Conceitos e procedimentos do AMS Accelerate

Guia do usuário do AMS Accelerate

Versão October 3, 2025

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

Guia do usuário do AMS Accelerate: Conceitos e procedimentos do AMS Accelerate

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 pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, conectados ou patrocinados pela Amazon.

Table of Contents

O que é o AMS Accelerate? 1
Planos de operações 1
Acelere o plano de operações 2
Plano de operações avançado 2
Como funciona 3
Principais termos 3
Service description (Descrição do serviço) 10
Recursos do plano operacional do AWS Managed Services (AMS) AMS Accelerate 10
Configurações compatíveis 14
Serviços com suporte 16
Perfis e responsabilidades 19
Escopo das mudanças realizadas pelo AMS Accelerate 34
Sistemas operacionais não suportados 35
Contato e escalonamento 36
Horário de contato 37
Horário comercial 37
Caminho de escalonamento 38
Inventário de recursos 38
Conceitos básicos 40
Integração 40
Pré-requisitos de integração 40
Etapa 1. Descoberta de contas 43
Etapa 2. Recursos de gerenciamento de integração 45
Etapa 3. Recursos de integração com políticas padrão 55
Etapa 4: Personalize recursos 65
Usando os consoles AMS 67
Padrões AMS 69
Como funcionam os padrões do AMS 69
Padrões AMS 70
Configuração automatizada de instâncias 74
Como funciona 74
Instalação automática do SSM Agent 76
Alterações automatizadas na configuração da instância 78
Fora do AMS Accelerate 82

Efeitos de desembarque ... 82
Desligamento com dependências ... 85
Obter assistência para desembarque ... 85
Configurações da notificação ... 86
Tags ... 87
Tags ... 88
O que são tags? ... 89
Como funcionam as tags ... 89
Etiquetas gerenciadas pelo cliente ... 89
Acelere as tags gerenciadas ... 93
Etiquetas fornecidas pelo cliente ... 94
Ferramentas de gerenciamento de tags ... 95
Marcador de recursos ... 95
CloudFormation ... 115
Terraform ... 119
Relatórios de incidentes, solicitações de serviço e perguntas sobre faturamento ... 121
Gerenciamento de incidentes ... 121
O que é gerenciamento de incidentes? ... 122
Como funcionam a resposta e a resolução de incidentes ... 123
Trabalhando com incidentes ... 124
Gerenciamento de solicitações de serviço ... 127
Quando usar uma solicitação de serviço ... 128
Como funciona o gerenciamento de solicitações de serviço ... 129
Criando uma solicitação de serviço ... 130
Monitorando e atualizando uma solicitação de serviço ... 131
Gerenciando solicitações de serviço com a API de suporte ... 132
Respondendo a uma solicitação de serviço gerada pelo AMS Accelerate ... 133
Relatório de incidentes e teste de solicitação de serviço ... 133
Perguntas sobre faturamento ... 134
Gestão planejada de eventos ... 135
Critérios AMS PEM ... 135
Tipos de PEM ... 135
O processo AMS PEM ... 136
PEM FAQs ... 136
Operações sob demanda ... 138
Solicitando operações de AMS sob demanda ... 148

Fazendo alterações nas ofertas do Operations on Demand ... 149
Relatórios e opções ... 150
Relatórios sob solicitação ... 150
Relatórios de gerenciamento de hosts do AMS ... 151
Relatórios de backup do AMS ... 151
AWS Config Relatório de conformidade de controle ... 154
Relatório de configuração de respostas do AMS Config Rules ... 155
Incidentes evitados e monitoramento dos relatórios do Top Talkers ... 158
Relatório de detalhes de cobranças ... 160
Relatórios do Trusted Remediator ... 161
Relatórios de autoatendimento ... 164
Operações internas de API ... 165
Relatório de patch (diário) ... 169
Relatório de backup (diário) ... 179
Relatório de incidentes (semanal) ... 183
Relatório de cobrança (mensal) ... 187
Relatórios agregados ... 190
Painéis de relatórios de autoatendimento do AMS ... 192
Política de retenção de dados ... 200
Fora do SSR ... 200
Gerenciamento de acesso ... 202
Acessar o console ... 202
Permissões para usar recursos ... 202
Por que e quando acessamos sua conta ... 217
Acionadores de acesso ... 217
Acesse as funções do IAM ... 218
Como acessamos sua conta ... 221
Como e quando usar o root ... 221
Gerenciamento de segurança ... 222
Usando o documento Log4j SSM para descobrir ocorrências ... 223
Monitoramento da segurança da infraestrutura ... 224
Uso de funções vinculadas a serviço ... 226
AWS políticas gerenciadas ... 240
Proteção de dados ... 249
Monitore com o Amazon Macie ... 249
Monitor com GuardDuty ... 250

Monitore com o Amazon Route 53 Resolver DNS Firewall ... 251
Criptografia de dados ... 253
AWS Identity and Access Management ... 253
Autenticação com identidades no AMS Accelerate ... 254
Gerenciar o acesso usando políticas ... 261
Resposta a incidentes de segurança ... 262
Como funciona ... 263
Preparar ... 263
Detectar ... 264
Analisar ... 265
Contenção ... 266
Erradicação ... 268
Recuperar ... 269
Relatório pós-incidente ... 269
Runbooks de resposta a incidentes de segurança ... 270
Registro e monitoramento de eventos de segurança no ... 276
Conformidade de configuração ... 276
Biblioteca de regras de configuração do AMS ... 277
Respostas às violações ... 303
Criação de exceções de regras ... 305
Reduzir AWS Config custos ... 306
Descobertas e respostas personalizadas ... 306
Resposta a incidentes ... 308
Resposta a incidentes e integração ... 309
Resiliência ... 309
Controle de segurança para sistemas end-of-support operacionais ... 310
Práticas recomendadas de segurança ... 310
Revisões de segurança da solicitação de alteração ... 310
Processo de gerenciamento de riscos de segurança do cliente ... 311
Padrões técnicos do AMS Accelerate ... 312
Controles padrão no AMS Accelerate ... 312
Alterações que introduzem riscos de segurança altos ou muito altos em seu ambiente ... 328
Perguntas frequentes sobre segurança ... 330
Quando os engenheiros de operações do AMS acessam meus ambientes? ... 330
Quais funções os engenheiros de operações do AMS assumem quando acessam minhas contas? ... 330

Como um engenheiro de operações do AMS acessa minha conta? 330
Como faço para rastrear as alterações feitas pelo AMS em minhas AWS contas gerenciadas pelo AMS? 331
Quais são os controles de processo para o acesso do engenheiro de operações do AMS à minha conta? 332
Como o acesso privilegiado é gerenciado? 332
Os engenheiros de operações da AMS usam o MFA? 332
O que acontece com o acesso deles quando um funcionário da AMS deixa a organização ou muda de cargo? 332
Quais controles de acesso regem o acesso do engenheiro operacional do AMS às minhas contas? 333
Como o AMS monitora o acesso do usuário root? 333
Como o AMS responde aos incidentes de segurança? 334
A quais certificações e estruturas padrão do setor a AMS adere? 334
Como posso ter acesso aos relatórios mais recentes sobre certificação de segurança, estruturas e conformidade em AWS? 335
O AMS compartilha diagramas de arquitetura de referência de diferentes aspectos dos recursos do AMS? 335
Como o AMS rastreia quem acessa minhas contas e qual é a necessidade de acesso da empresa? 335
Os engenheiros do AMS têm acesso aos meus dados armazenados em serviços de armazenamento de AWS dados, como Amazon S3, Amazon RDS, DynamoDB e Amazon Redshift? 336
Os engenheiros do AMS têm acesso aos dados do cliente armazenados no Amazon EBS, no Amazon EFS e na Amazon FSx? 336
Como o acesso é restrito ou controlado para funções de automação que têm altos privilégios em meus ambientes? 337
Como o AMS implementa o princípio do menor privilégio, conforme defendido no AWS Well-Architected Framework, para funções de automação? 337
Quais sistemas de registro e monitoramento são usados para detectar tentativas de acesso não autorizado ou atividades suspeitas envolvendo funções de automação? 337
Como os incidentes ou violações de segurança relacionados à infraestrutura de automação são tratados e quais protocolos ajudam na resposta e mitigação rápidas? 338
Avaliações regulares de segurança, verificações de vulnerabilidade e testes de penetração são conduzidos na infraestrutura de automação? 338
Como o acesso à infraestrutura de automação é restrito somente ao pessoal autorizado? .. 338

Quais medidas são implementadas para manter os padrões de segurança e evitar acesso não autorizado ou violações de dados no pipeline de automação? ... 338
A detecção ou o monitoramento de anomalias estão ativados para o acesso ou o registro de auditoria para detectar o aumento de privilégios ou o uso indevido do acesso para alertar proativamente a equipe do AMS? ... 339
Quais tipos de dados de clientes são extraídos das contas gerenciadas pelo AMS e como eles são utilizados e armazenados? ... 340
Monitoramento e gerenciamento de eventos ... 341
O que é monitoramento? ... 342
Como funciona o monitoramento ... 342
EC2 notificações agrupadas por instâncias ... 344
Notificação de alerta baseada em tag ... 345
Alertas do monitoramento de linha de base no AMS ... 346
Notificações de incidentes com reconhecimento de aplicativos no AMS ... 370
Integre AppRegistry e crie aplicativos ... 370
Crie tags para permitir o enriquecimento de casos ... 372
Personalize a gravidade do caso de suporte do AMS para seus aplicativos ... 372
Revise as permissões necessárias ... 373
Gerenciador de alarmes ... 374
Como funciona o Gerenciador de alarmes ... 374
Começando com o Gerenciador de alarmes ... 375
Tags do Gerenciador de alarmes ... 376
Perfis de configuração do Alarm Manager ... 381
Criação de CloudWatch alarmes adicionais ... 399
Visualizando o número de recursos monitorados pelo Alarm Manager ... 400
Remediação automática de alertas pelo AMS ... 401
EC2 falha na verificação de status: notas de automação de remediação ... 407
EC2 automação de remediação de uso de volume ... 407
Automação de remediação de eventos de baixo armazenamento do Amazon RDS ... 408
Roteador de eventos AMS ... 409
Amazon EventBridge Managed Rules implantadas pelo AMS ... 409
Criação de regras gerenciadas para AMS ... 412
Editando regras gerenciadas para AMS ... 412
Excluindo regras gerenciadas para AMS ... 412
Remediador confiável ... 412
Benefícios principais ... 412

Como funciona o Trusted Remediator 413
Principais termos 414
Comece a usar o Trusted Remediator 415
Recomendações compatíveis do Compute Optimizer 418
Trusted Advisor Verificações suportadas 421
Configurar a remediação de cheques 482
Fluxo de trabalho de decisão do modo execução 486
Configurar tutoriais de remediação 486
Trabalhe com remediações 490
Registros de remediação 494
Integração com QuickSight 498
Práticas recomendadas 501
FAQs 501
Monitoramento e gerenciamento de incidentes para EKS 505
O que é monitoramento e gerenciamento de incidentes para o Amazon EKS? 505
Como o monitoramento e o gerenciamento de incidentes do Amazon EKS funcionam 506
Matriz de responsabilidade da AMS (RACI) 507
Alertas de linha de base 509
Alertas e ações 510
Requisitos 518
Integração 520
Fora de bordo 521
Gerenciamento de continuidade 523
Como funciona o gerenciamento de continuidade 523
Selecione um plano de backup do AMS 524
Plano de backup padrão do AMS 525
Plano de backup aprimorado 525
Plano de backup sensível a dados 526
Plano de backup de integração do AMS Accelerate 526
Marque seus recursos para backup 527
Exibir backups em cofres do AMS 529
Monitoramento e emissão de relatórios para backups 530
Gerenciamento de patches 531
Recomendações de patches 532
Recomendações de responsabilidade do patch 533
Orientação para equipes de aplicação 534

Orientação para equipes de operações de segurança ... 534
Orientação para equipes de governança e conformidade ... 534
Exemplo de design para aplicativo Windows de alta disponibilidade ... 535
Recomendações de patch FAQs ... 536
Criar janela de patch ... 536
Limites da janela de manutenção de patches ... 537
Criar janela de patch do Patch Tuesday: console AMS ... 538
Crie uma janela de patch: CloudFormation ... 539
Criar janela de patch: console do Systems Manager ... 540
Criar janela de patch: Systems Manager CLI ... 542
Patch com ganchos ... 543
Patch hooks AMS RACI ... 544
Crie documentos SSM para patch hooks ... 545
Configure a janela de manutenção de patches do AMS para usar seus documentos do Comando SSM como ganchos de patch do AMS ... 546
Linha de base do patch AMS Accelerate ... 547
Linha de base do patch padrão ... 547
Linha de base do patch personalizado ... 548
Permissões de aplicação de patches sob demanda ... 549
Entenda as notificações de patches e as falhas de patches ... 550
Solicitações de serviço de patches e notificações por e-mail ... 550
Notificações de patches por meio de CloudWatch eventos ... 551
Investigação de falha de patch ... 556
Otimização de custos com o AMS Resource Scheduler ... 557
Usando recursos com o Resource Scheduler ... 558
Programador de recursos de integração ... 560
Personalizando o Agendador de Recursos ... 560
Usando o Agendador de Recursos ... 561
Trabalhando com períodos e horários ... 564
Marcação de recursos ... 570
Estimador de custos ... 571
Supressor de alarme ... 572
Gerenciamento de logs ... 573
Gerenciamento de registros — AWS CloudTrail ... 573
Acessando e auditando registros CloudTrail ... 575
Protegendo e retendo registros CloudTrail ... 575

Acessando os EC2 registros da Amazon 575
Retenção de registros da Amazon EC2 576
Gerenciamento de registros — Amazon EC2 576
Gerenciamento de registros — Amazon VPC Flow Logs 577
Rastreando alterações 579
Visualizando seus registros de alterações 580
Consultas padrão 581
Modificando o filtro de data e hora nas consultas 590
Exemplos de consulta padrão 592
Alterar permissões de registro 603
AWS Systems Manager em Accelerate 605
Documentos SSM do AMS Accelerate disponíveis 605
Versões de documentos SSM do AMS Accelerate 605
Preços do Systems Manager 606
Histórico do documento 607
Atualizações anteriores 628
..... dclvi

O que é o AMS Accelerate?

Bem-vindo ao AMS Accelerate for Amazon Web Services (AWS). O AMS Accelerate fornece uma variedade de serviços operacionais para ajudá-lo a alcançar a excelência operacional em AWS. Se você está apenas começando na nuvem, quer aumentar sua equipe atual ou precisa de uma solução operacional de longo prazo, o Accelerate pode ajudá-lo a atingir suas metas operacionais na nuvem. Aproveitando Serviços da AWS uma biblioteca de automações, configurações e runbooks, fornecemos uma solução end-to-end operacional para ambientes novos e existentes. AWS

O serviço Accelerate utiliza um conjunto de recursos Serviços da AWS e recursos nativos para fornecer um conjunto abrangente de recursos de gerenciamento de infraestrutura. Dentro deles Serviços da AWS, o Accelerate cria e mantém conjuntos selecionados de controles de monitoramento, proteções de detecção, automações e runbooks para operar a infraestrutura de forma compatível e segura.

Tópicos

- Planos de operações do AMS
- Usando o plano de operações do AMS Accelerate
- Termos-chave do AMS
- Service description (Descrição do serviço)
- Capacidades para sistemas operacionais sem suporte no Accelerate
- Contato e escalonamento
- Inventário de recursos para Accelerate

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.

Usando o plano de operações do AMS Accelerate

O AMS Accelerate é o plano de operações do AMS que pode operar a infraestrutura da AWS que suporta cargas de trabalho. Se suas cargas de trabalho já estão em uma conta da AWS ou você planeja migrar novas, 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 pode continuar usando seus mecanismos de acesso e mudança existentes, 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.

Embora o AMS Accelerate possa simplificar suas operações, você continua responsável pelo desenvolvimento, implantação, teste, ajuste e gerenciamento de aplicativos. O AMS Accelerate só faz alterações em sua conta como resultado de incidentes, alarmes, remediações e algumas solicitações de serviço. O AMS Accelerate não provisiona recursos na conta em seu nome. O AMS Accelerate fornece assistência para solução de problemas de infraestrutura que afetam os aplicativos, mas o AMS Accelerate não acessa nem valida suas configurações de aplicativos sem seu conhecimento e aprovação. Os serviços e alterações do AMS Accelerate são fornecidos diretamente no AWS console e APIs, portanto, você continua aproveitando suas contas existentes com AWS as soluções do AWS Marketplace disponíveis. O AMS Accelerate não modifica o código em seus infrastructure-as-code modelos (por exemplo, CloudFormation modelos), mas pode orientar suas equipes sobre quais mudanças são necessárias para seguir as melhores práticas operacionais e de segurança.

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 Accelerate é um plano operacional do serviço AWS Managed Services para gerenciar as operações da sua AWS infraestrutura.

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

O AMS Accelerate oferece os seguintes recursos:

- Gerenciamento de incidentes:

  O gerenciamento de incidentes é o processo que o serviço AMS usa para responder aos incidentes relatados.

  O AMS Accelerate detecta e responde proativamente a incidentes e auxilia sua equipe na resolução de problemas. Você pode entrar em contato com os engenheiros de operações do AMS Accelerate 24 horas por dia, 7 dias por semana, usando o AWS Support Center, com tempo de resposta SLAs dependendo do nível de resposta selecionado para sua conta.
- Monitoramento

  O monitoramento é o processo que o serviço AMS usa para rastrear seus recursos.

  As contas inscritas no AMS Accelerate são configuradas com uma implantação básica de CloudWatch eventos e alarmes da Amazon que foram otimizados para reduzir o ruído e identificar um possível incidente futuro. Depois de receber os alertas, a equipe do AMS usa remediações, pessoas e processos automatizados para trazer os recursos de volta a um estado saudável e interagir com suas equipes quando apropriado para fornecer informações sobre o comportamento e como evitá-lo. Se a remediação falhar, o AMS inicia o processo de gerenciamento de incidentes. Você pode alterar as linhas de base atualizando o arquivo de configuração padrão.
- Segurança:

O gerenciamento de segurança é o processo que o serviço AMS usa para proteger seus recursos. O AWS Managed Services protege seus ativos de informação e ajuda a manter sua infraestrutura da AWS segura usando vários controles, incluindo AWS Config Rules e Amazon GuardDuty.

O AMS Accelerate mantém uma biblioteca de Regras do AWS Config ações de remediação para garantir que todas as suas contas estejam em conformidade com os padrões do setor de segurança e integridade operacional. Regras do AWS Config rastreia continuamente a alteração de configuração entre seus recursos registrados. Se uma alteração violar qualquer condição de regra, o AMS relata suas descobertas e permite que você corrija as violações automaticamente ou mediante solicitação, de acordo com a gravidade da violação. Regras do AWS Config facilitar a conformidade com os padrões estabelecidos por: o Center for Internet Security (CIS), o Cloud Security Framework (CSF) do National Institute of Standards and Technology (NIST), a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) e o Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI).

Além disso, o AMS Accelerate utiliza GuardDuty a Amazon para identificar atividades potencialmente não autorizadas ou maliciosas em seu ambiente da AWS. GuardDuty as descobertas são monitoradas 24 horas por dia, 7 dias por semana, pelo AMS. A AMS colabora com você para entender o impacto das descobertas e remediações com base nas recomendações de melhores práticas. O AMS também oferece suporte ao Amazon Macie para proteger seus dados confidenciais, como informações pessoais de saúde (PHI), informações de identificação pessoal (PII) e dados financeiros. Por fim, o AMS monitora e faz a triagem de todos os eventos ALERT e BLOCK do Amazon Route 53 Resolver gerados em contas gerenciadas para inspecionar ainda mais o tráfego da rede e aumentar suas capacidades de detetive.

- Gerenciamento de patches:

  O gerenciamento de patches é o processo que o serviço AMS usa para atualizar seus recursos.

  Para uma AWS conta com o complemento de patch, o AWS Managed Services aplica e instala atualizações do fornecedor nas EC2 instâncias da Amazon para sistemas operacionais compatíveis durante as janelas de manutenção escolhidas. O AMS cria um instantâneo da instância antes da aplicação do patch, monitora a instalação do patch e notifica você sobre o resultado. Se o patch falhar, o AMS investiga a falha e recomenda um curso de ação para que você corrija o problema. Ou o AMS restaura a instância para reversão, se solicitado. O AMS fornece relatórios sobre a cobertura de conformidade de patches e aconselha você sobre o curso de ação recomendado para sua empresa.

- Gerenciamento de backup:

O AMS usa o gerenciamento de backup para tirar fotos de seus recursos.

O AWS Managed Services cria, monitora e armazena snapshots de AWS serviços suportados pelo AWS Backup. Você define os cronogramas de backup, a frequência e o período de retenção criando AWS Backup planos ao integrar contas e aplicativos. Você associa os planos aos recursos. O AMS monitora todas as tarefas de backup e, quando uma tarefa de backup falha, alerta nossa equipe para executar uma correção. O AMS aproveita seus instantâneos para realizar ações de restauração durante incidentes, se necessário. O AMS fornece um relatório de cobertura de backup e um relatório de status de backup.

- 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.

- Especialistas designados:

  O AMS Accelerate também designa um Cloud Service Delivery Manager (CSDM) e um Cloud Architect (CA) para fazer parceria com sua organização e promover a excelência operacional e de segurança. Seu CSDM e CA fornecem orientação durante e após a configuração e a integração do AMS Accelerate, entregam um relatório mensal de suas métricas operacionais e trabalham com você para identificar possíveis economias de custo usando ferramentas como AWS Cost Explorer, relatórios de custos e uso e. Trusted Advisor

- Ferramentas de operações:

  O AMS Accelerate pode fornecer operações contínuas para a infraestrutura da sua carga de trabalho na AWS. Nossos serviços de patch, backup, monitoramento e gerenciamento de incidentes dependem de ter recursos marcados e do AWS Systems Manager (SSM) e dos CloudWatch agentes instalados e configurados em suas EC2 instâncias da Amazon com um perfil de instância do IAM que os autorize a interagir com os serviços do SSM e da Amazon. CloudWatch O AMS Accelerate fornece ferramentas como o Resource Tagger para ajudá-lo a marcar seus recursos com base em regras e a configuração automática de instâncias para instalar os agentes necessários em suas EC2 instâncias da Amazon. Se você estiver seguindo práticas de infraestrutura imutáveis, poderá preencher os pré-requisitos diretamente no console ou nos modelos. infrastructure-as-code

- Otimização de custos:

  O AMS Resource Scheduler automatiza o início e a interrupção de instâncias do Amazon Elastic Compute Cloud (Amazon EC2), instâncias do Amazon Relational Database Service (Amazon RDS) e grupos do Amazon Auto Scaling. EC2 O AMS Resource Scheduler ajuda você a reduzir os custos operacionais interrompendo os recursos que não estão em uso e reiniciando-os quando sua capacidade é necessária.

- Registro e geração de relatórios:

  O AWS Managed Services agrega e armazena registros gerados como resultado de operações em CloudWatch CloudTrail, e Amazon VPC Flow Logs. O registro do AMS ajuda na resolução mais rápida de incidentes e nas auditorias do sistema. O AMS Accelerate também 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) da AMS designado para você.

- Gerenciamento de solicitações de serviço:

  Para solicitar informações sobre seu ambiente gerenciado, AMS ou ofertas de AWS serviços, envie solicitações de serviço usando o console do AMS Accelerate. 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.

Todos os clientes do AMS Accelerate começam com gerenciamento de incidentes, monitoramento, monitoramento de segurança, gravação de registros, ferramentas de pré-requisitos, gerenciamento de backup e recursos de geração de relatórios. Você pode adicionar o complemento de gerenciamento de patches do AMS por um preço adicional.

> **Note**
>
> Para obter uma lista de recursos não suportados no AWS GovCloud (US), consulte Como o AMS Accelerate difere em AWS GovCloud (US)

Configurações compatíveis

O AMS Accelerate suporta as seguintes configurações:

- Idioma: inglês.
- Regiões: veja as AWS regiões suportadas pelo AWS Managed Services na página de Serviços AWS Regionais.

> **Note**
>
> As regiões da AWS introduzidas antes de 20 de março de 2019 são consideradas regiões "originais" e estão habilitadas por padrão. As regiões introduzidas após essa data são regiões "opcionais" e estão desativadas por padrão. Se sua conta usa várias regiões e você incorpora o AMS Accelerate em uma conta com uma região "Opt-in" ativada como região padrão, o recurso de relatórios do AMS só está disponível nessa região. Se você não definir uma região padrão, a última região visitada será sua região padrão.
> Para habilitar uma região, consulte Habilitando uma região. Para definir uma região padrão, consulte Escolha de uma região. Para obter uma lista do status de Opt-in para cada região, consulte Regiões disponíveis no Guia do usuário do Amazon Elastic Compute Cloud.

- Arquitetura do sistema operacional (x86-64 ou ARM64): qualquer uma suportada pelo Systems Manager e. CloudWatch
- Sistemas operacionais com suporte:
  - AlmaLinux 8.3-8.9, 9.x (só AlmaLinux é compatível com a arquitetura x86)
  - 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 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 do Usuário do Accelerate, ou
> 3. você cumpre com 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
- Se você usa AWS Control Tower para gerenciar seu ambiente de várias contas, verifique se está executando a versão mais recente do AWS Control Tower para compatibilidade com o Accelerate. Ambientes que usam AWS Control Tower versões anteriores à 2.7 (lançada em abril de 2021) não são compatíveis. Para obter informações sobre como atualizar AWS Control Tower, consulte Atualizar sua zona de pouso.

Serviços com suporte

O AWS Managed Services fornece serviços de suporte de gerenciamento operacional para os seguintes AWS serviços. Cada AWS serviço é distinto e, como resultado, o nível de suporte de gerenciamento operacional do AMS varia de acordo com a natureza e as características do AWS serviço subjacente. Se você solicitar que o AWS Managed Services forneça serviços para qualquer software ou serviço que não esteja expressamente identificado como suportado na lista a seguir, qualquer AWS Managed Services fornecido para essas configurações solicitadas pelo cliente será tratado como um “Serviço Beta” de acordo com os Termos do Serviço.

- Incidentes: Todos os serviços AWS
- Solicitação de serviço: Todos os AWS serviços
- Aplicação de patches: Amazon EC2
- Backups e restauração: todos Serviços da AWS suportados pelo AWS Backup. Para obter uma lista dos serviços suportados pelo AWS Backup, consulte os recursos AWS Backup suportados.
- Agendador de recursos: instâncias do Amazon Elastic Compute Cloud EC2 (Amazon), grupos do Amazon Relational Database Service (Amazon RDS) e do Amazon Auto Scaling EC2
- Serviços monitorados para eventos operacionais: verificações suportadas e Trusted Advisor, Application Load Balancer, Aurora, EC2 Amazon, Elastic Load Balancing, Amazon FSx for NetApp ONTAP, FSx Amazon for Windows File Server, gateway NAT (um serviço de tradução de endereços de rede (NAT)),,, Amazon Health Dashboard Redshift OpenSearch, Amazon Relational Database Service (Amazon RDS), VPN. Site-to-Site Para saber mais sobre o que o AMS Accelerate está monitorando como parte de um serviço, consulte Alertas do monitoramento básico no AMS.
- Serviços monitorados por regras de configuração de segurança: AWS Account,, Macie GuardDuty, Amazon API Gateway,,,,, AWS Certificate Manager,, AWS Config, Amazon CloudTrail, Amazon CloudWatch AWS CodeBuild, Amazon, AWS Database Migration Service Amazon Elastic Block Store (Amazon EBS) ElastiCache, EC2 Amazon Elastic File System (Amazon EFS), Amazon Elastic Kubernetes Service (Amazon Elastic Kubernetes Service (Amazon EKS), Elastic Load Balancing, Amazon Service, Amazon EMR, (IAM),,, Amazon AWS Key Management Service Redshift, Amazon Relational Database OpenSearch Service, AWS Identity and Access Management Amazon S3, Amazon AI AWS Lambda,, SageMaker AWS Secrets Manager Amazon Simple Notification Service AWS Systems Manager, Amazon VPC (grupo de segurança, volume, endereço IP elástico, conexão VPN, gateways de Internet), Amazon VPC Flow Logs. Para obter mais detalhes, consulte Conformidade de configuração no Accelerate e Proteção de dados no Accelerate. Você pode encontrar informações adicionais de segurança do AMS em nosso Guia

de segurança privado AWS Artifact, que pode ser acessado por meio da guia Relatórios do AWS Managed Services.

> **Note**
>
> O AMS Accelerate para a região do Oriente Médio (EAU) oferece suporte a um conjunto de recursos dentro do escopo, conforme descrito na tabela a seguir. O acesso ao console e às instâncias da conta do AMS nesta região é orientado exclusivamente por acionadores de solicitação de serviço de entrada. Para obter mais informações sobre a disponibilidade do Accelerate na região do Oriente Médio (EAU), consulte seu gerente de contas ou o AWS Cloud Service Delivery Manager (CSDM).

Recursos dentro do escopo do AMS Accelerate para a região do Oriente Médio (EAU)	Descrição do recurso
Gerenciamento de incidentes	O AMS fornece assistência e resposta a incidentes para ajudar sua equipe a resolver problemas. Para que o AMS o ajude no gerenciamento de incidentes, você precisa enviar uma solicitação de serviço. O AMS não detecta nem responde proativamente a incidentes nessa região.
Monitoramento	Depois de receber sua solicitação de serviço, o AMS pode ajudar na remediação de recursos. O AMS usa remediação, pessoas e processos automatizados para trazer seus recursos de volta a um estado saudável. O AMS não configura CloudWatch eventos e alarmes de linha de base nessa região. Se você tiver ferramentas de monitoramento existentes, o rastreamento proativo de seus recursos pode estar disponível com base na avaliação do Cloud Architect (CA) e do CSDM.

Recursos dentro do escopo do AMS Accelerate para a região do Oriente Médio (EAU)	Descrição do recurso
Segurança	Depois de receber sua solicitação de serviço, o AMS pode ajudar na correção de problemas de segurança. O AMS não implanta controles de segurança como Regras do AWS Config GuardDuty e/ou monitora descobertas de segurança nesta região. Se você tiver ferramentas de segurança existentes, o monitoramento proativo da segurança pode estar disponível com base na avaliação da CA e do CSDM.
Gerenciamento de patches	O AMS pode aplicar atualizações do fornecedo r às EC2 instâncias da Amazon para sistemas operacionais compatíveis durante as janelas de manutenção escolhidas e criar instantân eos de pré-aplicação de patches. Para que o AMS o ajude no gerenciamento de patches, você precisa enviar uma solicitação de serviço. Notificações e relatórios de patches do AMS não estão disponíveis nesta região.
Gerenciamento de backup	O AMS pode criar e armazenar instantâneos para fins de Serviços da AWS AWS Backup suporte e auxiliar na remediação de backup. Para que o AMS o ajude no gerenciamento de backup, você precisa enviar uma solicitação de serviço. O AMS não rastreia trabalhos de backup nessa região.
Especialistas designados	A AMS designa um Cloud Architect (CA) e um Cloud Service Delivery Manager (CSDM) para fazer parcerias com organizações de clientes e promover a excelência operacional e de segurança.

Recursos dentro do escopo do AMS Accelerate para a região do Oriente Médio (EAU)	Descrição do recurso
Gerenciamento de solicitações de serviço	Para solicitar informações sobre seu ambiente gerenciado, AMS ou AWS service (Serviço da AWS) ofertas, envie solicitações de serviço por meio do console do AMS Accelerate. Você pode enviar uma solicitação de serviço para perguntas “Como fazer” Serviços da AWS e recursos, ou para solicitar serviços de AMS que estejam disponíveis nesta região, conforme descrito nesta tabela.

Perfis e responsabilidades

A matriz responsável, responsável, consultada e informada do AMS Accelerate, ou RACI, atribui a responsabilidade primária ao cliente ou à AMS por uma variedade de atividades. A tabela descreve suas responsabilidades (o “Cliente”) versus nossas responsabilidades (“AMS Accelerate”).

A Escopo das mudanças realizadas pelo AMS Accelerate seção lista as circunstâncias específicas em que o AMS está autorizado a fazer alterações em sua conta e alguns tipos de alterações que o AMS nunca faz.

Matriz AMS Accelerate RACI

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

- 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.

> **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.

Atividades	Cliente	AWS Managed Services (AMS)
Padrões AMS		
Crie novos padrões	eu	R
Implemente e personalize padrões	R	C, I
Teste e remova padrões	R	eu
Ciclo de vida do aplicação		
Desenvolvimento de aplicações	R	eu
Requisitos, análise e design da infraestrutura de aplicativos	R	eu
Implantação de aplicações	R	eu
Implantação de recursos da AWS	R	eu
Monitoramento de aplicações	R	eu
Teste/otimização de aplicativos	R	eu
Solucione e resolva problemas de aplicativos	R	eu
Solucione e resolva problemas	R	eu
Monitoramento suportado pela infraestrutura da AWS	C	R

Atividades	Cliente	AWS Managed Services (AMS)
Resposta a incidentes para problemas de rede da AWS	C	R
Resposta a incidentes para problemas de recursos da AWS	C	R
Integração de conta gerenciada		
Conceda acesso à conta gerenciada da AWS para a equipe e as ferramentas do AMS	R	C
Implemente alterações na conta ou no ambiente para permitir a implantação de ferramentas na conta. Por exemplo, mudanças nas políticas de controle de serviços (SCPs)	R	C
Instale agentes SSM em instâncias EC2	R	C
Instale e configure as ferramentas necessárias para fornecer serviços de AMS. Por exemplo, CloudWatch agentes, scripts para aplicação de patches, alarmes, registros e outros	eu	R
Gerencie o ciclo de vida de acesso e identidade para engenheiros do AMS	eu	R
Colete todas as entradas necessárias para configurar os serviços do AMS. Por exemplo, duração, cronograma e metas das janelas de manutenção de patches	R	eu
Solicite a configuração dos serviços AMS e forneça todas as entradas necessárias	R	eu
Configure os serviços do AMS conforme solicitado pelo cliente. Por exemplo, janelas de manutenção de patches, etiquetador de recursos e gerenciador de alarmes	C	R

Atividades	Cliente	AWS Managed Services (AMS)
Gerencie o ciclo de vida dos usuários e suas permissões, para serviços de diretórios locais, usados para acessar contas e instâncias da AWS	R	eu
Recomende a otimização de instâncias reservadas	eu	R
Conta (s) integrada (s) ao Trusted Remediator	C, I	R
Gerenciamento de patches		
Colete todas as entradas necessárias para configurar janelas de manutenção de patches, linhas de base de patches e metas	R	eu
Solicite a configuração das janelas e linhas de base de manutenção de patches e forneça todas as entradas necessárias	R	eu
Configure janelas de manutenção de patches, linhas de base e metas de patches conforme solicitado pelo cliente	C	R
Monitore as atualizações aplicáveis do sistema operacional compatíve l e do software pré-instalado com sistema operacional compatível para instâncias EC2	eu	R
Relatório de atualizações ausentes no sistema operacional compatível e na cobertura da janela de manutenção	eu	R
Faça capturas instantâneas das instâncias antes de aplicar as atualizaç ões	eu	R
Aplique atualizações às EC2 instâncias por configuração do cliente	eu	R
Investigue falhas nas atualizações das EC2 instâncias	C	R
Atualização AMIs e pilhas para grupos de escalonamento automático () ASGs	R	C

Atividades	Cliente	AWS Managed Services (AMS)
Corrija o sistema operacional Windows e os pacotes da Microsoft instalados no sistema operacional que são regidos pelo Windows Update	eu	R
Corrija aplicativos, software ou dependências de aplicativos instalados não gerenciados pelo Windows Update	R	eu
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
Corrija aplicativos, software ou dependências de aplicativos instalados não gerenciados pelo gerenciador de pacotes nativo do sistema operacional Linux	R	eu
Backup		
Colete todas as entradas necessárias para configurar planos de backup e recursos de destino	R	eu
Solicite a configuração dos planos de Backup e forneça todas as entradas necessárias	R	eu
Configure planos e metas de backup conforme solicitado pelo cliente	C	R
Especifique os cronogramas de backup e os recursos de destino	R	eu
Execute backups por plano	eu	R
Investigue trabalhos de backup que falharam	eu	R
Relatório sobre o status das tarefas de backup e a cobertura de backup	eu	R
Validar backups	R	eu

Atividades	Cliente	AWS Managed Services (AMS)
Solicite restauração de backup para recursos de recursos de serviços da AWS compatíveis como parte do gerenciamento de incidentes	R	eu
Execute atividades de restauração de backup para recursos de serviços compatíveis da AWS	eu	R
Restaure aplicativos personalizados ou de terceiros afetados	R	eu
Redes		
Provisionamento e configuração da conta gerenciada VPCs IGWs, do Direct Connect e de outros serviços de rede da AWS	R	eu
Configure e opere a segurança da AWS Groups/NAT/NACL dentro da conta gerenciada	R	eu
Configuração e implementação de rede na rede do cliente (por exemplo DirectConnect)	R	eu
Configuração e implementação de rede na rede AWS	R	eu
Monitor definido pelo AMS para segurança de rede, incluindo grupos de segurança	eu	R
Configuração e gerenciamento de registros em nível de rede (registros de fluxo de VPC e outros)	eu	R
Registro em log		
Registre todos os registros de alterações do aplicativo	R	eu
Registre registros de alterações na infraestrutura da AWS	eu	R
Habilite e agregue a trilha de auditoria da AWS	eu	R

Atividades	Cliente	AWS Managed Services (AMS)
Registros agregados dos recursos da AWS	eu	R
Monitoramento e remediação		
Colete todas as entradas necessárias para configurar o gerenciador de alarmes, o etiquetador de recursos e os limites de alarme	R	eu
Solicite a configuração do gerenciador de alarmes e forneça todas as entradas necessárias	R	eu
Configure o gerenciador de alarmes, o etiquetador de recursos e os limites de alarme conforme solicitado pelo cliente.	C	R
Implemente métricas e alarmes CloudWatch básicos do AMS por configuração do cliente	eu	R
Monitore os recursos compatíveis da AWS usando CloudWatch métricas e alarmes básicos	eu	R
Investigue alertas dos recursos da AWS	C	R
Corrija alertas com base na configuração definida ou crie um incidente	eu	R
Defina, monitore e investigue monitores específicos do cliente	R	eu
Investigue alertas do monitoramento de aplicativos	R	C
Configurar Trusted Advisor verificações para remediação	R	C
Corrija automaticamente as verificações suportadas Trusted Advisor	eu	R
Corrija manualmente as verificações suportadas Trusted Advisor	R	C
Relatar o status da remediação	eu	R
Solucionar problemas de falhas de remediação	R	C

Atividades	Cliente	AWS Managed Services (AMS)
Arquitetura de segurança		
Analise os recursos e o código do AMS em busca de problemas de segurança e possíveis ameaças	eu	R
Implemente controles de segurança nos recursos e códigos do AMS para mitigar os riscos de segurança	eu	R
Habilite serviços compatíveis da AWS para o gerenciamento de segurança da conta e de seus recursos da AWS	eu	R
Gerencie credenciais privilegiadas para acesso à conta e ao sistema operacional para engenheiros do AMS	eu	R
Gerenciamento de riscos de segurança		
Monitore serviços da AWS compatíveis para gerenciamento de segurança, como GuardDuty Macie	eu	R
Defina e crie regras de configuração definidas pela AMS para detectar se os recursos da AWS estão em conformidade com as melhores práticas de segurança do Center for Internet Security (CIS) e do NIST.	eu	R
Monitore as regras de configuração definidas pelo AMS	eu	R
Relate o status de conformidade do Config Rules	eu	R
Defina uma lista das regras de configuração necessárias e corrija-as	eu	R
Avalie o impacto da correção das regras de configuração definidas pelo AMS	R	eu
Solicite a correção das regras de configuração definidas pela AMS na conta da AWS	R	eu

Atividades	Cliente	AWS Managed Services (AMS)
Rastreie recursos isentos das regras de configuração definidas pela AMS	R	eu
Corrija as regras de configuração definidas pela AMS suportadas na conta da AWS	C	R
Corrija regras de configuração definidas pela AMS não suportadas na conta da AWS	R	eu
Defina, monitore e investigue regras de configuração específicas do cliente	R	eu
Gerenciamento de incidentes		
Notifique sobre incidentes detectados pelo AMS nos recursos da AWS	eu	R
Notificar sobre incidentes em recursos AWS	R	eu
Notifique sobre incidentes de AWS recursos com base no monitoram ento	eu	R
Lidar 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 ou restauração de infraestrutura para recursos com backups disponíveis	C	R
Resposta a incidentes de segurança — Prepare-se		
Comunicações		

Atividades	Cliente	AWS Managed Services (AMS)
Forneça e atualize os 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	C	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	R	R
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 um inventário abrangente de AWS recursos (Amazon EC2, Amazon S3 etc.), incluindo detalhes sobre o valor e a importância de cada ativo para a empresa. Essas informações serão fundamentais para determinar uma estratégia de contenção eficaz.	R	C
Use AWS tags para identificar recursos e cargas de trabalho	R	C
Definir e configurar a retenção e o arquivamento de registros	eu	R
Estabeleça uma linha de base segura definindo e aplicando as políticas e configurações de segurança da organização para AWS contas, serviços e gerenciamento de acesso	R	eu
Resposta a incidentes de segurança - Detecte		

Atividades	Cliente	AWS Managed Services (AMS)
Registro, indicadores e monitoramento		
Configure o registro e o monitoramento para permitir o gerenciamento de eventos, por exemplo e contas	eu	R
Monitor compatível com Serviços da AWS alertas de segurança	eu	R
Implemente e gerencie ferramentas de segurança de terminais	R	eu
Monitore malware em instâncias usando segurança de endpoint	R	eu
Notifique o cliente sobre eventos detectados por meio de mensagens de saída	eu	R
Coordene as comunicações internas com as partes interessadas e as atualizações da liderança para melhorar o tempo de resposta	R	eu
Defina, implante e mantenha os serviços de detecção padrão do AMS (por exemplo, Amazon GuardDuty e AWS Config)	C	R
Registre registros de alterações na AWS infraestrutura	R	eu
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	R	R
Relatórios de eventos de segurança		
Notifique o AMS sobre uma atividade suspeita ou uma investigação de segurança ativa	R	eu
Notifique eventos e incidentes de segurança detectados ao cliente	eu	R

Atividades	Cliente	AWS Managed Services (AMS)
Notificar o evento planejado que pode acionar o processo de resposta a incidentes de segurança	R	eu
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	R
Avalie false/true os pontos positivos usando os dados disponíveis	R	R
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	C
Colete registros de aplicativos para ajudar na investigação	R	eu
Colete dados e registros para auxiliar na investigação de alertas de segurança	R	R
SMEs Participe Serviços da AWS de investigações de segurança	C	R
Compartilhe registros de investigação do suporte Serviços da AWS aos 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 - Contenha		
Estratégia e execução de contenção		
Avalie os riscos e decida a estratégia de contenção, reconhecendo os possíveis impactos do serviço	R	C
Faça um backup dos sistemas afetados para análise posterior	eu	R
Contenha aplicativos e cargas de trabalho (por meio de configuração específica do aplicativo ou atividade de resposta)	R	C
Defina a estratégia de contenção com base no incidente de segurança e no recurso afetado	eu	R
Habilite a criptografia e o armazenamento seguro de backups pontuais dos sistemas afetados	C	R
Execute ações de contenção suportadas para AWS recursos, incluindo EC2 instâncias, rede e IAM	eu	R
Resposta a incidentes de segurança - Erradicar		
Estratégia e execução da erradicação		
Defina as opções de erradicação com base no incidente de segurança e no recurso afetado nas cargas de trabalho dos aplicativos do cliente	C	R
Decida sobre a estratégia de erradicação acordada, o momento da execução da erradicação e as consequências	R	eu

Atividades	Cliente	AWS Managed Services (AMS)
Defina as etapas de erradicação com base no incidente de segurança e no recurso afetado nas cargas de trabalho gerenciadas pelo AMS	C	R
Erradicar ameaças e fortalecer AWS recursos, incluindo EC2 instâncias, rede e erradicação do IAM	R	C
Erradicar ameaças 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	eu	R
Analise os planos de backup para restaurar cargas de trabalho gerenciadas pelo AMS	R	eu
Execute atividades de restauração de backup para obter recursos compatíveis Serviços da AWS	eu	R
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
Restaure 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

Atividades	Cliente	AWS Managed Services (AMS)
Gerenciamento de problemas		
Correlacione incidentes para identificar problemas	eu	R
Execute a análise da causa raiz (RCA) de problemas	eu	R
Corrija problemas	eu	R
Identifique e corrija problemas de aplicativos	R	eu
Gerenciamento de serviços		
Solicitar informações usando solicitações de serviço	R	eu
Responder às solicitações de serviço	eu	R
Forneça recomendações de otimização de custos	eu	R
Prepare e entregue um relatório de serviço mensal	eu	R
Gerenciamento de mudanças		
Processos e ferramentas de gerenciamento de mudanças para provision amento e atualização de recursos no ambiente gerenciado	R	eu
Manutenção do calendário de alterações do aplicativo	R	eu
Aviso da próxima janela de manutenção	R	eu
Registre as alterações feitas pelas operações do AMS	eu	R
Otimização de custos		
Colete todas as entradas necessárias para configurar o Resource Scheduler	R	eu

Atividades	Cliente	AWS Managed Services (AMS)
Solicite a integração e a configuração do Resource Scheduler e forneça todas as entradas necessárias	R	eu
Implemente o Resource Scheduler por configuração do cliente	C, I	R
Desative e ative o Agendador de Recursos na conta do cliente	R	C
Crie, exclua, descreva e atualize agendas	C	R
Crie, exclua, descreva e atualize períodos	C	R
Investigue e solucione problemas com o Resource Scheduler	eu	R
Solicitação de desativação do Agendador de Recursos	R	eu
Remova o Agendador de Recursos da conta	C, I	R

Escopo das mudanças realizadas pelo AMS Accelerate

O AMS Accelerate só faz alterações para as finalidades e situações específicas descritas a seguir. O AMS faz alterações somente no nível da infraestrutura, usando o console ou APIs. O AMS nunca altera suas camadas de aplicativo, controle ou domínio. Você pode ver todas as alterações feitas pelo AMS (ou por outros usuários) usando nosso conjunto de consultas pré-criadas; para fazer isso, consulte. Rastreando alterações em suas contas do AMS Accelerate

AWS recursos

O AMS Accelerate implanta ou atualiza AWS recursos somente nas seguintes situações:

- Para implantar e atualizar ferramentas e recursos exigidos pelo AMS.
- Como parte do monitoramento do AMS, em resposta a eventos e alarmes.
- Para remediar problemas de segurança como parte Respostas às violações no Accelerate (fazendo com que os recursos não compatíveis estejam em conformidade com as melhores práticas de segurança).

- Durante a remediação e restauração como parte de uma resposta a incidentes.
- Ao responder às solicitações do cliente para configurar os recursos do AMS, como os seguintes:
  - Gerenciador de alarmes
  - Marcador de recursos
  - Linhas de base do patch e janelas de manutenção
  - Agendador de recursos
  - Planos de backup

O AMS Accelerate não implanta nem atualiza recursos fora dessas situações. Se precisar da ajuda do AMS para fazer alterações em outras situações, considere usar o Operations on Demand.

Software do sistema operacional

O AMS Accelerate pode fazer alterações no software do seu sistema operacional durante situações de indisponibilidade por meio da resolução de incidentes, conforme definido em nosso Acordo de Nível de Serviço. O AMS também pode fazer alterações em seus sistemas operacionais como parte doConfiguração automatizada de instâncias no AMS Accelerate.

Código e configuração do aplicativo

O AMS Accelerate nunca modifica seu código (por exemplo, CloudFormation modelos da AWS, outros infrastructure-as-code modelos ou funções do Lambda), mas pode orientar suas equipes sobre quais mudanças são necessárias para seguir as melhores práticas operacionais e de segurança. O AMS Accelerate fornece assistência para solução de problemas de infraestrutura que afetam os aplicativos, mas o AMS Accelerate não acessa nem valida as configurações do seu aplicativo.

Capacidades para sistemas operacionais sem suporte no Accelerate

Um sistema operacional não suportado é qualquer sistema operacional não listado noConfigurações 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.
Monitoramento	O AMS monitora e responde às verificações de status EC2 do sistema e das instâncias da Amazon. As verificaç ões de status do sistema incluem: perda de conectivi dade 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: configura ção 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 e AWS Config regras da Amazon.
Gerenciamento de backups	O AMS fornece gerenciamento de continuidade no Accelerate para EC2 usar AWS Backup planos e cofres personalizados pelo AMS.

Contato e escalonamento

Você tem um gerente de prestação de serviços em nuvem (CSDM) designado que fornece assistência consultiva no AMS Accelerate 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 Accelerate.
- Responda e resolva solicitações de faturamento e relatórios de serviços.
- Forneça insights para recomendações financeiras e de otimização de capacidade.

Horário de contato

Você pode entrar em contato com o AMS Accelerate por diferentes motivos em momentos diferentes.

Recurso	AMS Accelerate
	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
Gerente de entrega de serviços em nuvem (CSDM)	Segunda a sexta-feira: das 08:00 às 17:00, horário comercial local

Horário comercial

Recurso	AMS Accelerate
	Nível Premium
Solicitação de serviço	24/7
Gerenciamento de incidentes (P1)	24/7

Recurso	AMS Accelerate
	Nível Premium
Gerenciamento de incidentes (P2-P3)	24/7
Backup e recuperação	24/7
Gerenciamento de patches	24/7
Monitoramento e alertas	24/7
Gerente de entrega de serviços em nuvem (CSDM)	Segunda a sexta-feira: das 09:00 às 17:00, horário comercial local

Caminho de escalonamento

O AMS oferece suporte aos clientes com gerenciamento de incidentes e gerenciamento de solicitações de serviço, 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 caso de incidente. Para obter detalhes, consulte Enviando um incidente para o Accelerate. Para obter informações gerais sobre o gerenciamento de incidentes do AMS, consulteGerenciamento de incidentes no AMS Accelerate.

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 no Accelerate. Para obter informações gerais sobre solicitações de serviço do AMS, consulteGerenciamento de solicitações de serviço no Accelerate.

Inventário de recursos para Accelerate

Todos os recursos que o AMS Accelerate implanta em suas Conta da AWS contas estão listados na planilha do `resource_inventory.zip`arquivo resource_inventory.xlsx (compactada).

> **Note**
>
> Na coluna Nome do recurso, o prefixo CFN: indica uma ID CloudFormation lógica em vez de um nome de recurso. Elas são mostradas para recursos sem nome, por exemplo, para políticas de bucket do S3.

O AMS implanta um conjunto de serviços conforme descrito noService description (Descrição do serviço). O custo de implantá-los é baixo quando implantados em uma conta vazia, mas o custo aumenta à medida que a utilização aumenta. Por exemplo, os registros são criados e as regras de configuração são invocadas conforme os recursos mudam.

Quando várias alterações são feitas nas regras de configuração, a invocação de conformidade de várias configurações pode ser acionada, resultando em custos mais altos. A mesma possibilidade se aplica à Amazon CloudWatch usada para monitorar instâncias: quanto mais granular for o monitoramento, maior será o custo do serviço. AWS Backup é outro exemplo. Se você tiver vários backups armazenados ou se tiver períodos de retenção mais altos, estará usando mais armazenamento e o custo será maior.

Esses números são difíceis de prever. Durante sua análise mensal de negócios com seu gerente de prestação de serviços em nuvem (CSDM), acompanhe as mudanças e trabalhe para identificar áreas de oportunidade para redução de custos.

Introdução ao AMS Accelerate

Se você ainda não tem uma conta do AWS Managed Services (AMS) operando, comece entrando em contato com um representante de vendas da Amazon Web Services (AWS) usando nossa página AWS Managed Services — Entre em contato com a equipe de vendas.

Depois de se inscrever em um AMS, a equipe do AMS Accelerate orienta você no seguinte processo de integração para cada um dos seus Contas da AWS.

Veja o conjunto de recursos aqui: AWS Managed Services Features

> **Note**
>
> O AMS Accelerate oferece suporte a GovCloud regiões. Se seu serviço residir em um AWS GovCloud (US) Region, consulte também Introdução ao AWS GovCloud (US).

Processo de integração de conta para Accelerate

A integração de uma conta no AMS Accelerate tem quatro etapas.

1. Etapa 1. Descoberta de contas no Acceleratevalia o estado atual da sua conta e identifica bloqueadores técnicos para a integração da sua conta.
2. Etapa 2. Recursos de gerenciamento de integração no Acceleratesolicita que você aceite os termos e condições e crie uma função de integração para os arquitetos de nuvem do AMS Accelerate (CAs), que ajudarão você a definir uma linha de base de segurança e a resolver problemas conforme necessário.
3. Etapa 3. Integração de recursos do AMS com políticas padrãopara recursos do Accelerate, como monitoramento, aplicação de patches e backup.
4. Etapa 4: Personalize recursos no Acceleratgarante que os recursos, incluindo EC2 instâncias, estejam configurados corretamente para seu aplicativo.

Acelere os pré-requisitos de integração

Antes de iniciar o processo de integração, é importante entender as dependências técnicas das quais os componentes do Accelerate dependem.

> **Note**
>
> Para usar o AMS Accelerate, você deve estar em um dos dois Suporte planos compatíveis: Enterprise On-Ramp ou Enterprise. Os planos Developer e Business não se qualificam para o AMS Accelerate. Para saber mais sobre os diferentes planos, consulte Comparar Suporte planos.

Endpoints de VPC do AMS Accelerate

Um VPC endpoint permite conexões privadas entre sua VPC AWS e serviços compatíveis e serviços de VPC endpoint desenvolvidos por. AWS Se você precisar filtrar a conectividade de saída com a Internet, configure os seguintes endpoints de serviço VPC para garantir que o AMS Accelerate tenha conectividade com suas dependências de serviço.

> **Note**
>
> Na lista a seguir, *region* representa o identificador de uma AWS região, por `us-east-2` exemplo, da região Leste dos EUA (Ohio).

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

Para obter informações sobre como configurar endpoints de VPC da AWS, consulte VPC endpoints.

> **Note**
>
> Se você estiver criando VPC endpoints em sua conta para todos os serviços mencionados acima, consulte este modelo de exemplo. CloudFormation Você pode atualizar esse modelo e remover ou adicionar a definição de VPC endpoints de acordo com seu caso de uso.

Conectividade de saída com a Internet no Accelerate

1. Baixar egressMgmt.zip.
2. Abra o arquivo **ams-egress.json**.
3. Encontre as propriedades URLs abaixo do JSON:
   - `WindowsPatching`
   - `RedHatPatching`
   - `AmazonLinuxPatching`
   - `EPELRepository`
4. Permita o acesso a eles URLs.

Testando a conectividade de saída no Accelerate

Teste a conectividade de saída usando um dos métodos a seguir.

> **Note**
>
> Antes de executar o script/comando, substitua o vermelho *region* pelo identificador da sua região, por exemplo,. `us-east-1`

PowerShell Script do Windows

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

Comando Linux

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

Amazon EC2 Systems Manager em Accelerate

Você deve instalar o AWS Systems Manager Agente (Agente SSM) em todas as EC2 instâncias que você deseja que o AMS gerencie. Você também precisa adicionar as permissões de bucket exigidas pelo SSM Agent. Para uma visão geral que inclui a Amazon EC2, consulteEtapa 3. Integração de recursos do AMS com políticas padrão.

IAM em Accelerate

Para permitir que seus usuários leiam e configurem os recursos do AMS Accelerate, como acessar o console do AMS ou configurar backups, você deve conceder permissões explícitas no AWS Identity and Access Management (IAM) para realizar essas ações. Por exemplo, políticas do IAM, consulte Permissões para usar os recursos do AMS.

Etapa 1. Descoberta de contas no Accelerate

O AMS trabalha com você durante a descoberta da conta para avaliar o estado atual da sua conta e identificar bloqueadores técnicos para a integração da sua conta. O AMS não fornece serviços operacionais durante a fase de descoberta da conta. O AMS usa a função `AWSServiceRoleForSupport` vinculada ao serviço para identificar bloqueadores técnicos e, em seguida, trabalha com você para corrigi-los, antes de passar para o estágio de integração no nível da conta.

Processo de descoberta de contas no Accelerate

Para ajudá-lo na análise e descoberta de sua conta, o AMS realiza verificações operacionais para identificar bloqueadores técnicos por meio de chamadas de API somente para leitura. Depois que sua conta é integrada ao AMS, essas verificações são realizadas sob demanda para manter a postura da conta. O AMS trabalha com você para corrigir quaisquer descobertas associadas a essas verificações, quando necessário. O AMS usa as seguintes verificações operacionais e ações de API somente para leitura como parte do Account Discovery:

Verificação operacional	Finalidade	AWS Chamadas de API usadas
AWS Control Tower Avaliação da versão	Identifica a AWS Control Tower versão para garantir que seja a versão mínima	• `ControlTower:GetLandingZone`

Verificação operacional	Finalidade	AWS Chamadas de API usadas
	compatível para integrar seu. Conta da AWS	• `ControlTower:ListEnabledControls` • `ControlTower:ListLandingZones`
AWS CloudTrail Avaliação	Identifica AWS CloudTrail trilhas e suas configurações para integração a fim de minimizar CloudTrail os Conta da AWS custos das trilhas.	• `CloudTrail:GetTrail` • `CloudTrail:ListTrails` • `S3:GetBucketOwnershipControls` • `S3:GetBucketPolicy` • `KMS:GetKeyPolicy` • `CloudTrail:GetEventSelectors` • `S3:GetBucketLogging` • `S3: GetBucketLifecycleConfiguration` • `S3: GetBucketEncryption`
CloudFormation Avaliação do gancho	Identifica CloudFormation ganchos em sua integração Conta da AWS que bloqueiam a implantação do serviço AMS em seu. Conta da AWS	• `CloudFormation:ListTypes`

Verificação operacional	Finalidade	AWS Chamadas de API usadas
Avaliação de EC2 instâncias da Amazon	Identifica EC2 instâncias na sua Conta da AWS que não estão executando o AWS Systems Manager Agente (Agente SSM) e que não são suportadas pelo AMS.	• `EC2:DescribeInstances` • `EC2:DescribeImages` • `SSM:DescribeInstanceInformation`

O AMS Accelerate segue as melhores práticas do setor para atender e manter a elegibilidade de conformidade. O acesso do AMS Accelerate Discovery à sua conta é registrado AWS CloudTrail por meio da função AWSServiceRoleForSupport vinculada ao serviço. Isso ajuda nos requisitos de monitoramento e auditoria. Para obter informações sobre AWS CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Etapa 2. Recursos de gerenciamento de integração no Accelerate

Esta é uma visão geral do processo de integração de recursos de gerenciamento.

Você aceita os termos

Seu gerente de entrega de serviços em nuvem (CSDM) orienta você no processo de aceitação. Você precisa aceitar os Termos e Condições, selecionar Regiões da AWS, complementos e um Acordo de Nível de Serviço (SLA).

Você concede permissões às funções do AMS

Você precisa conceder acesso aos processos do AMS e ao seu Cloud Architect. Você faz isso criando uma CloudFormation pilha para cada função. Veja O modelo para criar funções do AMS e depoisCrie `aws_managedservices_onboarding_role` com o CloudFormation for Accelerate. Para obter mais detalhes, consulte Gerenciamento de acesso no AMS Accelerate.

O AMS revisa sua configuração

Seu Cloud Architect (CA) também procura possíveis problemas de configuração em sua conta, como políticas de controle de serviços (SCPs) e descobertas de segurança que possam impedir o AMS de implantar as ferramentas e os recursos exigidos pelo AMS. Sua CA trabalha com você para ajudá-lo

a corrigir descobertas e remover quaisquer obstáculos à implantação de ferramentas e recursos do AMS.

O AMS analisa suas configurações de AWS CloudTrail trilhas

Seu Cloud Architect (CA) analisará as configurações da CloudTrail trilha e confirmará se você deseja que o AMS implante uma CloudTrail trilha global ou integre o Accelerate aos recursos da sua CloudTrail conta ou da organização. Se você optar por integrar o Accelerate à sua CloudTrail trilha, seu CA o guiará nas atualizações necessárias nas configurações dos recursos da CloudTrail trilha.

O AMS implanta recursos de gerenciamento

A equipe do AMS implanta ferramentas e AWS recursos para fornecer os diferentes serviços do AMS Accelerate. Depois de concluído, o AMS criou a conta do AWS Managed Services e o AMS notifica você de que sua conta está ativa.

Isso conclui a etapa de recursos de gerenciamento de integração. Você pode prosseguir diretamente para a próxima etapa do processo de integração:Etapa 3. Integração de recursos do AMS com políticas padrão.

> **Note**
>
> Agora que sua conta está ativa, você tem a opção de realizar qualquer uma dessas tarefas:
>
> - Crie incidentes e solicitações de serviço para AWS infraestrutura usando o Support Center Console. Consulte Relatórios de incidentes, solicitações de serviço e perguntas sobre faturamento no AMS Accelerate.
> - Veja o status de conformidade em sua conta das AWS Config regras implantadas pelo AMS,. Conformidade de configuração no Accelerate
> - Localize GuardDuty e analise as descobertas do Macie (opcional). Consulte Monitor com GuardDuty.
> - Registros de acesso e CloudTrail auditoria
> - Acompanhe as alterações em sua conta do AMS Accelerate. Consulte Rastreando alterações em suas contas do AMS Accelerate.
> - Use o Resource Tagger para criar tags. Consulte Acelere o marcador de recursos.
> - Solicite patches, backup e AWS Config relatórios. Consulte Relatórios e opções.

Revise e atualize suas configurações para permitir que o AMS Accelerate use sua trilha CloudTrail

O AMS Accelerate depende do AWS CloudTrail registro para gerenciar as auditorias e a conformidade de todos os recursos da sua conta. Durante a integração, você escolhe se o Accelerate implanta uma CloudTrail trilha na sua AWS região principal ou usa eventos gerados pela sua CloudTrail conta existente ou pela trilha da organização. Se sua conta não tiver uma trilha configurada, o Accelerate implantará uma CloudTrail trilha gerenciada durante a integração.

> **Important**
>
> CloudTrail A configuração do gerenciamento de registros só é necessária quando você opta por integrar o AMS Accelerate à sua CloudTrail conta ou trilha da organização.

Revise suas configurações de CloudTrail trilhas, a política de bucket do Amazon S3 AWS KMS e a política principal para o destino de entrega de CloudTrail seus eventos com seu Cloud Architect (CA)

Antes que o Accelerate possa usar sua CloudTrail trilha, você deve trabalhar com seu Cloud Architect (CA) para revisar e atualizar suas configurações para atender aos requisitos do Accelerate. Se você optar por integrar o Accelerate à trilha CloudTrail da sua organização, sua CA trabalhará com você para atualizar o bucket Amazon S3 de destino de entrega de CloudTrail eventos e as AWS KMS principais políticas para permitir consultas entre contas a partir de sua conta do Accelerate. Seu bucket do Amazon S3 pode estar em uma conta gerenciada pelo Accelerate ou em uma conta que você gerencia. Durante a integração, o Accelerate valida se as consultas podem ser feitas no destino de entrega dos eventos de trilha CloudTrail da sua organização e pausa a integração se as consultas falharem. Você trabalha com sua CA para corrigir essas configurações para que a integração possa ser retomada.

Revise e atualize as configurações CloudTrail da sua conta ou trilha da organização

As configurações a seguir são necessárias para integrar o gerenciamento de registros do CloudTrail Accelerate à sua CloudTrail conta ou aos recursos da trilha da organização:

- Sua CloudTrail trilha está configurada para registrar eventos de todos Regiões da AWS.
- Sua CloudTrail trilha tem eventos de serviço global ativados.
- A trilha da sua CloudTrail conta ou organização registra todos os eventos de gerenciamento, incluindo eventos de leitura e gravação, AWS KMS e o registro de eventos da API de dados do Amazon RDS está ativado.

- Sua CloudTrail trilha tem a validação da integridade do arquivo de log ativada.
- O bucket do Amazon S3, sua CloudTrail trilha, entrega eventos para criptografar eventos usando a criptografia SSE-S3 ou SSE-KMS.
- O bucket do Amazon S3 para o qual sua CloudTrail trilha entrega o evento tem o registro de acesso ao servidor ativado.
- O bucket do Amazon S3 para o qual sua CloudTrail trilha entrega o evento tem uma configuração de ciclo de vida que retém seus dados de CloudTrail trilha por pelo menos 18 meses.
- O bucket do Amazon S3 para o qual sua CloudTrail trilha entrega o evento tem a propriedade do objeto definida como proprietária do bucket aplicada.
- O bucket do Amazon S3 para o qual sua CloudTrail trilha entrega o evento pode ser acessado pelo Accelerate.

Revise e atualize a política de bucket do Amazon S3 para seu destino de entrega de CloudTrail eventos

Durante a integração, você trabalha com seu Cloud Architect (CA) para adicionar declarações de política de bucket do Amazon S3 ao CloudTrail seu destino de entrega de eventos. Para permitir que seus usuários consultem alterações no bucket Amazon S3 de destino de entrega de CloudTrail eventos a partir da sua conta do Accelerate, você pode implantar uma função do IAM nomeada uniformemente em cada conta gerenciada pelo Accelerate em sua organização e adicioná-la à `aws:PrincipalArn` lista em todas as declarações de política do bucket do Amazon S3. Com essa configuração, seus usuários podem consultar e analisar os eventos de trilha da CloudTrail organização da sua conta no Accelerate usando o Athena. Para obter mais informações sobre como atualizar uma política de bucket do Amazon S3, consulte Adicionar uma política de bucket usando o console do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

> **Important**
>
> A atualização da sua política de bucket do Amazon S3 é necessária somente quando o Accelerate se integra a uma CloudTrail trilha que entrega eventos a um bucket S3 centralizado. O Accelerate não oferece suporte à integração com uma CloudTrail trilha que entrega em um bucket centralizado, mas não tem as contas em uma AWS organização.

> **Note**
>
> Antes de atualizar sua política de bucket do Amazon S3, substitua *red* os campos por valores aplicáveis:
>
> - *amzn-s3-demo-bucket*com o nome do bucket do Amazon S3 que contém os eventos de trilha de suas contas.
> - *your-organization-id*com o ID da AWS organização da qual suas contas são membros.
> - *your-optional-s3-log-delievery-prefix*com o CloudTrail prefixo de entrega do bucket Amazon S3 da sua trilha. Por exemplomy-bucket-prefix, que você pode ter definido ao criar sua CloudTrail trilha.
>
>   Se você não configurou um prefixo de entrega de bucket do Amazon S3 para sua trilha, remova "*your-optional-s3-log-delievery-prefix*" e a barra contínua (/) das seguintes declarações de política de bucket do Amazon S3.

As três declarações de política de bucket do Amazon S3 a seguir concedem ao Accelerate acesso para recuperar as configurações e executar consultas do AWS Athena para analisar os eventos no bucket Amazon S3 de destino de entrega de CloudTrail eventos a partir da sua conta do Accelerate.

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

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

```
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

Revise e atualize a política AWS KMS principal para seu destino de entrega de CloudTrail eventos

Durante a integração, você trabalha com seu Cloud Architect (CA) para atualizar a política de AWS KMS chaves usada para criptografar os eventos de CloudTrail trilha entregues ao seu bucket do Amazon S3. Certifique-se de anexar as declarações de política de AWS KMS chave de referência à sua chave existente AWS KMS . Isso configura o Accelerate para se integrar ao seu destino atual de entrega de eventos de CloudTrail trilha, bucket do Amazon S3, e descriptografar eventos. Para permitir que seus usuários consultem alterações em seu bucket Amazon S3 de destino de entrega de CloudTrail eventos a partir de sua conta do Accelerate, você pode implantar uma função do IAM nomeada uniformemente em cada conta da sua organização que o Accelerate está gerenciando e adicioná-la à lista “aws:PrincipalArn”. Com essa configuração, seus usuários podem consultar eventos.

Há diferentes cenários AWS KMS principais de atualização de políticas a serem considerados. Você pode ter apenas uma AWS KMS chave configurada em sua CloudTrail trilha para criptografar todos os eventos, e não ter uma AWS KMS chave que criptografe objetos em seu bucket do Amazon S3. Ou você pode ter uma AWS KMS chave que criptografa eventos entregues por CloudTrail e outra AWS KMS chave que criptografa todos os objetos armazenados em seu bucket do Amazon S3. Quando você tem duas AWS KMS chaves, você atualiza a AWS KMS política de chaves de cada chave para conceder ao Accelerate acesso aos seus CloudTrail eventos. Certifique-se de alterar a declaração de política de AWS KMS chaves de referência à sua política de AWS KMS chaves existente antes de atualizar a política. Para obter mais informações sobre como atualizar uma política de AWS KMS chaves, consulte Alterar uma política de chaves no Guia AWS Key Management Service do usuário.

Important

Você precisa atualizar sua política de AWS KMS chaves somente quando o Accelerate se integra a uma CloudTrail trilha com a criptografia SSE-KMS do arquivo de log ativada.

Note

Antes de aplicar essa declaração de política de AWS KMS chaves à AWS KMS chave usada para criptografar seus AWS CloudTrail eventos entregues ao seu bucket do Amazon S3, substitua os *red* seguintes campos pelos valores aplicáveis:

- *YOUR-ORGANIZATION-ID*com o ID da AWS organização da qual suas contas são membros.

Essa declaração de política AWS KMS fundamental concede ao Accelerate acesso para decifrar e consultar eventos de trilha entregues ao bucket do Amazon S3 a partir de cada conta em sua organização, com acesso restrito ao Athena, usado pelo Accelerate para consultar e analisar eventos. CloudTrail .

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

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

O modelo para criar funções do AMS

A função do AMS a seguir concede permissões ao seu arquiteto de nuvem (CA) do AMS. O arquivo zip a seguir contém o código e o CloudFormation modelo do Terraform que simplificam a criação da função, da política de permissões e da política de confiança do IAM. Para obter mais informações, consulte seu CA.

Função	Exigido por	Modelos de exemplo
`aws_managedservices_onboarding_role`	Pessoal do AMS somente durante a integração	onboarding_role_minimal.zip

> **Note**
>
> Depois de selecionar e baixar um modelo de amostra (um por função), você os carregará como definições de CloudFormation pilhasCrie `aws_managedservices_onboarding_role` com o CloudFormation for Accelerate.

Crie **`aws_managedservices_onboarding_role`** com o CloudFormation for Accelerate

Você pode criar a AWS Identity and Access Management função,`aws_managedservices_onboarding_role`, com a CloudFormation partir do Console de gerenciamento da AWS. Ou você pode usar comandos de AWS CloudShell para implantar a função.

Use o Console de gerenciamento da AWS

> **Note**
>
> Antes de começar, tenha um arquivo JSON ou YAML para cada função pronto para ser carregado. Para obter mais informações, consulte O modelo para criar funções do AMS.

Para criar a função a partir do Console de gerenciamento da AWS, conclua as seguintes etapas:

1. Faça login no Console de gerenciamento da AWS e abra o CloudFormation console em https://console.aws.amazon.com/cloudformation.

2. Escolha Criar pilha > Com novos recursos (padrão). Você vê a página a seguir.

3. Escolha Carregar um arquivo de modelo, faça upload do arquivo JSON ou YAML da função do IAM e escolha Avançar. Você vê a página a seguir.

4. Insira o nome da pilha "**`ams-onboarding-role`**" no campo Nome da pilha. Insira um DateOfExpiryusando o formato “YYYY-MM-DDT 00:00:00 Z” (recomenda-se 30 dias a partir da data atual). Continue rolando para baixo e selecionando Avançar até chegar a esta página:

5. Verifique se a caixa de seleção está marcada e selecione Criar pilha.
6. Verifique se a pilha foi criada com sucesso.

Use comandos de AWS CloudShell

Para implantar a função `aws_managedservices_onboarding_role` do IAM, execute o seguinte comando em AWS CloudShell:

AWS CLI

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/onboarding_role_minimal.zip" -o "onboarding_role_minimal.zip"
```

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

AWS Tools for PowerShell

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

Depois de criar a função, trabalhe com seu Cloud Architect (CA) para concluir o Etapa 2. Recursos de gerenciamento de integração no Accelerate processo. Depois que o AMS informar que sua conta está ativa, você estará pronto para integrar suas instâncias.

Etapa 3. Integração de recursos do AMS com políticas padrão

Nesse estágio, você integra os recursos do AMS com políticas padrão. Isso inclui adicionar EC2 instâncias da Amazon e configurar monitoramento, backup, AWS Config remediação e correção (se aplicável, o AMS Patch Orchestrator é um complemento que você deve solicitar especificamente) de acordo com suas preferências. Você pode fazer isso sozinho ou solicitar que o AMS integre recursos com base em suas entradas. Para solicitar ajuda do AMS, crie uma solicitação de serviço e forneça todas as entradas necessárias para concluir a tarefa. Lembre-se de que as solicitações de serviço não são resolvidas imediatamente.

> **Note**
>
> Embora uma conta possa usar políticas padrão para backup, correção ou monitoramento, os recursos precisam ser marcados para que a política apropriada seja efetiva.

Tópicos

- (Opcional) Modelo de início rápido no Accelerate
- Integração Acelere o monitoramento
- EC2 Instâncias de integração para acelerar
- Integração no AWS Backup Accelerate
- Integração de patches no Accelerate
- Analise os relatórios de não conformidade no Accelerate

(Opcional) Modelo de início rápido no Accelerate

O modelo Quick Start automatiza a implantação e a configuração do AMS Resource Tagger em contas habilitadas para AWS Accelerate. Esse modelo economiza tempo e esforço em comparação com a configuração manual. Use esse modelo no estado em que se encontra para definir as noções básicas de monitoramento, aplicação de patches e backup em uma conta. Ou use-o StackSet para aplicar configurações em Organizations Units para padronizar as configurações de várias contas.

Você também pode usá-lo como ponto de partida para criar seu próprio perfil personalizado do AMS Resource Tagger e usar trechos da documentação para criar definições mais complexas para marcação.

Funcionalidade do modelo Quick Start

O modelo de Início Rápido conclui as seguintes tarefas:

- Cria e implanta uma versão de configuração para o AMS Resource Tagger.
- Aplica tags às EC2 instâncias da Amazon que permitem o gerenciamento do AMS e a criação de recursos de monitoramento.
- (Opcional) Aplica tags às EC2 instâncias gerenciadas que permitem que elas sejam corrigidas no cronograma desejado e cria uma janela de manutenção de patches para facilitar a aplicação de patches.

