aws

Guia do usuário

# DevOps Guru da Amazon

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

# DevOps Guru da Amazon: Guia do usuário

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

# Table of Contents

O que é o Amazon DevOps Guru? ..... 1
Como funciona o DevOps Guru? ..... 1
Fluxo de trabalho de alto nível do DevOps Guru ..... 2
Fluxo de trabalho detalhado DevOps do Guru ..... 4
Como faço para começar? ..... 5
Como faço para parar de incorrer em cobranças de DevOps Guru? ..... 5
Conceitos ..... 6
Anomalia ..... 6
Insight ..... 6
Métricas e eventos operacionais ..... 7
Grupos de logs e anomalias de log ..... 7
Recomendações ..... 8
Cobertura ..... 8
Lista de cobertura de serviços ..... 10
Configuração ..... 12
Cadastre-se para AWS ..... 12
Inscreva-se para um Conta da AWS ..... 12
Criar um usuário com acesso administrativo ..... 13
Determine a cobertura para o DevOps Guru ..... 14
Identifique seu tópico de notificações ..... 15
Permissões adicionadas ao seu tópico ..... 16
Estimar seu custo ..... 17
Conceitos básicos ..... 19
Etapa 1: configurar ..... 19
Etapa 2: Habilitar o DevOps Guru ..... 19
Monitorar contas em toda a sua organização ..... 19
Monitorar sua conta atual ..... 21
Etapa 3: Especifique sua cobertura de recursos do DevOps Guru ..... 22
Habilitando AWS serviços para análise do DevOps Guru ..... 25
Trabalhar com insights ..... 26
Visualizar insights ..... 26
Entendendo os insights no console do DevOps Guru ..... 27
Entender como comportamentos anômalos são agrupados em insights ..... 30
Entender as gravidades do insight ..... 31

Banco de dados de monitoramento ..... 32
Bancos de dados relacionais ..... 32
Monitoramento de operações de banco de dados no Amazon RDS ..... 32
Monitorando operações de banco de dados em Amazon Redshift ..... 34
Trabalhando com anomalias no DevOps Guru for RDS ..... 36
Bancos de dados não relacionais ..... 56
Monitorando operações de banco de dados em Amazon DynamoDB ..... 56
Monitorando operações de banco de dados em Amazon ElastiCache ..... 57
Integração com o Profiler CodeGuru ..... 58
Definir aplicativos usando recursos do AWS ..... 59
Usar tags para identificar recursos em seus aplicativos ..... 60
O que é uma tag? ..... 61
Definir um aplicativo usando uma tag ..... 61
Usando tags com o DevOps Guru ..... 62
Adicionar tags aos recursos ..... 63
Usando pilhas para identificar recursos em seus aplicativos DevOps Guru ..... 63
Escolher pilhas para analisar ..... 64
Trabalhando com EventBridge ..... 66
Eventos para DevOps Guru ..... 66
DevOpsGuruNovo evento aberto do Insight ..... 66
Padrão de evento de amostra personalizado para o novo Insight de alta gravidade ..... 68
Atualizar as configurações ..... 69
Atualizar sua conta de gerenciamento ..... 69
Atualizando sua cobertura AWS de análise ..... 69
Atualizar suas notificações ..... 70
Navegue até as configurações de notificação no console do DevOps Guru ..... 71
Adicionar tópicos de notificação do Amazon SNS ..... 71
Remover tópicos de notificação do Amazon SNS ..... 72
Atualizar as configurações de notificação do Amazon SNS ..... 72
Permissões adicionadas ao seu tópico ..... 73
Filtrar suas notificações ..... 74
Filtrar notificações com uma política de filtro de assinaturas do Amazon SNS ..... 74
Exemplo de notificação filtrada do Amazon SNS ..... 75
Atualizar a integração do Systems Manager ..... 76
Atualizar a detecção de anomalias do log ..... 77
Atualizar a criptografia ..... 77

Visualizar notificações ... 79
Novo insight ... 79
Insight fechado ... 80
Nova associação ... 82
Nova recomendação ... 83
Gravidade atualizada ... 84
Falha na validação de recursos ... 85
Visualizar recursos analisados ... 87
Atualizando sua cobertura AWS de análise ... 87
Remover a visualização de recursos analisados para usuários ... 89
Práticas recomendadas ... 90
Segurança ... 91
Proteção de dados ... 92
Criptografia de dados ... 93
Como o DevOps Guru usa subsídios em AWS KMS ... 94
Monitorando suas chaves de criptografia no DevOps Guru ... 95
Criar uma chave gerenciada pelo cliente ... 95
Privacidade do tráfego ... 97
Gerenciamento de Identidade e Acesso ... 97
Público ... 98
Autenticação com identidades ... 98
Gerenciar o acesso usando políticas ... 102
Atualizações da política ... 105
Como o Amazon DevOps Guru funciona com o IAM ... 110
Políticas baseadas em identidade ... 117
Uso de perfis vinculados ao serviço ... 130
DevOpsReferência de permissões do Guru ... 136
permissões para os tópicos do Amazon SNS ... 140
Permissões para tópicos do Amazon SNS criptografados ... 146
Solução de problemas ... 146
DevOpsGuru do monitoramento ... 151
Monitoramento com CloudWatch ... 151
Registrando chamadas de API do DevOps Guru com AWS CloudTrail ... 154
Endpoints da VPC (AWS PrivateLink) ... 157
Considerações sobre os endpoints DevOps Guru VPC ... 157
Criação de uma interface VPC endpoint para o Guru DevOps ... 158

Criação de uma política de VPC endpoint para o Guru DevOps ..... 158
Segurança da infraestrutura ..... 159
Resiliência ..... 159
Cotas e limites ..... 161
Notificações ..... 161
AWS CloudFormation pilhas ..... 161
DevOpsLimites de monitoramento de recursos do Guru ..... 161
DevOpsCotas do Guru para criar, implantar e gerenciar uma API ..... 162
Histórico de documentos ..... 163
AWS Glossário ..... 170
..... clxxi

# O que é o Amazon DevOps Guru?

Bem-vindo ao guia do usuário do Amazon DevOps Guru.

DevOpsO Guru é um serviço de operações totalmente gerenciado que facilita que desenvolvedores e operadores melhorem o desempenho e a disponibilidade de seus aplicativos. DevOpsO Guru permite que você descarregue as tarefas administrativas associadas à identificação de problemas operacionais para que você possa implementar rapidamente recomendações para melhorar seu aplicativo. DevOpsO Guru cria insights reativos que você pode usar para melhorar seu aplicativo agora. Ele também cria insights proativos para ajudá-lo a evitar problemas operacionais que possam afetar seu aplicativo no futuro.

DevOpsO Guru aplica o aprendizado de máquina para analisar seus dados operacionais e métricas e eventos de aplicativos para identificar comportamentos que se desviam dos padrões operacionais normais. Você é notificado quando o DevOps Guru detecta um problema ou risco operacional. Para cada problema, o DevOps Guru apresenta recomendações inteligentes para abordar problemas operacionais atuais e futuros previstos.

Para começar, consulte o Como faço para começar a usar o DevOps Guru?.

## Como funciona o DevOps Guru?

O fluxo de trabalho do DevOps Guru começa quando você configura sua cobertura e notificações. Depois de configurar o DevOps Guru, ele começa a analisar seus dados operacionais. Quando detecta um comportamento anômalo, ele cria um insight que contém recomendações e listas de indicadores, grupos de logs e eventos relacionados ao problema. Para cada insight, o DevOps Guru notifica você. Se você habilitou AWS Systems Manager OpsCenter, um OpsItem será criado para que você possa usar o Systems Manager OpsCenter para rastrear e gerenciar o tratamento de seus insights. Cada insight contém recomendações, indicadores, grupos de logs e eventos relacionados a comportamentos anômalos. Use as informações do insight para ajudá-lo a entender e lidar com o comportamento anômalo.

Consulte Fluxo de trabalho de alto nível do DevOps Guru para obter mais detalhes sobre as três etapas de alto nível do fluxo de trabalho. Veja Fluxo de trabalho detalhado DevOps do Guru para saber mais sobre o fluxo de trabalho mais detalhado do DevOps Guru, incluindo como ele interage com outros AWS serviços.

Tópicos

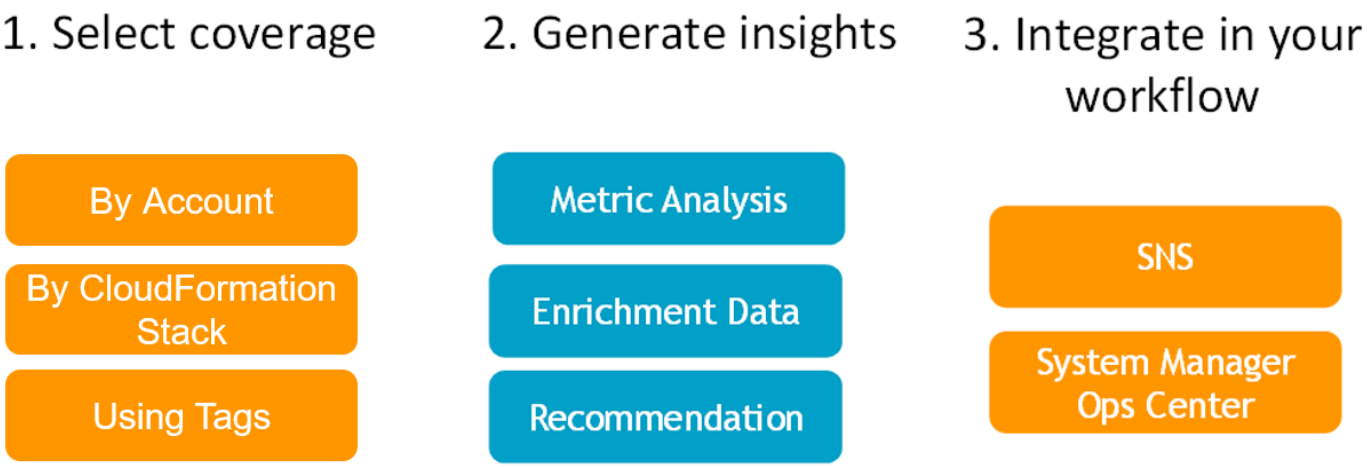
- Fluxo de trabalho de alto nível do DevOps Guru
- Fluxo de trabalho detalhado DevOps do Guru


## Fluxo de trabalho de alto nível do DevOps Guru

O fluxo de trabalho do Amazon DevOps Guru pode ser dividido em três etapas de alto nível.

1. Especifique a cobertura do DevOps Guru informando quais AWS recursos em sua AWS conta você deseja que ele analise.
2. DevOpsO Guru começa a analisar CloudWatch as AWS CloudTrail métricas e outros dados operacionais da Amazon para identificar problemas que você pode corrigir para melhorar suas operações.
3. DevOpsO Guru garante que você conheça insights e informações importantes enviando uma notificação para cada evento importante do DevOps Guru.

Você também pode configurar o DevOps Guru para criar um OpsItem in AWS Systems Manager OpsCenter para ajudá-lo a monitorar seus insights. O diagrama a seguir mostra esse fluxo de trabalho.



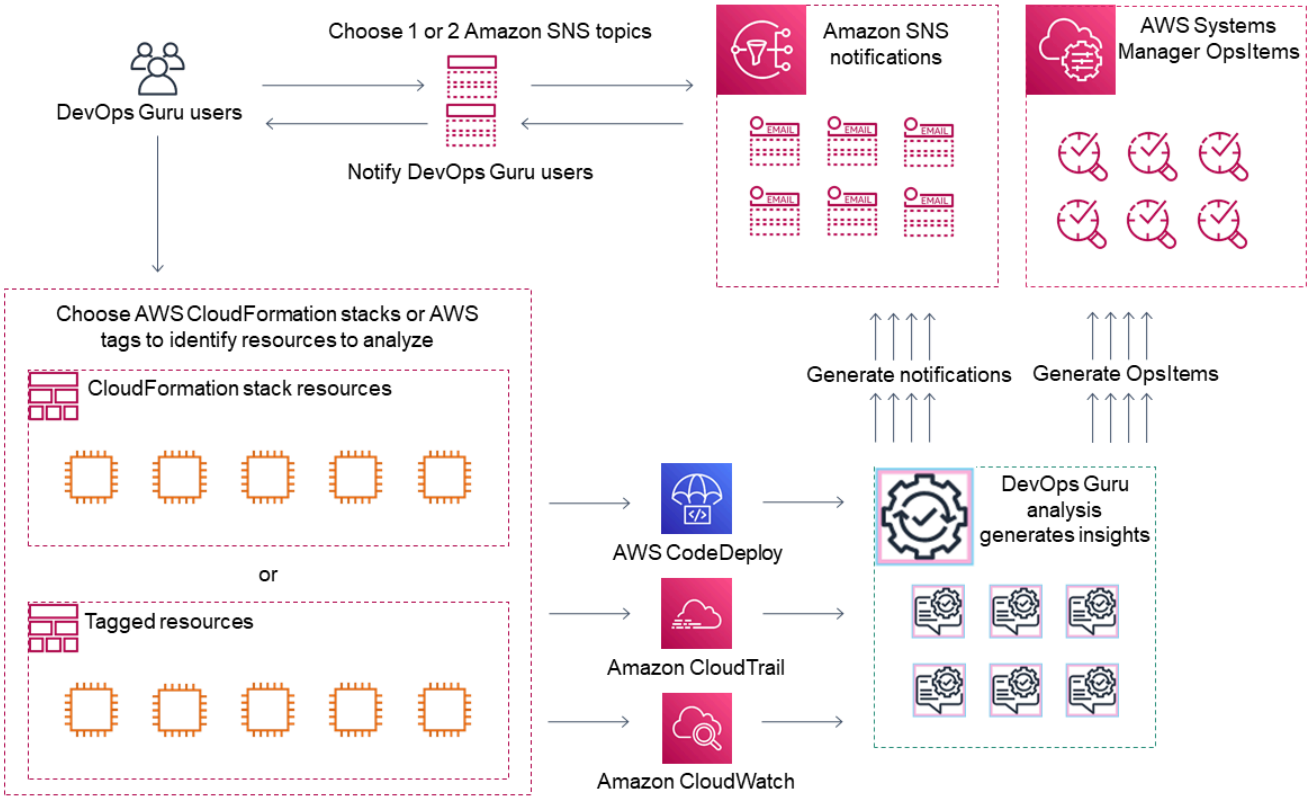

1. Na primeira etapa, você escolhe sua cobertura especificando quais AWS recursos em sua AWS conta serão analisados. DevOpsO Guru pode cobrir ou analisar todos os recursos em uma AWS conta, ou você pode usar AWS CloudFormation pilhas ou AWS tags para especificar um subconjunto dos recursos em sua conta para análise. Certifique-se de que os recursos que você especifica compõem seus aplicativos, cargas de trabalho e microsserviços essenciais para seus

negócios. Para obter mais informações sobre os serviços e recursos suportados, consulte os preços do Amazon DevOps Guru.

