloudFormation pilhas agora incluem exemplos de YAML.	Transformação AMS
Conteúdo atualizado, conta MALZ Tools	Há uma nova função do IAM para migrações: <code>AWSManagedServicesMigrationRole</code> .	AWS Serviço de migração de aplicativos (AWS MGN) e Habilitar o acesso à nova conta do AMS Tools

Alteração	Descrição	Link
Novo conteúdo, contas de landing zone com várias contas	Você pode criar uma conta Accelerate em sua conta de gerenciamento de AMS com várias contas na landing zone.	Contas AMS Accelerate
Conteúdo atualizado, instalação o API/CLI do SDK	As instruções de instalação listaram o nome de arquivo errado para Mac/Linux instalações e um comando incorreto. Isso foi corrigido.	Usando a API e a CLI do AMS
Conteúdo atualizado, conta Accelerate no MALZ	Havia um nome de regra incorreto (CustomerDefaultAdminRole), ele foi atualizado para o correto (AccelerateDefaultAdminRole).	Contas AMS Accelerate , seção “Acessando sua conta do Accelerate”
Conteúdo atualizado, monitoramento	O monitoramento do uso raiz foi revisado de 85% para 95%.	Alertas do monitoramento de linha de base no AMS
Conteúdo atualizado, notificações da AMI	Você pode criar vários tipos de notificações de SNS para novos AMS AMIs. Adicionam os informações sobre a criação de vários tipos.	Notificações AMI do AMS com SNS
Conteúdo atualizado, configurações padrão do AMS	Referências removidas ao Macie Classic, substituídas por Macie.	Alertas do monitoramento de linha de base no AMS
Conteúdo atualizado, prefixos reservados do AMS	Em ordem alfabética, a lista de prefixos reservados.	Prefixos reservados do AMS

Alteração	Descrição	Link
Conteúdo atualizado, descrição do serviço	As seções de recursos sobre gerenciamento de mudanças e provisionamento de autoatendimento foram atualizadas com mais informações sobre os modos do AMS.	Recursos do plano operacional do AWS Managed Services (AMS) AMS Advanced
Conteúdo atualizado, AWS Secrets Manager	Compartilhando chaves usando o Secrets Manager.	10 de fevereiro de 2022
Novo conteúdo, provisionamento de autoatendimento, Amazon Connect	Foram adicionadas perguntas frequentes sobre como solicitar a adição de uma lista de países para chamadas de saída ou entrada.	10 de fevereiro de 2022
Novo conteúdo, provisionamento de autoatendimento, Amazon EKS no Fargate	Foi adicionada uma restrição de perguntas frequentes de que a implantação de clusters EKS por meio do kit de desenvolvimento AWS em nuvem (CDK) ou do CloudFormation Ingest não é suportada no AMS.	10 de fevereiro de 2022
Conteúdo alterado, modo de desenvolvedor	Correção, você não usa uma RFC ou uma solicitação de serviço para atribuir usuários à sua solução de federação, você mesmo faz isso dependendo da sua solução.	10 de fevereiro de 2022

Alteração	Descrição	Link
Conteúdo alterado, modo Direct Change (DCM)	Observe que o IAM não é compatível com o DCM.	10 de fevereiro de 2022
	DCM, observe as validações que fazemos.	10 de fevereiro de 2022
	DCM, esclareça as restrições de diferentes funções.	10 de fevereiro de 2022
Conteúdo alterado, monitoramento de alertas de linha de base	Os alertas de recursos do cluster Redshift foram alterados.	10 de fevereiro de 2022
Conteúdo alterado, relatórios de autoatendimento	Foi adicionado o nome exato do bucket s3, (ams-reporting-data-a<Account_ID>) para os clientes usarem para buscar os relatórios.	10 de fevereiro de 2022

Alteração	Descrição	Link
Conteúdo alterado, conteúdo atualizado para referenciar tipos de alterações automatizadas em vez de Gerenciamento manual Outros Outros (MOO)	Conteúdo atualizado da conta do aplicativo de várias contas da landing zone (MALZ) para fazer referência aos tipos de alteração automatizada (três, “Associar o anexo do TGW a uma tabela de rotas”, “Criar rotas nas tabelas de rotas do TGW para se conectar a esta VPC” e “Configurar suas tabelas de rotas da VPC para apontar para o gateway de trânsito da zona de pouso multiconta do AMS”). Recebendo alertas gerados pelo AMS Notificações de alerta baseadas em tags	10 de fevereiro de 2022
Conteúdo alterado: AMS AMIs.	Foram adicionadas novas informações sobre segurança aprimorada AMIs. Consulte Configurações compatíveis, e. Imagens de máquinas AMS Amazon (AMIs) Segurança aprimorada AMIs	27 de janeiro de 2022
Novo conteúdo: provisionamento por autoatendimento.	Foi adicionado o Amazon Fsx para OpenZFS. Consulte Use o AMS SSP para provisionar o Amazon FSx for OpenZFS em sua conta AMS.	27 de janeiro de 2022

Alteração	Descrição	Link
Conteúdo alterado: serviço de provisionamento de autoatendimento (SSPS) Code-Deploy.	Nome da função adicional e nota de restrição adicional . Consulte Use o AMS SSP para provisionar AWS CodeDeploy em sua conta AMS	27 de janeiro de 2022
Conteúdo alterado: links atualizados.	Links quebrados corrigidos: AMS-AMIs, Encontrar suas configurações, Encontrar um ID de pilha, Encontrar um ID de VPC ListVpcSummaries, ListStackSummaries, e. GetStack APIs Por exemplo, consulte Encontre uma pilha IDs no AMS .	13 de janeiro de 2022
Conteúdo alterado: EKS Support for Fargate	Limitação adicionada para FAQs: EC2 Não há suporte para criar ou gerenciar grupos de nós com o EKS. Consulte Use o AMS SSP para provisionar o Amazon EKS AWS Fargate em sua conta AMS .	13 de janeiro de 2022
Conteúdo alterado: CloudFormation, Modo de mudança direta (DCM)	Instruções adicionais para criar ou atualizar pilhas de CF usando o. AmsStackTransform Consulte Criação de pilhas usando o modo Direct Change .	13 de janeiro de 2022

Alteração	Descrição	Link
Conteúdo alterado: Uniformidade nos nomes AWS de serviços	Referências do AMS Serviços da AWS que correspondam exatamente aos AWS títulos ou metadados oficiais. Anteriormente, havia pequenas variações que complicavam a correspondência de padrões. Por exemplo, consulte Use o AMS SSP para provisionar o Alexa for Business em sua conta AMS .	13 de janeiro de 2022
Conteúdo alterado: Provisionamento por autoatendimento do Elastic Container Registry (ECR)	Foi adicionado um item de perguntas frequentes sobre o uso do ECR para gerenciar as permissões do usuário. Consulte Use o AMS SSP para provisionar o Amazon Elastic Container Registry em sua conta AMS .	13 de janeiro 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.