> ⚠ Warning
>
> Por padrão, as instâncias são reinicializadas e as interrompidas são iniciadas automaticamente para a instalação do patch.

- (Opcional) Aplica tags às EC2 instâncias gerenciadas que permitem que elas sejam copiadas conforme definido no Plano de Backup padrão do AMS.
- (Opcional) Aplica tags aos recursos gerenciados do Amazon Relational Database Service (Amazon RDS) que permitem o backup deles de acordo com o plano de backup aprimorado. Um plano de backup também permite a recuperação pontual (PITR) para o Amazon RDS. Se o backup automático do Amazon RDS não estiver habilitado, o banco de dados será reiniciado próximo ao horário da próxima janela de backup.

Substituições e exclusões do modelo Quick Start

Depois de usar esse modelo para criar uma pilha de Início Rápido, use as etapas a seguir para excluir instâncias específicas do Gerenciamento/Monitoramento, Aplicação de Patches ou Backup:

- Gerenciamento e monitoramento: Para excluir uma EC2 instância de ser gerenciada e monitorada pelo AMS, adicione esta tag à instância:`ExcludeFromAMSQuickStartMonitoring=true`.
- Aplicação de patches: EC2 instâncias que são membros de um grupo do Auto Scaling, do Amazon Elastic Container Service ou do cluster do Amazon Elastic Kubernetes Service são excluídas da aplicação de patches por esse modelo de início rápido.

  Para desativar a criação de uma janela de patches e a marcação de EC2 instâncias relacionada a patches, defina o CloudFormation parâmetro stack como. `EnablePatching=false`

  Para excluir uma EC2 instância de ser alvo da janela de patches do Quick Start quando`EnablePatching=true`, adicione esta tag à instância:`ExcludeFromAMSQuickStartPatching=true`.
- Backup: EC2 instâncias que são membros de grupos do Auto Scaling, cluster ECS ou EKS são excluídas do Backup por esse modelo de Início Rápido.

  Para excluir uma EC2 instância de ser alvo do Plano de Backup padrão do AMS`EnableBackup=true`, quando, adicione esta tag a essa instância:`ExcludeFromAMSQuickStartBackup=true`.

> **Tip**
>
> Você pode marcar EC2 instâncias em massa. Use o Editor de tags para selecionar e marcar recursos em massa em uma etapa do. Console de gerenciamento da AWS

Parâmetros do modelo Quick Start

Esse modelo de início rápido configura o Resource Tagger para adicionar a tag `ams:rt:ams-managed=true` a todas as EC2 instâncias da conta, excluindo as instâncias às quais você adiciona a `ExcludeFromAMSQuickStartMonitoring=true` tag. Use os seguintes parâmetros para controlar as partes opcionais dessa pilha de acordo com seus requisitos:

Parâmetro CFN	Valor	Efeito
EnableBackup	'verdadeiro' (padrão)	Todas as EC2 instâncias gerenciadas pelo AMS (`ams:rt:ams-managed=true`) são marcadas `ams:rt:backup-orchestrator=true` para backup diariamente às 4h UTC, de acordo com o Plano de Backup padrão do AMS. Para todas as instâncias e clusters do RDS, o modelo aplica o `ams:rt:backup-orchestrator-enhanced=true` "backup contínuo" com retenção máxima (31 dias) de acordo com o plano de backup aprimorado. Se isso alterar seu período de retenção de PITR, o banco de dados poderá ser reiniciado em alguns casos, por exemplo, se houver

Parâmetro CFN	Valor	Efeito
		outras atualizações de configuração pendentes.
	'falso'	Nenhuma instância é destinada para backup de acordo com esse modelo de início rápido.
EnablePatching	'false' (padrão)	Nenhuma instância é alvo de patches de acordo com esse modelo de Início Rápido.
	'verdadeiro'	Todas as instâncias gerenciadas pelo AMS (`ams:rt:ams-managed=true`) são marcadas com `ams:rt:Patch Group=AMS QuickStartPatchWindow` e um recurso básico da janela de manutenção do SSM é criado para facilitar a aplicação de patches de acordo com o cronograma definido em. `CronExpression` Para aplicar a `ams:rt:Patch Group` tag à EC2 instância, você precisa desativar o acesso às tags nos metadados da instância.
CronExpression	-	O valor padrão de `cron(0 30 19 ? * SAT#2 *)` define o segundo sábado do mês às 19h30, de acordo com o `Timezone` parâmetro. Use a sintaxe cron.
Fuso horário	-	As instâncias de destino são corrigidas de acordo `CronExpression` com. Use o formato IANA.

Baixe o modelo de Início Rápido

Faça o download AMSQuickdo arquivo Start.zip.

Ou execute o comando a seguir AWS CloudShellpara implantar oAMSQuickStart.yaml:

AWS Command Line Interface

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/AMSQuickStart.zip" -o "AMSQuickStart.zip"
unzip -q -o AMSQuickStart.zip
for region in region1 region2 ;
do
aws cloudformation create-stack \
    --region $region \
    --stack-name "AMSQuickStart" \
    --template-body file://AMSQuickStart.yaml \
    --parameters \
        ParameterKey=EnableBackup,ParameterValue="true" \
        ParameterKey=EnablePatching,ParameterValue="false" \
        ParameterKey=Timezone,ParameterValue="US/Eastern" \
        ParameterKey=CronExpression,ParameterValue="cron(0 30 19 ? * SAT#2 *)" \
;
done
```

AWS Tools for PowerShell

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

```
}
```

Para obter uma descrição de cada parâmetro, consulte a seção anterior,Parâmetros do modelo Quick Start.

Integração Acelere o monitoramento

O monitoramento é ativado por padrão para todos os novos recursos, exceto as EC2 instâncias da Amazon. Você pode começar a monitorar suas EC2 instâncias da Amazon marcando suas instâncias.

Para integrar o monitoramento, primeiro certifique-se de que sua configuração monitore os recursos que você deseja que o AMS monitore e ignore os recursos que você deseja que ele ignore.

Você pode usar os CloudWatch painéis a seguir para explorar quantos de seus recursos são direcionados pelo monitoramento e marcação do AMS e quantos não são. Em sua conta, navegue até o console de CloudWatch painéis e selecione uma das seguintes opções:

- Painel de relatórios do AMS-Alarm-Manager
- Painel de relatórios do AMS-Resource-Tagger

Para obter uma descrição completa das métricas do painel, consulte:

- Visualizando o número de recursos monitorados pelo Alarm Manager for Accelerate
- Visualizando o número de recursos gerenciados pelo Resource Tagger

Recursos de integração a serem monitorados no Accelerate

Para substituir o comportamento padrão, por exemplo, para desativar o monitoramento padrão para não EC2 recursos, você precisa desmarcar esses recursos usando um perfil de configuração personalizado. Para obter mais informações sobre marcação para monitoramento, consulteMonitoramento em Accelerate.

O monitoramento é desativado para EC2 instâncias até que você as integre, o que inclui a marcação de suas instâncias usando um perfil de configuração personalizado. A próxima seção descreve a integração de EC2 instâncias.

Criação de um perfil de configuração de monitoramento no Accelerate

- Para obter informações sobre como usar a configuração padrão, consulteGerenciador de alarmes acelerado.
- Para obter informações sobre como usar uma configuração personalizada, consulteModificando a configuração padrão do alarme Accelerate.

EC2 Instâncias de integração para acelerar

EC2 as instâncias são integradas ao AMS Accelerate por meio de um processo chamado Configuração Automatizada de Instâncias, que garante que cada instância esteja gravando os registros corretos e emitindo as métricas corretas para que o AMS gerencie adequadamente a instância. Você deve integrar todas as suas EC2 instâncias, a menos que queira especificamente que o AMS ignore algumas. A configuração automatizada de instâncias exige que sejam atendidas condições específicas que permitam ao AMS configurar a instância (para obter detalhes, consultePré-requisitos para configuração automática de instâncias no Accelerate). A condição mais importante é que o AWS Systems Manager agente (agente SSM) precise ser instalado em cada EC2 instância da Amazon que você deseja que o AMS gerencie para você. Para obter mais informações sobre o agente SSM, consulte Trabalhando com o agente SSM.

SSM pré-instalado no padrão AMIs para Accelerate

O agente SSM já está instalado em AWS-fornecido AMIs para os seguintes sistemas operacionais.

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

Se você estiver usando um desses AWS fornecidos AMIs, consulteMarcar instâncias no Accelerate.

Instalação manual do SSM por SSM no Accelerate

Para os seguintes sistemas operacionais, ou ao usar uma AMI personalizada, você pode instalar manualmente o agente SSM. Ou você pode usar o recurso de instalação automática do AMS SSM Agent. Para saber mais sobre a instalação automática do SSM, consulteInstalação automática do SSM Agent. Para obter instruções sobre a instalação manual, selecione o link do seu sistema operacional:

- Instalação do CentOS SSM
- Instalação do Oracle SSM
- Instalação do Red Hat SSM
- Instalação do SUSE Linux Enterprise Server SSM
- Instalação do Windows SSM

Marcar instâncias no Accelerate

Depois que o agente SSM for instalado, você deverá marcar suas instâncias. Consulte Marcação no AMS Accelerate.

Configuração automatizada de instâncias no Accelerate

Depois que sua instância é marcada, o AMS executa uma configuração de instância automatizada, que inclui:

- Registre registros e métricas do sistema operacional
- Habilite o acesso remoto para engenheiros do AMS
- Execute comandos remotos na instância

Essas tarefas são essenciais para os serviços de monitoramento, correção e registro do AMS e para que o AMS responda a incidentes. Para obter detalhes sobre como configurar a configuração automatizada de instâncias, consulteConfiguração automatizada de instâncias no AMS Accelerate.

Depois que a configuração automatizada da instância for concluída, você poderá:

- Crie incidentes e solicitações de serviço para EC2 instâncias e sistemas operacionais da Amazon usando o console do Support Center. Para obter mais informações, consulte Relatórios de incidentes, solicitações de serviço e perguntas sobre faturamento no AMS Accelerate.
- Acesse e audite EC2 os registros da Amazon
- Obtenha relatórios de patches

Integração no AWS Backup Accelerate

Para configurar backups, você precisa criar políticas de backup chamadas planos de backup. Um plano de backup especifica quais AWS recursos devem ser copiados, com que frequência eles precisam ser copiados e o período de retenção do backup. Recomendamos avaliar os requisitos

de continuidade, segurança e conformidade da sua organização para determinar quais planos de backup você precisa.

Inscrever-se

- Certifique-se de que AWS Backup esteja habilitado para cada conta, região e tipo de recurso seguindo as etapas aqui:

  Introdução 1: Opção de serviço.

  Opcionalmente, Introdução 2: Crie backup sob demanda.

Escolha um plano de backup

- Para escolher um plano de backup, consulteSelecione um plano de backup do AMS.

Adicionar recursos

Por padrão, os recursos não estão associados a um plano de backup. Eles precisam ser adicionados a um plano de backup.

- Para adicionar recursos a um plano de backup, consulteMarque seus recursos para aplicar os planos de backup do AMS.
- Para habilitar o backup em todos os recursos usando tags, consulteGerenciando tags para backups no Accelerate.

Integração de patches no Accelerate

Você precisa configurar a aplicação de patches para garantir que seu software esteja up-to-date e atenda às suas políticas de conformidade.

AWS Backup pré-requisito: Para permitir a criação de um snapshot do volume raiz durante a janela de manutenção de patches, certifique-se de que ele AWS Backup esteja habilitado para cada conta e região para o tipo de recurso do Amazon EBS seguindo as etapas aqui: Introdução 1: Opção de serviço. (Você não precisa continuar em Introdução 2: Crie um backup sob demanda.)

Quando aplicar o patch: o patch ocorre durante uma janela de manutenção. Você pode programar janelas de manutenção para que os patches sejam aplicados somente em horários predefinidos.

O que corrigir: Você precisa associar as EC2 instâncias da Amazon que você deseja corrigir a uma janela de manutenção. Para associar as instâncias a uma janela de manutenção, as EC2 instâncias da Amazon devem ser marcadas e a janela de manutenção deve ter essas tags como destino.

Quais patches instalar: usando as linhas de base de patches, você define regras para aprovar automaticamente certos tipos de patches, como patches de sistema operacional ou patches de alta severidade. Você também pode especificar exceções às suas regras, por exemplo, listas de patches que são sempre aprovados ou rejeitados.

Consulte Recomendações de patches para obter orientação sobre as políticas de EC2 patches da Amazon.

- Para começar a configurar o gerenciamento de patches, consulte Entenda o gerenciamento de patches no AMS Accelerate
- Para criar uma configuração de patch personalizada, consulteLinha de base de patch personalizada com o AMS Accelerate.

Analise os relatórios de não conformidade no Accelerate

O AMS implanta AWS Config regras que ajudam você a identificar violações dos padrões estabelecidos pelo Center for Internet Security (CIS), pelo Cloud Security Framework (CSF) do National Institute of Standards and Technology (NIST). Recomendamos que você analise o relatório de não conformidade com sua equipe de entrega para priorizar as ações de remediação, de forma que sua conta seja definida como base para um estado de conformidade.

Etapa 4: Personalize recursos no Accelerate

Nesse estágio, você já integrou o monitoramento, a aplicação de patches e o backup com políticas padrão. Agora você tem a oportunidade de personalizar as políticas para atender às suas necessidades.

Você pode optar por usar as políticas padrão para correção, backup ou monitoramento, ou escolher uma política personalizada com base em suas necessidades. O AMS usa tags para associar recursos às políticas operacionais. O AMS fornece um marcador de recursos que permite especificar regras sobre como as tags são aplicadas aos seus AWS recursos com base no agrupamento de aplicativos ou em outra lógica de agrupamento. Para obter mais informações, consulte. Acelere o marcador de recursos

O recurso de tags fornecido pelo cliente permite que você adicione e exclua tags personalizadas aos recursos do AMS. Para obter mais informações, consulte Tags fornecidas pelo cliente no Accelerate.

Tópicos

- Personalize o monitoramento no Accelerate
- Personalize o backup no Accelerate
- Personalize a aplicação de patches no Accelerate

Personalize o monitoramento no Accelerate

Para personalizar o monitoramento de seus recursos de nuvem com base nas necessidades do seu aplicativo:

1. Crie uma política de monitoramento personalizada. Consulte Modificando a configuração padrão do alarme Accelerate.
2. Aplique uma política personalizada aos recursos usando tags. Consulte Monitoramento em Accelerate
3. Encaminhe alertas para o proprietário do recurso. Consulte Notificação de alerta baseada em tag.

Você pode usar os CloudWatch painéis a seguir para explorar quantos de seus recursos são direcionados pelo monitoramento e marcação do AMS e quantos não são. Em sua conta, navegue até o console de CloudWatch painéis e selecione uma das seguintes opções:

- Painel de relatórios do AMS-Alarm-Manager
- Painel de relatórios do AMS-Resource-Tagger

Para obter uma descrição completa das métricas do painel, consulte:

- Visualizando o número de recursos monitorados pelo Alarm Manager for Accelerate
- Visualizando o número de recursos gerenciados pelo Resource Tagger

Personalize o backup no Accelerate

Você não pode personalizar os planos de backup padrão do AMS. Em vez disso, crie um novo plano de backup com base nas necessidades do seu aplicativo e, em seguida, anexe recursos ao seu plano personalizado usando tags. Cabe a você escolher quais recursos o AMS deve fazer

backup, com que frequência e por qual período de retenção. Recomendamos avaliar os requisitos de continuidade, segurança e conformidade de sua organização para determinar quais planos de backup você precisa.

- Para criar um plano de backup, consulte Criação de um plano de backup.
- Para atribuir recursos a um plano de backup, consulte Atribuição de recursos a um plano de backup.

Personalize a aplicação de patches no Accelerate

A aplicação de patches garante que seu software esteja up-to-date e atenda às suas políticas de conformidade.

Quando aplicar o patch: o patch ocorre durante uma janela de manutenção. Você pode programar janelas de manutenção para que os patches sejam aplicados somente em horários predefinidos.

O que corrigir: Você precisa associar as EC2 instâncias da Amazon que você deseja corrigir a uma janela de manutenção. Para associar as instâncias a uma janela de manutenção, as EC2 instâncias da Amazon devem ser marcadas e a janela de manutenção deve ter essas tags como destino.

Quais patches instalar: usando as linhas de base de patches, você define regras para aprovar automaticamente certos tipos de patches, como patches de sistema operacional ou patches de alta severidade. Você também pode especificar exceções às suas regras, por exemplo, listas de patches que são sempre aprovados ou rejeitados.

- Para recomendações gerais de patches, consulteRecomendações de patches.
- Para criar janelas de manutenção personalizadas, consulteCrie uma janela de manutenção de patches no AMS.
- Para criar linhas de base de patch personalizadas, consulte. Linha de base de patch personalizada com o AMS Accelerate
- Para encaminhar alertas de patch para o proprietário do recurso, consulteEntenda as notificações de patches e as falhas de patches no AMS Accelerate.

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 Accelerate tem os seguintes recursos:

- Página de abertura: A página de abertura tem caixas de informações e links para facilitar seu acesso aos incidentes .
- Páginas de destaque, links no painel de navegação esquerdo:
  - Painel: fornece uma visão geral do status atual da sua conta, incluindo:
    - Incidentes em seus recursos: um botão para abrir um caso de incidente no AWS Support Center, além de quantos casos de incidentes estão aguardando aprovação e exigem sua atenção e quantos estão abertos
    - Status de conformidade: links para regras e recursos que não estão em conformidade ou estão em conformidade
    - Solicitações de serviço: um botão para abrir um caso de solicitação de serviço no AWS Support Center, além de quantas estão aguardando aprovação e precisam de sua atenção e quantas estão abertas
    - Segurança em nível de conta: links para detalhes sobre descobertas de detecção de ameaças em tempo real e GuardDuty descobertas de Macie sobre segurança e privacidade de dados

    - Ações rápidas: abra suas páginas de configuração de cofres de Backup ou instâncias de patch
  - Relatórios: abre a página Relatórios e os relatórios padrão, Backup Diário, Patch Diário e Cobrança Mensal
  - Configuração: garanta que seus recursos estejam sendo gerenciados com sucesso e de acordo com suas especificações.
    - Instalar o agente SSM: o agente SSM é obrigatório
    - Configurar regras de marcação: abre o AMS Resource Tagger
    - Configurar alarmes: abre a configuração de CloudWatch alarme do AMS
    - Configurar o cronograma de patches: abre o console do AWS Systems Manager
    - Configurar linhas de base de patches: abre o console do AWS Patch Manager
    - Configurar planos de backup: abre o console do AWS Backup
- Destaque do recurso: informações sobre as atualizações mais recentes do console
- Documentação: A página inicial da documentação do AWS Managed Services

Padrões AMS

Um padrão do AWS Managed Services (AMS) é uma solução generalizada que resolve uma família de casos de uso no ambiente gerenciado do AMS.

Ao operar na plataforma AMS, os arquitetos de nuvem do AMS (CAs) trabalham com você para atender aos seus requisitos comerciais e operacionais. Embora os clientes do AMS operem de uma forma única, notamos que os clientes têm casos de uso semelhantes. Nesses casos, CAs crie modelos gerais de solução, ou “padrões”, que sejam usados em vários ambientes de clientes com o mínimo esforço de configuração e implantação.

Os padrões do AMS são criados para ajudar a fornecer recursos aos clientes do AMS e geralmente criados pela CA da conta do cliente que os solicita.

Como funcionam os padrões do AMS

Para solicitar mais detalhes sobre cada padrão, incluindo os modelos de formação de nuvem necessários para que você possa implantar o padrão, envie uma solicitação de serviço do AMS com o assunto “Solicitação de detalhes adicionais sobre o padrão*Pattern_Name*” (substitua o padrão desejado) e adicione seu arquiteto de nuvem (CA) do AMS à opção Contatos adicionais.

Os padrões AMS são classificados em duas (2) categorias:

- Uso geral: os padrões são considerados estáveis, pois foram implantados e utilizados por vários clientes do AMS
- Modo de visualização: o AMS recomenda implantar padrões do modo de visualização em seus ambientes de não produção para validação e interagir com seu arquiteto de nuvem para discutir o caso de uso antes da implantação.

> **Important**
>
> Os padrões do AMS não aderem aos seus Acordos de Nível de Serviço padrão do AMS, Acordos de Nível de Serviço (SLAs) e Objetivos de Nível de Serviço (SLOs). Support e atualizações do padrão são feitos com base no melhor esforço.
> Este AWS conteúdo é fornecido de acordo com os termos do Contrato do AWS Cliente ou outro acordo escrito entre o cliente e a Amazon Web Services, Inc. ou a Amazon Web Services EMEA SARL (“AWS Europa”) ou ambas.
> O material incorporado neste software é fornecido a você “no estado em que se encontra” e sem garantia de qualquer tipo, expressa, implícita ou não, incluindo, sem limitação, qualquer garantia de adequação a uma finalidade específica.

Padrões AMS

Padrões AMS.

Padrões AMS

Nome	Visão geral	Benefícios	Categoria
Personalizar notificações CloudWatch de alarme	Personalize as notificações de CloudWatch alarme para incluir informações de tags de instância, como nome da instância, ID do	Adicionar informações contextuais às notificações de alarme as tornará mais significativas e fornecerá informações acionáveis.	Monitoramento

Nome	Visão geral	Benefícios	Categoria
	aplicativo e assim por diante.		
Relatórios de uso do disco	O padrão Disk Usage Reporting coleta o espaço de consumo de volumes em várias contas de aplicativos e apresenta o resultado como um relatório centralizado no Amazon S3 com o recurso de consulta de tabelas do Athena.	Forneça informações sobre o uso real dos volumes da conta para determinar oportunidades de redução de custos.	Otimização de custo
Pilha Prowler	Executa verificações do Prowler em contas que usam a Amazon EC2 onde não CloudShell podem ser usadas.	Ajude a desbloquear o Accelerate onboarding (Prowler) nos casos em que não CloudShell possa ser usado devido a permissões ou problemas de tempo limite, sem qualquer impacto em sua postura de segurança atual.	Segurança

Nome	Visão geral	Benefícios	Categoria
Replicação do AMS Amazon S3 com chaves de objeto personalizadas	Faça cópias dos objetos do Amazon S3 e retenha todos os metadados e chaves de objetos (pastas). Remove parte das chaves do objeto de origem ou cria chaves de objeto de destino personalizadas durante a replicação.	Personalize as chaves de objeto (pastas) durante a replicação do Amazon S3 sem precisar de scripts adicionais para mover objetos para as pastas necessárias.	Confiabilidade
Exclusão de snapshots do Amazon EBS	Automação baseada em Lambda e CloudWatch Eventos para automatizar a exclusão de snapshots do Amazon EBS tirados de fora AWS Backup, com base na retenção.	Ajude a eliminar instantâneos individuais tirados fora do AWS Backup orquestrador, economizando custos adicionais ao longo do tempo.	Otimização de custo

Nome	Visão geral	Benefícios	Categoria
Rotação de segredos do AMS Amazon RDS	Usando um CloudFormation modelo, implante automaticamente todos os recursos necessários (função Lambda, grupos de segurança, interfaces de rede elásticas ou ENIs) necessários para alternar segredos em bancos de dados Amazon RDS, Redshift e DocumentDB compatíveis.	Automatize a rotação de segredos do banco de dados e forneça um mecanismo de notificação quando ocorrer uma falha na rotação.	Segurança
Rotação automática de chaves	Alterne automaticamente as chaves de acesso e secretas para usuários do IAM com base em CloudWatch Eventos e Lambda.	Rotação mais fácil de acesso e chaves secretas para usuários do IAM.	Segurança

Nome	Visão geral	Benefícios	Categoria
Etiquetador de snapshots de volume do Amazon EBS	Marque todos os volumes e snapshots do Amazon EBS usando as tags nas instâncias da Amazon EC2 .	Ajude a categorizar e monitorar os custos com informações comerciais significativas e relevantes, facilitando a validação de onde o dinheiro está sendo gasto e possibilite o uso da automação para volumes e instantâneos marcados. Melhor prática altamente recomendada pelo pilar de otimização de AWS custos.	Etiquetagem (otimização de custos, segurança, gerenciamento de incidentes e automação)

Configuração automatizada de instâncias no AMS Accelerate

O AMS Accelerate fornece um serviço automatizado de configuração de instâncias. Esse serviço garante que uma instância esteja emitindo os registros e métricas corretos para que o AMS gerencie adequadamente a instância. A configuração automatizada de instâncias tem seus próprios pré-requisitos e etapas de integração, descritos posteriormente nesta seção.

Tópicos

- Como a configuração automatizada de instâncias funciona no Accelerate
- Instalação automática do SSM Agent
- Alterações automatizadas na configuração da instância

Como a configuração automatizada de instâncias funciona no Accelerate

A configuração automatizada de instâncias permite que o AMS Accelerate execute determinadas configurações diariamente nas instâncias que você indica adicionando agentes e tags específicos.

Pré-requisitos para configuração automática de instâncias no Accelerate

Essas condições devem ser atendidas para permitir que o AMS Accelerate execute as ações automatizadas descritas anteriormente em instâncias gerenciadas.

O agente SSM está instalado

A configuração automática da instância do AMS Accelerate exige que o Agente AWS Systems Manager SSM esteja instalado.

Para obter informações sobre como usar o recurso de instalação automática do AMS SSM Agent, consulteInstalação automática do SSM Agent.

Para obter informações sobre a instalação manual do SSM Agent, consulte o seguinte:

- Linux: instale manualmente o SSM Agent nas EC2 instâncias da Amazon para Linux - AWS Systems Manager
- Windows: instale manualmente o SSM Agent nas EC2 instâncias da Amazon para Windows Server - AWS Systems Manager

O agente SSM está no estado gerenciado

A configuração automatizada da instância do AMS Accelerate requer um agente SSM operacional. O agente SSM deve estar instalado e a EC2 instância da Amazon deve estar no estado gerenciado. Para obter mais informações, consulte a AWS documentação Trabalhando com o SSM Agent.

Configuração automatizada de instâncias

Supondo que os pré-requisitos tenham sido atendidos, adicionar uma tag de instância específica da Amazon inicia automaticamente a configuração automática da EC2 instância do AMS Accelerate. Use um dos métodos a seguir para adicionar essa tag:

1. (Altamente recomendado) Use o AMS Accelerate Resource Tagger

   Para configurar a lógica de marcação da sua conta, consulteComo funcionam as tags. Depois que a marcação for concluída, as tags e a configuração automatizada da instância serão tratadas automaticamente.
2. Adicionar tags manualmente

   Adicione manualmente a seguinte tag às EC2 instâncias da Amazon:

Chave: ams:rt:ams-managed, Valor: true.

> **Note**
>
> O serviço de configuração da instância tenta aplicar as configurações necessárias do AMS quando a tag ams:rt:ams-managed é aplicada à instância. O serviço declara as configurações necessárias do AMS sempre que uma instância é iniciada e quando ocorre uma verificação diária da configuração do AMS.

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**
>
> - Se sua conta estiver integrada ao AMS Accelerate após 6/03/2024, esse recurso estará ativado por padrão. Para desativar esse recurso, entre em contato com sua CA ou CSDM.
> - Para ativar esse recurso em contas integradas antes de 6/03/2024, entre em contato com sua CA ou CSDM.
> - 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.

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.

Alterações automatizadas na configuração da instância

A automação de configuração de instâncias do AMS Accelerate faz as seguintes alterações em sua conta:

1. Permissões do IAM

   Adiciona as políticas gerenciadas pelo IAM necessárias para conceder permissão à instância para usar os agentes instalados pelo AMS Accelerate.
2. Agentes
   a. O Amazon CloudWatch Agent é responsável por emitir registros e métricas do sistema operacional. A automação da configuração da instância garante que o CloudWatch agente esteja instalado e executando a versão mínima do AMS Accelerate.
   b. O agente AWS Systems Manager SSM é responsável por executar comandos remotos na instância. A automação da configuração da instância garante que o agente SSM esteja executando a versão mínima do AMS Accelerate.
3. CloudWatch Configuração

a. Para garantir que as métricas e os registros necessários sejam emitidos, o AMS Accelerate personaliza a CloudWatch configuração. Para obter mais informações, consulte a seção CloudWatch detalhes da alteração de configuração a seguir.

A configuração automatizada da instância faz alterações ou acréscimos aos perfis e à CloudWatch configuração da instância do IAM.

Detalhes da alteração de permissões do IAM

Cada instância gerenciada deve ter uma AWS Identity and Access Management função que inclua as seguintes políticas gerenciadas:

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

As duas primeiras são políticas AWS gerenciadas. A política gerenciada pela AMS é:

AMSInstanceProfileBasePolicy

JSON

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

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

Se sua instância já tiver uma função do IAM anexada, mas não tiver nenhuma dessas políticas, o AMS adicionará as políticas ausentes à sua função do IAM. Se sua instância não tiver uma função do IAM, o AMS anexará a função do AMSOSConfigurationCustomerInstanceProfileIAM. A função AMSOSConfigurationCustomerInstanceProfiledo IAM tem todas as políticas exigidas pelo AMS Accelerate.

> **Note**
>
> Se o limite padrão do perfil de instância de 10 for atingido, o AMS aumentará o limite para 20, para que os perfis de instância necessários possam ser anexados.

CloudWatch detalhes da alteração de configuração

Detalhes adicionais sobre a CloudWatch configuração.

- CloudWatch localização do arquivo de configuração na instância:
  - Windows:%ProgramData%\ Amazon\AmazonCloudWatchAgent\ amazon-cloudwatch-agent .json
  - Linux:/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/ams-accelerate-config.json
- CloudWatch localização do arquivo de configuração no Amazon S3:
  - Windows: https://ams-configuration-artifacts- *REGION_NAME* .s3. *REGION_NAME*.amazonaws. com/configurations/cloudwatch/latest/windows-cloudwatch-config.json
  - Linux: https://ams-configuration-artifacts- *REGION_NAME* .s3. *REGION_NAME*.amazonaws. com/ configurations/cloudwatch/latest/linux-cloudwatch-config.json
- Métricas coletadas:
  - Windows:
    - AWS Systems Manager Agente SSM (CPU_Usage)
    - CloudWatch Agente (CPU_Usage)

    - Utilização do espaço em disco para todos os discos (% de espaço livre)
    - Memória (% de bytes comprometidos em uso)
  - Linux
    - AWS Systems Manager Agente SSM (CPU_Usage)
    - CloudWatch Agente (CPU_Usage)
    - CPU (cpu_usage_idle, cpu_usage_iowait, cpu_usage_user, cpu_usage_system)
    - Disco (percentual usado, inodes_usado, inodes_total)
    - Diskio (io_time, write_bytes, read_bytes, gravações, leituras)
    - Mem (mem_used_percent)
    - Troca (swap_used_percent)
- Registros coletados:
  - Windows:
    - SSMAgentRegistro da Amazon
    - AmazonCloudWatchAgentLog
    - SSMErrorRegistro 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

Fora do AMS Accelerate

O AMS Accelerate fornece uma maneira fácil de operar um ambiente operacional de classe empresarial. Além disso, o AMS Accelerate fornece o modelo de operações de infraestrutura de suporte para AWS migração e uso. No entanto, depois de usar o AMS Accelerate, você pode decidir terceirizar ou reatribuir responsabilidades de operações de AWS infraestrutura a outras equipes. Para fazer isso, você deve excluir suas contas do serviço AMS.

Quando você desassocia uma conta do AMS Accelerate, o AMS transfere todas as responsabilidades definidas em nossa descrição do serviço de volta para você. Por exemplo, você não poderá cortar incidentes ou solicitações de serviço para o AMS. Da mesma forma, nossos engenheiros de operações e automação não terão mais acesso às suas contas do Accelerate, impedindo que corrijamos as descobertas de integridade, disponibilidade e segurança e conformidade. Suas AWS cargas de trabalho podem continuar sendo executadas nas mesmas contas em que o AMS estava operando.

A equipe que executará seus serviços de operações de infraestrutura daqui para frente deve ser incluída para definir quais pessoas, ferramentas e processos você usará após a desativação do Accelerate. O AMS deixa algumas das ferramentas do AMS, como grades de proteção e registros, para permitir o desenvolvimento de um ambiente e modelo operacionais “futuros”. Leia atentamente a documentação a seguir para entender as ferramentas que você pode continuar usando e como solicitar a exclusão de uma conta.

Efeitos de desativação do AMS Accelerate

Ao se preparar para sair do Accelerate, tenha em mente as seguintes considerações.

- Acesso: a `ams-access-management` CloudFormation pilha que define a `ams-access-management` AWS Identity and Access Management função não é excluída. Após a desativação, esses recursos permanecem, mas não são usados por outros componentes que são deixados para trás. Você pode excluir a pilha e a função conforme sua conveniência.
- Retenção de recursos do AMS: após a desativação, alguns recursos do AMS permanecem na sua conta. Para ver quais recursos são retidos e o que você pode fazer com eles, consulte a `resource_inventory.zip`planilha (compactada).
- Automação: após a desativação, os runbooks de automação do AWS SSM e as funções do AWS Lambda, organizados pela AMS, não estão mais disponíveis.
- Gerenciamento de backup: o AMS usa o gerenciamento de backup para tirar fotos de seus recursos. Após a desativação, você pode continuar usando as programações de backup, a frequência e os períodos de retenção definidos em, AWS Backup exceto nos planos de backup do AMS; consulte. Selecione um plano de backup do AMS Os AWS Identity and Access Management recursos criados pelo AMS Backup Orchestrator são removidos, mas não os cofres de backup criados pelo AMS e a chave correspondente. AWS KMS O Accelerate não monitora mais as tarefas de backup nem executa ações de restauração durante incidentes.
- Otimização de custos: após a desativação, o AMS Resource Scheduler é excluído. O AMS Resource Scheduler ajuda você a reduzir os custos operacionais interrompendo os recursos que não estão em uso e reiniciando-os quando sua capacidade é necessária. O AMS não continua fornecendo recomendações de otimização de custos. Para obter detalhes sobre o Resource Scheduler, consulte Otimização de custos com o AMS Resource Scheduler.
- Especialistas designados: após a transferência, o Cloud Service Delivery Manager (CSDM) e o Cloud Architect (CA) designados não fornecem mais orientação, relatam ou promovem a excelência operacional e de segurança para suas contas externas do Accelerate.
- Gerenciamento de incidentes: o gerenciamento de incidentes é o processo que o serviço AMS usa para responder aos incidentes relatados. Após a desativação, o Accelerate não detecta e responde mais a incidentes nem auxilia sua equipe na resolução de problemas. Você não poderá trocar comunicações sobre incidentes e solicitações de serviço com o Accelerate and Accelerate. O acesso ao console de suas contas do Accelerate está desativado.
- Registro e relatórios: após a desativação, você retém os registros armazenados como resultado dos CloudWatch registros de CloudTrail fluxo da VPC. Você pode deixar a configuração desses serviços como está para continuar gerando registros; no entanto, o AMS não monitora mais essas configurações. O Accelerate não fornece mais o relatório mensal de serviços que resume as principais métricas de desempenho do AMS. Você retém os dados gerados pelo Self-Service Reporting (SSR) (consulteRelatórios de autoatendimento), mas o Accelerate não gera novos.

- Monitoramento: o monitoramento é o processo que o serviço AMS usa para rastrear seus recursos. Durante a desativação, o AMS remove ferramentas específicas do AMS, como o Alarm Manager e o Resource Tagger, e quaisquer regras de EventBridge eventos e CloudWatch alarmes que o AMS implantou como parte da linha de base de monitoramento do AMS. O Accelerate não responderá mais aos alarmes nem configurará novos alarmes após a desativação. Para obter detalhes sobre o Gerenciador de alarmes e o Marcador de recursos, consulte Gerenciador de alarmes baseado em tags e Marcador de recursos.
- Ferramentas operacionais: o AMS Accelerate pode fornecer operações contínuas para a infraestrutura da sua carga de trabalho na AWS. Depois de desativar uma conta do Accelerate, você não tem mais acesso a ferramentas como o Resource Tagger para ajudá-lo a marcar seus recursos com base em regras ou a configuração automatizada de instâncias para instalar os agentes necessários em suas EC2 instâncias. CloudWatch e os agentes SSM nas instâncias permanecem no local com as configurações existentes. O perfil `AMSOSConfigurationCustomerInstanceRole` do IAM e o `AMSInstanceProfileBasePolicy` são separados de suas instâncias e removidos de suas contas do Accelerate.
- Gerenciamento de patches: o gerenciamento de patches é o processo que o serviço AMS usa para atualizar suas EC2 instâncias. Após a desativação, 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. 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 pelo Accelerate.
- Gerenciamento de problemas: após a desativação, o Accelerate não realiza mais análises para identificar e investigar problemas e identificar a causa raiz.
- Segurança: o gerenciamento de segurança é o processo que o serviço AMS usa para proteger seus recursos. Após a desativação, você mantém o GuardDuty detector e as descobertas da Amazon e todas AWS Config as regras que você criou. AWS Config as regras implantadas pelo Accelerate são removidas. O Accelerate não monitora, corrige ou relata mais as descobertas dessas ferramentas.
- 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.

Desativação do AMS Accelerate com dependências do Alarm Manager e do Resource Tagger

As CloudFormation pilhas personalizadas que implantam configurações relacionadas ao Alarm Manager ou ao Resource Tagger, junto com as pilhas de configuração do Alarm Manager e do Resource Tagger fornecidas pela AMS, permanecem na sua conta quando você sai do AWS Managed Services.

Para excluir as pilhas de configuração do AMS durante o processo de desativação, você deve remover todas as dependências e referências no Alarm Manager ou no Resource Tagger dos CloudFormation modelos personalizados antes de iniciar o processo de desativação. A remoção das referências ajuda a garantir que as pilhas sejam removidas adequadamente da sua conta quando você sai do AMS.

> **Important**
>
> Analise cuidadosamente seus CloudFormation modelos e remova todas as referências ao Alarm Manager e ao Resource Tagger antes de iniciar o processo de desativação. Não fazer isso pode resultar na retenção dessas pilhas em sua conta, mesmo depois de você sair do AMS. Observe que, embora essas pilhas contenham informações de configuração específicas do Alarm Manager e do Resource Tagger, sua presença não gera cobranças ou taxas contínuas.

Obter assistência de desembarque para uma conta Accelerate

O AMS desativa sua conta após receber um aviso prévio de pelo menos 30 dias por meio de uma Solicitação de Encerramento do Serviço de Conta do AMS. A Data de Rescisão do Serviço é o último dia do mês civil após o final do período de aviso de rescisão obrigatório de 30 dias; desde que, se o final do período de notificação de rescisão exigido cair após o 20º dia do mês civil, a Data de Rescisão do Serviço será o último dia do mês civil seguinte.

Para solicitar a desativação de uma conta, você deve:

1. Envie uma solicitação formal para desativar a conta usando uma solicitação de serviço. Uma solicitação de serviço (SR) documentando todas as contas que você deseja excluir ou uma SR por conta.

   Na solicitação, forneça a lista de contas IDs a serem excluídas, o motivo da exclusão e quaisquer considerações adicionais.
2. Informe seu CSDM sobre as contas que você deseja excluir e solicite sua ajuda para executar o processo de desativação.

Configurações de notificação no Accelerate

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

- Eventos criados por alertas de monitoramento
- Notificações do serviço de patches, se você tiver optado pelo complemento Patch
- Solicitações de serviço e relatórios de incidentes
- AWS Anúncios importantes ocasionais (seu CSDM entra em contato com você se alguma ação de sua parte for necessária)

Todas as notificações são enviadas usando um e-mail que você forneceu para notificações de patch quando estava integrado. Caso contrário, as notificações serão enviadas para o e-mail padrão 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.

Você pode usar listas nomeadas de contatos para notificações não baseadas em recursos, como alertas baseados em GuardDuty ou AWS Config. Por exemplo, você pode ter uma lista nomeada `SecurityContacts` e outra nomeada`0perationsContacts`. O AMS envia alarmes e notificações para essas listas.

Consulte AWS Config Relatório de conformidade de controle para obter mais detalhes.

Marcação no AMS Accelerate

A maioria dos recursos do Accelerate (aplicação de patches, backup, monitoramento) usa tags e perfis de configuração para decidir quais recursos gerenciar, quais ações aplicar e quando aplicá-las. As tags são rótulos que você aplica aos recursos. Os perfis de configuração contêm regras com base nessas tags.

Cada recurso do Accelerate tem seus próprios requisitos de marcação. Alguns recursos exigem que você use tags específicas, enquanto outros permitem que você use qualquer uma das suas próprias.

Para obter informações sobre as tags necessárias, consulteTags gerenciadas pelo cliente no Accelerate.

Para obter informações sobre tags que podem ser definidas como clientes, consulte Tags fornecidas pelo cliente no Accelerate

Sumário

- Etiquetas no AMS Accelerate
  - O que são tags?
  - Como funcionam as tags
  - Tags gerenciadas pelo cliente no Accelerate
    - Monitoramento em Accelerate
    - Configurando tags para EC2 instâncias no Accelerate
    - Gerenciando tags para backups no Accelerate
  - Acelere as tags gerenciadas
  - Tags fornecidas pelo cliente no Accelerate
- Ferramentas de gerenciamento de tags para Accelerate
  - Acelere o marcador de recursos
    - O que é o Resource Tagger?
    - Como funciona o Resource Tagger
    - Perfis de configuração do marcador de recursos no AMS Accelerate
      - Sintaxe e estrutura
    - Casos de uso do Resource Tagger no AMS Accelerate
      - Visualizando as tags aplicadas pelo Resource Tagger

        - Usando o Resource Tagger para criar tags
        - Impedindo que o Resource Tagger modifique recursos
        - Exemplo de perfil de configuração
        - Mesclando a configuração padrão
        - Desabilitando a configuração padrão
        - Removendo tags aplicadas pelo Resource Tagger
        - Visualizando ou fazendo alterações na configuração do Resource Tagger
        - Implantando alterações de configuração
        - Configurando o Terraform para ignorar as tags do Resource Tagger
        - Visualizando o número de recursos gerenciados pelo Resource Tagger
    - Usando CloudFormation para criar tags para o AMS Accelerate
        - CloudFormation Casos de uso do AMS Accelerate
            - Marcar uma EC2 instância com CloudFormation for Accelerate
            - Marcando um AutoScaling grupo (ASG) com CloudFormation o for Accelerate
            - Implantando um perfil de configuração com o CloudFormation for Accelerate
    - Usando o Terraform para criar tags para o AMS Accelerate

Etiquetas no AMS Accelerate

Sumário

- O que são tags?
- Como funcionam as tags
- Tags gerenciadas pelo cliente no Accelerate
    - Monitoramento em Accelerate
    - Configurando tags para EC2 instâncias no Accelerate
    - Gerenciando tags para backups no Accelerate
- Acelere as tags gerenciadas
- Tags fornecidas pelo cliente no Accelerate

O que são tags?

Uma tag é um rótulo que você atribui a um AWS recurso. Cada tag consiste em uma chave e um valor opcional, ambos definidos por você.

Você usa tags para categorizar seus AWS recursos de maneiras diferentes, por exemplo, por finalidade, proprietário ou ambiente. Por exemplo, você pode definir um conjunto de tags para as EC2 instâncias da Amazon da sua conta, o que ajuda a rastrear o proprietário e o nível de pilha de cada instância.

As tags não têm nenhum significado semântico para a Amazon EC2 e são interpretadas estritamente como uma sequência de caracteres.

Para saber mais, consulte AWS Recursos de marcação.

Como funcionam as tags

Há várias maneiras de aplicar tags aos seus recursos. Você pode marcar recursos diretamente no console de cada AWS serviço ao criar o recurso; usar o Editor de AWS tags para adicionar, remover ou editar tags de vários recursos; ou usar ferramentas de provisionamento, como a tag CloudFormation Resource. O AMS Accelerate também fornece o AMS Accelerate Resource Tagger que você usa para definir regras para um gerenciador automatizado do ciclo de vida de tags. Para obter informações sobre o uso do Resource Tagger no AMS Accelerate, consulteAcelere o marcador de recursos. O AMS Accelerate também fornece tags fornecidas pelo cliente para adicionar e remover tags personalizadas aos seus recursos do AMS. Para obter mais informações sobre as tags fornecidas pelo cliente, consulte. Tags fornecidas pelo cliente no Accelerate

Tags gerenciadas pelo cliente no Accelerate

Certas tags são necessárias para acionar várias ações do AMS Accelerate.

Sumário

- Monitoramento em Accelerate
- Configurando tags para EC2 instâncias no Accelerate
- Gerenciando tags para backups no Accelerate

Monitoramento em Accelerate

O AMS Accelerate monitora os recursos suportados quanto à integridade, disponibilidade e confiabilidade. Para obter mais informações sobre essa oferta de serviço, consulteMonitoramento e gerenciamento de eventos no AMS Accelerate.

O AMS Accelerate integra periodicamente, Serviços da AWS além do monitoramento básico. Se você usar a configuração padrão do Resource Tagger, essas atualizações serão implantadas automaticamente em suas contas e as alterações serão refletidas nos recursos suportados.

Para optar por ter suas EC2 instâncias da Amazon gerenciadas pelo AMS Accelerate, você deve aplicar a seguinte tag por meio do perfil de personalização em AppConfig; para obter mais informações, consulte Etapa 3: Criar uma configuração e um perfil de configuração.

Aplique a seguinte tag aos seus recursos:

Chave	Valor
ams:rt:ams-managed	true

Por exemplo, você pode criar um documento de configuração personalizado como este para aplicar as tags a todos os recursos compatíveis com o AMS EC2 :

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

> **Important**
>
> Lembre-se de implantar suas alterações de configuração depois de fazê-las. No SSM AppConfig, você deve implantar uma nova versão da configuração depois de criá-la.

Outros serviços além da Amazon EC2 terão monitoramento de linha de base padrão. Para optar por não permitir que seus recursos sejam monitorados pelo AMS Accelerate, você pode usar o perfil de configuração de personalização para excluir recursos específicos ou Serviços da AWS. Isso permite que você controle quais recursos devem ter tags de monitoramento para implantar definições básicas de alarme. Consulte Casos de uso do Resource Tagger no AMS Accelerate.

Usando o Resource Tagger

A configuração do AMS Accelerate Resource Tagger em sua conta ajuda a garantir que as seguintes tags sejam implantadas automaticamente, se você aplicar essa tag (ams:rt:ams-managed).

Você verá as seguintes tags sendo aplicadas aos seus recursos suportados para monitoramento básico.

Chave	Valor	Regra
ams: rt: ams-monitoring-policy	sou monitorado	Aplica-se a todos os EC2 recursos suportados pelo AMS
ams: rt: ams-monitoring-policy-platform	ams-monitored-linux	Aplica-se a todas as EC2 instâncias da Amazon que executam o sistema operacional Linux
ams: rt: ams-monitoring-policy-platform	ams-monitored-windows	Aplica-se a todas as EC2 instâncias da Amazon que executam o sistema operacional Windows

Para outros serviços compatíveis

Aplique as seguintes tags aos seus recursos, de acordo com as regras fornecidas:

Chave	Valor	Regra
ams: rt: ams-monitoring-policy	sou monitorado	Aplica-se a todos os recursos suportados pelo monitoram ento do AMS Accelerate.
ams: rt: ams-monitoring-with-kms	ams-monitored-with-kms	OpenSearch Domínio com KMS
ams: rt: ams-monitoring-with-master	ams-monitored-with-master	OpenSearch Domínio com nó principal dedicado

Se você não estiver usando o Resource Tagger

Consulte Acelere as tags sem o Resource Tagger para obter ajuda sobre como aplicar as tags de monitoramento corretas usando métodos diferentes do AMS Resource Tagger.

Configurando tags para EC2 instâncias no Accelerate

O AMS Accelerate gerencia agentes em suas EC2 instâncias da Amazon, como o agente SSM e o CloudWatch agente. Para obter mais informações sobre essa oferta de serviço, consulte Configuração automatizada de instâncias no AMS Accelerate

Para optar por ter suas EC2 instâncias da Amazon gerenciadas pelo AMS Accelerate, você deve aplicar a seguinte tag às suas EC2 instâncias da Amazon:

Chave	Valor
ams:rt:ams-managed	true

Gerenciando tags para backups no Accelerate

O AMS Accelerate gerencia o backup dos recursos suportados. Para obter mais informações sobre essa oferta de serviço, consulteGerenciamento de continuidade no AMS Accelerate.

O gerenciamento de backup do AMS Accelerate usa tags para identificar quais recursos devem ser copiados automaticamente (e também fornece recursos de backup manual). Você pode usar

qualquer combinação de tag chave-valor para associar seus recursos aos planos de backup. Para optar por fazer backups automatizados usando o ams-default-backup-plan AWS Backup plano, você deve aplicar a seguinte tag aos recursos suportados:

Chave	Valor
ams:rt:backup-orchestrator	true

> **Note**
>
> Durante a integração, o AMS Accelerate marca todos os recursos com ams:rt: backup-orchestrator-onboarding com valor verdadeiro para instantâneos de curto intervalo e retenção curta. Isso é gerenciado pelo plano ams-onboarding-backup-plande backup. Para obter mais informações sobre os AWS Backup planos gerenciados pelo AMS Accelerate, consulte. Selecione um plano de backup do AMS

Acelere as tags gerenciadas

Durante a integração com o AMS Accelerate, vários AWS recursos são implantados em sua conta. Para que você possa identificá-los, esses recursos são marcados com o seguinte:

Chave	Valor
AMS: proprietário do recurso	AMS
Braços: resourceOwnerService	Uma descrição de qual serviço do AMS Accelerate oferece esse recurso vem, por exemplo, do AMS Deployment, Backup, Controls, Monitoring, Patch e assim por diante.
AppId	AMSInfrastructure
AppName	
Ambiente	

> **Note**
>
> Essas tags são aplicadas usando tags de CloudFormation nível de pilha e dependem da CloudFormation propagação das tags para os recursos criados. Para obter mais informações, consulte Etiqueta de recurso.

Tags fornecidas pelo cliente no Accelerate

O que são tags fornecidas pelo cliente?

As tags fornecidas pelo cliente são um recurso do serviço AMS Accelerate usado para especificar regras que regem como os recursos do AMS são marcados em sua conta. Com as tags fornecidas pelo cliente, você pode adicionar tags personalizadas definidas pelo usuário aos recursos do AMS implantados em suas contas. O recurso de tags fornecido pelo cliente é adicionado automaticamente às contas solicitadas quando você solicita ao Cloud Service Delivery Manager (CSDM) usando um serviço automatizado. Observe que você não pode substituir as tags do AMS. As tags AMS começam com 'ams: '.

Você pode definir suas próprias tags (rótulos) e especificar as funcionalidades dessas tags para todos os seus recursos do AMS Accelerate. Você pode fornecer essas tags antes de embarcar no AMS para que as tags AMS e suas tags personalizadas sejam aplicadas durante o processo de integração. Ou você pode fornecer etiquetas após a integração.

Como posso adicionar tags fornecidas pelo cliente?

Para solicitar a adição dessas tags aos seus recursos, entre em contato com seu CSDM. Essas tags serão aplicadas aos recursos do AMS em sua conta.

Qual é o escopo das tags?

Atualmente, esse recurso está disponível apenas para clientes do Accelerate e em regiões AWS comerciais. Você pode adicionar tags a todas as contas que você possui ou a uma lista específica de contas.

> **Note**
>
> Essas tags se aplicam somente aos recursos do AMS e não afetam seus próprios recursos.

Ferramentas de gerenciamento de tags para Accelerate

Índice

- Acelere o marcador de recursos
- Usando CloudFormation para criar tags para o AMS Accelerate
- Usando o Terraform para criar tags para o AMS Accelerate

Acelere o marcador de recursos

Com o Resource Tagger, você pode especificar regras para controlar como AWS os recursos são marcados em sua conta. Ao integrar uma conta, o AMS Accelerate implanta sua política de marcação para garantir que os recursos em suas contas gerenciadas sejam marcados.

Sumário

- O que é o Resource Tagger?
- Como funciona o Resource Tagger
- Perfis de configuração do marcador de recursos no AMS Accelerate
  - Sintaxe e estrutura
- Casos de uso do Resource Tagger no AMS Accelerate
  - Visualizando as tags aplicadas pelo Resource Tagger
  - Usando o Resource Tagger para criar tags
  - Impedindo que o Resource Tagger modifique recursos
  - Exemplo de perfil de configuração
  - Mesclando a configuração padrão
  - Desabilitando a configuração padrão
  - Removendo tags aplicadas pelo Resource Tagger
  - Visualizando ou fazendo alterações na configuração do Resource Tagger
  - Implantando alterações de configuração
  - Configurando o Terraform para ignorar as tags do Resource Tagger
  - Visualizando o número de recursos gerenciados pelo Resource Tagger

O que é o Resource Tagger?

O Resource Tagger é uma oferta de serviço do AMS Accelerate que você usa para especificar regras para controlar como AWS os recursos são marcados em sua conta. O objetivo é fornecer visibilidade completa de como suas tags são aplicadas aos seus AWS recursos.

O Resource Tagger cria, atualiza e exclui automaticamente tags em AWS recursos compatíveis, com base nas regras de marcação que você especifica em seus perfis de configuração. Por exemplo, você pode especificar uma regra que aplique uma tag a uma coleção de EC2 instâncias da Amazon, indicando que elas devem ser gerenciadas pelo AMS Accelerate, o que resulta no monitoramento ou no backup das instâncias. Você pode usar tags como essa para identificar o status de conformidade dos AWS recursos com base na política definida em seus perfis AWS AppConfig de configuração. Para obter mais informações, consulte AWS AppConfig.

O AMS Accelerate fornece uma configuração padrão de marcação gerenciada para que você possa ter seus recursos monitorados pelo AMS Accelerate. Você define quais recursos devem ser gerenciados pelo AMS Accelerate, e as regras de marcação gerenciada garantem que os recursos com as tags apropriadas sejam monitorados pelo AMS Accelerate.

Com o Resource Tagger, se você escolher, você pode substituir ou desativar as tags gerenciadas padrão do AMS Accelerate, fornecer suas próprias regras de marcação para atender às suas políticas e usar outros mecanismos, como o Terraform, para evitar desvios. Você pode definir as exceções para escalar, com base em suas operações. Por exemplo, você pode definir uma política para aplicar tags a todas as EC2 instâncias da Amazon com plataformas compatíveis (como Windows e Linux) e excluir da marcação de uma instância IDs específica.

> **Important**
>
> O Resource Tagger controla todas as tags em sua conta que têm o prefixo ams:rt:. Todas as tags que começam com esse prefixo são excluídas, a menos que estejam presentes nas regras de configuração do Resource Tagger. Resumindo, qualquer tag nos recursos suportados que comece com ams:rt: é considerada propriedade do Resource Tagger. Se você marcar manualmente algo com, por exemplo, ams:rt:, essa tag será removida automaticamente se não tiver sido especificada em um dos perfis de configuração do Resource Tagger.

Como funciona o Resource Tagger

Quando sua conta é integrada ao AMS Accelerate, dois documentos de configuração JSON são implantados em sua conta em. AWS AppConfig Os dois documentos, chamados de perfis de configuração, são AMSManagedTags, chamados de perfil de configuração padrão e CustomerManagedTags, chamados de perfil de configuração de personalização. Você usa o perfil de configuração de personalização para definir suas próprias políticas e regras para suas contas, e elas não são substituídas pelo AMS Accelerate.

Ambos os perfis residem no aplicativo AMSResourceTagger e no AMSInfrastructureambiente. Todas as tags aplicadas pelo marcador de recursos têm o prefixo de chave ams:rt:.

Perfil de configuração de personalização:

O perfil de configuração de personalização está inicialmente vazio no momento da integração da conta; no entanto, todas as regras colocadas no documento do perfil são aplicadas, além das regras no perfil de configuração padrão. Qualquer configuração no perfil de configuração de personalização é totalmente gerenciada por você e não é substituída pelo AMS Accelerate, exceto por sua solicitação.

Você pode especificar quaisquer regras de marcação personalizadas que desejar no perfil de configuração personalizado dos AWS recursos suportados e também pode especificar modificações na configuração padrão gerenciada pelo AMS Accelerate aqui, consulte. Casos de uso do Resource Tagger no AMS Accelerate

> **Important**
>
> Se você atualizar esse perfil, o Resource Tagger aplica automaticamente as alterações em todos os recursos relevantes do seu. Conta da AWS As alterações são promulgadas automaticamente, mas podem levar até 60 minutos para entrarem em vigor.

Você pode atualizar esse perfil usando as Console de gerenciamento da AWS ferramentas AWS CLI/SDK ou por meio delas. Para obter informações sobre como atualizar um perfil de configuração de personalização, consulte o guia AWS AppConfig do usuário: O que é AWS AppConfig?

Perfil de configuração padrão:

O documento de perfil de configuração padrão é interno ao AMS Accelerate e contém regras padrão fornecidas pelo AMS Accelerate que você não pode modificar ou excluir permanentemente.

Esse perfil pode ser atualizado a qualquer momento pelo AMS Accelerate e disponibilizado para análise; todas as alterações feitas nele são excluídas automaticamente. Se você quiser modificar ou desativar qualquer uma das regras de configuração padrão, use o perfil de configuração de personalização, consulteCasos de uso do Resource Tagger no AMS Accelerate.

Perfis de configuração do marcador de recursos no AMS Accelerate

Os perfis de configuração ajudam a garantir que as tags sejam aplicadas uniformemente aos recursos durante toda a vida útil dos recursos.

Sintaxe e estrutura

Um perfil de configuração é um objeto JSON com a seguinte estrutura:

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

Opções: (opcional) Especifique as opções de como você gostaria que o se ResourceTagger comportasse. Omitir o bloco equivale a definir todas as opções com seus valores padrão. Veja abaixo as configurações de opções disponíveis:

- ReadOnly: (opcional, o padrão é false): especifica o ReadOnly modo para o Resource Tagger. ReadOnly Defina como true para desativar a criação ou remoção de tags do Resource Tagger nos recursos da AWS. Para obter mais informações, consulte Impedindo que o Resource Tagger modifique recursos.

ResourceType: essa chave deve ser uma das seguintes cadeias de caracteres suportadas e representa todas as configurações relacionadas ao tipo de recurso indicado:

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

ConfigurationId: essa chave deve ser exclusiva no documento de perfil e nomear de forma exclusiva o seguinte bloco de configuração. Se dois blocos de configuração no mesmo ResourceTypebloco tiverem o mesmo ID de configuração, o que aparecer por último no perfil entrará em vigor. Se você especificar um ConfigurationID em seu perfil de personalização que seja igual ao especificado no documento padrão, o bloco de configuração definido no perfil de personalização entrará em vigor.

> **Important**
>
> O ConfigurationID deve ***not***se sobrepor ao perfil do AMS Accelerate; por exemplo, não deve ser AMSMonitoringLinux ou AMSMonitoringWindows, caso contrário, desabilita a respectiva configuração do perfil de configuração de Tags. AMSManaged

Ativado (opcional, o padrão é verdadeiro): especifica se o bloco de configuração entra em vigor. Defina isso como false para desativar um bloco de configuração. Um bloco de configuração desativado não tem efeito.

Filtro: especifica os recursos aos quais a configuração se aplica. Cada objeto de filtro pode ter qualquer um (mas somente um) dos seguintes campos:

- AWS::AutoScaling::AutoScalingGrupo:
  - AutoScalingGroupName: O nome do grupo de escalonamento automático. Esse campo oferece suporte à correspondência de caracteres curinga.
- AWS::DynamoDB::Table:
  - TableName: o nome da tabela do DynamoDB. Esse campo oferece suporte à correspondência de caracteres curinga.
- AWS::EC2::Instance:
  - AvailabilityZone: o filtro corresponde a uma EC2 instância na zona de disponibilidade especificada. Esse campo suporta a correspondência de caracteres curinga, então *a corresponde a us-east-1a, ap-northeast-1a e assim por diante.
  - InstanceId: o filtro corresponde a uma EC2 instância com o ID de instância especificado. Esse campo é compatível com a correspondência de caracteres curinga, portanto, i-00000* corresponderia a qualquer instância que tenha um ID de instância começando com i-00000.
  - Plataforma: o filtro combina uma EC2 instância com a plataforma especificada. Os valores válidos são windows, linux ou o caractere curinga * (para corresponder a qualquer plataforma).
- AWS::EC2::NatGateway:
  - NatGatewayId: O ID do NAT Gateway. Esse campo oferece suporte à correspondência de caracteres curinga.
  - Estado: o estado do gateway NAT (pendente | falhou | disponível | excluindo | excluído ou caractere curinga “*”)
  - VpcId: o ID da VPC na qual o NAT Gateway reside. Esse campo oferece suporte à correspondência de caracteres curinga.
  - SubnetId: o ID da sub-rede na qual o NAT Gateway reside. Esse campo oferece suporte à correspondência de caracteres curinga
- AWS:EC2:: VPNConnection:
  - VpnConnectionId: o ID da conexão. Esse campo oferece suporte à correspondência de caracteres curinga.

- AWS::EFS::FileSystem:
  - FileSystemId: A ID do sistema de arquivos EFS. Esse campo oferece suporte à correspondência de caracteres curinga.
- AWS::EKS::Cluster:
  - ClusterName: o nome do cluster. Esse campo oferece suporte à correspondência de caracteres curinga.
- AWS::ElasticLoadBalancing::LoadBalancer (Classic Load Balancer):
  - LoadBalancerName: O LoadBalancer nome. Esse campo oferece suporte à correspondência de caracteres curinga.
  - Esquema: pode ser “voltado para a Internet”, “interno” ou curinga “*”.
  - VPCId: o local VPCId em que o balanceador de carga é implantado pode ser o caractere curinga “*”.
- AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer (ALB)):
  - LoadBalancerArn: O nome do recurso LoadBalancer da Amazon (ARN).
  - DNSName: O DNSName do LoadBalancer. Esse campo oferece suporte à correspondência de caracteres curinga.
  - LoadBalancerName: O LoadBalancer nome. Esse campo oferece suporte à correspondência de caracteres curinga.
- AWS::Elasticsearch::Domain:
  - DomainId: O DomainId do ElasticSearch recurso. Esse campo oferece suporte à correspondência de caracteres curinga.
  - DomainName: O DomainName do ElasticSearch recurso. Esse campo oferece suporte à correspondência de caracteres curinga.
  - HasMasterNode: valor booleano de verdadeiro ou falso. Corresponde se o domínio tiver um nó principal dedicado.
  - HasKmsKeyValor booleano de verdadeiro ou falso. Corresponde se o domínio tem uma chave KMS para criptografia em repouso.
- AWS::FSx::FileSystem:
  - FileSystemId: O ID do sistema de FSx arquivos. Esse campo oferece suporte à correspondência de caracteres curinga.
- AWS::OpenSearch::Domain:

  - DomainId: O DomainId do OpenSearch recurso. Esse campo oferece suporte à correspondência de caracteres curinga.
  - DomainName: O DomainName do OpenSearch recurso. Esse campo oferece suporte à correspondência de caracteres curinga.
  - HasMasterNode: Boolean; Se o domínio tiver um nó principal dedicado, isso poderá ser definido como verdadeiro.
  - HasKmsKey: se o domínio tiver uma chave KMS para criptografia em repouso, ela poderá ser definida como verdadeira.
- AWS: :RDS::: DBCluster
  - DBClusterIdentificador: o filtro combina um identificador de cluster RDS com o identificador especificado. Esse campo não oferece suporte à correspondência de caracteres curinga, portanto, um identificador de cluster deve ser especificado.
  - Mecanismo: O mecanismo em uso pela instância do RDS. Esse campo oferece suporte à correspondência de caracteres curinga.
  - EngineVersion: A versão do motor. Esse campo oferece suporte à correspondência de caracteres curinga.
- AWS: :RDS::: DBInstance
  - DBInstanceIdentificador: o filtro combina uma instância do RDS com o ID de instância especificado. Esse campo não oferece suporte à correspondência de caracteres curinga, portanto, um identificador de instância deve ser especificado.
  - Mecanismo: O mecanismo em uso pela instância do RDS. Esse campo oferece suporte à correspondência de caracteres curinga.
  - EngineVersion: A versão do motor. Esse campo oferece suporte à correspondência de caracteres curinga.
- AWS::Redshift::Cluster:
  - ClusterIdentifier: O identificador do cluster. Esse campo oferece suporte à correspondência de caracteres curinga.
- AWS::S3::Bucket:
  - BucketName: O nome do bucket do S3. Esse campo oferece suporte à correspondência de caracteres curinga.
- AWS::Synthetics::Canary:
  - CanaryName: O nome do canário Synthetics.

Outras propriedades do filtro:

- Tag: O filtro se aplica a qualquer recurso que já tenha a tag especificada aplicada. O valor dessa propriedade deve ser um objeto JSON com os seguintes campos:
  - Chave: deve ser uma string exata e especifica que os recursos devem ter uma tag com essa chave exata.
  - Valor: especifica o valor correspondente para a tag. Suporta curingas, portanto, um valor de Sample corresponde a qualquer valor que termine com a string Sample.
- Fn: :AND: Uma matriz JSON de objetos JSON. Cada objeto segue as mesmas regras do bloco de configuração do Filtro. Isso especifica que o filtro corresponda a qualquer recurso que corresponda a todos os subfiltros.
- Fn: :OR: Uma matriz JSON de objetos JSON. Cada objeto segue as mesmas regras do bloco de configuração do Filtro. Isso especifica que o filtro corresponda a qualquer recurso que corresponda a qualquer um dos subfiltros.
- Fn: :NOT: Um objeto JSON que segue as mesmas regras do bloco de configuração Filter. Isso especifica que o filtro não corresponda explicitamente a nenhum recurso que corresponda ao subfiltro. Use isso para especificar exclusões às suas regras de marcação.

Tags: as tags a serem aplicadas aos recursos correspondentes. (Consulte Convenções de nomenclatura e uso de tags.) Esse campo é uma matriz de pares de valores-chave:

- Chave: A chave da tag a ser aplicada.
- Valor: o valor da tag a ser aplicada.

> **Note**
>
> As tags aplicadas pelo Resource Tagger sempre têm chaves que começam com ams:rt:. Se você não especificar esse prefixo em seu perfil, o Resource Tagger o insere para você. É assim que o Resource Tagger distingue as tags que possui e gerencia das tags usadas por outras ferramentas para outros fins.

Casos de uso do Resource Tagger no AMS Accelerate

Esta seção lista as ações comumente executadas com o Resource Tagger.

Visualizando as tags aplicadas pelo Resource Tagger

Todas as tags aplicadas pelo Resource Tagger têm o prefixo de chave ams:rt:. Por exemplo, a definição de tag a seguir resulta em uma tag com a chave ams:rt:sampleKey e o valor sampleValue. Todas as tags com esse prefixo são tratadas como parte do Resource Tagger.

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

> **Important**
>
> Se você criar manualmente sua própria tag com o prefixo ams:rt:, ela será considerada gerenciada pelo Resource Tagger. Isso significa que, se o recurso for gerenciado pelo Resource Tagger, mas os perfis de configuração não indicarem que a tag deve ser aplicada, o Resource Tagger removerá sua tag adicionada manualmente. Se você marcar manualmente os recursos gerenciados pelo Resource Tagger, não use o prefixo ams:rt: para as chaves de tag.

Usando o Resource Tagger para criar tags

O AMS Accelerate Resource Tagger é um componente implantado em sua conta durante a integração do AMS Accelerate. O Resource Tagger tem um conjunto configurável de regras que definem como seus recursos devem ser marcados e, em seguida, aplica essas regras, adicionando e removendo automaticamente tags nos recursos para garantir que estejam em conformidade com suas regras.

Se você quiser usar o Resource Tagger para marcar seus recursos, consulteAcelere o marcador de recursos.

Veja a seguir um exemplo de trecho de configuração do Resource Tagger que adiciona a tag ams:rt:ams-managed com o valor true para todas as instâncias da Amazon. EC2 A tag ams:rt:ams-managed permite que você tenha seus recursos monitorados pelo AMS Accelerate.

```
{
    "AWS::EC2::Instance": {
        "SampleConfigurationBlock": {
            "Enabled": true,
```

```
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> Tenha cuidado ao especificar o nome da sua nova configuração (`SampleConfigurationBlock`no exemplo fornecido), pois você pode inadvertidamente substituir a configuração gerenciada pelo AMS com o mesmo nome.

Impedindo que o Resource Tagger modifique recursos

O Resource Tagger pode ser configurado para um modo somente leitura que impede que ele adicione ou remova quaisquer tags em seus recursos. Isso é útil se você quiser fornecer seu próprio mecanismo de marcação.

No modo somente leitura, o Resource Tagger ainda examina as regras de marcação que estão sendo especificadas nos perfis gerenciado e de configuração do cliente e verifica os recursos que não atendem a essas regras de marcação. Todos os recursos não compatíveis são apresentados. AWS Config O Regras do AWS Config que você pode procurar tem o `AMSResourceTagger-` prefixo. Por exemplo, a `AMSResourceTagger-EC2Instance` AWS Config regra avalia se as tags apropriadas são criadas para `AWS::EC2::Instance` os recursos com base no perfil de configuração.

O Resource Tagger para nesse momento e não faz nenhuma alteração em seus recursos (não adiciona nem remove tags).

Você pode ativar o modo somente leitura modificando o perfil de configuração do cliente para incluir a ReadOnlychave no bloco Opções. Por exemplo, o trecho de perfil de configuração a seguir mostra como isso pode parecer:

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

O Resource Tagger reagiria a essa nova configuração assim que terminasse a implantação e pararia de adicionar e remover tags nos recursos.

> **Note**
>
> Para reativar a modificação da tag, altere o ReadOnlyvalor para false ou remova completamente a chave, pois o valor padrão é false.

Para obter mais informações sobre a configuração de OpçõesSintaxe e estrutura, consulte a seguir.

Exemplo de perfil de configuração

O exemplo de documento de perfil a seguir especifica que todas as EC2 instâncias do Windows que fazem parte de uma CloudFormation pilha stack-* sejam gerenciadas pelo AMS Accelerate; no entanto, exclui explicitamente uma instância específica com ID i-00000000000000001. EC2

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "Windows"
                    },
                    {
                        "Tag": {
                            "Key": "aws:cloudformation:stack-name",
                            "Value": "stack-*"
                        }
                    },
                    {
```

```
                        "Fn::NOT": {
                            "InstanceId": "i-00000000000000001"
                        }
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> Tenha cuidado ao especificar o nome da sua nova configuração (`SampleConfigurationBlock`no exemplo fornecido), pois você pode inadvertidamente substituir a configuração gerenciada pelo AMS com o mesmo nome.

Mesclando a configuração padrão

O perfil de configuração padrão é fornecido pelo AMS Accelerate no momento da integração da conta. Esse perfil fornece regras padrão que são implantadas em sua conta.

Embora você não possa modificar o perfil de configuração padrão, você pode substituir os padrões especificando um bloco de configuração em seu perfil de configuração de personalização com o mesmo configurationId do bloco de configuração padrão. Se você fizer isso, seu bloco de configuração substituirá o bloco de configuração padrão.

Por exemplo, considere o seguinte documento de configuração padrão:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
```

```
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

Para alterar o valor da tag aplicada aqui de `SampleValueA` para `SampleValueB` e fazer com que a tag seja aplicada a todas as instâncias, não apenas às instâncias do Windows, você forneceria o seguinte perfil de configuração de personalização:

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

> **Important**
>
> Lembre-se de implantar suas alterações de configuração depois de fazê-las. Para obter mais informações, consulte Implantando alterações de configuração. No SSM AppConfig, você deve implantar uma nova versão da configuração depois de criá-la.

Desabilitando a configuração padrão

Você pode desativar uma regra de configuração padrão adicionando um bloco de configuração com o mesmo configurationId ao seu perfil de configuração de personalização e atribuindo ao campo Enabled o valor false.

Por exemplo, se a seguinte configuração estiver presente no perfil de configuração padrão:

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

Você pode desativar essa regra de marcação incluindo o seguinte em seu perfil de configuração de personalização:

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

> **Important**
>
> Lembre-se de implantar suas alterações de configuração depois de fazê-las; para obter informações, consulteImplantando alterações de configuração. No SSM AppConfig, você deve implantar uma nova versão da configuração depois de criá-la.

Removendo tags aplicadas pelo Resource Tagger

Todas as tags prefixadas com ams:rt são removidas pelo Resource Tagger se as tags não existirem nos perfis de configuração ou, se existirem, se o filtro não corresponder. Isso significa que você pode remover as tags aplicadas pelo Resource Tagger seguindo um destes procedimentos:

- Modificando a seção de configuração de personalização que define a tag.

- Adicionar uma exceção para os recursos específicos para que eles não correspondam mais ao filtro.

Por exemplo: se uma instância do Linux tiver as seguintes tags:

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

E você implanta o seguinte perfil de configuração do Resource Tagger:

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

O Resource Tagger reage às novas alterações de configuração, e a única tag na instância se torna:

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

> **Warning**
>
> Tenha cuidado ao especificar o nome da sua nova configuração (`SampleConfigurationBlock`no exemplo fornecido), pois você pode inadvertidamente substituir a configuração gerenciada pelo AMS com o mesmo nome.

> **Important**
>
> Lembre-se de implantar suas alterações de configuração depois de fazê-las; para obter informações, consulteImplantando alterações de configuração. No SSM AppConfig, você deve implantar uma nova versão da configuração depois de criá-la.

Visualizando ou fazendo alterações na configuração do Resource Tagger

Os dois perfis de configuração JSON, AMSManagedTags e CustomerManagedTags, implantados em sua conta AppConfig na AWS durante a integração e residência no aplicativo AMSResource Tagger e no AMSInfrastructureambiente, podem ser revisados por meio da API da. AppConfig GetConfiguration

Veja a seguir um exemplo dessa GetConfiguration chamada:

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

Aplicação: unidade AppConfig lógica para fornecer recursos; para o Resource Tagger, esse é o AMSResource Tagger.

- Meio ambiente: AMSInfrastructure.
- Configuração: para visualizar as definições de tag padrão do AMS Accelerate, o valor é AMSManaged Tags, enquanto para visualizar as definições de tag do cliente, o valor é CustomerManagedTags.
- ID do cliente: o identificador exclusivo da instância do aplicativo, que pode ser qualquer string.