2. Na segunda etapa, o DevOps Guru analisa os recursos para gerar insights. Esse é um processo contínuo. Você pode ver os insights e ver as recomendações e informações relacionadas que eles contêm no console do DevOps Guru. DevOps O Guru analisa os dados a seguir para encontrar problemas e criar insights.
   - CloudWatch Métricas individuais da Amazon emitidas por seus AWS recursos. Quando um problema é identificado, o DevOps Guru reúne essas métricas.
   - Registre anomalias dos grupos de CloudWatch registros da Amazon. Se você ativar a detecção de anomalias de log, o DevOps Guru exibirá anomalias de log relacionadas quando ocorrer um problema.
   - DevOpsO Guru extrai dados de enriquecimento dos registros de AWS CloudTrail gerenciamento para encontrar eventos relacionados às métricas coletadas. Os eventos podem ser de implantação de recursos e alterações de configuração.
   - Se você usa AWS CodeDeploy, o DevOps Guru analisa os eventos de implantação para ajudar a gerar insights. Eventos para todos os tipos de CodeDeploy implantações (servidor local, EC2 servidor Amazon, Lambda ou Amazon EC2) são analisados.
   - Quando o DevOps Guru encontra um padrão específico, ele gera uma ou mais recomendações para ajudar a mitigar ou corrigir o problema identificado. As recomendações são coletadas em um único insight. O insight também contém uma lista de indicadores e eventos relacionados ao problema. Você usa os dados do insight para abordar e entender o problema identificado.
3. Na terceira etapa, o DevOps Guru integra a notificação de insights em seu fluxo de trabalho para ajudá-lo a gerenciar problemas e resolvê-los rapidamente.
   - Os insights gerados em sua AWS conta são publicados no tópico Amazon Simple Notification Service (Amazon SNS) escolhido DevOps durante a configuração do Guru. Assim, você é notificado assim que um insight é criado. Para obter mais informações, consulte Atualizando suas notificações no DevOps Guru.
   - Se você ativou AWS Systems Manager durante a configuração do DevOps Guru, cada insight cria um correspondente OpsItem para ajudá-lo a rastrear e gerenciar os problemas descobertos. Para obter mais informações, consulte Atualizando AWS Systems Manager a integração no DevOps Guru.

# Fluxo de trabalho detalhado DevOps do Guru

O fluxo de trabalho do DevOps Guru se integra a vários AWS serviços, incluindo Amazon CloudWatch, AWS CloudTrail Amazon Simple Notification Service e. AWS Systems Manager O diagrama a seguir mostra um fluxo de trabalho detalhado que inclui como ele funciona com outros AWS serviços.




Este diagrama mostra um cenário no qual a cobertura do DevOps Guru é especificada pelos AWS recursos definidos em AWS CloudFormation pilhas ou usando AWS tags. Se nenhuma pilha ou etiqueta for escolhida, a cobertura do DevOps Guru analisa todos os AWS recursos em sua conta. Para ter mais informações, consulte Definir aplicativos usando recursos do AWS e Determine a cobertura para o DevOps Guru.

1. Durante a configuração, você especifica um ou dois tópicos do Amazon SNS que são usados para notificá-lo sobre eventos importantes do DevOps Guru, como quando um insight é criado. Em seguida, você pode especificar AWS CloudFormation pilhas que definem os recursos que você deseja analisar. Você também pode ativar o Systems Manager para gerar um OpsItem para cada insight para ajudá-lo a gerenciar seus insights.
2. Depois que o DevOps Guru é configurado, ele começa a analisar CloudWatch métricas, grupos de registros e eventos que são emitidos de seus recursos e AWS CloudTrail dados relacionados

às CloudWatch métricas. Se suas operações incluem CodeDeploy implantações, o DevOps Guru também analisa os eventos de implantação.

DevOpsO Guru cria insights quando identifica comportamentos incomuns e anômalos nos dados analisados. Cada insight contém uma ou mais recomendações, uma lista dos indicadores usados para gerar o insight, uma lista de grupos de logs relacionados e uma lista dos eventos usados para gerar o insight. Use essas informações para resolver o problema identificado.

3. Depois que cada insight é criado, o DevOps Guru envia uma notificação usando o tópico ou tópicos do Amazon SNS especificados DevOps durante a configuração do Guru. Se você habilitou o DevOps Guru para gerar um OpsItem no Systems Manager OpsCenter, cada insight também acionará um novo Systems Manager. OpsItem Você pode usar o Systems Manager para gerenciar sua visão OpsItems.

## Como faço para começar a usar o DevOps Guru?

É recomendável que você realize as etapas a seguir:

1. Saiba mais sobre o DevOps Guru lendo as informações em DevOpsConceitos de guru.
2. Configure sua AWS conta AWS CLI, o e um usuário administrativo seguindo as etapas emConfigurando o Amazon DevOps Guru.
3. Use o DevOps Guru, seguindo as instruções emComeçando com o DevOps Guru.

## Como faço para parar de incorrer em cobranças de DevOps Guru?

Para desativar o Amazon DevOps Guru para que ele pare de incorrer em cobranças pela análise de recursos em sua AWS conta e região, atualize suas configurações de cobertura para que ele não analise os recursos. Para fazer isso, siga as etapas em Atualizando sua cobertura AWS de análise no DevOps Guru e escolha Nenhum na etapa 4. Você deve fazer isso para cada AWS conta e região em que o DevOps Guru analisa os recursos.

> **Note**
>
> Se você atualizar sua cobertura para parar de analisar recursos, poderá continuar incorrendo em pequenas cobranças se analisar os insights existentes gerados pelo DevOps Guru no passado. Essas cobranças estão associadas às chamadas de API usadas para recuperar e

exibir informações de insights. Para obter mais informações, consulte os preços do Amazon DevOps Guru.

# DevOpsConceitos de guru

Os conceitos a seguir são importantes para entender como o Amazon DevOps Guru funciona.

Tópicos


- Anomalia
- Insight
- Métricas e eventos operacionais
- Grupos de logs e anomalias de log
- Recomendações


## Anomalia

Uma anomalia representa uma ou mais métricas relacionadas detectadas pelo DevOps Guru que são inesperadas ou incomuns. DevOpsO Guru gera anomalias usando o aprendizado de máquina para analisar métricas e dados operacionais relacionados aos seus recursos. AWS Você especifica os AWS recursos que deseja analisar ao configurar o Amazon DevOps Guru. Para obter mais informações, consulte Configurando o Amazon DevOps Guru.

## Insight

Um insight é uma coleção de anomalias criadas durante a análise dos AWS recursos que você especifica ao configurar DevOps o Guru. Cada insight contém observações, recomendações e dados analíticos que você pode usar para melhorar seu desempenho operacional. Existem dois tipos de insight:

- Reativo: um insight reativo identifica um comportamento anômalo quando ele ocorre. Contém anomalias com recomendações, métricas relacionadas e eventos para ajudar você a entender e resolver os problemas agora.
- Proativo: um insight proativo informa você sobre um comportamento anômalo antes que ele ocorra. Contém anomalias com recomendações para ajudar você a resolver os problemas antes de quando estão previstos para acontecer.

## Métricas e eventos operacionais

As anomalias que compõem um insight são geradas pela análise das métricas retornadas pela Amazon CloudWatch e dos eventos operacionais emitidos por seus recursos. AWS Você pode visualizar as métricas e os eventos operacionais que criam um insight para ajudar você a entender melhor os problemas em seu aplicativo.

## Grupos de logs e anomalias de log

Quando você ativa a detecção de anomalias no registro, os grupos de registros relevantes são exibidos nas páginas do DevOps Guru Insight no console do DevOps Guru. Um grupo de logs permite que você tome conhecimento de informações críticas de diagnóstico sobre o desempenho e o acesso de um recurso.

Uma anomalia de log representa um cluster de eventos de log anômalos semelhantes encontrados em um grupo de logs. Exemplos de eventos de log anômalos que podem ser exibidos no DevOps Guru incluem anomalias de palavras-chave, anomalias de formato, anomalias de código HTTP e muito mais.

Você pode usar anomalias de log para diagnosticar a causa raiz de um problema operacional. DevOpsO Guru também faz referência às linhas de registro nas recomendações de insights para fornecer mais contexto para as soluções recomendadas.

> **Note**
>
> DevOpsO Guru trabalha com a Amazon CloudWatch para permitir a detecção de anomalias de log. Quando você ativa a detecção de anomalias de log, o DevOps Guru adiciona tags aos seus grupos de CloudWatch registros. Quando você desativa a detecção de anomalias nos registros, o DevOps Guru remove as tags dos seus grupos de CloudWatch registros. Além disso, os administradores devem garantir que somente usuários com permissões para visualizar CloudWatch registros tenham permissões para visualizar registros CloudWatch anômalos. Recomendamos usar as políticas do IAM para permitir ou negar acesso à operação do `ListAnomalousLogs`. Para obter mais informações, consulte Identity and Access Management for DevOps Guru.

## Recomendações

Cada insight fornece recomendações com sugestões para ajudar você a melhorar o desempenho do seu aplicativo. A recomendação inclui:

- Uma descrição das ações de recomendação para lidar com as anomalias que compõem o insight.
- Uma lista das métricas analisadas nas quais o DevOps Guru encontrou um comportamento anômalo. Cada métrica inclui o nome da AWS CloudFormation pilha que gerou o recurso associado às métricas, o nome do recurso e o nome do AWS serviço associado ao recurso.
- Uma lista dos eventos relacionados às métricas anômalas associadas ao insight. Cada evento relacionado contém o nome da AWS CloudFormation pilha que gerou o recurso associado ao evento, o nome do recurso que gerou o evento e o nome do AWS serviço associado ao evento.
- Uma lista dos grupos de logs relacionados aos comportamentos anômalos associados ao insight. Cada grupo de log contém um exemplo de mensagem de log, informações sobre os tipos de anomalias de log relatadas, os horários em que as anomalias de log ocorreram e um link para ver as linhas de log. CloudWatch

# DevOpsCobertura do Guru

DevOpsO Guru aborda e cria insights para vários AWS serviços diferentes. Para cada serviço para o qual o DevOps Guru cria insights, o DevOps Guru exibe uma variedade de métricas analisadas e insights gerados.