- As definições da tag podem então ser visualizadas no arquivo de saída especificado, neste caso, outfile.json.

As definições de alarme podem então ser visualizadas no arquivo de saída especificado, neste caso, outfile.json.

Você pode ver qual versão da configuração foi implantada em sua conta visualizando as implantações anteriores no AMSInfrastructureambiente.

Para substituir as regras de tag:

Qualquer uma das regras de tag existentes pode ser substituída atualizando o perfil de personalização com CloudFormation by Implantando um perfil de configuração com o CloudFormation for Accelerate ou, ou diretamente usando AppConfig a API. CreateHostedConfigurationVersion Usar o mesmo configurationId como regra de tag de configuração padrão substitui a regra padrão e aplica a regra personalizada em seu lugar.

Para implantar as alterações feitas no CustomerManagedTagsdocumento:

Depois de fazer alterações no perfil de configuração de personalização, você deve implantar as alterações para eles. Para implantar as novas alterações, AppConfig a StartDeploymentAPI deve ser executada usando o AWS AppConfig console ou a CLI.

Implantando alterações de configuração

Depois que a personalização for concluída, essas alterações deverão ser implantadas por meio da AWS AppConfig StartDeploymentAPI. As instruções a seguir mostram como implantar usando AWS CLI o. Além disso, você pode usar o Console de gerenciamento da AWS para fazer essas alterações. Para obter informações, consulte Etapa 5: Implantação de uma configuração.

```
aws appconfig start-deployment
--application-id <application_id>
--environment-id <environment_id>
--deployment-strategy-id <deployment_strategy_id>
--configuration-profile-id <configuration_profile_id>
--configuration-version 1
```

- ID do aplicativo: O ID do aplicativo AMSResource Tagger. Obtenha isso com a chamada de ListApplicationsAPI.

- ID do ambiente: a ID do ambiente; obtenha isso com a chamada ListEnvironmentsda API.
- ID da estratégia de implantação: a ID da estratégia de implantação; obtenha isso com a chamada ListDeploymentStrategiesda API.
- ID do perfil de configuração: o ID do perfil de configuração de CustomerManagedTags; obtenha isso com a chamada da ListConfigurationProfilesAPI.
- Versão de configuração: a versão do perfil de configuração que você pretende implantar.

> **Important**
>
> O Resource Tagger aplica as tags conforme especificado nos perfis de configuração. Todas as modificações manuais feitas (com o ou CloudWatch CLI/SDK) nas tags de recursos são automaticamente revertidas Console de gerenciamento da AWS, portanto, certifique-se de que suas alterações sejam definidas por meio do Resource Tagger. Para saber quais tags são criadas pelo Resource Tagger, procure as chaves de tag prefixadas com. `ams:rt:`

Restrinja o acesso à implantação com as ações da StopDeploymentAPI StartDeploymente às ações da API a usuários confiáveis que entendam as responsabilidades e as consequências da implantação de uma nova configuração em seus alvos.

Para saber mais sobre como usar AWS AppConfig recursos para criar e implantar uma configuração, consulte a documentação em Como trabalhar com a AWS AppConfig.

Configurando o Terraform para ignorar as tags do Resource Tagger

Se você usa o Terraform para provisionar seus recursos e quiser usar o Resource Tagger para marcar seus recursos, as tags do Resource Tagger podem ser identificadas como deriva pelo Terraform.

Você pode configurar o Terraform para ignorar todas as tags do Resource Tagger usando o bloco de configuração do ciclo de vida ou o bloco de configuração global ignore_tags. Para obter mais informações, consulte a documentação do Terraform sobre marcação de recursos em Marcação de recursos.

O exemplo a seguir mostra como criar uma configuração global para ignorar todas as tags que começam com o prefixo `ams:rt:` da tag Resource Tagger:

```
provider "aws" {
```

```
  # ... potentially other configuration ...

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

Visualizando o número de recursos gerenciados pelo Resource Tagger

O Resource Tagger envia métricas a cada hora para a Amazon CloudWatch, no `AMS/ResourceTagger` namespace. As métricas são emitidas somente para tipos de recursos compatíveis com o Resource Tagger.

Nome da métrica	Dimensões	Descrição
ResourceCount	Componente, ResourceType	Número de recursos (do tipo de recurso especificado) implantados nessa região. Unidades: contagem
ResourcesMissingManagedTags	Componente, ResourceType	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. Unidades: contagem
UnmanagedResources	Componente, ResourceType	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. Unidades: contagem
MatchingResourceCount	Componente ResourceType, ConfigClauseName	Número de recursos (do tipo de recurso especificado) que correspondem ao bloco de configuração do Resource Tagger. Para que um recurso corresponda ao bloco de configuração, o bloco

Nome da métrica	Dimensões	Descrição
		deve estar ativado e o recurso deve correspon der ao filtro do bloco. Unidades: contagem

Essas métricas também podem ser visualizadas como gráficos no painel AMS-Resource-Tagger-Reporting-Dashboard. Para ver o painel, no console de CloudWatch gerenciamento da Amazon, selecione AMS-Resource-Tagger-Reporting-Dashboard. Por padrão, os gráficos nesse painel exibem os dados do período anterior de 12 horas.

O AMS Accelerate implanta CloudWatch alarmes em sua conta para detectar aumentos significativos no número de recursos não gerenciados, por exemplo, recursos excluídos do gerenciamento pelo AMS Resource Tagger. As operações do AMS investigarão aumentos nos recursos não gerenciados que excedam: três recursos do mesmo tipo ou um aumento de 50% em relação a todos os recursos do mesmo tipo. Se a alteração não parecer deliberada, a AMS Operations poderá entrar em contato com você para analisar a alteração.

Usando CloudFormation para criar tags para o AMS Accelerate

Você pode usar CloudFormation para aplicar tags no nível da pilha (consulte a CloudFormation documentação, tag de recurso) ou no nível do recurso individual (por exemplo, consulte Como marcar EC2 seus recursos da Amazon).

> **Important**
>
> Alguns componentes do serviço AMS Accelerate exigem etiquetas com o prefixo ams:rt:. O Resource Tagger acredita que possui essas tags e as excluirá se nenhuma regra de configuração do Resource Tagger permitir. Você sempre precisa implantar um perfil de configuração do Resource Tagger para essas tags, mesmo se estiver usando o CloudFormation Terraform.

CloudFormation Casos de uso do AMS Accelerate

Esta seção lista as ações comumente executadas com CloudFormation.

Tópicos

- Marcar uma EC2 instância com CloudFormation for Accelerate
- Marcando um AutoScaling grupo (ASG) com CloudFormation o for Accelerate
- Implantando um perfil de configuração com o CloudFormation for Accelerate

Marcar uma EC2 instância com CloudFormation for Accelerate

Veja a seguir um exemplo de como você pode aplicar a tag ams:rt:ams-managed com o valor true a uma instância da Amazon gerenciada por. EC2 CloudFormation A tag ams:rt:ams-managed permite que você tenha seus recursos monitorados pelo AMS Accelerate.

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

Properties:
  InstanceType: "t3.micro"

  # ...other properties...

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

Marcando um AutoScaling grupo (ASG) com CloudFormation o for Accelerate

Veja a seguir um exemplo de como você pode aplicar a tag ams:rt:ams-managed com o valor true a um grupo de Auto Scaling gerenciado por. CloudFormation Observe que o grupo Auto Scaling propagará suas tags para as EC2 instâncias da Amazon criadas por ele. A tag ams:rt:ams-managed permite que você tenha seus recursos monitorados pelo AMS Accelerate.

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

  # ...other properties...

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

Implantando um perfil de configuração com o CloudFormation for Accelerate

Se você deseja implantar seu perfil de `CustomerManagedTags` configuração usando CloudFormation, você pode usar os seguintes CloudFormation modelos. Coloque a configuração JSON desejada no `AMSResourceTaggerConfigurationVersion.Content` campo.

Quando você implanta os modelos em uma CloudFormation pilha ou conjunto de pilhas, a implantação do `AMSResourceTaggerDeployment` recurso falhará se você não tiver seguido o formato JSON exigido para a configuração. Consulte Sintaxe e estrutura para obter detalhes sobre o formato esperado.

Para obter ajuda na implantação desses modelos como uma CloudFormation pilha ou conjunto de pilhas, consulte a documentação relevante AWS CloudFormation abaixo:

- Criando uma pilha no console AWS CloudFormation
- Criando uma pilha com AWS CLI
- Criação de um conjunto de pilhas

> **Note**
>
> Se você implantar uma versão de configuração usando um desses modelos e, posteriormente, excluir a CloudFormation pilha/conjunto de pilhas, a versão de configuração do modelo permanecerá como a versão atual implantada e nenhuma implantação adicional será feita. Se quiser voltar para uma configuração padrão, você precisará implantar manualmente uma configuração vazia (ou seja, apenas`{}`) ou atualizar sua pilha para uma configuração vazia, em vez de excluir a pilha.

JSON

```
{
  "Description": "Custom configuration for the AMS Resource Tagger.",
  "Resources": {
    "AMSResourceTaggerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
```

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

YAML

```
Description: Custom configuration for the AMS Resource Tagger.
Resources:
  AMSResourceTaggerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
```

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

Usando o Terraform para criar tags para o AMS Accelerate

Se você não quiser usar o AMS Accelerate Resource Tagger, você pode aplicar suas próprias tags usando o Terraform. No entanto, se você não quiser usar o Resource Tagger devido ao desvio das definições do Terraform, existe uma maneira de usar o Resource Tagger e ignorar o desvio que ele causa; veja. Configurando o Terraform para ignorar as tags do Resource Tagger

> **Important**
>
> Alguns componentes do serviço AMS Accelerate exigem etiquetas com o prefixo ams:rt:. O Resource Tagger acredita que possui essas tags e as exclui se nenhuma regra de configuração do Resource Tagger permitir. Você deve implantar um perfil de configuração do Resource Tagger para essas tags, mesmo se estiver usando o CloudFormation Terraform.

Veja a seguir um exemplo de como você pode aplicar a tag ams:rt:ams-managed com o valor true a uma instância da Amazon gerenciada pelo Terraform. EC2 A tag ams:rt:ams-managed permite que você tenha seus recursos monitorados pelo AMS Accelerate.

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

    instance_type = "t3.micro"

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

Veja a seguir um exemplo de como você pode aplicar a tag ams:rt:ams-managed com o valor true a um grupo de Auto Scaling gerenciado pelo Terraform. Observe que o grupo Auto Scaling propaga suas tags para as EC2 instâncias da Amazon que são criadas por ele. A tag ams:rt:ams-managed permite que você tenha seus recursos monitorados pelo AMS Accelerate.

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

    name = "terraform-sample"

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

Para obter uma descrição de como gerenciar tags de recursos criadas pelo Terraform, consulte. Configurando o Terraform para ignorar as tags do Resource Tagger

Relatórios de incidentes, solicitações de serviço e perguntas sobre faturamento no AMS Accelerate

Com o AMS Accelerate, você pode solicitar ajuda com problemas e solicitações operacionais a qualquer momento por meio do AWS Support Center no Console de gerenciamento da AWS. Os engenheiros de operações do AMS Accelerate estão disponíveis para responder aos seus incidentes e solicitações de serviço round-the-clock, com Acordos de Nível de Serviço (SLAs) em tempo de resposta para o serviço. Os engenheiros de operações do AMS Accelerate notificam você de forma proativa sobre alertas e perguntas importantes usando os mesmos mecanismos.

O AMS Accelerate fornece uma variedade de serviços operacionais para ajudá-lo a alcançar a excelência operacional em AWS. Para obter uma compreensão rápida de como o AMS ajuda suas equipes a alcançar a excelência operacional geral Nuvem AWS com alguns de nossos principais recursos operacionais, incluindo round-the-clock suporte técnico, monitoramento proativo, segurança, aplicação de patches, registro e backup, consulte Diagramas de arquitetura de referência do AMS.

Tópicos

- Gerenciamento de incidentes no AMS Accelerate
- Gerenciamento de solicitações de serviço no Accelerate
- Relatório de incidentes e teste de solicitação de serviço no Accelerate
- Perguntas sobre faturamento para o AMS Accelerate

Gerenciamento de incidentes no AMS Accelerate

No AMS Accelerate, você usa o AWS Support Center Consolepara arquivar relatórios de incidentes. Incidentes são problemas de AWS service (Serviço da AWS) desempenho que afetam seu ambiente gerenciado, conforme determinado pelo AMS Accelerate ou por você. Os incidentes identificados pela equipe do AMS Accelerate 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 Accelerate determina se o evento não está impactando, se é um incidente (uma interrupção ou degradação do serviço) ou um problema (a causa raiz subjacente de um ou mais incidentes).

> **Note**
>
> A equipe do AMS Accelerate também recebe incidentes criados por você de forma programática usando a API do AWS Support com código de serviço. `service-ams-operations-report-incident`

Para obter informações sobre o uso Suporte, consulte Introdução ao Suporte.

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.

Como funcionam a resposta e a resolução de incidentes

O AMS Accelerate usa as melhores práticas 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 centros de operações em todo o mundo, com operadores dedicados monitorando ativamente os painéis de monitoramento e as filas de incidentes.

Nossos engenheiros de operações usam ferramentas internas de rastreamento de incidentes para identificar, registrar, categorizar, priorizar, diagnosticar, resolver e fechar incidentes. Fornecemos atualizações sobre todas essas atividades por meio do Support Center e da AWS Support API. AWS Nossos operadores utilizam uma variedade de ferramentas de AWS suporte interno para ajudar em todas essas atividades. Esses operadores estão profundamente familiarizados com a infraestrutura suportada pelo AMS Accelerate e têm habilidades técnicas de nível especializado para resolver os problemas de suporte identificados. Caso nossos operadores precisem de ajuda, as equipes de suporte e AWS serviço Premium estão disponíveis.

Depois que seu incidente for recebido pela equipe de operações do AMS Accelerate, validamos a prioridade e a classificação trabalhando com você se houver algum esclarecimento necessário. Por exemplo, se o relatório do incidente for melhor classificado como uma solicitação de serviço, ele será reclassificado e a equipe de solicitação de serviço do AMS Accelerate assumirá o controle e você será notificado. Se o incidente puder ser resolvido pelo operador receptor, serão tomadas medidas para resolvê-lo rapidamente. Os operadores do AMS Accelerate 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. Depois de resolvido, a equipe de operações do AMS Accelerate documenta o incidente e a resolução para uso futuro.

Nos casos em que incidentes críticos de gravidade estão afetando suas cargas de trabalho críticas, o AMS Accelerate pode recomendar uma restauração da infraestrutura. Geralmente, há uma compensação entre solucionar um problema e simplesmente restaurar a partir de um backup funcional conhecido, e os riscos e impactos do tempo de inatividade do serviço são os fatores

decisivos. Se você tiver tempo para se dedicar à solução de problemas, o AMS Accelerate ajudará você e seu gerente de prestação de serviços em nuvem (CSDM) poderá se envolver, mas se a urgência de restaurar for alta, o AMS Accelerate poderá iniciar uma restauração imediatamente.

Trabalhando com incidentes no AMS Accelerate

No AWS Support Center, você pode realizar as seguintes tarefas:

- Relate e atualize um incidente. Para relatar um incidente do AMS Accelerate, escolha Operações do AMS -- Relatar incidente no menu Serviços.
- Obtenha uma lista e informações detalhadas sobre todos os incidentes enviados.
- Limite sua busca por incidentes por status e outros filtros.
- Adicione comunicações e anexos de arquivos aos seus incidentes e adicione destinatários de e-mail para correspondência de casos.
- Inicie um bate-papo ao vivo ou solicite uma ligação sobre seu incidente.

> **Note**
>
> O recurso de bate-papo ao vivo não serve para eventos de segurança; para problemas de segurança, crie um caso de suporte de alta prioridade (P1 ou P2).

- Resolva incidentes.
- Avalie as comunicações de incidentes.

Os exemplos a seguir descrevem o uso do Support Center para enviar um incidente. Depois de enviado, a equipe do AMS Accelerate trabalha com você para resolver o incidente de acordo com o SLA padrão do AMS Accelerate.

Enviando um incidente para o Accelerate

Para relatar um incidente usando o Support Center, consulte a documentação de suporte: Criando um caso de suporte

Para relatar um incidente usando o Suporte centro:

1. Clique em Criar caso. A página de criação de caso de incidente é aberta.
2. Abra o menu Tipo de problema do suporte técnico e escolha Operações do AMS -- Relatar incidente. Forneça informações sobre seu incidente e escolha Criar.

3. Para se manter informado por e-mail em cada etapa do processo de resolução de incidentes, certifique-se de preencher a opção E-mails CC; se você se conectar por federação, faça login antes de seguir o link no e-mail que o AMS Accelerate lhe envia sobre o incidente.

> **Note**
>
> Faça a descrição com o máximo de detalhes possível. Inclua informações de recursos relevantes com outras informações que possam nos ajudar a entender o problema. Por exemplo, para solucionar problemas de performance, inclua time stamps e logs. Para solicitações de recursos ou perguntas de orientação geral, inclua uma descrição do seu ambiente e a finalidade. Em todos os casos, siga a Orientação da descrição que aparece no formulário de envio de caso.
> Ao fornecer o máximo de detalhes possível, você aumenta as chances de que seu caso seja resolvido rapidamente.

Você também pode usar a API do AWS Support com código de serviço `service-ams-operations-report-incident` para relatar um incidente.

Monitorando e atualizando um incidente do Accelerate

Você pode atualizar, monitorar e revisar relatórios de incidentes e solicitações de serviço, ambos chamados de casos, usando o Support Center ou programaticamente usando a operação Suporte API. `DescribeCases`

Para monitorar um caso, incidente ou solicitação de serviço usando o Suporte Center, siga estas etapas.

1. No console AWS de gerenciamento, navegue até Support.
2. No painel de navegação à esquerda, selecione Seus casos de suporte, navegue até um caso e escolha o link Assunto para abrir uma página de detalhes com o status atual e as correspondências.

   Se você quiser usar o telefone ou o chat neste momento, clique em Abrir caso no Support Center para abrir a página Criar caso no Suporte Centro, preenchida automaticamente com o tipo de serviço AMS.

Quando um incidente relatado ou um caso de solicitação de serviço é atualizado pela equipe de operações do Accelerate, você recebe um e-mail e um link para o incidente no Support Center para poder responder.

> **Note**
>
> Você não pode responder à correspondência do caso respondendo ao e-mail.

Se houver muitos casos no painel, você poderá usar a opção Filtro:

- Assunto: Use esse filtro para pesquisar palavras-chave no assunto do caso.
- Gravidade: use isso para filtrar os casos por gravidade selecionando uma severidade na lista.
- Tipo de caso: use isso para ver todos os casos de um determinado tipo de caso. Os incidentes do Accelerate e as solicitações de serviço aparecem no Tipo de caso de Suporte Técnico junto com quaisquer casos específicos do serviço.
- Status: use isso para filtrar casos por status selecionando um status específico na lista.

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.

   Certifique-se de avaliar o serviço por meio da classificação de 1 a 5 estrelas para que a AMS saiba como estamos.

Gerenciando incidentes do Accelerate com a API de suporte

Você pode usar a Suporte API para criar incidentes e adicionar correspondência com a Suporte equipe durante as investigações sobre seus problemas. A Suporte API modela grande parte do comportamento do AWS Support Center.

Para obter informações sobre como usar esse serviço de AWS suporte, consulte Programming the Life of an AWS Support Case.

> **Note**
>
> A equipe do AMS Accelerate recebe incidentes criados por você de forma programática usando o código de serviço com. `service-ams-operations-report-incident`

Respondendo a um incidente gerado pelo AMS Accelerate

O AMS Accelerate monitora proativamente seus recursos. Para obter mais informações, consulte Monitoramento e gerenciamento de eventos no AMS Accelerate. Às vezes, o AMS Accelerate identifica e cria um incidente, na maioria das vezes para notificá-lo sobre um evento. Se for necessária uma ação de sua parte para resolver um incidente, a notificação será enviada pela equipe do AMS Accelerate às informações de contato que você forneceu para a conta. Você responde a essa notificação da mesma forma que a qualquer outro incidente, geralmente por meio do Support Center, embora em alguns casos seja necessário entrar em contato por e-mail ou telefone.

> **Important**
>
> Para receber notificações de mudança de estado para um caso de incidente ou solicitação de serviço, insira um endereço de e-mail no campo de endereços.

Assista ao vídeo de Akshay para saber mais (4:15)

Gerenciamento de solicitações de serviço no Accelerate

Tópicos

- Quando usar uma solicitação de serviço para o Accelerate
- Como funciona o gerenciamento de solicitações de serviço no Accelerate
- Criando uma solicitação de serviço no Accelerate
- Monitorando e atualizando uma solicitação de serviço para o Accelerate
- Gerenciando solicitações de serviço com a API de suporte do Accelerate
- Respondendo a uma solicitação de serviço gerada pelo AMS Accelerate

O AMS Accelerate usa o gerenciamento de solicitações de serviço para registrar, agir, comunicar o progresso e fornecer notificações de solicitações de serviço ativas.

O objetivo do processo de gerenciamento de solicitações de serviço é garantir que seu serviço gerenciado esteja fornecendo o que você precisa.

Para consultas relacionadas ao faturamento, crie uma solicitação de serviço.

> **Note**
>
> A equipe do AMS Accelerate recebe solicitações de serviço criadas por você de forma programática usando a API do AWS Support com código de serviço. `service-ams-operations-service-request`

Usando o AWS Support Center, você pode realizar as seguintes tarefas:

- Relate e atualize uma solicitação de serviço. Para uma solicitação de serviço do AMS Accelerate, escolha Operação do AMS -- Solicitação de serviço no menu Serviços.
- Obtenha uma lista e informações detalhadas sobre todas as solicitações de serviço enviadas.
- Limite sua busca por solicitações de serviço por status e outros filtros.
- Adicione comunicações e anexos de arquivos às suas solicitações e adicione destinatários de e-mail para correspondência de casos.
- Resolva solicitações de serviço.
- Avalie as comunicações de solicitação de serviço.

Quando usar uma solicitação de serviço para o Accelerate

Os exemplos a seguir descrevem uma solicitação de serviço. Depois de enviar uma solicitação de serviço, a equipe do AMS Accelerate trabalha com você para resolver a solicitação de acordo com seu SLA do AMS.

- 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

Como funciona o gerenciamento de solicitações de serviço no Accelerate

As solicitações de serviço são tratadas pela equipe de operações de plantão do AMS Accelerate.

Depois que sua solicitação de serviço é recebida pela equipe de operações do AMS Accelerate, ela é analisada para garantir que esteja devidamente classificada como uma solicitação de serviço ou um incidente. Se for reclassificado como um incidente, o processo de gerenciamento de incidentes do AMS Accelerate será iniciado e você receberá uma notificação.

Se o operador do AMS Accelerate 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 Accelerate, a operadora enviará a solicitação para seu gerente de prestação de serviços em nuvem, para que ele possa se comunicar com você, ou para a equipe de AWS suporte apropriada, junto com um e-mail para você informando quais etapas estão sendo tomadas.

A solicitação de serviço não é resolvida até que você indique que está satisfeito com o resultado.

> **Note**
>
> Recomendamos que você forneça um e-mail de contato, nome e número de telefone em todos os casos para facilitar as comunicações.

Criando uma solicitação de serviço no Accelerate

Para criar uma solicitação de serviço, siga estas etapas:

1. No console do AMS Accelerate, navegue até Painel.
2. Escolha Abrir uma solicitação de serviço, o AMS — Solicitação de serviço está pré-selecionado.
3. Escolha uma categoria.
4. Escolha Severidade (somente nos níveis Plus ou Premium).
5. Insira as informações para:
   - Assunto: Um título descritivo para a solicitação de serviço.
   - Descrição: uma descrição abrangente da solicitação de serviço, dos sistemas afetados e do resultado esperado de uma resolução.
6. Para adicionar um anexo, escolha Anexar arquivos, navegue até o anexo desejado e escolha Abrir. Para excluir o anexo, escolha o ícone de exclusão
7. Entre em contato conosco: O contato padrão do AMS pela web. Para selecionar outras opções:
   - Idioma de contato preferencial: o inglês é o idioma suportado para solicitações de serviço do AMS Accelerate.
   - Web: Sua solicitação de serviço é enviada pela web e tratada pela equipe de operações do AMS.
   - Bate-papo: converse on-line com um representante de operações do AMS Accelerate. Essa opção adiciona você à fila de bate-papo.
   - Telefone: Um representante de operações do AMS liga de volta para você. Insira sua região, número de telefone e extensão da AWS, se aplicável.
   - Contatos adicionais: insira os endereços de e-mail adicionais que você deseja copiar em sua solicitação de serviço.
8. Selecione Enviar.

   Uma página de detalhes do caso é aberta com informações sobre a solicitação de serviço, como Tipo, Assunto, Criado, ID e Status. Além disso, uma área de correspondência que inclui a descrição da solicitação que você criou.

   Para abrir uma área de correspondência e fornecer detalhes adicionais ou atualizações no status, escolha Responder.

Depois que a solicitação de serviço for resolvida, escolha Resolver caso.

Se houver tantas correspondências que nem todas apareçam na página, escolha Carregar mais.

Certifique-se de avaliar o serviço por meio da classificação de 1 a 5 estrelas para que a AMS saiba como estamos nos saindo.

> **Note**
>
> Se você for testar a funcionalidade da solicitação de serviço, recomendamos adicionar um sinalizador de não ação ao assunto da solicitação de serviço, como`AMSTestNoOpsActionRequired`. Depois, você pode testar sem iniciar o processo de resolução da solicitação de serviço.
> A equipe do AMS Accelerate recebe solicitações de serviço criadas por você de forma programática usando a API do AWS Support com código de serviço. `service-ams-operations-service-request`

Monitorando e atualizando uma solicitação de serviço para o Accelerate

Para monitorar um caso, incidente ou solicitação de serviço usando o Suporte Center, siga estas etapas.

1. No console AWS de gerenciamento, navegue até Support.
2. No painel de navegação à esquerda, selecione Seus casos de suporte, navegue até um caso e escolha o link Assunto para abrir uma página de detalhes com o status atual e as correspondências.

   Se você quiser usar o telefone ou o chat neste momento, clique em Abrir caso no Support Center para abrir a página Criar caso no Suporte Centro, preenchida automaticamente com o tipo de serviço AMS.

   Quando um incidente relatado ou um caso de solicitação de serviço é atualizado pela equipe de operações do Accelerate, você recebe um e-mail e um link para o incidente no Support Center para poder responder.

> **Note**
>
> Você não pode responder à correspondência do caso respondendo ao e-mail.

Se houver muitos casos no painel, você poderá usar a opção Filtro:

- Assunto: Use esse filtro para pesquisar palavras-chave no assunto do caso.
- Gravidade: use isso para filtrar casos por gravidade selecionando uma severidade na lista.
- Tipo de caso: use isso para ver todos os casos de um determinado tipo de caso. Os incidentes do Accelerate e as solicitações de serviço aparecem no Tipo de caso de Suporte Técnico junto com quaisquer casos específicos do serviço.
- Status: use isso para filtrar casos por status selecionando um status específico na lista.

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.

   Certifique-se de avaliar o serviço por meio da classificação de 1 a 5 estrelas para que a AMS saiba como estamos.

Gerenciando solicitações de serviço com a API de suporte do Accelerate

Você pode usar a API AWS Support para criar solicitações de serviço e adicionar correspondência a elas durante as investigações de seus problemas e interações com a equipe de AWS suporte. A API de AWS suporte modela grande parte do comportamento do AWS Support Center.

A equipe do AMS também recebe solicitações de serviço criadas por você de forma programática usando a API do AWS Support com o código service-ams-operations-service de serviço -request.

Para obter mais informações sobre como você pode usar esse serviço de AWS suporte, consulte Programando a vida útil de um AWS Support Case.

Respondendo a uma solicitação de serviço gerada pelo AMS Accelerate

O AMS Accelerate monitora proativamente seus recursos; para obter mais informações, consulteMonitoramento e gerenciamento de eventos no AMS Accelerate. Às vezes, o AMS Accelerate cria uma solicitação de serviço ou uma notificação de serviço para você, normalmente se for necessária uma ação de sua parte para resolver uma solicitação de serviço. Nesse caso, a equipe do AMS Accelerate envia uma notificação ao contato que você forneceu para a conta. Você responde a essa solicitação de serviço da mesma forma que em qualquer outro caso, geralmente por meio do Support Center, embora, em alguns casos, seja necessária correspondência por e-mail ou telefone.

> **Important**
>
> Para receber notificações de mudança de estado para uma solicitação de serviço ou caso de incidente, você deve ter inserido um endereço de e-mail no campo de endereços. As notificações vão somente para o endereço de e-mail adicionado ao caso quando ele é criado.

O link no e-mail de notificação funciona somente se você estiver usando um servidor de e-mail na sua rede federada do AMS Accelerate. Caso contrário, você pode responder à correspondência acessando o console do AMS Accelerate e usando a página de detalhes do caso.

> **Note**
>
> O AMS Accelerate envia comunicações para seu endereço de e-mail principal em sua AWS conta; recomendamos adicionar um alias alternativo de e-mail de contato de operações para facilitar o processo request/notification de gerenciamento do serviço. Isso é abordado durante o processo de integração do AMS Accelerate e na documentação de integração relacionada.

Relatório de incidentes e teste de solicitação de serviço no Accelerate

Ao testar relatórios de incidentes ou solicitações de serviço, pedimos que você inclua AMSTestNoOpsActionRequiredno texto do assunto. Isso permite que o AMS saiba que o incidente ou a solicitação é apenas para testes. Quando os engenheiros de operações da AMS virem isso, eles não responderão de forma alguma.

Perguntas sobre faturamento para o AMS Accelerate

Para enviar uma pergunta relacionada ao faturamento, conclua as seguintes etapas:

1. Abra o AWS Support Centro 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.

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 atividades relacionadas 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.
- Evento de segurança do cliente: eventos de segurança planejados. Por exemplo, 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 obter ajuda com seus requisitos específicos, entre em contato com seu CSDM.

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 por meio de Cases: Service Request (SRs) /Incident durante um evento de PEM?

- Use o ID do PEM compartilhado pelo seu CSDM na linha de RFC/SR assunto do formato. *PEM-ID*

  Onde aplicável, você pode usar a opção de contato ao vivo.
- 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 um caso relacionado ao PEM é enviado?

- 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.

- Um link para os detalhes do PEM é fornecido internamente aos engenheiros da AMS.

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 (Solicitação de Serviço, Incidentes), são definidos pelo AMS. SLOs

  Para obter mais informações, consulte Relatórios de incidentes, solicitações de serviço e perguntas sobre faturamento no AMS Accelerate.

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).

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 AWSlugares 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 compilaçõ es de AMI usando o Monitoring. CloudWatch Também fornecemo s assistência para solução de problemas e relatórios detalhado s para todos os AMIs usados nas contas designadas. Essa oferta exige que os pipelines de criação da AMI sejam implantad os 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 implement ar 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 rapidamen te 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 sobrecarg a de gerenciam ento detectand o 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 pouso, 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 operacion ais subjacentes de gerenciamento AWS Control Tower, AWS Transit Gateway AWS Organizations e.

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 remediaçã o 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 gerenciam ento 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 atualizaç ões contínuas com reconheci mento 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 resiliênc ia 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 integrida de contínuas de suas implantaç ões do Amazon Elastic Kubernete s 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

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 de gerenciamento de hosts do AMS
- Relatórios de backup do AMS
- AWS Config Relatório de conformidade de controle
- Relatório de configuração de respostas do AMS Config Rules
- 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 de gerenciamento de hosts do AMS

Relatórios disponíveis

- Relatório de cobertura do agente SSM

Relatório de cobertura do agente SSM

O relatório de cobertura do agente SSM do AMS informa se as EC2 instâncias na conta têm ou não o agente SSM 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
Tamanho do backup	Tamanho do backup em GB
ARN do ponto de recuperação	O ARN do backup criado

Nome do campo	Definição
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 suportado s 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.

AWS Config Relatório de conformidade de controle

O relatório AWS Config de conformidade de controle fornece uma análise aprofundada da conformidade de recursos e AWS Config regras das contas do AMS. Você filtra o relatório por Config Rule Severity para priorizar as descobertas mais críticas. A tabela a seguir lista os dados fornecidos por esse relatório:

Campo	Descrição
Data	Data do relatório

Campo	Descrição
Nome do cliente	Nome do cliente
AWS ID da conta	ID AWS da conta associada para o cliente
Identificador de origem	AWS Config identificador de fonte exclusivo da regra
Descrição da regra	AWS Config descrição da regra
Tipo de regra	AWS Config tipo de regra
Sinalizador de conformidade	AWS Config estado de conformidade da regra
Tipo de recurso	AWS tipo de recurso
Nome do recurso	AWS nome do recurso
Gravidade	Gravidade padrão recomendada definida pelo AMS para a AWS Config regra
Categoria de remediação	Categoria de resposta de remediação associada a uma regra AWS Config
Descrição da remediação	Ação de remediação explicada para tornar a AWS Config regra compatível
Ação do cliente	Ação do cliente necessária para que a AWS Config regra esteja em conformidade
Relatório de métricas Delta	Alterações para conformidade de uma regra entre determinadas duas datas

Relatório de configuração de respostas do AMS Config Rules

O relatório de configuração de resposta das regras de configuração do AMS fornece uma visão aprofundada de como você atualmente tem o Accelerate configurado para responder às regras de configuração do AMS que não estão em conformidade. Para obter mais informações sobre

como alterar a resposta das regras de configuração do AMS, consulte Respostas de descobertas personalizadas do AMS Accelerate.

Esse relatório mostra somente as configurações que você alterou e exclui as configurações padrão do AMS que estão listadas na Biblioteca de Regras de Configuração do AMS. O relatório fornece dados sobre a configuração de recursos e respostas da regra de configuração do AMS das contas do AMS, incluindo o seguinte:

- A lista de AWS contas para as quais você alterou a resposta padrão para as regras de configuração do AMS.
- A lista de tags às quais você associou uma resposta para as regras de configuração do AMS.
- A lista de configurações de resposta para cada regra, conta e tag.
- A lista de recursos para os quais você alterou a resposta padrão das regras de configuração do AMS.

Relatório de configurações de resposta mais recente

Campo	Descrição
Data	Data em que o relatório foi gerado
Nome do cliente	Nome do cliente
AWS ID da conta	O ID da AWS conta associado à configuração
Nome da conta	AWS nome da conta do grupo de recursos no nível da conta
Tipo de descoberta	Tipo de descoberta identificada. Nesse caso, AWS Config
Identificador de origem	AWS Config Identificador de fonte exclusivo da regra
ID do grupo de recursos	O ID do grupo de recursos associado à configuração da resposta
Ação de resposta configurada	Tipo de ação acionada pelo AMS

Campo	Descrição
SSM Runbook associado	O Runbook de Remediação que será executado, se houver
Tipo de grupo de recursos	Isso pode ser Conta ou Tag

Recursos com resposta padrão personalizada das regras de configuração

Nome do campo	Definição
Nome do cliente	Nome do cliente
Data	Data em que o relatório foi gerado
AWS Nome da conta	AWS nome da conta
ID da conta	ID AWS da conta associada
Regra de configuração do AMS	Regra de configuração do AMS que tem como alvo o recurso e é aplicada com uma configura ção
ID do recurso	O ID do recurso na conta do cliente alvo da regra de configuração do AMS
Região de recursos	A AWS região na qual a configuração é aplicada
Tipo de recurso	AWS tipo de recurso
ID do grupo de recursos	O ID do grupo de recursos associado à configuração da resposta
Sinalizador AMS de recursos	Se o AWS recurso for implantado pelo AMS, esse campo será definido como `True`
Tipo de gatilho	O tipo de resposta configurada para o recurso

Nome do campo	Definição
Sinalizador de conformidade	Estado de conformidade da regra de configuração do AMS

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
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
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; adjusted_ aws_charges * uplift_percent

Nome do campo	Definição
Gastos do EC2 RDS em instâncias	Gastos em EC2 instâncias do RDS e suas
Taxas do AMS	Total de cobranças do AMS pelo produto; uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + 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
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.

Nome do campo	Definição
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
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

Nome do campo	Definição
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
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

Nome do campo	Definição
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.
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.

Para permitir que seus usuários visualizem os relatórios do AMS Accelerate no console do AMS, você deve conceder permissões explícitas no AWS Identity and Access Management (IAM) para

realizar essas ações. Por exemplo, políticas do IAM, consulte Permissões para usar os recursos do AMS.

> **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

- Resumo dos detalhes da instância para a aplicação de patches do AMS
- Detalhes do patch
- Instâncias que perderam os patches

Resumo dos detalhes da instância para a aplicação de patches do AMS

Esse é um relatório informativo que ajuda a identificar todas as instâncias integradas ao AMS Patching, 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

Nome do campo do console	Nome do campo do conjunto de dados	Definição
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 da instância	nome_instância	Nome da EC2 instância
Grupo de patches de instância	grupo_patch_instância	Nome do grupo de patches usado para agrupar instância s e aplicar a mesma janela de manutenção
Tipo de grupo de patches de instância	tipo de grupo_patch_de_ins tância	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 relaciona da a Malz

Nome do campo do console	Nome do campo do conjunto de dados	Definição
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
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 aplicativ os 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”

Nome do campo	Nome do campo do conjunto de dados	Definição
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”
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)

Nome do campo	Nome do campo do conjunto de dados	Definição
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
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

Nome do campo	Nome do campo do conjunto de dados	Definição
Janela de manutenção: próxima data de execução	janela_seguinte 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”
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”

Nome do campo	Nome do campo do conjunto de dados	Definição
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.
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

Nome do campo	Nome do campo do conjunto de dados	Definição
	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_HHMI	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	

Nome do campo	Nome do campo do conjunto de dados	Definição
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
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

Nome do campo	Nome do campo do conjunto de dados	Definição
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

Nome do campo	Nome do campo do conjunto de dados	Definição
SLA da conta	conta_sla	Compromisso de serviço da conta AMS
	bandeira_mala	Bandeira para conta relaciona da 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
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

Nome do campo	Nome do campo do conjunto de dados	Definição
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
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

Nome do campo	Nome do campo do conjunto de dados	Definição
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
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

Nome do campo	Nome do campo do conjunto de dados	Definição
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
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 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.

Nome do campo	Nome do campo do conjunto de dados	Definição
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.
Dia resolvido	dia_resolvido	O dia em que o incidente foi resolvido em YYYY-MM-DD formato.

Nome do campo	Nome do campo do conjunto de dados	Definição
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; adjusted_ aws_charges * 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; ris_charges * 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; sp_charges * uplift_percent
Taxas do AMS	ams_charges	Total de cobranças de ams pelo produto; uplifted_ aws_charges + instance_ ec2_rds_spend + uplifted_ris + 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 Agregated 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 proprieda 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 sinalizad or 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 configura ção gerenciada e nenhum identificador para uma regra de configuração personali zada.
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.
sinalizador_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 para o AMS Patching	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 configura ção 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.

Gerenciamento de acesso no AMS Accelerate

O gerenciamento de acesso é a forma como seus recursos são protegidos, permitindo somente acesso autorizado e autenticado. Com o AMS Accelerate, você é responsável por gerenciar o acesso aos seus recursos subjacentes Contas da AWS e aos deles, como soluções de gerenciamento de acesso, políticas de acesso e processos relacionados. Para ajudá-lo a gerenciar sua solução de acesso, o AMS Accelerate implanta AWS Config regras que detectam configurações incorretas comuns do IAM e, em seguida, entregam notificações de remediação. Uma configuração incorreta comum do IAM é que o usuário root tem chaves de acesso. A regra de `iam-root-access-key-check` configuração verifica se a chave de acesso do usuário root está disponível e é compatível ou se a chave de acesso não existe. Para obter uma lista das regras de configuração implantadas pelo AMS, consulte a biblioteca de AWS Config regras do AMS.

Tópicos

- Tenha acesso ao console Accelerate
- Permissões para usar os recursos do AMS
- Por que e quando o AMS acessa sua conta
- Como o AMS acessa sua conta
- Como e quando usar a conta de usuário raiz no AMS

Tenha acesso ao console Accelerate

Ao fazer a integração com o Accelerate, você tem acesso automático ao console do Accelerate. Você pode acessar o console pesquisando Managed Services no console de gerenciamento da AWS. O console do Accelerate oferece uma visão resumida dos recursos que você tem com o Accelerate. Essa visualização inclui componentes individuais apresentados no painel e nas páginas de configuração.

Permissões para usar os recursos do AMS

Para permitir que seus usuários leiam e configurem os recursos do AMS Accelerate, como acessar o console do AMS ou configurar backups, você deve conceder permissões explícitas às funções do IAM para realizar essas ações. O CloudFormation modelo a seguir contém as políticas necessárias para ler e configurar os serviços associados ao AMS para que você possa atribuí-los às suas

funções do IAM. Eles foram projetados para se alinharem estreitamente às responsabilidades de trabalho comuns no setor de TI, onde as permissões de administrador ou somente leitura são necessárias; no entanto, se você precisar conceder permissões diferentes aos usuários, poderá editar a política para incluir ou excluir permissões específicas. Você também pode criar a sua própria política personalizada.

O modelo fornece duas políticas. A `AMSAccelerateAdminAccess` política deve ser usada para configurar e operar os componentes do AMS Accelerate. Essa política geralmente é assumida por um administrador de TI e concede permissões para configurar recursos do AMS, como patches e backups. Isso `AMSAccelerateReadOnly` concede as permissões mínimas necessárias para visualizar os recursos relacionados ao AMS Accelerate.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Por que e quando o AMS acessa sua conta

Os operadores do AMS Accelerate (Accelerate) podem acessar o console e as instâncias da sua conta, em determinadas circunstâncias, para gerenciar seus recursos. Esses eventos de acesso estão documentados em seus registros AWS CloudTrail (CloudTrail). Para obter detalhes sobre como analisar as atividades da equipe de operações do AMS Accelerate e da automação do AMS Accelerate em sua conta, consulteRastreando alterações em suas contas do AMS Accelerate.

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
Investigação interna de problemas	AMS	Problema (um problema que foi identificado como sistêmico)

Acesso	Iniciador	Trigger
Investigação e remediação de alertas	AMS	Itens de trabalho operacionais (SSM OpsItems) do AWS Systems Manager
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

Os operadores de AMS exigem as seguintes funções para atender sua conta.

> **Note**
>
> As funções de acesso do AMS permitem que os operadores do AMS acessem seus recursos para fornecer recursos do AMS (consulteService description (Descrição do serviço)). Alterar essas funções pode inibir nossa capacidade de fornecer esses recursos. Se você precisar alterar as funções de acesso ao AMS, consulte seu Cloud Architect.

Funções do IAM para acesso do AMS às contas de clientes

Função	Descrição
ams-access-admin	Essa função tem acesso administrativo total à sua conta sem restrições. Os serviços do AMS usam essa função com políticas de sessão restritivas que limitam o acesso para implantar a infraestrutura do AMS e operar sua conta.
ams-access-admin-operations	Essa função concede aos operadores do AMS permissões administrativas para operar sua conta. Essa função não concede permissões de leitura, gravação ou exclusão ao conteúdo do cliente em AWS serviços comumente usados como armazenamentos

Função	Descrição
	de dados, como Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift e Amazon. ElastiCache Somente operadores de AMS qualificados que tenham um forte conhecimento e experiência em gerenciam ento de acesso podem assumir essa função. Esses operadores servem como um ponto de escalonam ento para problemas de gerenciamento de acesso e acessam suas contas para solucionar problemas de acesso do operador do AMS.
ams-access-management	Implantado manualmente durante a integração. O sistema AMS Access exige essa função para gerenciar `ams-access-roles` e `ams-access-managed-policies` empilhar.
ams-access-operations	Essa função tem permissões para realizar tarefas administrativas em suas contas. Essa função não tem permissões de leitura, gravação ou exclusão do conteúdo do cliente em AWS serviços comumente usados como armazenamentos de dados, como Amazon Simple Storage Service, Amazon Relationa l Database Service, Amazon DynamoDB, Amazon Redshift e Amazon. ElastiCache As permissões para realizar operações de AWS Identity and Access Management gravação também são excluídas dessa função. A equipe de operações e os arquitetos de nuvem (CAs) do AMS Accelerate podem assumir essa função.

Função	Descrição
ams-access-read-only	Essa função tem acesso somente para leitura à sua conta. A equipe de operações e os arquitetos de nuvem (CAs) do AMS Accelerate podem assumir essa função. Permissões de leitura para o conteúdo do cliente em AWS serviços comumente usados como armazenamentos de dados, como Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift e, não recebem essa função. ElastiCache
ams-access-security-analyst	Essa função de segurança do AMS tem permissões em sua conta do AMS para realizar monitoramento dedicado de alertas de segurança e tratamento de incidentes de segurança. Somente algumas pessoas selecionadas da AMS Security podem assumir essa função.
ams-access-security-analyst-somente leitura	Essa função de segurança do AMS está limitada às permissões somente de leitura em sua conta do AMS para realizar monitoramento dedicado de alertas de segurança e tratamento de incidentes de segurança.

Note

Esse é o modelo para a ams-access-management função. É a pilha que os arquitetos de nuvem (CAs) implantam manualmente em sua conta no momento da integração: management-role.yaml.

Esse é o modelo para as diferentes funções de acesso para os diferentes níveis de acesso: ams-access-read-only,, ams-access-operations ams-access-admin-operations, ams-access-admin: accelerate-roles.yaml.

Como o AMS acessa sua conta

Os operadores do AMS Accelerate podem acessar o console e as instâncias da sua conta, em determinadas circunstâncias.

Os operadores do AMS usam o serviço interno de acesso AMS Accelerate para acessar suas contas de forma segura e auditada. Para acessar suas instâncias, os operadores do AMS usam o mesmo serviço de acesso interno do AMS que o agente e, após a concessão do acesso, os operadores do AMS Accelerate usam o gerenciador de sessões do SSM para obter acesso usando as credenciais da sessão. O acesso RDP para instâncias do Windows é fornecido estabelecendo o encaminhamento de portas para a instância e criando um usuário local usando SSM. As credenciais do usuário local são usadas para acesso RDP e removidas no final da sessão.

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.

Faça root com o AMS Accelerate:

O AMS não proíbe você de usar sua conta de usuário root. No entanto, o AMS Operations and Security trata seu uso como um problema a ser investigado e entraremos em contato com sua equipe de segurança a cada uso.

Recomendamos que você entre em contato com o CSDM e a CA com vinte e quatro horas de antecedência para informá-los sobre o trabalho de acesso raiz que você pretende realizar.

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.

Gerenciamento de segurança no AMS Accelerate

O AWS Managed Services usa vários controles para proteger seus ativos de informação e ajudar você a manter sua AWS infraestrutura segura. O AMS Accelerate mantém uma biblioteca de Regras do AWS Config ações de remediação para garantir que todas as suas contas estejam em conformidade com os padrões do setor de segurança e integridade operacional. Regras do AWS Config rastreia continuamente a alteração de configuração entre seus recursos gravados. Se uma alteração violar qualquer condição de regra, o AMS relata suas descobertas e permite que você corrija as violações automaticamente ou mediante solicitação, de acordo com a gravidade da violação. Regras do AWS Config facilitar a conformidade com os padrões estabelecidos por: o Center for Internet Security (CIS), o Cloud Security Framework (CSF) do National Institute of Standards and Technology (NIST), a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) e o Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI).

Além disso, o AMS utiliza GuardDuty a Amazon para identificar atividades potencialmente não autorizadas ou maliciosas em seu AWS ambiente. O AMS monitora GuardDuty as descobertas 24x7. A AMS colabora com você para entender o impacto das descobertas e identificar a remediação com base nas recomendações de melhores práticas. O AMS também usa o Amazon Macie para proteger seus dados confidenciais, como informações pessoais de saúde (PHI), informações de identificação pessoal (PII) e dados financeiros.

> **Note**
>
> O Amazon Macie é um serviço opcional e não está habilitado por padrão.

O AMS Accelerate fornece uma variedade de serviços operacionais para ajudá-lo a alcançar a excelência operacional em AWS. Para saber mais sobre como o AMS ajuda suas equipes a alcançar a excelência operacional geral Nuvem AWS com os principais recursos operacionais do AMS, incluindo suporte técnico 24 horas por dia, 7 dias por semana, monitoramento proativo, segurança, aplicação de patches, registro e backup, consulte Diagramas de arquitetura de referência do AMS.

Tópicos

- Use o documento Log4j SSM para descobrir ocorrências no Accelerate
- Monitoramento da segurança da infraestrutura no AMS
- Proteção de dados no Accelerate

- AWS Identity and Access Management no AMS Accelerate
- Resposta a incidentes de segurança no AMS
- Registro e monitoramento de eventos de segurança no Accelerate
- Conformidade de configuração no Accelerate
- Resposta a incidentes no Accelerate
- Resiliência em aceleração
- Controle de segurança para sistemas end-of-support operacionais
- Melhores práticas de segurança no Accelerate
- Revisões de segurança da solicitação de alteração
- Perguntas frequentes sobre segurança

Use o documento Log4j SSM para descobrir ocorrências no Accelerate

O documento Log4j (AWS Systems Manager documento SSM) ajuda você a pesquisar a biblioteca Apache Log4j2 nas cargas de trabalho ingeridas. O documento de automação fornece um relatório do ID do processo dos aplicativos Java nos quais a biblioteca Log4j2 está ativa.

O relatório inclui informações sobre os arquivos Java (arquivos JAR), encontrados no ambiente especificado que contém a JndiLookup classe. É uma prática recomendada atualizar as bibliotecas descobertas para a versão mais recente disponível. Essa atualização atenua a Execução Remota de Código (RCE) identificada por meio do CVE-2021-44228. Baixe a versão mais recente da biblioteca Log4j do Apache. Para obter mais informações, consulte Baixar o Apache Log4j 2.

O documento é compartilhado com todas as regiões integradas ao Accelerate,. Para acessar o documento, conclua as seguintes etapas:

1. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, escolha Documents.
3. Escolha Compartilhado comigo.
4. Na caixa de pesquisa, insira AWSManagedServices-GatherLog4jInformation.
5. Use o controle de taxa para executar o documento em grande escala.

O documento AWSManagedServices-GatherLog 4JInformation reúne os seguintes parâmetros:

- InstanceId: (Obrigatório) ID da sua EC2 instância.
- S3Bucket: (Opcional) O URL pré-assinado do S3 ou o URI do S3 (s3://BUCKET_NAME) para o qual carregar os resultados.
- AutomationAssumeRole: (Obrigatório) O ARN da função que permite que a automação execute ações em seu nome.

É uma prática recomendada executar este documento usando o controle de taxa. Você pode definir o parâmetro de controle de taxa como o. InstanceIde atribuir uma lista de instâncias a ele ou aplicar uma combinação de tag-chave para atingir todas as EC2 instâncias que têm uma determinada tag. O AWS Managed Services também recomenda que você forneça um bucket do Amazon Simple Storage Service (Amazon S3) para fazer o upload dos resultados, para que você possa criar um relatório a partir dos dados armazenados no S3. Para ver um exemplo de como agregar os resultados no S3, consulte EC2 Instance Stack | Gather Log4j Information.

Se você não conseguir atualizar o pacote, siga as diretrizes descritas em AWS Segurança em Usando serviços de AWS segurança para proteger, detectar e responder à vulnerabilidade do Log4j. Para mitigar vulnerabilidades removendo a funcionalidade da JndiLookup classe, execute o hot patch Log4j em linha com seus aplicativos Java. Para obter mais informações sobre o hot patch, consulte Hotpatch para Apache Log4j.

Em caso de dúvidas sobre o resultado da automação ou sobre como proceder com mitigações adicionais, envie uma solicitação de serviço.

Monitoramento da segurança da infraestrutura no AMS

Quando você se integra ao AMS Accelerate, AWS implanta a seguinte infraestrutura AWS Config básica e o conjunto de regras, o AMS Accelerate usa essas regras para monitorar suas contas.

- AWS Config função vinculada ao serviço: o AMS Accelerate implanta a função vinculada ao serviço chamada AWSServiceRoleForConfig, que é usada AWS Config para consultar o status de outros serviços. AWS A função AWSServiceRoleForConfigvinculada ao serviço confia no AWS Config serviço para assumir a função. A política de permissões para a AWSServiceRoleForConfigfunção contém permissões somente leitura e somente gravação em recursos e permissões somente leitura para AWS Config recursos em outros serviços que oferecem suporte. AWS Config Se você já tem uma função configurada com o AWS Config Recorder, o AMS Accelerate valida se a função existente tem uma política gerenciada do AWS

Config anexada. Caso contrário, o AMS Accelerate substitui a função pela função vinculada ao serviço. AWSServiceRoleForConfig

- AWS Config gravador e canal de entrega: AWS Config usa o gravador de configuração para detectar alterações em suas configurações de recursos e capturar essas alterações como itens de configuração. O AMS Accelerate implanta o gravador de configuração em todos os serviços Regiões da AWS, com gravação contínua de todos os recursos. O AMS Accelerate também cria o canal de entrega de configuração, um bucket do Amazon S3, que é usado para registrar as alterações que ocorrem em AWS seus recursos. O gravador de configuração atualiza os estados de configuração por meio do canal de entrega. O gravador de configuração e o canal de entrega são necessários AWS Config para funcionar. O AMS Accelerate cria o gravador em tudo Regiões da AWS e um canal de entrega em um único Região da AWS. Se você já tem um gravador e um canal de entrega em um Região da AWS, o AMS Accelerate não exclui os AWS Config recursos existentes. Em vez disso, o AMS Accelerate usa seu gravador e canal de entrega existentes depois de validar se eles estão configurados corretamente. Para obter mais informações sobre como reduzir AWS Config custos, consulteReduza AWS Config custos no Accelerate.
- AWS Config regras: O AMS Accelerate mantém uma biblioteca de Regras do AWS Config ações de remediação para ajudá-lo a cumprir os padrões do setor de segurança e integridade operacional. Regras do AWS Config rastreia continuamente as alterações de configuração entre seus recursos registrados. Se uma alteração violar qualquer condição de regra, o AMS relata suas descobertas e permite que você corrija as violações automaticamente ou mediante solicitação, de acordo com a gravidade da violação. Regras do AWS Config facilitar a conformidade com os padrões estabelecidos por: o Center for Internet Security (CIS), o Cloud Security Framework (CSF) do National Institute of Standards and Technology (NIST), a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) e o Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI).
- AWS Config autorização de agregador: um agregador é um tipo de AWS Config recurso que coleta dados de AWS Config configuração e conformidade de várias contas e várias regiões. O AMS Accelerate integra sua conta a um agregador de configuração a partir do qual o AMS Accelerate agrega as informações de configuração de recursos da sua conta e os dados de conformidade de configuração e gera o relatório de conformidade. Se houver agregadores existentes configurados na conta de propriedade da AMS, o AMS Accelerate implanta um agregador adicional e o agregador existente não será modificado.

> **Note**
>
> O agregador Config não está configurado em suas contas; em vez disso, ele está configurado em contas de propriedade da AMS e suas contas são integradas a ele.

Para saber mais sobre AWS Config, consulte:

- AWS Config: O que é Config?
- Regras do AWS Config: Avaliando recursos com regras
- Regras do AWS Config: Verificação dinâmica de conformidade: Regras do AWS Config — Verificação dinâmica de conformidade para recursos de nuvem
- AWS Config Agregador: agregação de dados multirregional de várias contas

Para obter informações sobre relatórios, consulteAWS Config Relatório de conformidade de controle.

Usando funções vinculadas a serviços para o AMS Accelerate

O AMS Accelerate usa AWS Identity and Access Management funções vinculadas a serviços (IAM). Uma função vinculada ao serviço (SLR) é um tipo exclusivo de função do IAM vinculada diretamente ao AMS Accelerate. As funções vinculadas ao serviço são predefinidas pelo AMS Accelerate e incluem todas as permissões que o serviço exige para ligar para outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração do AMS Accelerate porque você não precisa adicionar manualmente as permissões necessárias. O AMS Accelerate define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, somente o AMS Accelerate pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte AWS Serviços que funcionam com IAM e procure os serviços que têm Sim na coluna Funções vinculadas ao serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

Função vinculada ao serviço do kit de ferramentas de implantação para o AMS Accelerate

O AMS Accelerate usa a função vinculada ao serviço (SLR) chamada AWSServiceRoleForAWSManagedServicesDeploymentToolkit— essa função implanta a infraestrutura do AMS Accelerate nas contas dos clientes.

> **Note**
>
> Esta política foi atualizada recentemente; para obter detalhes, consulteAcelere as atualizações de funções vinculadas a serviços.

Kit de ferramentas de implantação do AMS Accelerate SLR

A função AWSService RoleFor AWSManaged ServicesDeploymentToolkit vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `deploymenttoolkit.managedservices.amazonaws.com`

A política nomeada AWSManagedServicesDeploymentToolkitPolicypermite que o AMS Accelerate execute ações nos seguintes recursos:

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

Essa SLR concede ao Amazon S3 permissões para criar e gerenciar o bucket de implantação usado pelo AMS para carregar recursos, CloudFormation como modelos ou pacotes de ativos Lambda, na conta para implantações de componentes. Essa SLR concede CloudFormation permissões para implantar a CloudFormation pilha que define os buckets de implantação. Para obter detalhes ou fazer o download da política, consulte AWSManagedServices_DeploymentToolkitPolicy.

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 ter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Criação de um kit de ferramentas de implantação SLR para o AMS Accelerate

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você se integra ao AMS na Console de gerenciamento da AWS, na ou na AWS API AWS CLI, o AMS Accelerate 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 Accelerate antes de 09 de junho de 2022, quando ele começou a oferecer suporte a funções vinculadas ao serviço. Depois, o AMS Accelerate criou a AWSService RoleFor AWSManaged ServicesDeploymentToolkit 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 Accelerate cria a função vinculada ao serviço para você novamente.

Editando um kit de ferramentas de implantação SLR para AMS Accelerate

O AMS Accelerate não permite que você edite a função AWSService RoleFor AWSManaged ServicesDeploymentToolkit 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 um kit de ferramentas de implantação SLR para AMS Accelerate

Você não precisa excluir manualmente a AWSService RoleFor AWSManaged ServicesDeploymentToolkit função. Quando você desconecta do AMS na Console de gerenciamento da AWS, na ou na AWS API AWS CLI, o AMS Accelerate 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 Accelerate 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 os recursos do AMS Accelerate usados pela função vinculada ao AWSService RoleFor AWSManaged ServicesDeploymentToolkit serviço

Exclua a `ams-cdk-toolkit` pilha de todas as regiões às quais sua conta foi integrada no AMS (talvez seja necessário esvaziar manualmente os buckets do S3 primeiro).

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 AWSService RoleFor AWSManaged ServicesDeploymentToolkit vinculada ao serviço. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Detective controla a função vinculada ao serviço do AMS Accelerate

O AMS Accelerate usa a função vinculada ao serviço (SLR) chamada AWSServiceRoleForManagedServices_DetectiveControlsConfig— O AWS Managed Services usa essa função vinculada ao serviço para implantar gravador de configuração, regras de configuração e controles de detetive de bucket do S3.

A seguinte política gerenciada está AWSServiceRoleForManagedServices_DetectiveControlsConfiganexada à função vinculada ao serviço: AWSManagedServices_DetectiveControlsConfig _. ServiceRolePolicy Para obter atualizações dessa política, consulte Acelere as atualizações das políticas AWS gerenciadas.

Permissões para controles de detetive SLR para AMS Accelerate

A função AWSServiceRoleForManagedServices_DetectiveControlsConfig vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `detectivecontrols.managedservices.amazonaws.com`

Anexada a essa função está a política `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS

gerenciada (consulte AWS política gerenciada: AWSManagedServices_DetectiveControlsConfig _ ServiceRolePolicy O serviço usa a função para criar a configuração do AMS Detective Controls em sua conta), o que requer a implantação de recursos como buckets s3, regras de configuração e um agregador. Você deve configurar permissões para permitir que uma entidade do IAM (como um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de função vinculadas ao serviço no Guia do usuário do AWS Identity and Access Management.

Criando uma SLR de controle de detetive para o AMS Accelerate

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você se integra ao AMS na Console de gerenciamento da AWS, na ou na AWS API AWS CLI, o AMS Accelerate 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 Accelerate antes de 09 de junho de 2022, quando ele começou a oferecer suporte a funções vinculadas ao serviço e, em seguida, o AMS Accelerate criou a AWSServiceRoleForManagedServices_DetectiveControlsConfig 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 Accelerate cria a função vinculada ao serviço para você novamente.

Editando uma SLR de controles de detetive para AMS Accelerate

O AMS Accelerate não permite que você edite a função AWSServiceRoleForManagedServices_DetectiveControlsConfig 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 uma função vinculada a serviço no Guia do usuário do IAM.

Excluindo uma SLR de controles de detetive para AMS Accelerate

Você não precisa excluir manualmente a AWSServiceRoleForManagedServices_DetectiveControlsConfig função. Quando você desconecta do

AMS na Console de gerenciamento da AWS, na ou na AWS API AWS CLI, o AMS Accelerate 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 Accelerate 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 os recursos do AMS Accelerate usados pela função vinculada ao AWSServiceRoleForManagedServices_DetectiveControlsConfig serviço

`ams-detective-controls-config-recorder`Exclua `ams-detective-controls-config-rules-cdk` e `ams-detective-controls-infrastructure-cdk` acumule pilhas de todas as regiões às quais sua conta foi integrada no AMS (talvez seja necessário esvaziar manualmente os buckets do S3 primeiro).

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_DetectiveControlsConfig vinculada ao serviço. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Função vinculada ao serviço de EventBridge regras da Amazon para o AMS Accelerate

O AMS Accelerate usa a função vinculada ao serviço (SLR) chamada. AWSServiceRoleForManagedServices_Events Essa função confia em um dos diretores de serviços do AWS Managed Services (events.managedservices.amazonaws.com) para assumir a função para você. O serviço usa a função para criar a regra EventBridge gerenciada pela Amazon. Essa regra é a infraestrutura necessária em sua conta da AWS para entregar informações de alteração do estado de alarme da sua conta para o AWS Managed Services.

Permissões para EventBridge SLR for AMS Accelerate

A função AWSServiceRoleForManagedServices_Events vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `events.managedservices.amazonaws.com`

A política `AWSManagedServices_EventsServiceRolePolicy` AWS gerenciada está anexada a essa função (consulteAWS política gerenciada: AWSManagedServices_EventsServiceRolePolicy). O serviço usa a função para fornecer informações de alteração do estado do alarme da sua conta para o AMS. 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 da função vinculada ao serviço no Guia do usuário do AWS Identity and Access Management .

Você pode baixar o JSON AWSManagedServices_EventsServiceRolePolicy neste ZIP: EventsServiceRolePolicy.zip.

Criação de uma EventBridge SLR para o AMS Accelerate

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você se integra ao AMS na Console de gerenciamento da AWS, na ou na AWS API AWS CLI, o AMS Accelerate 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 Accelerate antes de 7 de fevereiro de 2023, quando 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 Accelerate cria a função vinculada ao serviço para você novamente.

Editando uma EventBridge SLR para o AMS Accelerate

O AMS Accelerate 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 Accelerate

Você não precisa excluir manualmente a AWSServiceRoleForManagedServices_Events função. Quando você desconecta do AMS na Console de gerenciamento da AWS, na ou na AWS API AWS CLI, o AMS Accelerate 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 Accelerate 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 os recursos do AMS Accelerate 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.

Função vinculada ao serviço de contatos do AMS Accelerate

O AMS Accelerate usa a função vinculada ao serviço (SLR) chamada AWSServiceRoleForManagedServices_Contacts— Essa função facilita as notificações automatizadas quando ocorrem incidentes, permitindo que o serviço leia as tags existentes do recurso afetado e recupere o e-mail configurado do ponto de contato apropriado.

Esse é o único serviço que usa essa função vinculada ao serviço.

Anexada à função AWSServiceRoleForManagedServices_Contactsvinculada ao serviço está a seguinte política gerenciada:. AWSManagedServices_ContactsServiceRolePolicy Para obter atualizações dessa política, consulte Acelere as atualizações das políticas AWS gerenciadas.

Permissões para contatos SLR para AMS Accelerate

A função AWSServiceRoleForManagedServices_Contacts vinculada ao serviço confia nos seguintes serviços para assumir a função:

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

Anexada a essa função está a política gerenciada da `AWSManagedServices_ContactsServiceRolePolicy` AWS (consulteAWS política gerenciada: AWSManagedServices_ContactsServiceRolePolicy). O serviço usa a função para ler as tags em qualquer AWS recurso e encontrar o e-mail contido na tag, do ponto de contato apropriado para quando ocorrerem incidentes. Essa função facilita as notificações automatizadas quando ocorrem incidentes, permitindo que o AMS leia essa tag em um recurso afetado e recupere o e-mail. Para obter mais informações, consulte Permissões de função vinculadas ao serviço no Guia do usuário do AWS Identity and Access Management.

> **Important**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. O AMS usa tags para fornecer serviços administrativos. As tags não devem ser usadas para dados privados ou confidenciais.

A política de permissões de função nomeada AWSManagedServices_ContactsServiceRolePolicy permite que o AMS Accelerate conclua as seguintes ações nos recursos especificados:

- Ação: permite que o Serviço de Contatos leia as tags especificamente configuradas para conter o e-mail para que o AMS envie notificações de incidentes em qualquer recurso da AWS.

Você pode baixar o JSON AWSManagedServices_ContactsServiceRolePolicy neste ZIP: ContactsServicePolicy.zip.

Criando uma SLR de contatos para o AMS Accelerate

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você se integra ao AMS na Console de gerenciamento da AWS, na ou na AWS API AWS CLI, o AMS Accelerate 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 Accelerate antes de 16 de fevereiro de 2023, quando começou a oferecer suporte a funções vinculadas ao serviço e, em seguida, o AMS Accelerate criou a AWSServiceRoleForManagedServices_Contacts 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 Accelerate cria a função vinculada ao serviço para você novamente.

Editando uma SLR de contatos para o AMS Accelerate

O AMS Accelerate não permite que você edite a função AWSServiceRoleForManagedServices_Contacts 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 SLR de contatos para o AMS Accelerate

Você não precisa excluir manualmente a AWSServiceRoleForManagedServices_Contacts função. Quando você desconecta do AMS na Console de gerenciamento da AWS, na ou na AWS API AWS CLI, o AMS Accelerate 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 Accelerate 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 os recursos do AMS Accelerate usados pela função vinculada ao AWSServiceRoleForManagedServices_Contacts 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_Contacts vinculada ao serviço. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas pelas funções vinculadas ao serviço do AMS Accelerate

O AMS Accelerate oferece suporte ao uso de funções vinculadas a serviços em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints da AWS.

Acelere as atualizações de funções vinculadas a serviços

Veja detalhes sobre as atualizações das funções vinculadas ao serviço do Accelerate desde que esse serviço começou a monitorar essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na Histórico de documentos do Guia do usuário do AMS Accelerate página Accelerate.

Alteração	Descrição	Data

Política atualizada — Kit de ferramentas de implantação	• Essas novas permissões foram adicionadas para o recurso `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		4 de abril de 2024

Alteração	Descrição	Data

Política atualizada — Kit de ferramentas de implantação	• Essas novas permissões foram adicionadas para o recurso `arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*` :
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
	• Essas novas permissões foram adicionadas para o recurso `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :
	`ecr:CreateRepository`
	`ecr:DeleteLifecyclePolicy`
	`ecr:DeleteRepository`
	`ecr:DeleteRepositoryPolicy`
	`ecr:DescribeRepositories`
	`ecr:GetLifecyclePolicy`
	`ecr:ListTagsForResource`
	`ecr:PutImageTagMutability`
	`ecr:PutLifecyclePolicy`
	`ecr:SetRepositoryPolicy`
	`ecr:TagResource`
	`ecr:UntagResource`
	• Além disso, algumas ações existentes com caracteres curinga foram reduzidas a ações individuais:
	`- s3:DeleteObject*`
	`+ s3:DeleteObject`
	`+ s3:DeleteObjectTagging`
	`+ s3:DeleteObjectVersion`
	`+ s3:DeleteObjectVersionTagging`
	
	`- s3:GetObject*`
	`+ s3:GetObject`
	`+ s3:GetObjectAcl`
	`+ s3:GetObjectAttributes`
		09 de maio de 2023

Alteração	Descrição	Data

	<pre>+ s3:GetObjectLegalHold
	+ s3:GetObjectRetention
	+ s3:GetObjectTagging
	+ s3:GetObjectVersion
	+ s3:GetObjectVersionAcl
	+ s3:GetObjectVersionAttributes
	+ s3:GetObjectVersionForReplication
	+ s3:GetObjectVersionTagging
	+ s3:GetObjectVersionTorrent
	
	- cloudformation:UpdateTermination*
	+ cloudformation:UpdateTerminationProt
	ection</pre>	

Política atualizada — Detective Controls	• As CloudFormation ações foram ampliadas ainda mais após a confirmação com a equipe de segurança e acesso • As ações do Lambda foram removidas da política porque não afetam o embarque onboarding/off	10 de abril de 2023
Política atualizada — Detective Controls	Atualizou a política e adicionou a política de limite de permissões.	21 de março de 2023
Nova função vinculada ao serviço — Contacts SLR	O Accelerate adicionou uma nova função vinculada ao serviço de Contatos. Essa função facilita as notificações automatizadas quando ocorrem incidentes, permitindo que o serviço leia as tags existentes do recurso afetado e recupere o e-mail configurado do ponto de contato apropriado.	16 de fevereiro de 2023

Alteração	Descrição	Data
Nova função vinculada ao serviço — EventBridge	O Accelerate adicionou uma nova função vinculada a serviços para uma regra da Amazon EventBridge . Essa função confia em um dos diretores de serviços do AWS Managed Services (events.managedservices.amazonaws.com) para assumir a função para você. O serviço usa a função para criar a regra EventBridge gerenciada pela Amazon. Essa regra é a infraestrutura necessária em sua conta da AWS para entregar informações de alteração do estado de alarme da sua conta para o AWS Managed Services.	7 de fevereiro de 2023
Função vinculada ao serviço atualizada — Kit de ferramentas de implantação	Acelere a atualização AWSService RoleFor AWSManaged ServicesDeploymentToolkit com as novas permissões do S3. Essas novas permissões foram adicionadas: `"s3:GetLifecycleConfiguration", "s3:GetBucketLogging", "s3:ListBucket", "s3:GetBucketVersioning", "s3:PutLifecycleConfiguration", "s3:GetBucketLocation", "s3:GetObject*"`	30 de janeiro de 2023
Acelere o início do rastreamento de alterações	A Accelerate começou a monitorar as mudanças em suas funções vinculadas a serviços.	30 de novembro de 2022
Nova função vinculada a serviços — Detective Controls	O Accelerate adicionou uma nova função vinculada ao serviço para implantar os controles de detetive do Accelerate. O AWS Managed Services usa essa função vinculada ao serviço para implantar gravador de configuração, regras de configuração e controles de detetive de bucket do S3.	13 de outubro de 2022

Alteração	Descrição	Data
Nova função vinculada ao serviço — Kit de ferramentas de implantação	O Accelerate adicionou uma nova função vinculada a serviços para implantar a infraestrutura do Accelerate. essa função implanta a infraestrutura do AMS Accelerate nas contas dos clientes.	9 de junho de 2022

AWS políticas gerenciadas para o AMS Accelerate

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

Para obter uma tabela de alterações, consulteAcelere as atualizações das políticas AWS gerenciadas.

AWS política gerenciada: AWSManagedServices_AlarmManagerPermissionsBoundary

AWS Managed Services (AMS) usa a política `AWSManagedServices_AlarmManagerPermissionsBoundary` AWS gerenciada. Essa política AWS gerenciada é usada no AWSManagedServices_AlarmManager _ ServiceRolePolicy para restringir as permissões das funções do IAM criadas por AWSServiceRoleForManagedServices_AlarmManager.

Essa política concede funções do IAM criadas como parte deComo funciona o Gerenciador de alarmes, permissões para realizar operações como avaliação de AWS configuração, leitura de configuração para buscar a AWS configuração do Alarm Manager e criação dos alarmes necessários da Amazon. CloudWatch

A `AWSManagedServices_AlarmManagerPermissionsBoundary` política é anexada à função `AWSServiceRoleForManagedServices_DetectiveControlsConfig` vinculada ao serviço. Para atualizações dessa função, consulteAcelere as atualizações de funções vinculadas a serviços.

É possível anexar essa política às suas identidades do IAM.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `AWS Config`— Permite permissões para avaliar as regras de configuração e selecionar a configuração do recurso.
- `AWS AppConfig`— Permite permissões para buscar a AlarmManager configuração.
- `Amazon S3`— Permite permissões para operar AlarmManager buckets e objetos.
- `Amazon CloudWatch`— Permite permissões para ler e colocar alarmes e métricas AlarmManager gerenciados.
- `AWS Resource Groups and Tags`— Permite permissões para ler tags de recursos.
- `Amazon EC2`— Permite permissões para ler EC2 recursos da Amazon.
- `Amazon Redshift`— Permite permissões para ler instâncias e clusters do Redshift.
- `Amazon FSx`— Permite permissões para descrever sistemas de arquivos, volumes e tags de recursos.
- `Amazon CloudWatch Synthetics`— Permite permissões para ler recursos do Synthetics.
- `Amazon Elastic Kubernetes Service`— Permite permissões para descrever o cluster Amazon EKS.
- `Amazon ElastiCache`— Permite permissões para descrever recursos.

Você pode baixar o arquivo de política neste ZIP: RecommendedPermissionBoundary.zip.

AWS política gerenciada: AWSManagedServices_DetectiveControlsConfig _ ServiceRolePolicy

AWS Managed Services (AMS) usa a política `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS gerenciada. Essa política AWS gerenciada é anexada à [função `AWSServiceRoleForManagedServices_DetectiveControlsConfig` vinculada ao serviço](#) (consulte). [Detective controla a função vinculada ao serviço do AMS Accelerate](#) Para atualizações da função `AWSServiceRoleForManagedServices_DetectiveControlsConfig` vinculada ao serviço, consulte. [Acelere as atualizações de funções vinculadas a serviços](#)

A política permite que a função vinculada ao serviço realize ações em seu nome.

Você pode anexar a ServiceRolePolicy política AWSManagedServices_DetectiveControlsConfig _ às suas entidades do IAM.

Para obter mais informações, consulte [Usando funções vinculadas a serviços para o AMS Accelerate](#).

Detalhes das permissões

Essa política tem as seguintes permissões para permitir que o AWS Managed Services Detective Controls implante e configure todos os recursos necessários.

- `CloudFormation`— Permite que o AMS Detective Controls implante CloudFormation pilhas com recursos como buckets s3, regras de configuração e gravador de configuração.
- `AWS Config`— Permite que o AMS Detective Controls crie regras de configuração do AMS, configure um agregador e marque recursos.
- `Amazon S3`— permite que o AMS Detective Controls gerencie seus buckets s3.

Você pode baixar o arquivo de política JSON neste ZIP: [DetectiveControlsConfig_ ServiceRolePolicy .zip](#).

AWS política gerenciada: AWSManaged ServicesDeploymentToolkitPolicy

AWS Managed Services (AMS) usa a política `AWSManagedServicesDeploymentToolkitPolicy` AWS gerenciada. Essa política AWS gerenciada é anexada à [função `AWSServiceRoleForAWSManagedServicesDeploymentToolkit` vinculada ao serviço](#)

(consulte). Função vinculada ao serviço do kit de ferramentas de implantação para o AMS Accelerate A política permite que a função vinculada ao serviço realize ações em seu nome. Não é possível anexar essa política a suas entidades do IAM. Para obter mais informações, consulte Usando funções vinculadas a serviços para o AMS Accelerate.

Para atualizações da função `AWSServiceRoleForManagedServicesDeploymentToolkitPolicy` vinculada ao serviço, consulte. Acelere as atualizações de funções vinculadas a serviços

Detalhes das permissões

Essa política tem as seguintes permissões para permitir que o AWS Managed Services Detective Controls implante e configure todos os recursos necessários.

- `CloudFormation`— Permite que o AMS Deployment Toolkit implante pilhas CFN com os recursos do S3 exigidos pelo CDK.
- `Amazon S3`— permite que o AMS Deployment Toolkit gerencie seus buckets S3.
- `Elastic Container Registry`— permite que o AMS Deployment Toolkit gerencie seu repositório ECR, usado para implantar os ativos necessários aos aplicativos AMS CDK.

Você pode baixar o arquivo de política JSON neste ZIP: AWSManagedServicesDeploymentToolkitPolicy.zip.

AWS política gerenciada: AWSManagedServices_EventsServiceRolePolicy

AWS Managed Services (AMS) usa a política gerenciada `AWSManagedServices_EventsServiceRolePolicy` da AWS. Essa política AWS gerenciada é anexada à função vinculada ao `AWSServiceRoleForManagedServices_Eventsserviço`. A política permite que a função vinculada ao serviço realize ações em seu nome. Não é possível anexar essa política a suas entidades do IAM. Para obter mais informações, consulte Usando funções vinculadas a serviços para o AMS Accelerate.

Para atualizações da função `AWSServiceRoleForManagedServices_Events` vinculada ao serviço, consulte. Acelere as atualizações de funções vinculadas a serviços

Detalhes das permissões

Essa política tem as seguintes permissões para permitir que EventBridge a Amazon entregue informações de alteração do estado de alarme da sua conta para o AWS Managed Services.

- `events`— Permite que o Accelerate crie uma regra EventBridge gerenciada pela Amazon. Essa regra é a infraestrutura necessária Conta da AWS para fornecer informações de alteração do estado de alarme de sua conta para AWS Managed Services.

Você pode baixar o arquivo de política JSON neste ZIP: EventsServiceRolePolicy.zip.

AWS política gerenciada: AWSManagedServices_ContactsServiceRolePolicy

AWS Managed Services (AMS) usa a política gerenciada `AWSManagedServices_ContactsServiceRolePolicy` da AWS. Essa política AWS gerenciada é anexada à função `AWSServiceRoleForManagedServices_Contacts` vinculada ao serviço (consulte). Criando uma SLR de contatos para o AMS Accelerate A política permite que a SLR de contatos do AMS veja suas tags de recursos e seus valores nos recursos da AWS. Não é possível anexar essa política a suas entidades do IAM. Para obter mais informações, consulte Usando funções vinculadas a serviços para o AMS Accelerate.

> **Important**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. O AMS usa tags para fornecer serviços administrativos. As tags não devem ser usadas para dados privados ou confidenciais.

Para atualizações da função `AWSServiceRoleForManagedServices_Contacts` vinculada ao serviço, consulte. Acelere as atualizações de funções vinculadas a serviços

Detalhes das permissões

Essa política tem as seguintes permissões para permitir que a SLR de contatos leia suas tags de recursos para recuperar as informações de contato do recurso que você configurou com antecedência.

- `IAM`— Permite que o serviço de contatos veja as tags nas funções do IAM e nos usuários do IAM.
- `Amazon EC2`— Permite que o serviço de contatos veja as tags nos EC2 recursos da Amazon.
- `Amazon S3`— Permite que o Contacts Service veja as tags nos buckets do Amazon S3. Essa ação usa uma condição para garantir que o AMS acesse suas tags de bucket usando o cabeçalho de autorização HTTP, usando o protocolo de assinatura SigV4 e usando HTTPS com TLS 1.2 ou

superior. Para obter mais informações, consulte Métodos de autenticação e chaves de política específicas de autenticação do Amazon S3 Signature versão 4.

- Tag— Permite que o serviço de contatos veja as tags em outros AWS recursos.

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

Você pode baixar o arquivo de política JSON neste ZIP: ContactsServicePolicy.zip.

Acelere as atualizações das políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Accelerate desde que esse serviço começou a monitorar essas alterações.

Alteração	Descrição	Data

Política atualizada — Kit de ferramentas de implantação	• Essas novas permissões foram adicionadas para o recursoarn:aws:ecr:*:*:repository/ams-cdktoolkit* :
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		4 de abril de 2024

Política atualizada — Kit de ferramentas de implantação	• Essas novas permissões foram adicionadas para o recursoarn:aws:cloudformation:*:*:stack/ams-cdk-toolkit* :
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
	• Essas novas permissões foram adicionadas para o recursoarn:aws:ecr:*:*:repository/ams-cdktoolkit* :
		9 de maio de 2023

Alteração	Descrição	Data

	<pre>ecr:CreateRepository
	
	ecr:DeleteLifecyclePolicy
	ecr:DeleteRepository
	ecr:DeleteRepositoryPolicy
	ecr:DescribeRepositories
	ecr:GetLifecyclePolicy
	ecr:ListTagsForResource
	ecr:PutImageTagMutability
	ecr:PutLifecyclePolicy
	ecr:SetRepositoryPolicy
	ecr:TagResource
	ecr:UntagResource</pre>	

	• Além disso, algumas ações existentes com caracteres curinga foram reduzidas a ações individuais:
	<pre>- s3:DeleteObject*
	
	+ s3:DeleteObject
	+ s3:DeleteObjectTagging
	+ s3:DeleteObjectVersion
	+ s3:DeleteObjectVersionTagging
	
	- s3:GetObject*
	+ s3:GetObject
	+ s3:GetObjectAcl
	+ s3:GetObjectAttributes
	+ s3:GetObjectLegalHold
	+ s3:GetObjectRetention
	+ s3:GetObjectTagging
	+ s3:GetObjectVersion
	+ s3:GetObjectVersionAcl
	+ s3:GetObjectVersionAttributes
	+ s3:GetObjectVersionForReplication
	+ s3:GetObjectVersionTagging
	+ s3:GetObjectVersionTorrent
	
	- cloudformation:UpdateTermination*</pre>	

Alteração	Descrição	Data
	`+ cloudformation:UpdateTerminationProtection`	
Política atualizada — Detective Controls	• As CloudFormation ações foram ampliadas ainda mais após a confirmação com a equipe de segurança e acesso • As ações do Lambda foram removidas da política porque não afetam o embarque onboarding/off	10 de abril de 2023
Política atualizada — Detective Controls	A `ListAttachedRolePolicies` ação é removida da política. A ação tinha Recurso como curinga (*). Como a “lista” é uma ação não mutativa, ela tem acesso a todos os recursos e o curinga não é permitido.	28 de março de 2023
Política atualizada — Detective Controls	Atualizou a política e adicionou a política de limite de permissões.	21 de março de 2023
Nova política — Serviço de contatos	O Accelerate adicionou uma nova política para analisar as informações de contato da sua conta a partir das tags de recursos. O Accelerate adicionou uma nova política para ler suas tags de recursos para que possa recuperar as informaçõ es de contato do recurso que você configurou com antecedência.	16 de fevereiro de 2023
Nova política — Serviço de Eventos	A Accelerate adicionou uma nova política para fornecer informações de alteração do estado de alarme da sua conta para o AWS Managed Services. Concede funções do IAM criadas como parte das Como funciona o Gerenciador de alarmes permissões para criar uma regra EventBridge gerenciada necessária pela Amazon.	07 de fevereiro de 2023

Alteração	Descrição	Data
Política atualizada — Kit de ferramentas de implantação	Foram adicionadas permissões do S3 para apoiar a saída de clientes do Accelerate.	30 de janeiro de 2023
Nova política — Detective Controls	Permite que a função vinculada ao serviço,Detective controla a função vinculada ao serviço do AMS Accelerate, conclua ações para que você implante os controles de detetive do Accelerate.	19 de dezembro de 2022
Nova política — Gerenciador de alarmes	O Accelerate adicionou uma nova política para permitir permissões para realizar tarefas do gerenciador de alarmes. Concede funções do IAM criadas como parte das Como funciona o Gerenciador de alarmes permissões para realizar operações como avaliação do AWS Config, leitura do AWS Config para obter a configuração do gerenciador de alarmes e criação dos alarmes necessários da Amazon. CloudWatch	30 de novembro de 2022
Acelere o início do rastreamento de alterações	A Accelerate começou a monitorar as mudanças em suas políticas AWS gerenciadas.	30 de novembro de 2022
Nova política — Kit de ferramentas de implantação	O Accelerate adicionou essa política para tarefas de implantação. Concede à função vinculada ao serviço AWSServiceRoleForAWSManagedServicesDeploymentToolkitpermissões para acessar e atualizar buckets e pilhas do Amazon S3 relacionados à implantação. CloudFormation	9 de junho de 2022

Proteção de dados no Accelerate

O AMS Accelerate utiliza ferramentas e processos nativos GuardDuty, Serviços da AWS como Amazon, Amazon Macie (opcionalmente) e outras ferramentas e processos proprietários internos, para monitorar continuamente suas contas gerenciadas. Depois que um alarme é acionado, o AMS Accelerate assume a responsabilidade pela triagem inicial e pela resposta ao alarme. Os processos de resposta do AMS são baseados nos padrões do NIST. O AMS Accelerate testa regularmente os 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 Accelerate detecta uma violação ou ameaça iminente de violação de suas políticas de AWS segurança, o Accelerate coleta informações, incluindo recursos afetados e quaisquer alterações relacionadas à configuração. O AMS Accelerate fornece follow-the-sun suporte 24 horas por dia, 7 dias por semana, 365 dias por ano, com operadores dedicados que analisam e investigam ativamente painéis de monitoramento, filas de incidentes e solicitações de serviço em todas as suas contas gerenciadas. O Accelerate investiga as descobertas com especialistas internos em segurança para analisar a atividade e notificá-lo por meio dos contatos de escalonamento de segurança listados em sua conta.

Com base nas descobertas, o Accelerate interage proativamente com você. Se você achar que a atividade não é autorizada ou suspeita, a AMS trabalha com você para investigar, corrigir ou conter o problema. Há certos tipos de descoberta gerados por GuardDuty que exigem que você confirme o impacto antes que o Accelerate execute qualquer ação. Por exemplo, o tipo de GuardDuty descoberta UnauthorizedAccess:IAMUser/ConsoleLoginindica 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.

Monitore com o Amazon Macie

O AMS Accelerate oferece suporte ao Amazon Macie, e é uma prática recomendada de usar, para detectar uma lista grande e abrangente de dados confidenciais, como informações pessoais de saúde (PHI), informações de identificação pessoal (PII) e dados financeiros.

Você pode configurar o Macie para ser executado periodicamente em qualquer bucket do Amazon S3. Isso automatiza a avaliação de objetos novos ou modificados em um bucket ao longo do tempo. À medida que as descobertas de segurança são geradas, o AMS notifica você e trabalha com você para corrigir as descobertas conforme necessário.

Para obter mais informações, consulte Análise das descobertas do Amazon Macie.

Monitor com 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. AWS Isso pode incluir problemas como escalonamento de privilégios, uso de credenciais expostas ou comunicação com endereços IP ou domínios maliciosos. GuardDuty monitora o comportamento de Conta da AWS acesso em busca de sinais de comprometimento, como implantações de infraestrutura não autorizadas, instâncias implantadas em uma AWS região que você nunca usou. GuardDuty também detecta chamadas de API incomuns, como uma alteração na política de senha para reduzir a força da senha. Para obter mais informações, consulte o Guia do usuário do GuardDuty .

Para visualizar e analisar suas GuardDuty descobertas, conclua as seguintes etapas:

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Escolha Descobertas e, em seguida, selecione 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.

Use regras de GuardDuty supressão para filtrar descobertas

Uma regra de supressão é um conjunto de critérios que consiste em um atributo de filtro emparelhado com um valor. Você pode usar regras de supressão para filtrar descobertas de baixo valor sobre as quais você não pretende agir, como descobertas falsas positivas ou atividades conhecidas. Filtrar suas descobertas ajuda a facilitar o reconhecimento das ameaças à segurança que podem ter o maior impacto em seu ambiente.

Para filtrar as descobertas, as regras de supressão arquivam automaticamente as novas descobertas que correspondam aos critérios especificados. As descobertas arquivadas não são enviadas para o AWS Security Hub, Amazon S3 ou Events. CloudTrail Portanto, os filtros de supressão reduzem os dados não acionáveis se você consumir GuardDuty descobertas por meio do Security Hub ou de um aplicativo de emissão de alertas e tickets SIEM de terceiros.

O AMS tem um conjunto definido de critérios para identificar regras de supressão para suas contas gerenciadas. Quando uma conta gerenciada atende a esses critérios, o AMS aplica os filtros e cria uma solicitação de serviço (SR) para você que detalha o filtro de supressão implantado.

Você pode se comunicar com o AMS por meio de um SR para modificar ou reverter os filtros de supressão.

Veja as descobertas arquivadas

GuardDuty continua gerando descobertas mesmo quando essas descobertas correspondem às suas regras de supressão. As descobertas suprimidas são marcadas como arquivadas. GuardDuty armazena a descoberta arquivada por 90 dias. Você pode visualizar as descobertas arquivadas no GuardDuty console durante esses 90 dias selecionando Arquivado na tabela de descobertas. Ou visualize as descobertas arquivadas por meio da GuardDuty API usando a ListFindingsAPI com um FindingCriteria de service.archived igual a true.

Casos de uso comuns para regras de supressão

Veja a seguir os tipos de descoberta em casos de uso comuns para aplicar regras de supressão:

- Recon: EC2 /Portscan: use uma regra de supressão para arquivar automaticamente as descobertas ao usar um scanner de vulnerabilidade autorizado.
- UnauthorizedAccess:EC2/SSHBruteForce: use uma regra de supressão para arquivar automaticamente as descobertas quando elas forem direcionadas a instâncias do Bastion.
- Recon:EC2/PortProbeUnprotectedPort: Use uma regra de supressão para arquivar automaticamente as descobertas quando elas forem direcionadas a instâncias expostas intencionalmente.

Monitore com o Amazon Route 53 Resolver DNS Firewall

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 grupos e regras 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 serviço.

Criptografia de dados no AMS Accelerate

O AMS Accelerate usa vários Serviços da AWS para criptografia de dados.

O Amazon Simple Storage Service oferece várias opções de criptografia de objetos que protegem 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.

AWS Identity and Access Management no AMS Accelerate

AWS Identity and Access Management 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 Accelerate, você é responsável por criar funções de administrador do IAM entre contas em cada uma de suas contas gerenciadas.

No AMS Accelerate, você é responsável por gerenciar o acesso aos seus recursos subjacentes Contas da AWS e aos deles, como soluções de gerenciamento de acesso, políticas de acesso e processos relacionados. Isso significa que você gerencia o ciclo de vida do usuário, as permissões nos serviços de diretório e o sistema de autenticação federada para acessar o AWS console ou. AWS APIs Para ajudá-lo a gerenciar sua solução de acesso, o AMS Accelerate implanta AWS Config regras que detectam configurações incorretas comuns do IAM e fornece notificações de remediação. Para obter mais informações, consulte Regras gerenciadas do AWS Config.

Autenticação com identidades no AMS Accelerate

O AMS usa funções do IAM, que são um tipo de identidade do IAM. Uma função do IAM é semelhante à de um usuário, pois é uma identidade com políticas de permissões que determinam o que a identidade pode ou não fazer AWS. No entanto, uma função não tem credenciais associadas a ela e, em vez de ser associada exclusivamente a uma pessoa, pode 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. O AMS usa as seguintes funções do IAM.

> **Note**
>
> As funções de acesso do AMS permitem que os operadores do AMS acessem seus recursos para fornecer recursos do AMS (consulteService description (Descrição do serviço)). Alterar essas funções pode inibir nossa capacidade de fornecer esses recursos. Se você precisar alterar as funções de acesso ao AMS, consulte seu Cloud Architect.

Nome da função	Descrição
Usado por (entidade): somente AMS Access Service	
ams-access-management	Implantado manualmente por você durante a integração. Presumido somente pelo AMS Access para implantar ou atualizar funções de acesso. Permanece em sua conta após a integração para futuras atualizações das funções de acesso.
Usado por (entidade): AMS Operations	
ams-access-admin-operations	Essa função tem permissões administr ativas para operar em contas, mas não tem permissões para ler, gravar ou excluir conteúdo do cliente em AWS serviços comumente usados como armazenamentos de dados,

Nome da função	Descrição
	como Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift e Amazon. ElastiCache Apenas alguns poucos indivíduo s selecionados do AMS podem assumir essa função.
ams-access-operations	Essa função de operações do AMS tem permissões para realizar tarefas administr ativas em suas contas. Essa função não tem permissões de leitura, gravação ou exclusão do conteúdo do cliente em AWS serviços comumente usados como armazenamentos de dados, como Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift e Amazon. ElastiCache As permissões para realizar operações de AWS Identity and Access Management gravação também são excluídas dessa função.
ams-access-read-only	Essa função de somente leitura do AMS está limitada às permissões de somente leitura em sua conta do AMS. As permissões de leitura para o conteúdo do cliente em AWS serviços comumente usados como armazenamentos de dados, como Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift e, não são concedidas por essa função. ElastiCache
Usado por (entidade): AMS Operations e AMS Services	
função de automação ams_ssm_	Presumido por AWS Systems Manager executar documentos de automação SSM em sua conta.
função de automação ams_ssm_	

Nome da função	Descrição
Usado por (entidade): AMS Security	
ams-access-security-analyst	Essa função de segurança do AMS tem permissões em sua conta do AMS para realizar monitoramento dedicado de alertas de segurança e tratamento de incidentes de segurança. Somente algumas pessoas selecionadas da AMS Security podem assumir essa função. As permissões de leitura para o conteúdo do cliente em AWS serviços que são comumente usados como armazenamentos de dados, como Amazon S3;, Amazon RDS;, Amazon DynamoDB, Amazon Redshift e, não são concedidas por essa função. ElastiCache
ams-access-security-analyst-somente leitura	Essa função de segurança do AMS está limitada às permissões somente de leitura em sua conta do AMS para realizar monitoramento dedicado de alertas de segurança e tratament o de incidentes de segurança. As permissões de leitura para o conteúdo do cliente em AWS serviços que são comumente usados como armazenamentos de dados, como Amazon S3;, Amazon RDS;, Amazon DynamoDB, Amazon Redshift e, não são concedidas por essa função. ElastiCache
Usado por (entidade): AWS Services	
ams-access-admin	Essa função de administrador do AMS tem permissões completas para operar em contas sem restrições. Somente os serviços internos do AMS (com uma política de sessão com escopo reduzido) podem assumir a função de administrador.

Nome da função	Descrição
ams-opscenter-eventbridge-role	Presume-se EventBridge que a Amazon crie AWS Systems Manager OpsItems como parte do fluxo de trabalho de Regras do AWS Config remediação específico da AMS.
AMSOSConfigurationCustomerInstanceRole	Essa função do IAM é aplicada às suas EC2 instâncias da Amazon quando o serviço de configuração do sistema operacional do AMS descobre que as políticas necessárias do IAM estão ausentes. Ele permite que suas EC2 instâncias da Amazon interajam com AWS Systems Manager a Amazon CloudWatch e EventBridge os serviços da Amazon. Ele também anexou a política gerenciada personalizada do AMS para permitir o acesso RDP às suas instâncias do Windows.
mc-patch-glue-service-função	Assumido pelo fluxo de trabalho AWS Glue ETL para realizar a transformação de dados e prepará-los para o gerador de relatórios AMS Patch.
Usado por (entidade): Serviço AMS	
ams-alarm-manager- AWSManaged ServicesAlarmManagerDe - <8-digit hash>	Assumido pela infraestrutura do gerenciador de alarmes do AMS em sua conta AMS para realizar a Regras do AWS Config avaliação de uma nova AWS AppConfig implantação.
ams-alarm-manager- AWSManaged ServicesAlarmManagerRe - <8-digit hash>	Assumido pela infraestrutura de remediação do gerenciador de alarmes do AMS em sua conta AMS para permitir a criação ou exclusão de alarmes para remediação.

Nome da função	Descrição
ams-alarm-manager- AWSManaged ServicesAlarmManager SS- <8-digit hash>	Presumido por AWS Systems Manager invocar o serviço de remediação do gerenciador de alarmes do AMS em sua conta do AMS.
ams-alarm-manager- AWSManaged ServicesAlarmManagerTr - <8-digit hash>	Assumido pela infraestrutura do gerenciador de alarmes do AMS em sua AWS conta para realizar uma Regras do AWS Config avaliação periódica do AMS.
ams-alarm-manager- AWSManaged ServicesAlarmManagerVa - <8-digit hash>	Assumido pela infraestrutura do gerenciador de alarmes do AMS em sua conta AMS para garantir que os alarmes necessários existam na AWS conta.
ams-backup-iam-role	Essa função é usada para ser executada AWS Backup em suas contas.
monitoramento de ams- - AWSManaged ServicesLogGroupLimitLamb <8-digit hash>	Assumido pela infraestrutura de registro e monitoramento do AMS em sua conta do AMS para avaliar o limite de grupos do Amazon CloudWatch Logs e comparar com as cotas de serviço.
ams-monitoring- AWSManaged Serviços RDSMonitoring RDSE- <8-digit hash>	Assumido pela infraestrutura de registro e monitoramento do AMS em sua conta do AMS para encaminhar eventos do Amazon RDS para o Amazon CloudWatch Events.
monitoramento de ams- - AWSManaged ServicesRedshiftMonitorin <8-digit hash>	Assumido pela infraestrutura de registro e monitoramento do AMS em sua conta do AMS para encaminhar eventos do Amazon Redshift (CreateCluster e DeleteCuster) para o Amazon CloudWatch Events.

Nome da função	Descrição
ams-monitoring-infrastruc- AWSManaged ServicesMonito - <8-digit hash>	Presume-se que a infraestrutura de registro e monitoramento do AMS em sua conta do AMS publique mensagens no Amazon Simple Notification Service para validar se a conta está relatando todos os dados necessários.
ams-opscenter-role	Assumido pelo sistema de gerenciamento de notificações do AMS em sua conta AMS para gerenciar alertas AWS Systems Manager OpsItems relacionados a alertas em sua conta.
ams-opsitem-autoexecution-role	Assumido pelo sistema de gerenciamento de notificações da AMS para lidar com a remediação automatizada usando documento s SSM para monitorar alertas relacionados aos recursos em sua conta.
ams-patch-infrastructure-amspatchconfigrulero leC1- <8-digit hash>	Presumido por AWS Config avaliar os recursos de patch do AMS e detectar desvios em suas CloudFormation pilhas.
ams-patch-infrastructure-amspatchcwruleopsite mams- <8-digit hash>	Assumido pela Amazon EventBridge AWS Systems Manager OpsItems para criar falhas de correção.
ams-patch-infrastructure-amspatchser vicebusamspat- <8-digit hash>	Presume-se EventBridge que a Amazon envie um evento ao barramento de eventos do AMS Patch Orchestrator para notificações de alteração de estado do AWS Systems Manager Maintenance Windows.
ams-patch-reporting-infra-amspatch reporting configr- <8-digit hash>	Presumido por AWS Config avaliar os recursos de relatórios do AMS Patch e detectar desvios em suas CloudFormation pilhas.

Nome da função	Descrição
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Assumido pela infraestrutura do AMS Resource Tagger em sua conta AMS para realizar uma Regras do AWS Config avaliação após a nova AWS AppConfig implantação.
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Assumido pela infraestrutura do AMS Resource Tagger em sua conta AMS para validar a existência das AWS tags necessárias para os recursos gerenciados.
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Presumido por AWS Systems Manager para invocar o fluxo de trabalho de remediação do AMS Resource Tagger em sua conta AMS.
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Assumido pela infraestrutura de remediação do AMS Resource Tagger em sua conta AMS para criar ou excluir AWS tags para os recursos gerenciados.
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Assumido pela infraestrutura do AMS Resource Tagger em sua AWS conta para realizar uma avaliação periódica do AMS Config Rule.
ams_os_configuration_event_rule_role- <AWS Region>	Presume-se EventBridge que a Amazon encaminhe eventos de sua conta para o serviço de configuração do AMS OS EventBus na região correta.
mc-patch-reporting-service	Assumido pelo agregador de dados de patch e gerador de relatórios do AMS.

> **Note**
>
> Esse é o modelo para a ams-access-management função. É a pilha que os arquitetos de nuvem (CAs) implantam manualmente em sua conta na integração: management-role.yaml.

Esse é o modelo para as diferentes funções e níveis de acesso: ams-access-read-only,, ams-access-operations ams-access-admin-operations, ams-access-admin: accelerate-roles.yaml.

Para saber mais sobre identificadores AWS Cloud Development Kit (AWS CDK) (AWS CDK), incluindo hashes, consulte Exclusivo. IDs

Os serviços de recursos do AMS Accelerate assumem a ams-access-adminfunção de acesso programático à conta, mas com uma política de sessão definida para o respectivo serviço de recursos (por exemplo, patch, backup, monitoramento e assim por diante).

O AMS Accelerate segue as melhores práticas do setor para atender e manter a elegibilidade de conformidade. O acesso do AMS Accelerate à sua conta é registrado CloudTrail e também está disponível para sua análise por meio do rastreamento de alterações. Para obter informações sobre consultas que você pode usar para obter essas informações, consulteRastreando alterações em suas contas do AMS Accelerate.

Gerenciar o acesso usando políticas

Várias equipes de suporte do AMS Accelerate, como engenheiros de operações, arquitetos de nuvem e gerentes de prestação de serviços em nuvem (CSDMs), às vezes exigem acesso às suas contas para responder a solicitações e incidentes de serviço. Seu acesso é controlado por um serviço de acesso interno do AMS que impõe controles, como justificativa comercial, solicitações de serviço, itens operacionais e casos de suporte. O acesso padrão é somente leitura e todo o acesso é rastreado e registrado; consulte também. Rastreando alterações em suas contas do AMS Accelerate

Validação de recursos do IAM

O sistema de acesso do AMS Accelerate assume periodicamente funções em suas contas (pelo menos a cada 24 horas) e valida se todos os nossos recursos do IAM estão conforme o esperado.

Para proteger suas contas, o AMS Accelerate tem um “canário” que monitora e alerta sobre a presença e o status das funções do IAM, bem como suas políticas anexas, mencionadas acima. Periodicamente, o canário assume a ams-access-read-onlyfunção e inicia CloudFormation chamadas de API do IAM em suas contas. O canário avalia o status das funções de acesso do AMS Accelerate para garantir que elas estejam sempre inalteradas e. up-to-date Essa atividade cria CloudTrail registros na conta.

O nome da sessão AWS Security Token Service (AWS STS) do canário é AMS-Access-Roles-Auditor- {uuid4 ()}, conforme visto em, e as seguintes chamadas de API ocorrem: CloudTrail

- Chamadas da API Cloud Formation: `describe_stacks()`
- Chamadas de API do IAM:
  - `get_role()`
  - `list_attached_role_policies()`
  - `list_role_policies()`
  - `get_policy()`
  - `get_policy_version()`
  - `get_role_policy()`

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 (IAMEC2, 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 feeds internos da Amazon GuardDuty, do Network Traffic e do Amazon Threat Intelligence.

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. 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.

Registro e monitoramento de eventos de segurança no Accelerate

As contas inscritas no AMS Accelerate são configuradas com uma implantação básica de CloudWatch eventos e alarmes que foram otimizados para reduzir o ruído e identificar indícios de um incidente real. O AMS Accelerate também emprega GuardDuty para monitoramento de contas. Para obter mais informações, consulte Monitor com GuardDuty.

Conformidade de configuração no Accelerate

O AMS Accelerate ajuda você a configurar seus recursos de acordo com altos padrões de segurança e integridade operacional e a cumprir os seguintes padrões do setor:

- Centro de Segurança na Internet (CIS)
- Estrutura de segurança em nuvem (CSF) do Instituto Nacional de Padrões e Tecnologia (NIST)
- Health Insurance Portability and Accountability Act (HIPAA)
- Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI)

Fazemos isso implantando todo o nosso conjunto de AWS Config regras de conformidade em sua conta, consulteBiblioteca de regras de configuração do AMS. Uma AWS Config regra representa as

configurações desejadas para um recurso e é avaliada em relação às alterações nas configurações de seus AWS recursos. Qualquer alteração na configuração aciona um grande número de regras para testar a conformidade. Por exemplo, suponha que você crie um bucket do Amazon S3 e o configure para ser legível publicamente, violando os padrões do NIST. A bucket-public-read-prohibited regra ams-nist-cis-s 3 detecta a violação e rotula seu bucket do S3 como não compatível em seu relatório de configuração. Como essa regra pertence à categoria de remediação automática de incidentes, ela cria imediatamente um relatório de incidente, alertando você sobre o problema. Outras violações de regras mais graves podem fazer com que o AMS corrija automaticamente o problema. Consulte Respostas às violações no Accelerate.

> **Important**
>
> Se você quiser que façamos mais, por exemplo, se quiser que a AMS corrija uma violação para você, independentemente de sua categoria de remediação, envie uma Solicitação de Serviço solicitando que a AMS corrija os recursos não compatíveis para você. Na Solicitação de Serviço, inclua um comentário como “Como parte da correção da regra de configuração do AMS, corrija os recursos que não são de reclamação*RESOURCE_ARNS_OR_IDs*, configure a regra *CONFIG_RULE_NAME* na conta” e adicione as entradas necessárias para remediar a violação.
>
> Se você quiser que façamos menos, por exemplo, se não quiser que tomemos medidas em um determinado bucket do S3 que requer acesso público por design, você pode criar exceções, consulte. Criação de exceções de regras no Accelerate

Biblioteca de regras de configuração do AMS

O Accelerate implanta uma biblioteca de regras de configuração do AMS para proteger sua conta. Essas regras de configuração começam com`ams-`. Você pode visualizar as regras em sua conta e seu estado de conformidade no AWS Config console, na AWS CLI ou na AWS Config API. Para obter informações gerais sobre o uso AWS Config, consulte ViewingConfiguration Conformidade.

> **Note**
>
> Para regiões opt-in Regiões da AWS e gov cloud, implantamos apenas um subconjunto das regras de configuração devido às restrições da região. Verifique a disponibilidade da regra nas regiões verificando o link associado ao identificador na tabela de regras de configuração do AMS Accelerate.

Você não pode remover nenhuma das regras de configuração do AMS implantadas.

Tabela de regras

Faça o download como ams_config_rules.zip.

Regras de configuração do AMS

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-guardduty-habilitado-centralizado	GuardDuty	Periódico	Remediar	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 2.2,3.4,8.2.1;
ams-nist-cis-vpc-flow-logs-enabled	VPC	Periódico	Remediar	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164,308 (a) (3) (ii) (A), 164,312 (b); PCI: 2.2,10.1,10.3.2,10.3.3,10.3.4,10.3.5,10.3.6;
ams-eks-secrets-encrypted	EKS	Periódico	O incidente	CIS: NA; NIST-CSF: NA; HIPAA: NA; PCI: NA;
ams-eks-endpoint-no-acesso público	EKS	Periódico	O incidente	CIS: NA; NIST-CSF: NA; HIPAA: NA; PCI: NA;
ams-nist-cis-vpc-default-security-group-closed	VPC	Alterações de configuração	O incidente	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.312 (e) (1);

Nome da regra	Serviço	Trigger	Ação	Frameworks
				PCI: 1.2,1.3,2.1,2.2,1. 2.1,1.3.2.2.2.2;
ams-nist-cis-iam-política de senha	IAM	Periódico	O incidente	CIS: NA; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A) ,164,308 (a) (3) (ii) (B) ,164,308 (a) (4) (i), 164,308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 7.1.2, 7.1.3, 7.2.1, 7.2.2;
ams-nist-cis-iam-root-acces s-key-check	IAM	Periódico	O incidente	CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164,308 (a) (3) (i) ,164,308 (a) (3) (ii) (A) ,164,308 (a) (4) (3) (ii) (B)) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 2.2.7.1.2.7.1.3, 7.2.1, 7.2.2;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-iam-user-mfa-enabled	IAM	Periódico	O incidente	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A) ,164,308 (a) (3) (ii) (B) ,164,308 (a) (4) (i), 164,308 (a) a) (4) (ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 2.2,7.1.2,7.1.3,7.2.1,7.2.2;
ams-nist-cis-restricted-cinza	Grupos de segurança	Alterações de configuração	O incidente	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A) ,164,308 (a) (4) (ii) (B) ,164,308 (a) (4) (ii) (C) 312 (a) (1); PCI: 2.2, 7.2.1, 8.1.4;
ams-nist-cis-restricted-portas comuns	Grupos de segurança	Alterações de configuração	O incidente	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (3) (ii) (B) ,164.308 (a) (4) (i) 4.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.3.2 .2.2.2;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-s3 account-level-public-access - blocos	S3	Alterações de configuração	O incidente	CIS: CIS.9, CIS.12, CIS.14; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) 8 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1,2,1.2.1,1.3,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2.2;
ams-nist-cis-s3- bucket-public-read-prohibited	S3	Alterações de configuração	O incidente	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) 8 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1,2,1.3,2,2,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-s3- bucket-public-write-prohibited	S3	Alterações de configuração	O incidente	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) 8 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1,2,1.3,2,2,1.2.1,1.3.1,1.3 .2,1.3.4,1.3.6,2.2.2;
ams-nist-cis-s3 bucket-server-side-encryption - ativado	S3	Alterações de configuração	O incidente	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164,312 (a) (2) (iv), 164,312 (c) (2), 164,312 (e) (2) (ii); PCI: 2.2,3.4,10.5,8.2.1;
ams-nist-cis-securityhub-habilitado	Security Hub	Periódico	O incidente	CIS: CIS.3, CIS.4, CIS.6, CIS.12, CIS.16, CIS.19; NIST-CSF: PR.DS-5, PR.PT-1; HIPAA: 164.312 (b); PCI: NA;
ams-nist-cis-ec2 instance-managed-by-systems - gerente	EC2	Alterações de configuração	Relatório	CIS: CIS.2, CIS.5; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: 164.308 (a) (5) (ii) (B); PCI: 2,4;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-cloudtrail-habilitado	CloudTrail	Periódico	Relatório	CIS: CIS.16, CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.MA-2, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A), 164.308 (a) (5) (ii) (C), 164.312 (b); PCI: 10.1,10.2.1,10.2.2 , 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1,10 .3.2, 10.3.2, 10.3.3, 10.3.3, 10.3.4, 10.3.5, 10.3.6;
ams-nist-cis-access-teclas giradas	IAM	Periódico	Relatório	CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164.308 (a) (4) (ii) (B); PCI: 2,2;
ams-nist-cis-acm-certificat e-expiration-check	Certificate Manager	Alterações de configuração	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.AC-5, PR.PT-4; HIPAA: NA; PCI: 4,1;
ams-nist-cis-alb- http-to-h ttps-redirection -verificar	ALB	Periódico	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (1), 164.312 (e) (2) (i), 164.312 (e) (2) (ii); PCI: 2.3,4.1, 8.2.1;
ams-nist-cis-api- gw-cache-enabled-and -criptografado	API Gateway	Alterações de configuração	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164,312 (a) (2) (iv), 164,312 (e) (2) (ii); PCI: 3,4;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-api-gw-execution-logging-enabled	API Gateway	Alterações de configuração	Relatório	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164,312 (b); PCI: 10.1,10.3 .1,10.3.2,10.3.3,10.3.4,10. 3.5,10.3.6,10.5.4;
ams-nist-autoscaling-group-elb-healthcheck-required	ELB	Alterações de configuração	Relatório	CIS: NA; NIST-CSF: PR.PT-1, PR.PT-5; HIPAA: 164.312 (b); PCI: 2,2;
ams-nist-cis-cloud-trail-encryption-enabled	CloudTrail	Periódico	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164,312 (a) (2) (iv), 164,312 (e) (2) (ii); PCI: 2,2,3,4,10,5;
ams-nist-cis-cloud- trail-log-file-validation ativado	CloudTrail	Periódico	Relatório	CIS: CIS.6; NIST-CSF: PR.DS-6; HIPAA: 164,312 (c) (1), 164,312 (c) (2); PCI: 2,2,10,5,11,5, 10.5.2,10.5.5;
ams-nist-cis-cloudtrail-s3-dataevents habilitado	CloudTrail	Periódico	Relatório	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164,308 (a) (3) (ii) (A) ,164.312 (b); PCI: 2.2,10.1,10.2.1,10.2.2,10.2 .3,10.2.5,10.3.2,10.3.2,10. 3.3, 10.3.4, 10.3.5, 10.3.6;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-cloudwatch-alarm-action-check	CloudWatch	Alterações de configuração	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: NA; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3,4;
ams-nist-cis-cloudwatch-log-group-encrypted	CloudWatch	Periódico	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: NA; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3,4;
ams-nist-cis-codebuild-project-envvar-awscred-check	CodeBuild	Alterações de configuração	Relatório	CIS: CIS.18; NIST-CSF: PR.DS-5; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 8.2.1;
ams-nist-cis-codebuild- project-source-repo-url-verificar	CodeBuild	Alterações de configuração	Relatório	CIS: CIS.18; NIST-CSF: PR.DS-5; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 8.2.1;
ams-nist-cis-db-instance-backup-enabled	RDS	Alterações de configuração	Relatório	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i), 164.308 (a) (7) (7) (ii) (B); PCI: NA;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-dms-replication-not-public	DMS	Periódico	Relatório	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) 8 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1,2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2;
ams-nist-dynamodb-autoscaling-habilitado	DynamoDB	Periódico	Relatório	CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i), 164,308 (a) (7) (ii) (C); PCI: NA;
ams-nist-cis-dynamodb-habilitado para pitr	DynamoDB	Periódico	Relatório	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i), 164.308 (a) (7) (7) (ii) (B); PCI: NA;
ams-nist-dynamodb-throughput-verificação de limite	DynamoDB	Periódico	Relatório	CIS: NA; NIST-CSF: NA; HIPAA: 164.312 (b); PCI: NA;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-ebs-optimized-instância	EBS	Alterações de configuração	Relatório	CIS: NA; NIST-CSF: NA; HIPAA: 164.308 (a) (7) (i); PCI: NA;
ams-nist-cis-ebs-snapshot-public-restorable-check	EBS	Periódico	Relatório	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) 8 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1,2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2;
ams-nist-ec2- instance-detailed-monitoring-enabled	EC2	Alterações de configuração	Relatório	CIS: NA; NIST-CSF: DE.AE-1, PR.PT-1; HIPAA: 164.312 (b); PCI: NA;
ams-nist-cis-ec2- instance-no-public-ip	EC2	Alterações de configuração	Relatório	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4)) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1,2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-ec2-managedinstance-association-compliance-status -verificação	EC2	Alterações de configuração	Relatório	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1,2,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2;
ams-nist-cis-ec2-managedinstance-patch-compliance-status -verificação	EC2	Alterações de configuração	Relatório	CIS: CIS.2, CIS.5; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: 164.308 (a) (5) (ii) (B); PCI: 6,2;
ams-nist-cis-ec2 instâncias interrompidas	EC2	Periódico	Relatório	CIS: CIS.2; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: NA; PCI: NA;
ams-nist-cis-ec2- volume-in use-check	EC2	Alterações de configuração	Relatório	CIS: CIS.2; NIST-CSF: PR.IP-1; HIPAA: NA; PCI: NA;
ams-nist-cis-efs-cheque criptografado	EFS	Periódico	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4,8.2.1;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-eip-anexado	EC2	Alterações de configuração	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4,8.2.1;
ams-nist-cis-elasticache-redis-cluster-automatic-backup -verificar	ElastiCache	Periódico	Relatório	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i), 164.308 (a) (7) (7) (ii) (B); PCI: NA;
ams-nist-cis-opensearch-encrypted-at-rest	OpenSearch	Periódico	Relatório	CIS: CIS.14, CIS.13; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4,8.2.1;
ams-nist-cis-opensearch-in-vpc-only	OpenSearch	Periódico	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4,8.2.1;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-elb-acm-certificate-required	Certificate Manager	Alterações de configuração	Relatório	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.2.1 ,1.3.1.3.2,1.3.4,1.3.4,1.3.6,2.2.2;
ams-nist-elb-deletion-habilitado para proteção	ELB	Alterações de configuração	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (1), 164.312 (e) (2) (i), 164.312 (e) (2) (ii); PCI: 4.1,8.2.1;
ams-nist-cis-elb-habilitado para registro	ELB	Alterações de configuração	Relatório	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164,312 (b); PCI: 10.1,10.3 .1,10.3.2,10.3.3,10.3.4,10.3.5,10.3.6,10.5.4;
ams-nist-cis-emr-habilitado para kerberos	EMR	Periódico	Relatório	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164,312 (b); PCI: 10.1,10.3 .1,10.3.2,10.3.3,10.3.4,10.3.5,10.3.6,10.5.4;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-emr-master-no-public-ip	EMR	Periódico	Relatório	CIS: CIS.14, CIS.16; NIST-CSF: PR.AC-1, PR.AC-4, PR.AC-6; HIPAA: 164,308 (a) (3) (i) ,164,308 (a) (3) (ii) (A) ,164,308 (a) (4) (3) (ii) (B)) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 7.2.1;
ams-nist-cis-encrypted-volumes	EBS	Alterações de configuração	Relatório	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1,2,1.2.1,1.3.1,1.3.2,1.3.4 ,1.3.6,2.2.2;
ams-nist-cis-guardduty-non-archived-findings	GuardDuty	Periódico	Relatório	CIS: CIS.12, CIS.13, CIS.16, CIS.19, CIS.3, CIS.4, CIS.6, CIS.8; NIST-CSF: DE.AE-2, DE.AE-3, DE.CM-4, DE.DP-5, ID.RA-1, ID.RA-3, PR.DS-5, PR.PT-1; HIPAA: 164,308 (a) (5) (ii) (C), 164.308 (a) (6) (ii), 164.312 (b); PCI: 6.1,11.4, 5.1.2;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-iam-group-has-users-check	IAM	Alterações de configuração	Relatório	CIS: NA; NIST-CSF: PR.AC-4, PR.AC-1; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A) ,164,308 (a) (3) (ii) (B) ,164,308 (a) (4) (i), 164,308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 7.1.2, 7.1.3, 7.2.1, 7.2.2;
ams-nist-cis-iam- policy-no-statements-with -acesso de administrador	IAM	Alterações de configuração	Relatório	CIS: CIS.16; NIST-CSF: PR.AC-6, PR.AC-7; HIPAA: 164.308 (a) (4) (ii) (B), 164.308 (a) (5) (ii) (D), 164.312 (d); PCI: 8.2.3,8.2 .4,8.2.5;
ams-nist-cis-iam-user-group-membership-check	IAM	Alterações de configuração	Relatório	CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4)) (ii) (C), 164.312 (a) (1), 164.312 (a) (2) (i); PCI: 2.2.7.1.2, 7.2.1, 8.1.1;
ams-nist-cis-iam-user-no-policies-check	IAM	Alterações de configuração	Relatório	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-7; HIPAA: 164,308 (a) (4) (ii) (B), 164,312 (d); PCI: 8,3;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-iam-user-unused-credentials-check	IAM	Periódico	Relatório	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (3) (ii) (A) ,164.308 (a) (3) (ii) (B) ,164.308 (a) (4) (i) 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 2.2.7.1.2,7.1.3,7.2.1,7.2.2;
ams-nist-cis-ec2- instances-in-vpc	EC2	Alterações de configuração	Relatório	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (3) (ii) (B) ,164.308 (a) (4) (i) 4.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.3.2 .2.2.2;
ams-nist-cis-internet-gateway-authorized-vpc-only	Gateway da Internet	Periódico	Relatório	CIS: CIS.9, CIS.12; NIST-CSF: NA; HIPAA: NA; PCI: NA;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-kms- cmk-not-scheduled-for-exclusão	KMS	Periódico	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: NA; PCI: 3,5,3,6;
ams-nist-lambda-concurrency-verificar	Lambda	Alterações de configuração	Relatório	CIS: NA; NIST-CSF: NA; HIPAA: 164.312 (b); PCI: NA;
ams-nist-lambda-dlq-verificar	Lambda	Alterações de configuração	Relatório	CIS: NA; NIST-CSF: NA; HIPAA: 164.312 (b); PCI: NA;
ams-nist-cis-lambda-function-public-access-prohibited	Lambda	Alterações de configuração	Relatório	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1,2,1.2.1 ,1.3.1,1.3.2,1.3.4,2.2.2;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-lambda-interior-vpc	Lambda	Alterações de configuração	Relatório	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1,2,1.2.1,1.3.1,1.3.2,1.3.4 ,2.2.2;
ams-nist-cis-mfa- enabled-for-iam-console-acesso	IAM	Periódico	Relatório	CIS: CIS.16; NIST-CSF: PR.AC-7; HIPAA: 164,312 (d); PCI: 2,2,8,3;
ams-nist-cis-multi-region-cloudtrail-enabled	CloudTrail	Periódico	Relatório	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.MA-2, PR.PT-1; HIPAA: 164,308 (a) (3) (ii) (A) ,164.312 (b); PCI: 2.2,10.1,10.2.1,10 .2.12,10.2.2,10.2.2,10.2.3, 10.2.0.2,5, 10.2.6, 10.2.7, 10.3.1,10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6;
ams-nist-rds-enhanced-habilitado para monitoramento	RDS	Alterações de configuração	Relatório	CIS: NA; NIST-CSF: PR.PT-1; HIPAA: 164.312 (b); PCI: NA;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-rds-instance-public-access-check	RDS	Alterações de configuração	Relatório	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) 8 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1,2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2;
ams-nist-rds-multi-az-support	RDS	Alterações de configuração	Relatório	CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i), 164,308 (a) (7) (ii) (C); PCI: NA;
ams-nist-cis-rds-snapshots-public-prohibited	RDS	Alterações de configuração	Relatório	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) 8 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1,2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-rds-armazenamento criptografado	RDS	Alterações de configuração	Relatório	CIS: CIS.13, CIS.5, CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-1, PR.PT-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (b), 164.312 (e) (2) (ii); PCI: 3.4,10.1,10.2.2.1,10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.3.1,10.3.2, 10.3.3, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 8.2.1;
ams-nist-cis-redshift-cluster-configuration-check	RedShift	Alterações de configuração	Relatório	CIS: CIS.6, CIS.13, CIS.5; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-1, PR.PT-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (b), 164.312 (e) (2) (ii); PCI: 3.4,8.2.1,10.10.0.2.1,10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.3.1,10.3.2, 10.3.3, 10.3.3, 10.3.4, 10.3.5, 10.3.6;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-redshift-cluster-public-access-check	RedShift	Alterações de configuração	Relatório	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164.308 (a) (4) (ii) (A) ,164.308 (a) 8 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1,2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2;
ams-nist-cis-redshift-require-tls-ssl	RedShift	Periódico	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (1), 164.312 (e) (2) (i), 164.312 (e) (i), 164.312 (e) (2) (ii); PCI: 2.3,4.1;
ams-nist-cis-root-account-hardware-mfa-enabled	IAM	Periódico	Relatório	CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-7; HIPAA: 164,312 (d); PCI: 2,2,8,3;
ams-nist-cis-root-account-mfa-enabled	IAM	Periódico	Relatório	CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-7; HIPAA: 164,312 (d); PCI: 2,2,8,3;
ams-nist-cis-s3- bucket-default-lock-enabled	S3	Alterações de configuração	Relatório	CIS: CIS.14, CIS.13; NIST-CSF: ID.BE-5, PR.PT-5, RC.RP-1; HIPAA: NA; PCI: NA;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-s3- bucket-logging-enabled	S3	Alterações de configuração	Relatório	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164,308 (a) (3) (ii) (A) ,164.312 (b); PCI: 2.2,10.1,10.2.2,10.2.2,10.2.3,10.2.4,10.2.7,10., 10.3.1,10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6;
ams-nist-cis-s3- bucket-replication-enabled	S3	Alterações de configuração	Relatório	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i), 164.308 (a) (7) (7) (ii) (B); PCI: 2,2, 10,5,3;
ams-nist-cis-s3- bucket-ssl-requests-only	S3	Alterações de configuração	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv), 164.312 (c) (2), 164.312 (e) (1), 164.312 (e) (2) (i), 164.312 (e) (2) (ii); PCI: 2.2,4.1, 8.2.1;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-s3- bucket-versioning-enabled	S3	Periódico	Relatório	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.DS-6, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i) ,164.308 (a) (7) (ii) (A) ,164.308 (a) (7) (ii) (B), 164,312 (c) (1), 164,312 (c) (2); PCI: 10.5.3;
ams-nist-cis-sagemaker-endpoint-configuration-kms-key - configurado	SageMaker	Periódico	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4,8.2.1;
ams-nist-cis-sagemaker-notebook-instance-kms-key -configurado	SageMaker	Periódico	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4,8.2.1;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-sagemaker-notebook-no-direct-internet-acesso	SageMaker	Periódico	Relatório	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.2.1 ,1.3.1.3.2,1.3.4,1.3.4,1.3. 6,2.2.2;
ams-nist-cis-secretsmanager-rotation-enabled-check	Secrets Manager	Alterações de configuração	Relatório	CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164.308 (a) (4) (ii) (B); PCI: NA;
ams-nist-cis-secretsmanager-scheduled-rotation-success-check	Secrets Manager	Alterações de configuração	Relatório	CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164.308 (a) (4) (ii) (B); PCI: NA;
ams-nist-cis-sns-kms criptografado	SNS	Alterações de configuração	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 8.2.1;

Nome da regra	Serviço	Trigger	Ação	Frameworks
ams-nist-cis-vpc- -portas sg-open-only-to autorizadas	VPC	Alterações de configuração	Relatório	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.312 (e) (1); PCI: 1,2,1.3,1.2.1,1.3. 1,1.3.2,2.2.2;
ams-nist-vpc-vpn-2 túneis acima	VPC	Alterações de configuração	Relatório	CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i); PCI: NA;
ams-cis-ec2-ebs-encry ption-by-default	EC2	Periódico	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 2.2,3.4,8.2.1;
ams-cis-rds-snapshot-criptografado	RDS	Alterações de configuração	Relatório	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4,8.2.1;
ams-cis-r edshift-cluster-configurações de manutençã o - verificar	RedShift	Alterações de configuração	Relatório	CIS: CIS.5; NIST-CSF: PR.DS-4, PR.IP-1, PR.IP-4; HIPAA: 164,308 (a) (5) (ii) (A), 164,308 (a) (7) (ii) (A); PCI: 6,2;

Respostas às violações no Accelerate

Todas as violações do Config Rule aparecem no seu relatório de configuração. Essa é uma resposta universal. Dependendo da categoria de remediação (severidade) da regra, o AMS pode tomar medidas adicionais, resumidas na tabela a seguir. Para obter detalhes sobre como personalizar o Código de Ação para determinadas regras, consulteDescobertas e respostas personalizadas.

Ações de remediação

Código de ação	Ações do AMS
Relatório	1. Adicionar ao relatório de configuração
O incidente	1. Adicionar ao relatório de configuração 2. Relatório automático de incidentes no Accelerate
Remediar	1. Adicionar ao relatório de configuração 2. Relatório automático de incidentes no Accelerate 3. Remediação automática no Accelerate

Solicitando ajuda adicional

> **Note**
>
> O AMS pode remediar qualquer violação para você, independentemente de sua categoria de remediação. Para solicitar ajuda, envie uma solicitação de serviço e indique quais recursos você deseja que o AMS corrija com um comentário como “Como parte da correção da regra de configuração do AMS, corrija o *RESOURCE_ARNS_OR_IDs* recurso de recursos não reclamados ARNs/IDs>, regra de configuração *CONFIG_RULE_NAME* na conta” e adicione as entradas necessárias para remediar a violação.

O AMS Accelerate tem uma biblioteca de documentos de AWS Systems Manager automação e runbooks para ajudar na correção de recursos não compatíveis.

Adicionar ao relatório de configuração

O AMS gera um Config Report que rastreia o status de conformidade de todas as regras e recursos em sua conta. Você pode solicitar o relatório do seu CSDM. Você também pode revisar o status de conformidade no console AWS Config, na AWS CLI ou na API Config. AWS Seu Config Report inclui:

- Os principais recursos incompatíveis em seu ambiente para descobrir possíveis ameaças e configurações incorretas
- Conformidade de recursos e regras de configuração ao longo do tempo
- Configure as descrições das regras, a severidade das regras e as etapas de correção recomendadas para corrigir recursos não compatíveis

Quando qualquer recurso entra em um estado não compatível, o status do recurso (e o status da regra) se torna Não compatível em seu Config Report. Se a regra pertencer à categoria de remediação Config Report Only, por padrão, o AMS não tomará nenhuma ação adicional. Você sempre pode criar uma solicitação de serviço para solicitar ajuda adicional ou remediação do AMS.

Para obter mais detalhes, consulte AWS Config Reporting.

Relatório automático de incidentes no Accelerate

Para violações de regras moderadamente graves, o AMS cria automaticamente um Relatório de Incidente para notificá-lo de que um recurso entrou em um estado de não conformidade e pergunta quais ações você gostaria que fossem realizadas. Você tem as seguintes opções ao responder a um incidente:

- Solicite que o AMS corrija os recursos não compatíveis listados no incidente. Em seguida, tentamos corrigir o recurso não compatível e notificá-lo assim que o incidente subjacente for resolvido.
- Você pode resolver o item não compatível manualmente no console ou por meio de seu sistema de implantação automatizado (por exemplo, atualizações do modelo do CI/CD Pipeline); então, você pode resolver o incidente. O recurso não compatível é reavaliado de acordo com o cronograma da regra e, se o recurso for avaliado como não compatível, um novo relatório de incidentes será criado.
- Você pode optar por não resolver o recurso não compatível e simplesmente resolver o incidente. Se você atualizar a configuração do recurso posteriormente, o AWS Config acionará uma reavaliação e você será novamente alertado para avaliar a não conformidade desse recurso.

Remediação automática no Accelerate

As regras mais críticas pertencem à categoria Auto Remediate. A não conformidade com essas regras pode afetar fortemente a segurança e a disponibilidade de suas contas. Quando um recurso viola uma dessas regras:

1. O AMS notifica você automaticamente com um relatório de incidente.
2. O AMS inicia uma remediação automatizada usando nossos documentos SSM automatizados.
3. O AMS atualiza o Relatório de Incidentes com sucesso ou falha da remediação automatizada.
4. Se a correção automatizada falhar, um engenheiro da AMS investiga o problema.

Criação de exceções de regras no Accelerate

O Regras do AWS Config recurso de exceção de recursos permite que você suprima a emissão de relatórios de recursos específicos e não compatíveis para regras específicas.

> **Note**
>
> Os recursos isentos ainda aparecem como Não compatíveis no console do Config AWS Service. Os recursos isentos aparecem com um sinalizador especial em Config Reports (resource_exception:true). Você CSDMs pode filtrar esses recursos de acordo com essa coluna ao gerar relatórios.

Se você tem recursos que sabe que não estão em conformidade, você pode eliminar um recurso específico para uma regra de configuração específica em seus Relatórios de Configuração. Para fazer isso:

Envie uma solicitação de serviço para o Accelerate em sua conta, com uma lista das regras e recursos de configuração que devem ser isentos do relatório. Você deve fornecer uma justificativa comercial explícita (por exemplo, não é necessário denunciar isso *`resource_name_1`* e *`resource_name_2`* não fazer backup porque não queremos que seja feito backup). Para obter ajuda para enviar uma solicitação de serviço do Accelerate, consulteCriando uma solicitação de serviço no Accelerate.

Cole na solicitação as seguintes entradas (para cada recurso, adicione um bloco separado com todos os campos obrigatórios, conforme mostrado) e envie:

```
[
    {
        "resource_name": "resource_name_1",
        "config_rule_name": "config_rule_name_1",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    },
    {
        "resource_name": "resource_name_2",
        "config_rule_name": "config_rule_name_2",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    }
]
```

Reduza AWS Config custos no Accelerate

Você pode reduzir os custos do AWS Config usando a opção de registrar periodicamente o tipo de `AWS::EC2::Instance` recurso. A gravação periódica captura as últimas alterações de configuração de seus recursos uma vez a cada 24 horas, reduzindo o número de alterações entregues. Quando ativado, registra AWS Config somente a configuração mais recente de um recurso no final de um período de 24 horas. Isso permite que você personalize os dados de configuração para casos de uso específicos de planejamento operacional, conformidade e auditoria que não exigem monitoramento contínuo. Essa alteração é recomendada somente se você tiver aplicativos que dependem de arquiteturas efêmeras, o que significa que você aumenta ou diminui constantemente o número de instâncias.

Para optar pela gravação periódica do tipo de `AWS::EC2::Instance` recurso, entre em contato com a equipe de entrega do AMS.

Descobertas e respostas personalizadas

Você pode escolher como deseja que o AMS Accelerate responda a algumas descobertas (regras de configuração não compatíveis). Você pode configurar o AMS para responder às descobertas, corrigindo a descoberta, solicitando sua aprovação para remediar ou apenas reportando a você em sua próxima Análise Empresarial Mensal (MBR). Você pode alterar as respostas padrão das regras do AMS Accelerate Config. Para ver as regras, acesse Conformidade de configuração > Tabela de regras ou baixe a tabela de regras como um arquivo ZIP ams_config_rules.zip.

Alterar as respostas padrão ajuda você a aumentar o estado de segurança e conformidade da sua conta, permitindo que mais descobertas sejam corrigidas. Quando você corrige mais descobertas, você tem menos casos que precisam esperar por uma revisão e aprovação manuais. A extensa biblioteca de runbooks de remediação do AMS corrige constantemente recursos não compatíveis e você é contatado somente quando necessário.

As respostas personalizadas são usadas somente com novos recursos ou recursos existentes com novos eventos. Por exemplo, um recurso que não está em conformidade após uma alteração. Isso ocorre porque os recursos mais antigos tendem a exigir uma inspeção mais profunda antes da remediação e é mais fácil impor a remediação de recursos à medida que são criados ou alterados. Para solicitar a correção da descoberta de qualquer recurso a qualquer momento, envie uma solicitação de serviço.

Solicitando uma alteração nas respostas padrão

Os Cloud Architects (CAs) trabalham com você durante a integração para coletar suas preferências. CAsem seguida, configure a configuração inicial em sistemas AMS internos. Depois de integrado, crie uma solicitação de serviço para solicitar atualizações em suas configurações. Você pode solicitar atualizações de configuração quantas vezes forem necessárias. Observe que o Operations atualiza somente as configurações da conta na qual a solicitação de serviço foi criada. Se você precisar atualizar várias contas ao mesmo tempo, entre em contato com seu Cloud Architect. Sua CA solicitará que você corte uma solicitação de serviço com suas preferências para fins de auditoria.

Alterando as respostas padrão para suas descobertas e contas

Você sempre precisa de uma preferência de resposta para cada conta e descoberta. O AMS fornece uma resposta padrão (consulte Conformidade de configuração), portanto, essa configuração é opcional. Você pode alterar as respostas padrão para cada descoberta para as seguintes opções:

- Remediar: o AMS corrige manualmente ou automaticamente a descoberta. O AMS analisa a remediação e informa se ela falhar.
- Solicitar aprovação: o AMS cria um caso de saída para notificá-lo sobre a descoberta. Use essa opção quando quiser revisar a descoberta antes de aprovar sua remediação ou isentá-la. O AMS então executa a ação que você preferir.
- Nenhuma ação (somente relatório): a AMS não toma nenhuma ação para remediar ou intensificar a descoberta. As descobertas ainda podem aparecer no console e nos relatórios apresentados durante MBRs.

> **Note**
>
> Você não pode alterar a configuração das regras que devem ser corrigidas pelo AMS. Por exemplo, habilitar Amazon GuardDuty e VPC Flow Logs.

Alteração das respostas padrão por recursos

Você pode configurar ainda mais a resposta a recursos específicos usando tags. Você pode usar suas tags preexistentes ou recursos de tag usando o Resource Tagger. Para obter detalhes, consulteAcelere o marcador de recursos). A configuração de recursos com tags tem precedência sobre a ação padrão para a descoberta. Quando um recurso tem várias tags com diferentes configurações associadas, o AMS não pode executar correções personalizadas. Em vez disso, o AMS envia uma solicitação de serviço de saída para informá-lo sobre a situação. Por exemplo, para a descoberta bucket-server-side-encryptionhabilitada para s3, você pode:

- Altere a resposta para 'remediar' buckets S3 não criptografados com o par de valores de chave de tag “Regulated: True”
- Altere a resposta para “nenhuma ação” quando buckets S3 não criptografados tiverem as tags “Regulado: Falso” e
- Altere a resposta padrão de buckets S3 não criptografados para “solicitar aprovação”. Isso se aplica a todos os buckets S3 que não têm as tags “Regulado: Verdadeiro” ou “Regulado: Falso”

Você também pode adicionar a entrada necessária para executar a resposta de busca personalizada. Por exemplo, para remediações que exigem uma chave de criptografia, você pode fornecer sua chave IDs ao AMS. Você pode alterar os parâmetros de entrada dos runbooks de remediação, mas o AMS não oferece suporte à integração com runbooks personalizados. Para obter uma descrição dos runbooks de remediação do AMS no Config Report, consulte. AWS Config Relatório de conformidade de controle

Resposta a incidentes no Accelerate

Ao receber um alerta, a equipe do AMS usa remediações automatizadas e manuais para trazer os recursos de volta a um estado saudável. Se a remediação falhar, o AMS inicia o processo de gerenciamento de incidentes para colaborar com sua equipe. Você pode alterar as linhas de base atualizando a configuração padrão em um arquivo de configuração.

Resposta a incidentes e integração no AMS Accelerate

Durante a integração, o AMS Accelerate suprime a criação automática de incidentes para seus recursos não compatíveis existentes; em vez disso, seu Cloud Service Deliver Manager (CSDM) fornece um relatório que contém todas as regras e recursos de não conformidade para sua análise. Depois de identificar as regras que você deseja que o AMS corrija, crie uma solicitação de serviço no console Suporte central indicando essas regras e recursos. O modelo de solicitação de serviço a seguir é um exemplo de uma solicitação do cliente à AMS para corrigir manualmente os recursos não compatíveis. Se o AMS tiver dúvidas adicionais, trabalharemos com você na Solicitação de Serviço para coletar as informações necessárias.