Exemplo de caso de uso para insights reativos:

| Nome do serviço | Caso de uso | Exemplos | Métricas |
| --- | --- | --- | --- |
| AWS Lambda | Detecte anomalias na latência ou duração das funções do Lambda resultantes de várias causas-raiz, como inícios a frio, aumento de solicitações, controle de utilização downstrea | Implantação de código: a Amazon API Gateway latência é afetada por um aumento na latência do Lambda após uma recente implantação do código Lambda. Controle de utilizaçã | Duração<br><br>Controles de utilização |

| Nome do serviço | Caso de uso | Exemplos | Métricas |
| --- | --- | --- | --- |
| | m ou implantações de código. Recomenda formas de mitigar rapidamente. | o downstream: o operador reduziu a capacidade nas unidades de leitura do DynamoDB, causando um aumento nas novas tentativas. Isso resulta em controle de utilização. Início a frio: a função do Lambda está subprovisionada, portanto o Lambda leva mais tempo quando as solicitaç ões são feitas. | |

Exemplo de caso de uso para insights proativos:

| Nome do serviço | Caso de uso | Métricas |
| --- | --- | --- |
| Amazon DynamoDB | A capacidade consumida de leitura da tabela do DynamoDB corre o risco de atingir o limite da tabela. Ação recomendada: se você estiver usando o modo de capacidade provisionada, use o ajuste de escala automátic o para gerenciar ativamente a capacidade de throughpu t para tabelas ou comprar com antecedência capacidade reservada para tabelas. Mude | ConsumedReadCapacityUnits |

| Nome do serviço | Caso de uso | Métricas |
| --- | --- | --- |
| | para o modo de capacidade sob demanda para pagar pela solicitação de leitura; somente será cobrado o que for usado. Tempo de detecção: 6 dias | |

## Lista de cobertura de serviços

Para alguns serviços, o DevOps Guru cria insights reativos. Um insight reativo identifica um comportamento anômalo quando ele ocorre. Contém anomalias com recomendações, métricas relacionadas e eventos para ajudar você a entender e resolver os problemas agora.

Para alguns serviços, o DevOps Guru cria insights proativos. Um insight proativo informa sobre um comportamento problemático antes que ele ocorra. Contém anomalias com recomendações para ajudar você a resolver os problemas antes de quando estão previstos para acontecer.

DevOpsO Guru cria insights reativos para serviços como os seguintes:

- Amazon API Gateway
- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2

> **Note**
>
> DevOpsO monitoramento do Guru está no nível do grupo do Auto Scaling, e não no nível de uma única instância.

- Amazon ECS
- Amazon EKS
- AWS Elastic Beanstalk
- Elastic Load Balancing
- Amazon Kinesis
- AWS Lambda

- Amazon OpenSearch Service
- Amazon RDS
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- Amazon SageMaker AI
- AWS Step Functions
- Amazon SNS
- Amazon SQS
- Amazon SWF
- Amazon VPC

DevOpsO Guru cria insights proativos para serviços como os seguintes:

- Amazon DynamoDB
- Amazon Kinesis
- AWS Lambda
- Amazon RDS
- Amazon SQS

# Configurando o Amazon DevOps Guru

Conclua as tarefas nesta seção para configurar o Amazon DevOps Guru pela primeira vez. Se você já tem uma AWS conta, sabe qual AWS conta ou contas deseja analisar e tem um tópico do Amazon Simple Notification Service para usar nas notificações de insights, você pode pular paraComeçando com o DevOps Guru.

Opcionalmente, você pode usar a Configuração Rápida, um recurso do AWS Systems Manager, para configurar o DevOps Guru e configurar rapidamente suas opções. Você pode usar a Configuração rápida para configurar o DevOps Guru para uma conta independente ou uma organização. Para usar a Configuração Rápida no Systems Manager para configurar o DevOps Guru para uma organização, você deve ter os seguintes pré-requisitos em vigor:

- Uma organização com AWS Organizations. Para obter mais informações, consulte terminology and concepts AWS Organizations (Terminologia e conceitos) no Guia do usuário do AWS Organizations .
- Duas ou mais unidades organizacionais (OUs).
- Uma ou mais AWS contas de destino em cada OU.
- Uma conta de administrador com privilégios para gerenciar as contas de destino.

Para saber como configurar o DevOps Guru usando a Configuração Rápida, consulte Configurar o DevOps Guru com a Configuração Rápida no Guia do AWS Systems Manager Usuário.

Use as etapas a seguir para configurar o DevOps Guru sem a Configuração rápida.

- Etapa 1 — Inscreva-se no AWS
- Etapa 2 — Determinar a cobertura para o DevOps Guru
- Etapa 3: identifique seu tópico de notificações do Amazon SNS

## Etapa 1 — Inscreva-se no AWS

### Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

## Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

Para obter instruções, consulte Habilitar o AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center .

# Etapa 2 — Determinar a cobertura para o DevOps Guru

Sua cobertura de limites determina os AWS recursos que são analisados pelo Amazon DevOps Guru em busca de comportamento anômalo. Recomendamos que você agrupe seus atributos em seus aplicativos operacionais. Todos os atributos em seu limite de atributos devem incluir um ou mais dos seus aplicativos. Se você tiver uma solução operacional, então seu limite de cobertura deve incluir todos os recursos dela. Se você tiver vários aplicativos, escolha os recursos que compõem cada solução e agrupe-os usando AWS CloudFormation pilhas ou AWS tags. Todos os recursos

combinados que você especifica, independentemente de definirem um ou mais aplicativos, são analisados pelo DevOps Guru e compõem seu limite de cobertura.

Use um dos métodos a seguir para especificar os recursos em suas soluções operacionais.

- Escolha que sua AWS região e sua conta definam seu limite de cobertura. Com essa opção, o DevOps Guru analisa todos os recursos em sua conta e região. É uma boa opção para escolher se você usa a conta para apenas um aplicativo.
- Use AWS CloudFormation pilhas para definir os recursos em seu aplicativo operacional. AWS CloudFormation os modelos definem e geram seus recursos para você. Especifique as pilhas que criam os recursos do seu aplicativo ao configurar o DevOps Guru. É possível atualizar suas pilhas a qualquer momento. Todos os recursos nas pilhas que você escolher definem sua cobertura limite. Para obter mais informações, consulte Usando AWS CloudFormation pilhas para identificar recursos em seus aplicativos DevOps Guru.
- Use AWS tags para especificar AWS recursos em seus aplicativos. DevOpsO Guru analisa somente os recursos que contêm as tags que você escolhe. Esses recursos formam seu limite.

  Uma AWS tag consiste em uma chave de tag e um valor de tag. Você pode especificar uma chave de tag e um ou mais valores com essa chave. Use um valor para todos os recursos em um dos seus aplicativos. Se você tiver vários aplicativos, use uma tag com a mesma chave para todos eles e agrupe os recursos em seus aplicativos usando os valores das tags. Todos os recursos com as tags que você escolhe compõem o limite de cobertura do DevOps Guru. Para obter mais informações, consulte Usando tags para identificar recursos em seus aplicativos DevOps Guru.

Se a cobertura de limites incluir recursos que compõem mais de um aplicativo, você pode usar tags para filtrar os insights e visualizá-los em um aplicativo por vez. Para obter mais informações, consulte a Etapa 4 em Visualizando os DevOps insights do Guru.

Para obter mais informações, consulte Definir aplicativos usando recursos do AWS. Para obter mais informações sobre os serviços e recursos suportados, consulte os preços do Amazon DevOps Guru.

## Etapa 3: identifique seu tópico de notificações do Amazon SNS

Você usa um ou dois tópicos do Amazon SNS para gerar notificações sobre eventos importantes do DevOps Guru, como quando um insight é criado. Isso garante que você conheça os problemas que o DevOps Guru encontra o mais rápido possível. Tenha seus tópicos prontos ao configurar o DevOps Guru. Ao usar o console do DevOps Guru para configurar o DevOps Guru, você especifica

um tópico de notificação usando seu nome ou seu Amazon Resource Name (ARN). Para obter mais informações, consulte Enable DevOps Guru. Você pode usar o console do Amazon SNS para visualizar o nome e o ARN de cada um dos seus tópicos. Se você não tiver um tópico, poderá criar um ao habilitar o DevOps Guru usando o console do DevOps Guru. Para obter mais informações, consulte Creating a topic (Criar um tópico) no Guia do desenvolvedor do Amazon Simple Notification Service.

## Permissões adicionadas ao seu tópico do Amazon SNS

Um tópico do Amazon SNS é um recurso que contém uma política de recursos AWS Identity and Access Management (IAM). Quando você especifica um tópico aqui, o DevOps Guru acrescenta as seguintes permissões à sua política de recursos.

```
{
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
    }
  }
}
```

Essas permissões são necessárias para que o DevOps Guru publique notificações usando um tópico. Se você preferir não ter essas permissões no tópico, você pode removê-las com segurança e o tópico continuará funcionando como antes de você escolhê-lo. No entanto, se essas permissões anexadas forem removidas, o DevOps Guru não poderá usar o tópico para gerar notificações.

# Estimando os custos de análise de recursos do Amazon DevOps Guru

Você pode estimar seu custo mensal para que o Amazon DevOps Guru analise seus recursos da AWS. Você paga pelo número de horas analisadas para cada recurso ativo da AWS em sua cobertura de recursos especificada. Um recurso só estará ativo se produzir indicadores, eventos ou entradas de log em uma hora.

DevOps O Guru examina seus recursos selecionados para criar uma estimativa de custo mensal. Você pode ver os recursos, o preço faturável por hora e a cobrança mensal estimada. O estimador de custos pressupõe como padrão que os recursos ativos analisados sejam utilizados 100 por cento do tempo. Você pode alterar essa porcentagem para cada serviço analisado com base no uso estimado para criar uma estimativa de custo mensal atualizada. A estimativa é do custo de analisar seus recursos e não inclui os custos associados às chamadas da API DevOps Guru.

Você pode criar uma estimativa de custo de cada vez. O tempo necessário para gerar uma estimativa de custo depende do número de recursos que você especifica ao criar a estimativa de custo. Quando você especifica alguns recursos, a conclusão pode levar de 1 a 2 horas. Quando você especifica muitos recursos, a conclusão pode levar até 4 horas. Seus custos reais variam e dependem da porcentagem de tempo que os recursos ativos analisados são utilizados.

> **Note**
>
> Para uma estimativa de custo, você pode especificar somente uma AWS CloudFormation pilha. Para seu limite de cobertura real, você pode especificar até 1000 pilhas.

Para criar uma estimativa mensal de custo de análise de recursos

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.
2. No painel de navegação, selecione Estimador de custo.
3. Se você não habilitou o DevOps Guru, você deve criar uma função do IAM. Na janela pop-up Criar função do IAM para o DevOps Guru que aparece, escolha Concordar para criar a função do IAM. Isso permite que o DevOps Guru crie uma função vinculada ao serviço do IAM para você quando você optar por iniciar a análise da estimativa de custo ou começar a usar o Guru. DevOps Dessa forma, o DevOps Guru tem as permissões necessárias para criar a estimativa de custo. Se você já habilitou o DevOps Guru, a função já foi criada e essa opção não aparece.

4. Escolha os recursos que você deseja usar para criar sua estimativa.

   - Se você quiser estimar o custo para o DevOps Guru analisar os recursos definidos por uma AWS CloudFormation pilha, faça o seguinte.
     1. Escolha a CloudFormation pilha na região atual.
     2. Em Escolha uma CloudFormation pilha, escolha o nome de uma AWS CloudFormation pilha na sua AWS conta. Você também pode inserir o nome de uma pilha para encontrá-la rapidamente. Para obter informações sobre como visualizar suas pilhas e trabalhar com elas, consulte Como trabalhar com pilhas no Guia do usuário do AWS CloudFormation .
     3. (Opcional) Se você usa uma AWS CloudFormation pilha que não está analisando no momento, escolha Habilitar análise de recursos para permitir que o DevOps Guru comece a analisar seus recursos. Essa opção não está disponível se você não tiver ativado o DevOps Guru ou se já estiver analisando os recursos na pilha.
   - Se você quiser estimar o custo para o DevOps Guru analisar recursos com uma tag, faça o seguinte.
     1. Escolha tags em AWS recursos na região atual
     2. Em Chave de tag, escolha a chave da sua tag
     3. Em Valor do Tag, escolha (todos os valores) ou escolha um valor.
   - Se você quiser estimar o custo para o DevOps Guru analisar o recurso em sua AWS conta e região, escolha AWS conta na região atual.
5. Escolha Estimar custo mensal.
6. (Opcional) Na coluna Active resource utilization % (% de utilização ativa de recursos), insira um valor percentual atualizado para um ou mais serviços da AWS. A porcentagem padrão de utilização do recurso ativo é 100%. Isso significa que o DevOps Guru gera a estimativa para o serviço da AWS calculando o custo de uma hora de análise de seus recursos e, em seguida, extrapolando isso em 30 dias para um total de 720 horas. Se um serviço estiver ativo menos de 100% do tempo, você poderá atualizar a porcentagem com base na estimativa de uso para obter uma estimativa mais precisa. Por exemplo, se você atualizar a utilização ativa de recursos de um serviço para 75%, o custo de uma hora de análise de seus recursos será extrapolado em (720 x 0,75) horas ou 540 horas.

Se sua estimativa for de zero dólares, então os recursos que você escolheu provavelmente não incluem recursos apoiados pelo DevOps Guru. Para obter mais informações sobre os serviços e recursos suportados, consulte os preços do Amazon DevOps Guru.

# Começando com o DevOps Guru

Nesta seção, você aprende como começar a usar o Amazon DevOps Guru para que ele possa analisar os dados operacionais e as métricas do seu aplicativo para gerar insights.

Tópicos


- Etapa 1: configurar
- Etapa 2: Habilitar o DevOps Guru
- Etapa 3: Especifique sua cobertura de recursos do DevOps Guru


## Etapa 1: configurar

Antes de começar, prepare-se seguindo as etapas no Configurando o Amazon DevOps Guru.