```
Hello,
Please remediate the following resources for the Config Rule "ENCRYPTED_VOLUMES".
Resource List:
    "Vol-12345678"
    "Vol-87654312"
Thank you
```

Depois que o processo de integração for concluído, o AMS Accelerate cria automaticamente um incidente para cada recurso não compatível com as regras marcadas como Incidente automático.

Resiliência em aceleração

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, você pode projetar e operar aplicativos e bancos de dados que realizam o failover automático entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis do que as infraestruturas tradicionais de data center único ou múltiplo.

Para obter mais informações Regiões da AWS e zonas de disponibilidade, consulte infraestrutura AWS global.

Para obter informações sobre o gerenciamento de continuidade do AMS Accelerate, consulteGerenciamento de continuidade no AMS Accelerate.

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.

Melhores práticas de segurança no Accelerate

O AMS Accelerate usa pacotes de conformidade, que fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operacionais ou de otimização de custos usando ações gerenciadas ou personalizadas e de remediação. Regras do AWS Config AWS Config Para obter informações sobre a melhor forma de configurar esses pacotes de conformidade, consulte AWS Config as Melhores Práticas Operacionais para o NIST CSF e as Melhores Práticas Operacionais para as 20 Melhores Práticas do CIS.

Revisões de segurança da solicitação de alteração

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 do AMS Acceleratedefina 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 AMS Accelerate Customer Security Risk Management (CSRM) 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 do AMS Accelerate

A seguir estão as categorias de padrões técnicos do Accelerate:

ID	Categoria
AMS-STD-X002	AWS Identity and Access Management
AMS-STD-X003	Segurança de rede
AMS-STD-X004	Teste de penetração
AMS-STD-X005	Amazon GuardDuty
AMS-STD-X007	Registro em log

Controles padrão no AMS Accelerate

A seguir estão os controles padrão no AMS:

AMS-STD-X002 - (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.
1.2	O tempo limite da sessão RDP para o Microsoft Windows Server está definido para 15 minutos e pode ser estendido com base no caso de uso.
2.0	AWS Uso da conta raiz

ID	Padrão técnico
2.1	Se houver uso da conta raiz por qualquer motivo, a Amazon GuardDuty deverá ser configurada para gerar descobertas relevantes.
2.2	As chaves de acesso para a conta raiz não devem ser criadas.
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:GetObj ect) em todos os buckets do Amazon Simple Storage Service na conta não é permitida.
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.

ID	Padrão técnico
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 específic os estejam no escopo e nas operações de marcação em tags não relacionadas ao AMS.
3.3	Nos servidores Microsoft Windows, somente a Conta de Serviço Gerenciada do Grupo Microsoft (gMSA) deve ser criada.
4,0	Políticas, ações e APIs
4.4	Uma política não deve fornecer acesso ao administrador com uma declaração equivalen te a “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*” 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.
4.8	Ações que alterem os registros DNS da infraestrutura do AMS no Amazon Route 53 não devem ser permitidas.

ID	Padrão técnico
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.
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	O acesso ao ARN do bucket do S3 que ainda não foi criado nas contas do cliente pode ser fornecido restringindo o acesso aos compartimentos às contas do cliente por meio da especificação do número da conta usando a chave de condição S3 específica do serviço s3:. ResourceAccount
4.15.1	Você pode visualizar, criar, listar e excluir o acesso ao painel personalizado da lente de armazenamento do S3.

ID	Padrão técnico
4.16	Permissões completas relacionadas ao SQL Workbench podem ser concedidas roles/users para trabalhar nos bancos de dados do Amazon Redshift.
4.17	Qualquer AWS CloudShell permissão pode ser concedida às funções do cliente como alternativa à CLI.
4.18	Uma função do IAM com o AWS serviço como principal confiável também precisa estar alinhada 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	A política do IAM não deve permitir a leitura de objetos (por exemplo, S3:GetObject) em todos os buckets do S3 na conta.
4.21	Todas as permissões do IAM para o tipo de recurso “savingsplan” podem ser concedidas aos clientes.
4.22	O engenheiro do AMS não tem permissão para copiar ou mover dados do cliente (arquivos, objetos do S3, bancos de dados etc.) 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.
6.0	Políticas de contas cruzadas

ID	Padrão técnico
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.
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.

ID	Padrão técnico
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.
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 o 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 o domínio de e-mail). com AWS Organizations o nome da empresa do cliente).

ID	Padrão técnico
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.
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
8.4	Os recursos de infraestrutura do AMS devem ser protegidos do gerenciamento por identidades não autorizadas por meio da anexação de políticas baseadas em recursos.

ID	Padrão técnico
8.2	Os recursos do cliente devem ser configura dos com políticas baseadas em recursos com privilégios mínimos, a menos que o cliente especifique explicitamente uma política diferente.

AMS-STD-X003 - Segurança de rede

A seguir está o controle padrão para X003 - Network Security:

ID	Padrão técnico
	Redes
1,0	Reservado para controle futuro
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.
5,0	Um grupo de segurança não deve ter origem como 0.0.0.0/0 na regra de entrada se não 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/1 37-139 não deve ser permitido de fora da VM VPC por meio de grupos de segurança.

ID	Padrão técnico
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 via 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
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	O AMS Security consultará os padrões sempre que for solicitado que um grupo de segurança seja anexado a uma instância.

ID	Padrão técnico
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.
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

ID	Padrão técnico
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.
23,0	A solicitação de ICMP recebida da infraestr utura EC2 do cliente para a Amazon exigirá uma notificação de risco.
24,0	Solicitações de entrada do público IPs roteadas para a Amazon VPC via DX, VPC-peer ou VPN via grupo de segurança são permitidas.
25.0	Solicitações de entrada de um público IPs não roteado para a Amazon VPC via DX, VPC-peer ou VPN via grupo de segurança exigiriam uma aceitação de risco.
26,0	A solicitação ICMP de saída da Amazon EC2 para qualquer destino é permitida.
27,0	Compartilhamento de grupos de segurança
27.1	Se um grupo de segurança atender a esse padrão de segurança, ele poderá ser compartil hado VPCs na mesma conta e entre contas na mesma organização.

ID	Padrão técnico
27.2	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 compartil hamento 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-X004 - Teste de penetração

O seguinte é o controle padrão para X004 - 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-X005 - GuardDuty

A seguir está o controle padrão para o X005 - GuardDuty

1. GuardDuty deve estar habilitado em todas as contas de clientes em todos os momentos.
2. GuardDuty os alertas devem ser armazenados na mesma conta ou em qualquer outra conta gerenciada da mesma organização.
3. 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.

AMS-STD-X007 - Registro

A seguir está o controle padrão para X007 - 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 de configuração aos buckets do S3 pelo menos uma vez por dia.
1,7	Registros de aplicativos: os clientes têm o poder de ativar o login em seus aplicativos

ID	Padrão técnico
	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
2.3	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 contato de segurança autorizado do cliente.
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.

ID	Padrão técnico
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.
5.0	Integridade
5.1	O mecanismo de integridade do arquivo de log deve estar ativado. Isso significa configura r a “validação do arquivo de log” 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.

ID	Padrão técnico
6.2	Qualquer registro pode ser encaminhado do AMS para uma conta não 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.

Alterações que introduzem riscos de segurança altos ou muito altos em seu ambiente

As alterações a seguir introduzem um risco de segurança alto ou muito alto 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

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
- High_risk-log-002: desative os registros de fluxo da VPC.
- 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

Diversos

- High_Risk-ENC-001: Desative a criptografia em qualquer recurso se ela estiver ativada

Perguntas frequentes sobre segurança

O AMS fornece suporte 24/7/365 follow-the-sun por meio de centros operacionais globais. Engenheiros de operações dedicados do AMS monitoram ativamente painéis e filas de incidentes. Normalmente, o AMS gerencia suas contas por meio da automação. Em raras circunstâncias que exigem experiência específica em solução de problemas ou implantação, um engenheiro de operações do AMS pode acessar suas AWS contas.

A seguir estão perguntas comuns sobre as melhores práticas de segurança, controles, modelos de acesso e mecanismos de auditoria que o AMS Accelerate usa quando um engenheiro de operações ou automação do AMS acessa suas contas.

Quando os engenheiros de operações do AMS acessam meus ambientes?

Os engenheiros de operações do AMS não têm acesso permanente às suas contas ou instâncias. O acesso às contas dos clientes é concedido aos operadores do AMS somente para casos de uso comercial justificáveis, como alertas, incidentes, solicitações de alteração e assim por diante. O acesso é documentado em AWS CloudTrail registros.

Para justificativa de acesso, gatilhos e iniciadores de gatilhos, consulte. Acionadores de acesso à conta do cliente do AMS

Quais funções os engenheiros de operações do AMS assumem quando acessam minhas contas?

Nos raros casos (~ 5%) que exigem intervenção humana em seu ambiente, os engenheiros de operações do AMS fazem login em sua conta com uma função de acesso padrão somente para leitura. A função padrão não tem acesso a nenhum conteúdo normalmente armazenado em armazenamentos de dados, como Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift e Amazon. ElastiCache

Para obter uma lista das funções que os engenheiros de operações e sistemas do AMS exigem para fornecer serviços em sua conta, consulteFunções do IAM para acesso à conta do cliente do AMS.

Como um engenheiro de operações do AMS acessa minha conta?

Para acessar as contas dos clientes, os engenheiros de operações do AMS usam um serviço AWS interno de acesso ao AMS. Esse serviço interno está disponível somente por meio de um canal seguro e privado para que o acesso às suas contas seja seguro e auditado.

1. Os engenheiros de operações do AMS usam a autenticação interna do serviço de acesso AMS junto com uma autenticação de dois fatores. Além disso, o engenheiro de operações deve fornecer uma justificativa comercial (tíquete do incidente ou ID da solicitação de serviço) que descreva a necessidade de acessar sua AWS conta.
2. Com base na autorização do engenheiro de operação, o serviço de acesso do AMS fornece ao engenheiro a função apropriada (leituraonly/Operator/Admin) e a URL de login em seu AWS console. O acesso à sua conta é de curta duração e tem limite de tempo.
3. Para acessar as EC2 instâncias da Amazon, os engenheiros de operações do AMS usam o mesmo serviço de acesso interno do AMS que o agente. Depois que o acesso é concedido, os engenheiros de operações do AMS usam AWS Systems Manager Session Manager para acessar suas instâncias com credenciais de sessão de curta duração.

   Para fornecer acesso RDP às instâncias do Windows, o engenheiro de operações usa o Amazon EC2 Systems Manager para criar um usuário local na instância e estabelecer o encaminhamento de portas para a instância. O engenheiro de operações usa credenciais de usuário local para acesso RDP à instância. As credenciais do usuário local são removidas no final da sessão.

O diagrama a seguir descreve o processo usado pelos engenheiros de operações do AMS para acessar sua conta:

Como faço para rastrear as alterações feitas pelo AMS em minhas AWS contas gerenciadas pelo AMS?

Acesso à conta

Para ajudá-lo a monitorar as alterações feitas pela automação ou pela equipe de operações do AMS Accelerate, o AMS fornece a interface SQL do registro de alterações no console do Amazon Athena e os registros do AMS Accelerate. Esses recursos fornecem as seguintes informações:

- Quem acessou sua conta.
- Quando a conta foi acessada.
- Quais privilégios foram usados para acessar sua conta.
- Quais alterações foram feitas pelo AMS Accelerate em sua conta.
- Por que as alterações foram feitas em sua conta.

Configuração de recursos

Visualize CloudTrail registros para monitorar as configurações em seus AWS recursos nos últimos 90 dias. Se sua configuração for anterior a 90 dias, acesse os logs no Amazon S3.

Registros de instâncias

O Amazon CloudWatch Agent coleta registros do sistema operacional. Visualize os CloudWatch registros para ver os registros de login e outros registros de ações que seu sistema operacional suporta.

Para obter mais informações, consulte Rastreando alterações em suas contas do AMS Accelerate.

Quais são os controles de processo para o acesso do engenheiro de operações do AMS à minha conta?

Antes de ingressar na AMS, os engenheiros de operações passam por uma verificação de antecedentes criminais. Como os engenheiros da AMS gerenciam a infraestrutura do cliente, eles também têm uma verificação anual obrigatória de antecedentes. Se um engenheiro falhar na verificação de antecedentes, o acesso será revogado.

Todos os engenheiros de operações da AMS devem concluir o treinamento obrigatório de segurança, como segurança da infraestrutura, segurança de dados e resposta a incidentes, antes de receberem acesso aos recursos.

Como o acesso privilegiado é gerenciado?

Um subconjunto de usuários deve concluir um treinamento adicional e manter direitos de acesso privilegiado para acesso elevado. O acesso e o uso são inspecionados e auditados. O AMS limita o acesso privilegiado a circunstâncias excepcionais ou quando o acesso com privilégios mínimos não pode atender à sua solicitação. O acesso privilegiado também é limitado por tempo.

Os engenheiros de operações da AMS usam o MFA?

Sim. Todos os usuários devem usar o MFA e o Proof of Presence para fornecer serviços a você.

O que acontece com o acesso deles quando um funcionário da AMS deixa a organização ou muda de cargo?

O acesso às contas e aos recursos dos clientes é provisionado por meio da associação interna ao grupo. A associação é baseada em critérios rígidos, incluindo a função específica, o gerente de

relatórios e a situação profissional no AMS. Se a família profissional de um engenheiro de operações mudar ou sua ID de usuário for desativada, o acesso será revogado.

Quais controles de acesso regem o acesso do engenheiro operacional do AMS às minhas contas?

Há várias camadas de controles técnicos para aplicar os princípios de “necessidade de saber” e “privilégio mínimo” para acessar seu ambiente. A seguir está uma lista dos controles de acesso:

- Todos os engenheiros de operações devem fazer parte de um AWS grupo interno específico para acessar as contas e os recursos dos clientes. A associação ao grupo é estritamente baseada na necessidade de conhecimento e automatizada com critérios predefinidos.
- O AMS pratica o acesso “não persistente” ao seu ambiente. Isso significa que o acesso às suas AWS contas pelas operações do AMS é "just-in-time" com credenciais de curta duração. O acesso às suas contas é fornecido somente depois que uma justificativa interna de caso de negócios (solicitação de serviço, incidente, solicitação de gerenciamento de mudanças etc.) é enviada e analisada.
- O AMS segue o princípio do menor privilégio. Portanto, os engenheiros de operações autorizados presumem o acesso somente leitura por padrão. O acesso de gravação só é usado por engenheiros quando mudanças em seu ambiente são necessárias devido a um incidente ou a uma solicitação de alteração.
- O AMS usa AWS Identity and Access Management funções padrão e facilmente identificáveis que usam o prefixo “ams” para monitorar e gerenciar suas contas. Todo o acesso está logado AWS CloudTrail para você auditar.
- O AMS usa ferramentas de back-end automatizadas para detectar alterações não autorizadas em sua conta durante a fase de validação das informações do cliente nas execuções de alterações.

Como o AMS monitora o acesso do usuário root?

O acesso root sempre aciona o processo de resposta a incidentes. O AMS usa a GuardDuty detecção da Amazon para monitorar a atividade do usuário raiz. Se GuardDuty gerar um alerta, o AMS cria um evento para investigação adicional. O AMS notifica você se uma atividade inesperada da conta raiz for detectada, e a equipe de segurança do AMS inicia uma investigação.

Como o AMS responde aos incidentes de segurança?

O AMS investiga eventos de segurança gerados por serviços de detecção, como Amazon GuardDuty, Amazon Macie, e por problemas de segurança relatados por clientes. O AMS colabora com sua equipe de resposta de segurança para executar o processo de Resposta a Incidentes de Segurança (SIR). O processo AMS SIR é baseado na estrutura do Guia de Tratamento de Incidentes de Segurança de Computadores do NIST SP 800-61 Rev. 2 e fornece uma resposta de segurança 24 horas por dia, 7 dias por semana, 365 dias por ano. follow-the-sun O AMS trabalha com você para analisar e conter rapidamente incidentes de segurança.

A quais certificações e estruturas padrão do setor a AMS adere?

Como outros AWS serviços, o AWS Managed Services é certificado para OSPAR, HIPAA, HITRUST, GDPR, SOC*, ISO*, FedRAMP (médio/alto), IRAP e PCI. Para obter mais informações sobre as certificações, regulamentações e estruturas de conformidade do cliente que AWS se alinham, consulte Conformidade da AWS.

Guardrails de segurança

O AWS Managed Services usa vários controles para proteger seus ativos de informação e ajudar você a manter sua AWS infraestrutura segura. O AMS Accelerate mantém uma biblioteca de AWS Config regras e ações de remediação para ajudar você a garantir que suas contas estejam em conformidade com os padrões do setor de segurança e integridade operacional. AWS Config as regras rastreiam continuamente as alterações de configuração em seus recursos registrados. Se uma alteração violar as condições de uma regra, o AMS reporta suas descobertas para você. Você pode corrigir violações automaticamente ou mediante solicitação, de acordo com a gravidade da violação.

O AMS usa AWS Config regras para ajudar a atender aos requisitos dos seguintes padrões:

- Centro de Segurança na Internet (CIS)
- Estrutura de segurança em nuvem (CSF) do Instituto Nacional de Padrões e Tecnologia (NIST)
- Health Insurance Portability and Accountability Act (HIPAA)
- Padrão de segurança de dados (DSS) do setor de cartões de pagamento (PCI)

Para obter mais informações, consulte Gerenciamento de segurança no AMS Accelerate.

Como posso ter acesso aos relatórios mais recentes sobre certificação de segurança, estruturas e conformidade em AWS?

Você pode encontrar relatórios atuais de segurança e conformidade para AWS serviços usando os seguintes métodos:

- Você pode usar AWS Artifactpara baixar o relatório mais recente sobre segurança, disponibilidade e confidencialidade de um AWS serviço.
- Para obter uma lista da maioria dos AWS serviços, incluindo o AWS Managed Services, que estão em conformidade com as estruturas globais de conformidade, consulte. https://aws.amazon.com/compliance/services-in-scope/ Por exemplo, selecione PCI e pesquise por AWS Managed Services.

  Você pode pesquisar por “AMS” para encontrar artefatos de segurança específicos do AMS em uma AWS conta gerenciada do AMS. O AWS Managed Services está no escopo do SOC 3.
- O relatório AWS SOC 2 (System and Organizations Controls) é publicado no AWS Artifact repositório. Este relatório avalia os AWS controles que atendem aos critérios de segurança, disponibilidade e confidencialidade da seção 100 do TSP, Critérios de Serviços de Confiança do Instituto Americano de Contadores Públicos Certificados (AICPA).

O AMS compartilha diagramas de arquitetura de referência de diferentes aspectos dos recursos do AMS?

Para ver a arquitetura de referência do AMS, baixe o PDF do AWS Managed Services for Proactive Monitoring.

Como o AMS rastreia quem acessa minhas contas e qual é a necessidade de acesso da empresa?

Para apoiar a continuidade do serviço e a segurança de suas contas, o AMS acessa sua conta ou instâncias somente em resposta a atividades proativas de saúde ou manutenção, eventos de saúde ou segurança, atividades planejadas ou solicitações de clientes. O acesso às suas contas é autorizado por meio de processos do AMS, conforme descrito no modelo de acesso do AMS Accelerate. Esses fluxos de autorização contêm barreiras para evitar acesso inadvertido ou inapropriado. Como parte do fluxo de acesso, a AMS fornece ao sistema de autorização uma necessidade comercial. Essa necessidade comercial pode ser um item de trabalho associado à sua

conta, como um caso que você abriu com o AMS. Ou a necessidade comercial pode ser um fluxo de trabalho autorizado, como a solução Patching. Todo acesso exige uma justificativa que seja validada, verificada e autorizada em tempo real pelos sistemas internos da AMS com base nas regras de negócios para alinhar as solicitações de acesso a uma necessidade comercial.

Os engenheiros de operações do AMS não têm um caminho para acessar suas contas sem necessidades comerciais válidas. Todo o acesso à conta e a necessidade comercial associada são emitidos para AWS CloudTrail entradas dentro de suas AWS contas. Isso proporciona total transparência e a oportunidade de você realizar sua própria auditoria e inspeção. Além de sua inspeção, a AMS tem inspeções automatizadas e realiza inspeções manuais, conforme necessário, das solicitações de acesso e realiza auditorias de ferramentas e acesso humano para revisar o acesso anômalo.

Os engenheiros do AMS têm acesso aos meus dados armazenados em serviços de armazenamento de AWS dados, como Amazon S3, Amazon RDS, DynamoDB e Amazon Redshift?

Os engenheiros do AMS não têm acesso ao conteúdo do cliente armazenado em AWS serviços que são comumente usados para armazenamento de dados. O acesso aos dados AWS APIs usados para ler, gravar, modificar ou excluir dados nesses serviços é restrito por uma política explícita de negação do IAM associada às funções do IAM usadas para acesso de engenheiros do AMS. Além disso, as proteções e automações internas do AMS impedem que os engenheiros de operações do AMS removam ou modifiquem as condições de negação.

Os engenheiros do AMS têm acesso aos dados do cliente armazenados no Amazon EBS, no Amazon EFS e na Amazon FSx?

Os engenheiros do AMS podem fazer login nas EC2 instâncias da Amazon como administradores. O acesso do administrador é necessário para remediação em determinados cenários que incluem, mas não estão limitados a, problemas do sistema operacional (SO) e falhas de patch. Os engenheiros do AMS normalmente acessam o volume do sistema para corrigir problemas detectados. No entanto, o acesso dos engenheiros do AMS não é limitado ou restrito ao volume do sistema.

Como o acesso é restrito ou controlado para funções de automação que têm altos privilégios em meus ambientes?

A `ams-access-admin` função é usada exclusivamente pela automação do AMS. Essas automações implantam, gerenciam e mantêm os recursos necessários usados pelo AMS para implantação em seus ambientes para coleta de dados de telemetria, saúde e segurança para realizar funções operacionais. Os engenheiros do AMS não podem assumir funções de automação e são restringidos pelo mapeamento de funções em sistemas internos. Em tempo de execução, o AMS aplica dinamicamente uma política de sessão de privilégios mínimos com escopo reduzido a cada automação. Essa política de sessão limita a capacidade e as permissões da automação.

Como o AMS implementa o princípio do menor privilégio, conforme defendido no AWS Well-Architected Framework, para funções de automação?

Em tempo de execução, o AMS aplica uma política de sessão com escopo reduzido e com privilégios mínimos a cada automação. Essa política de sessão com escopo reduzido limita a capacidade e as permissões da automação. As políticas de sessão que têm permissões para criar recursos do IAM também precisam anexar um limite de permissão. Esse limite de permissão reduz o risco de escalonamento de privilégios. Cada equipe incorpora uma política de sessão que é usada somente por essa equipe.

Quais sistemas de registro e monitoramento são usados para detectar tentativas de acesso não autorizado ou atividades suspeitas envolvendo funções de automação?

AWS mantém repositórios centralizados que fornecem a principal funcionalidade de arquivamento de registros para uso interno pelas AWS equipes de serviço. Esses registros são armazenados no Amazon S3 para alta escalabilidade, durabilidade e disponibilidade. AWS As equipes de serviço podem então coletar, arquivar e visualizar registros de serviço em um serviço de registro central.

Os hosts de produção em AWS são implantados usando imagens principais de linha de base. As imagens de linha de base são equipadas com um conjunto padrão de configurações e funções que incluem registro e monitoramento para fins de segurança. Esses registros são armazenados e acessíveis pelas equipes AWS de segurança para análise da causa raiz no caso de uma suspeita de incidente de segurança.

Os registros de um determinado host estão disponíveis para a equipe proprietária desse host. As equipes podem pesquisar seus registros para análise operacional e de segurança.

Como os incidentes ou violações de segurança relacionados à infraestrutura de automação são tratados e quais protocolos ajudam na resposta e mitigação rápidas?

AWS planos de contingência e manuais de resposta a incidentes definiram e testaram ferramentas e processos para detectar, mitigar, investigar e avaliar incidentes de segurança. Esses planos e manuais incluem diretrizes para responder a possíveis violações de dados de acordo com os requisitos contratuais e regulamentares.

Avaliações regulares de segurança, verificações de vulnerabilidade e testes de penetração são conduzidos na infraestrutura de automação?

AWS A segurança realiza varreduras regulares de vulnerabilidades nos sistemas operacionais, aplicativos web e bancos de dados do host no AWS ambiente usando uma variedade de ferramentas. AWS As equipes de segurança também assinam feeds de notícias sobre falhas aplicáveis do fornecedor e monitoram proativamente os sites dos fornecedores e outros veículos relevantes em busca de novos patches.

Como o acesso à infraestrutura de automação é restrito somente ao pessoal autorizado?

O acesso aos AWS sistemas é alocado com base no menor privilégio e aprovado por uma pessoa autorizada. Os deveres e áreas de responsabilidade (por exemplo, solicitação e aprovação de acesso, solicitação e aprovação de gerenciamento de mudanças, desenvolvimento de mudanças, testes e implantação, etc.) são segregados entre diferentes indivíduos para reduzir a modificação não autorizada ou não intencional ou o uso indevido dos sistemas. AWS Contas em grupo ou compartilhadas não são permitidas dentro dos limites do sistema.

Quais medidas são implementadas para manter os padrões de segurança e evitar acesso não autorizado ou violações de dados no pipeline de automação?

O acesso aos recursos, incluindo serviços, hosts, dispositivos de rede e grupos Windows e UNIX, é aprovado no sistema AWS proprietário de gerenciamento de permissões pelo proprietário ou

gerente apropriado. O registro da ferramenta de gerenciamento de permissões captura solicitações de alterações de acesso. As alterações na função Job revogam automaticamente o acesso do funcionário aos recursos. O acesso contínuo desse funcionário deve ser solicitado e aprovado.

AWS requer autenticação de dois fatores em um canal criptográfico aprovado para autenticação na AWS rede interna a partir de locais remotos. Os dispositivos de firewall restringem o acesso ao ambiente de computação, impõem os limites dos clusters de computação e restringem o acesso às redes de produção.

Os processos são implementados para proteger as informações e ferramentas de auditoria contra acesso, modificação e exclusão não autorizados. Os registros de auditoria contêm um conjunto de elementos de dados para apoiar os requisitos de análise necessários. Além disso, os registros de auditoria estão disponíveis para usuários autorizados para inspeção ou análise sob demanda e em resposta a eventos relacionados à segurança ou que afetem os negócios.

Os direitos de acesso do usuário aos AWS sistemas (por exemplo, rede, aplicativos, ferramentas etc.) são revogados dentro de 24 horas após a rescisão ou desativação. As contas de usuário inativas são desativadas e and/or removidas pelo menos a cada 90 dias.

A detecção ou o monitoramento de anomalias estão ativados para o acesso ou o registro de auditoria para detectar o aumento de privilégios ou o uso indevido do acesso para alertar proativamente a equipe do AMS?

Os hosts de produção em AWS são equipados com registro para fins de segurança. Esse serviço registra ações humanas nos hosts, incluindo logons, tentativas de login malsucedidas e desconexões. Esses registros são armazenados e acessíveis pelas equipes AWS de segurança para análise da causa raiz no caso de uma suspeita de incidente de segurança. Os registros de um determinado host também estão disponíveis para a equipe proprietária desse host. Uma ferramenta de análise de registros de front-end está disponível para as equipes de serviço pesquisarem seus registros para análise operacional e de segurança. Os processos são implementados para ajudar a proteger registros e ferramentas de auditoria contra acesso, modificação e exclusão não autorizados. A equipe AWS de segurança realiza análises de registros para identificar eventos com base nos parâmetros definidos de gerenciamento de riscos.

Quais tipos de dados de clientes são extraídos das contas gerenciadas pelo AMS e como eles são utilizados e armazenados?

O AMS não acessa nem usa seu conteúdo para nenhuma finalidade. O AMS define o conteúdo do cliente como software (incluindo imagens de máquinas), dados, texto, áudio, vídeo ou imagens para os quais um cliente ou qualquer usuário final transfere AWS para processamento, armazenamento ou hospedagem Serviços da AWS em conexão com a conta de um cliente e quaisquer resultados computacionais que um cliente ou seu usuário final obtenham do exposto acima por meio do uso de. Serviços da AWS

Monitoramento e gerenciamento de eventos no AMS Accelerate

O sistema de monitoramento AMS Accelerate monitora seus AWS recursos em busca de falhas, degradação do desempenho e problemas de segurança.

Como uma conta gerenciada, o AMS Accelerate configura e implanta alarmes para AWS recursos aplicáveis, monitora esses recursos e executa correções quando necessário.

O sistema de monitoramento AMS Accelerate depende de ferramentas internas, como o Resource Tagger e o Alarm Manager Serviços da AWS, e utiliza ferramentas como AWS AppConfigAmazon CloudWatch ()CloudWatch, Amazon EventBridge (anteriormente conhecida como) CloudWatch, Amazon, Amazon GuardDuty Macie e. AWS Health

O AMS Accelerate fornece uma variedade de serviços operacionais para ajudá-lo a alcançar a excelência operacional em AWS. Para obter uma compreensão rápida de como o AMS ajuda suas equipes a alcançar a excelência operacional geral Nuvem AWS com alguns de nossos principais recursos operacionais, incluindo suporte técnico 24 horas por dia, 7 dias por semana, monitoramento proativo, segurança, aplicação de patches, registro e backup, consulte Diagramas de arquitetura de referência do AMS.

Tópicos

- O que é monitoramento?
- Como funciona o monitoramento
- Alertas do monitoramento de linha de base no AMS
- Notificações de incidentes com reconhecimento de aplicativos no AMS
- Gerenciador de alarmes acelerado
- Remediação automática de alertas pelo AMS
- Usando as regras EventBridge gerenciadas da Amazon no AMS
- Remediador confiável no AMS

Para obter informações sobre o monitoramento do Amazon EKS, consulte Monitoramento e gerenciamento de incidentes para o Amazon EKS no AMS Accelerate

O que é monitoramento?

O monitoramento do AMS Accelerate oferece os seguintes benefícios:

- Uma configuração padrão que cria, gerencia e implanta políticas em toda a sua conta gerenciada para todos os AWS recursos que você selecionar ou para os recursos compatíveis.
- 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 obter mais informações, consulte Alertas do monitoramento de linha de base no AMS.
- A capacidade de personalizar os alarmes de recursos básicos para atender às suas necessidades.
- Remediação automática de alertas pelo AMS Operations, 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.
- Visibilidade de alertas ativos e previamente resolvidos usando 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. Para obter mais informações, consulte Gerenciamento de incidentes no AMS Accelerate.
- 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 os parâmetros do recurso, consulteAlertas 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 AWS serviço, como GuardDuty ou AWS Health.

Como funciona o monitoramento

Veja os gráficos a seguir sobre a arquitetura de monitoramento no AWS Managed Services (AMS).

O diagrama a seguir mostra a arquitetura de monitoramento do AMS Accelerate.

Depois que seus recursos forem marcados com base na política definida usando o Resource Tagger e as definições de alarme forem implantadas, a lista a seguir descreve os processos de monitoramento 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: 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 da Amazon. 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.
- 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.

    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 emComo 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

Alertas do monitoramento de linha de base no AMS

Saiba mais sobre os padrões de monitoramento do AMS Accelerate. Para obter mais informações, consulte Monitoramento e gerenciamento de eventos no AMS Accelerate.

A tabela a seguir mostra o que é monitorado e os limites de alerta padrão. Você pode alterar os limites de alerta com um documento de configuração personalizado ou enviar uma solicitação de serviço. Para obter instruções sobre como alterar sua configuração de alarme personalizada, consulteAlterando a configuração do alarme Accelerate. Para receber notificações quando os alarmes ultrapassarem seu limite, além do processo de alerta padrão do AMS, você pode sobrescrever as configurações de alarme. Para instruções, consulte Gerenciador de alarmes acelerado.

A Amazon CloudWatch fornece retenção estendida de métricas. Para obter mais informações, consulte CloudWatch Limites.

> **Note**
>
> O AMS Accelerate 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 Accelerate atualiza periodicamente o monitoramento básico das contas existentes e você pode enfrentar um atraso antes que as atualizações sejam implementadas.

Alertas do monitoramento de linha de base

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
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, se você optar pelo tópico Direct-Customer-Alerts SNS, esses alertas serão enviados diretamente para seu e-mail.		
Instância do Application Load Balancer	ApplicationLoadBalancerErrorCount (HTTPCode_ELB_5xx_count/RequestCount) *100 soma > 15% por 1 min, 5 vezes consecutivas.	Contagem de erros LoadBalancer HTTP 5XX do aplicativo CloudWatch alarme sobre o número excessivo de códigos de resposta HTTP 5XX gerados pelo Loadbalancer.
Instância do Application Load Balancer	RejectedConnectionCount soma > 0% por 1 min, 5 vezes consecutivas.	Contagem de conexões LoadBalancer rejeitadas pelo aplicativo CloudWatch alarme se o número de conexões que foram rejeitadas porque o

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
		balanceador de carga atingiu seu máximo
Destino do Application Load Balancer	TargetConnectionErrorCount (HTTPCode_Target_5 xx_count/RequestCount) *100 soma > 15% por 1 min, 5 vezes consecutivas.	$ {ElasticLoadBalancingV2::TargetGroup:FullName} - Contagem de erros de conexão de LoadBalancer destino do aplicativo - $ {ElasticLoadBalancingV2::TargetGroup: :UID} CloudWatch alarme sobre o número excessivo de códigos de resposta HTTP 5XX gerados por um alvo.
Destino do Application Load Balancer	ApplicationLoadBalancerTargetGroupErrorCount soma > 0% por 1 min, 5 vezes consecutivas.	$ {ElasticLoadBalancingV2::TargetGroup:FullName} - Contagem de erros HTTP 5XX do aplicativo LoadBalancer alvo - $ {ElasticLoadBalancingV2::: TargetGroup :UID} CloudWatch alarme se o número de conexões foi estabelecido sem sucesso entre o balanceador de carga e as instâncias registradas.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
EC2 Instância da Amazon - tudo OSs	CPUUtilization* > 95% por 5 minutos, 6 vezes consecutivas.	$ {EC2::InstanceId}: CPU muito alta CloudWatch alarme. A alta utilização da CPU é um indicador de uma mudança no estado do aplicativo, como bloqueios, loops infinitos, ataques maliciosos e outras anomalias. São Direct-Customer-Alerts alarmes.
EC2 Instância da Amazon - tudo OSs	StatusCheckFailed > 0% por 5 minutos, 3 vezes consecutivas.	$ {EC2::InstanceId}: Falha na verificação de status CloudWatch alarme. Falha na verificação de status indica que uma EC2 instância da Amazon com o ID especific ado falhou em uma ou mais de suas verificações de status automatizadas. Isso significa que a instância está enfrentan do um problema que impede que ela opere corretamente ou seja acessível.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
EC2 Instância da Amazon - Linux	Percentual mínimo de mem_used_percent >= 95% por 5 minutos, 6 vezes consecutivas.	$ {EC2::InstanceId}: Sem memória CloudWatch alarme. Memória livre indica que a memória disponível (RAM) na EC2 instância especificada da Amazon caiu abaixo de um limite definido. Isso pode causar problemas de memória, falhas no sistema e indica que a instância pode precisar de mais RAM. São Direct-Customer-Alerts alarmes.
EC2 Instância da Amazon - Linux	Média de swap_used_percent >= 95% por 5 minutos, 6 vezes consecutivas.	$ {EC2::InstanceId}: Troca gratuita CloudWatch alarme. A média de swap_used _percent em uma instância da EC2 Amazon indica que a porcentagem média do espaço de swap alocado atualmente em uso ultrapass ou um limite predefinido. Isso pode causar degradação do desempenho, gargalos e problemas de memória. São Direct-Customer-Alerts alarmes.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
EC2 Instância da Amazon - Linux	Porcentagem máxima de utilização_de_disco >= 95% por 5 minutos, 6 vezes consecutivas.	$ {EC2::InstanceId}: Uso de disco muito alto - $ {EC2: :Disk: :UUID} CloudWatch alarme. Uso de disco muito alto indica que a utilização do disco em uma Amazon específica EC2 ou no disco identificado está se aproximando de sua capacidade. Isso pode levar à degradação do desempenho, erros de aplicativos e instabilidade do sistema. São Direct-Customer-Alerts alarmes.
EC2 Instância da Amazon - Windows	% de memória mínima de bytes comprometidos em uso >= 95% por 5 minutos, 6 vezes consecutivas.	$ {EC2::InstanceId}: Sem memória CloudWatch alarme. Memória livre indica que a memória disponível (RAM) na EC2 instância especificada da Amazon caiu abaixo de um limite definido. Isso pode causar problemas de memória, falhas no sistema e indica que a instância pode precisar de mais RAM. São Direct-Customer-Alerts alarmes.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
EC2 Instância da Amazon - Windows	LogicalDisk % máximo de espaço livre <= 5% por 5 minutos, 6 vezes consecutivas.	$ {EC2::InstanceId}: Uso de disco muito alto - $ {EC2: :Disk: :UUID} CloudWatch alarme. Indica que a porcentagem de espaço livre em um disco lógico (uma partição do sistema de arquivos) em uma instância EC2 do Amazon Windows ultrapassou um limite predefinido. A falta de espaço em disco pode causar escassez de espaço em disco São Direct-Customer-Alerts alarmes.
Amazon EFS	AMSEFSBurstCreditBalanceExhausted. BurstCreditBalance menos de 1000 por quinze minutos.	$ {EFS::FileSystemId}: EFS: estouro do saldo de crédito CloudWatch alarme no sistema BurstCreditBalance de arquivos Amazon EFS.
Amazon EFS	AMSEFSClientConnectionsLimit. ClientConnections > 24.000 por quinze minutos.	$ {EFS::FileSystemId}: EFS: Limite de conexões do cliente CloudWatch alarme no sistema ClientConnections de arquivos Amazon EFS.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
Amazon EFS	AMSEFSThroughputUtilization Limit. Utilização da taxa de transferência do EFS > 80% por uma hora.	$ {EFS::FileSystemId}: EFS: limite de utilização da taxa de transferência CloudWatch alarme sobre a utilização da taxa de transferência do sistema de arquivos Amazon EFS.
Amazon EFS	AMSEFSPercentIOLimit. Porcentagem IOLimit > 95 por setenta e cinco minutos.	$ {EFS::FileSystemId}: EFS: Porcentagem IOLimit CloudWatch alarme sobre a porcentagem IOLimit do sistema de arquivos Amazon EFS.
Amazon EKS	Consulte o Amazon EKSAlertas básicos em monitoramento e gerenciamento de incidentes para o Amazon EKS no AMS Accelerate.	
Instância do Elastic Load Balancing	SpilloverCountBackendConnectionErrors > 1 por 1 minuto, 15 vezes consecutivas.	LoadBalancer Alarme clássico de contagem de transbordamentos CloudWatch alarme se houver um número excessivo de solicitações rejeitadas porque a fila de sobrecarga está cheia.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
Instância do Elastic Load Balancing	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.
Instância do Elastic Load Balancing	SurgeQueueLength > 100 por 1 minuto, 15 vezes consecutivas.	Alarme clássico LoadBalancer de comprimento de fila de sobretensão. CloudWatch alarme se um número excessivo de solicitações estiver pendente de roteamento.
FSx para ONTAP	AMSFSXONTAPIOPSUtilization. FSX:Utilização de IOPS do ONTAP > 80% por duas horas.	$ {FSx:FileSystemId}: Utilização do FSX:ONTAP IOPS CloudWatch alarme sobre o limite de utilização de IOPS da instância FSx for ONTAP.
FSx para ONTAP	AMSFSXONTAPThroughputUtilização. Utilização da taxa de transferência do FSX:ONTAP > 80% por duas horas.	$ {FSx::FileSystemId}: Utilização da taxa de transferência do FSX:ONTAP CloudWatch alarme sobre o limite de taxa de transferência do volume do FSx ONTAP.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
FSx para ONTAP	AMSFSXONTAPVolumeI nodeUtilization. FSX:ONTAP Inode Utilização > 80% por duas horas.	$ {FSx::FileSystemId} :$ {: :ONTAPFSx::VolumeI d} Utilização do código FSX:ONTAP CloudWatch alarme sobre o limite de utilização da capacidade de arquivo do volume FSx for ONTAP.
FSx para ONTAP	AMSFSXONTAPVolumeC apacityUtilization. FSX: Utilização da capacidad e de volume do ONTAP > 80% por duas horas.	$ {FSx::FileSystemId} :$ {: :ONTAPFSx::} VolumeId CloudWatch alarme sobre o limite de utilização da capacidade de volume do volume FSx para ONTAP.
FSx para Windows File Server	AMSFSXWindowsThrou ghputUtilization. FSX: Utilização da taxa de transferência do Windows > 80% por duas horas.	$ {FSx::FileSystemId}: FSX:Utilização da taxa de transferência do Windows CloudWatch alarme sobre o limite de taxa de transferência da FSx instância do Windows File Server.
FSx para Windows File Server	AMSFSXWindowsIOPSU tilization. FSX: Utilização de IOPS do Windows > 80% por duas horas.	$ {FSx:FileSystemId}: FSX:Utilização de IOPS do Windows CloudWatch alarme sobre o limite de utilização de IOPS da instância do FSx Windows File Server.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
GuardDuty Serviço	Não aplicável; todas as descobertas (propósitos de ameaça) são monitoradas. Cada descoberta corresponde a um alerta. Mudanças nas GuardDuty descobertas. Essas alteraçõe s incluem descobertas recém-geradas ou as ocorrências subsequentes das descobert as existentes.	Para obter uma lista dos tipos de GuardDuty descoberta compatíveis, consulte Tipos de descoberta GuardDuty ativos.
Saúde	AWS Health Dashboard	As notificações são enviadas quando há mudanças no status dos eventos AWS Health Dashboard (AWS Health) em relação aos serviços monitorados pelo AMS. Para obter mais informações, consulte Serviços compatíveis.
IAM	O perfil de instância do Amazon EC2 IAM não existe. O perfil da instância do IAM está ausente.	Para obter instruções sobre como substituir um perfil de instância EC2 do Amazon IAM, consulte a documenta ção do IAM em Substituir a função do IAM.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
IAM	O Amazon EC2 IAM Instance Profile tem muitas políticas. O perfil da instância do IAM tem 10 políticas e políticas adicionais não podem ser adicionadas.	• Modifique a cota de AWS serviço do IAM para aumentar o número de políticas gerenciadas por função para 20. Para obter informações sobre cotas de serviço, consulte Visualização de cotas de serviço. • Reduza a contagem de políticas gerenciadas abaixo da cota atual do IAM removendo políticas gerenciadas desnecessárias para a função do IAM associada a essas instâncias. Certifique-se de manter as políticas exigidas pelo AMS. • Reduza a contagem de políticas gerenciadas abaixo da cota atual do IAM consolidando as políticas para a função do IAM associada a essas instâncias. Certifique-se de manter as políticas exigidas pelo AMS. Para as políticas necessárias do AMS, consulte o Guia do usuário do AMS Accelerat

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
		e:Detalhes da alteração de permissões do IAM.
Macie	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 Amazon Macie compatíveis, consulte Analisando as descobertas do Amazon Macie. Observe que o Macie não está habilitado para todas as contas.
NATGateways	PacketsDropCount : Alarme se o packetsdropcount for > 0 em um período de 15 minutos	NatGateway PacketsDropCount Um valor maior que zero pode indicar um problema temporário contínuo com o gateway NAT.
NATGateways	ErrorPortAllocation : Alarme se os gateways NAT não puderem alocar a porta por mais de 15 minutos no período de avaliação	NatGateway ErrorPortAllocation O número de vezes que o gateway NAT não conseguiu alocar uma porta de origem. Um valor maior que zero indica que muitas conexões simultâneas estão abertas.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
OpenSearch agrupamento	ClusterStatus o máximo vermelho é >= 1 por 1 minuto, 1 vez consecutiva.	ClusterStatus Vermelho CloudWatch alarme. A chave de AWS KMS criptografia usada para criptografar dados em repouso no seu domínio está desativada. Reative-a para restaurar as operações normais. Para saber mais, consulte Red Cluster Status.
OpenSearch Domínio	KMSKeyErro >= 1 por 1 minuto, 1 vez consecutiva.	Erro de chave KMS CloudWatch alarme. Pelo menos um fragmento principal e suas réplicas não estão alocados para um nó. Para saber mais, consulte Criptografia de dados em repouso para o Amazon OpenSearch Service.
OpenSearch Domínio	KMSKeyInacessível >= 1 por 1 minuto, 1 vez consecutiva.	Erro de chave inacessível do KMS CloudWatch alarme. Pelo menos um fragmento principal e suas réplicas não estão alocados para um nó. Para saber mais, consulte Criptografia de dados em repouso para o Amazon OpenSearch Service.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
OpenSearch Domínio	ClusterStatus o máximo amarelo é >= 1 por 1 minuto, 1 vez consecutiva.	ClusterStatus Amarelo Pelo menos um fragmento de réplica não está alocado para um nó. Para saber mais, consulte Yellow Cluster Status.
OpenSearch Domínio	FreeStorageSpace o mínimo é <= 20480 por 1 minuto, 1 vez consecutiva.	Pouco espaço de armazenamento livre Um nó no seu cluster tem 20 GiB de espaço de armazenamento livre. Para saber mais, consulte Falta de espaço de armazenamento disponível.
OpenSearch Domínio	ClusterIndexWritesBlocked >= 1 por 5 minutos, 1 vez consecutiva.	Gravações de índice de cluster bloqueadas O cluster está bloqueando as solicitações de gravação. Para saber mais, consulte ClusterBlockException.
OpenSearch Domínio	Nós mínimo < x por 1 dia, 1 vez consecutiva.	Nodos inativos 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.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
OpenSearch Domínio	CPUUtilization média >= 80% por 15 minutos, 3 vezes consecutivas.	Alto uso da CPU no nó de dados 100% de utilização da CPU não é raro, mas médias altas contínuas são problemát icas. Considere o dimension amento correto de um tipo de instância existente ou a adição de instâncias.
OpenSearch Domínio	JVMMemoryPressão máximo >= 80% por 5 minutos, 3 vezes consecuti vas.	Alto uso de memória no nó de dados O cluster poderá apresentar erros de memória insuficiente se o uso aumentar. Considere a escalabilidade vertical. O OpenSearch usa metade da RAM de uma instância para o heap do Java, com um tamanho de heap de 32 GiB. Você pode dimension ar instâncias verticalmente até 64 GiB de RAM, sendo que nesse ponto você poderá dimensionar horizontalmente adicionando instâncias.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
OpenSearch Domínio	Mestre CPUUtilization média >= 50% por 15 minutos, 3 vezes consecutivas.	Alto uso da CPU do Master Nodes Considere usar tipos de instância maiores para seus nós principais dedicados. Devido à sua função na estabilidade do cluster e implantações azuis/verdes, os nós principais dedicados devem ter uma média de uso de CPU menor do que os nós de dados.
OpenSearch Domínio	JVMMemoryPressão principal máximo >= 80% por 15 minutos, 1 vez consecutiva.	Alta pressão de memória JVM dos nós principais Considere usar tipos de instância maiores para seus nós principais dedicados. Devido à sua função na estabilidade do cluster e implantações azuis/verdes, os nós principais dedicados devem ter uma média de uso de CPU menor do que os nós de dados.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
OpenSearch instância	AutomatedSnapshotFailure o máximo é >= 1 por 1 minuto, 1 vez consecutiva.	Falha automática no snapshot CloudWatch alarme. Ocorreu falha em um snapshot automatizado. Essa falha normalmente é o resultado de um status de integridade vermelho do cluster. Para saber mais, consulte Red Cluster Status.
Amazon RDS	Utilização média da CPU > 90% por 15 minutos, 2 vezes consecutivas.	$ {RDS:: DBInstance Identificador}: CPUUtilization CloudWatch alarmes.
Amazon RDS	Soma de DiskQueueDepth > 75% por 1 minuto, 15 vezes consecutivas.	$ {RDS:: DBInstance Identificador}: DiskQueue CloudWatch alarmes.
Amazon RDS	Média FreeStorageSpace < 1.073.741.824 bytes por 5 minutos, 2 vezes consecutivas.	$ {RDS:: DBInstance Identificador}: FreeStorageSpace CloudWatch alarmes.
Amazon RDS	Alerta de baixo armazenamento É acionado quando o armazenamento alocado para a instância de banco de dados está esgotado.	RDS-EVENT-0007, veja detalhes em Usando a notificação de eventos do Amazon RDS.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
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.	RDS-EVENT-0031, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
Amazon RDS	Não houve tentativa de failover do RDS -0034. O Amazon RDS não está tentando um failover solicitado porque ocorreu um failover recentemente na instância de banco de dados.	RDS-EVENT-0034, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
Amazon RDS	RDS - parâmetros inválidos da instância de banco de dados 0035 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 sua ação seria modificar o parâmetro de memória e reinicializar a instância de banco de dados.	RDS-EVENT-0035, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
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, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
Amazon RDS	Erro de réplica de leitura da instância de banco de dados RDS-0045 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.	RDS-EVENT-0045, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
Amazon RDS	RDS-0057 Erro ao criar conta de usuário do statspack A replicação na réplica de leitura foi encerrada.	Evento de serviço. RDS-EVENT-0057, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
Amazon RDS	A replicação de leitura da instância de banco de dados RDS-0058 terminou 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, veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
Amazon RDS	Início da recuperação da instância de banco de dados A instância de banco de dados do SQL Server está restabelecendo seu espelho. O performance 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 veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
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.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
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 veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
Amazon RDS	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.
Amazon RDS	Alerta de baixo armazenamento quando a instância de banco de dados consumiu mais de 90% do armazenamento alocado.	Evento de serviço. RDS-EVENT-0089 veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
Amazon RDS	Serviço de notificação quando o escalonamento falhou para o cluster de banco de dados Aurora Serverless.	Evento de serviço. RDS-EVENT-0143 veja detalhes em Categorias de eventos e mensagens de eventos do Amazon RDS.
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.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
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.
Amazon RDS	Esse evento indica que o escalonamento automático do armazenamento de instâncias do Amazon 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.
Amazon RDS	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.
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.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
Amazon RDS	O Amazon 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.
Amazon RDS	O armazenamento para você 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.
Cluster do Amazon Redshift	A integridade do cluster quando não está no modo de manutenção < 1 por 5 min	RedshiftClusterHealthStatus Para obter mais informaçõ es, consulte Monitoramento do Amazon Redshift usando CloudWatch métricas.
Site-to-Site VPN	VPNTunnelPara baixo TunnelState <= 0 por 1 min, 20 vezes consecutivas.	$ {AWS::EC2::VpnConn ectionId} - VPNTunnel Inativo TunnelState é 0 quando os dois túneis estão desativados, 0,5 quando um túnel está ativo e 1,0 quando os dois túneis estão ativos.

Serviço/Tipo de recurso	Fonte de alerta e condição de gatilho	Nome e notas do alerta
Systems Manager Agent	EC2 Instâncias não gerenciadas pelo Systems Manager O agente SSM não está instalado. O agente SSM está instalado na instância, mas o serviço do agente não está em execução. O agente SSM não tem uma rota de rede para o serviço AWS Systems Manager.	Há condições adicionais que causam interrupções no Systems Manager Agent; para obter mais informações, consulte Solução de problemas de disponibilidade de nós gerenciados.

Para obter informações sobre os esforços de remediação, consulteRemediação automática de alertas pelo AMS.

Assista ao vídeo de Andrew para saber mais (7:03)

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 AppRegistrypara 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, você deve primeiro integrar o. AWS Service Catalog AppRegistry

Para saber mais sobre os padrões de monitoramento do AMS Accelerate, consulte. Monitoramento e gerenciamento de eventos no AMS Accelerate

Integre AppRegistry e crie aplicativos

Para integrá-lo AppRegistry, consulte Introdução AppRegistry no Guia do AWS Service Catalog AppRegistry administrador. Após a integração, use um dos seguintes métodos para criar aplicativos:

1. AWS console: Para saber mais sobre como criar um aplicativo AppRegistry por meio do AWS console, 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 .
3. Automação do AMS: para simplificar o processo de registro do aplicativo, o AMS fornece o documento `AWSManagedServices-CreateAppRegistryApplication` de automação do SSM. Para usar esse método, invoque o documento do AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/, ou com o, AWS CLI conforme descrito no exemplo a seguir.

```
# The following registers a new application with customized severity
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["normal"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# The following registers a new application with no customizations
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# You can also register applications using CloudFormation stacks
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["STACKS"],"AppTagValue":
[""],"CFNStackNames":["arn:aws:cloudformation:us-east-1:123456789012:stack/
stack-2343eddq/1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p"],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
```

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 as tags necessárias.

As tags com o prefixo `ams:rt:` são aplicadas por meio do Resource Tagger.

Chave de tag	Valor da tag
gerenciado por ams	true
ams:rt:ams-managed	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

Criticalidade

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 SeverityLevela 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-*
```

Gerenciador de alarmes acelerado

O AMS Accelerate aplica alarmes aos seus AWS recursos usando o Gerenciador de alarmes baseado em tags para implementar uma estratégia básica de monitoramento e garantir que todos os seus AWS recursos sejam monitorados e protegidos. Ao se integrar ao Gerenciador de alarmes baseado em tags, você pode personalizar a configuração de seus AWS recursos com base em seu tipo, plataforma e outras tags, para garantir que os recursos sejam monitorados. O Alarm Manager é implantado em sua conta do Accelerate durante a integração.

Como funciona o Gerenciador de alarmes

Quando sua conta é integrada ao AMS Accelerate, dois documentos JSON, chamados perfis de configuração, são implantados em sua conta em. AWS AppConfig Ambos os documentos de perfil residem no aplicativo Alarm Manager e no ambiente de infraestrutura do AMS Accelerate.

Os dois perfis de configuração são chamados de AMSManagedAlarmes (o perfil de configuração padrão) e CustomerManagedAlarms(o perfil de configuração de personalização).

- Perfil de configuração padrão:
  - A configuração encontrada nesse perfil contém a configuração padrão que o AMS Accelerate implanta em todas as contas de clientes. Essa configuração contém a política de monitoramento padrão do AMS Accelerate, que você não deve modificar porque o AMS Accelerate pode atualizar esse perfil a qualquer momento, apagando todas as alterações feitas.
  - Se você quiser modificar ou desativar qualquer uma dessas definições, consulte Modificando a configuração padrão do alarme Accelerate Desativando a configuração padrão de alarme do Accelerate e.
- Perfil de configuração de personalização:
  - Qualquer configuração nesse perfil é totalmente gerenciada por você; o AMS Accelerate não substitui esse perfil, a menos que você o solicite explicitamente.
  - Você pode especificar qualquer definição de alarme personalizada que desejar nesse perfil e também pode especificar modificações na configuração padrão gerenciada pelo AMS

Accelerate. Para obter mais informações, consulte Modificando a configuração padrão do alarme Accelerate e Desativando a configuração padrão de alarme do Accelerate.

- Se você atualizar esse perfil, o Alarm Manager aplica automaticamente suas alterações em todos os recursos relevantes da sua AWS conta. Observe que, embora suas alterações sejam promulgadas automaticamente, elas podem levar até 60 minutos para entrarem em vigor.
- Você pode atualizar esse perfil usando as Console de gerenciamento da AWS CLI/SDK ferramentas da AWS. Consulte o Guia AWS AppConfig do usuário para obter instruções sobre como atualizar uma configuração.
- O perfil de personalização está inicialmente vazio; no entanto, todas as definições de alarme colocadas no documento do perfil são aplicadas, além da configuração padrão.

Todos os CloudWatch alarmes criados pelo Gerenciador de alarmes contêm a chave de tag ams:alarm-manager:managed e o valor da tag true. Isso é para garantir que o Gerenciador de alarmes gerencie somente os alarmes que ele cria e não interfira com nenhum de seus próprios alarmes. Você pode ver essas tags usando a CloudWatch ListTagsForResourceAPI da Amazon.

> **Important**
>
> Se as definições de alarme personalizadas e as definições de alarme padrão forem especificadas com o mesmo ID de configuração (consulte Perfil de configuração acelerada: monitoramento), as definições personalizadas terão prioridade sobre as regras padrão.

Introdução ao Accelerate Alarm Manager

Por padrão, quando você se integra ao AMS Accelerate, sua configuração é implantada AWS AppConfig, definindo uma linha de base de alarme para seus recursos. As definições de alarme são aplicadas somente aos recursos com as tags ams:rt: *. Recomendamos que essas tags sejam aplicadas usando Acelere o marcador de recursos: você configura uma configuração básica do Resource Tagger para que o AMS Accelerate saiba quais recursos você deseja gerenciar.

Use o Resource Tagger para aplicar a chave de tag ams:rt:ams-managed com valor de tag true a todos os recursos que você deseja que o AMS Accelerate monitore.

Veja a seguir um exemplo de perfil de personalização do Resource Tagger que você pode usar para optar pelo monitoramento de todas as suas instâncias da Amazon EC2 . Para obter informações gerais, consulte Acelere o marcador de recursos.

```
{
    "AWS::EC2::Instance": {
        "AMSManageAllEC2Instances": {
            "Enabled": true,
            "Filter": {
                "InstanceId": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

Para obter informações sobre como aplicar essa configuração do Resource Tagger, consulteVisualizando ou fazendo alterações na configuração do Resource Tagger.

Acelere as tags do Alarm Manager

Por padrão, quando você se integra ao AMS Accelerate, sua configuração é implantada AWS AppConfig, definindo uma linha de base de alarme para seus recursos. As definições de alarme são aplicadas somente aos recursos com as tags ams:rt: *. Recomendamos que essas tags sejam aplicadas usandoAcelere o marcador de recursos: você configura uma configuração básica do Resource Tagger para que o AMS Accelerate saiba quais recursos você deseja gerenciar.

Use o Resource Tagger para aplicar a chave de tag ams:rt:ams-managed com valor de tag true a todos os recursos que você deseja que o AMS Accelerate monitore.

Tópicos

- Acelere as tags usando o Resource Tagger
- Acelere as tags sem o Resource Tagger
- Acelere as tags usando CloudFormation
- Acelere as tags usando o Terraform

Acelere as tags usando o Resource Tagger

O Gerenciador de alarmes baseado em tags gerencia o ciclo de vida dos CloudWatch alarmes por recurso; no entanto, ele exige que os recursos gerenciados tenham tags específicas definidas pelo AMS Accelerate. Para usar o Resource Tagger para aplicar o conjunto padrão de alarmes gerenciados pelo AMS às instâncias baseadas em Linux e Windows, siga estas etapas.

1. Navegue até o AppConfigconsole em sua conta.
2. Selecione o ResourceTagger aplicativo.
3. Selecione a guia Perfis de configuração e, em seguida, selecione CustomerManagedTags.
4. Clique em Criar para criar um novo perfil.
5. Selecione JSON e defina sua configuração. Para obter mais exemplos de definição de filtro e plataforma, consulteAcelere o marcador de recursos.

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

6. Clique em Criar versão de configuração hospedada.
7. Clique em Iniciar implantação.
8. Defina os seguintes detalhes de implantação:

```
Environment: AMSInfrastructure Hosted configuration version: <Select the version
 that you have just created>
               Deployment Strategy: AMSNoBakeDeployment
```

9. Clique em Iniciar implantação.

Suas instâncias são marcadas com `"ams:rt:ams-managed": "true"` o que garante que outras `"ams:rt:ams-monitoring-policy": "ams-monitored"` e `"ams:rt:ams-monitoring-policy-platform": "ams-monitored-linux"` sejam aplicadas às instâncias. Essas tags resultam na criação dos alarmes apropriados para a instância. Para ter mais informações sobre esse processo, consulte Monitoramento em Accelerate.

Assista ao vídeo de Himanshu para saber mais (11:04)

Acelere as tags sem o Resource Tagger

O Gerenciador de alarmes baseado em tags gerencia o ciclo de vida dos CloudWatch alarmes por recurso; no entanto, ele exige que os recursos gerenciados tenham tags específicas definidas pelo AMS Accelerate. O AMS Accelerate fornece um perfil de configuração padrão que pressupõe que suas tags foram aplicadas pelo Resource Tagger.

Se você quiser usar um método alternativo de aplicar tags aos seus recursos, como CloudFormation o Terraform, e não o Resource Tagger, você precisa desativar o Resource Tagger para que ele não aplique tags aos seus recursos e concorra com o método de marcação escolhido. Para obter instruções sobre como alterar seu perfil de configuração personalizado do Resource Tagger para ativar o modo somente leitura, consulte. Impedindo que o Resource Tagger modifique recursos

Depois que o Resource Tagger for configurado para o modo somente leitura e o perfil de configuração for implantado, use o método de marcação escolhido para aplicar tags aos seus recursos de acordo com as diretrizes a seguir:

Tipo de recurso	Chave de tag	Valor da tag
Todos os recursos compatíveis (descritos nesta tabela)	ams: rt: ams-monitoring-policy	sou monitorado
EC2 instâncias (Linux)	ams: rt: ams-monitoring-policy-platform	ams-monitored-linux
EC2 instâncias (Windows)	ams: rt: ams-monitoring-policy-platform	ams-monitored-windows
OpenSearch Domínio com KMS	ams: rt: ams-monitoring-with-kms	ams-monitored-with-kms

Tipo de recurso	Chave de tag	Valor da tag
OpenSearch Domínio com nó principal dedicado	ams: rt: ams-monitoring-with-master	ams-monitored-with-master

Os recursos que têm essas chaves e valores de tag são gerenciados pelo AMS Accelerate Alarm Manager.

Acelere as tags usando CloudFormation

> **Note**
>
> Certifique-se de ter definido o Resource Tagger para o modo somente leitura antes de aplicar as tags CloudFormation, caso contrário, o Resource Tagger poderá modificar as tags com base no perfil de configuração. Para obter informações sobre como configurar o Resource Tagger para o modo somente leitura e diretrizes sobre como fornecer suas próprias tags, consulte. Acelere as tags sem o Resource Tagger

Para aplicar tags usando CloudFormation, você pode aplicar tags no nível da pilha (consulte Tags de CloudFormation recursos) ou, no nível do recurso individual (por exemplo, consulte Criação de tags de EC2 instância).

Veja a seguir um exemplo de como você pode aplicar as tags de gerenciamento de alarmes do AMS Accelerate a uma EC2 instância da Amazon gerenciada por CloudFormation:

```
Type: AWS::EC2::Instance
Properties:
 InstanceType: "t3.micro"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

Veja a seguir um exemplo de como você pode aplicar as tags de gerenciamento de alarmes do AMS Accelerate a um grupo de Auto Scaling gerenciado por. CloudFormation Observe que o grupo Auto Scaling propagará suas tags para as EC2 instâncias da Amazon criadas por ele:

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

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

Acelere as tags usando o Terraform

> **Note**
>
> Certifique-se de ter definido o Resource Tagger para o modo somente leitura antes de aplicar as tags CloudFormation, caso contrário, o Resource Tagger poderá modificar as tags com base no perfil de configuração. Para obter informações sobre como configurar o Resource Tagger para o modo somente leitura e diretrizes sobre como fornecer suas próprias tags, consulte. Acelere as tags sem o Resource Tagger

Para obter uma descrição de como gerenciar tags de recursos usando o Terraform, consulte a documentação do Terraform Resource Tagging.

Veja a seguir um exemplo de como você pode aplicar as tags de gerenciamento de alarmes do AMS Accelerate a uma EC2 instância da Amazon gerenciada pelo Terraform.

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

     instance_type = "t3.micro"

     tags = {
       "aws:rt:ams-monitoring-policy" = "ams-monitored"
```

```
      "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
    }
  }
```

Veja a seguir um exemplo de como você pode aplicar as tags de gerenciamento de alarmes do AMS a um grupo de Auto Scaling gerenciado pelo Terraform. Observe que o grupo Auto Scaling propaga suas tags para EC2 instâncias criadas por ele:

```
resource "aws_autoscaling_group" "test_asg" {
name = "terraform-test"
# ...other properties...

tags = {
  "aws:rt:ams-monitoring-policy" = "ams-monitored"
  "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
}
}
```

Acelere os perfis de configuração do Alarm Manager

Quando sua conta é integrada ao AMS Accelerate, dois documentos JSON, chamados perfis de configuração, são implantados em sua conta com AWS AppConfig (consulte O que é). AWS AppConfig Ambos os documentos de perfil residem no aplicativo Alarm Manager e no ambiente de infraestrutura do AMS Accelerate.

Tópicos

- Perfil de configuração acelerada: monitoramento
- Perfil de configuração acelerada: substituição de pseudoparâmetros
- Exemplos de configuração de alarmes acelerados
- Visualizando a configuração do Accelerate Alarm Manager
- Alterando a configuração do alarme Accelerate
- Modificando a configuração padrão do alarme Accelerate
- Implantando alterações na configuração do Accelerate Alarm
- Revertendo Acelere as alterações do alarme
- Retenção dos alarmes do Accelerate
- Desativando a configuração padrão de alarme do Accelerate

Perfil de configuração acelerada: monitoramento

Tanto o documento de perfil de configuração padrão quanto o documento de perfil de configuração de personalização seguem a mesma estrutura:

```
  {
    "<ResourceType>": {
        "<ConfigurationID>": {
            "Enabled": true,

            "Tag": {
                "Key": "...",
                "Value": "..."
            },
            "AlarmDefinition": {
                ...
            }
        },
        "<ConfigurationID>": {
            ...
        }
    },
    "<ResourceType>": {
        ...
    }
}
```

- ResourceType: essa chave deve ser uma das seguintes sequências de caracteres suportadas. A configuração dentro desse objeto JSON se relacionará somente ao tipo de AWS recurso especificado. Tipos de recursos compatíveis:

```
AWS::EC2::Instance
AWS::EC2::Instance::Disk
AWS::RDS::DBInstance
AWS::RDS::DBCluster
AWS::Elasticsearch::Domain
AWS::OpenSearch::Domain
AWS::Redshift::Cluster
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::ElasticLoadBalancingV2::LoadBalancer::TargetGroup
AWS::ElasticLoadBalancing::LoadBalancer
AWS::FSx::FileSystem::ONTAP
```

```
AWS::FSx::FileSystem::ONTAP::Volume
AWS::FSx::FileSystem::Windows
AWS::EFS::FileSystem
AWS::EC2::NatGateway
AWS::EC2::VPNConnection
```

- ConfigurationId: essa chave deve ser exclusiva no perfil e nomear de forma exclusiva o seguinte bloco de configuração. Se dois blocos de configuração no mesmo ResourceTypebloco tiverem o mesmo ID de configuração, aquele que aparecer por último no perfil entrará em vigor. Se você especificar um ConfigurationID em seu perfil de personalização que seja igual ao especificado no perfil padrão, o bloco de configuração definido no perfil de personalização entrará em vigor.
  - Ativado: (opcional, default=true) Especifique se o bloco de configuração entrará em vigor. Defina isso como false para desativar um bloco de configuração. Um bloco de configuração desativado se comporta como se não estivesse presente no perfil.
  - Tag: especifique a tag à qual essa definição de alarme se aplica. Qualquer recurso (do tipo de recurso apropriado) que tenha essa chave e valor de tag terá um CloudWatch alarme criado com a definição fornecida. Esse campo é um objeto JSON com os seguintes campos:
    - Chave: A chave da etiqueta correspondente. Lembre-se de que, se você estiver usando o Resource Tagger para aplicar as tags ao recurso, a chave da tag sempre começará com ams:rt:.
    - Valor: o valor da tag correspondente.
  - AlarmDefinition: Define o alarme a ser criado. Esse é um objeto JSON cujos campos são passados como estão para a chamada da CloudWatch `PutMetricAlarm` API (com exceção dos pseudoparâmetros; para obter mais informações, consulte). Perfil de configuração acelerada: substituição de pseudoparâmetros Para obter informações sobre quais campos são obrigatórios, consulte a PutMetricAlarmdocumentação.

    OU

    CompositeAlarmDefinition: define um alarme composto a ser criado. Ao criar um alarme composto, você especifica uma expressão de regra para o alarme que leva em conta o estado de alarme de outros alarmes que você criou. Esse é um objeto JSON cujos campos são passados no estado em que se encontram para o. `CloudWatchPutCompositeAlarm` O alarme composto entrará no estado ALARM somente se todas as condições da regra forem atendidas. Os alarmes especificados na expressão de regra de um alarme composto podem incluir alarmes de métrica e outros alarmes compostos. Para obter informações sobre quais campos são obrigatórios, consulte a PutCompositeAlarmdocumentação.

Ambas as opções fornecem os seguintes campos:

- AlarmName: especifique o nome do alarme que você deseja criar para o recurso. Esse campo tem todas as mesmas regras especificadas na PutMetricAlarmdocumentação; no entanto, como o nome do alarme deve ser exclusivo em uma região, o Gerenciador de alarmes tem um requisito adicional: você deve especificar o pseudoparâmetro identificador exclusivo no nome do alarme (caso contrário, o Gerenciador de alarmes anexará o identificador exclusivo do recurso à frente do nome do alarme). Por exemplo, para o tipo de AWS::EC2::Instancerecurso, você deve especificar `${EC2::InstanceId}` o nome do alarme, ou ele será adicionado implicitamente no início do nome do alarme. Para obter a lista de identificadores, consultePerfil de configuração acelerada: substituição de pseudoparâmetros.

  Todos os outros campos estão conforme especificado na documentação PutMetricAlarmou na PutCompositeAlarmdocumentação.

- AlarmRule: especifique quais outros alarmes devem ser avaliados para determinar o estado desse alarme composto. Para cada alarme que você referenciar, eles devem existir CloudWatch ou estar especificados no perfil de configuração do Gerenciador de alarmes em sua conta.

> **Important**
>
> Você pode especificar qualquer um AlarmDefinitionou CompositeAlarmDefinitionno documento de configuração do Gerenciador de alarmes, mas os dois não podem ser usados ao mesmo tempo.

No exemplo a seguir, o sistema cria um alarme quando dois alarmes métricos especificados excedem seu limite:

```
{
  "AWS::EC2::Instance": {
    "LinuxResourceAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:mylinuxinstance",
        "Value": "true"
      },
```

```
      "CompositeAlarmDefinition": {
        "AlarmName": "${EC2::InstanceId} Resource Usage High",
        "AlarmDescription": "Alarm when a linux EC2 instance is using too much CPU and
 too much Disk",
        "AlarmRule": "ALARM(\"${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}\") AND ALARM(\"${EC2::InstanceId}: CPU Too High\")"
      }
    }
  }
}
```

Important

Quando o Alarm Manager não consegue criar ou excluir um alarme devido a uma configuração interrompida, ele envia a notificação para o tópico Direct-Customer-Alerts SNS. Esse alarme é chamado AlarmDependencyError.
É altamente recomendável que você tenha confirmado sua assinatura deste tópico do SNS. Para receber mensagens publicadas em um tópico, você deve inscrever um endpoint no tópico. Para obter detalhes, consulte Etapa 1: Criar um tópico.

Note

Quando os alarmes de detecção de anomalias são criados, o Alarm Manager cria automaticamente os modelos de detecção de anomalias necessários para as métricas especificadas. Quando os alarmes de detecção de anomalias são excluídos, o Gerenciador de alarmes não exclui os modelos de detecção de anomalias associados.
A Amazon CloudWatch limita o número de modelos de detecção de anomalias que você pode ter em uma determinada AWS região. Se você exceder a cota do modelo, o Alarm Manager não criará novos alarmes de detecção de anomalias. Você deve excluir modelos não utilizados ou trabalhar com seu parceiro do AMS para solicitar um aumento de limite.
Muitas das definições de alarmes de linha de base fornecidas pelo AMS Accelerate listam o tópico do SNS, o tópico do MMS, como alvo. Isso é para uso no serviço de monitoramento do AMS Accelerate e é o mecanismo de transporte para que suas notificações de alarme cheguem ao AMS Accelerate. Não especifique o MMS-Topic como alvo para nenhum alarme diferente dos fornecidos na linha de base (e substituições dos mesmos), pois o serviço ignora alarmes desconhecidos. Isso não faz com que o AMS Accelerate atue em seus alarmes personalizados.

Perfil de configuração acelerada: substituição de pseudoparâmetros

Em qualquer um dos perfis de configuração, você pode especificar pseudoparâmetros que são substituídos no local da seguinte forma:

- Global - em qualquer lugar no perfil:
  - $ {AWS::AccountId}: Substituído pelo ID AWS da sua conta
  - $ {AWS::Partition}: Substituído pela partição em que Região da AWS o recurso está (isso é 'aws' para a maioria das regiões); para obter mais informações, consulte a entrada para partição na referência do ARN.
  - $ {AWS::Region}: Substituído pelo nome da região na qual seu recurso está implantado (por exemplo, us-east-1)
- Em um bloco AWS::EC2::Instancede tipo de recurso:
  - $ {EC2::InstanceId}: (identificador) substituído pelo ID da instância da sua EC2 instância da Amazon.
  - $ {EC2::InstanceName}: substituído pelo nome da sua EC2 instância da Amazon.
- Em um bloco do tipo de recurso AWS::EC2::Instance: :Disk:
  - $ {EC2::InstanceId}: (identificador) Substituído pelo ID da instância da sua EC2 instância da Amazon.
  - $ {EC2::InstanceName}: Substituído pelo nome da sua EC2 instância da Amazon.
  - $ {EC2: :Disk: :Device}: (identificador) Substituído pelo nome do disco. (Somente Linux, em instâncias gerenciadas pelo CloudWatch Agente).
  - $ {EC2: :Disk::FSType}: (identificador) Substituído pelo tipo de sistema de arquivos do disco. (Somente Linux, em instâncias gerenciadas pelo CloudWatchAgent).
  - $ {EC2: :Disk: :Path}: (identificador) Substituído pelo caminho do disco. No Linux, esse é o ponto de montagem do disco (por exemplo,/), enquanto no Windows esse é o rótulo da unidade (por exemplo, c:/) (somente em uma instância gerenciada pelo CloudWatch Agente).
  - $ {EC2: :Disk: :UUID}: (identificador) Substituído por um UUID gerado que identifica exclusivamente o disco, isso deve ser especificado no nome do alarme, pois um alarme sob AWS::EC2::Instance::Disk o tipo de recurso criará um alarme por volume. Especificar $ {EC2: :Disk: :UUID} manterá a exclusividade dos nomes dos alarmes.
- Em um bloco AWS::EKS::Clusterde tipo de recurso:
  - $ {EKS::ClusterName}: (identificador) substituído pelo nome do seu cluster EKS.
- Em um bloco AWS::OpenSearch::Domainde tipo de recurso:

  - $ {OpenSearch::DomainName}: (identificador) substituído pelo nome do seu domínio EKS.
- Em um bloco AWS::ElasticLoadBalancing::LoadBalancerde tipo de recurso:
  - $ {ElasticLoadBalancing::LoadBalancer: :Name}: (identificador) substituído pelo nome do seu Load Balancer V1.
- Em um bloco AWS::ElasticLoadBalancingV2::LoadBalancerde tipo de recurso:
  - $ {ElasticLoadBalancingV2:: :Arn}LoadBalancer: (identificador) substituído pelo ARN do seu Load Balancer V2.
  - $ {ElasticLoadBalancingV2::LoadBalancer: :Name}: (identificador) substituído pelo nome do seu Load Balancer V2.
  - $ {ElasticLoadBalancingV2:::LoadBalancer:FullName}: (identificador) substituído pelo nome completo do seu Load Balancer V2.
- Em um bloco de tipo de TargetGroup recurso AWS::ElasticLoadBalancingV2::LoadBalancer::
  - $ {ElasticLoadBalancingV2:::TargetGroup:FullName}: (identificador) substituído pelo nome do grupo-alvo do seu Load Balancer V2.
  - $ {ElasticLoadBalancingV2:: :UUID}TargetGroup: (identificador) substituído por um UUID gerado para seu Load Balancer V2.
- Em um bloco AWS::EC2::NatGatewayde tipo de recurso:
  - $ {NatGateway::NatGatewayId}: (identificador) substituído pelo ID do NAT Gateway.
- Em um bloco de tipo de DBInstance recurso AWS: :RDS::
  - $ {RDS:: DBInstance Identifier}: (identificador) substituído pelo identificador da sua instância de banco de dados do RDS.
- Em um bloco de tipo de DBCluster recurso AWS: :RDS::
  - $ {RDS:: DBCluster Identifier}: (identificador) substituído pelo seu identificador de cluster de banco de dados RDS.
- Em um bloco AWS::Redshift::Clusterde tipo de recurso:
  - $ {Redshift::ClusterIdentifier}: (identificador) substituído pelo seu identificador de cluster do Redshift.
- Em um bloco AWS::Synthetics::Canaryde tipo de recurso:
  - $ {Synthetics::CanaryName}: (identificador) substituído pelo nome do seu canário Synthetics CloudWatch .
- Em um bloco do tipo de VPNConnection recurso AWSEC2::::
  - $ {AWS::EC2::VpnConnectionId}: (identificador) substituído pelo seu ID de VPN.

- Em um bloco AWS::EFS::FileSystemde tipo de recurso:
  - $ {EFS::FileSystemId}: (identificador) Substituído pelo ID do sistema de arquivos do seu sistema de arquivos EFS.
- Em um bloco de tipo de recurso AWS::FSx::FileSystem: :ONTAP:
  - $ {FSx::FileSystemId}: (identificador) Substituído pelo ID do sistema de arquivos do seu sistema de arquivos FSX.
  - $ {FSx::FileSystem: :Throughput}: Substituído pela taxa de transferência do seu sistema de arquivos FSX.
  - $ {FSx:FileSystem: :Iops}: Substituído pelo IOPS do sistema de arquivos FSX.
- Em um bloco do tipo de recurso AWS::FSx::FileSystem: :ONTAP: :Volume:
  - $ {FSx::FileSystemId}: (identificador) Substituído pelo ID do sistema de arquivos do seu sistema de arquivos FSX.
  - $ {FSx: :ONTAP::VolumeId}: (identificador) Substituído pelo ID do volume.
- Em um bloco de tipo de recurso AWS::FSx::FileSystem: :Windows:
  - $ {FSx::FileSystemId}: (identificador) Substituído pelo ID do sistema de arquivos do seu sistema de arquivos FSX.
  - $ {FSx::FileSystem: :Throughput}: Substituído pela taxa de transferência do seu sistema de arquivos FSX.

> **Note**
>
> Todos os parâmetros marcados com identificador são usados como prefixo para o nome dos alarmes criados, a menos que você especifique esse identificador no nome do alarme.

Exemplos de configuração de alarmes acelerados

No exemplo a seguir, o sistema cria um alarme para cada disco conectado à instância Linux correspondente.

```
{
    "AWS::EC2::Instance::Disk": {
        "LinuxDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mylinuxinstance",
```

```
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "disk_used_percent",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "device",
                        "Value": "${EC2::Disk::Device}"
                    },
                    {
                        "Name": "fstype",
                        "Value": "${EC2::Disk::FSType}"
                    },
                    {
                        "Name": "path",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

No exemplo a seguir, o sistema cria um alarme para cada disco conectado à instância correspondente do Windows.

```
{
     "AWS::EC2::Instance::Disk": {
        "WindowsDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mywindowsinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "LogicalDisk % Free Space",
```

```
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "objectname",
                        "Value": "LogicalDisk"
                    },
                    {
                        "Name": "instance",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

Visualizando a configuração do Accelerate Alarm Manager

Tanto os AMSManagedalarmes quanto os CustomerManagedAlarmspodem ser revisados AppConfig com GetConfiguration.

Veja a seguir um exemplo da `GetConfiguration` chamada:

```
aws appconfig get-configuration --application AMSAlarmManager --environment
 AMSInfrastructure --configuration AMSManagedAlarms --client-id
      any-string outfile.json
```

- Aplicação: esta AppConfig é a unidade lógica para fornecer recursos; para o Gerenciador de alarmes, isso é `AMSAlarmManager`
- Meio ambiente: este é o AMSInfrastructure meio ambiente
- Configuração: para visualizar os alarmes de linha de base do AMS Accelerate, o valor é`AMSManagedAlarms`; para visualizar as definições de alarme do cliente, a configuração é `CustomerManagedAlarms`
- ID do cliente: é um identificador exclusivo da instância do aplicativo, que pode ser qualquer string

- As definições de alarme podem ser visualizadas no arquivo de saída especificado, que neste caso é `outfile.json`

Você pode ver qual versão da configuração foi implantada em sua conta visualizando as implantações anteriores no AMSInfrastructure ambiente.

Alterando a configuração do alarme Accelerate

Para adicionar ou atualizar novas definições de alarme, você pode implantar o documento Usando CloudFormation para implantar o Accelerate as alterações de configuração de configuração ou invocar a CreateHostedConfigurationVersionAPI.

Esse é um comando de linha de comando do Linux que gera o valor do parâmetro em base64, que é o que o comando AppConfig CLI espera. Para obter informações, consulte a AWS CLI documentação Binary/Blob (objeto binário grande).

Exemplo:

```
aws appconfig create-hosted-configuration-version --application-id application-id --
configuration-profile-id configuration-profile-id --content base64-string
      --content-type application/json
```

- ID do aplicativo: ID do aplicativo AMS AlarmManager; você pode descobrir isso com a chamada da ListApplicationsAPI.
- ID do perfil de configuração: ID da configuração CustomerManagedAlarms; você pode descobrir isso com a chamada da ListConfigurationProfilesAPI.
- Conteúdo: string Base64 do conteúdo, a ser criada criando um documento e codificando-o em base64: cat alarms-v2.json | base64 (consulte Binário/Blob (objeto binário grande)).

  Tipo de conteúdo: tipo MIME, `application/json` porque as definições de alarme são escritas em JSON.

> **Important**
>
> Restrinja o acesso às ações StopDeploymentda API StartDeploymente às ações da API a usuários confiáveis que entendam as responsabilidades e as consequências da implantação de uma nova configuração em seus alvos.

Para saber mais sobre como usar os AppConfig recursos da AWS para criar e implantar uma configuração, consulte Como trabalhar com a AWS AppConfig.

Modificando a configuração padrão do alarme Accelerate

Embora você não possa modificar o perfil de configuração padrão, você pode substituir os padrões especificando um bloco de configuração em seu perfil de personalização com o mesmo configurationId do bloco de configuração padrão. Se você fizer isso, todo o seu bloco de configuração substituirá o bloco de configuração padrão ao qual a configuração de marcação deve ser aplicada.

Por exemplo, considere o seguinte perfil de configuração padrão:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 5,
                ...
            }
        }
    }
}
```

Para alterar o limite desse alarme para 10, você deve fornecer toda a definição do alarme, não apenas as partes que deseja alterar. Por exemplo, você pode fornecer o seguinte perfil de personalização:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 10,
                ...
            }
        }
    }
}
```

Important

Lembre-se de implantar suas alterações de configuração depois de fazê-las. No SSM AppConfig, você deve implantar uma nova versão da configuração depois de criá-la.

Implantando alterações na configuração do Accelerate Alarm

Depois de concluir uma personalização, você precisa implantá-la, com AppConfig ou CloudFormation.

Tópicos

- Usando AppConfig para implantar alterações na configuração do Accelerate Alarm
- Usando CloudFormation para implantar o Accelerate as alterações de configuração

Usando AppConfig para implantar alterações na configuração do Accelerate Alarm

Depois que a personalização for concluída, use AppConfig para implantar suas alterações com StartDeployment.