## Etapa 2: Habilitar o DevOps Guru

Para configurar o Amazon DevOps Guru para ser usado pela primeira vez, você deve escolher como deseja configurar o DevOps Guru. Você pode monitorar aplicativos em sua organização ou monitorar aplicativos em sua conta atual.

Você pode monitorar seus aplicativos em toda a organização ou habilitar o DevOps Guru exclusivamente para a conta corrente. Os procedimentos a seguir descrevem maneiras diferentes de configurar o DevOps Guru com base em suas necessidades.

### Monitorar contas em toda a sua organização

Se você optar por monitorar aplicativos em toda a organização, faça login na conta de gerenciamento da organização. Opcionalmente, você pode configurar uma conta de membro da organização como administrador delegado. Você só pode ter um administrador delegado de cada vez e pode modificar as configurações do administrador posteriormente. A conta de gerenciamento e a conta de administrador delegado que você configurou têm acesso a todos os insights em todas as contas da sua organização.

Você pode adicionar suporte entre contas para sua organização usando o console ou pode fazer isso usando a AWS CLI.

## Integrado com o console DevOps Guru

Você pode usar o console para adicionar suporte para contas em toda a sua organização.

Use o console para permitir que o DevOps Guru visualize insights agregados

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.
2. Escolha Monitorar aplicativos em suas organizações como o tipo de configuração.
3. Escolha qual conta você gostaria de usar como administrador delegado. Selecione Registrar administrador delegado. Isso fornece acesso a uma visão consolidada para qualquer conta que tenha o DevOps Guru ativado. O administrador delegado tem uma visão consolidada de todos os insights e métricas do DevOps Guru em sua organização. Você pode ativar outras contas com a configuração rápida do SSM ou conjuntos de pilhas do AWS CloudFormation . Para saber mais sobre a configuração rápida, consulte Configurar o DevOps Guru com a Configuração Rápida. Para saber mais sobre a configuração com conjuntos de pilhas, consulte Como trabalhar com pilhas no Guia do usuário do AWS CloudFormation , e Etapa 2 — Determinar a cobertura para o DevOps Guru, e Usando AWS CloudFormation pilhas para identificar recursos em seus aplicativos DevOps Guru.

## Integrado com a CLI do AWS

Você pode usar a AWS CLI para permitir que o DevOps Guru visualize insights agregados. Execute os seguintes comandos.

```
aws iam create-service-linked-role --aws-service-name devops-guru.amazonaws.com --
description "My service-linked role to support DevOps Guru"

aws organizations enable-aws-service-access --service-principal devops-
guru.amazonaws.com

aws organizations register-delegated-administrator --account-id >ACCOUNT_ID< --service-
principal devops-guru.amazonaws.com
```

A tabela a seguir descreve os comandos.

| Comando | Descrição |
| --- | --- |
| `create-service-linked-role` | |

| Comando | Descrição |
| --- | --- |
| | Permite que o DevOps Guru colete informaçõ es sobre sua organização. Não prossiga se essa etapa não for bem-sucedida. |
| `enable-aws-service-access` | Integra sua organização ao DevOps Guru. |
| `register-delegated-administrator` | Dá acesso à conta do membro para ver os insights. |

## Monitorar sua conta atual

Se você optar por monitorar aplicativos em sua AWS conta corrente, escolha quais AWS recursos em sua conta e região serão cobertos ou analisados e especifique um ou dois tópicos do Amazon Simple Notification Service que serão usados para notificá-lo quando um insight for criado. Essas configurações podem ser atualizadas posteriormente, conforme necessário.

Permita que o DevOps Guru monitore aplicativos em sua conta atual AWS

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.
2. Escolha Monitorar aplicativos na conta atual AWS conta como o tipo de configuração.
3. Na cobertura da análise do DevOps Guru, escolha uma das opções a seguir.

   - Analise todos os AWS recursos na AWS conta corrente: o DevOps Guru analisa todos os AWS recursos da sua conta.
   - Escolher os atributos da AWS para analisar posteriormente: você escolhe seu limite de análise posteriormente. Para ter mais informações, consulte Determine a cobertura para o DevOps Guru e Atualizando sua cobertura AWS de análise no DevOps Guru.

   DevOpsO Guru pode analisar qualquer recurso associado à AWS conta que ele suporta. Para obter mais informações sobre os serviços e recursos suportados, consulte os preços do Amazon DevOps Guru.
4. Você pode adicionar até dois tópicos. DevOpsO Guru usa o tópico ou tópicos para notificá-lo sobre eventos importantes do DevOps Guru, como a criação de uma nova visão. Se você não

especificar um tópico agora, poderá adicionar um posteriormente escolhendo Configurações no painel de navegação.

a. Em Especificar um tópico do Amazon SNS, escolha um tópico para usar.

b. Para adicionar um tópico do Amazon SNS, siga um dos procedimentos abaixo.

- Escolha Gerar um novo tópico do SNS usando e-mail. Depois, em Especificar o endereço de e-mail, informe o endereço de e-mail no qual você deseja receber notificações. Para inserir endereços de e-mail adicionais, escolha Adicionar novo e-mail.
- Escolha Usar um tópico SNS existente. Em seguida, em Escolha um tópico na sua AWS conta, escolha o tópico que você deseja usar.
- Escolha Usar um ARN de tópico do SNS existente para especificar um tópico existente de outra conta. Depois, em Inserir um ARN para um tópico, insira o ARN do tópico. O ARN é o nome do recurso da Amazon do tópico. Você pode especificar um tópico em uma conta diferente. Se você usar um tópico em outra conta, deverá adicionar uma política de atributos ao tópico. Para obter mais informações, consulte permissões para os tópicos do Amazon SNS.

5. Escolha Habilitar.

Para configurar o Amazon DevOps Guru para ser usado pela primeira vez, você deve escolher quais AWS recursos em sua conta e região serão cobertos ou analisados e especificar um ou dois tópicos do Amazon Simple Notification Service que serão usados para notificá-lo quando um insight for criado. Essas configurações podem ser atualizadas posteriormente, conforme necessário.

## Etapa 3: Especifique sua cobertura de recursos do DevOps Guru

Se você optar por especificar AWS recursos posteriormente ao ativar o DevOps Guru, precisará escolher as AWS CloudFormation pilhas em sua AWS conta que criam os recursos que você deseja analisar. Uma AWS CloudFormation pilha é uma coleção de AWS recursos que você gerencia como uma única unidade. Você pode usar uma ou mais pilhas para incluir todos os recursos necessários para executar seus aplicativos operacionais e, em seguida, especificá-los para que sejam analisados pelo DevOps Guru. Se você não especificar pilhas, o DevOps Guru analisará todos os AWS recursos da sua conta. Para mais informações, consulte Como trabalhar com pilhas no Guia do usuário do AWS CloudFormation , e Determine a cobertura para o DevOps Guru, e Usando AWS CloudFormation pilhas para identificar recursos em seus aplicativos DevOps Guru.

> **Note**
>
> Para obter mais informações sobre serviços e recursos suportados, consulte os preços do Amazon DevOps Guru.

Especifique a cobertura de recursos do DevOps Guru

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.
2. Selecione Configurações no painel de navegação.
3. Em Atributos analisados, escolha Editar atributos analisados.
4. Escolha uma das seguintes opções de cobertura.

   - Escolha Todos os recursos da conta se quiser que o DevOps Guru analise todos os recursos suportados em sua AWS conta e região. Se você escolher essa opção, sua AWS conta será o limite de cobertura da análise de recursos. Todos os recursos de cada pilha da sua conta são agrupados em um aplicativo próprio. Todos os recursos restantes que não estão em uma pilha são agrupados em um aplicativo próprio.
   - Escolha CloudFormation pilhas se quiser que o DevOps Guru analise os recursos que estão nas pilhas que você escolher e, em seguida, escolha uma das opções a seguir.
     - Todos os recursos: todos os recursos que estão em pilhas na sua conta são analisados. Os recursos em cada pilha são agrupados em seu próprio aplicativo. Os recursos em sua conta que não estejam em uma pilha não são analisados.
     - Selecionar pilhas — Selecione as pilhas que você deseja que o DevOps Guru analise. Os recursos em cada pilha que você seleciona são agrupados em seu próprio aplicativo. Você pode inserir o nome de uma pilha em Localizar pilhas para localizar rapidamente uma pilha específica. Você pode selecionar até 1.000 pilhas.

     Para obter mais informações, consulte Usando AWS CloudFormation pilhas para identificar recursos em seus aplicativos DevOps Guru.
   - Escolha Tags se quiser que o DevOps Guru analise todos os recursos que contêm as tags que você escolher. Escolha uma chave e depois uma das seguintes opções.
     - Todos os recursos da conta: analise todos os recursos na região e na conta atuais. Os recursos com a chave de tag selecionada são agrupados por valor de tag, se houver. Os recursos sem essa chave de tag são agrupados e analisados separadamente.

- Escolha valores de tag específicos — Todos os recursos que contêm uma tag com a chave que você escolheu são analisados. DevOpsO Guru agrupa seus recursos em aplicativos de acordo com os valores da sua tag.

  Para obter mais informações, consulte Usando tags para identificar recursos em seus aplicativos DevOps Guru.

- Escolha Nenhum se você não quiser que o DevOps Guru analise nenhum recurso. Essa opção desativa o DevOps Guru para que você pare de incorrer em cobranças decorrentes da análise de recursos.

5. Escolha Salvar.

# Habilitando AWS serviços para análise do DevOps Guru

O Amazon DevOps Guru pode analisar o desempenho de qualquer AWS recurso que ele ofereça suporte. Quando encontrar um comportamento anômalo, ele vai gerar um insight com detalhes sobre o comportamento e como lidar com ele. Para obter mais informações sobre os serviços e recursos suportados, consulte os preços do Amazon DevOps Guru.

DevOpsO Guru usa CloudWatch métricas, AWS CloudTrail eventos e muito mais da Amazon para ajudar a analisar recursos. A maioria dos recursos que ele suporta gera automaticamente as métricas necessárias para a análise do DevOps Guru. No entanto, alguns AWS serviços exigem ações extras para gerar as métricas necessárias. Para alguns serviços, habilitar essas métricas fornece uma análise adicional da cobertura existente do DevOps Guru. Para outros, a análise não é possível até que você habilite esses indicadores. Para ter mais informações, consulte Determine a cobertura para o DevOps Guru e Atualizando sua cobertura AWS de análise no DevOps Guru.

Serviços que exigem ação para a análise do DevOps Guru

- Amazon Elastic Container Service — Para gerar métricas adicionais que melhorem a cobertura de seus recursos pelo DevOps Guru, siga as etapas em Configurar insights de contêineres no Amazon ECS. Fazer isso pode incorrer em CloudWatch cobranças da Amazon.
- Amazon Elastic Kubernetes Service — Para gerar métricas DevOps para o Guru analisar, siga as etapas em Configuração de insights de contêineres no Amazon EKS e no Kubernetes. DevOpsO Guru não analisa nenhum recurso do Amazon EKS até que a geração dessas métricas seja configurada. Fazer isso pode incorrer em CloudWatch cobranças da Amazon.
- Amazon Simple Storage Service — Para gerar métricas para o DevOps Guru analisar, você deve ativar as métricas de solicitação. Siga as etapas em Criar uma configuração de CloudWatch métricas para todos os objetos em seu bucket. DevOps O Guru não analisa nenhum recurso do Amazon S3 até que a geração dessas métricas seja configurada. Isso pode resultar em cobranças adicionais CloudWatch do Amazon S3.

Para obter mais informações, consulte os CloudWatch preços da Amazon.

# Trabalhando com insights no DevOps Guru

O Amazon DevOps Guru gera uma visão quando detecta comportamentos anômalos em seus aplicativos operacionais. DevOpsO Guru analisa as métricas, os eventos e muito mais nos AWS recursos que você especificou ao configurar DevOps o Guru. Cada insight contém uma ou mais recomendações que você deve seguir para mitigar o problema. Ele também contém uma lista das métricas, uma lista do grupo de logs e uma lista dos eventos que foram usados para identificar o comportamento incomum.

Existem dois tipos de insights.

- Os insights reativos têm recomendações que você pode seguir para resolver problemas que estão acontecendo agora.
- Os insights proativos têm recomendações que abordam problemas que o DevOps Guru prevê que ocorrerão no futuro.

Tópicos


- Visualizando os DevOps insights do Guru
- Entendendo os insights no console do DevOps Guru
- Entender como comportamentos anômalos são agrupados em insights
- Entender as gravidades do insight


## Visualizando os DevOps insights do Guru

Você pode ver seus insights usando AWS Management Console o.

Veja suas ideias sobre o DevOps Guru

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.
2. Abra o painel de navegação e escolha Insights.
3. Na guia Reativo, você pode ver uma lista de insights reativos. Na guia Proativo, você pode ver uma lista de insights proativos.
4. (Opcional) Use um ou mais dos seguintes filtros para encontrar as informações que está procurando.

- Escolha a guia Reativo ou Proativo, dependendo do tipo de insight que você está procurando.
- Escolha Filtrar insights e, depois, escolha uma opção para especificar um filtro. Você pode adicionar uma combinação de filtros de status, gravidade, recursos e tags. Use um filtro de AWS tags para ver insights gerados somente por recursos com tags específicas. Para saber mais, consulte Usando tags para identificar recursos em seus aplicativos DevOps Guru.

> **Note**
>
> DevOpsO Guru pode analisar os seguintes recursos, mas não pode filtrar seus insights usando tags.
>
> - Caminhos e rotas do Amazon API Gateway
> - Amazon DynamoDB Streams
> - Instâncias de grupo do Amazon EC2 Auto Scaling
> - AWS Elastic Beanstalk ambientes
> - Nós do Amazon Redshift

- Escolha ou especifique um intervalo de tempo para filtrar por tempo de criação do insight.
  - 12h mostra insights criados nas últimas 12 horas.
  - 1d mostra insights criados no dia anterior.
  - 1s mostra os insights criados na semana anterior.
  - 1m mostra insights criados no mês anterior.
  - Personalizado permite que você especifique outro intervalo de tempo. O intervalo máximo de tempo que você pode usar para filtrar insights é de 180 dias.

5. Para exibir detalhes de um insight, escolha seu nome.

# Entendendo os insights no console do DevOps Guru

Use o console do Amazon DevOps Guru para visualizar informações úteis em seus insights para ajudá-lo a diagnosticar e lidar com comportamentos anômalos. Quando o DevOps Guru analisa seus recursos e encontra CloudWatch métricas, AWS CloudTrail eventos e dados operacionais relacionados da Amazon que indicam um comportamento incomum, ele cria uma visão que contém

recomendações para resolver o problema e informações sobre as métricas e eventos relacionados. Use dados de insights Melhores práticas no DevOps Guru para resolver problemas operacionais detectados pelo DevOps Guru.

Para visualizar um insight, siga as etapas de Visualizar insights para encontrar um e escolha seu nome. A página de insight contém os seguintes detalhes:

Visão geral do Insight

Nesta seção, você obtém uma visão geral de alto nível do processo. Você pode ver o status do insight (em andamento ou fechado), quantas AWS CloudFormation pilhas são afetadas, quando o insight começou, terminou e foi atualizado pela última vez, e o item de operações relacionado, se houver um.

Se um insight for agrupado no nível da pilha, você poderá escolher o número de pilhas afetadas para visualizar seus nomes. O comportamento anômalo que criou o insight ocorreu nos recursos criados pelas pilhas afetadas. Se um insight for agrupado no nível da conta, o número é zero ou não aparece.

Para obter mais informações, consulte Entender como comportamentos anômalos são agrupados em insights.

Nome do insight

O nome de um insight depende de se ele está agrupado no nível da pilha ou no nível da conta.

- Os nomes de insights no nível da pilha incluem o nome da pilha que contém o recurso com seu comportamento anômalo.
- Os nomes de insights no nível da conta não incluem um nome de pilha.

Para obter mais informações, consulte Entender como comportamentos anômalos são agrupados em insights.

Métrica agregada

Escolha a guia Métricas agregadas para visualizar as métricas relacionadas ao insight. Na tabela, cada linha representa uma métrica. Você pode ver qual AWS CloudFormation pilha criou o recurso que emitiu a métrica, o nome do recurso e seu tipo. Nem todas as métricas estão associadas a uma AWS CloudFormation pilha ou têm um nome.

Quando há vários recursos anômalos simultâneos, a visualização da linha do tempo agrega os recursos e apresenta suas métricas anômalas em uma única linha do tempo para facilitar a análise. As linhas vermelhas em uma linha do tempo indicam períodos de tempo em que uma

métrica emitiu valores incomuns. Para ampliar, use seu mouse para escolher um intervalo de tempo específico. Você também pode usar os ícones da lupa para aumentar e diminuir o zoom.

Escolha uma linha vermelha na linha do tempo para ver informações detalhadas. Na janela que se abre, você pode:

- Escolha Exibir CloudWatch para ver a aparência da métrica no CloudWatch console. Para obter mais informações, consulte Estatísticas e dimensões no Guia do CloudWatch usuário da Amazon.
- Passar o mouse sobre o gráfico para ver detalhes sobre os dados métricos anômalos e quando eles ocorreram.
- Escolher a caixa com a seta para baixo para baixar uma imagem PNG do gráfico.

Anomalias representadas graficamente

Escolha a guia Anomalias representadas em gráfico para ver gráficos detalhados de cada uma das anomalias do insight. Vai aparecer um bloco para cada anomalia com detalhes sobre o comportamento incomum detectado nas métricas relacionadas. Você pode investigar e observar uma anomalia em nível de recurso e por estatística. Os gráficos são agrupados pelo nome da métrica. Em cada bloco, você pode escolher um intervalo de tempo específico na linha do tempo para ampliar. Você também pode usar os ícones da lupa para aumentar e diminuir o zoom ou escolher uma duração predefinida em horas, dias ou semanas (1H, 3H, 12H, 1D, 3D, 1S ou 2S).

Escolha Exibir todas as estatísticas e dimensões para ver detalhes sobre a anomalia. Na janela que se abre, você pode:

- Escolha Exibir CloudWatch para ver a aparência da métrica no CloudWatch console.
- Passar o mouse sobre o gráfico para ver detalhes sobre os dados métricos anômalos e quando eles ocorreram.
- Escolher Estatísticas ou Dimensão para personalizar a exibição do gráfico. Para obter mais informações, consulte Estatísticas e dimensões no Guia do CloudWatch usuário da Amazon.

Grupos de logs

Quando você ativa a detecção de anomalias de registro, o DevOps Guru marca seus grupos de CloudWatch registros para que você possa visualizar grupos de registros relacionados aos seus insights. Na seção Grupo de logs na página de detalhes do insight, cada linha da tabela representa um grupo de registros e lista o recurso relacionado.

Quando há vários grupos de logs anômalos simultâneos, a visualização da linha do tempo os agrega e os apresenta em uma única linha do tempo para facilitar a análise. As linhas roxas

de uma linha do tempo indicam períodos de tempo em que um grupo de logs experimentou anomalias do log.

Escolha uma linha roxa na linha do tempo para ver uma amostra de informações de anomalias do log, como exceções de palavras-chave e desvios numéricos. Escolha Visualizar detalhes do grupo de logs para ver as anomalias do registro. Na janela que se abre, você pode:

- Visualizar um gráfico de anomalias de log e eventos relevantes.
- Passar o mouse sobre o gráfico para ver detalhes sobre os dados de log anômalos e quando eles ocorreram.
- Visualizar as anomalias do log em detalhes com mensagens de amostra, frequência de ocorrência, recomendações relacionadas e horário da ocorrência.
- Clique em Exibir detalhes em CloudWatch para ver as linhas de registro de uma anomalia de registro.

Eventos relacionados

Em Eventos relacionados, visualize AWS CloudTrail eventos relacionados à sua visão. Use esses eventos para entender, diagnosticar e tratar a causa subjacente do comportamento anômalo.

Recomendações

Em Recomendações, você pode ver sugestões que podem ajudar você a resolver o problema subjacente. Quando o DevOps Guru detecta um comportamento anômalo, ele tenta criar recomendações. Um insight pode conter uma, várias ou zero recomendações.

# Entender como comportamentos anômalos são agrupados em insights

Um insight é agrupado em nível da pilha ou em nível da conta. Se um insight for gerado para um recurso que está em uma pilha do AWS CloudFormation , então é um insight em nível da pilha. Caso contrário, é um insight em nível da conta.

A forma como uma pilha é agrupada pode depender de como você configurou sua cobertura de análise de recursos no Amazon DevOps Guru.

Se sua cobertura for definida por pilhas do AWS CloudFormation

Todos os recursos contidos nas pilhas escolhidas são analisados e todos os insights detectados são agrupados em nível da pilha.

Se sua cobertura for sua AWS conta corrente e região

Todos os recursos da sua conta e região são analisados, e há três cenários de agrupamento possíveis para os insights detectados.

- Um insight gerado a partir de um recurso que não faz parte de uma pilha é agrupado em nível da conta.
- Um insight gerado a partir de um recurso que está em uma das primeiras 10.000 pilhas analisadas é agrupado em nível da pilha.
- Um insight gerado a partir de um recurso que não está em uma das primeiras 10.000 pilhas analisadas é agrupado em nível da conta. Por exemplo, um insight gerado para um recurso na 10.001ª pilha analisada é agrupado em nível da conta.

Para obter mais informações, consulte Determine a cobertura para o DevOps Guru.

# Entender as gravidades do insight

Um insight pode ter uma das três gravidades: alta, média ou baixa. Um insight é criado pelo Amazon DevOps Guru depois que ele detecta anomalias relacionadas e atribui uma gravidade a cada anomalia. DevOpsO Guru atribui a uma anomalia uma severidade alta, média ou baixa usando conhecimento de domínio e anos de experiência coletiva. A gravidade de um insight é determinada pela anomalia mais grave que contribuiu para criar o insight.

- Se a gravidade de todas as anomalias que geraram o insight for baixa, a gravidade do insight será baixa.
- Se a gravidade mais alta de todas as anomalias que geraram o insight for média, então a gravidade do insight será média. A gravidade de algumas das anomalias que geraram o insight pode ser baixa.
- Se a maior gravidade de todas as anomalias que geraram o insight for alta, então a gravidade do insight será alta. A gravidade de algumas das anomalias que geraram o insight pode ser baixa ou média.

# Monitorando bancos de dados usando o DevOps Guru

DevOpsO Guru fornece um valor significativo para operar bancos de dados em. AWS Ao aproveitar seus algoritmos de aprendizado de máquina, o DevOps Guru pode ajudar a otimizar o desempenho do banco de dados, melhorar a confiabilidade e reduzir a sobrecarga operacional. Esta seção do guia do usuário fornece uma visão geral de alto nível desses recursos de banco de dados, incluindo casos de uso específicos do DevOps Guru para diferentes serviços de AWS banco de dados.

DevOpsO Guru pode fornecer informações para bancos de dados relacionais, como Amazon RDS e. Amazon Redshift Ele também pode fornecer informações para bancos de dados não relacionais ou NoSQL, como e. Amazon DynamoDB Amazon ElastiCache

Tópicos


- Monitorando bancos de dados relacionais usando o DevOps Guru
- Monitoramento de bancos de dados não relacionais usando o Guru DevOps


## Monitorando bancos de dados relacionais usando o DevOps Guru

DevOpsO Guru usa duas fontes de dados primárias para procurar informações e anomalias em bancos de dados relacionais. Para o Amazon RDS e Amazon Redshift, as métricas CloudWatch vendidas são analisadas para todos os tipos de instância. Para o Amazon RDS, os dados do Performance Insights também são ingeridos para os seguintes tipos de mecanismo: RDS para PostgreSQL, Aurora PostgreSQL e Aurora MySQL.

### Monitoramento de operações de banco de dados no Amazon RDS

Esta seção inclui informações específicas sobre casos de uso e métricas monitoradas no DevOps Guru for RDS, incluindo dados de métricas CloudWatch vendidas e Performance Insights. Para obter mais informações sobre o DevOps Guru for RDS, incluindo os principais conceitos, configurações e benefícios, consulte. the section called “Trabalhando com anomalias no DevOps Guru for RDS”

#### Monitoramento do RDS usando dados de métricas CloudWatch vendidas

DevOpsO Guru é capaz de monitorar todo tipo de instância do RDS ingerindo CloudWatch métricas padrão, como utilização da CPU e latência da operação de leitura e gravação. Como essas métricas são fornecidas por padrão, quando você monitora suas instâncias do RDS com o DevOps Guru, nenhuma configuração adicional é necessária para obter insights. DevOpsO Guru estabelece

automaticamente uma linha de base para essas métricas com base em padrões históricos e as compara com dados em tempo real para detectar anomalias e possíveis problemas em seu banco de dados.

A tabela a seguir mostra uma lista de possíveis insights reativos para o Amazon RDS a partir de métricas vendidas CloudWatch .

| AWS recurso monitorado pelo DevOps Guru | Cenário que o DevOps Guru identifica | CloudWatch métricas monitoradas |
|---|---|---|
| Amazon RDS (todos os tipos de instância) | CPU ou memória atingindo limites | DBLoad, DBLoad CPU |
| RDS para PostgreSQL | Alto atraso no slot de replicaçã o | OldestReplicationSlotLag |

Métricas adicionais CloudWatch vendidas de instâncias do Amazon RDS que o DevOps Guru monitora:

- CPUUtilization
- DatabaseConnections
- DiskQueueDepth
- Falhou SQLServer AgentJobsCount
- ReadLatency
- ReadThroughput
- ReplicaLag
- WriteLatency

## Monitorando o RDS usando dados do Performance Insights

Para certos tipos de instâncias do Amazon RDS, como Aurora PostgreSQL, Aurora MySQL e RDS for PostgreSQL, você libera mais recursos do monitoramento do Guru ao garantir que o Performance Insights DevOps esteja habilitado nessas instâncias.