```
  aws appconfig start-deployment --application-id application_id
   --environment-id environment_id Vdeployment-strategy-id
   deployment_strategy_id --configuration-profile-id configuration_profile_id --
configuration-version 1
```

- ID do aplicativo: ID do aplicativo`AMSAlarmManager`, você pode encontrá-lo com a chamada da ListApplicationsAPI.
- ID do ambiente: você pode encontrar isso com a chamada ListEnvironmentsda API.
- ID da estratégia de implantação: você pode encontrar isso com a chamada ListDeploymentStrategiesda API.
- ID do perfil de configuração: ID de`CustomerManagedAlarms`; você pode encontrar isso com a chamada ListConfigurationProfilesda API.
- Versão de configuração: a versão do perfil de configuração a ser implantado.

> **Important**
>
> O Alarm Manager aplica as definições de alarme conforme especificado nos perfis de configuração. Qualquer modificação manual que você fizer nos CloudWatch alarmes Console de gerenciamento da AWS ou no CloudWatch CLI/SDK será automaticamente revertida, portanto, certifique-se de que suas alterações sejam definidas por meio do Gerenciador de alarmes. Para entender quais alarmes são criados pelo Gerenciador de alarmes, você pode procurar a `ams:alarm-manager:managed` tag com valor`true`.
> Restrinja o acesso às ações StopDeploymentda API StartDeploymente às ações da API a usuários confiáveis que entendam as responsabilidades e as consequências da implantação de uma nova configuração em seus alvos.

Para saber mais sobre como usar os AppConfig recursos da AWS para criar e implantar uma configuração, consulte a AppConfig documentação da AWS.

Usando CloudFormation para implantar o Accelerate as alterações de configuração

Se você deseja implantar seu perfil de `CustomerManagedAlarms` configuração usando CloudFormation, você pode usar os seguintes CloudFormation modelos. Coloque a configuração JSON desejada no `AMSAlarmManagerConfigurationVersion.Content` campo.

Quando você implanta os modelos em uma CloudFormation pilha ou conjunto de pilhas, a implantação do `AMSResourceTaggerDeployment` recurso falhará se você não tiver seguido o formato JSON exigido para a configuração. Consulte Perfil de configuração acelerada: monitoramento para obter detalhes sobre o formato esperado.

Para obter ajuda na implantação desses modelos como uma CloudFormation pilha ou conjunto de pilhas, consulte a documentação relevante da AWS CloudFormation abaixo:

- Criação de uma pilha no console da AWS CloudFormation
- Criação de uma pilha com o AWS CLI
- Criação de um conjunto de pilhas

> **Note**
>
> Se você implantar uma versão de configuração usando um desses modelos e, posteriormente, excluir a CloudFormation pilha/conjunto de pilhas, a versão de configuração do modelo permanecerá como a versão atual implantada e nenhuma implantação adicional será feita. Se você quiser voltar para uma configuração padrão, precisará implantar manualmente uma configuração vazia (ou seja, apenas {}) ou atualizar sua pilha para uma configuração vazia, em vez de excluir a pilha.

JSON

```
{
  "Description": "Custom configuration for the AMS Alarm Manager.",
  "Resources": {
    "AMSAlarmManagerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
```

```
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "Content": "{}",
        "ContentType": "application/json"
      }
    },
    "AMSAlarmManagerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSAlarmManagerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Alarm Manager.
Resources:
  AMSAlarmManagerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
```

```
      Content: |
        {

        }
      ContentType: application/json
  AMSAlarmManagerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      ConfigurationVersion:
        !Ref AMSAlarmManagerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-Alarm-Manager-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-Alarm-Manager-Configuration-EnvironmentId
```

Revertendo Acelere as alterações do alarme

Você pode reverter as definições de alarme por meio do mesmo mecanismo de implantação, especificando uma versão anterior do perfil de configuração e executando StartDeployment.

Retenção dos alarmes do Accelerate

Quando os recursos monitorados pelo AMS são excluídos, todos os alarmes criados pelo Alarm Manager para esses recursos são automaticamente excluídos pelo Alarm Manager. Se você precisar reter determinados alarmes para fins de auditoria, conformidade ou histórico, use o recurso de retenção de etiquetas do Alarm Manager.

Para reter um alarme mesmo após a exclusão do recurso monitorado, adicione uma `"ams:alarm-manager:retain"` tag à configuração personalizada do alarme, conforme mostrado no exemplo a seguir.

```
{
  "AWS::EC2::Instance": {
    "AMSCpuAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:ams-monitoring-policy",
        "Value": "ams-monitored"
```

```
      },
      "AlarmDefinition": {
        "AlarmName": "${EC2::InstanceId}: CPU Too High",
        "AlarmDescription": "AMS Baseline Alarm for EC2 CPUUtilization",
        [...]
        "Tags": [
          {
            "Key": "ams:alarm-manager:retain",
            "Value": "true"
          }
        ]
      }
    }
  }
}
```

Um alarme configurado com a "`ams:alarm-manager:retain`" tag não é excluído automaticamente pelo Gerenciador de alarmes quando o recurso monitorado é encerrado. O alarme retido persiste CloudWatch indefinidamente até que você o remova manualmente usando. CloudWatch

Desativando a configuração padrão de alarme do Accelerate

O AMS Accelerate fornece o perfil de configuração padrão em sua conta com base nos alarmes de linha de base. No entanto, essa configuração padrão pode ser desativada substituindo qualquer uma das definições de alarme. Você pode desativar uma regra de configuração padrão substituindo o configurationId da regra em seu perfil de configuração de personalização e especificando o campo ativado com o valor false.

Por exemplo, se a seguinte configuração estiver presente no perfil de configuração padrão:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                ...
            }
```

```
        }
    }
```

Você pode desativar essa regra de marcação incluindo o seguinte em seu perfil de configuração de personalização:

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

Para fazer essas alterações, a CreateHostedConfigurationVersionAPI deve ser chamada com o documento de perfil JSON (consulteAlterando a configuração do alarme Accelerate) e, posteriormente, implantada (consulteImplantando alterações na configuração do Accelerate Alarm). Observe que, ao criar a nova versão de configuração, você também deve incluir todos os alarmes personalizados criados anteriormente que desejar no documento de perfil JSON.

> **Important**
>
> Quando o AMS Accelerate atualiza o perfil de configuração padrão, ele não é calibrado em relação aos alarmes personalizados configurados, portanto, revise as alterações nos alarmes padrão ao substituí-las em seu perfil de configuração de personalização.

Criação de CloudWatch alarmes adicionais para o Accelerate

Você pode criar CloudWatch alarmes adicionais para o AMS Accelerate usando CloudWatch métricas e alarmes personalizados para instâncias da Amazon EC2 .

Produza seu script de monitoramento de aplicativos e sua métrica personalizada. Para obter mais informações e acessar exemplos de scripts, consulte Monitoramento de memória e métricas de disco para instâncias EC2 Linux da Amazon.

Os scripts de CloudWatch monitoramento para EC2 instâncias Linux da Amazon demonstram como produzir e consumir CloudWatch métricas personalizadas. 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.

> **Important**
>
> O AMS Accelerate não monitora CloudWatch os alarmes criados por você.

Visualizando o número de recursos monitorados pelo Alarm Manager for Accelerate

O Alarm Manager envia métricas a cada hora para a Amazon CloudWatch, no `AMS/AlarmManager` namespace. As métricas são emitidas somente para tipos de recursos suportados pelo Gerenciador de alarmes.

Nome da métrica	Dimensões	Descrição
ResourceCount	Componente, ResourceType	Número de recursos (do tipo de recurso especificado) implantados nessa região. Unidades: contagem
ResourcesMissingManagedAlarms	Componente, ResourceType	Número de recursos (do tipo de recurso especificado) que exigem alarmes gerenciados, mas o Alarm Manager ainda não aplicou os alarmes. Unidades: contagem
UnmanagedResources	Componente, ResourceType	Número de recursos (do tipo de recurso especificado) que não têm nenhum alarme gerenciado aplicado a eles pelo Alarm Manager. Normalmente, esses recursos não correspondem a nenhum bloco de configuração do Alarm Manager ou são explicitamente excluídos dos blocos de configuração. Unidades: contagem
MatchingResourceCount	Componente, ResourceType, ConfigClauseName	Número de recursos (do tipo de recurso especificado) que correspondem ao bloco de configuração do Alarm Manager. Para que um recurso corresponda ao

Nome da métrica	Dimensões	Descrição
		bloco de configuração, o bloco deve estar ativado e o recurso deve ter as mesmas tags especificadas no bloco de configuração. Unidades: contagem

Essas métricas também podem ser visualizadas como gráficos no painel do AMS-Alarm-Manager-Reporting-Dashboard. Para ver o painel, no console de AWS CloudWatch gerenciamento, selecione AMS-Alarm-Manager-Reporting-Dashboard. Por padrão, os gráficos nesse painel exibem os dados do período anterior de 12 horas.

O AMS Accelerate implanta CloudWatch alarmes em sua conta para detectar aumentos significativos no número de recursos não gerenciados, por exemplo, recursos excluídos do gerenciamento pelo AMS Alarm Manager. As operações do AMS investigarão aumentos nos recursos não gerenciados que excedam: três recursos do mesmo tipo ou um aumento de 50% em relação a todos os recursos do mesmo tipo. Se a alteração não parecer deliberada, a AMS Operations poderá entrar em contato com você para analisar a alteração.

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
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

Nome do alerta	Descrição	Limites	Ação
			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 designado em um volume) na sua EC2 instância estiver sendo preenchido.	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.
AMSWindowsDiskUsage	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: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

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: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

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: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

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: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

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.

Usando as regras EventBridge gerenciadas da Amazon no AMS

O AMS Accelerate 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 Accelerate 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

AmsAccessRolesRule	Essa regra escuta modificações em funções e políticas específicas do AMS Accelerate.	<pre>{
		"source": ["aws.iam"],
		"detail-type": ["AWS API Call via CloudTrail"],
		"detail": {
		"eventName": [
		"DeleteRole",
		"DeletePolicy",
		"CreatePolicyVersion",
		"AttachRolePolicy",
		"DetachRolePolicy"
		],
		"requestParameters": {
		"$or": [
		{
		"roleName": [
		"ams-access-admin",</pre>

Nome da regra	Descrição	Definição

```
                    "ams-access-admin-operations",
                    "ams-access-operations",
                    "ams-access-read-only",
                    "ams-access-security-analyst",
                    "ams-access-security-analyst-
read-only"
                ]
            },
            {
                "policyArn": [
                    "arn:*:iam::*:policy/ams-ac
cess-allow-pass-role",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-cloudshell-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-operations-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-update-iam-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-ssr-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-read-only-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-extended-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-operations-policy"
                ]
            },
        ]
      },
   },
}
```

Nome da regra	Descrição	Definição

AMSCoreRegra	Essa regra encaminha os CloudWatch eventos da Amazon para os serviços de remediação AWS Config e monitoramento do AMS Config, respeitosamente. Os AWS Config eventos criam e resolvem AWS Systems Manager OpsItems. Os CloudWatch eventos da Amazon monitoram os CloudWatch alarmes.	<pre>{
		    {
		        "source": ["aws.config", "aws.cloudwatch"],
		        "detail-type": ["Config Rules Compliance Change", "CloudWatch Alarm State Change"],
		    }
		}</pre>

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 AdvisorAWS 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 inicia o documento de automação.

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. Para obter mais informações, consulte Relatórios do Trusted Remediator.

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 Advisorverificações e AWS Compute Optimizerrecomendações. 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. Você pode usar o AWS AppConfig console ou a API para editar as configurações.
- 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 Accelerate.
  - 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.

- Regiões da AWS: Regiões 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. Depois da integração, você pode usar o AWS AppConfig console ou a API para gerenciar as configurações. 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.

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. Atualize sua configuração para ativar a correção para as Trusted Advisor verificações selecionadas. Para obter instruções sobre como selecionar cheques, consulteConfigurar 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, consulteRastreie as remediações no Trusted Remediator.

Execute correções manuais no Trusted Remediator

Você pode corrigir manualmente as Trusted Advisor verificações. Quando você inicia uma remediação manual, o Trusted Remediator cria uma execução manual. OpsItem Você deve revisar e iniciar o documento de automação do SSM para corrigir o. OpsItems 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 OptimizerTrusted 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	• CreateSnapshot: para criar um instantâneo antes de modificar o volume, defina como “Verdadei

Opção de otimização	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-confi gurados suportados
	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.).	ro”. Para não criar um instantâneo, defina como 'False'. O padrão é “Verdadeiro”. Sem restrições • 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

Opção de otimização	Nome do documento SSM e resultado esperado	Parâmetros e restrições pré-configurados suportados
		• RemediateStackDrift: Para iniciar a correção do desvio, se algum desvio for causado pela modificação do volume, defina como “Verdadeiro”. Para não tentar 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 instâncias 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-StopIdleRDSInstance 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, escolha`true`. Para não criar um backup antes de encerrar, escolha`false`. 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`true`, a automação cria um snapshot do volume do Amazon EBS antes de ser excluído. A configuração padrão é `true`. Os valores válidos são `true` e `false` (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`0`, o documento SSM não verifica o período não anexado e exclui o volume se o volume estiver atualmente desconectado. O padrão é value is7. 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 para `true` forçar a parada de instâncias usando o armazenamento de instâncias. Caso contrário, defina como `false`. O valor padrão de `false` 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. `true` Para não criar um backup, escolha`false`. O padrão é `false`. Os valores válidos são `true` e `false` (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`true`. Para não redimensionar automaticamente a instância se estiver em um estado interrompido, escolha`false`. Os valores válidos são `true` e `false` (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 AMIBefore encerramento: defina essa opção para `true` ou `false` para criar uma AMI de instância como backup antes de encerrar a EC2 instância. O padrão é `true`. Os valores válidos são `true` e `false` (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 deRecomendações 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-TrustedRemediatorEnableAPIGateWayExecutionLogging 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-TrustedRemediatorEnableAutoScalingGroupELBHealthCheck 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-TrustedRemediatorEnableCloudTrailLogValidation 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-TrustedRemediatorEnableCodeBuildLoggingConfig 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-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot 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-TrustedRemediatorEnableDocumentDBClusterDeletionProtection 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-TrustedRemediatorEnableDynamoDBTableDeletionProtection 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-TrustedRemediatorDisablePublicAccessOnEBSSnapshot 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 reinicializada 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, escolha`true`. Para não criar um backup antes de encerrar, escolha`false`. 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, escolha`true`. Para não criar um backup antes de encerrar, escolha`false`. 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
Hs4Ma3G121 - 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-TrustedRemediatorHabilitar 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
Hs4Ma3G325 - 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 `AWSLogs`. 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-TrustedRemediatorEnableEMRBlockPublicAccess 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-TrustedRemediatorEnableNeptuneDBClusterDeletionProtection 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-TrustedRemediatorEnableNetworkFirewallDeletionProtection- 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-TrustedRemediatorDisablePublicAccessOnRDSInstance 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-TrustedRemediatorEnableRDSEnhancedMonitoring 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 `rds-monitoring-role` 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 MonitoringRoleName valores MonitoringInterval 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-TrustedRemediatorEnableRDSDeletionProtection 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-TrustedRemediatorEnableRDSDeletionProtection 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-TrustedRemediatorEnableRDSLogExports 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-UpdateRDSIAMDatabaseAuthentication 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. `true` Para programar a alteração para a próxima janela de manutenção, escolha`false`. 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. `true` Para programar a alteração para a próxima janela de manutenção, escolha`false`. 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 `available` 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 `CopyTagtosnapshot` 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-TrustedRemediatorEnableRedshiftClusterEnhancedVPCRouting 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-TrustedRemediatorBlockS3BucketPublicAccess 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`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 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-TrustedRemediatorEnableBucketAccessLoggingV2 - 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 TargetBucketTagValuemarque 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 TargetBucketTagKeypara 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: TargetBucketTagKeye. TargetBucketTagValue 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.
Pfx0 RwqBli 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-00000 0000000).

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-TrustedRemediatorDisableSageMakerNotebookInstanceRootAccess 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 `alias/aws/sns` . 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-TrustedRemediatorDisableSSMDocPublicSharing- 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.	• SqsManagedSseEnabled: Defina como `true` para habilitar a criptografia de filas do lado do servidor usando chaves de criptografia de propriedade do Amazon SQS, defina como para `false` habilitar a criptografia de filas do lado do servidor usando uma chave. AWS KMS • KMSKeyID: 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, alias/aws/sqs é usado. • KmsDataKeyReusePeriodSeconds: 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 `SqsManagedSseEnabled` estiver definida como`true`.

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-00000 0000000).
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. `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` . Os valores válidos são `SimplePrefix` `PartitionedPrefixEventTime` e `PartitionedPrefixDeliveryTime` (com distinção entre maiúsculas e minúsculas). Para ativar a correção automática, os seguintes parâmetros pré-configurados devem ser fornecidos: • 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 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-TrustedRemediatorEnableRDSMultiAZ 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-TrustedRemediatorCreateEBSSnapshot A Amazon EBSsnapshots é criada.	Não são permitidos parâmetros pré-configurados. Sem restrições
em QPADk ZvH Backups do RDS	AWSManagedServices-EnableRDSBackupRetention 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 como`true`, 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-TrustedRemediatorEnableRDSInstanceStorageAutoScaling- 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 como26. 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-TrustedRemediatorEnableCLBConnectionDraining 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-TrustedRemediatorRemediateRDSParameterGroupParameter `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-TrustedRemediatorRemediateRDSParameterGroupParameter `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-TrustedRemediatorRemediateRDSParameterGroupParameter `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-TrustedRemediatorRemediateRDSParameterGroupParameter `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 subprovisionadas 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
ZRxQlPsb6c Instâncias Amazon EC2 de alta utilização	AWSManagedServices-ResizeInstanceByOneLevel 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.	• MinimumDaysSinceLastChange: 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`. • Criar AMIBefore redimensionamento: para criar a AMI da instância como backup antes do redimensionamento, escolha. `true` Para não criar um backup, escolha`false`. O padrão é `false`. Os valores válidos são `true` e `false` (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`true`. Para não redimensionar automaticamente a instância se estiver em um estado interrompido, escolha`false`. Os valores válidos são `true` e `false` (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-TrustedRemediatorRemediateRDSParameterGroupParameter 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-TrustedRemediatorRemediateRDSParameterGroupParameter `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-TrustedRemediatorRemediateRDSParameterGroupParameter `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-TrustedRemediatorRemediateRDSParameterGroupParameter `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 `innodb_stats_persistent` parâmetro Amazon RDS está desativado	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter `innodb_stats_persistent` O parâmetro está ativado para o Amazon RDS.	Não são permitidos parâmetros pré-configurados. Sem restrições
c1qf5bt037 O `general_logging` parâmetro Amazon RDS está ativado	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter `general_logging` 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 0K 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
	Internet VPC. Por padrão, o limite é aumentado em três.	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.
JI7pp0I7j9 VPC	AWSManagedServices-IncreaseServiceQuota Um novo limite para VPC 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.
Fw7hh0I7j9 Grupos de Auto Scaling	AWSManagedServices-IncreaseServiceQuota 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-IncreaseServiceQuota 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 CloudWatc

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-TrustedRemediatorEnableELBDeletionProtection- 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-TrustedRemediatorEnableRDSPerformanceInsights 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) ou731. • PerformanceInsightsKMSKeyID : O ID da AWS KMS chave para criptografia dos dados do Performance Insights. Se você não especificar um valor para PerformanceInsights KMSKey Id, 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
c1fd6b96l4 Logs de acesso do Amazon S3 habilitados	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 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 configurar as 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-percentageA 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 e executa manualmente o documento SSM a partir OpsItem do AWS Systems Manager OpsCenter console.
  - 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 emTrusted Advisor verificações suportadas pelo Trusted Remediator.
Por exemplo, para verificarQch7DwouX1, há três documentos SSM associados: AWSManagedServices-StopEC 2Instance 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 corrigidoQch7DwouX1).

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-onlyatributos automated-for-tagged-onlye 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 compatíveisTrusted Advisor verificações suportadas pelo Trusted Remediator.
3. Adicione uma tag aos recursos com a chave e o valor a seguir:
   - 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 correção manualmente a partir do OpsItem.
     - 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 é`Automated`.

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. Abra o AWS AppConfig console em https://console.aws.amazon.com/systems-manager/appconfig.

   Certifique-se de entrar como a conta de administrador delegado.
2. Selecione Trusted Remediator na lista de aplicativos.
3. Escolha o perfil de configuração de otimização de custos.
4. Selecione a bandeira de volumes subutilizados do Amazon EBS.
5. Para o modo de execução, selecione Manual.
6. Certifique-se de que os manual-for-tagged-onlyatributos automated-for-tagged-onlye estejam em branco. Esses atributos são usados para substituir o modo de execução padrão para recursos com tags correspondentes.

   Veja a seguir um exemplo da seção Atributos com valores em branco para automated-for-tagged-onlye manual-for-tagged-onlye Manual para o modo de execução:

7. Escolha Salvar para atualizar o valor e, em seguida, escolha Salvar nova versão para aplicar as alterações. Você deve escolher Salvar nova versão para que o Trusted Remediator reconheça a alteração.
8. Certifique-se de que seus volumes do Amazon EBS não tenham uma etiqueta com a chave`TR-DAvU99Dc4C-Execution-Mode`. Essa chave de tag substitui o modo de execução padrão desse volume do EBS.

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. Abra o AWS AppConfig console em https://console.aws.amazon.com/systems-manager/appconfig.

   Certifique-se de entrar como a conta de administrador delegado.
2. Selecione Trusted Remediator na lista de aplicativos.
3. Escolha o perfil de configuração de otimização de custos.
4. Selecione a bandeira de volumes subutilizados do Amazon EBS.
5. Para o modo de execução, selecione Automatizado.
6. Certifique-se de que os manual-for-tagged-onlyatributos automated-for-tagged-onlye estejam em branco. Esses atributos são usados para substituir o modo de execução padrão para recursos com tags correspondentes.

   Veja a seguir um exemplo da seção Atributos com valores em branco para automated-for-tagged-onlye manual-for-tagged-onlye Automatizado para o modo de execução:

7. Escolha Salvar para atualizar o valor e, em seguida, escolha Salvar nova versão para aplicar as alterações. Você deve escolher Salvar nova versão para que o Trusted Remediator reconheça a alteração.

   Nesse momento, todos os volumes do Amazon EBS estão configurados para correção automática.
8. Substitua a remediação automática para volumes selecionados do Amazon EBS:

   a. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
   b. Escolha Elastic Block Store, Volumes.
   c. Escolha Tags.
   d. Selecione Gerenciar tags.
   e. Adicione a seguinte tag:

      - Chave: Modo de execução TR- DAv U99Dc4C
      - Valor: Inativo

      Veja a seguir um exemplo da seção Tags que mostra os campos Chave e Valor:

f. Repita as etapas de 2 a 5 para todos os volumes do Amazon EBS que você deseja excluir da remediação.

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. Abra o AWS AppConfig console em https://console.aws.amazon.com/systems-manager/appconfig.

   Certifique-se de entrar como a conta de administrador delegado.
2. Selecione Trusted Remediator na lista de aplicativos.
3. Escolha o perfil de configuração de otimização de custos.
4. Selecione a bandeira de volumes subutilizados do Amazon EBS.
5. Para o modo de execução, selecione Condicional.
6. Defina automated-for-tagged-only como `Stage=NonProd` . Esse atributo substitui o padrão `execution-mode` para recursos com tags correspondentes. Certifique-se de que os manual-for-tagged-onlyatributos estejam em branco.

   Veja a seguir um exemplo da seção Atributos automated-for-tagged-onlydefinida como Stage= NonProd e Condicional para o modo de execução:

7. Opcionalmente, defina os parâmetros pré-configurados como um dos seguintes:

   - `CreateSnapshot=false`para não criar um snapshot do volume do Amazon EBS antes que ele seja excluído
   - `MinimumUnattachedDays=10`definir que o mínimo de dias não anexados do volume do Amazon EBS a ser excluído seja de 10 dias
   - `CreateSnapshot=false`, `MinimumUnattachedDays=10` para ambas as opções acima

8. Escolha Salvar para atualizar o valor e, em seguida, escolha Salvar nova versão para aplicar as alterações. Você deve escolher Salvar nova versão para que o Trusted Remediator reconheça a alteração.
9. Certifique-se de que seus volumes do Amazon EBS não tenham uma etiqueta com a chave`TR-DAvU99Dc4C-Execution-Mode`. Essa chave de tag substitui o modo de execução padrão desse volume do EBS.

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.
6. Para corrigir manualmente o OpsItem, conclua as seguintes etapas:
   a. Em Runbooks, escolha um dos runbooks associados (documentos SSM).
   b. Clique em Executar.
   c. Para AutomationAssumeRole , escolha `arn:aws:iam::`*`Conta da AWS ID`*`:role/ams_ssm_automation_role`. Substitua o Conta da AWS ID pelo ID da conta em que a correção é executada. Para outros valores de parâmetros, consulte os dados da operação.

      Para corrigir recursos manualmente, a função ou o usuário usado para se autenticar no Conta da AWS deve ter `iam:PassRole` as permissões para a função do IAM. `ams-ssm-automation-role` Para obter mais informações, consulte Conceder permissões a um usuário para passar uma função para um AWS service (Serviço da AWS) ou entrar em contato com seu Cloud Architect.
   d. Clique em Executar.
   e. Monitore o progresso da execução do documento SSM na coluna Status e resultados mais recentes.
   f. Depois que o documento for concluído, escolha Definir status, Resolvido para resolver manualmente o. OpsItem Se o documento falhar, revise os detalhes e execute novamente o. SSMdocument Para obter suporte adicional para solução de problemas, crie uma solicitação de serviço.

   Para resolver um problema OpsItem sem remediação, selecione Definir status como Resolvido.
7. Repita as etapas 3 e 4 para todas as correções manuais restantes. OpsItems

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 DocumentNamee 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, execute manualmente o documento SSM novamente.

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.

Para obter mais informações, consulte Integração do Trusted Remediator com QuickSight.

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"}
```

Registro de contas de membros

O Trusted Remediator cria o `Member accounts log` quando sua conta está integrada ou desembarcada. Você pode usar o `Member accounts log` para encontrar o ID da conta, a integração Regiões da AWS e o tempo de execução de cada conta de membro.

Localização do registro das contas dos membros

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/configuration_logs/member_accounts.json`

URL do arquivo de amostra de registro de contas de membros

`s3://ams-trusted-remediator-`*`111122223333`*`-logs/configuration_logs/member_accounts.json`

Formato de registro de contas de membros

```
{
    "delegated_administrator_account_id": Delegated Administrator account id,
    "appconfig_configuration_region": Trusted Remediator AppConfig Region,
    "member_accounts": [
        {
            "account_id": Member account id
            "account_partition": Member account partition (for example, aws),
            "regions": [
                {
                    "execution_time": Remediation execution time in cron schedule
 expression,
                    "execution_timezone": Timezone for the remediation execution time,
                    "region_name": Região da AWS name
                }
                ...
            ]
        }
        ...
    ],
    "updated_at": Log update time,
}
```

Exemplo de conteúdo do formato de registro de contas de membros

```
{
```

```
    "delegated_administrator_account_id": "111122223333",
    "appconfig_configuration_region": "ap-southeast-2",
    "member_accounts": [
        {
            "account_id": "222233334444",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 9 * * 6",
                    "execution_timezone": "Australia/Sydney",
                    "region_name": "ap-southeast-2"
                },
                {
                    "execution_time": "0 5 * * 7",
                    "execution_timezone": "UTC",
                    "region_name": "us-east-1"
                }
            ]
        },
        {
            "account_id": "333344445555",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 1 * * 5",
                    "execution_timezone": "Asia/Seoul",
                    "region_name": "ap-northeast-2"
                }
            ]
        }
    ],
    "updated_at": "1730869607"
}
```


Integração do Trusted Remediator com QuickSight

Você pode integrar os registros do Trusted Remediator armazenados no Amazon S3 para criar um relatório QuickSight de remediação personalizado. QuickSight a integração é opcional. Esse recurso permite que você use os registros para criar painéis de relatórios personalizados. Para obter relatórios sob solicitação para o Trusted Remediator, entre em contato com seu CSDM. Para obter mais informações sobre os relatórios disponíveis do Trusted Remediator, consulteRelatórios do Trusted Remediator.

Para obter mais informações sobre como visualizar dados em QuickSight, consulte Visualizando dados em. QuickSight

Adicionar um conjunto de dados ao registro QuickSight do item de remediação

Para adicionar um conjunto de dados ao registro QuickSight de itens de remediação, siga estas etapas:

1. Faça login no QuickSight console. Você pode criar o QuickSight relatório em qualquer um Região da AWS que QuickSight suporte. No entanto, para melhorar o desempenho e reduzir os custos, é uma prática recomendada criar o relatório na região em que o bucket de registro do Trusted Remediator está localizado.
2. Escolha Conjuntos de dados.
3. Selecione S3.
4. Na nova fonte de dados do S3, insira os seguintes valores:

   - Nome da fonte de dados: `trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-items`.
   - Faça upload de um arquivo de manifesto: crie um arquivo JSON com o conteúdo a seguir e use-o. Ao criar o arquivo, `logging_bucket_name` substitua a URIPrefixes chave.

     ```
     {
         "fileLocations": [
             {
                 "URIPrefixes": [
                     "s3://{logging_bucket_name}/remediation_items/"
                 ]
             }
         ],
         "globalUploadSettings": {
             "format": "JSON",
             "delimiter": ",",
             "textqualifier": "'",
             "containsHeader": "true"
         }
     }
     ```

   - Selecione Conectar.
   - Na janela Concluir criação do conjunto de dados, escolha Visualizar.

- QuickSight abre a nova página da planilha de análise. Agora você está pronto para criar uma nova análise usando o registro de itens de remediação.

A seguir está uma análise de amostra:

Adicione um conjunto de dados ao registro QuickSight de execução de remediação automatizada

1. Faça login no QuickSight console. Você pode criar o QuickSight relatório em qualquer um Região da AWS que QuickSight suporte. No entanto, para melhorar o desempenho e reduzir os custos, é uma prática recomendada criar o relatório na região em que o bucket de registro do Trusted Remediator está localizado.
2. Escolha Conjuntos de dados.
3. Selecione S3.
4. Na nova fonte de dados do S3, insira os seguintes valores:

   - Nome da fonte de dados:`trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-executions`.
   - Faça upload de um arquivo de manifesto: crie um arquivo JSON com o conteúdo a seguir e use esse arquivo. Ao criar o arquivo, `logging_bucket_name` substitua a URIPrefixes chave.

```
{
    "fileLocations": [
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_executions/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
}
```

- Selecione Conectar.
- Na janela Concluir criação do conjunto de dados, escolha Visualizar.
- QuickSight abre a nova página da planilha de análise. Agora você está pronto para criar uma nova análise usando o registro de itens de remediação.

A seguir está uma análise de amostra:

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 pode entrar em contato com sua CA ou CDSM para obter ajuda no gerenciamento de suas configurações. Você também pode entrar em contato com o AMS por meio de uma solicitação de serviço para suporte de configuração, correções manuais e solução de problemas de falhas de correção.

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 Accelerate. 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?

Você pode desativar o Trusted Remediator por meio do AWS AppConfig aplicativo. Para pausar ou interromper o Trusted Remediator, conclua as seguintes etapas:

1. Abra o AWS AppConfig console em https://console.aws.amazon.com/systems-manager/appconfig.
2. Selecione Trusted Remediator.
3. Escolha Configurações no perfil de configuração.
4. Selecione o indicador Suspender Trusted Remediator.
5. Defina o valor do `suspended` atributo como. `true`

> **Note**
>
> Tenha cuidado ao usar esse procedimento, pois isso interrompe o Trusted Remediator para todas as contas vinculadas à conta do administrador delegado.

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.

Como o Trusted Remediator é diferente da AWS Config remediação?

AWS Config A remediação é outra solução que ajuda você a otimizar os recursos da nuvem e manter a conformidade com as melhores práticas. A seguir estão algumas das diferenças operacionais entre as duas soluções:

- O Trusted Remediator usa Trusted Advisor o Compute Optimizer como mecanismos de detecção. AWS Config A remediação usa AWS Config regras como mecanismo de detecção.
- Para o Trusted Remediator, a remediação acontece de acordo com seu cronograma de remediação predefinido. Em AWS Config, a remediação acontece em tempo real.
- Os parâmetros para cada remediação no Trusted Remediator são facilmente personalizáveis com base em seu caso de uso, e a correção pode ser automatizada ou feita manualmente adicionando tags aos recursos.

- O Trusted Remediator fornece funcionalidade de geração de relatórios.
- O Trusted Remediator envia uma notificação por e-mail com a lista de remediação e o status da remediação.

Algumas Trusted Advisor verificações e recomendações do Compute Optimizer podem ter a mesma regra em. AWS ConfigÉ uma prática recomendada habilitar somente uma correção se houver uma AWS Config regra e Trusted Advisor verificação correspondentes. Para obter informações sobre AWS Config as regras para cada Trusted Advisor verificação, consulteTrusted Advisor verificações suportadas pelo Trusted Remediator.

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.

Monitoramento e gerenciamento de incidentes para o Amazon EKS no AMS Accelerate

O monitoramento e o gerenciamento de incidentes do Amazon EKS monitoram seus recursos do Amazon EKS em busca de falhas, degradação do desempenho e problemas de segurança. O AMS Accelerate configura e implanta as regras do gerenciador de alertas do Amazon Managed Service for Prometheus, monitora os alertas e, em seguida, executa o gerenciamento de incidentes quando esses alertas são acionados. O monitoramento e o gerenciamento de incidentes do Amazon EKS dependem do AMS Alarm Manager e aproveitam AWS serviços nativos, como Amazon Managed Service for Prometheus, Amazon Managed Grafana, Amazon e. GuardDuty AWS LambdaAWS Config

> **Note**
>
> O monitoramento e o gerenciamento de incidentes do Amazon EKS não oferecem suporte AWS GovCloud (US) a nós do Windows ou contêineres do Windows.

O que é monitoramento e gerenciamento de incidentes para o Amazon EKS no AMS Accelerate?

O monitoramento e o gerenciamento de incidentes para o Amazon EKS fornecem o seguinte:

- Uma configuração padrão que cria, gerencia e implanta monitores e políticas em toda a sua conta gerenciada para os clusters Amazon EKS selecionados por você.
- Uma linha de base de monitoramento para permitir que suas cargas de trabalho do Amazon EKS tenham maior disponibilidade, mesmo que você não configure nenhum outro monitoramento para seus clusters do Amazon EKS. Para obter mais informações, consulte Alertas básicos em monitoramento e gerenciamento de incidentes para o Amazon EKS no AMS Accelerate.
- Notificações que são geradas pelo monitoramento de linha de base configurado para seu cluster Amazon EKS. Essas notificações são conhecidas como alertas. Os alertas são gerados quando há falhas iminentes, contínuas, recorrentes ou potenciais, degradação do desempenho ou problemas de segurança. Exemplos de alertas incluem um alerta do Prometheus, um evento ou uma descoberta de AWS um serviço, como a Amazon. GuardDuty

- Investigação de alertas com orientação sobre as ações de remediação apropriadas que você pode tomar. Para obter mais informações, consulte Relatórios de incidentes e solicitações de serviço no AMS Accelerate.
- Correção de alertas e incidentes pelas operações do AMS, quando possível e com sua aprovação, para evitar ou reduzir o impacto em seus aplicativos. Para obter mais informações, consulte Relatórios de incidentes e solicitações de serviço no AMS Accelerate.
- Painéis opcionais predefinidos do Amazon Managed Grafana que fornecem visibilidade sobre a utilização de recursos, desempenho, integridade do CoreDNS, alertas ativos e alertas resolvidos anteriormente. Se você configurar o Amazon Managed Grafana usando o modelo fornecido pela AMS, poderá abrir o console do Amazon Managed Grafana para visualizar métricas e alertas para seu cluster Amazon EKS.

Como o monitoramento e o gerenciamento de incidentes do Amazon EKS funcionam no AMS Accelerate

Geração: como parte do monitoramento de integração e do gerenciamento de incidentes do EKS, o AMS configura o monitoramento básico para os clusters do Amazon EKS que você selecionou em sua conta gerenciada. O AMS usa uma combinação das regras do gerenciador de alertas do Amazon Managed Service for Prometheus e das regras de eventos da CloudWatch Amazon para configurar o monitoramento básico. Um servidor Prometheus configurado pelo AMS em seu cluster coleta e grava remotamente suas métricas do Prometheus em um endpoint do Amazon Managed Service for Prometheus na mesma região. A configuração básica de monitoramento gera um alerta quando uma regra do gerenciador de alertas do Prometheus é acionada ou CloudWatch um evento é gerado.

Agregação: o AMS envia todos os alertas que seus recursos geram para o sistema de monitoramento do AMS, direcionando-os para um tópico do Amazon Simple Notification Service gerenciado pelo AMS.

Processamento e análise de impacto: o AMS analisa os alertas e os processa com base em seu potencial de impacto. O AMS classifica os alertas da seguinte forma:

- Alertas com impacto conhecido no cliente: para esses alertas, o AMS cria um novo relatório de incidentes usando o processo de gerenciamento de incidentes.
- Alertas com impacto incerto no cliente: para esses alertas, o AMS envia um relatório de incidentes. Em muitos casos, esses alertas solicitam que você verifique o impacto antes que o AMS possa

agir. Para esses alertas, o AMS envia uma notificação de alerta com os detalhes e verifica se o alerta precisa de uma ação mitigadora. O AMS fornece opções para mitigar ações na notificação. Se sua resposta confirmar que o alerta é um incidente, o AMS aciona a criação de um novo relatório de incidentes e inicia o processo de gerenciamento de incidentes. Qualquer notificação de serviço que receba uma resposta “sem impacto no cliente” ou nenhuma resposta por três dias é marcada como resolvida. Além disso, o alerta correspondente é marcado como resolvido.

- Alertas sem impacto no cliente: se, após a avaliação, o AMS determinar que o alerta não tem nenhum impacto no cliente, o alerta será encerrado.

Matriz de responsabilidade da AMS (RACI)

O AMS responsável, responsável, consultado e informado, ou a matriz RACI, atribui a responsabilidade principal ao cliente ou à AMS por uma variedade de atividades. A tabela a seguir fornece uma visão geral das responsabilidades do cliente e do AMS pelas atividades em um aplicativo que usa monitoramento e gerenciamento de incidentes para o Amazon EKS.

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

Atividades	Cliente	AMS
Descoberta para requisitos de AMS	eu	R
Ativar permissões AMS (RBAC) para acesso ao cluster	R	C
Instale o Amazon EC2 Systems Manager Agent nos	R	C

Atividades	Cliente	AMS
nós de trabalho, caso ele ainda não esteja presente		
Implante componentes do AMS no cluster, como Prometheus, Prometheu s Node Exporter e em um namespace AMS, conforme necessário. kube-state-metrics	C	R
Provisione o Amazon Managed Service para Prometheus no plano de controle do AMS	eu	R
Configurar o gerenciador de alertas Prometheus no plano de controle do AMS	eu	R
Forneça o modelo Amazon Managed Grafana e ajude na configuração	C	R
Ative o monitoramento do registro de auditoria do GuardDuty EKS	C	R
Habilite o registro do plano de controle do Amazon EKS	eu	R
Monitore a integridade e o desempenho do plano de controle Amazon EKS	eu	R

Atividades	Cliente	AMS
Monitore a integridade e o desempenho do seu cluster Amazon EKS (cluster, nó, carga de trabalho, pod, servidor de API e CoreDNS)	eu	R
Faça a triagem de alertas e forneça respostas a incidentes para o Amazon EKS	eu	R
Execute comandos de diagnóstico durante incidentes	eu	R
Analise os registros durante incidentes (plano de controle e registros do pod)	eu	R
Resposta a incidentes para problemas AWS de rede	eu	R
Responda às descobertas do GuardDuty EKS Audit Log Monitoring	eu	R
Forneça orientação ao cliente sobre ações para remediar incidentes quando possível	eu	R

Alertas básicos em monitoramento e gerenciamento de incidentes para o Amazon EKS no AMS Accelerate

Depois de verificar os alertas, o AMS ativa os seguintes alertas para o Amazon EKS e, em seguida, se envolve no monitoramento e no gerenciamento de incidentes para seus clusters selecionados do Amazon EKS. O tempo de resposta dos Acordos de Nível de Serviço (SLAs) e os Objetivos de Nível de Serviço (SLOs) dependem do Nível de Serviço de sua conta selecionada (Plus, Premium).

Para obter mais informações, consulte Relatórios de incidentes e solicitações de serviço no AMS Accelerate.

Alertas e ações

A tabela a seguir lista os alertas do Amazon EKS e as respectivas ações que o AMS executa:

Alerta	Limites	Ação
O contêiner OOM foi eliminado	O número total de reinicial izações de contêineres nos últimos 10 minutos é de pelo menos 1 e um contêiner Kubernetes em um pod foi encerrado com o motivo “OOMKilled” nos últimos 10 minutos.	O AMS investiga se a eliminação do OOM é causada por ter atingido o limite de contêineres ou a sobrecarga do limite de memória e, em seguida, aconselha você sobre ações corretivas.
Falha no Pod Job	Falha na conclusão de um trabalho do Kubernetes. A falha é indicada pela presença de pelo menos um status de trabalho com falha.	O AMS investiga por que o trabalho do Kubernetes ou o cron job correspondente está falhando e, em seguida, aconselha você sobre ações corretivas.
StatefulSet Para baixo	O número de réplicas prontas para atender ao tráfego não corresponde ao número atual de réplicas existentes StatefulSet por pelo menos 1 minuto.	O AMS determina por que os pods não estão prontos analisando as mensagens de erro nos eventos do pod e os trechos do registro de erros nos logs do pod e, em seguida, aconselha você sobre ações corretivas.
Capacidade de escalabilidade HPA	O escalonador automático horizontal de pods (HPA) não pode ser escalado porque a condição de status “AbleToSc	O AMS determina qual Kubernetes Horizontal Pod Autoscaler (HPA) não consegue escalar pods para

Alerta	Limites	Ação
	ale” é falsa por pelo menos 2 minutos.	seu recurso de carga de trabalho subsequente, como uma implantação ou. StatefulS et
Disponibilidade da métrica HPA	O Horizontal Pod Autoscaler (HPA) não consegue coletar métricas porque a condição de status “ScalingActive” é falsa por pelo menos 2 minutos.	O AMS determina por que o HPA não pode coletar métricas, como métricas relacionadas a problemas de configuração do servidor ou problemas de autorização do RBAC.
O pod não está pronto	Um pod do Kubernetes permanece em um estado sem execução (como Pendente, Desconhecido ou Falha) por mais de 15 minutos.	O AMS investiga os pods afetados para obter detalhes, analisa os registros dos pods em busca de erros e eventos relacionados e, em seguida, aconselha você sobre ações corretivas.
Pod Crash Looping	Um contêiner de cápsulas reinicia pelo menos uma vez a cada 15 minutos por um período de 1 hora.	O AMS investiga os motivos da não inicialização do pod, como recursos insuficie ntes, um arquivo bloqueado por outro contêiner, banco de dados bloqueado por outro contêiner, falhas nas dependências do serviço, problemas de DNS para serviços externos e configura ções incorretas.

Alerta	Limites	Ação
Daemonset está programado incorretamente	Há pelo menos um pod do Kubernetes Daemonset programado incorretamente em um período de 10 minutos.	O AMS determina por que um Daemonset está programad o em um nó onde eles não deveriam ser executados. Isso pode acontecer quando o pod errado nodeSelector/ taints/affinities foi aplicado aos pods do Daemonset ou quando os nós (pools de nós) foram contaminados e os pods existentes não foram programados para serem despejados.
Erros da API Kubernetes	A taxa de erro do servidor da API Kubernetes excede 3% em um período de 2 minutos.	O AMS analisa os registros do plano de controle para determinar o volume e os tipos de erros que estão causando esse alerta e identifica quaisquer problemas de contenção de recursos para grupos de escalonamento automático do nó principal ou do etcd. Se o servidor da API não se recuperar, o AMS contrata a equipe de serviço do Amazon EKS.

Alerta	Limites	Ação
Latência da API Kubernetes	A latência do 99º percentil das solicitações para o servidor da API Kubernetes excede 1 segundo em um período de 2 minutos.	O AMS analisa os registros do plano de controle para determinar o volume e os tipos de erros que estão causando latência e identifica quaisquer problemas de contenção de recursos para grupos de auto-scaling do nó principal ou do etcd. Se o servidor da API não se recuperar, o AMS contrata a equipe de serviço do Amazon EKS.
Expiração do certificado do cliente Kubernetes	O certificado do cliente usado para se autenticar no servidor da API Kubernetes expirará em menos de 24 horas.	O AMS envia essa notificaç ão para informá-lo de que seu certificado de cluster expirará em 24 horas.
O Node não está pronto	O status da condição “Pronto” do Node é falso por pelo menos 10 minutos.	O AMS investiga as condições e os eventos do nó, como problemas de rede, que impedem o acesso do kubelet ao servidor da API.
CPU Node High	A carga da CPU excede 80% em um período de 5 minutos.	O AMS determina se um ou mais pods estão consumindo uma quantidade anormalme nte alta de CPU. Em seguida, o AMS verifica com você se suas solicitações, limites e atividades do pod estão conforme o esperado.

Alerta	Limites	Ação
Detectada a morte do Node OOM	Há pelo menos uma eliminação de OOM do host relatada pelo nó em uma janela de 4 minutos.	O AMS determina se a eliminação do OOM é causada pelo alcance do limite do contêiner ou pela sobrecarga do nó. Se a atividade do aplicativo for normal, o AMS o aconselhará sobre solicitações e limites para supercomprometimentos e sobre a revisão dos limites dos pods.
Limite de conexão do Node	A proporção entre o número atual de entradas de rastreamento de conexão e o limite máximo excede 80% em um período de 5 minutos.	O AMS aconselha você sobre o valor de conexão recomendado por núcleo. Os nós do Kubernetes definem o valor máximo do conntrack proporcional à capacidade total de memória do nó. Aplicações de alta carga, especialmente em nós menores, podem facilmente exceder o valor máximo do conntrack, resultando em redefinições e tempos limite de conexão.
O relógio do Node não está sincronizado	O status mínimo de sincronização em um período de 2 minutos é 0 e o erro máximo em segundos é 16 ou superior.	O AMS determina se o Network Time Protocol (NTP) está instalado e funcionando corretamente.

Alerta	Limites	Ação
CPU Pod High	O uso da CPU de um contêiner excede 80% em uma taxa de 3 minutos por um período mínimo de 2 minutos.	O AMS investiga os registros do pod para determinar as tarefas do pod que consomem uma grande quantidade de CPU.
Pod de alta memória	O uso de memória de um contêiner excede 80% do limite de memória especific ado em um período de 2 minutos.	O AMS investiga os registros do pod para determinar as tarefas do pod que consomem uma grande quantidade de memória.
CoreDNS inativo	O CoreDNS desapareceu da descoberta de alvos do Prometheus por mais de 15 minutos.	Esse é um alerta crítico que indica que a resolução do nome de domínio para serviços de cluster internos ou externos foi interrompida. O AMS verifica o status dos pods do CoreDNS, verifica a configuração do CoreDNS, verifica os endpoints de DNS que apontam para os pods do CoreDNS, verifica os limites do CoreDNS e, com sua aprovação, ativa o registro de depuração do CoreDNS.

Alerta	Limites	Ação
Erros do CoreDNS	O CoreDNS retorna erros SERVFAIL para mais de 3% das solicitações de DNS em um período de 10 minutos.	Esse alerta pode indicar um problema com um aplicativo ou uma configuração incorreta . O AMS verifica o status dos pods do CoreDNS, verifica a configuração do CoreDNS, verifica os endpoints de DNS que apontam para os pods do CoreDNS, verifica os limites do CoreDNS e, com sua aprovação, ativa o registro de depuração do CoreDNS.
Latência do CoreDNS	O 99º percentil da duração das solicitações de DNS excede 4 segundos por 10 minutos.	Esse alerta indica que o CoreDNS pode estar sobrecarregado. O AMS verifica o status dos pods do CoreDNS, verifica a configura ção do CoreDNS, verifica os endpoints de DNS que apontam para os pods do CoreDNS, verifica os limites do CoreDNS e, com sua aprovação, ativa o registro de depuração do CoreDNS.

Alerta	Limites	Ação
Latência de encaminhamento do CoreDNS	O 99º percentil do tempo de resposta das solicitações de encaminhamento do CoreDNS para o kube-dns excede 4 segundos em um período de 10 minutos.	Quando o CoreDNS não é o servidor autoritativo ou não tem uma entrada de cache para um nome de domínio, o CoreDNS encaminha a solicitação de DNS para um servidor DNS upstream. Esse alerta indica que o CoreDNS pode estar sobrecarregado ou que pode haver um problema com um servidor DNS upstream. O AMS verifica o status dos pods do CoreDNS, verifica a configuração do CoreDNS, verifica os endpoints de DNS que apontam para os pods do CoreDNS, verifica os limites do CoreDNS e, com sua aprovação, ativa o registro de depuração do CoreDNS.

Alerta	Limites	Ação
Erro de encaminhamento do CoreDNS	Mais de 3% das consultas de DNS falham em um período de 5 minutos.	Quando o CoreDNS não é o servidor autoritativo ou não tem uma entrada de cache para um nome de domínio, o CoreDNS encaminha a solicitação de DNS para um servidor DNS upstream. Esse alerta sinaliza uma possível configuração incorreta ou um problema com um servidor DNS upstream. O AMS verifica o status dos pods do CoreDNS, verifica a configuração do CoreDNS, verifica os endpoints de DNS que apontam para os pods do CoreDNS, verifica os limites do CoreDNS e, com sua aprovação, ativa o registro de depuração do CoreDNS.

Requisitos para monitoramento e gerenciamento de incidentes para o Amazon EKS no AMS Accelerate

Esses são os recursos and/or necessários para monitoramento e gerenciamento de incidentes do Amazon EKS for AMS Accelerate

- Versões compatíveis do Kubernetes: consulte as versões do Kubernetes do Amazon EKS no Guia do usuário do Amazon EKS.
- Tipos de nós: os nós gerenciados do Amazon EKS são compatíveis. Não há suporte para nós e contêineres do Windows.
- Acesso ao cluster Kubernetes: o AMS requer a função de cluster RBAC e o usuário do cluster system:masters.

- Agente SSM nos EC2 nós da Amazon: Tanto o Bottle Rocket quanto o Amazon EKS AMIs têm o SSM Agent pré-instalado. Certifique-se de que o SSM Agent esteja instalado em seus EC2 nós personalizados AMIs e da Amazon.
- Para obter mais informações, consulte as cotas de serviço do Amazon Managed Service for Prometheus e do Amazon Managed Grafana.
- AWS Regiões suportadas:

Nome da região	Região	Região de armazenamento de métricas
Leste dos EUA (Ohio)	us-east-2	us-east-2
Leste dos EUA (Norte da Virgínia)	us-east-1	us-east-1
Oeste dos EUA (Oregon)	us-west-2	us-west-2
Ásia-Pacífico (Tóquio)	ap-northeast-1	ap-northeast-1
Ásia-Pacífico (Seul)	ap-northeast-2	ap-northeast-2
Ásia-Pacífico (Singapura)	ap-southeast-1	ap-southeast-1
Ásia-Pacífico (Sydney)	ap-southeast-2	ap-southeast-2
Europa (Frankfurt)	eu-central-1	eu-central-1
Europa (Irlanda)	eu-west-1	eu-west-1
Europa (Londres)	eu-west-2	eu-west-2
África (Cidade do Cabo)	af-south-1	eu-west-1 eu-west-2
Ásia-Pacífico (Hong Kong)	ap-east-1	ap-northeast-1 ap-northeast-2

> **Note**
>
> As métricas para clusters do Amazon EKS em af-south-1, África (Cidade do Cabo) e ap-east-1, Ásia-Pacífico (Hong Kong) são exportadas para o serviço de monitoramento AMS no mesmo local, respectivamente. Região da AWS As métricas para elas Regiões da AWS são então transportadas dentro do serviço de monitoramento do AMS para diferentes regiões onde são processadas e armazenadas. Consulte a tabela anterior para as regiões que o serviço de monitoramento do AMS usa para armazenar métricas.

Integre-se ao monitoramento e ao gerenciamento de incidentes do Amazon EKS no AMS Accelerate

Execute as etapas a seguir para integrar o monitoramento e o gerenciamento de incidentes do Amazon EKS.

1. Ative as tags de otimização de custos do Amazon EKS: consulte Como marcar seus recursos para faturamento no Guia do usuário do Amazon EKS.
2. Inicie a integração do monitoramento e gerenciamento de incidentes para o EKS: entre em contato com seu Cloud Service Delivery Manager (CSDM) com os nomes da conta IDs e do cluster para integrar.
3. Valide os requisitos: Seu Cloud Architect (CA) valida se todos os requisitos foram atendidos antes do início da integração.
4. Atualize o controle de acesso baseado em funções (RBAC) do Kubernetes: o AMS compartilha os comandos para implementar essas mudanças. `eksctl` Você pode revisar essas alterações e depois implantar. Você deve implantar atualizações do RBAC para que o AMS tenha permissões para executar comandos em seu nome. Essas atualizações incluem mapear a função do AMS IAM para um usuário do Kubernetes, criar uma nova função de cluster do Kubernetes para o AMS e vincular a função de cluster do AMS Kubernetes ao usuário.
5. Implante componentes de cluster: O AMS implanta os seguintes componentes em um namespace gerenciado pelo AMS em seu cluster:
   - Servidor Prometheus
   - Exportador de nós Prometheus (não aplicável para) AWS Fargate
   - kube-state-metrics

6. Execute atualizações de configuração do Prometheus: o AMS configura o Prometheus para permitir a gravação remota de métricas.
7. (Opcional) Configurar painéis: sua CA ajuda você a configurar painéis do Amazon Managed Grafana em sua conta.

> **Note**
>
> Depois que seu cluster Amazon EKS é integrado, o AMS analisa os sinais de alerta e realiza uma avaliação básica para identificar problemas existentes em seu cluster. Após a conclusão da avaliação básica, o AMS compartilha descobertas e recomendações de remediação por meio do Trusted Advisor e de uma solicitação de serviço que você pode usar para resolver problemas em seu cluster. A partir da avaliação, o AMS cria uma linha de base de monitoramento do Amazon EKS específica para seus clusters EKS ajustando nossos limites de alarme em nível de conta. Para eliminar respostas duplicadas do AMS contra essas descobertas, ajustamos nosso monitoramento para excluir esses sinais de alerta. Reajustamos nosso monitoramento para incluir os sinais quando seu CSDM nos informa que os problemas subjacentes foram corrigidos.

Fora do monitoramento e gerenciamento de incidentes para o Amazon EKS no AMS Accelerate

Notifique seu gerente de entrega de serviços em nuvem (CSDM) com os nomes da conta IDs e do cluster para iniciar o processo de desligamento. Após a desativação, o processamento de alertas, o armazenamento de métricas e a consulta de métricas são suspensos e as métricas são excluídas de acordo com as políticas padrão de retenção de dados do Amazon Managed Service for Prometheus.

O AMS executa as seguintes etapas de desativação:

1. O AMS desativa os alertas que são enviados para você e para as operações do AMS.
2. O AMS remove a instância Prometheus do seu cluster Amazon EKS.
3. O AMS remove outros AWS recursos que estão instalados na sua conta, como funções e AWS Config regras do IAM.

Depois que essas etapas forem concluídas, você deverá concluir as seguintes etapas de desativação:

1. Use `eksctl` para remover as permissões RBAC do Kubernetes do. `aws-auth` `ConfigMap`
2. Se você a instalou anteriormente, remova a instância Amazon Managed Grafana que você configurou para se conectar ao AMS.

Gerenciamento de continuidade no AMS Accelerate

O AMS aproveita AWS Backup para centralizar e automatizar o backup de seus dados em todos os serviços. AWS Os planos de backup do AMS fornecem as melhores práticas para vários casos de uso; no entanto, você pode continuar usando seus planos de backup existentes. Depois de integrar o gerenciamento de backup do AMS, o AMS fornece relatórios de backup e os especialistas do AMS monitoram continuamente suas tarefas de backup para garantir que você tenha uma solução de backup confiável.

Para saber mais, consulte AWS Backup: Como funciona e AWS recursos suportados e aplicativos de terceiros.

O AMS Accelerate fornece uma variedade de serviços operacionais para ajudá-lo a alcançar a excelência operacional em AWS. Para obter uma compreensão rápida de como o AMS ajuda suas equipes a alcançar a excelência operacional geral Nuvem AWS com alguns de nossos principais recursos operacionais, incluindo suporte técnico 24 horas por dia, 7 dias por semana, monitoramento proativo, segurança, aplicação de patches, registro e backup, consulte Diagramas de arquitetura de referência do AMS.

Assista ao vídeo de Carl para saber mais (9:29)

Tópicos

- Como o gerenciamento de continuidade funciona no AMS
- Selecione um plano de backup do AMS
- Marque seus recursos para aplicar os planos de backup do AMS
- Exibir backups em cofres do AMS
- Monitoramento e relatórios de backup do AMS

Como o gerenciamento de continuidade funciona no AMS

Os planos de backup do AMS definem a frequência com que seus dados são copiados e a política de retenção para seus backups. Os cofres de backup do AMS mantêm seus dados de backup organizados. Depois que um recurso é associado a um plano de backup, os recursos compatíveis são copiados de forma incremental. O primeiro backup é uma cópia completa e os backups subsequentes capturam alterações incrementais. Dependendo do recurso e do plano de backup

do AMS selecionado, a Point-in-time restauração (PITR) permite que você retroceda seus recursos selecionando um horário para sua recuperação. Para começar a usar o AMS Backup Management, basta selecionar um plano de backup do AMS e marcar seus recursos.

> **Note**
>
> Certifique-se de que AWS Backup esteja habilitado para cada conta e tipo de recurso seguindo as etapas aqui: Introdução 1: Opção de serviço. Região da AWS
> Você não precisa continuar em Introdução 2: Criar backup sob demanda.

Tópicos relacionados de AWS Backup

- Trabalhando com backups (criar, editar, copiar, restaurar, excluir)
- Criar um backup sob demanda
- Criação de cópias de backup em Regiões da AWS
- AWS Backup Supported Services (Serviços compatíveis)
- Point-in-time restaurar
- AWS Backup Atributos

Selecione um plano de backup do AMS

O AMS fornece três planos de backup diferentes, com um quarto plano de backup para minimizar os custos durante a integração. Para selecionar um plano de backup do AMS para cada recurso suportado, marque o recurso com a tag associada ao plano. À medida que você se inscreve no Accelerate, o AMS trabalhará com você para identificar o plano de backup que melhor atenda às suas necessidades.

> **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. Para obter mais informações, consulte Criação de um plano de backup.

Plano de backup padrão do AMS

AWS Backup o backup contínuo não está habilitado para esse plano de backup; para obter detalhes, consulte Restauração em um horário especificado usando point-in-time restauração (PITR).

Chave TAG: `ams:rt:backup-orchestrator`

Valor da TAG: `true`

Plano de backup padrão do AMS	Horário de início do cluster	Retenção
backup de hora em hora	N/D	N/D
backup diário	diariamente 4:00 UTC	7 dias
backup semanal	Sábado, 2:00 UTC	4 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 aprimorado

AWS Backup o backup contínuo é ativado com retenção máxima (31 dias) dos recursos suportados; para obter detalhes, consulte Restauração em um tempo especificado usando point-in-time restauração (PITR) e Serviços e aplicativos suportados para point-in-time restauração (PITR).

Chave TAG: `ams:rt:backup-orchestrator-enhanced`

Valor da TAG: `true`

Plano de backup aprimorado	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

Plano de backup aprimorado	Horário de início do cluster	Retenção
backup mensal	1º dia do mês, 2:00 UTC	26 semanas
backup anual	1º de janeiro, 2:00 UTC	2 anos

Plano de backup sensível a dados

AWS Backup o backup contínuo é ativado com retenção máxima (31 dias) dos recursos suportados; para obter detalhes, consulte Restauração em um tempo especificado usando point-in-time restauração (PITR) e Serviços e aplicativos suportados para point-in-time restauração (PITR).

Chave TAG: `ams:rt:backup-orchestrator-data-sensitive`

Valor da TAG: `true`

Plano de backup sensível a dados	Horário de início do cluster	Retenção
backup de hora em hora	a cada 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

Plano de backup de integração do AMS Accelerate

AWS Backup o backup contínuo não está habilitado para esse plano de backup; para obter detalhes, consulte Restauração em um horário especificado usando point-in-time restauração (PITR).

Chave TAG: `ams:rt:backup-orchestrator-onboarding`

Valor da TAG: `true`

Plano de backup de integração do AMS Accelerate	Horário de início do cluster	Retenção
backup de hora em hora	a cada hora	2 semanas
backup diário	N/D	N/D
backup semanal	N/D	N/D
backup mensal	N/D	N/D
backup anual	N/D	N/D

AWS Backup Tópicos relacionados

- Criação de um plano de backup
- Point-in-time A restauração (PITR) permite backups contínuos dos recursos suportados e permite que você selecione um horário específico para sua recuperação. Para obter uma lista dos recursos compatíveis, consulte Disponibilidade de recursos por recurso.

Marque seus recursos para aplicar os planos de backup do AMS

Para atribuir recursos a um plano de backup do AMS, marque o recurso com o par de chave-valor da etiqueta do plano. Você pode usar o AMS Resource Tagger para aplicar os planos de backup do AMS a um subconjunto de seus recursos ou a todos os recursos suportados em sua conta. Se você quiser usar um método alternativo para aplicar tags aos seus recursos, como AWS CloudFormation ou Terraform, desative o Resource Tagger para que ele não concorra com o método de marcação escolhido. Para obter mais informações, consulte Impedindo que o Resource Tagger modifique recursos.

O exemplo a seguir demonstra como você pode usar o Resource Tagger para aplicar o plano de backup padrão do AMS nas instâncias do Amazon Elastic Compute Cloud em sua conta. Para esse plano de backup, aplique a chave `ams:rt:backup-orchestrator` e o valor da tag`true`. Para usar um plano de backup diferente, altere a chave para corresponder à chave de tag do plano de backup desejado. Para saber mais sobre o AMS Resource Tagger e entender como integrar o perfil referenciado a seguir com o perfil atual (já configurado) em sua conta do Accelerate, consulte. Acelere o marcador de recursos

1. Abra o AWS AppConfig console em https://console.aws.amazon.com/systems-manager/appconfig.
2. Escolha o aplicativo do ResourceTagger.
3. Escolha a guia Perfis de configuração e, em seguida, escolha CustomerManagedTags
4. Escolha Criar para criar uma nova versão.
5. Escolha JSON e, em seguida, copie e cole o seguinte objeto JSON:

```
{
    "AWS::EC2::Instance": {
        "AccelerateBackupPlan": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "*"
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:backup-orchestrator",
                    "Value": "true"
                }
            ]
        }
    }
}
```

6. Escolha Criar versão de configuração hospedada.
7. Selecione Iniciar implantação.
8. Defina os seguintes detalhes de implantação:

```
Environment: AMSInfrastructure
Hosted configuration version: Select the version that you have just created.
Deployment Strategy: AMSNoBakeDeployment
```

9. Selecione Iniciar implantação. O Resource Tagger marca suas instâncias`ams:rt:backup-orchestrator: true`, garantindo que seu backup seja feito de acordo com o plano de backup padrão do AMS.

Exibir backups em cofres do AMS

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	Chave de etiqueta do plano de backup do AMS
ams-automated-backups	ams:rt:backup-orchestrator
ams-automated-enhanced-backups	ams: rt: backup-orchestrator-enhanced
ams-automated-data-sensitive-backups	ams: rt: backup-orchestrator-data-sensitive
ams-onboarding-backups	ams: rt: backup-orchestrator-onboarding

Outros cofres AMS

Nome do AMS Vault	Descrição
ams-manual-backups	Esse cofre contém backups iniciados manualmente criados pelo documento `AWSManagedServices-StartBackupJob` SSM Automation e backups pré-patch criados pelas automações de patch do AMS antes da aplicação de patches.
ams-custom-backups	Esse é o cofre recomendado para backups criados fora dos planos de backup do AMS.

AWS Backup Tópicos relacionados

- Exibir backups por recurso
- Trabalhando com backups

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 backup diário Relatório .

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.

Entenda o gerenciamento de patches no AMS Accelerate

Important

O Accelerate Patch Reporting implanta periodicamente uma política baseada em AWS Glue recursos. Esteja ciente de que as atualizações do AMS no sistema de patches substituem as políticas existentes baseadas em AWS Glue recursos.

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

Você pode usar o sistema de patches do AMS Accelerate, Patch Add-On, para corrigir suas instâncias com atualizações relacionadas à segurança e outros tipos de atualizações. O Accelerate Patch Add-On é um recurso que fornece patches baseados em tags para instâncias do AMS. Ele 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. O complemento AMS Accelerate Patch é uma opção de integração. Se você não o obteve durante a integração de sua conta do Accelerate, entre em contato com seu gerente de prestação de serviços em nuvem (CSDM) para obtê-lo.

O gerenciamento de patches do AMS Accelerate usa a funcionalidade básica de patches do Systems Manager para controlar a definição dos patches que são aplicados em uma instância. A linha de base do patch contém a lista de patches pré-aprovados; por exemplo, todos os patches de

segurança. A conformidade da instância é medida em relação à linha de base do patch associada a ela. O AMS Accelerate, por padrão, instala todos os patches disponíveis para manter a instância atualizada.

> **Note**
>
> O AMS Accelerate aplica somente patches do sistema operacional (SO). Por exemplo, para o Windows, somente as atualizações do Windows são aplicadas, não as atualizações da Microsoft.

Para obter informações sobre relatórios, consulteRelatórios de gerenciamento de hosts do AMS.

O AMS Accelerate fornece uma variedade de serviços operacionais para ajudá-lo a alcançar a excelência operacional em AWS. Para obter uma compreensão rápida de como o AMS ajuda suas equipes a alcançar a excelência operacional geral Nuvem AWS com alguns de nossos principais recursos operacionais, incluindo suporte técnico 24 horas por dia, 7 dias por semana, monitoramento proativo, segurança, aplicação de patches, registro e backup, consulte Diagramas de arquitetura de referência do AMS.

Tópicos

- Recomendações de patches
- Crie uma janela de manutenção de patches no AMS
- Patch com ganchos
- Linha de base do patch AMS Accelerate
- Criação de uma função do IAM para aplicação de patches sob demanda do AMS Accelerate
- Entenda as notificações de patches e as falhas de patches no AMS Accelerate

Recomendações de patches

Se você está envolvido em operações de aplicativos ou infraestrutura, você entende a importância de uma solução de patches do sistema operacional (OS) que seja flexível e escalável o suficiente para atender aos diversos requisitos de suas equipes de aplicativos. Em uma organização típica, algumas equipes de aplicativos usam uma arquitetura que envolve instâncias imutáveis, enquanto outras implantam seus aplicativos em instâncias mutáveis.

Para obter mais informações sobre a orientação AWS prescritiva para aplicação de patches, consulte Correção automática de patches para instâncias mutáveis na nuvem híbrida usando. AWS Systems Manager

> **Note**
>
> O Accelerate Patch Add-On é um recurso que fornece patches baseados em tags para instâncias do AMS. Ele 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. O complemento AMS Accelerate Patch é uma opção de integração. Se você não o obteve durante a integração de sua conta do Accelerate, entre em contato com seu gerente de prestação de serviços em nuvem (CSDM) para obtê-lo.

Recomendações de responsabilidade do patch

O processo de aplicação de patches para instâncias persistentes deve envolver as seguintes equipes e ações:

- As equipes de application (DevOps) definem os grupos de patches para seus servidores com base no ambiente do aplicativo, no tipo de sistema operacional ou em outros critérios. Também definem as janelas de manutenção específicas para cada grupo de patches. Essas informações devem ser armazenadas em tags anexadas às instâncias. Os nomes de tag recomendados são 'Grupo de patches' e 'Janela de manutenção'. Durante cada ciclo de patch, as equipes de aplicativos se preparam para o patch, testam o aplicativo após o patch e solucionam quaisquer problemas com seus aplicativos e sistemas operacionais durante o patch.
- A equipe de operações de segurança define as linhas de base de patches para vários tipos de sistemas operacionais usados pelas equipes de aplicativos e disponibiliza os patches por meio do Systems Manager Patch Manager.
- A solução automatizada de patches é executada regularmente e implanta os patches definidos nas linhas de base do patch, com base nos grupos de patches definidos pelo usuário e nas janelas de manutenção.
- As equipes de governança e conformidade definem diretrizes de correção e processos e mecanismos de exceção.

Para obter mais informações, consulte Design da solução de patches para instâncias mutáveis EC2 .

Orientação para equipes de aplicação

- Analise e familiarize-se com a criação e o gerenciamento de janelas de manutenção; consulte Janelas de AWS Systems Manager manutenção e Crie uma janela de manutenção do SSM para aplicação de patches para saber mais. Compreender a estrutura geral e o uso das janelas de manutenção ajuda você a entender quais informações fornecer se você não for a pessoa que as criou.
- Para configurações de alta disponibilidade (HA), planeje ter uma janela de manutenção por zona de disponibilidade e por ambiente (Dev/Test/Prod). Isso garantirá a disponibilidade contínua durante a aplicação de patches.
- A duração recomendada da janela de manutenção é de 4 horas com um limite de 1 hora, mais 1 hora adicional por 50 instâncias
- Atualize as versões de desenvolvimento e teste com tempo suficiente entre elas para permitir que você identifique possíveis problemas antes da aplicação de patches de produção.
- Automatize tarefas comuns de pré e pós-aplicação de patches por meio da automação SSM e execute-as como tarefas da janela de manutenção. Observe que, para tarefas de pós-aplicação de patches, você deve garantir que haja tempo suficiente, pois as tarefas não serão iniciadas quando o limite for atingido.
- Familiarize-se com as linhas de base de patches e seus recursos, principalmente com relação aos atrasos na aprovação automática de tipos de severidade de patches que podem ser usados para garantir que somente os patches aplicados sejam aplicados na produção Dev/Test posteriormente. Consulte Sobre as linhas de base do patch para obter detalhes.

Orientação para equipes de operações de segurança

- Revise e familiarize-se com as linhas de base do patch. A aprovação de patches é feita de forma automatizada e tem diferentes opções de regras. Consulte Sobre as linhas de base do patch para obter mais informações.
- Discuta as necessidades relacionadas à aplicação de patches Dev/Test/Prod com as equipes de aplicativos e desenvolva várias linhas de base para acomodar essas necessidades.

Orientação para equipes de governança e conformidade

- A correção deve ser uma função de “exclusão”. Uma janela de manutenção padrão e uma marcação automatizada devem existir para garantir que nada fique sem correção. O AMS

Resource Tagger pode ajudar com isso; discuta essa opção com seu arquiteto de nuvem (CA) ou gerente de prestação de serviços em nuvem (CSDM) para obter orientação sobre a implementação.

- Os pedidos de isenção da aplicação de patches devem exigir documentação que justifique a isenção. Um diretor de segurança da informação (CISO) ou outro oficial de aprovação deve aprovar ou negar a solicitação.
- A conformidade dos patches deve ser revisada regularmente por meio do console do Patch Manager, do Security Hub ou de um scanner de vulnerabilidades.

Exemplo de design para aplicativo Windows de alta disponibilidade

Visão geral:

- Uma janela de manutenção por AZ.
- Um conjunto de janelas de manutenção por ambiente.
- Uma linha de base de patch por ambiente:
  - Desenvolvedor: aprove toda a severidade e classificação após 0 dias.
  - Teste: aprove os patches críticos de atualização de segurança após 0 dias e todas as outras classificações e severidades após 7 dias.
  - Prod: Aprove os patches críticos de atualização de segurança após 0 dias e todas as outras classificações e severidades após 14 dias.

CloudFormation Roteiros:

Esses scripts são configurados para criar janelas de manutenção, linhas de base e tarefas de correção para um EC2 aplicativo Windows HA de duas zonas de disponibilidade usando as configurações básicas de aprovação descritas acima.

- Exemplo de pilha CFN para desenvolvedores do Windows: ha-patching-dev-stack.json
- Exemplo de pilha CFN de teste do Windows: ha-patching-test-stack.json
- Exemplo de pilha CFN do Windows Prod: ha-patching-prod-stack.json

Recomendações de patch FAQs

P: Como faço para lidar com correções não programadas para exploits de “0” dias?

R: O SSM oferece suporte ao recurso Patch Now que usa a linha de base padrão atual para o sistema operacional da instância. O AMS implanta um conjunto padrão de linhas de base de patches que aprova todos os patches após 0 dias. No entanto, ao usar o recurso Patch Now, um instantâneo de pré-patch não é obtido, pois esse comando executa o documento AWS- RunPatchBaseline SSM. Recomendamos que você faça um backup manual antes de aplicar o patch.

P: O AMS oferece suporte à aplicação de patches para instâncias em grupos de escalonamento automático ()? ASGs

R: Não. No momento, os clientes do Accelerate não oferecem suporte à aplicação de patches do ASG.

P: Há alguma limitação que o Windows de manutenção deva ter em mente?

R: Sim, existem algumas limitações que você deve conhecer.

- Windows de manutenção por conta: 50
- Tarefas por janela de manutenção: 20
- Número máximo de automações simultâneas por janela de manutenção: 20
- Número máximo de janelas de manutenção simultâneas: 5

Para obter uma lista completa dos limites padrão de SSM, consulte AWS Systems Manager endpoints e cotas.

Crie uma janela de manutenção de patches no AMS

Uma janela de manutenção de patches executa as automações de patches do AMS em um cronograma definido para EC2 instâncias específicas da Amazon. Os destinos são definidos por uma tag ou tags para um grupo de instâncias. Você pode definir horários com base em dias e horários próximos ao Patch Tuesday, ou você pode definir um cronograma usando uma expressão cron. Para obter mais informações, consulte Referência: expressão cron e expressão rate para Gerenciador de Sistemas no Guia do usuário do AWS Systems Manager . Antes da aplicação de patches, o AMS cria um instantâneo do volume raiz de cada instância. Se o AMS detectar que a aplicação de patches afeta a integridade da instância, ou se você notificar o AMS sobre o impacto da aplicação de patches

no aplicativo, o AMS usará esse snapshot para restaurar o volume raiz para um estado anterior ao patch.

Limites da janela de manutenção do patch AMS Accelerate

Usos de patches do AMS AWS Systems Manager (Systems Manager). Além dos limites de serviço do Systems Manager, a aplicação de patches do AMS tem um limite de 300 instâncias de destino por janela de manutenção de patches. Considerando um tempo geral de conclusão do patch de 30 minutos por instância, a tabela a seguir fornece exemplos de números de janelas e durações de manutenção.

Instâncias a serem corrigidas	Duração das janelas de manutenção (horas)	Janelas de manutenção simultâneas necessárias
100	1	1
200	1	1
300	2	1
600	3	2
800	4	3
1200	6	4
1500	8	5

> **Important**
>
> Esses exemplos pressupõem que nenhuma outra janela de manutenção do Systems Manager esteja ativa e que nenhuma outra automação esteja em execução.

Para obter mais informações sobre limites, consulte AWS Systems Manager endpoints e cotas.

Tópicos

- Crie uma janela de manutenção recorrente “Patch Tuesday” a partir do console AMS (recomendado)

- Crie uma janela de manutenção de patches usando o CloudFormation AMS Accelerate
- Crie uma janela de manutenção no console do Systems Manager para o AMS Accelerate
- Crie uma janela de manutenção com a interface de linha de comando (CLI) do Systems Manager para o AMS Accelerate

Crie uma janela de manutenção recorrente “Patch Tuesday” a partir do console AMS (recomendado)

A Microsoft lança patches para seus sistemas operacionais na segunda terça-feira de cada mês, também conhecida como Patch Tuesday. É comum programar patches para instâncias do Windows e do Linux em relação ao Patch Tuesday. Para agendar janelas recorrentes de manutenção de patches no primeiro ou no segundo fim de semana após o Patch Tuesday, visite o console AMS e siga estas etapas:

1. Forneça um nome para sua janela de manutenção de patches.
2. [opcional] Forneça uma descrição para a janela de manutenção do patch.
3. Selecione um dia relativo ao Patch Tuesday.
4. Insira um horário para o início da janela de manutenção do patch em hh:mm. Por exemplo, meia-noite é 00:00 e 23:00 são 23:00. Em seguida, selecione um fuso horário.
5. [opcional] Altere a duração para atender às suas necessidades. O AMS recomenda uma duração mínima de quatro horas.
6. Insira a chave e o valor da etiqueta de patch para o destino. Para obter informações, consulte O que são tags? .
7. [opcional] Expanda os parâmetros opcionais para ajustar a simultaneidade, a taxa de erro e o limite da janela de manutenção.

    1. A simultaneidade controla quantas instâncias de destino estão sendo corrigidas ao mesmo tempo. Por exemplo, uma simultaneidade de 50% para 10 instâncias de destino não corrigirá mais do que 5 instâncias por vez, enquanto 100% de simultaneidade corrigirá todas as 10 de uma só vez.
    2. A taxa de erro controla a tolerância a erros antes que o patch seja suspenso. Por exemplo, uma taxa de erro de 100% para 10 instâncias de destino corrigirá todas as instâncias, independentemente de quantas falharem, enquanto uma taxa de erro de 50% suspenderá a correção quando 5 instâncias falharem na correção. O AMS recomenda uma taxa de erro de 100%.

3. O corte da janela de manutenção de patches evita a violação da janela de manutenção de patches ao suspender o início de novas atividades de patch nas horas especificadas antes do final da janela de manutenção de patches. Por exemplo, um limite de 1 hora (recomendado) interrompe as novas atividades do patch 1 hora antes do final da janela de manutenção do patch.

> **Important**
>
> Verifique a próxima hora de execução.
> Visite o console do SSM Maintenance Window, pesquise sua janela de manutenção de patches recém-criada e verifique a próxima hora de execução. Se você tiver alguma dúvida ou precisar editar sua janela de manutenção de patches, crie uma solicitação de serviço para falar com um especialista em patches do AMS

Para agendar uma janela de manutenção de patches baseada em Cron usando CloudFormation, consulte. Crie uma janela de manutenção de patches usando o CloudFormation AMS Accelerate

Crie uma janela de manutenção de patches usando o CloudFormation AMS Accelerate

Para criar uma janela de manutenção de patches do AMS Accelerate usando AWS CloudFormation, primeiro faça login em sua conta do Accelerate e selecione Região da AWS onde residem suas instâncias de destino. Em seguida, siga estas etapas no https://console.aws.amazon.com/cloudformation:

1. Selecione um dos dois CloudFormation modelos personalizados de patches do Accelerate.

   - Programação do Patch Tuesday: A Microsoft lança patches para seus sistemas operacionais na segunda terça-feira de cada mês, também conhecida como Patch Tuesday, para agendar janelas de manutenção de patches no primeiro ou segundo fim de semana após o Patch Tuesday: Depois de fazer login no console do Accelerate, use este modelo de link. PatchTuesdayScheduling CloudFormation
   - Programação do CRON: Para criar janelas de manutenção de patches usando o CRON para definir o dia de início, use este modelo de link. CRONScheduling CloudFormation Lembre-se de que os números CRON do Systems Manager são de 1 a 7 (para obter detalhes sobre o

SYSTEMS Manager CRON, consulte Referência: Cron e expressões de taxa para o Systems Manager).

A escolha de um desses links faz com que o modelo seja carregado automaticamente no CloudFormation console. Em seguida, clique em Próximo.

2. Na página Especificar detalhes da pilha (etapa 2 das páginas Criar pilha), insira o nome da pilha e os parâmetros do modelo (os parâmetros padrão mostrados são os padrões recomendados pelo AMS, selecione dia e horário para seu caso de uso). Quando terminar, clique em Next (Próximo).
3. Configurar opções de pilha (opcional). Para obter informações sobre as opções, consulte Como configurar as opções de CloudFormation pilha da AWS. Quando terminar, clique em Next (Próximo).
4. Revise os valores da pilha (opcional). Para obter informações sobre como revisar os detalhes da pilha para estimar os custos, consulte Como revisar sua pilha e estimar o custo da pilha. Quando estiver pronto, clique em Criar pilha.

   A pilha pode levar até um minuto para ser criada. Depois que a pilha é criada com sucesso, sua janela de manutenção de patches é executada no horário especificado. Você pode fazer alterações na janela de manutenção de patches criando e executando um conjunto de CloudFormation alterações (recomendado) (para obter detalhes sobre como fazer isso, consulte Criação de pilhas usando conjuntos de alterações) ou atualizando a janela de manutenção de patches no console da janela de manutenção do Systems Manager (). https://console.aws.amazon.com/systems-manager/maintenance-windows

Assista ao vídeo de Namrata para saber mais (5:41)

Crie uma janela de manutenção no console do Systems Manager para o AMS Accelerate

Para criar uma janela de manutenção do AMS Accelerate a partir do console do Systems Manager, siga estas etapas:

1. Na barra de navegação esquerda na área Gerenciamento de alterações, clique em Janelas de manutenção e, em seguida, clique em Criar janela de manutenção no canto superior direito da tela. Preencha o formulário. Para obter detalhes sobre qualquer uma das opções, consulte Criar uma janela de manutenção (console). Ao terminar, clique em Criar janela de manutenção.

A página da lista de janelas de manutenção é aberta.

2. Selecione a janela de manutenção recém-criada.

   A página de detalhes da janela de manutenção é aberta.

3. Vá até a guia Metas e escolha Registrar alvo.

   A página Registrar destino é aberta.

4. Adicione sua meta de aceleração. Para obter informações sobre alvos, consulte Atribuir alvos a uma janela de manutenção (console). Ao terminar, clique em Registrar alvo. Anote o alvo conforme necessário mais tarde.

   A página de detalhes das janelas de manutenção é reaberta na guia Alvos com uma lista que inclui o novo alvo.

5. Na guia Tarefas da página de detalhes da janela de manutenção, escolha Registrar tarefa e, em seguida, escolha Registrar tarefa de automação na lista suspensa. Preencha o formulário. Acelere as notas:

   - Forneça um nome significativo para a tarefa. Por exemplo: AcceleratePatch.
   - Na área Documento de automação, clique na caixa de pesquisa, escolha Proprietário e, em seguida, Documentos compartilhados.
   - Selecione o documento de automação clicando na caixa de pesquisa e escolhendo Prefixo do nome do documento --> Igual a e digitando:. AWSManagedServices-PatchInstance Em seguida, selecione o AWSManagedServices-PatchInstancedocumento selecionando seu botão de rádio.
   - Em Versão do documento, escolha Versão padrão em tempo de execução.
   - Na seção Metas:
     - Defina o alvo por: para Selecionar grupos-alvo registrados.
     - Na lista de alvos, selecione o alvo que você registrou na guia Alvos.
   - Na seção Parâmetros de entrada, preencha o formulário.
     - InstanceId: `{{TARGET_ID}}`
     - StartInactiveInstances: `True` para iniciar as instâncias se elas forem interrompidas durante a janela de manutenção do patch.

> **Note**
>
> O valor do InstanceIdparâmetro diferencia maiúsculas de minúsculas e o valor do StartInactiveInstancesparâmetro pode ser verdadeiro ou falso.
> As instâncias interrompidas não podem ser iniciadas quando segmentadas por tags.
> Para obter mais informações, consulte Nenhuma invocação a ser executada.

- Na seção Controle de taxas, escolha porcentagens. O AMS Accelerate recomenda 100% para simultaneidade e 100% para limite de erro para tentar corrigir todas as instâncias simultaneamente, independentemente dos erros de automação. Se você quiser corrigir metade de suas metas por vez, por exemplo, para manter metade das instâncias de destino atrás de um balanceamento de carga em execução, defina Concorrência como 50%.
- Na seção Função de serviço do IAM, escolha Usar uma função de serviço personalizada e, em seguida, escolha ams_ssm_automation_role.

Clique em Registrar tarefa de automação.

A janela de manutenção de patches é criada. Na guia Descrição, você pode ver o próximo horário de execução.

Crie uma janela de manutenção com a interface de linha de comando (CLI) do Systems Manager para o AMS Accelerate

Para criar uma janela de manutenção do AMS Accelerate com a interface da linha de comando:

1. Siga o tutorial do SSM: Crie e configure uma janela de manutenção (AWS CLI). Para cada etapa do tutorial, aqui estão exemplos de comandos da CLI para aplicação de patches.

> **Note**
>
> Esses exemplos são específicos para Linux ou macOS. Os comandos também podem ser executados AWS CloudShell , o que pode ser mais simples do que configurar `awscli` em uma máquina local. Para obter detalhes, consulte Trabalhando com AWS CloudShell.

   a. Na etapa 1 do tutorial, para criar uma janela de manutenção:

```
aws ssm create-maintenance-window \
                --name Sample-Maintenance-Window \
                --schedule "cron(0 30 23 ? * TUE#2 *)" \
                --duration 4 \
                --cutoff 1 \
                --allow-unassociated-targets \
                --tags "Key=Environment,Value=Production"
```

Em caso de conclusão bem-sucedida, `window-id` é retornado.

b. Na etapa 2 do tutorial, para registrar um nó de destino:

```
aws ssm register-target-with-maintenance-window \
                --window-id "mw-xxxxxxxxx" \
                --resource-type "INSTANCE" \
                --target "Key=tag:Environment,Values=Prod"
```

Em caso de conclusão bem-sucedida, `WindowTargetID` s são devolvidos.

c. Na etapa 3 do tutorial, para registrar uma tarefa:

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-xxxxxx" \
    --targets "Key=WindowTargetIds,Values=63d4f63c-xxxxxx-9b1d-xxxxxfff" \
    --task-arn "AWSManagedServices-PatchInstance" \
    --service-role-arn "arn:aws:iam::AWS-Account-ID:role/ams_ssm_automation_role"
 \
    --task-invocation-parameters "{\"Automation\":{\"DocumentVersion\":\"\$DEFAULT
\",\"Parameters\":{\"InstanceId\":[\"{{TARGET_ID}}\"],\"StartInactiveInstances\":
[\"True\"]}}}" \
    --max-concurrency 50 \
    --max-errors 50 \
    --name "AutomationExample" \
    --description "Sample Description" \
    --task-type=AUTOMATION
```

Patch com ganchos

Você pode configurar o patch do AMS para executar comandos no nível do sistema operacional (OS) antes e depois do patch, usando os patch hooks do AMS. Use os patch hooks do AMS para executar

documentos de comando SSM para interromper um serviço antes da aplicação e, em seguida, iniciar o serviço após a correção, ou para executar comandos para confirmar se seu aplicativo está íntegro após a correção.