DevOpsO Guru fornece insights reativos para uma variedade de situações, incluindo os seguintes cenários:

| Cenário que o DevOps Guru identifica para gerar uma visão reativa |
| --- |
| Problema de bloqueio de contenção |
| Índice ausente |
| Configuração incorreta do pool de aplicativos |
| Padrões de JDBC abaixo do ideal |

DevOpsO Guru fornece insights proativos para uma variedade de situações, incluindo os seguintes cenários:

| AWS recurso monitorado pelo DevOps Guru | Cenário que o DevOps Guru identifica para gerar uma visão proativa |
| --- | --- |
| Aurora MySQL | A lista de histórico do InnoDB está ficando muito grande, o que pode levar à degradaçã o do desempenho, como um longo tempo de desligamento do banco de dados |
| Aurora MySQL | Um aumento nas tabelas temporárias criadas em disco que pode afetar o desempenho do banco de dados |
| RDS para PostgreSQL, Aurora PostgreSQL | Uma conexão que ficou inativa na transação por muito tempo, impacto potencial de manter bloqueios, bloquear outras consultas e impedir que o vácuo (incluindo o autovacuum) limpe linhas mortas |

## Monitorando operações de banco de dados em Amazon Redshift

DevOpsO Guru é capaz de monitorar seus Amazon Redshift recursos ingerindo CloudWatch métricas padrão, incluindo a utilização da CPU e a porcentagem de espaço em disco usado. Como essas métricas são fornecidas por padrão, nenhuma configuração adicional é necessária para que o DevOps Guru monitore automaticamente seus Amazon Redshift recursos. DevOpsO Guru

estabelece uma linha de base para essas métricas com base em padrões históricos e as compara com dados em tempo real para detectar anomalias.

| Cenário que o DevOps Guru identifica | CloudWatch métricas monitoradas |
| --- | --- |
| Detecte a alta utilização da CPU de uma Amazon Redshift instância causada por fatores como carga de trabalho do cluster, dados distorcidos e não classificados ou tarefas do nó líder | CPUUtilization |
| Detecte quando uma Amazon Redshift instância está ficando sem espaço em disco devido a problemas com processamento de consultas, distribuição e chave de classific ação, operações de manutenção ou blocos de lápides | PercentageDiskSpaceUsed |

Métricas adicionais CloudWatch de vendas de Amazon Redshift instâncias que o DevOps Guru monitora:

- DatabaseConnections
- HealthStatus
- MaintenanceMode
- NumExceededSchemaQuotas
- PercentageQuotaUsed
- QueryDuration
- QueryRuntimeBreakdown
- ReadIOPS
- ReadLatency
- WLMQueueComprimento
- WLMQueueWaitTime
- WLMQueryDuração
- WriteLatency

# Trabalhando com anomalias no DevOps Guru for RDS

DevOpsO Guru detecta, analisa e fornece recomendações para AWS recursos compatíveis, incluindo mecanismos do Amazon RDS. Para instâncias de banco de dados Amazon Aurora e RDS para PostgreSQL com o Performance Insights ativado DevOps, o Guru for RDS fornece análises detalhadas e específicas do banco de dados sobre problemas de desempenho e recomenda ações corretivas.

Tópicos


- Visão geral do DevOps Guru for RDS
- Habilitando o DevOps Guru para RDS
- Analisar anomalias no Amazon RDS


## Visão geral do DevOps Guru for RDS

A seguir, você encontrará um resumo dos principais benefícios e recursos do DevOps Guru for RDS. Para obter informações sobre insights e anomalias, consulte DevOpsConceitos de guru.

Tópicos


- Benefícios do DevOps Guru para RDS
- Conceitos-chave para ajuste do desempenho do banco de dados
- Conceitos-chave do DevOps Guru for RDS
- Como funciona o DevOps Guru for RDS
- Mecanismos de banco de dados compatíveis


### Benefícios do DevOps Guru para RDS

Se você é responsável por um banco de dados Amazon RDS, talvez não esteja ciente da existência de um evento ou regressão que está afetando esse banco de dados. Quando você ficar sabendo do problema, talvez não saiba por que ele está ocorrendo ou o que fazer a respeito. Em vez de recorrer a um administrador de banco de dados (DBA) para obter ajuda ou confiar em ferramentas de terceiros, você pode seguir as recomendações do DevOps Guru for RDS.

Você obtém as seguintes vantagens com a análise detalhada do DevOps Guru for RDS:

Diagnóstico rápido

DevOpsO Guru for RDS monitora e analisa continuamente a telemetria do banco de dados. Performance Insights, Enhanced Monitoring e Amazon CloudWatch coletam dados de telemetria para suas instâncias de banco de dados. DevOpsO Guru for RDS usa técnicas estatísticas e de aprendizado de máquina para extrair esses dados e detectar anomalias. Para saber mais sobre dados de telemetria para bancos de dados do Amazon Aurora, consulte Como monitorar a carga do banco de dados com o Performance Insights no Amazon Aurora e Como monitorar o sistema operacional utilizando o Enhanced Monitoring, no Guia do usuário do Amazon Aurora. Para saber mais sobre dados de telemetria para outros bancos de dados do Amazon RDS, consulte Como monitorar a carga do banco de dados com o Performance Insights no Amazon Relational Database Service e Como monitorar o sistema operacional utilizando Enhanced Monitoring, no Guia do usuário do Amazon Aurora.

Resolução rápida

Cada anomalia identifica o problema de performance e sugere rotas de investigação ou ações corretivas. Por exemplo, o DevOps Guru for RDS pode recomendar que você investigue eventos de espera específicos. Ou ele pode recomendar que você ajuste as configurações do seu grupo de aplicações para limitar o número de conexões de banco de dados. Com base nessas recomendações, é possível resolver problemas de performance mais rapidamente do que solucionando problemas manualmente.

Insights proativos

DevOpsO Guru for RDS usa métricas de seus recursos para detectar comportamentos potencialmente problemáticos antes que se tornem um problema maior. Por exemplo, ele pode detectar quando as sessões conectadas ao banco de dados não estão executando um trabalho ativo e pode estar mantendo os recursos do banco de dados bloqueados. DevOps O Guru então fornece recomendações para ajudá-lo a resolver os problemas antes que eles se tornem problemas maiores.

Conhecimento profundo dos engenheiros da Amazon e de "machine learning"

Para detectar problemas de desempenho e ajudar você a resolver gargalos, o DevOps Guru for RDS conta com aprendizado de máquina (ML) e análise estatística avançada. Os engenheiros de banco de dados da Amazon contribuíram para o desenvolvimento das descobertas do DevOps Guru for RDS, que resumem muitos anos de gerenciamento de centenas de milhares de bancos de dados. Com base nesse conhecimento coletivo, o DevOps Guru for RDS pode ensinar as melhores práticas.

## Conceitos-chave para ajuste do desempenho do banco de dados

DevOpsO Guru for RDS presume que você esteja familiarizado com alguns conceitos-chave de desempenho. Para saber mais sobre esses conceitos, consulte Visão geral do Performance Insights no Guia do usuário do Amazon Aurora ou Visão geral do Performance Insights no Guia do usuário do Amazon RDS.

Tópicos

- Indicadores
- Detecção de problemas
- Carga de banco de dados
- Eventos de espera

### Indicadores

Um indicador representa um conjunto de pontos de dados ordenados por tempo. Considere um indicador como variável a ser monitorado, e os pontos de dados representando os valores dessa variável ao longo do tempo. O Amazon RDS dispõe de indicadores em tempo real para o banco de dados e o sistema operacional (SO) no qual sua instância de banco de dados é executada. Você pode visualizar todas as métricas do sistema e informações do processo para suas instâncias de banco de dados do Amazon RDS no console do Amazon RDS. DevOps O Guru for RDS monitora e fornece informações sobre algumas dessas métricas. Para obter mais informações, consulte Como monitorar indicadores em um cluster do Amazon Aurora ou Como monitorar indicadores em uma instância do Amazon Relational Database Service.

### Detecção de problemas

DevOpsO Guru for RDS emprega métricas de banco de dados e sistema operacional (SO) para detectar problemas críticos de desempenho do banco de dados, sejam eles iminentes ou contínuos. Há duas maneiras principais pelas quais o DevOps Guru for RDS funciona:

- Usando limites
- Usando anomalias

#### Detectando problemas com limites

Os limites são os valores vinculantes em relação aos quais as métricas monitoradas são avaliadas. Você pode pensar em um limite como uma linha horizontal em um gráfico métrico que separa o

comportamento normal do comportamento potencialmente problemático. DevOps O Guru for RDS monitora métricas específicas e cria limites analisando quais níveis são considerados potencialmente problemáticos para um recurso específico. DevOpsO Guru for RDS então cria insights no console do DevOps Guru quando novos valores métricos ultrapassam um limite especificado em um determinado período de tempo de forma consistente. Os insights contêm recomendações para evitar um impacto futuro no desempenho do banco de dados.

Por exemplo, o DevOps Guru for RDS pode monitorar o número de tabelas temporárias usando disco por um período de 15 minutos e criar uma visão quando a taxa de tabelas temporárias usando disco por segundo é anormalmente alta. Níveis maiores de uso de tabelas temporárias em disco podem afetar o desempenho do banco de dados. Ao expor essa situação antes que ela se torne crítica, o DevOps Guru for RDS ajuda você a tomar ações corretivas para evitar problemas.

Detectar problemas com anomalias

Embora os limites forneçam uma maneira simples e eficaz de detectar problemas no banco de dados, em algumas situações eles não são suficientes. Considere um caso em que os valores indicadores estão aumentando e se transformando em comportamentos potencialmente problemáticos regularmente devido a um processo conhecido, como um trabalho diário de gerar relatórios. Como esses picos são esperados, criar insights e notificações para cada um deles seria contraproducente e provavelmente levaria à fadiga por excesso de alertas.

No entanto, ainda é necessário detectar picos altamente incomuns, pois indicadores muito mais altas que as demais ou que duram muito mais podem representar problemas reais de desempenho do banco de dados. Para resolver essa preocupação, o DevOps Guru for RDS monitora determinadas métricas para detectar quando o comportamento de uma métrica se torna altamente incomum ou anômalo. DevOpsO Guru então relata essas anomalias em insights.

Por exemplo, o DevOps Guru for RDS pode criar uma visão quando a carga do banco de dados não é apenas alta, mas também se desvia significativamente de seu comportamento normal, o que indica uma grande desaceleração inesperada das operações do banco de dados. Ao reconhecer apenas os picos anômalos de carga do banco de dados, o DevOps Guru for RDS permite que você se concentre nas questões que são realmente importantes.

Carga de banco de dados

O conceito-chave para o ajuste do banco de dados é o indicador de carga do banco de dados (carga do BD). A carga do BD representa o quanto o seu banco de dados está ocupado em um determinado momento. Um aumento na carga do banco de dados significa um aumento na atividade do banco de dados.

Uma sessão de banco de dados relacional representa o diálogo de um aplicativo com um banco de dados relacional. Uma sessão ativa é uma sessão que está executando uma solicitação de banco de dados. Uma sessão fica ativa quando está em execução na CPU ou aguardando a disponibilidade de um recurso para que ela possa continuar. Por exemplo, uma sessão ativa pode esperar que uma página seja lida na memória e, em seguida, consumir CPU enquanto faz a leitura dos dados na página.

A média de sessões ativas (AAS) é o indicador `DBLoad` no Performance Insights. Para calcular a AAS, o Performance Insights faz uma amostra do número de sessões ativas a cada segundo. Para um período de tempo específico, a AAS é o número total de sessões, dividido pelo número total de amostra. Um valor AAS igual a 2 significa que, em média, duas sessões estavam ativas em solicitações em um determinado momento.

Uma analogia à carga de banco de dados é a atividade em um armazém. Suponha que o armazém empregue 100 trabalhadores. Se um pedido chegar, um trabalhador atenderá a esse pedido, enquanto os demais permanecerão ociosos. Se 100 ou mais pedidos chegarem, todos os 100 trabalhadores atenderão aos pedidos simultaneamente. Se você obtiver amostras periodicamente de quantos trabalhadores estão ativos durante um determinado período, poderá calcular o número médio de trabalhadores ativos. O cálculo mostra que, em média, N trabalhadores estão ocupados atendendo a pedidos em um determinado momento. Se a média era de 50 trabalhadores ontem e hoje é de 75 trabalhadores, significa que nível de atividades no armazém aumentou. Da mesma maneira, a carga do banco de dados aumenta à medida que a atividade da sessão aumenta.

Para saber mais, consulte Carga do banco de dados no Guia do usuário do Amazon Aurora ou Carga do banco de dados no Guia do usuário do Amazon RDS.

Eventos de espera

Um evento de espera é um tipo de instrumentação de banco de dados que informa qual recurso uma sessão de banco de dados está aguardando para continuar. Quando o Performance Insights conta as sessões ativas para calcular a carga do banco de dados, ele também registra os eventos de espera que estão fazendo com que as sessões ativas esperem. Essa técnica permite que o Performance Insights mostre quais eventos de espera estão contribuindo para a carga do banco de dados.

Todas as sessões ativas estão em um estado de espera ou de execução na CPU. Por exemplo, sessões consomem CPU quando procuram memória, realizam um cálculo ou executam um código processual. Quando as sessões não estão consumindo CPU, elas podem estar aguardando a

leitura de um arquivo de dados ou a gravação em um log. Quanto mais tempo uma sessão aguardar recursos, menos tempo ela será executada na CPU.

Ao ajustar um banco de dados, muitas vezes você tenta descobrir os recursos que as sessões estão aguardando. Por exemplo, dois ou três eventos de espera podem representar 90% da carga do banco de dados. Essa medida significa que, em média, as sessões ativas estão passando a maior parte do tempo aguardando um pequeno número de recursos. Se você conseguir descobrir a causa dessas esperas, poderá tentar solucionar o problema.

Considere a analogia de um trabalhador de armazém. Chega um pedido de um livro. O trabalhador pode estar atrasado no processamento desse pedido. Por exemplo, outro trabalhador pode estar reabastecendo as prateleiras, ou talvez um carrinho não esteja disponível. Ou talvez o sistema utilizado para informar o status do pedido esteja lento. Quanto mais tempo o trabalhador aguardar, mais tempo ele demorará para atender ao pedido. Esperar é uma parte natural do fluxo de trabalho do armazém, mas, se o tempo de espera se tornar excessivo, a produtividade diminuirá. Da mesma maneira, esperas de sessão repetidas ou longas podem prejudicar o desempenho do banco de dados.

Para obter mais informações sobre eventos de espera no Amazon Aurora, consulte Ajustar eventos de espera para o Aurora PostgreSQL e Ajustar eventos de espera para o Aurora MySQL, no Guia do usuário do Amazon Aurora.

Para obter mais informações sobre eventos de espera em outros bancos de dados do Amazon RDS, consulte Tuning with wait events for RDS for PostgreSQL no Guia do usuário do Amazon RDS.

Conceitos-chave do DevOps Guru for RDS

Um insight é gerado pelo DevOps Guru quando ele detecta comportamentos anômalos ou problemáticos em seus aplicativos operacionais. Um insight contém anomalias em um ou mais recursos. Uma anomalia representa uma ou mais métricas relacionadas detectadas pelo DevOps Guru que são inesperadas ou incomuns.

Um insight tem gravidade alta, média ou baixa. A gravidade do insight é determinada pela anomalia mais grave que contribuiu para criar o insight. Por exemplo, se o insight AWS-ECS_ MemoryUtilization _e_others incluir uma anomalia com baixa severidade e outra com alta severidade, a severidade geral do insight é alta.

Se as instâncias de banco de dados do Amazon RDS tiverem o Performance Insights ativado, o DevOps Guru for RDS fornecerá análises detalhadas e recomendações sobre as anomalias dessas instâncias. Para identificar uma anomalia, o DevOps Guru for RDS desenvolve uma linha de base

para os valores métricos do banco de dados. DevOpsEm seguida, o Guru for RDS compara os valores métricos atuais com a linha de base histórica.

Tópicos


- Insights proativos
- Insights reativos
- Recomendações


## Insights proativos

Um insight proativo informa você sobre um comportamento problemático antes que ele ocorra. Ele contém anomalias com recomendações e indicadores relacionados para ajudar você a resolver os problemas antes que se tornem maiores.

Cada página proativa de insights fornece detalhes sobre uma anomalia.

## Insights reativos

Um insight reativo identifica um comportamento anômalo quando ele ocorre. Contém anomalias com recomendações, métricas relacionadas e eventos para ajudar você a entender e resolver os problemas agora.

### Anomalias causais

Uma anomalia causal é uma anomalia de nível superior dentro de um insight reativo. Ela é mostrada como métrica primária na página de detalhes da anomalia no console do DevOps Guru. A carga do banco de dados (carga do banco de dados) é a anomalia causal do DevOps Guru for RDS. Por exemplo, o insight AWS-ECS_ MemoryUtilization _and_others pode ter várias anomalias métricas, uma das quais é a carga do banco de dados (carga do banco de dados) para o recurso AWS/RDS.

Em um insight, a carga anormal do banco de dados pode ocorrer em várias instâncias de banco de dados do Amazon RDS. A gravidade da anomalia pode ser diferente para cada instância de banco de dados. Por exemplo, a gravidade de uma instância de banco de dados pode ser alta, enquanto a gravidade das outras é baixa. O console usa como padrão a anomalia com a maior gravidade.

### Anomalias contextuais

Uma anomalia contextual é uma descoberta em Carga do banco de dados (carga do BD) que é relatada a um insight reativo. Ela é exibida na seção Métricas relacionadas da página de detalhes da anomalia no console do DevOps Guru. Cada anomalia contextual descreve um problema de

performance específico do Amazon RDS que requer investigação. Por exemplo, uma anomalia causal pode incluir as seguintes anomalias contextuais:

- Capacidade da CPU excedida: a fila de execução da CPU ou a utilização da CPU estão acima do normal.
- Memória baixa do banco de dados: os processos não têm memória suficiente.
- Conexões de banco de dados aumentaram: o número de conexões de banco de dados está acima do normal.

### Recomendações

Cada insight tem pelo menos uma ação sugerida. Os exemplos a seguir são recomendações geradas pelo DevOps Guru para RDS:

- Ajuste o SQL IDs *`list_of_IDs`* para reduzir o uso da CPU ou atualize o tipo de instância para aumentar a capacidade da CPU.
- Analise o pico associado às conexões atuais do banco de dados. Considere ajustar as configurações do pool de aplicativos para evitar a alocação dinâmica frequente de novas conexões de banco de dados.
- Procure instruções SQL que executem operações de memória excessivas, como classificação na memória ou junções grandes.
- Investigue o uso intenso de E/S para o seguinte SQL IDs:*`list_of_IDs`*.
- Verifique as instruções que criam grandes quantidades de dados temporários, por exemplo, aquelas que realizam grandes classificações ou usam grandes tabelas temporárias.
- Verifique os aplicativos para ver o que está causando o aumento na carga de trabalho do banco de dados.
- Considere a hablitação do esquema de performance do MySQL
- Verifique se há transações de longa duração e finalize-as com uma confirmação ou reversão.
- Configure o parâmetro idle_in_transaction_session_timeout para encerrar qualquer sessão que estivesse no estado 'inativo na transação' por mais tempo do que o tempo especificado.

## Como funciona o DevOps Guru for RDS

DevOpsO Guru for RDS coleta dados métricos, os analisa e, em seguida, publica anomalias no painel.

Tópicos


- Coleta e análise de dados
- Publicação de anomalias


## Coleta e análise de dados

DevOpsO Guru for RDS coleta dados sobre seus bancos de dados do Amazon RDS a partir do Amazon RDS Performance Insights. Esse recurso monitora as instâncias de banco de dados do Amazon RDS, coleta indicadores e possibilita que você explore os indicadores em um gráfico. A métrica de desempenho mais importante é`DBLoad`. DevOpsO Guru for RDS consome métricas do Performance Insights e as analisa para detectar anomalias. Para obter mais informações sobre Performance Insights, consulte Como monitorar a carga do banco de dados com Performance Insights no Amazon Aurora no Guia do usuário do Amazon Aurora ou Como monitorar a carga do banco de dados com Performance Insights no Amazon RDS no Guia do usuário do AmazonRDS.

DevOpsO Guru for RDS usa aprendizado de máquina e análise estatística avançada para analisar os dados coletados do Performance Insights. Se o DevOps Guru for RDS encontrar problemas de desempenho, ele prosseguirá para a próxima etapa.

## Publicação de anomalias

Um problema de desempenho do banco de dados, como a alta carga do banco de dados, pode degradar a qualidade do serviço do seu banco de dados. Quando o DevOps Guru detecta um problema em um banco de dados do RDS, ele publica uma visão no painel. O insight contém uma anomalia para o recurso AWS/RDS.

Se o Performance Insights estiver ativado para suas instâncias, a anomalia conterá uma análise detalhada do problema. DevOps O Guru for RDS também recomenda que você realize uma investigação ou uma ação corretiva específica. Por exemplo, a recomendação pode ser investigar uma instrução SQL específica de alta carga, considerar o aumento da capacidade da CPU ou fechar idle-in-transaction sessões.

### Mecanismos de banco de dados compatíveis

DevOpsO Guru for RDS é compatível com os seguintes mecanismos de banco de dados:

#### Compatibilidade entre o Amazon Aurora e o MySQL

Para saber mais sobre esse mecanismo, consulte Como trabalhar com o Amazon Aurora MySQL no Guia do usuário do Amazon Aurora.

Compatibilidade entre o Amazon Aurora e o PostgreSQL

Para saber mais sobre esse mecanismo, consulte Como trabalhar com o Amazon Aurora PostgreSQL no Guia do usuário do Amazon Aurora.

Compatibilidade com o Amazon RDS para PostgreSQL

Para saber mais sobre esse mecanismo, consulte Amazon RDS for PostgreSQL no Guia do usuário do Amazon RDS.

DevOpsO Guru relata anomalias e fornece análises básicas para outros mecanismos de banco de dados. DevOpsO Guru for RDS fornece análises e recomendações detalhadas somente para Amazon Aurora e RDS para instâncias do PostgreSQL.

## Habilitando o DevOps Guru para RDS

Ao habilitar o DevOps Guru para RDS, você permite que o DevOps Guru analise anomalias em recursos, como instâncias de banco de dados. O Amazon RDS facilita a descoberta e a habilitação da funcionalidade recomendada para uma instância de banco de dados ou cluster de banco de dados do RDS. Para conseguir isso, o RDS faz chamadas de API para outros serviços, como Amazon EC2, DevOps Guru e IAM. Quando o console do RDS faz essas chamadas de API, elas são AWS CloudTrail registradas para fins de visibilidade.

Para permitir que o DevOps Guru publique insights para um banco de dados do Amazon RDS, conclua as tarefas nas seções a seguir.

Tópicos

- Ativar o Performance Insights para suas instâncias de banco de dados Amazon Aurora
- Configurando políticas de acesso para o DevOps Guru for RDS
- Adicionando instâncias de banco de dados do Amazon RDS à sua cobertura do DevOps Guru

Ativar o Performance Insights para suas instâncias de banco de dados Amazon Aurora

Para que o DevOps Guru for RDS analise anomalias em uma instância de banco de dados, certifique-se de que o Performance Insights esteja ativado. Se o Performance Insights não estiver ativado para uma instância de banco de dados, o DevOps Guru for RDS notificará você nos seguintes locais:

Painel

Se você visualizar insights por tipo de recurso, o quadro do RDS avisará que o Performance Insights não está ativado. Escolha o link para ativar o Performance Insights no console do Amazon RDS.

Insights

Na seção Recomendações na parte inferior da página, escolha Habilitar Amazon RDS Performance Insights.

Configurações

Na seção Serviço: Amazon RDS, escolha o link para ativar o Performance Insights no console do Amazon RDS.

Para obter mais informações, consulte Como ativar e desativar o Performance Insights no Guia do usuário do Amazon Aurora ou Como ativar e desativar o Performance Insights no Guia do usuário do Amazon RDS.

Configurando políticas de acesso para o DevOps Guru for RDS

Para que um usuário acesse o DevOps Guru for RDS, ele deve ter permissões de uma das seguintes políticas:

- A política AWS gerenciada `AmazonRDSFullAccess`
- Uma política gerenciada pelo cliente que permita as seguintes ações:
  - `pi:GetResourceMetrics`
  - `pi:DescribeDimensionKeys`
  - `pi:GetDimensionKeyDetails`

Para obter mais informações, consulte Como configurar políticas de acesso para Performance Insights no Guia do usuário do Amazon Aurora ou Configuração de políticas de acesso para Performance Insights no Guia do usuário do Amazon RDS.

Adicionando instâncias de banco de dados do Amazon RDS à sua cobertura do DevOps Guru

Você pode configurar o DevOps Guru para monitorar seus bancos de dados do Amazon RDS no console do DevOps Guru ou no console do Amazon RDS.

No console do DevOps Guru, você tem as seguintes opções:

- Ative o DevOps Guru no nível da conta. Esse é o padrão. Quando você escolhe essa opção, o DevOps Guru analisa todos os AWS recursos compatíveis em seu Região da AWS e Conta da AWS, inclusive, bancos de dados Amazon RDS.
- Especifique AWS CloudFormation as pilhas para o DevOps Guru for RDS.

  Para obter mais informações, consulte Usando AWS CloudFormation pilhas para identificar recursos em seus aplicativos DevOps Guru.
- Marcar com tag os recursos do Amazon EC2

  Uma tag é um rótulo de atributo personalizado que você atribui a um AWS recurso. Use tags para identificar os AWS recursos que compõem seu aplicativo. Em seguida, você pode filtrar seus insights por tag para visualizar somente aqueles criados pelo seu aplicativo. Para visualizar somente os insights gerados pelos recursos do Amazon RDS em seu aplicativo, adicione um valor como `Devops-guru-rds` às suas tags de recursos do Amazon RDS. Para obter mais informações, consulte Usando tags para identificar recursos em seus aplicativos DevOps Guru.

  > **Note**
  >
  > Ao marcar recursos do Amazon RDS, você deve marcar a instância do banco de dados, e não o cluster.