Para usar os patch hooks do AMS, você precisa fazer o seguinte:

1. Crie documentos de comando SSM para usar como patch hooks.
2. Crie uma janela de manutenção de patches do AMS ou use uma janela de manutenção de patches do AMS existente. Para obter detalhes, consulte a janela de manutenção de patches do AMS.
3. Configure uma janela de manutenção de patches do AMS para usar seus documentos do Comando SSM para ganchos de patch do AMS.

Patch hooks AMS RACI

A matriz responsável, responsável, consultada e informada, ou RACI, atribui a responsabilidade primária ao cliente ou à AMS por uma variedade de atividades. A tabela a seguir fornece uma visão geral das responsabilidades do cliente e do AMS pelas atividades em um aplicativo que usa patch hooks do AMS.

- R significa a parte responsável que faz o trabalho para realizar a tarefa
- A significa a parte responsável
- C significa consultado; a parte cujas opiniões são solicitadas, normalmente como especialistas no assunto; e com quem há comunicação bilateral
- I significa informado; a parte que é informada sobre o progresso, muitas vezes somente após a conclusão da tarefa ou entrega

Atividades	Cliente	AMS
Crie o documento do comando SSM do pre/post patch e o conteúdo do documento	R	C
Configurar parâmetros de patch hook para aplicação de patches do AMS	R	C

Atividades	Cliente	AMS
Execute o documento de comando SSM do pre/post patch	eu	R
Faça a triagem e responda às falhas do patch hook	eu	R
Notifique o cliente sobre falha no patch hook	eu	R
Reverta para um estado de pré-patch, se solicitado pelo cliente	C	R

Crie documentos SSM para patch hooks

Os patch hooks do AMS usam documentos do Amazon EC2 Systems Manager (SSM) durante a aplicação de patches. Crie um documento de Comando SSM ou compartilhe um documento de Comando SSM existente com a conta em que a correção ocorre. Para obter informações sobre documentos SSM, incluindo limitações, consulte Compartilhamento de documentos SSM.

Para criar um documento de comando SSM, siga estas etapas:

1. Crie um documento SSM com Tipo de documento = “Comando”.
2. Digite seu (s) comando (s) na seção Conteúdo. Para obter mais informações, consulte Criação de conteúdo de documento SSM.

> **Note**
>
> Documentos SSM para patch hooks AMS também podem ser criados com AWS CLI ou. CloudFormation Se precisar de ajuda para criar documentos SSM para seus patch hooks do AMS, entre em contato com seu Cloud Architect.

Configure a janela de manutenção de patches do AMS para usar seus documentos do Comando SSM como ganchos de patch do AMS

Uma janela de manutenção de patches do AMS é uma janela de manutenção do Systems Manager que executa sua automação de patches configurada do AMS.

Para editar uma janela de manutenção de patches do AMS para usar ganchos de patch, siga estas etapas:

1. No https://console.aws.amazon.com/systems-manager/, em Ferramentas de gerenciamento de alterações no painel de navegação esquerdo, selecione Janelas de manutenção.

   Uma página listando as janelas de manutenção existentes é aberta.
2. Selecione um ID de janela que comece com mw-.

   A página de detalhes dessa janela de manutenção é aberta.
3. Selecione a guia Tarefas e a janela ID da tarefa com o ARN da tarefa do AMS- PatchInstance e clique em Editar.
4. Role para baixo até a seção Parâmetros e atualize os parâmetros a seguir.

Parâmetros do patch hook AMS:

- PrePatchHook: o nome do documento SSM com o tipo “Comando” que você deseja executar antes da aplicação do patch. Deixe isso em branco ou digite “AWS-noop” (com distinção entre maiúsculas e minúsculas) se você não estiver executando um comando antes de aplicar o patch.
- PostPatchHook: o nome do documento SSM com o tipo “Comando” que você deseja executar após a correção. Deixe isso em branco ou digite “AWS-noop” (com distinção entre maiúsculas e minúsculas) se você não estiver executando um comando após a correção.
- ExecutePatchBasedOnPreHookStatus: execute a aplicação de patches com base no sucesso ou na falha da PrePatchHook execução, escolha uma:
  - OnPreHookSuccess: execute a automação de patches do AMS somente quando PrePatchHook for bem-sucedida.
  - Sempre: Execute a automação de patches do AMS quando PrePatchHook for bem-sucedida e quando falhar.

  - OnPreHookFailure- Execute a automação de patches do AMS somente quando PrePatchHook houver falha.
  - Nunca: Não execute a automação de patches do AMS. Isso pode ser útil ao testar seu PrePatchHook.
- ExecutePostHookBasedOnPatchStatus: Execute o gancho pós-patch com base no sucesso ou na falha da automação de patches do AMS, escolha um:
  - OnPatchSuccess: Execute o somente PostPatchHook quando a automação de patches do AMS for executada com êxito.
  - Sempre: Execute o PostPatchHook quando a automação de patches do AMS for bem-sucedida e quando falhar.
  - OnPatchFailure- Execute o PostPatchHook somente quando a automação de patches do AMS falhar.

> **Note**
>
> Se alguma dessas variáveis não tiver sua caixa de texto, corrija isso rolando até a seção Documento de automação na mesma página, selecionando um documento diferente e, em seguida, selecionando novamente o documento original. Isso atualiza os parâmetros de entrada para que você possa editá-los.

Linha de base do patch AMS Accelerate

Uma linha de base de patch define quais patches são aprovados para instalação nas suas instâncias. Você pode especificar individualmente os patches aprovados ou rejeitados. Pode também criar regras de aprovação automática para especificar que determinados tipos de atualização (por exemplo, atualizações essenciais) devem ser aprovados automaticamente. A lista se rejeitados substitui as regras e a lista de aprovados.

Linha de base do patch padrão

Quando você se integra ao patch do AMS Accelerate, as linhas de base do patch padrão são substituídas pelas linhas de base do patch padrão do AMS Accelerate para os seguintes sistemas operacionais.

- Windows

- Amazon Linux 1
- Amazon Linux 2
- CentOS
- Suse
- Rhel
- Ubuntu

> **Important**
>
> As linhas de base do patch padrão são gerenciadas pelo AMS. Não edite as linhas de base do patch padrão, pois suas alterações podem ser perdidas. Em vez disso, crie uma linha de base de patch personalizada. Consulte Linha de base de patch personalizada com o AMS Accelerate

> **Note**
>
> As linhas de base do patch do AMS Accelerate definidas como product = * significam que todos os patches são aplicados à instância de todas as seguranças e classificações.

Linha de base de patch personalizada com o AMS Accelerate

Para usar uma linha de base de patch personalizada com o AMS Accelerate, primeiro verifique se você tem um grupo de patches e, em seguida, crie a linha de base personalizada.

Para obter mais informações, consulte os seguintes recursos:

- Trabalhando com grupos de patches
- Criação de uma linha de base de patch personalizada (Windows)
- Criação de uma linha de base de patch personalizada (Linux)
- Atualizando ou excluindo uma linha de base de patch personalizada (console)

Criação de uma função do IAM para aplicação de patches sob demanda do AMS Accelerate

Depois que sua conta é integrada ao AMS Accelerate patching, o AMS Accelerate implanta uma política gerenciada, amspatchmanagedpolicy. Essa política contém as permissões necessárias para aplicação de patches sob demanda usando o documento de automação do AMS. `AWSManagedServices-PatchInstance` Para usar esse documento de automação, o administrador da conta cria uma função do IAM para os usuários. Siga estas etapas:

Crie uma função usando o Console de gerenciamento da AWS:

1. Faça login no Console de gerenciamento da AWS e abra o console do IAM.
2. No painel de navegação do console, escolha Funções e, em seguida, Criar função.
3. Escolha o outro tipo de Conta da AWS função.
4. Em ID da conta, insira a ID da AWS conta à qual você deseja conceder acesso aos seus recursos.

   O administrador da conta especificada pode conceder permissão para assumir essa função a qualquer usuário do IAM dessa conta. Para fazer isso, o administrador anexa uma política ao usuário ou grupo que concede permissão para a AssumeRole ação sts:. Essa política deve especificar o Amazon Resource Name (ARN) da função como recurso. Observe o seguinte:

   - Se você estiver concedendo permissões a usuários de uma conta que você não controla e os usuários assumirem essa função programaticamente, escolha Exigir ID externa. O ID externo pode ser qualquer palavra ou número combinado entre você e o administrador da conta de terceiros. Essa opção adiciona automaticamente uma condição à política de confiança que permite que o usuário assuma a função somente se a solicitação incluir o STS:ExternalID correto. Para obter mais informações, consulte Como usar uma ID externa ao conceder acesso aos seus AWS recursos a terceiros.
   - Se você quiser restringir a função aos usuários que fazem login com a autenticação multifator (MFA), escolha Exigir MFA. Isso adiciona uma condição à política de confiança da função que verifica a existência de um login MFA. Um usuário que desejar assumir a função deverá fazer login com uma senha de uso único temporária a partir de um dispositivo MFA configurado. Usuários sem autenticação de MFA não podem assumir a função. Para obter mais informações sobre MFA, consulte Usando a autenticação multifator (MFA) em. AWS
5. Escolha Próximo: Permissões.

O IAM inclui uma lista de políticas na conta. Em Adicionar permissões, insira amspatchmanagedpolicy na caixa de filtro e marque a caixa de seleção dessa política de permissões. Clique em Next.

6. Em Detalhes da função, insira um nome de função PatchRole, como, adicione uma descrição para a função (recomendado) e também adicione tags para ajudá-lo a identificar essa função. Os nomes das funções não diferenciam maiúsculas de minúsculas, mas devem ser exclusivos no Conta da AWS. Ao terminar, clique em Criar função.

> **Note**
>
> Os nomes das funções não podem ser editados depois de serem criados.

Entenda as notificações de patches e as falhas de patches no AMS Accelerate

> **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.

Solicitações de serviço de patches e notificações por e-mail

O AMS cria uma nova solicitação de serviço quatro dias antes da próxima janela de manutenção de patches. Por exemplo, quatro dias antes da execução de uma janela de manutenção de patches chamada App1 PROD, o AMS cria uma solicitação de serviço chamada Janela de manutenção de patches de abril para App1 Prod for Account [id da conta]. Use a solicitação de serviço de patch para se comunicar com o AMS se precisar de ajustes no patch agendado ou para pular um patch futuro. Quando uma solicitação de serviço é criada, um e-mail é enviado para seu endereço de notificação de patch com um link para a solicitação de serviço. Você recebe um e-mail adicional sempre que o AMS atualiza a solicitação de serviço.

> **Note**
>
> O AMS cria uma nova solicitação de serviço, mesmo que a janela de manutenção de patches seja criada menos de quatro dias antes da data programada para execução.
> A janela de manutenção de patches deve estar em um estado “ativado” para receber notificações de solicitação de serviço.

Uma hora antes do início do patch, o AMS notifica você por meio da solicitação do serviço de patch. Após a conclusão do patch, o AMS atualiza a solicitação do serviço de patch com um link para o console do Patch Manager. Use o link para ver a conformidade de patches para as instâncias visadas pela janela de manutenção de patches.

> **Note**
>
> Os links no console do Patch Manager mostram a conformidade atual das instâncias. O Patch Manager mostra uma instância como incompatível se novos patches forem lançados entre o momento em que o AMS conclui a correção e você acessa o link.

Notificações de patches por meio de CloudWatch eventos

O AMS envia CloudWatch eventos três vezes durante o processo de patch, incluindo o seguinte:

- Quatro dias antes da execução da janela de manutenção de patches.
- Uma hora antes da janela de manutenção de patches ser executada.
- Quando a janela de manutenção do patch for concluída.

A seguir está o esquema de eventos de aviso avançado da Janela de Manutenção de Patch:

```
{
    "version": "0",
    "id": "37004d81-458d-2cef-fe1c-8afa8af30406",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "145917996532",
    "time": "2021-05-20T02:00:00Z",
    "region": "us-east-1",
```

```
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {
        "State": "PREEMPTIVE",
        "StartTime": "2021-05-24T02:00:00.000000",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\"}, {\"instanceId\":
 \"i-0000000aaaaaaaaab\"}]"
    }
}
```

A tabela a seguir descreve o esquema de eventos de aviso prévio da Janela de Manutenção de Patch:

Detalhes da notificação de patch

Nome da propriedade	Descrição	Valores de amostra
Estado	O estado da janela de manutenção de patches	PREEMPTIVO - A janela de patches programada para começar em breve
Status	O status da janela de manutenção de patches	SUCESSO - Todas as instâncias foram corrigidas sem falhas FALHA — Pelo menos uma instância falhou na correção
StartTime	A hora de início, no formato ISO, da janela de manutenção de patches	2021-02-03T 22:14:05.814 308
WindowArn	O identificador exclusivo da janela de manutenção de patches	arn: aws: ssm: us-east-1 :123456789012: janela de manutenção/mw-0000 0001235

Nome da propriedade	Descrição	Valores de amostra
Resultados	A lista de instâncias que são alvo da janela de patch	InstanceId — o ID da instância de destino

A seguir está o esquema do evento final da Janela de Manutenção de Patch:

```
{"version": "0",
    "id": "0f25add5-44a9-0702-d2bc-bd2102affefe",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "123456789012",
    "time": "2021-02-03T22:14:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {"State": "[COMPLETED]",
        "Status": "SUCCESS",
        "StartTime": "2021-02-03T22:12:00.814308",
        "EndTime": "2021-02-03T22:14:05.814309",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "WindowExecutionId": "e32088eb-c05f-4c63-b766-6866e163c818",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\", \"status\":
 \"Success\", \"missing_critical_patch_count\": 0, \"missing_total_patch_count
\": 0} }, {\"instanceId\": \"i-0000000aaaaaaaaab\", \"status\": Success},
 \"missing_critical_patch_count\": 0, \"missing_total_patch_count\": 0}]"
    }
}
```

A tabela a seguir descreve o esquema do evento final da Janela de Manutenção de Patch:

Detalhes do final da janela de patch

Nome da propriedade	Descrição	Valores de amostra
Estado	O estado da janela de manutenção de patches	CONCLUÍDA — A janela de correção está concluída

Nome da propriedade	Descrição	Valores de amostra
Status	O status da janela de manutenção de patches	SUCESSO — Todas as instâncias foram corrigidas sem falhas FALHA — Pelo menos uma instância falhou na correção
StartTime	A hora de início, no formato ISO, da janela de manutenção de patches	2021-02-03T 22:14:05.814 308
EndTime	A hora de término, no formato ISO, da janela de manutenção de patches	2021-02-03T 23:14:05.814 308
WindowArn	O identificador exclusivo da janela de manutenção de patches.	arn: aws: ssm: us-east-1 :123456789012: janela de manutenção/mw-0000 0001235
WindowExecutionId	O ID de execução da janela, que pode ser visto no console da janela de manutenção do SSM	e32088eb-c05f-4c63- b766-6866e163c818

Nome da propriedade	Descrição	Valores de amostra
Resultados	A lista de instâncias que serão alvo da janela de patch	InstanceId — o ID da instância segmentada status — o status do patch da instância missing_critical_patch_count - a contagem de patches críticos ausentes na instância missing_total_patch_count - a contagem do total de patches ausentes na instância

Você pode usar o evento CloudWatch Events para acionar uma CloudWatch regra que o notifica quando um aviso prévio da Janela de Manutenção de Patches é enviado. Para fazer isso, configure a CloudWatch regra com a seguinte configuração:

```
{
    "source": [
        "aws.managedservices"
    ],
    "detail-type": [
        "AMS Patch Window Execution State Change"
    ],
    "detail": {
        "State": ["PREEMPTIVE"]
    }
}
```

> **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.

Investigação de falha de patch no AMS

O AWS Managed Services (AMS) gerencia a aplicação de patches e inclui a correção de falhas de patches. Quando a correção falha, as operações do AMS são alertadas e tentam remediar seguindo as AWS melhores práticas do AMS para resolver o problema.

<instance-id>Se um patch falhar, o AMS cria um SSM OpsItem na conta com o seguinte título: AWS Managed Services — Falha na instância de patch, por exemplo.

O AMS então investiga o. OpsItem Se o AMS puder corrigir a falha sem sua intervenção, o AMS resolverá o. OpsItem Se sua intervenção for necessária, o AMS o notificará por meio de uma solicitação de serviço que contém os resultados da investigação e as etapas de remediação recomendadas. Se você não tomar medidas para resolver o problema, o AMS tentará corrigir a instância durante a próxima janela de manutenção de patches programada.

> **Note**
>
> OpsItems As falhas de patch não são criadas para instâncias que têm sistemas operacionais incompatíveis ou que estão no estado Parado durante a janela de manutenção de patches.

Otimização de custos com o AMS Resource Scheduler

A AWS solução AMS Resource Scheduler on ajuda você a reduzir seus custos AWS e os do AMS interrompendo recursos que não estão em uso e iniciando recursos quando a capacidade é necessária. Por exemplo, você pode usar o AMS Resource Scheduler AWS em um ambiente de desenvolvimento para interromper automaticamente as instâncias fora do horário comercial todos os dias. Se você deixar todas as suas instâncias funcionando em plena utilização, essa solução pode resultar na redução da utilização da instância, o que reduz o custo geral com base nos cronogramas que você configura.

Use o AWS Managed Services (AMS) Resource Scheduler para programar o início e a parada automáticos de grupos de Auto Scaling, instâncias da EC2 Amazon e instâncias do Amazon 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 AWS Instance Scheduler, mas contém recursos adicionais e personalizações específicas para as necessidades dos clientes do AMS. A personalização inclui suporte para programar grupos de Auto Scaling CloudWatch , supressor de alarmes para alarmes do Elastic Load Balancing, suporte para AWS Systems Manager várias janelas de manutenção para a EC2 Amazon, um estimador de economia de custos e suporte operacional do AMS.

O Agendador de Recursos do AMS usa períodos e horários. Os períodos definem os horários em que o recurso deve ser executado, como horário de início, horário de término e dias do mês. As programações contêm seus períodos definidos, juntamente com configurações adicionais — janela de manutenção do SSM, fuso horário, hibernação etc. — e especificam quando os recursos devem ser executados. Você pode configurar esses períodos e cronogramas usando os runbooks de automação fornecidos pela AMS AWS Systems Manager . Cada agendamento deve conter pelo menos um período que defina o (s) horário (s) em que a instância deve ser executada. Um cronograma pode conter mais de um período. Quando mais de um período é usado em um cronograma, o Agendador de Instâncias aplica a ação inicial apropriada quando pelo menos uma das regras do período é verdadeira. Para obter mais detalhes sobre cronogramas e períodos, consulte Componentes de soluções do AWS Instance Scheduler.

O Agendador de AWS Recursos do AMS usa tags de recursos para associar uma agenda a um ou mais recursos a fim de direcioná-los para ações programadas de início e término. Você marca seus recursos com a chave de tag (o padrão é`Schedule`) configurada no Agendador com o nome do agendamento como valor. Você configura a mesma chave de tag da etiqueta de alocação de

custos no AWS Cost Explorer recurso de estimativa de custos do Scheduler para rastrear e relatar a economia de custos.

O AMS Resource Scheduler é um recurso opcional que você pode ativar por conta.

Usando recursos com o AMS Resource Scheduler

Amazon EC2

- EC2 As instâncias da Amazon que fazem parte de um grupo de Auto Scaling não são processadas individualmente e ignoradas pelo AMS Resource Scheduler, mesmo que estejam marcadas.
- Se o volume raiz da instância de destino for criptografado com uma chave mestra AWS KMS do cliente (CMK), 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 precisar dessa permissão, você pode adicionar a permissão atualizando a CloudFormation pilha,`ams-resource-scheduler`, com uma lista de CMK como valor para o `UseCMK` parâmetro (use uma ou mais chaves CMK no formato ARNs em `arn:`*`partition`*`:kms:`*`region`*`:`*`account-id`*`:key/`*`key-id`* vez de um alias KMS).
- Se suas EC2 instâncias da Amazon estiverem configuradas com software específico ou licenças de fornecedores gerenciadas pelo AWS License Manager, o Resource Scheduler precisará de permissões para as AWS License Manager licenças específicas para poder iniciar a instância. Você pode conceder ao Resource Scheduler as permissões necessárias adicionando a lista de ARN (s) das AWS License Manager licenças à licença do gerenciador de licenças, EC2 por exemplo, parâmetro CloudFormation da pilha (). `ams-resource-scheduler`

Amazon EC2 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).
- Marque o grupo Auto Scaling com a tag especificada e não 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.

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 AWS 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.

> **Note**
>
> O Agendador de Recursos não valida se um recurso foi iniciado ou interrompido. Ele faz com que a API chame o serviço relevante e segue em frente. Se a chamada da API falhar, ela registrará o erro para investigação.
>
> O AMS Resource Scheduler não oferece suporte à AWS Backup janela. Se você mapear uma instância do RDS AWS Backup habilitada com o agendamento do Resource Scheduler, para que o backup funcione conforme o esperado, a janela de backup deve estar dentro da janela de execução do agendamento.

Integração do AMS Resource Scheduler

Sua conta não é automaticamente integrada ao AMS Resource Scheduler quando sua conta é integrada ao plano de operações do AMS Accelerate. No entanto, como parte da integração da conta no plano operacional do AMS Accelerate, ou a qualquer momento posterior, você pode solicitar que seu Cloud Service Delivery Manager (CSDM) integre a conta ao AMS Resource Scheduler. Depois que seu CSDM integra a conta, uma CloudFormation pilha contendo recursos do AMS Resource Scheduler com configuração padrão é automaticamente provisionada em sua conta.

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 recomendadasPersonalizando o Agendador de Recursos do AMS, consulte a seguir.

Personalizando o Agendador de Recursos do AMS

Quando integrado, o AMS Resource Scheduler é implantado como uma CloudFormation pilha, com nome, `ams-resource-scheduler` na região principal da AWS para sua conta do AMS Accelerate. Você pode configurar as propriedades do AMS Resource Scheduler com base em suas preferências por meio de parâmetros de CloudFormation pilha e executando uma atualização de pilha. Para obter informações sobre como atualizar CloudFormation pilhas, consulte Como atualizar pilhas diretamente.

Recomendamos que você personalize as propriedades a seguir e deixe o restante como padrão para otimizar a funcionalidade.

- Nome da tag: o nome da tag que o Resource Scheduler usará para associar agendamentos de instâncias a recursos. O valor padrão é `Schedule`.
- Serviço (s) a serem agendados: uma lista separada por vírgulas dos serviços 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`.
- CMK para volumes criptografados do EBS: uma lista separada por vírgulas da Chave Gerenciada pelo Cliente (CMK) do Amazon KMS para a ARNs qual o Resource Scheduler pode receber permissões.

- Licença do gerenciador de licenças, por EC2 exemplo: Uma lista separada por vírgulas do AWS License Manager ARNs para esse Resource Scheduler pode receber permissões.

> **Note**
>
> O AMS ocasionalmente lança recursos e correções para manter o AMS Resource Scheduler atualizado em sua conta. Quando isso acontece, qualquer personalização feita na pilha do Agendador de Recursos do AMS por meio dos parâmetros da pilha é preservada.
> É altamente recomendável não fazer qualquer personalização diretamente em qualquer recurso componente do AMS Resource Scheduler. Isso afeta a funcionalidade do Resource Scheduler e a capacidade do AMS de mantê-lo atualizado.

Usando o Agendador de Recursos do AMS

Como usar os períodos do AMS Resource Scheduler nas contas do AMS Accelerate.

Use o seguinte conjunto de runbooks de AWS Systems Manager automação para administrar o cronograma e o período necessários no AMS Resource Scheduler.

> **Note**
>
> Esses runbooks de automação de SSM estão disponíveis na região principal da AWS da sua conta.

- `AWSManagedServices-AddOrUpdatePeriod`
- `AWSManagedServices-AddOrUpdateSchedule`
- `AWSManagedServices-DeleteScheduleOrPeriod`
- `AWSManagedServices-DescribeScheduleOrPeriods`
- `AWSManagedServices-EnableOrDisableAMSResourceScheduler`

Além disso, o AMS AWS Identity and Access Management fornece uma função`ams_resource_scheduler_ssm_automation_role`,, que AWS Systems Manager exige e assume para usar os runbooks. O escopo da função do IAM é definido com uma política embutida

de privilégios mínimos que concede as permissões de SSM necessárias para a funcionalidade dos runbooks.

Pré-requisitos

Execute as etapas a seguir antes de começar a usar o runbook de automação do SSM e o Agendador de Recursos do AMS.

Anexe a política a seguir à entidade do IAM apropriada (usuário, grupo ou função) que você deseja permitir que use os runbooks de automação para administrar o cronograma e o período no AMS Resource Scheduler. A política não é necessária se sua entidade do IAM tiver administrador ou PowerUser permissão em sua conta.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPassingResourceSchedulerRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/
ams_resource_scheduler_ssm_automation_role",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "ListAndDescribeAutomationExecutions",
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:DescribeAutomationStepExecutions"
            ],
            "Resource": "arn:aws:ssm:*:111122223333:automation-execution/*"
        },
        {
            "Sid": "ListAndDescribeResourceSchedulerSSMDocuments",
            "Effect": "Allow",
```

```
            "Action": [
                "ssm:ListDocumentVersions",
                "ssm:DescribeDocument",
                "ssm:ListDocumentMetadataHistory",
                "ssm:DescribeDocumentParameters",
                "ssm:GetDocument",
                "ssm:DescribeDocumentPermission"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdatePeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdateSchedule",
                "arn:aws:ssm:*::document/AWSManagedServices-
DeleteScheduleOrPeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-
DescribeScheduleOrPeriods",
                "arn:aws:ssm:*::document/AWSManagedServices-
EnableOrDisableAMSResourceScheduler"
            ]
        },
        {
            "Sid": "AllowExecutionOfResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdatePeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdateSchedule:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DeleteScheduleOrPeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DescribeScheduleOrPeriods:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
EnableOrDisableAMSResourceScheduler:*"
            ]
        },
        {
            "Sid": "AllowListingAllDocuments",
            "Effect": "Allow",
            "Action": "ssm:ListDocuments",
            "Resource": "*"
        },
```

```
        {
            "Sid": "AllowListingAllSSMExecutions",
            "Effect": "Allow",
            "Action": "ssm:DescribeAutomationExecutions",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingIAMRolesForStartingExecutionViaConsole",
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        }
    ]
}
```

Você pode executar a automação a partir do AWS Systems Manager console ou usando a AWS CLI. Se estiver usando a AWS CLI, talvez seja necessário instalá-la e configurá-la ou as AWS ferramentas para ela PowerShell, caso ainda não tenha feito isso. Para obter informações, consulte Instalar ou atualizar ferramentas de linha de AWS comando.

Assista ao vídeo da Navish para saber mais (4:52)

Trabalhando com períodos e cronogramas no AWS Managed Services Resource Scheduler

Você pode usar o Agendador de Recursos do AMS para adicionar, atualizar ou excluir agendas ou períodos nas contas do AMS Accelerate.

Adicionar ou atualizar períodos no AMS Resource Scheduler

Adicione ou atualize um período do Resource Scheduler em suas contas do AMS.

Dados que você precisará:

- Ação: O tipo de operação a ser executada. Use “adicionar” se quiser adicionar um período ou “atualizar” se quiser atualizar um período existente.
- Nome: O nome do período. Você deve especificar um valor exclusivo se estiver adicionando um novo período.

- AutomationAssumeRole: o ARN da função AWS Identity and Access Management (IAM) que permite ao runbook adicionar ou atualizar o período em seu nome. Especifique a função como`ams_resource_scheduler_ssm_automation_role`.
- Descrição (opcional): uma descrição significativa para o período.
- BeginTime(Opcional): A hora no formato HH:MM em que você deseja iniciar os recursos.
- EndTime(Opcional): A hora no formato HH:MM em que você deseja interromper os recursos.
- Meses (opcional): uma lista de meses delimitada por vírgula ou um intervalo de meses hifenizado durante o qual os recursos devem ser executados.
- MonthDays(Opcional): uma lista delimitada por vírgulas dos dias do mês ou um intervalo de dias hifenizado durante o qual os recursos devem ser executados.
- WeekDays(Opcional): uma lista delimitada por vírgula dos dias da semana ou de um intervalo de dias da semana durante os quais os recursos devem ser executados.

Como fazer isso:

- Veja o documento em AWSManagedServices-AddOrUpdatePeriod(talvez seja necessário escolher sua região integrada).

  Especifique os requisitos na seção Parâmetros de entrada e escolha Executar. Depois que a operação for concluída, visualize os resultados na guia Saída.

- AWS CLI:

  Execute o comando a seguir para iniciar uma automação. *placeholders*Substitua por suas próprias informações.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdatePeriod" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"],
    "Description":["DESCRIPTION"],"BeginTime":["TIME"], "EndTime":["TIME"],
    "Months":["MONTH"],"MonthDays":["DAY"], "WeekDays":["DAY"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

Exemplo:

O exemplo a seguir mostra como você pode adicionar um novo período usando o AWS Systems Manager console. Nomeamos o período Period-Name e o configuramos para cobrir das 9h às 18h, de segunda a sexta-feira, nos primeiros 15 dias de cada mês.

1. Veja o documento de AWS Systems Manager automação em AWSManagedServices-AddOrUpdatePeriod(talvez seja necessário escolher sua região integrada).

2. Forneça valores para os parâmetros.

3. Clique em Executar e aguarde a conclusão da automação.

Adicionar ou atualizar agendas no AMS Resource Scheduler

Adicione ou atualize uma agenda do Resource Scheduler nas contas do AMS Accelerate.

Dados que você precisará:

- Ação: O tipo de operação a ser executada. Use “adicionar” se quiser adicionar uma agenda ou “atualizar” se quiser atualizar uma agenda existente.
- Nome: O nome da agenda. Você deve especificar um valor exclusivo se estiver adicionando uma nova agenda.
- AutomationAssumeRole: o ARN da função AWS Identity and Access Management (IAM) que permite que o runbook adicione ou atualize a programação em seu nome. Especifique a função`ams_resource_scheduler_ssm_automation_role`.
- Descrição (opcional): uma descrição significativa para o cronograma.
- Programações (opcional): especifique uma lista delimitada por vírgulas dos períodos que devem ser usados com essa programação. Cada período já deve ter sido criado.
- RetainRunning(Opcional): especifique “verdadeiro” para evitar que o Agendador de Recursos interrompa um recurso em execução no final de um período de execução se o recurso tiver sido iniciado manualmente antes do início do período de execução. Por padrão, o Agendador de Recursos interrompe o recurso.
- StopNewInstances(Opcional): especifique “false” para evitar que o Agendador de Recursos interrompa um recurso na primeira vez em que ele for marcado, caso esteja sendo executado fora do período de execução. Por padrão, o Agendador de Recursos interrompe o recurso.
- SSMMaintenanceJanela (opcional): especifique uma lista delimitada por vírgulas das janelas de manutenção do AWS Systems Manager (SSM) que você deseja adicionar como períodos de

execução do cronograma. Você também deve especificar a propriedade UseMaintenanceWindow "" como “verdadeira”.

- TimeZone(Opcional): especifique o fuso horário que você deseja que o Agendador de Recursos use. Por padrão, o Resource Scheduler usa UTC.
- UseMaintenanceWindow(Opcional): especifique “true” se quiser que o Resource Scheduler considere a janela de manutenção do Amazon Relational Database Service (RDS) do Amazon Relational Database Service (RDS) como um período de execução para um cronograma de instância do Amazon RDS ou adicione janelas de manutenção do AWS Systems Manager (SSM) como um período de execução ao cronograma de uma instância da Amazon. EC2
- UseMetrics(Opcional): especifique “verdadeiro” para ativar CloudWatch as métricas no nível do cronograma e “falso” para desativar CloudWatch as métricas. A especificação dessa propriedade substitui a configuração de CloudWatch métricas definida no nível da pilha.

Como fazer isso:

- Veja o documento em AWSManagedServices-AddOrUpdateSchedule(talvez seja necessário escolher sua região integrada).

  Especifique os requisitos na seção Parâmetros de entrada e escolha Executar. Depois que a operação for concluída, visualize os resultados na guia Saída.

- AWS CLI:

  Execute o comando a seguir para iniciar uma automação. *placeholders*Substitua por suas próprias informações.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdateSchedule" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"], "Description":
["DESCRIPTION"],
    "Hibernate":["true or false"],"Enforced":["true or false"],
    "OverrideStatus":["running or stopped"],"Periods":["PERIOD-A, PERIOD-B"],
    "RetainRunning":["true or false"],"StopNewInstances":["true or false"],
    "SSMMaintenanceWindow":["WINDOW-NAME"],"TimeZone":["TIMEZONE"],
    "UseMaintenanceWindow":["true or false"],"UseMetrics":["true or false"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

Exemplo:

O exemplo a seguir mostra como adicionar uma agenda para o AMS Resource Scheduler. Neste exemplo, você adiciona uma agenda chamada CustomSchedule usando CustomPeriod.

1. Veja o documento de AWS Systems Manager automação em AWSManagedServices-AddOrUpdateSchedule(talvez seja necessário escolher sua região integrada).

2. Forneça valores para os parâmetros.

3. Clique em Executar e aguarde a conclusão da automação.

Excluindo períodos ou agendas no AMS Resource Scheduler

Para excluir períodos ou agendas do Resource Scheduler nas contas do AMS Accelerate, você precisa dos seguintes dados:

- ConfigurationType: o tipo de configuração que você deseja excluir. Use “período” se quiser excluir períodos ou “agenda” se quiser excluir agendamentos.
- Nome: O nome da agenda ou período que você deseja excluir.
- AutomationAssumeRole: o ARN da função AWS Identity and Access Management (IAM) que permite que o runbook exclua agendas ou períodos em seu nome. Especifique a função`ams_resource_scheduler_ssm_automation_role`.

Como fazer isso:

- Veja o documento em AWSManagedServices-DeleteScheduleOrPeriod(talvez seja necessário escolher sua região de embarque).

  Especifique os requisitos na seção Parâmetros de entrada e escolha Executar. Depois que a operação for concluída, visualize os resultados na guia Saída.
- AWS CLI:

  Execute o comando a seguir para iniciar uma automação. *`placeholders`*Substitua por suas próprias informações.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DeleteScheduleOrPeriod" --document-version "\$DEFAULT"
```

```
--parameters '{"ConfigurationType":["period" or "schedule"],"Name":["NAME"],
    "AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}' --region ONBOARDED_REGION
```

Exemplo:

O exemplo a seguir mostra como você pode excluir um período usando o AWS Systems Manager console.

1. Veja o documento de AWS Systems Manager automação em AWSManagedServices-DeleteScheduleOrPeriod(talvez seja necessário escolher sua região integrada).

2. Forneça valores para os parâmetros.

3. Clique em Executar e aguarde a conclusão da automação.

Descrevendo períodos ou programações no AMS Resource Scheduler

Para descrever (ver detalhes sobre) um período ou cronograma do Resource Scheduler nas contas do AMS Accelerate, você precisa dos seguintes dados:

- ConfigurationType: o tipo de configuração que você deseja descrever. Use “períodos” se quiser descrever todos os períodos ou “horários” se quiser descrever todos os horários.
- AutomationAssumeRole: o ARN da função AWS Identity and Access Management (IAM) que permite que o runbook descreva cronogramas ou períodos em seu nome. Especifique a funçãoams_resource_scheduler_ssm_automation_role.

Como fazer isso:

- Veja o documento em AWSManagedServices-DescribeScheduleOrPeriods(talvez você precise escolher sua região integrada):
  1. Especifique os requisitos na seção Parâmetros de entrada e escolha Executar.
  2. Depois que a operação for concluída, visualize os resultados na guia Saída.
- AWS CLI:
  1. Execute o comando a seguir para iniciar uma automação. *placeholders*Substitua por suas próprias informações.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DescribeScheduleOrPeriods" --document-version "\$DEFAULT"
                --parameters '{"ConfigurationType":["period" or
 "schedule"],"AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}'
                --region ONBOARDED_REGION
```

Exemplo:

O exemplo a seguir mostra como você pode descrever um período usando o AWS Systems Manager console.

1. Veja o documento de AWS Systems Manager automação em AWSManagedServices-DescribeScheduleOrPeriods(talvez seja necessário escolher sua região integrada).

2. Forneça valores para os parâmetros.

3. Clique em Executar e aguarde a conclusão da automação.

Recursos de marcação para o AMS Resource Scheduler

Recursos de marcação para o AMS Resource Scheduler.

Depois de adicionar agendas e períodos à Programação de Recursos do AMS, você precisa marcar seus recursos com o nome da tag do Resource Scheduler como chave da tag, ou a chave personalizada, e o nome da agenda como o valor da tag. Para obter detalhes sobre como marcar seus recursos em sua conta do AMS Accelerate, consulteMarcação no AMS Accelerate.

> **Note**
>
> Se o Resource Tagger for usado para marcar os recursos, a chave de tag padrão do Resource Scheduler deverá ser personalizada para ter o prefixo '`ams:rt:`', pois todas as tags aplicadas pelo marcador de recursos têm o prefixo ". `ams:rt:` Caso contrário, os recursos marcados com o marcador de recursos não serão gerenciados pelo Resource Scheduler. Para saber mais sobre como personalizar a chave de tag padrão para o Resource Scheduler, consulte. Personalizando o Agendador de Recursos do AMS

Estimador de custos no AMS Resource Scheduler

Para monitorar a economia de custos, o AMS Resource Scheduler apresenta um componente que calcula de hora em hora a economia de custo estimada para os recursos da Amazon e do EC2 Amazon 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 24x0,125 = $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 de custos definidas pelo usuário

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

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.

> **Note**
>
> 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.

Supressor de alarme no AMS Resource Scheduler

O AMS Resource Scheduler vem com um supressor de CloudWatch alarmes, que é implantado como uma função Lambda separada chamada `AMSAlarmSuppressor` que suprime alarmes para instâncias que estão por trás de um Elastic Load Balancing, Application Load Balancer ou Network Load Balancer. A função é executada a cada 5 minutos, recupera todos os alarmes presentes na conta e os agrupa com base no namespace; por exemplo,,,. `AWS/ELB` `AWS/ApplicationELB` `AWS/NetworkELB` Para cada grupo de alarmes, o supressor encontra o nome do balanceador de carga (grupo and/or alvo) e verifica o estado da instância para ALB/NLB) from alarm dimensions, finds the instances that are registered with the load balancer and/or descobrir se as instâncias estão programadas pelo AMS Resource Scheduler. Se as instâncias forem agendadas pelo Resource Scheduler e interrompidas pelo Resource Scheduler, o supressor marcará os alarmes para desativá-los. Se pelo menos uma instância na lista de instâncias registradas estiver em execução, o supressor marca os alarmes correspondentes para ativar os alarmes marcados para ativação e desabilitar os alarmes marcados para desativação. Os registros para isso são armazenados no grupo de `/aws/lambda/AMSAlarmSuppressor` registros.

Gerenciamento de registros no AMS Accelerate

O AMS Accelerate configura AWS serviços compatíveis para coletar registros. Esses registros são usados pelo AMS Accelerate para garantir a conformidade e a auditoria dos recursos em sua conta.

O AMS Accelerate fornece uma variedade de serviços operacionais para ajudar você a alcançar a excelência operacional na AWS. Para obter uma compreensão rápida de como o AMS ajuda suas equipes a alcançar a excelência operacional geral na Nuvem AWS com alguns de nossos principais recursos operacionais, incluindo suporte técnico 24 horas por dia, 7 dias por semana, monitoramento proativo, segurança, aplicação de patches, registro e backup, consulte Diagramas de arquitetura de referência do AMS.

Tópicos

- Gerenciamento de registros — AWS CloudTrail
- Gerenciamento de registros — Amazon EC2
- Gerenciamento de registros — Amazon VPC Flow Logs

Gerenciamento de registros — AWS CloudTrail

AWS CloudTrailé um serviço usado para governança de contas: conformidade, auditoria operacional e auditoria de risco. Com CloudTrail, você pode registrar, monitorar continuamente e reter as atividades da conta relacionadas às ações em toda a sua AWS infraestrutura.

O AMS AWS CloudTrail Accelerate exige registro para gerenciar auditorias e conformidade de todos os recursos em sua conta. Durante a integração, você pode escolher uma das seguintes opções:

- Trilha implantada pelo AMS: se você escolher essa opção, o AMS cria, implanta e gerencia uma trilha CloudTrail multirregional em sua AWS região principal, independente de qualquer trilha existente em sua conta.
- Traga sua própria trilha: se você optar por fornecer sua própria CloudTrail trilha de conta ou organização, deverá trabalhar com seu Cloud Architect (CA) para garantir que ele atenda às configurações necessárias para o Accelerate. Se você escolher essa opção, mas não fornecer sua própria trilha, o Accelerate implantará automaticamente sua própria CloudTrail trilha para manter a cobertura contínua de segurança e auditoria. Se você fornecer sua própria trilha posteriormente, o AMS removerá a trilha implantada para evitar redundância e custos adicionais. Essa abordagem

ajuda a manter uma única CloudTrail trilha ativa em sua conta e evita custos duplicados de registro.

> **Note**
>
> Se sua conta tiver uma CloudTrail trilha existente e você não tiver configurado ou solicitado especificamente uma trilha gerenciada pelo AMS durante a integração, o AMS Accelerate removerá automaticamente a trilha implantada do AMS da sua conta. Isso evita registros duplicados, otimiza o uso de recursos e economiza custos adicionais.

O AMS Accelerate cria um bucket Amazon S3 para uma CloudTrail trilha implantada do Accelerate como destino de entrega de eventos e usa AWS Key Management Service ()AWS KMS criptografia. Seus eventos de trilha são acessados pelos operadores do AMS Accelerate para fins de investigação e diagnóstico. Se a conta já tiver uma CloudTrail trilha existente ativada, essa trilha é um acréscimo a essa, caso você opte por fazer com que o Accelerate implante uma trilha gerenciada pelo Accelerate durante a integração.

O AMS Accelerate implanta AWS Config regras para garantir que as trilhas de sua CloudTrail conta, incluindo uma CloudTrail trilha implantada pelo Accelerate, sejam configuradas e criptografadas corretamente. Para saber mais, consulte AWS Config. Estas são as regras usadas, apresentadas como links para a AWS documentação que as descreve:

- multi-region-cloudtrail-enabled. Verifica se o AMS Accelerate CloudTrail está configurado corretamente com as configurações corretas.
- cloud-trail-encryption-enabled. Verifica se AWS CloudTrail está configurado para usar a criptografia do lado do servidor (SSE) com criptografia de chave mestra AWS KMS do cliente (CMK).
- cloud-trail-log-file-habilitado para validação. Quando ativado, verifica se AWS CloudTrail cria um arquivo de resumo assinado com registros. É altamente recomendável que você habilite a validação de arquivos em todas as trilhas.
- s-3. bucket-default-lock-enabled Quando ativado, verifica se o bucket do Amazon S3 tem o bloqueio ativado.
- s-3. bucket-logging-enabled Quando ativado, verifica se o registro está habilitado para buckets do Amazon S3.

O AMS Accelerate usa AWS KMS para criptografar os eventos registrados de uma CloudTrail trilha implantada pelo Accelerate em sua conta. Essa chave é controlada e acessível aos administradores da conta, operadores do AMS Accelerate e. CloudTrail Para obter mais informações sobre AWS KMS, consulte a documentação do produto sobre AWS Key Management Service recursos.

Acessando e auditando registros CloudTrail

CloudTrail os registros de uma CloudTrail trilha implantada pelo AMS Accelerate são armazenados em um bucket do Amazon S3 em sua conta. Os dados de trilhas armazenados no bucket do Amazon S3 são criptografados usando uma chave do AWS KMS criada CloudTrail quando os recursos são provisionados.

Os buckets do Amazon S3 utilizam um padrão de nomenclatura de ams-a ***`aws account id`*** - cloudtrail-***`AWS Region`***, (exemplo: ams-a123456789- -1a) e todos os eventos são armazenados com o prefixo AWS/. cloudtrail-us-east CloudTrail Todo o acesso ao bucket primário é registrado e os objetos de log são criptografados e versionados para fins de auditoria.

Para obter mais informações sobre como rastrear alterações e consultar os registros, consulteRastreando alterações em suas contas do AMS Accelerate.

Protegendo e retendo registros CloudTrail

O AMS Accelerate permite o bloqueio de objetos do Amazon S3 com o Modo de Governança para uma CloudTrail trilha implantada pelo Accelerate para garantir que os usuários não possam sobrescrever ou excluir uma versão do objeto ou alterar suas configurações de bloqueio sem permissões especiais. Para obter mais informações, consulte Bloqueio de objetos do Amazon S3.

Por padrão, todos os registros nesse bucket são mantidos indefinidamente. Se quiser alterar o período de retenção, você pode enviar uma solicitação de serviço por meio do AWS Support Centro para configurar uma política de retenção diferente.

Acessando os EC2 registros da Amazon

Você pode acessar os registros de EC2 instâncias da Amazon usando Console de gerenciamento da AWS o. Os registros produzidos por instâncias e AWS serviços estão disponíveis no CloudWatch Logs, que está disponível em cada conta gerenciada pelo AMS Accelerate. Para obter informações sobre como acessar seus registros, consulte a documentação de CloudWatch registros.

Retenção de registros da Amazon EC2

Por padrão EC2 , os registros de instâncias da Amazon são mantidos indefinidamente. Se quiser alterar o período de retenção, você pode enviar uma solicitação de serviço por meio do AWS Support Centro para configurar uma política de retenção diferente.

Gerenciamento de registros — Amazon EC2

O AMS Accelerate instala o CloudWatch agente em todas as EC2 instâncias da Amazon que você identificou como gerenciadas pelo AMS Accelerate. Esse agente envia registros em nível de sistema para o Amazon CloudWatch Logs. Para obter mais informações, consulte O que são Amazon CloudWatch Logs?

Os arquivos de registro a seguir são enviados para o CloudWatch Logs, em um grupo de registros com o mesmo nome do registro. Dentro de cada grupo de log, um stream de log é criado para cada EC2 instância da Amazon, nomeado de acordo com o ID da EC2 instância da Amazon.

Linux

- /var/log/amazon/ssm/amazon-ssm-agent.log
- /var/log/amazon/ssm/errors.log
- /var/log/audit/audit.log
- /var/log/auth.log
- /var/log/cloud-init-output.log
- /var/log/cron
- /var/log/dnf.log
- /var/log/dpkg.log
- /var/log/maillog
- /var/log/messages
- /var/log/secure
- /var/log/spooler
- /var/log/syslog
- /var/log/yum.log
- /var/log/zypper.log

Para obter mais informações, consulte Criar ou editar manualmente o arquivo de configuração do CloudWatch agente.

Windows

- SSMAgentRegistro da Amazon
- AmazonCloudWatchAgentLog
- SSMErrorRegistro da Amazon
- AmazonCloudFormationLog
- ApplicationEventLog
- EC2ConfigServiceEventLog
- MicrosoftWindowsAppLockerEXEAndDLLEventRegistro
- MicrosoftWindowsAppLockerMSIAndScriptEventLog
- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog

Para obter mais informações, consulte Início rápido: habilite suas EC2 instâncias da Amazon executando o Windows Server 2016 para enviar registros para CloudWatch registros usando o agente de CloudWatch registros.

Gerenciamento de registros — Amazon VPC Flow Logs

Os registros de fluxo da VPC são um recurso que captura informações sobre o tráfego IP que entra e sai das interfaces de rede na sua VPC. Os dados do log de fluxo podem ser publicados nos CloudWatch registros da Amazon ou no Amazon S3. A coleta de dados do log de fluxo não afeta a taxa de transferência ou a latência da rede. Você pode criar ou excluir registros de fluxo sem nenhum impacto no desempenho da rede.

Os logs de fluxo podem ajudar em diversas tarefas, como:

- Diagnosticando regras de grupos de segurança excessivamente restritivas
- Monitorando o tráfego que chega à sua instância
- Determinar a direção de entrada e saída do tráfego das interfaces de rede

Você não precisa ativar os registros de fluxo da VPC para cada VPC recém-criada nas contas do Accelerate. O AMS detectará automaticamente se uma VPC tem um registro de fluxo usando a regra - ams-nist-cis-vpcConfig flow-logs-enabled. Se os registros de fluxo da VPC não estiverem habilitados, o AMS os remediará automaticamente criando um registro de fluxo da VPC com campos personalizados. Ter esses campos adicionais permitirá que o AMS e os clientes monitorem melhor o tráfego da VPC, entendam as dependências da rede, solucionem problemas de conectividade de rede e identifiquem ameaças à rede.

Para obter informações sobre como visualizar e pesquisar registros de fluxo, consulte Trabalhar com registros de fluxo.

Rastreando alterações em suas contas do AMS Accelerate

Important

O serviço Change Record foi descontinuado em 1º de julho de 2025.
Novas contas não podem ser integradas ao serviço Change Record.
Para consultar CloudTrail dados em suas contas do AMS Accelerate, você pode usar estes serviços:

- Em AWS CloudTrail, escolha Histórico de eventos e filtre eventos usando atributos de pesquisa. Você pode usar o filtro de intervalo de tempo e optar por filtrar o histórico de eventos por fonte de eventos com a `s3.amazon.aws.com` especificação, ou optar por filtrar o histórico de eventos por nome de usuário. Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.
- Use o AWS CloudTrail Lake para coletar dados por meio de consultas. Em, AWS CloudTrail escolha Lake e, em seguida, escolha Consulta. Você pode criar suas próprias consultas, usar o gerador de consultas ou usar exemplos de consultas para coletar dados baseados em eventos. Por exemplo, você pode perguntar quem excluiu uma EC2 instância da Amazon na semana passada. Para obter mais informações, consulte Criação de um data lake a partir de uma AWS CloudTrail fonte e CloudTrailLake consultas.
- Crie uma tabela do Amazon Athena AWS CloudTrail e defina o local de armazenamento como o bucket do Amazon S3 associado à sua trilha. Verifique se a região inicial da sua trilha e do bucket do Amazon S3 são iguais. No Amazon Athena, use o editor de consultas para executar as consultas padrão que o Accelerate fornece para uso com o console do Athena. Para obter mais informações sobre como criar uma tabela do Athena para dois CloudTrail registros de consulta, consulte Registros de consulta AWS CloudTrail.

Tópicos

- Visualizando seus registros de alterações
- Consultas padrão
- Alterar permissões de registro

O AWS Managed Services ajuda você a monitorar as alterações feitas pela equipe de operações do AMS Accelerate e pela automação do AMS Accelerate, fornecendo uma interface que pode ser

consultada usando o console Amazon Athena (Athena) e o gerenciamento de registros do AMS Accelerate.

O Athena é um serviço de consulta interativo que você pode usar para analisar dados no Amazon S3 usando a linguagem de consulta estruturada (SQL) padrão (consulte a referência de SQL para o Amazon Athena). Como o Athena é sem servidor, não há infraestrutura para gerenciar, e você paga apenas pelas consultas executadas. O AMS Accelerate cria tabelas do Athena com partições diárias em CloudTrail registros e fornece consultas sobre sua AWS região principal e dentro do grupo de trabalho. ams-change-record Você pode escolher qualquer uma das consultas padrão e executá-las conforme necessário. Para saber mais sobre os grupos de trabalho do Athena, consulte Como funcionam os grupos de trabalho.

> **Note**
>
> Somente o Accelerate pode consultar CloudTrail eventos para sua conta do Accelerate usando o Athena quando o Accelerate está integrado à trilha CloudTrail da sua organização, a menos que o administrador da organização tenha implantado uma função do IAM para usar o Athena para consultar e analisar CloudTrail eventos em sua conta durante a integração.

Usando o registro de alterações, você pode responder facilmente a perguntas como:

- Quem (AMS Accelerate Systems ou AMS Accelerate Operators) acessou sua conta
- Quais alterações foram feitas pelo AMS Accelerate em sua conta
- Quando o AMS Accelerate realizou alterações em sua conta?
- Onde ir para ver as alterações feitas em sua conta
- Por que o AMS Accelerate precisou fazer as alterações em sua conta
- Como modificar as consultas para obter respostas a todas essas perguntas também para quaisquer alterações que não sejam do AMS

Visualizando seus registros de alterações

Para usar as consultas do Athena, entre no console de AWS gerenciamento e navegue até o console do Athena na sua região principal. AWS

> **Note**
>
> Se você ver a página de introdução do Amazon Athena enquanto executa qualquer uma das etapas, clique em Começar. Isso pode aparecer para você mesmo que sua infraestrutura de registro de alterações já esteja instalada.

1. Escolha Grupo de trabalho no painel de navegação superior no console do Athena.
2. Escolha o ams-change-recordgrupo de trabalho e clique em Alternar grupo de trabalho.
3. Escolha na caixa ams-change-record-databasede combinação de banco de dados. ams-change-record-databaseIsso inclui a ams-change-record-tabletabela.
4. Escolha Consultas salvas no painel de navegação superior.
5. A janela Consultas salvas mostra uma lista de consultas fornecidas pelo AMS Accelerate, que você pode executar. Escolha a consulta que você deseja executar na lista Consultas salvas. Por exemplo, consulta ams_session_accesses_v1.

   Para obter a lista completa das consultas predefinidas do AMS Accelerate, consulte. Consultas padrão
6. Ajuste o filtro de data e hora na caixa do editor de consultas conforme necessário; por padrão, a consulta só verifica as alterações do último dia.
7. Selecione Executar consulta.

Consultas padrão

O AMS Accelerate fornece várias consultas padrão que você pode usar no console do Athena. As consultas padrão estão listadas nas tabelas a seguir.

> **Note**
>
> - Todas as consultas aceitam o intervalo de data e hora como um filtro opcional; todas as consultas são executadas nas últimas 24 horas, por padrão. Para informações esperadas, consulte a subseção a seguir,Modificando o filtro de data e hora nas consultas.
> - As entradas de parâmetros que você pode ou precisa alterar são mostradas na consulta como *<PARAMETER_NAME>* se fossem chaves angulares. Substitua o espaço reservado e as chaves angulares pelo valor do seu parâmetro.

- Todos os filtros são opcionais. Nas consultas, alguns filtros opcionais são comentados com um traço duplo (--) no início da linha. Todas as consultas serão executadas sem elas, com parâmetros padrão. Se você quiser especificar valores de parâmetros para esses filtros opcionais, remova o traço duplo (--) no início da linha e substitua o parâmetro conforme desejar.
- Todas as consultas retornam `IAM PincipalId` e `IAM SessionId` nas saídas
- O custo calculado para executar uma consulta depende de quantos CloudTrail registros são gerados para a conta. Para calcular o custo, use a calculadora de preços do AWS Athena.

Consultas predefinidas

Finalidade/Descrição	Entradas	Saídas
Nome da consulta: `ams_access_session_query_v1`		
Rastreando as sessões de acesso do AMS Fornece informaçõ es sobre uma sessão de acesso específic a do AMS Accelerate. A consulta aceita o ID principal do IAM como um filtro opcional e retorna a hora do evento, a necessidade comercial de acessar a conta, o solicitante e assim por diante. Você pode filtrar por uma ID principal específica do IAM descomentando a linha e substituindo o espaço *IAM Principal*	(Opcional)`IAM PrincipalId` : o identificador principal do IAM do recurso que está tentando acessar. O formato é*UNIQUE_ID ENTIFIER* :*RESOURCE_ NAME* . Para obter detalhes, consulte identificadores exclusivos. Você pode executar a consulta sem esse filtro para determinar o IAM exato com PrincipalId o qual você deseja filtrar.	• EventTime: Hora de obter o acesso • EventName: Nome do evento da AWS (AssumeRole) • EventRegion: Região da AWS que recebe a solicitação • EventId: ID CloudTrail do evento • BusinessNeed Tipo: Tipo de motivo comercial para acessar a conta. Os valores permitidos são: SupportCase, OpsItem, Problema, Texto. • BusinessNeed: As empresas precisam acessar a conta. Por exemplo, Support Case ID, Ops Item ID e assim por diante. • Solicitante: ID do operador que acessa a conta ou sistema de automação que acessa a conta.

Finalidade/Descrição	Entradas	Saídas
Id reservado por uma ID específica no editor de consultas. Você também pode listar sessões de acesso não AMS removendo a linha de filtro useragent na cláusula WHERE da consulta.		• RequestAccessType: Tipo de solicitante (Sistema, OpsAPI OpsConsole, Não definido)
Nome da consulta: `ams_events_query_v1`		
Acompanhe todas as ações de mutação realizadas pelo AMS Accelerate Retorna todas as ações de gravação realizadas na conta usando esse filtro de função do AMS Accelerate. Você também pode rastrear ações de mutação realizadas por funções que não são do AMS removendo as linhas de filtro useridentity.arn da cláusula WHERE da consulta.	(Opcional) Somente intervalo de data e hora. Consulte Modificando o filtro de data e hora nas consultas .	• AccountId: ID da conta da AWS • RoleArn: RoleArn para o solicitante • EventTime: Hora de obter o acesso • EventName: Nome do evento da AWS (AssumeRole) • EventRegion: Região da AWS que recebe a solicitação • EventId: ID CloudTrail do evento • RequestParameters : Parâmetros de solicitação para a solicitação • ResponseElements: elementos de resposta para a resposta. • UserAgent: Agente de CloudTrail usuário da AWS
Nome da consulta: `ams_instance_access_sessions_query_v1`		

Finalidade/Descrição	Entradas	Saídas
Rastreie os acessos à instância pelo AMS Accelerate Retorna uma lista de acessos à instância do AMS Accelerate; cada registro inclui hora do evento, região do evento, ID da instância , ID principal do IAM, ID da sessão do IAM, ID da sessão do SSM. Você pode usar a ID principal do IAM para obter mais detalhes sobre a necessidade comercial de acessar a instância usando a consulta `ams_access_sessions_query_v1` Athena. Você pode usar o SSM Session ID para obter mais detalhes sobre a sessão de acesso à instância, incluindo o horário de início e término da sessão, detalhes do registro e o uso do console do AWS Session Manager na AWS região da instância. Os usuários também podem listar acessos de	Somente `datetime range`. Consulte Modificando o filtro de data e hora nas consultas .	• InstanceId: ID da instância • SSMSession ID: ID da sessão SSM • RoleArn: RoleArn para o solicitante • EventTime: Hora de obter o acesso • EventName: Nome do evento da AWS (AssumeRole) • EventRegion: Região da AWS que recebe a solicitação • EventId: ID CloudTrail do evento

Finalidade/Descrição	Entradas	Saídas
instâncias que não são do AMS removendo a linha de filtro useridentity na cláusula WHERE da consulta.		
Nome da consulta: ams_privilege_escalation_events_query_v1		

Finalidade/Descrição	Entradas	Saídas
Rastreie eventos de permissão (escalonamento) para usuários do AMS e não AMS Fornece uma lista de eventos que podem levar direta ou potencialmente a um aumento de privilégios. A consulta aceita ActionedBy como um filtro opcional e retorna EventName,, EventId EventTime, e assim por diante. Todos os campos associados ao evento também são retornados. Os campos ficam em branco se não forem aplicáveis a esse evento. O ActionedBy filtro está desativado, por padrão; para ativá-lo, remova “--" dessa linha. Por padrão, o ActionedBy filtro está desativado (ele mostrará eventos de escalonamento de privilégios de todos os usuários). Para mostrar eventos para um determinado usuário ou função, remova o traço duplo (--) da linha	(Opcional)`ACTIONEDBY_PUT_USER_NAME` : Nome de usuário do usuário ActionedBy. Pode ser um usuário ou um perfil do IAM. Por exemplo, ams-access-admin. (Opcional) `datetime range`. Consulte Modificando o filtro de data e hora nas consultas .	• AccountId: ID da conta • ActionedByNome de usuário ActionedBy : • EventTime: Hora de obter o acesso • EventName: Nome do evento da AWS (AssumeRole). • EventRegion: Região da AWS que recebe a solicitação • EventId: ID CloudTrail do evento

Finalidade/Descrição	Entradas	Saídas
de filtro de identidade do usuário na cláusula WHERE e substitua o espaço reservado *ACTIONEDBY_PUT_USER_NAME_HERE* por um nome de usuário ou função do IAM. Você pode executar a consulta sem o filtro para determinar o usuário exato com o qual deseja filtrar.		

Nome da consulta: ams_resource_events_query_v1

Finalidade/Descrição	Entradas	Saídas
Rastreie eventos de gravação para recursos específicos AMS ou não AMS Fornece uma lista de eventos realizados em um recurso específic o. A consulta aceita o ID do recurso como parte dos filtros (substitu a o espaço reservado *RESOURCE_INFO* na cláusula WHERE da consulta) e retorna todas as ações de gravação realizadas nesse recurso.	(Obrigatório)`RESOURCE_INFO` : O identificador do recurso pode ser um ID para qualquer recurso da AWS na conta. Não confunda isso com recurso ARNs. Por exemplo, um ID de instância para uma EC2 instância, nome de tabela para uma tabela do DynamoDB logGroupN ame , para CloudWatch um log etc. (Opcional) `datetime range`. Consulte Modificando o filtro de data e hora nas consultas .	• AccountId: ID da conta • ActionedByNome de usuário ActionedBy : • EventTime: Hora de obter o acesso • EventName: Nome do evento da AWS (AssumeRole). • EventRegion: Região da AWS que recebe a solicitação • EventId: ID CloudTrail do evento
Nome da consulta: `ams_session_events_query_v1`		

Finalidade/Descrição	Entradas	Saídas
Acompanhe as ações de gravação realizadas pelo AMS Accelerate durante uma sessão específica Fornece uma lista de eventos realizados em uma sessão específica. A consulta aceita a ID principal do IAM como parte dos filtros (substitua o espaço reservado *PRINCIPAL_ID* na cláusula WHERE da consulta) e retorna todas as ações de gravação realizadas nesse recurso.	(Obrigatório)`PRINCIPAL_ID` : ID principal da sessão. O formato é*UNIQUE_ID ENTIFIER* :*RESOURCE_NAME* . Para obter detalhes, consulte identificadores exclusivos. Você pode executar a consulta “ams_session_ids_by_requester_v1" para obter uma lista do IAM Principal para um solicitante. IDs Você também pode executar a consulta sem esse filtro para determinar o IAM exato com o qual PrincipalId você deseja filtrar. (Opcional) `datetime range`. Consulte Modificando o filtro de data e hora nas consultas .	• AccountId: ID da conta • ActionedByNome de usuário ActionedBy : • EventTime: Hora de obter o acesso • EventName: Nome do evento da AWS (AssumeRole) • EventRegion: Região da AWS que recebe a solicitação • EventId: ID CloudTrail do evento
Nome da consulta: `ams_session_ids_by_requester_v1`		

Finalidade/Descrição	Entradas	Saídas
Rastreie Principal/ Session IDs o IAM para um solicitante específico. A consulta aceita “solicitante” (substitua o espaço reservado *Requester* na cláusula WHERE da consulta) e retorna todos os IDs principais do IAM desse solicitante durante o intervalo de tempo especificado.	(Obrigatório)`Requester` : ID do operador que acessa a conta (por exemplo: alias de um operador) ou sistema de automação que acessa a conta (por exemplo: OsConfiguration, AlarmManager, etc.). (Opcional) `datetime range`. Consulte Modificando o filtro de data e hora nas consultas .	• IAM PrincipalId - ID principal do IAM da sessão. O formato é*UNIQUE_ID ENTIFIER* :*RESOURCE_NAME* . Para obter detalhes, consulte identificadores exclusivos. Você pode executar a consulta sem esse filtro para determinar o IAM exato com o qual PrincipalId você deseja filtrar. • IAM SessionId - ID da sessão do IAM para a sessão de acesso • EventTime: Hora de obter o acesso

Modificando o filtro de data e hora nas consultas

Todas as consultas aceitam o intervalo de data e hora como um filtro opcional. Por padrão, todas as consultas são executadas no último dia.

O formato usado para o campo de data e hora é yyyy/MM/dd (por exemplo: 2021/01/01). Lembre-se de que ele armazena apenas a data e não o carimbo de data/hora inteiro. Para todo o timestamp, use o campo eventime, que armazena o timestamp no formato ISO 8601 yyyy-MM-dd T HH:mm:ss Z (por exemplo: 2021-01-01T 23:59:59 Z). No entanto, como a tabela é particionada no campo datetime, você precisará passar os filtros datetime e eventtime para a consulta. Veja os exemplos de a seguir.

> **Note**
>
> Para ver todas as formas aceitas de modificar o intervalo, consulte a documentação mais recente da função Presto com base na versão do mecanismo Athena usada atualmente para

as funções e operadores de data e hora para ver todas as formas aceitas de modificar o intervalo.

Nível de data: Último dia ou últimas 24 horas (padrão) Exemplo: se o CURRENT_DATE='2021/01/01', o filtro subtrairá um dia da data atual e o formatará como data/hora > '2020/12/31'

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
```

Nível de data: exemplo dos últimos 2 meses:

```
datetime > date_format(date_add('month', - 2, CURRENT_DATE), '%Y/%m/%d')
```

Nível de data: Entre 2 datas, exemplo:

```
datetime > '2021/01/01'
      AND
      datetime < '2021/01/10'
```

Nível de registro de data e hora: exemplo das últimas 12 horas:

Particione os dados digitalizados para durar 1 dia e, em seguida, filtre todos os eventos nas últimas 12 horas

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND
      eventtime > date_format(date_add('hour', - 12, CURRENT_TIMESTAMP), '%Y-%m-%dT%H:
%i:%sZ')
```

Nível de timestamp: entre 2 timestamps, exemplo:

Obtenha eventos entre 1º de janeiro de 2021 às 12h e 10 de janeiro de 2021 às 15h.

```
datetime > '2021/01/01' AND datetime < '2021/01/10'
      AND
      eventtime > '2021-01-01T12:00:00Z' AND eventtime < '2021-01-10T15:00:00Z'
```

Exemplos de consulta padrão

ams_access_session_query_v1

```
Name: ams_access_session_query_v1

Description: >-
   The query provides more information on specific AMS access session.
   The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   By default; the query filter last day events only, the user can change the datetime
 filter to search for more wide time range.
   By default; the IAM PrincipalId filter is disabled. To enable it, remove "-- " from
 that line.

AthenaQueryString: |-
   /*
     The query provides list of AMS access sessions during specific time range.
     The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
     If you want to only show access sessions for a particular IAM principal ID, remove
 the double-dash (--) from
     the "IAM Principal ID" filter line in the WHERE clause of the query, and replace
 the placeholder "<IAM PrincipalId>" with the specific ID that you want.
     You can run the query without the filter to determine the exact IAM PrincipalId
 you want to filter with.

     By default; the query only shows AMS access sessions. If you also want to show
 non-AMS access sessions,
     remove the "useragent" filter in the WHERE clause of the query.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
```

```
      json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
      json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionId",
      eventtime AS "EventTime",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventid AS "EventId",
      json_extract_scalar(requestparameters, '$.tags[0].value') AS "BusinessNeed",
      json_extract_scalar(requestparameters, '$.tags[1].value') AS "BusinessNeedType",
      json_extract_scalar(requestparameters, '$.tags[2].value') AS "Requester",
      json_extract_scalar(requestparameters, '$.tags[3].value') AS "AccessRequestType"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND eventname = 'AssumeRole'
      AND useragent = 'access.managedservices.amazonaws.com'
      -- AND  json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId')
 = '<IAM PrincipalId>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of AMS access sessions during specific time range.
   # The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   #
   # By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
   # If you want to only show access sessions for a particular IAM principal ID, remove
 the # (#) from
   # the "IAM Principal ID" filter of the query, and replace the placeholder "<IAM
 PrincipalId>" with the specific ID that you want.
   # You can run the query without the filter to determine the exact IAM PrincipalId
 you want to filter with.
   #
   # By default; the query only shows AMS access sessions. If you also want to show
 non-AMS access sessions,
   # remove the "useragent" filter from the query.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter eventName="AssumeRole" AND userAgent="access.managedservices.amazonaws.com"
```

```
   # | filter responseElements.assumedRoleUser.assumedRoleId= "<IAM PrincipalId>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
      requestParameters.tags.0.value as BusinessNeed,
      requestParameters.tags.1.value as BusinessNeedType,
      requestParameters.tags.2.value as Requester,
      requestParameters.tags.3.value as AccessRequestType
```

ams_events_query_v1

```
ams_events_query_v1.yaml
/*
  The query provides list of events to track write actions for all AMS changes.
  The query returns all write actions done on the account using that AMS role filter.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  You can also track mutating actions done by non-AMS roles by removing the
 "useridentity.arn" filter lines from the WHERE clause of the query.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   useridentity.arn AS "RoleArn",
   eventid AS "EventId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventsource AS "EventService",
   eventtime AS "EventTime",
   requestparameters As "RequestParameters",
```

```
   responseelements AS "ResponseElements",
   useragent AS "UserAgent"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   readonly <> 'true'
   AND
   (
      LOWER(useridentity.arn) LIKE '%/ams%'
      OR LOWER(useridentity.arn) LIKE '%/customer_ssm_automation_role%'
   )
ORDER BY eventtime
```

ams_instance_access_sessions_query_v1

```
ams_instance_access_sessions_query_v1
/*
  The query provides list of AMS Instance accesses during specific time range.

  The query returns the list of AMS instance accesses; every record includes the event
 time, the event AWS Region, the instance ID, the IAM session ID, and the SSM session
 ID.
  You can use the IAM Principal ID to get more details on the business need for
 accessing the instance by using ams_access_session_query_v1 athena query.
  You can use the SSM session ID to get more details on the instance access session,
 including the start and end time of the session and log details, using the AWS Session
 Manager Console in the instance's AWS Region.

  You can also list non-AMS instance accesses by removing the "useridentity" filter
 line in the WHERE clause of the query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   json_extract_scalar(requestparameters, '$.target') AS "InstanceId",
   json_extract_scalar(responseelements, '$.sessionId') AS "SSM SessionId",
```

```
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventsource AS "EventService",
   eventtime AS "EventTime"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   useridentity.sessionContext.sessionIssuer.arn like '%/ams_%'
   AND eventname = 'StartSession'
ORDER BY eventtime
```

ams_privilege_escalation_events_query_v1

```
ams_privilege_escalation_events_query_v1.yaml
/*
  The query provides list of events that can directly or potentially lead to a
 privilege escalation.

  The query accepts ActionedBy as an optional filter and returns EventName, EventId,
 EventTime, ... etc.
  All fields associated with the event are also returned. Some fields are blank if not
 applicable for that event.
  You can use the IAM Session ID to get more details about events happened in that
 session by using ams_session_events_query_v1 query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  By default, the ActionedBy filter is disabled (it shows privilege escalation events
 from all users).
  To show events for a particular user or role, remove the double-dash (--) from the
 useridentity filter line in the WHERE clause of the query
  and replace the placeholder "<ACTIONEDBY_PUT_USER_NAME_HERE>" with an IAM user or
 role name.
  You can run the query without the filter to determine the exact user you want to
 filter with.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
```

```
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventtime AS "EventTime",
   json_extract_scalar(requestparameters, '$.userName') AS "UserName",
   json_extract_scalar(requestparameters, '$.roleName') AS "RoleName",
   json_extract_scalar(requestparameters, '$.groupName') AS "GroupName",
   json_extract_scalar(requestparameters, '$.policyArn') AS "PolicyArn",
   json_extract_scalar(requestparameters, '$.policyName') AS "PolicyName",
   json_extract_scalar(requestparameters, '$.permissionsBoundary') AS
 "PermissionsBoundary",
   json_extract_scalar(requestparameters, '$.instanceProfileName') AS
 "InstanceProfileName",
   json_extract_scalar(requestparameters, '$.openIDConnectProviderArn') AS
 "OpenIDConnectProviderArn",
   json_extract_scalar(requestparameters, '$.serialNumber') AS "SerialNumber",
   json_extract_scalar(requestparameters, '$.serverCertificateName') AS
 "ServerCertificateName",
   json_extract_scalar(requestparameters, '$.accessKeyId') AS "AccessKeyId",
   json_extract_scalar(requestparameters, '$.certificateId') AS "CertificateId",
   json_extract_scalar(requestparameters, '$.newUserName') AS "NewUserName",
   json_extract_scalar(requestparameters, '$.newGroupName') AS "NewGroupName",
   json_extract_scalar(requestparameters, '$.newServerCertificateName') AS
 "NewServerCertificateName",
   json_extract_scalar(requestparameters, '$.name') AS "SAMLProviderName",
   json_extract_scalar(requestparameters, '$.sAMLProviderArn') AS "SAMLProviderArn",
   json_extract_scalar(requestparameters, '$.sSHPublicKeyId') AS "SSHPublicKeyId",
   json_extract_scalar(requestparameters, '$.virtualMFADeviceName') AS
 "VirtualMFADeviceName"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   (
     -- More event names can be found at https://docs.aws.amazon.com/IAM/latest/
UserGuide/list_identityandaccessmanagement.html
     eventname LIKE 'Add%' OR
     eventname LIKE 'Attach%' OR
     eventname LIKE 'Delete%' AND eventname != 'DeleteAccountAlias' OR
     eventname LIKE 'Detach%' OR
     eventname LIKE 'Create%' AND eventname != 'CreateAccountAlias' OR
```

```
     eventname LIKE 'Put%' OR
     eventname LIKE 'Remove%' OR
     eventname LIKE 'Update%' OR
     eventname LIKE 'Upload%' OR
     eventname = 'DeactivateMFADevice' OR
     eventname = 'EnableMFADevice' OR
     eventname = 'ResetServiceSpecificCredential' OR
     eventname = 'SetDefaultPolicyVersion'
   )
   AND eventsource = 'iam.amazonaws.com'
ORDER BY eventtime
```

ams_resource_events_query_v1

```
Name: ams_resource_events_query_v1

Description: >-
   The query provides list of events done on specific resource.
   The query accepts resource id as part of the filters, and return all write actions
 done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of events done on specific resource.

     The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the WHERE clause of the query),
     and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
     Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
```

```
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventid AS "EventId",
      eventsource AS "EventService",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
      AND
      (
         requestparameters LIKE '%<RESOURCE_INFO>%'
         OR responseelements LIKE '%<RESOURCE_INFO>%'
      )
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of events done on specific resource.
   #
   # The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the filter of the query),
   # and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
   # Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
   # | filter RequestParameters like "RESOURCE_INFO" or ResponseElements like
 "<RESOURCE_INFO>"
   | fields
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
```

```
      awsRegion as EventRegion,
      eventID as EventId,
      eventSource as EventService,
      eventTime as EventTime
   | display IAMPrincipalId, IAMSessionId, AccountId, ActionedBy, EventName,
 EventRegion, EventId, EventService, EventTime
   | sort eventTime desc
```

ams_session_events_query_v1

```
Name: ams_session_events_query_v1

Description: >-
   The query provides list of events done on specific session.
   The query accepts IAM Principal Id as part of the filters, and return all write
 actions done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides a list of events executed on a specific session.

     The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the WHERE clause of the query),
     and returns all write actions done on that resource.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventsource AS "EventService",
      eventtime AS "EventTime",
```

```
      requestparameters As "RequestParameters",
      responseelements AS "ResponseElements",
      useragent AS "UserAgent"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate   WHERE
      useridentity.principalid = '<PRINCIPAL_ID>'
      AND datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides a list of events executed on a specific session.
   #
   # The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the filter of the query),
   # and returns all write actions done on that resource.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0 AND userIdentity.principalId = "<IAM Principal>"
   | sort eventTime desc
   | fields
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventSource as EventService,
      eventTime as EventTime,
      userAgent as UserAgent
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
```

ams_session_ids_by_requester_v1

```
Name: ams_session_ids_by_requester_v1

Description: >-
   The query provides list of IAM Principal/Session Ids for specific requester.
   The query accepts requester and return all IAM Principal/Session Ids by that
 requester during specific time range.
```

```
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of IAM Principal IDs for a specific requester.

     The query accepts the requester (replace placeholder "<Requester>" in the WHERE
 clause of the query),
     and returns all IAM Principal IDs by that requester during a specific time range.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
      json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionIId",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND json_extract_scalar(requestparameters, '$.tags[2].value') = '<Requester>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of IAM Principal IDs for a specific requester.
   #
   # The query accepts the requester (replace placeholder "<Requester>" in the filter
 of the query),
   # and returns all IAM Principal IDs by that requester during a specific time range.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   filter eventName="AssumeRole" AND requestParameters.tags.2.value="<Requester>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
```

```
    responseElements.credentials.accessKeyId as IAMSessionId,
    eventTime as EventTime
```

Alterar permissões de registro

As seguintes permissões são necessárias para executar consultas de registro de alterações:

- Athena
  - Atena: GetWorkGroup
  - Atena: StartQueryExecution
  - Atena: ListDataCatalogs
  - Atena: GetQueryExecution
  - Atena: GetQueryResults
  - Atena: BatchGetNamedQuery
  - Atena: ListWorkGroups
  - Atena: UpdateWorkGroup
  - Atena: GetNamedQuery
  - Atena: ListQueryExecutions
  - Atena: ListNamedQueries
- AWS KMS
  - kms:Decrypt
  - AWS KMS ID de chave ou seus IDs de AWS KMS chave AMSCloudTrailLogManagement, se o Accelerate estiver usando seu armazenamento de dados de bucket Amazon S3 de eventos de CloudTrail trilha usando criptografia SSE-KMS.
- AWS Glue
  - cola: GetDatabase
  - cola: GetTables
  - cola: GetDatabases
  - cola: GetTable
- Acesso de leitura ao Amazon S3
  - CloudTrail Armazenamento de dados de bucket do Amazon S3: ams-a *`AccountId`* - cloudtrail-*`primary region`*, ou o nome do seu bucket do Amazon S3, eventos de trilha Armazenamento de dados do bucket do Amazon S3. CloudTrail

- Acesso de gravação ao Amazon S3
  - Resultados da consulta de eventos do Athena Amazon S3 bucket: ams-a athena-results-*AccountId primary region*

AWS Systems Manager em Accelerate

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 da Amazon. O processo do AMS para desenvolvimento e publicação de documentos SSM segue as melhores práticas da AWS e exige várias revisões por pares durante todo o ciclo de vida do documento. Para obter mais informações sobre as melhores práticas da AWS para compartilhar documentos de SSM, acesse Melhores práticas para documentos de SSM compartilhados.

Documentos SSM do AMS Accelerate disponíveis

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

Para ver os documentos SSM do AMS Accelerate 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 AWS CLI obter instruções, consulte Como usar documentos SSM compartilhados.

Versões de documentos SSM do AMS Accelerate

Os documentos SSM oferecem suporte ao controle de versão. Os documentos SSM do AMS Accelerate não podem ser modificados na conta do cliente e não podem ser compartilhados

novamente. Eles são gerenciados e mantidos centralmente pelo AMS Accelerate para operar a conta.

Os números de versão são incrementados com cada atualização de documento em uma região específica 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 Accelerate, recomendamos comparar seus hashes com: AWS CLI

```
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

Não há custo associado ao acesso a documentos SSM do AMS Accelerate. 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.

Histórico de documentos do Guia do usuário do AMS Accelerate

A tabela a seguir descreve as mudanças importantes em cada versão do Guia do Usuário do AMS Accelerate. Para receber notificações sobre atualizações dessa documentação, é possível inscrever-se em um feed RSS.

Alteração	Descrição	Data
Gerenciamento de registros atualizado — AWS CloudTrail seção	Novas informações e notas sobre o AWS CloudTrail registro.	25 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 de depreciação atualizada para o serviço Change Record	Nota de depreciação atualizada para o serviço Change Record com soluções alternativas.	11 de setembro de 2025
Verificações Trusted Advisor de segurança atualizadas suportadas pelo Trusted Remediator	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
Verificações Trusted Advisor de segurança atualizadas suportadas pelo Trusted Remediator	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
Verificações de excelência Trusted Advisor operacional atualizadas suportadas pela seção Trusted Remediator	Verificações de excelência Trusted Advisor operacional atualizadas suportadas pelo Trusted Remediator para adicionar uma nova verificação suportada c1fd6b96l4 Amazon S3 Access Logs Enabled.	28 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
O link do glossário do TOC foi removido	AWS Glossário.	8 de agosto de 2025
Novo campo no relatório diário do Patch	Tags de instância: as tags associadas ao ID da EC2 instância da Amazon.	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-TrustedRemediator EnableBucketAccessLoggingV 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
Perfis de configuração atualizados do Resource Tagger no Accelerate	Foi adicionado um novo AvailabilityZone filtro nos perfis de configuração do Resource Tagger no Accelerate.	25 de julho de 2025

Relatórios de incidentes, solicitações de serviço e perguntas de cobrança atualizados no Accelerate.	As referências aos níveis de serviço Plus e Premium foram substituídas por um link para o SLA de serviço.	25 de julho de 2025
Gerenciamento de incidentes atualizado no Accelerate.	Informações atualizadas sobre os centros de operações.	25 de julho de 2025
Página de padrões AMS atualizada com links corretos.	Os links de SLA e SLO foram corrigidos.	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
Novo recurso para backups	Personalize as notificações nos cofres de backup com uma nova tag.	25 de julho de 2025
Seção atualizada para configurações suportadas no Accelerate	Configurações suportadas atualizadas para sistemas operacionais suportados e sistemas operacionais Supported End of Support (EOS) no Accelerate.	26 de junho de 2025
Página removida Gerenciando tags para gerenciamento de patches no Accelerate	Página removida Gerencian do tags para gerenciamento de patches no Accelerate, pois esse recurso está obsoleto.	19 de junho de 2025
Nota de segurança important 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 Accelerate.	10 de junho de 2025

Depreciação do registro de alterações do AMS Accelerate.	O serviço AMS Accelerate Change Record será descontinuado a partir de 1º de julho de 2025.	27 de maio de 2025
Atualizações de sistemas operacionais compatíveis.	Os sistemas operacionais compatíveis com o AMS Accelerate foram atualizados, alguns adicionados e outros removidos.	22 de maio de 2025
Nota sobre os serviços suportados pela região do Oriente Médio (EAU).	Suporte limitado para alguns serviços na região do Oriente Médio (EAU).	22 de maio de 2025
Somente interno APIs.	Somente internos APIs que aparecem em alguns registros . CloudWatch	22 de maio de 2025
Foram adicionados locais de registro ausentes.	Alguns locais de registro do Windows ausentes foram adicionados.	22 de maio de 2025
Atualizações do AMS Accelerate Trusted Remediator.	Como usar um novo parâmetro,`preconfigured-parameters` , para personalizar as Trusted Advisor verificações no Trusted Remediator.	22 de maio de 2025

Perguntas frequentes e atualizações do AMS Accelerate Trusted Remediator.	Várias atualizações nas Trusted Advisor verificaç ões 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 Accelerate Standard.	Foram adicionados controles de “Compartilhamento de grupos de segurança”.	8 de maio de 2025
Acelere a atualização dos alertas de monitoramento.	Alertas adicionais adicionad os, além do nome do alerta adicionado à coluna Notas.	28 de abril de 2025
Acelere o inventário de recursos.	O arquivo da planilha de inventário de recursos (compactado) é atualizado.	24 de abril de 2025
Acelere a localização dos registros.	Localizações de registro adicionais adicionadas.	24 de abril de 2025
Acelere novas funções e responsabilidades (RACI) para resposta a incidentes de segurança.	RACI para resposta a incidentes de segurança.	27 de março de 2025
Acelere o novo alerta de remediação automática do Amazon RDS.	ID do alerta: - 0224, é acionado quando o armazenamento alocado solicitado atinge ou excede o limite máximo de armazenam ento configurado.	27 de março de 2025

Acelere a atualização do modelo de função de integração.	O modelo de função de integração do AMS Accelerate foi atualizado para oferecer suporte às GovCloud regiões da AWS.	25 de março de 2025
Acelere o alerta RDS de novas remediações automáticas.	RDS-EVENT-0224 adicionado.	17 de março de 2025
Acelerar Novo recurso: notificações de incidentes.	Você pode usar AppRegistry para criar aplicativos e personalizar as notificações de incidentes para esses aplicativos.	13 de março de 2025
Acelere a atualização do 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
Acelere a atualização para a correção automática da tabela de alertas do AMS.	A tabela de correção de alertas foi expandida com novos conteúdos.	20 de fevereiro de 2025
Acelere o novo recurso: Retain Alarms.	Você pode configurar o Gerenciador de alarmes para reter os alarmes em CloudWatch vez de excluí-los automaticamente.	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) • Painel do Resource Tagger • Painel de regras de configuração de segurança	28 de janeiro de 2025

Foram adicionadas AWS Trusted Advisor verificações adicionais suportadas pelo Trusted Remediator	As seguintes Trusted Advisor verificações agora são suportadas pelo Trusted Remediator:
	• Otimização de custo
	  • c1cj39rr6v - Configuração incompleta de cancelamento de upload em várias partes do Amazon S3
	• Segurança
	  • Hs4Ma3G199 - As instâncias de banco de dados do RDS devem publicar registros nos registros CloudWatch
	  • Hs4Ma3G326 - A configuração de bloqueio de acesso público do Amazon EMR deve estar ativada
	  • Hs4Ma3G272 - Os usuários não devem ter acesso root às instâncias do notebook AI SageMaker
	  • Hs4Ma3G325 - Os clusters EKS devem ter o registro de auditoria ativado
	  • HHs4Ma3G118 - Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou saída
		28 de janeiro de 2025

- Hs4Ma3G127 - O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados
- Hs4Ma3G124 - As instâncias da EC2 Amazon devem usar o Instance Metadata Service versão 2 () IMDSv2

- Tolerância a falhas
  - c1qf5bt013 - As instâncias de banco de dados do Amazon RDS têm o escalonamento automático de armazenamento desativado
  - 7q GXs KIUw - Drenagem de conexão do Classic Load Balancer
  - c18d2gz106 - Amazon EBS não incluído no plano AWS Backup
  - c18d2gz107 - Tabela do Amazon DynamoDB não incluída no plano AWS Backup
  - cc18d2gz117 - Amazon EFS não incluído no plano AWS Backup
  - c18d2gz105 - Balanceamento de carga cruzado do Network Load Balancer

    - c1qf5bt026 - O parâmetro synchronous_commit do Amazon RDS está desativado
    - c1qf5bt030 - O parâmetro innodb_flush_log_at_trx_commit do Amazon RDS não é 1
    - c1qf5bt031 - O parâmetro sync_binlog do Amazon RDS está desativado
    - c1qf5bt036 - A configuração do parâmetro innodb_default_row_format do Amazon RDS não é segura
    - c18d2gz144 - Monitoramento detalhado da Amazon não ativado EC2
- Excelência operacional
    - c18d2gz125 - O Amazon API Gateway não registra registros de execução
    - c18d2gz168 - Proteção de carga elástica não habilitada para balanceadores de carga Balancing Deletion
    - c1qf5bt012 - O Amazon RDS Performance Insights está desativado
- Desempenho
    - c1qf5bt021 - Parâmetro innodb_change_buffering

	do Amazon RDS usando menos do que o valor ideal • c1qf5bt025 - O parâmetro de autovacuum do Amazon RDS está desativado • c1qf5bt028 - O parâmetro enable_indexonlyscan do Amazon RDS está desativado • c1qf5bt029 - O parâmetro enable_indexscan do Amazon RDS está desativado • c1qf5bt032 - O parâmetro innodb_stats_persistent do Amazon RDS está desativado • c1qf5bt037 - O parâmetro Amazon _logging está ativado RDSgeneral	
Planilha de inventário de recursos atualizada	Planilha de inventário de recursos atualizada.	23 de janeiro de 2025
Novo recurso do AMS: relatórios de autoatendimento agregados	Os relatórios de autoatend imento agregados (SSR) fornecem uma visão dos relatórios de autoatendimento existentes agregados no nível da organização, entre contas.	21 de janeiro de 2025

Novo recurso de aceleração de patches: Patch Hooks	Use esse recurso para configurar “ganchos” com documentos de comando SSM para executar comandos no nível do sistema operacional antes ou depois da correção.	16 de janeiro de 2025
Atualização para a seção Como o monitoramento funciona	Foram adicionadas informaçõ es sobre um novo recurso, configurando notificações de alerta por recurso ou ID da instância, em vez de por incidente.	8 de janeiro de 2025
Atualização na seção de integração do EKS Monitoring and Incident Management	A nota do procedimento de integração foi atualizada para esclarecer quando os sinais de alerta são suspensos e retomados.	19 de dezembro de 2024
Registro da conta do membro adicionado ao Trusted Remediator	Você pode usar o registro de contas de membros para encontrar o ID da conta, a integração e o Regiões da AWS tempo de execução de cada conta de membro.	19 de dezembro de 2024
Pré-requisitos para o uso do SSM Agent	O conteúdo sobre o bloqueio do tráfego de saída é atualizad o.	4 de dezembro de 2024
O monitoramento acelerado e o gerenciamento de incidentes do EKS agora são suportados na Ásia-Pacífico (Hong Kong) Região da AWS	A região Ásia-Pacífico (Hong Kong) agora conta com o apoio do Accelerate Monitorin g and Incident Management for EKS	21 de novembro de 2024

Tabela atualizada de ofertas do Operations On Demand	Os seguintes sistemas operacionais são compatíveis com atualizações no local: • Microsoft Windows 2016 a Microsoft Windows 2022 e superior	11 de novembro de 2024
O monitoramento acelerado e o gerenciamento de incidentes do EKS agora são suportados na África (Cidade do Cabo) Região da AWS.	A África (Cidade do Cabo) agora é apoiada pelo Accelerate Monitoring and Incident Management for EKS	4 de novembro de 2024
Tabela atualizada de ofertas do Operations On Demand	Os seguintes sistemas operacionais são compatíveis com atualizações no local: • 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	1.º de novembro de 2024
Modelo de início rápido atualizado	Diagrama atualizado, parâmetros de modelo e arquivo de modelo yaml.	28 de outubro de 2024

Trusted Advisor verificações adicionadas ao Trusted Remediator no AMS	As seguintes Trusted Advisor verificações agora estão disponíveis no Trusted Remediator: • Z4 AUBRNSmz - Endereços IP elásticos não associados • c18d2gz128 - Repositório Amazon ECR sem política de ciclo de vida configurada • c18d2gz138 - Recuperação do DynamoDB Point-in-time • Hs4Ma3G323 - O Dynamo deve ter a proteção de exclusão ativada DBtables • Hs4Ma3G247 - O Amazon Transit EC2 Gateway não deve aceitar automatic amente solicitações de anexos de VPC • Hs4Ma3G308 - Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada • Hs4Ma3G299 - Os clusters de banco de dados Neptune devem ter a proteção de exclusão ativada • Hs4Ma3G306 - Os snapshots manuais do cluster do Amazon DocumentDB não devem ser públicos	25 de outubro de 2024

	• Hs4Ma3G109 - a validação do arquivo de CloudTrail log deve ser ativada • Hs4Ma3G217 - os ambientes do CodeBuild projeto devem ter uma configuração AWS de log 4 • Hs4Ma3G158 - Documento s SSM não devem ser públicos • Hs4Ma3G319 - Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada	
Configurações suportadas atualizadas	Os sistemas operacionais Oracle Linux compatíve is foram atualizados para 9.0-9.3, 8.0-8.9, 7.5-7.9.	24 de outubro de 2024
Nova seção adicionada ao Offboard do AMS Accelerate	Instruções sobre como desligar com as dependênc ias do Alarm Manager e do Resource Tagger adicionadas ao Offboard a partir do AMS Accelerate.	24 de outubro de 2024
O painel do Resource Tagger já está disponível.	O painel do Resource Tagger agora está disponível nos relatórios de autoatendimento.	26 de setembro de 2024
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

Os limites do AMS Accelerate agora estão incluídos no gerenciamento de patches do AMS.	Os limites do AMS Accelerate estão incluídos no Gerenciamento de patches - Crie uma janela de manutenção de patches.	30 de agosto de 2024
Atualização da descoberta de contas do AMS Accelerate	Uma nova seção no Account Discovery foi adicionada para a Amazon EC2 Instance Evaluation.	29 de agosto de 2024
A linha de base de patches padrão do AMS Accelerate agora está disponível para sistemas operacionais Ubuntu.	A linha de base de patches padrão do AMS Accelerate agora está disponível para sistemas operacionais Ubuntu.	22 de agosto de 2024
Atualização da descoberta de contas do AMS Accelerate	Quatro novas chamadas de AWS API foram adicionadas à seção AWS CloudTrail Avaliação na tabela de verificação operacional.	2 de agosto de 2024
O Trusted Remediator agora oferece suporte a uma verificação adicional	O Trusted Remediator agora suporta a verificação de segurança Hs4Ma3G192 - as instâncias de banco de dados do RDS devem proibir o acesso público.	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
O AMS Accelerate onboarding_role_minimal.zip agora contém o código do Terraform	O AMS Accelerate onboarding_role_minimal.zip agora contém o código do Terraform.	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 Accelerate agora é compatível com Oracle Linux 8.9, RHEL 8.10 e RHEL 9.4.	O AMS Accelerate agora é compatível com Oracle Linux 8.9, RHEL 8.10 e RHEL 9.4.	5 de julho de 2024
O processo de descoberta de contas do AMS Accelerate foi atualizado.	O processo de descoberta de contas usado na integração com Contas da AWS o AMS Accelerate é atualizado.	1º de julho de 2024
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.	24 de junho de 2024
O 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
Sistemas operacionais compatíveis atualizados	O AMS Accelerate agora suporta AlmaLinux 8.3-8.9, 9.0-9.2 (só AlmaLinux é compatível com a arquitetura x86)	19 de junho de 2024
O limite automático do perfil de instância agora aumenta se o padrão for atingido.	O AMS agora aumenta o limite padrão do perfil de instância para 20 se o limite padrão de 10 for atingido.	18 de junho de 2024

O recurso de instalação automática do AMS SSM Agent agora está ativado por padrão.	O recurso de instalação automática do AMS SSM Agent está ativado por padrão para contas integradas após 6/03/2024.	7 de junho de 2024
Perguntas frequentes sobre segurança adicionadas ao gerenciamento de segurança.	Agora, está disponível uma seção de perguntas frequentes sobre as melhores práticas de segurança, controles , modelos de acesso e mecanismos de auditoria usados quando um engenheiro de operações ou automação do AMS acessa suas contas.	3 de junho de 2024
AWS Regiões adicionais agora são suportadas pelo monitoramento e gerenciamento de incidentes do Amazon EKS.	Agora, três AWS regiões adicionais são suportadas pelo monitoramento e gerenciamento de incidentes do Amazon EKS.	23 de maio de 2024
As notificações de patch de solicitação de serviço agora são enviadas antes das janelas de manutenção de patches.	O AMS Accelerate Patching cria uma nova solicitação de serviço 4 dias antes da janela de manutenção de patches. Você pode usar a solicitação de serviço para se comunicar com o AMS para ajustes no patch ou para pular um patch.	3 de maio de 2024
Limites de alerta adicionados à tabela de alertas de linha de base de monitoramento do AMS Accelerate EKS.	Os limites de alerta detalhados agora estão disponíveis na tabela de alertas de linha de base para monitoramento do Amazon EKS.	3 de maio de 2024

Atualizado: Perfis de configuração do Alarm Manager.	Foram adicionadas notas sobre a criação de alarmes de detecção de anomalias com o Gerenciador de alarmes.	25 de abril de 2024
Adições aos perfis de configuração do Resource Tagger.	As tabelas do DynamoDB e os buckets do Amazon S3 agora estão disponíveis no Resource Tagger	25 de abril de 2024
Foi adicionada a seção de informações sobre Gerenciamento de Eventos Planejados (PEM).	Informações detalhadas sobre a oferta do serviço PEM agora estão disponíveis no Guia do usuário do AMS Accelerate.	25 de abril de 2024
O AMS é compatível com o Red Hat Enterprise Linux (RHEL) 9.x.	O AMS é compatível com o Red Hat Enterprise Linux (RHEL) 9.x.	25 de abril de 2024
O AMS Accelerate suporta relatórios para todas as configurações de AWS região.	O AMS Accelerate suporta relatórios de inventário SSM para todas as configurações de AWS região.	25 de abril de 2024
Atualizado: políticas AWS gerenciadas.	Atualizado o AWSManaged ServicesDeploymentToolkitPolicy com novas permissões de ECR.	4 de abril de 2024
Atualizado: seção de perfis de configuração do Resource Tagger	Adicionado `AWS::EFS::FileSystem` à ResourceTypelista.	21 de março de 2024

Atualizado: relatórios de incidentes e solicitações de serviço na seção Acelerar.	O título do tópico foi alterado para Relatórios de incidente s, solicitações de serviço e perguntas sobre faturamento no Accelerate. Foi adicionad a uma nova seção, Perguntas sobre faturamento.	21 de março de 2024
Atualizado: seção Como funciona o gerenciamento de solicitações de serviço.	Foi adicionado um esclareci mento sobre como o AMS lida com solicitações de serviço que contêm uma solicitação de recurso ou um bug.	21 de março de 2024
Atualizado: Crie a função aws_managedservice s_onboarding_role com a seção CloudFormation	Comandos adicionados para criar a função AWS CloudShel l.	21 de março de 2024
Atualizado: modelo de início rápido (opcional)	Comandos adicionados para baixar o modelo AWS CloudShell.	21 de março de 2024
Novos tipos de recursos disponíveis para perfis de configuração do Alarm Manager.	Foram adicionados tipos de recursos para Amazon FSx, Amazon EFS e Elasticsearch aos perfis de configuração do Alarm Manager.	21 de março de 2024
Substituições adicionais de pseudoparâmetros disponíveis para o perfil de configuração.	Foram adicionadas substitui ções de FSx pseudopar âmetros do Amazon EFS e do Amazon.	21 de março de 2024
Foi adicionada uma nova seção aos Recursos no tópico Descrição do serviço.	Foi adicionada uma nova seção, Gerenciamento de solicitações de serviço, nos recursos do AMS Accelerate.	21 de março de 2024

Novas colunas adicionadas ao relatório de autoatendimento Relatório semanal de incidentes	Novas colunas foram adicionadas ao relatório semanal de incidentes para que você possa filtrar os incidentes com base no trimestre, mês, semana ou dia em que o incidente foi criado ou resolvido.	11 de março de 2024

Atualizações anteriores

A tabela a seguir descreve as mudanças importantes na documentação do guia AMS Accelerate antes de março de 2024.

Alteração	Descrição	Data
Melhorias na integração de CloudTrail trilhas do AMS Accelerate	Melhorias na integração de CloudTrail trilhas do AMS Accelerate: • Reúna todas as políticas de bucket em um único bloco • Remova o segundo ID AWS da organização nas declarações de política • Esclareça os requisitos do ambiente do cliente Para obter mais informações, consulte Revise e atualize suas configurações para permitir que o AMS Accelerate use sua trilha CloudTrail.	23 de fevereiro de 2024
Atualizado: processo de integração da conta.	Reestruturou a seção do processo de integração da conta para tornar as etapas mais claras. Também foi adicionado um modelo opcional de Início Rápido para recursos de integração.	22 de fevereiro de 2024

Alteração	Descrição	Data
	Consulte (Opcional) Modelo de início rápido no Accelerate.	
Atualizado: Offboarding AMS Accelerate.	A seção de considerações de desativação do AMS Accelerate foi atualizada para indicar que a `ams-access-management` CloudFormation pilha e a função `ams-access-management` do IAM não são excluídas pelo processo de desativação. Consulte Efeitos de desativação do AMS Accelerate.	22 de fevereiro de 2024
Atualizado: conformidade de configuração no Accelerate.	Alterou o “Relatório de incidentes” para “Solicitação de serviço”, quando aplicável, para evitar confusão nesses termos. Consulte Conformidade de configuração no Accelerate.	22 de fevereiro de 2024
Atualizado: descoberta de contas no Accelerate.	Descoberta de contas reorganizada no Accelerate para agrupar melhor os pré-requisitos com a seção relevante. Consulte Etapa 1. Descoberta de contas no Accelerate.	22 de fevereiro de 2024
Renomeado: AMS Patch reportando para o gerenciamento de host do AMS.	Renomeou o relatório de patches do AMS para gerenciamento de host do AMS e renomeou o relatório, relatório de detalhes do patch, para relatório de cobertura do agente SSM. Consulte Relatórios de gerenciamento de hosts do AMS.	22 de fevereiro de 2024

Alteração	Descrição	Data
Catálogo atualizado de operações sob demanda	Atualizou a tabela do catálogo de ofertas do Operations on Demand para remover referênci as a “saúde” em`Amazon EKS cluster maintenance` . Consulte Solicitando operações de AMS sob demanda.	22 de fevereiro de 2024
Roteador de eventos AMS atualizado	Atualizado `AMSCoreRule` na seção Roteador de Eventos do AMS. Consulte Usando as regras EventBridge gerenciadas da Amazon no AMS.	22 de fevereiro de 2024
Sistemas operacionais suportados atualizados.	Sistemas operacionais compatíveis atualizados para incluir o SUSE Linux Enterprise Server 15 SP5. Consulte Configurações compatíveis.	22 de fevereiro de 2024
Automação atualizada da remediação do uso do EC2 volume	Atualizou a seção de automação de remediaçã o de uso de EC2 volume com o cronograma correto de expansão de capacidade. Consulte EC2 automação de remediação de uso de volume.	22 de fevereiro de 2024
Atualizado: revise e atualize suas configurações para permitir que o Accelerate use sua trilha CloudTrail	A seção de política de bucket do AMS Accelerate Organization CloudTrail S3 foi atualizada. Consulte Revise e atualize suas configurações para permitir que o AMS Accelerate use sua trilha CloudTrail	15 de fevereiro de 2024
Novo recurso adicionado: instalação automática do SSM Agent	Foi adicionada uma nova seção para instalação automática do SSM Agent Consulte Instalação automática do SSM Agent.	26 de janeiro de 2024

Alteração	Descrição	Data
Atualizado: configurações suportadas	Foram adicionadas informações sobre as versões suportadas do AWS Control Tower Consulte Configurações compatíveis.	26 de janeiro de 2024
Atualizado: relatório do AMS Patch.	Três seções do relatório do AMS Patch foram removidas: • Relatório resumido de detalhes da instância de patch • Relatório de detalhes do patch • Relatório de instâncias que perderam patches Consulte Relatórios de gerenciamento de hosts do AMS.	22 de dezembro de 2023
Atualizado: acelere os pré-requisitos de integração.	Atualizamos os planos de suporte necessários para integrar o AMS Accelerate. Consulte Acelere os pré-requisitos de integração.	15 de dezembro de 2023
Atualizado: Crie uma janela de manutenção de patches.	A seção do ciclo de patches padrão foi removida, pois esse recurso está obsoleto. Consulte Crie uma janela de manutenção de patches no AMS.	13 de dezembro de 2023
Atualizado: configurações de notificação no Accelerate.	Esclareceu qual e-mail é usado para notificações. Consulte Configurações de notificação no Accelerate para obter mais informações.	12 de dezembro de 2023

Alteração	Descrição	Data
Atualizado: `AMSAccelerateCustomerAccessPolicies` modelo.	O `AMSAccelerateCustomerAccessPolicies` modelo foi atualizado para corrigir um erro de sintaxe. Consulte Permissões para usar os recursos do AMS para obter mais informações.	12 de dezembro de 2023
Adicionado: revisões de segurança da solicitação de alteração	Foi adicionada uma nova seção Revisões de segurança de solicitações de alteração em Gerenciamento de segurança. Consulte Revisões de segurança da solicitação de alteração para obter mais informações.	11 de dezembro de 2023
Atualizado: resource_inventory.xlsx	O resource_inventory.xlsx foi atualizado para incluir funções de analista de segurança. Consulte Inventário de recursos para Accelerate para obter mais informações.	17 de novembro de 2023
Atualizado: descrição da ams-access-admin-operations função	ams-access-admin-operationsDescrição atualizada. Consulte Por que e quando o AMS acessa sua conta e Autenticação com identidades no AMS Accelerate para obter mais informações.	17 de novembro de 2023
Atualizado: considerações sobre o desligamento do AMS Accelerate	Seção de segurança atualizada para esclarecer o que está disponível na Amazon GuardDuty e AWS Config as regras após a desativação. Consulte Efeitos de desativação do AMS Accelerate para obter mais informações.	17 de novembro de 2023

Alteração	Descrição	Data
Adicionado: monitoramento e gerenciamento de incidentes para o Amazon EKS	O monitoramento e o gerenciamento de incidentes do Amazon EKS monitoram seus recursos do Amazon EKS em busca de falhas, degradação do desempenho e problemas de segurança. Consulte Monitoramento e gerenciamento de incidentes para o Amazon EKS no AMS Accelerate para obter mais informações.	14 de novembro de 2023
Atualizado: Marcação	Foram adicionadas informações sobre a marcação fornecida pelo cliente. Consulte Tags fornecidas pelo cliente no Accelerate para obter mais informações.	7 de novembro de 2023
Atualizado: Perfis de configuração do Resource Tagger	Adicionado AWS::AutoScaling::AutoScalingGroup, AWS::EKS::Cluster, AWS::Elasticsearch::Domain, and AWS::FSx::FileSystem à seção Filtro. Consulte Perfis de configuração do marcador de recursos no AMS Accelerate para obter mais informações.	27 de outubro de 2023
Atualizado: Descrição do serviço	Adicionou o Ubuntu 22.04 aos sistemas operacionais compatíveis. Consulte Service description (Descrição do serviço)	29 de setembro de 2023
Atualizado: Pré-requisitos de integração do AMS Accelerate	Foi adicionada uma nota aos endpoints VPC do AMS Accelerate para incluir o modelo. CloudFormation Consulte Acelere os pré-requisitos de integração.	29 de setembro de 2023
Atualizado: Detectar	O tipo de proteção de endpoint foi removido da resposta de segurança do AMS Accelerate. Consulte Detectar.	29 de setembro de 2023

Alteração	Descrição	Data
Atualizado: Alertas do monitoramento de linha de base no AMS	Adicionado AWS Outposts à tabela Alertas do monitoramento de linha de base. Consulte Detectar monitoring-default-metrics.	29 de setembro de 2023
Atualizado: Crie a função aws_managedservices_onboarding_role com CloudFormation	Captura de tela atualizada para especificar detalhes da pilha. Consulte Crie `aws_managedservices_onboarding_role` com o CloudFormation for Accelerate.	29 de setembro de 2023
Atualizado: Amazon EventBridge Managed Rules implantado pelo AMS Accelerate	Foi adicionada a nova regra gerenciada do AMS Accelerate Amazon EventBridge Managed AMSCoreRule. O AMS Accelerate Amazon EventBridge Managed Rule foi atualizado AMSAccessRolesRulepara adicionar uma nova função. Consulte Amazon EventBridge Managed Rules implantadas pelo AMS para obter mais informações.	19 de setembro de 2023
Atualizado: Perfis de configuração do Alarm Manager	Foram adicionados identificadores de substituição de pseudoparâmetros do AWS Outposts. Consulte Monitoramento e gerenciamento de eventos no AMS Accelerate.	11 de setembro de 2023
Atualizado: Perfis de configuração do Resource Tagger	Foi adicionado o tipo de recurso AWS Outposts. Consulte Perfil de configuração acelerada: substituição de pseudoparâmetros.	11 de setembro de 2023
Atualizado: serviços suportados	O Amazon Elastic File System foi adicionado à seção Serviços monitorados por CloudWatch alarmes. Consulte Service description (Descrição do serviço) para obter mais informações.	6 de setembro de 2023

Alteração	Descrição	Data
Atualizado: monitoramento de patches e correção de falhas	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 Entenda o gerenciamento de patches no AMS Accelerate para obter mais informaçõ es.	6 de setembro de 2023
Atualizado: Runbook de respostas esclarecidas a eventos de malware	Runbook de resposta esclarecida a eventos de malware para resposta a incidentes de segurança. Consulte Resposta a incidentes de segurança no AMS para obter mais informaçõ es.	6 de setembro de 2023
Atualizado: Conectando sua conta Accelerate ao Transit Gateway	Etapas esclarecidas para conectar uma nova conta Accelerate VPC à rede AMS Multi-Account Landing Zone (criando um anexo TGW VPC): consulte Conectando sua conta Accelerate ao Transit Gateway para obter mais informações.	5 de setembro de 2023
Atualizado: Alertas do monitoramento de linha de base no AMS	Foi removida a referência a dois alarmes obsoletos e. AMSRead LatencyAlarm AMSWrite LatencyAlarm Consulte Alertas do monitoramento de linha de base no AMS para obter mais informações.	5 de setembro de 2023
Adicionado: roteador de eventos AMS	Documentação adicionada para o AMS Event Router Consulte Usando as regras EventBrid ge gerenciadas da Amazon no AMS para obter mais informações.	5 de setembro de 2023

Alteração	Descrição	Data
Atualizado: Lista de pseudoparâmetros do Alarm Manager.	Atualizou a lista de pseudoparâmetros do Alarm Manager. EC2 o parâmetro de nome da EC2 instância foi adicionado às configurações de alarme de instância e EC2 disco. Consulte Perfil de configuração acelerada: substituição de pseudoparâmetros para obter mais informações.	29 de agosto de 2023
Adicionado: AMS Access Offboarding	Consideração adicional ao desativar o AMS Access. Consulte Efeitos de desativação do AMS Accelerate.	24 de 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.	18 de agosto de 2023
Atualizado: funções de acesso do AMS Accelerate	Corrigido um erro de digitação nos nomes das funções. Consulte AWS Identity and Access Management no AMS Accelerate.	10 de agosto de 2023
Atualizado: declarações de política	Substituiu os nomes de funções codificados por curingas. Consulte Revise e atualize suas configurações para permitir que o AMS Accelerate use sua trilha CloudTrail.	10 de agosto de 2023
Atualizado: lista de serviços monitorados com alertas do EFS.	Atualizou a lista de serviços de monitoramento com novos alertas de EFS para monitoramento de linha de base do AMS. Foram adicionados 4 novos tipos de alerta de EFS. Consulte Alertas do monitoramento de linha de base no AMS para obter mais informações.	03 de agosto de 2023
Atualizado: acelere a tabela de inventário de recursos	ams-backup-config-rule-stack e recursos relacionados removidos. Consulte Inventário de recursos para Accelerate.	18 de julho de 2023

Alteração	Descrição	Data
Atualizado: funções de acesso do AMS Accelerate	<8-digit hash>As funções ams-backup-config-rule -st- amsBackupAlert ConfigRul e - <8-digit hash>e ams-backup-config-rule -st- amsBackupPlan ConfigRule H- foram removidas. Consulte AWS Identity and Access Management no AMS Accelerate.	18 de julho 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 para obter mais informações.	19 de junho de 2023
Novo: funções de acesso do AMS Accelerate	Foram adicionadas novas funções de acesso para o AMS Security.	16 de junho de 2023
Novo: o gerenciamento de registros do AMS CloudTrai l Accelerate agora pode usar CloudTrail trilhas de clientes.	Opções atualizadas suportadas pelo Accelerat e para gerenciamento de CloudTrail registros , incluindo a trilha implantada do Accelerat e ou a integração com a CloudTrail conta gerenciada pelo cliente ou a trilha da organizaç ão. Consulte Revise e atualize suas configura ções para permitir que o AMS Accelerate use sua trilha CloudTrail para obter mais informaçõ es.	09 de junho de 2023
Atualizado: Relatório de configuração de resposta do AMS Accelerate Config Rules.	Relatórios atualizados sob solicitação para o AWS Config Rules Response Configuration Report. Consulte Acelerar as atualizações dos relatórios sob solicitação. Consulte Relatório de configuração de respostas do AMS Config Rules.	26 de maio de 2023

Alteração	Descrição	Data
Atualizado: Política de data de início do faturamento de serviços.	Definições atualizadas da data de início do faturamento emTermos-chave do AMS.	15 de maio de 2023
Atualizado: políticas AWS gerenciadas.	Atualizou o AWSManaged ServicesDeployment ToolkitPolicy com novas permissões de CFN e ECR e reduziu o escopo das ações existente s com curingas. Consulte Acelerar atualizaç ões de funções vinculadas a serviços. Consulte Acelere as atualizações de funções vinculadas a serviços.	09 de maio de 2023
Atualizado: links da política de funções de acesso.	Agora, as funções de acesso podem ser baixadas diretamente dos locais de bucket do Accelerate S3. Consulte Por que e quando o AMS acessa sua conta e AWS Identity and Access Management no AMS Accelerate.	
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).	13 de abril de 2023
Atualizado: Lista de alertas.	CloudTrail Referências removidas. Consulte Gerenciamento de registros no AMS Accelerate.	13 de abril de 2023

Alteração	Descrição	Data
Atualizado: Lista de alertas.	Foram adicionados três novos alertas do agente SSM. Consulte Alertas do monitoramento de linha de base no AMS.	13 de abril de 2023
Atualizado: acelere os pré-requisitos.	Esclareceu que o Accelerate exige que um dos quatro planos do AWS Support esteja em vigor e exclui o plano Developer. Consulte Acelere os pré-requisitos de integração.	13 de abril de 2023
Atualizado: acelere a política de funções vinculadas a serviços.	O arquivo zip da política do Serviço de Contatos foi atualizado. Consulte AWS políticas gerenciadas para o AMS Accelerate.	13 de abril de 2023
Atualizado: AMS Resource Scheduler.	Nome de função incorreto AWSManagedServices-DescribeScheduleOrPeriod, corrigido para AWSManagedServices-DescribeScheduleOrPeriods. Consulte Otimização de custos com o AMS Resource Scheduler.	13 de abril de 2023
Atualizado: políticas AWS gerenciadas.	Atualizado Descobertas e respostas personalizadas com instruções para atualizar respostas personalizadas em uma ou várias contas.	13 de abril de 2023
Atualizado: Resource Tagger	Foram adicionados avisos sobre “especificar o nome da sua nova configuração (SampleConfigurationBlock no exemplo fornecido), pois você pode inadvertidamente substituir a configuração gerenciada pelo AMS com o mesmo nome”. Consulte Casos de uso do Resource Tagger no AMS Accelerate.	16 de março de 2023

Alteração	Descrição	Data
Atualizado: Patch RACI	Várias atualizações e esclarecimentos sobre o RACI para aplicação de patches. Consulte Service description (Descrição do serviço).	16 de março de 2023
Atualizado: ações no kit de ferramentas de implantação SLR JSON	Política e ações atualizadas. Consulte: Usando funções vinculadas a serviços para o AMS Accelerate.	16 de março de 2023
Atualizado: remediação automática	Removido o suporte LVM para automação de EC2 volume. Consulte: Remediação automática de alertas pelo AMS.	16 de março de 2023
Atualizado: acelere a integração.	Uso esclarecido de funções, especialmente a função mínima. O modelo para criar funções do AMS	16 de março de 2023
Atualizado: relatórios de autoatendimento.	Os relatórios diários de backup agora oferecem suporte às regiões primária e secundária. Ambos são relatados no campo Região de Recursos deRelatório de backup (diário).	16 de março de 2023
Atualizado: orientação de aplicação de patches	Foi adicionado um aviso para não personalizar as linhas de base de patches padrão, que são gerenciadas pelo AMS. Em vez disso, crie uma nova linha de base de patches personalizada. Veja: Linha de base do patch padrão Linha de base de patch personalizada com o AMS Accelerate e.	16 de março de 2023
Política de rescisão de serviço atualizada.	Definições atualizadas de rescisão do serviço e data de rescisão do serviço emTermos-chave do AMS. Os avisos de rescisão devem ser emitidos até o vigésimo dia do mês anterior ao seu último mês completo.	16 de março de 2023

Alteração	Descrição	Data
Atualizado: políticas AWS gerenciadas.	Nome esclarecido da política:Função vinculada ao serviço de contatos do AMS Accelerate.	16 de fevereiro de 2023
Novo: políticas AWS gerenciadas.	Política adicionada:Função vinculada ao serviço de contatos do AMS Accelerate.	16 de fevereiro de 2023
Atualizado: conformidade de configuração.	Corrigiu uma palavra com erro ortográfico em:. Conformidade de configuração no Accelerate	16 de fevereiro de 2023
Novo conteúdo: Não suportado OSes	Foram adicionadas informações sobre quais serviços o AMS fornece para sistemas operacionais não suportados (OSes), consulteCapacidades para sistemas operacionais sem suporte no Accelerate.	16 de fevereiro de 2023
Atualizado: Crie janelas de patch	Foi adicionado um link para CloudShell usar emCrie uma janela de manutenção com a interface de linha de comando (CLI) do Systems Manager para o AMS Accelerate.	16 de fevereiro de 2023
Conteúdo atualizado: recursos de gerenciamento de integração	Os modelos JSON compactados foram atualizados em. O modelo para criar funções do AMS	16 de fevereiro de 2023
Novo conteúdo: Conformidade de configuração	Adicionou um novo tópico:Descobertas e respostas personalizadas.	16 de fevereiro de 2023
Novo: políticas AWS gerenciadas.	Política adicionada:Função vinculada ao serviço de EventBridge regras da Amazon para o AMS Accelerate.	07 de fevereiro de 2023

Alteração	Descrição	Data
Atualizado: políticas AWS gerenciadas.	Atualizado o `AWSManagedServices DeploymentToolkitPolicy` com novas permissões do S3. Consulte Acelere as atualizações de funções vinculadas a serviços.	30 de janeiro de 2023
Nova região de inscrição: CPT.	O AMS Accelerate agora está disponível na região de opt-in da Cidade do Cabo (CPT). Para se inscrever, consulte Gerenciamento Regiões da AWS.	12 de janeiro de 2023
Atualizado: Descrição do serviço.	FSx Serviços adicionados monitorados por CloudWatch alarmes aoService description (Descrição do serviço).	12 de janeiro de 2023
Atualizado: Monitorando métricas padrão.	Foram adicionados 6 FSx alarmes ao. Alertas do monitoramento de linha de base no AMS	12 de janeiro de 2023
Atualizado: padrões AMS.	Foram adicionadas notificações de alarme personalizadas do Cloudwatch ao. Padrões AMS	12 de janeiro de 2023
Atualizado: recursos de gerenciamento de integração.	Atualizou a tabela de modelos, adicionando uma linha para `ams-onboarding-ssm-execution-role` entradaO modelo para criar funções do AMS.	12 de janeiro de 2023
Atualizado: conformidade de configuração.	Detalhes adicionais para solicitar remediaçõ es personalizadas (na caixa Importante) em. Conformidade de configuração no Accelerate	12 de janeiro de 2023
Atualizado: Service-linked-role permissões.	Permissões antigas ou duplicadas removidas . Consulte Usando funções vinculadas a serviços para o AMS Accelerate.	15 de dez de 2022

Alteração	Descrição	Data
Atualizado: gerenciamento de patches, janelas de manutenção.	Foi adicionada orientação às instruções do console, etapa 5, para criar uma janela de manutenção. Consulte Crie uma janela de manutenção no console do Systems Manager para o AMS Accelerate.	15 de dez de 2022
Novo: seção de gerenciam ento de patches.	Foi adicionada uma seção para as janelas de manutenção do Patch Tuesday. Consulte Crie uma janela de manutenção recorrente “Patch Tuesday” a partir do console AMS (recomend ado).	15 de dez de 2022
Atualizado: AMS Resource Scheduler.	Atualizou o nome da CloudFormation pilha. Consulte Usando recursos com o AMS Resource Scheduler.	15 de dez de 2022
Atualizado: marque seus recursos para backup.	Foi adicionada orientação para o uso do AMS Resource Tagger. Consulte Marque seus recursos para aplicar os planos de backup do AMS.	15 de dez de 2022
Atualizado: selecione um plano de backup.	Indicou quais planos oferecem backup contínuo. Consulte Selecione um plano de backup do AMS.	15 de dez de 2022
Atualizado: AMS Resource Scheduler.	Atualizou o exemplo de AWS CLI para excluir um período ou uma programação. Consulte Trabalhando com períodos e cronogramas no AWS Managed Services Resource Scheduler.	15 de dez de 2022
Atualizado: políticas AWS gerenciadas.	Adicionou `AWSManagedServices DeploymentToolkitPolicy` o. Consulte AWS políticas gerenciadas para o AMS Accelerate.	15 de dez de 2022

Alteração	Descrição	Data
Novo: seção adicionada descrevendo a nova função vinculada ao serviço do AMS,. AWSServiceRoleForManagedServices_DetectiveControlsConfig	GovCloud Regiões e permissões adicionadas. Consulte Detective controla a função vinculada ao serviço do AMS Accelerate.	15 de dez de 2022
Novo: política AWS gerenciada	Foi adicionada uma seção que descreve como a política AWS gerenciada, AWSManagedServices_AlarmManagerPermissionsBoundary, é usada na política de função vinculada ao serviço, AWSManagedServices_AlarmManager _ServiceRolePolicy, para restringir as permissões das funções do IAM criadas pela função vinculada ao serviço. AWSServiceRoleForManagedServices_AlarmManager Consulte AWS políticas gerenciadas para o AMS Accelerate.	15 de dez de 2022
Atualizado: Operações sob demanda.	Ofertas adicionais: SQL Server on EC2 Operations e criação e venda de AMI. Consulte Operações sob demanda.	10 de novembro de 2022
Atualizado: Monitoramento e gerenciamento de eventos.	Explicação atualizada das notificações de serviço e relatórios de incidentes. Consulte Como funciona o monitoramento.	10 de novembro de 2022
Atualizado: regiões de função vinculadas a serviços	GovCloud Regiões e permissões adicionadas. Consulte Usando funções vinculadas a serviços para o AMS Accelerate.	10 de novembro de 2022
Novo: função vinculada ao serviço.	Nova função adicionada:`AWSServiceRoleForAMSDetectiveControls` . Consulte Detective controla a função vinculada ao serviço do AMS Accelerate.	10 de novembro de 2022

Alteração	Descrição	Data
Atualizado: gerenciamento de acesso.	Subseções atualizadas com instruções aprimoradas. Consulte Gerenciamento de acesso no AMS Accelerate.	10 de novembro de 2022
Atualizado: descrição do serviço.	Padrões AMS atualizados na matriz RACI. Consulte Service description (Descrição do serviço).	10 de novembro de 2022
Atualizado: padrões AMS.	Os clientes são responsáveis pelas implantaç ões de padrões. Consulte Padrões AMS.	10 de novembro de 2022
Atualizado: Offboarding.	Detalhes adicionais sobre o que acontece com recursos específicos de Backup e Monitoram ento durante a desativação. Consulte Fora do AMS Accelerate.	10 de novembro de 2022
Atualizado: gerenciamento de patches..	Orientações atualizadas e resumidas sobre as políticas do IAM. Consulte Criação de uma função do IAM para aplicação de patches sob demanda do AMS Accelerate.	10 de novembro de 2022
Novo: links para diagramas de arquitetura.	Links adicionados aos diagramas de arquitetu ra de referência do AMS para vários tópicos. Por exemplo, consulte Monitoramento e gerenciamento de eventos no AMS Accelerate.	10 de novembro de 2022
Novo: oferta de operações sob demanda	Adicionou “Operações do Acelerador da Zona de Aterrissagem”. Consulte Operações sob demanda.	13 de outubro de 2022
Atualização: gerenciamento de monitoramento. Os alertas geram relatórios de incidentes, não solicitações de serviço	Como funciona o monitoramento.	13 de outubro de 2022

Alteração	Descrição	Data
Novo: Criação de uma janela de manutenção de patches com um modelo CFN personalizado do Accelerate	CloudFormation modelos de configuração da janela de patch. Consulte Crie uma janela de manutenção de patches no AMS.	15 de setembro de 2022
Atualizado: Offboarding	Enfatizou que os planos de backup no Accelerate não funcionam mais após a desativação. Consulte Fora do AMS Accelerate.	15 de setembro de 2022
Atualizado: detalhes CloudWatch da alteração de configuração	Corrigido um erro nos exemplos do Windows e do Linux. Consulte CloudWatch detalhes da alteração de configuração.	15 de setembro de 2022
Atualizado: Usando o AMS Resource Scheduler	Foram adicionadas orientações sobre tags de alocação de custos. Consulte Estimador de custos no AMS Resource Scheduler.	15 de setembro de 2022
Atualizado: Biblioteca de regras de configuração do AMS	Foram adicionadas duas regras de `ams-eks-` configuração à Tabela de Regras. Consulte Biblioteca de regras de configuração do AMS.	15 de setembro de 2022
Atualizado: Gerenciamento de backup	O rótulo enganoso PITR (point-in-time-recovery) foi removido dos títulos e descrições dos planos de backup. Consulte Selecione um plano de backup do AMS.	15 de setembro de 2022
Atualizado: Accelerate a descrição do serviço	Descrições atualizadas das regras de configuração e dos canários. Consulte Service description (Descrição do serviço).	15 de setembro de 2022
Atualizado: descrição do serviço, configurações suportadas	end-of-serviceData removida para o Windows 2008 R2. O Accelerate não é compatível com o Windows 2008. Consulte Configurações compatíveis.	11 de agosto de 2022

Alteração	Descrição	Data
Atualizado: Descrição do serviço, funções e responsab ilidades	A tabela RACI foi atualizada. Os registros de acesso do ELB foram removidos da última linha da seção Rede. Não habilitamos registros de acesso do ELB para clientes do Accelerate. Consulte Perfis e responsabilidades.	11 de agosto de 2022
Atualizado: Conformidade de configuração	Corrigido um erro de digitação na coluna Tabela de Regras, Estruturas. O NIST-CSF foi listado incorretamente como NIST-CIS. Consulte Conformidade de configuração no Accelerate.	11 de agosto de 2022
Novo: acelere a desativação	Considerações e processo de desligamento. Consulte Offboarding AMS Accelerate.	11 de agosto de 2022
Atualizado: lista de sistemas operacionais de agentes SSM pré-instalados	Adicionado “Ubuntu Linux 18.04 e 20.04" à lista. Consulte EC2 Instâncias de integração para acelerar.	11 de agosto de 2022
Novo: Agendador de recursos	Use o AMS Resource Scheduler para otimizar os custos interrompendo e iniciando os recursos somente conforme necessário. Consulte Otimização de custos com o AMS Resource Scheduler.	14 de julho de 2022
Atualizado: Descrição do serviço para o Resource Scheduler	Várias seções da descrição do serviço foram atualizadas para a nova oferta do Resource Scheduler. Consulte Service description (Descrição do serviço).	14 de julho de 2022
Novo: Padrões AMS	O AMS oferece modelos de padrões, uma solução generalizada que resolve uma família de casos de uso no ambiente gerenciado do AMS. Primeiro padrão em oferta:Padrões AMS.	14 de julho de 2022

Alteração	Descrição	Data
Novo: nota de otimização de custos	Foi adicionada uma nota explicando como os custos podem aumentar com o uso de recursos. Consulte Inventário de recursos para Accelerate.	14 de julho de 2022
Atualizado: regras de configuração do AMS	Reorganizou as tabelas noBiblioteca de regras de configuração do AMS. A tabela HTML tem menos colunas, para facilitar a leitura rápida. A planilha para download tem colunas adicionais para permitir a classificação e a filtragem.	14 de julho de 2022
Atualizado: Gerenciamento de acesso	Atualizou o CloudFormation modelo de amostra emPermissões para usar os recursos do AMS. A `AMSAccelerateAdminAccess` política agora inclui `AmsResourceSchedulerPassRolePolicy` as `IAMReadOnlyPolicy` políticas e.	14 de julho de 2022
Atualizado: Relatórios de autoatendimento	Foram adicionadas instruções para criptografar AWS Glue metadados com chaves KMS. Veja a caixa chamada Importante em. Relatórios de autoatendimento	14 de julho de 2022
Atualizado: monitoramento de linha de base do AMS	Alerta DeleteRecoveryPoint de backup adicionado. Alertas do monitoramento de linha de base no AMS	14 de julho de 2022
Atualizado: sistemas operacionais compatíveis	Data de fim do suporte adicionada para Amazon Linux 2. Service description (Descrição do serviço)	14 de julho de 2022
Atualizado: Relatórios do AMS	Foi adicionada uma observação sobre as regiões de aceitação. Relatórios e opções	14 de julho de 2022

Alteração	Descrição	Data
Programador de recursos	Foram adicionadas informações sobre a integração e o uso do AMS Resource Scheduler para auxiliar na otimização de custos ao programar os horários de parada e início dos recursos. Além disso, atualizei a descrição do serviço Accelerate para incluir a menção ao Resource Scheduler. Além disso, atualizou a data de fim do suporte suportado pelo Amazon Linux 2 para 2024. Consulte Otimização de custos com o AMS Resource Scheduler e Service description (Descrição do serviço)	30 de junho de 2022
Novo alarme	Adicionou um AWS Backup alarme. Alertas do monitoramento de linha de base no AMS	21 de junho de 2022
Novo conteúdo	Foi adicionado o conteúdo da função vinculada ao serviço. Usando funções vinculadas a serviços para o AMS Accelerate	16 de junho de 2022
	AWS Operações de Firewall de Rede adicionadas ao catálogo de ofertas do Operations on Demand (OOD). Operações sob demanda	16 de junho de 2022
	Foi adicionada a descrição do recurso de gerenciamento de problemas. Service description (Descrição do serviço)	16 de junho de 2022
	Foi adicionada uma observação sobre o conjunto de regras de configuração que não oferece suporte a determinadas regiões opcionais. Conformidade de configuração no Accelerate	16 de junho de 2022

Alteração	Descrição	Data
Conteúdo atualizado	Conformidade de configuração. “Biblioteca de regras de configuração do AMS” -> “Tabela de regras” foi atualizada e removida somente para ZIP. Conformidade de configuração no Accelerate	16 de junho de 2022
	E-mails de escalonamento removidos. Caminho de escalonamento	16 de junho de 2022
	A lista de tópicos foi movida para os parágrafos iniciais abaixo. O que é o AMS Accelerate?	16 de junho de 2022
	Atualizou o conteúdo de remeditação automática. Remediação automática de alertas pelo AMS	16 de junho de 2022
Conteúdo atualizado: Descrição do serviço	O EKS foi adicionado à lista de serviços monitorados pelo AMS Config Rules em. Serviços com suporte Descrição de monitoramento atualizada na tabela RACI emPerfis e responsabilidades.	12 de maio de 2022
Conteúdo atualizado: Conformidade de configuração	Foram adicionadas regras de configuração relacionadas ao EKS. Consulte Conformidade de configuração no Accelerate.	12 de maio de 2022
Conteúdo atualizado: Introdução, Account Discovery	Foi adicionada uma versão mais recente do AwsAccountDiscoveryCli script (no arquivo zip do Account Discovery Changelog) em. Etapa 1. Descoberta de contas no Accelerate	12 de maio de 2022
Conteúdo atualizado: monitoramento, métricas padrão	Condições de gatilho atualizadas para métricas relacionadas ao ALB. Consulte Alertas do monitoramento de linha de base no AMS.	12 de maio de 2022

Alteração	Descrição	Data
Conteúdo atualizado: integração de patches	Foi adicionado um pré-requisito explícito de correção: você precisa se inscrever no EBS. Consulte Integração de patches no Accelerate.	12 de maio de 2022
Conteúdo atualizado: acelere a tabela de inventário de recursos	ams-detective-controls-configRegras de -rules-cdk alteradas, regras adicionadas para ams-detective-controls-recorder -cdk e -cdk. ams-detective-controls-infrastructure Consulte Inventário de recursos para Accelerate.	14 de abril de 2022
Conteúdo atualizado: Conformidade de configuração	Introdução aos padrões do setor, regras de configuração e tipos de respostas. Enfatiza que os clientes não escolhem regras ou respostas de configuração individuais. Conformidade de configuração no Accelerate.	14 de abril de 2022
Conteúdo atualizado: Descrição do serviço	A seção Escopo de mudanças existente foi movida para Funções e responsabilidades. Consulte Perfis e responsabilidades.	14 de abril de 2022
Conteúdo atualizado: Marcação e monitoramento	Adicionado `AWS::Synthetics:Canary` às listas de tipos de recursos permitidos para marcação e monitoramento. Consulte Perfis de configuração do marcador de recursos no AMS Accelerate e Perfil de configuração acelerada: substituição de pseudoparâmetros.	14 de abril de 2022
Conteúdo atualizado: Acelere os pré-requisitos	Foram adicionadas as permissões de bucket exigidas pelo SSM ao. Amazon EC2 Systems Manager em Accelerate	14 de abril de 2022

Alteração	Descrição	Data
Novo conteúdo: Aplicação de patches e monitoramento	Foi adicionado um exemplo de código para usar o Cloudformation para implantar configurações de marcação e monitoramento. Consulte Implantando um perfil de configuração com o CloudFormation for Accelerate e Usando CloudFormation para implantar o Accelerate as alterações de configuração.	10 de março de 2022
Conteúdo atualizado: console de manutenção de patches	Etapas reordenadas Crie uma janela de manutenção no console do Systems Manager para o AMS Accelerate para corresponder à interface do console.	10 de março de 2022
Conteúdo atualizado: CLI de manutenção de patches	Parâmetros CLI atualizados (cronograma, duração e limite) para Crie uma janela de manutenção com a interface de linha de comando (CLI) do Systems Manager para o AMS Accelerate	10 de março de 2022
Novo conteúdo: Auto Instance Config	Definição adicionada `AMSInstanceProfile BasePolicy` de Detalhes da alteração de permissões do IAM	10 de março de 2022
Novo conteúdo: Integração	Foi adicionado um exemplo de comando Linux ao Conectividade de saída com a Internet no Accelerate	10 de março de 2022
Novo conteúdo: Integração	Foi adicionada uma opção de privilégio mínimo ao. O modelo para criar funções do AMS	10 de março de 2022
Conteúdo atualizado: acelere as instruções de escalonamento	Orientações, links e contatos de e-mail adicionados ao Caminho de escalonamento	10 de março de 2022

Alteração	Descrição	Data
Conteúdo atualizado: configurações suportadas	A AMS espera encerrar o suporte para o RHEL 6 e CentOs em 14 de março de 2023. Consulte Configurações compatíveis	10 de março de 2022
Conteúdo atualizado: tabela de recursos	Funções do IAM de acesso ao AMS adicionadas à tabela de Inventário de recursos para Accelerate recursos	10 de março de 2022
Conteúdo atualizado: Integração e Backup	Instruções adicionadas para optar por AWS Backup e Integração no AWS Backup Accelerate e Gerenciamento de continuidade no AMS Accelerate	10 de março de 2022
Conteúdo atualizado: Gerenciamento de acesso	As instruções específicas avançadas foram removidas da orientação do Accelerate. Como e quando usar a conta de usuário raiz no AMS	10 de março de 2022
Conteúdo atualizado: configurações suportadas	O AMS agora oferece suporte ao Oracle Linux 8.3 e ao Ubuntu 18.04 e 20.04. Consulte Configurações compatíveis.	28 de fevereiro de 2022
Conteúdo atualizado: Acordo de nível de serviço	Atualizou o Acordo de Nível de Serviço disponível para download emServiços com suporte.	28 de fevereiro de 2022
Conteúdo atualizado: Gerenciamento de acesso	Atualizado Como o AMS acessa sua conta com FAQs as funções do console do operador do AMS e um aviso para não modificá-las ou excluí-las.	28 de fevereiro de 2022
Conteúdo atualizado: Gerenciador de alarmes	Atualizado Perfil de configuração acelerada: monitoramento. O Gerenciador de alarmes não está mais limitado a alarmes de métrica única.	28 de fevereiro de 2022

Alteração	Descrição	Data
Conteúdo atualizado: Primeiros passos	Atualizado Etapa 2. Recursos de gerenciamento de integração no Accelerate. Foi adicionada a uma função do IAM com acesso mínimo aos recursos de integração.	28 de fevereiro de 2022
Novo conteúdo: Escopo das mudanças na descrição do serviço	Foi adicionada uma nova seção, Escopo das mudanças realizadas pelo AMS Accelerate que enfatiza limites e ações que o AMS Accelerate não executa.	10 de fevereiro de 2022
Conteúdo atualizado: Primeiros passos	O novo processo de integração começa com a definição dos recursos e configurações padrão antes da personalização. As subseções contêm metas específicas do recurso e links relacionados. Consulte Introdução ao AMS Accelerate.	10 de fevereiro de 2022
Conteúdo atualizado: AMS Backup Management.	Reduziu e reorganizou o Gerenciamento de continuidade no AMS Accelerate capítulo para facilitar a leitura.	10 de fevereiro de 2022
Conteúdo atualizado: Marcação	Foi adicionada uma seção Ferramentas de marcação para acomodar exemplos de código CloudFormation e outras ferramentas. Consulte Marcação no AMS Accelerate.	10 de fevereiro de 2022
Conteúdo atualizado: Monitoramento de linha de base	A condição de gatilho aprimorada para o alarme de RedShift cluster reduz os alarmes falsos durante a manutenção. Consulte Alertas do monitoramento de linha de base no AMS.	10 de fevereiro de 2022
Conteúdo atualizado: Patching	Exemplo de comando CLI atualizado para registrar uma janela de manutenção. Consulte Crie uma janela de manutenção com a interface de linha de comando (CLI) do Systems Manager para o AMS Accelerate.	10 de fevereiro de 2022

Alteração	Descrição	Data
Conteúdo atualizado: AWS Config Rules Inventory.	Removida a regra de configuração obsoleta da tabela Config `ams-nist-cis-ec2-security-group-attached-to-eni` Rules AWS Inventory. Consulte Tabela de regras.	27 de janeiro de 2022
Novo conteúdo: Criação de janelas de manutenção de patches.	Foi adicionado um link para o tutorial do SSM e exemplos de comandos para criar janelas de manutenção de patches a partir da linha de comando. Consulte Crie uma janela de manutenção com a interface de linha de comando (CLI) do Systems Manager para o AMS Accelerate.	27 de janeiro de 2022
Novo conteúdo: o Resource Tagger reconhece o novo tipo de recurso do Auto Scaling Groups (ASG).	Foram adicionados grupos de Auto Scaling aos tipos de recursos filtráveis com os perfis de configuração do Resource Tagger. Consulte Sintaxe e estrutura.	13 de janeiro de 2022
Novo conteúdo: planos de backup e cofres adicionais.	Foram adicionados novos planos de backup e cofres para mitigar cenários de alto risco, incluindo ataques de ransomware. Consulte Exibir backups em cofres do AMS e Exibir backups em cofres do 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.