Para habilitar o monitoramento do DevOps Guru a partir do console do Amazon RDS, consulte Ativando o DevOps Guru no console do RDS. Observe que, para habilitar o DevOps Guru no console do Amazon RDS, você deve usar tags. Para obter mais informações sobre tags, consulte the section called “Usar tags para identificar recursos em seus aplicativos”.

## Analisar anomalias no Amazon RDS

Quando o DevOps Guru for RDS publica uma anomalia de desempenho no painel, você normalmente executa as seguintes etapas:

1. Veja as informações no painel do DevOps Guru. DevOpsO Guru for RDS relata insights reativos e proativos.

   Para obter mais informações, consulte Visualizar insights.
2. Visualize anomalias dos recursos do AWS/RDS.

Para ter mais informações, consulte Visualizar anomalias reativas e Visualizar anomalias proativas.

3. Responda ao DevOps Guru para obter recomendações do RDS.

   Para obter mais informações, consulte Resposta às recomendações.

4. Monitore a integridade de suas instâncias de banco de dados para garantir que os problemas de desempenho resolvidos não se repitam.

   Para obter mais informações, consulte Indicadores de monitoramento em um cluster de banco de dados Amazon Aurora no Guia do usuário do Amazon Aurora e Indicadores de monitoramento em uma instância do Amazon RDS no Guia do usuário do Amazon RDS.

## Visualizar insights

Acesse a página Insights no console do DevOps Guru para encontrar insights reativos e proativos. A partir daí, você pode escolher um insight da lista para ver uma página detalhada de indicadores, recomendações e mais informações sobre o insight.

Para visualizar um insight

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.
2. Abra o painel de navegação e depois escolha Insights.
3. Escolha a guia Reativos para visualizar insights reativos ou escolha Proativos para visualizar insights proativos.
4. Escolha o nome de um insight, priorizando por status e gravidade.

   A página de insights detalhados é exibida.

## Visualizar anomalias reativas

Em um insight, você pode visualizar anomalias nos recursos do Amazon RDS. Em uma página de insights reativos, na seção Indicadores agregados, você pode ver uma lista de anomalias com os cronogramas correspondentes. Também há seções que exibem informações sobre grupos de logs e eventos relacionados às anomalias. Cada anomalia causal em uma visualização reativa tem uma página correspondente com detalhes sobre a anomalia.

### Visualizar a análise detalhada de uma anomalia reativa do RDS

Nesse estágio, detalhe a anomalia para obter a análise detalhada e as recomendações para suas instâncias de banco de dados do Amazon RDS.

A análise detalhada só está disponível para instâncias de banco de dados Amazon RDS com o Performance Insights ativado.

Para ver os pormenores da página de detalhes da anomalia

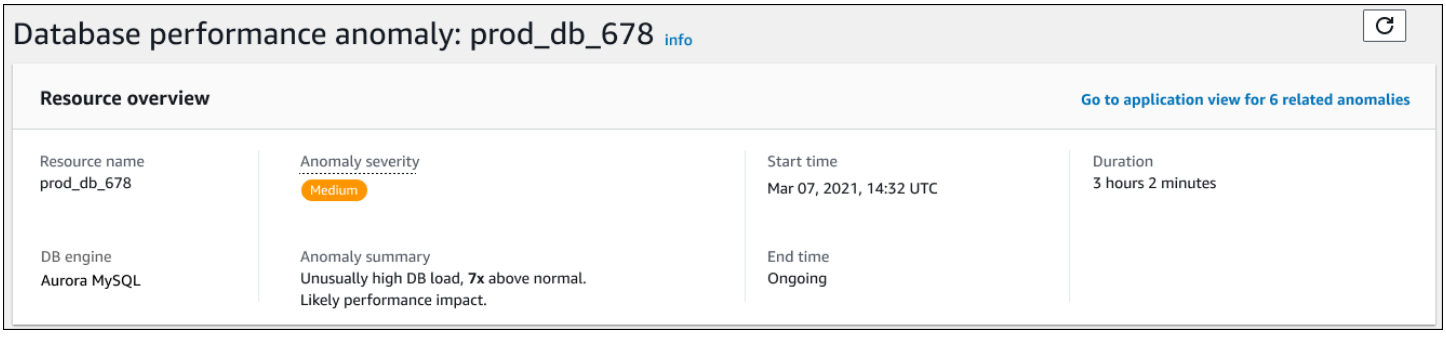
1. Na página de insights, encontre uma métrica agregada com o tipo de recurso AWS/RDS.
2. Escolha Exibir detalhes.

   A página de detalhes da anomalia é exibida. O título começa com Anomalia de desempenho do banco de dados e nomeia o recurso mostrado. O console usa como padrão a anomalia de maior gravidade, independentemente de quando a anomalia ocorreu.
3. (Opcional) Se vários recursos forem afetados, escolha outro recurso na lista na parte superior da página.

Veja a seguir descrições dos componentes da página de detalhes.

#### Visão geral do recurso

A seção superior da página de detalhes é Visão geral do recurso. Esta seção resume a anomalia de performance experimentada pela instância de banco de dados do Amazon RDS.



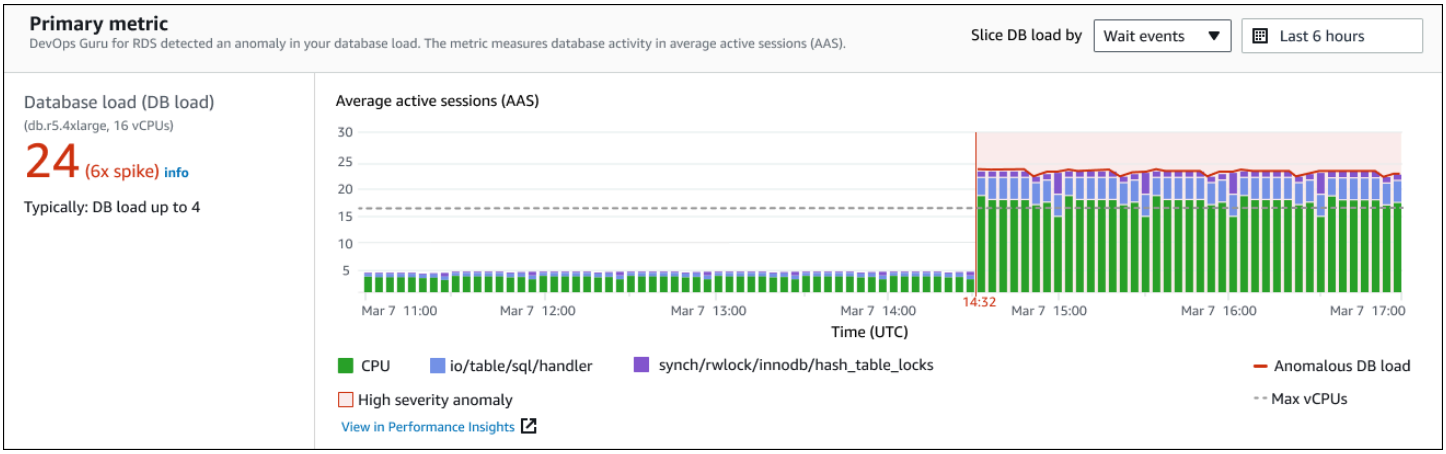

A seção pode incluir os seguintes campos:

- Nome do recurso: o nome da instância de banco de dados que está enfrentando a anomalia. Neste exemplo, o grupo de recursos é chamado de prod_db_678.
- Mecanismo do banco de dados: o nome da instância de banco de dados que está enfrentando a anomalia. Neste exemplo, o mecanismo é o Aurora MySQL.

- Gravidade da anomalia: a medida do impacto negativo da anomalia na sua instância. As gravidades possíveis são Alta, Média e Baixa.
- Resumo da anomalia: um breve resumo do problema. Um resumo típico é Carga de banco de dados excepcionalmente alta.
- Hora de início e hora de término: as horas em que a anomalia começou e terminou. Se o horário de término for contínuo, a anomalia ainda está ocorrendo.
- Duração: a duração do comportamento anômalo. Neste exemplo, a anomalia está em andamento e está ocorrendo há 3 horas e 2 minutos.

### Indicador primário

A seção Indicador primário resume a anomalia casual, que é a anomalia de nível superior dentro do insight. Você pode pensar na anomalia causal como o problema geral enfrentado pela sua instância de banco de dados.




O painel esquerdo fornece mais detalhes sobre o problema. Neste exemplo, o resumo inclui as seguintes informações:

- Carga do banco de dados : uma categorização da anomalia como um problema de carga do banco de dados. O indicador correspondente no Performance Insights é `DBLoad`. Essa métrica também é publicada na Amazon CloudWatch.
- db.r5.4xlarge: a classe de instância de banco de dados. O número de vCPUs, que é 16 neste exemplo, corresponde à linha pontilhada no gráfico Average active sessions (AAS).
- 24 (pico de 6x): a carga do banco de dados, medida em média de sessões ativas (AAS) durante o intervalo de tempo relatado no insight. Assim, em qualquer momento durante o período da anomalia, uma média de 24 sessões estavam ativas no banco de dados. A carga do banco de dados é 6 vezes a carga normal do banco de dados para essa instância.

- Normalmente: carga de banco de dados até 4: a referência da carga de banco de dados, medida em AAS, durante uma carga de trabalho típica. O valor 4 significa que, durante as operações normais, uma média de 4 ou menos sessões estão ativas no banco de dados a qualquer momento.

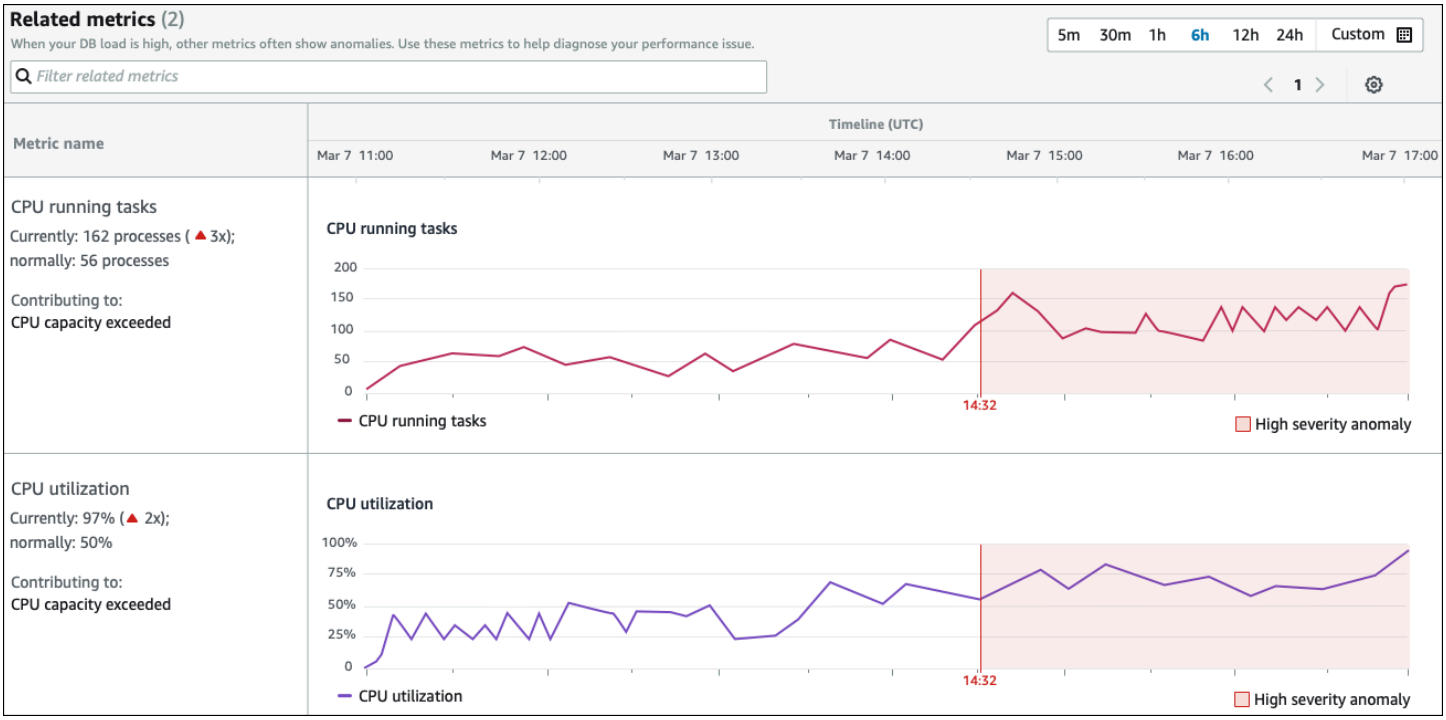
Por padrão, o gráfico de carga é dividido por eventos de espera. Isso significa que, para cada barra no gráfico, a maior área colorida representa o evento de espera que mais contribui para a carga total do banco de dados. O gráfico mostra a hora (em vermelho) em que o problema começou. Concentre sua atenção nos eventos de espera que ocupam mais espaço no bar:

- `CPU`
- `IO:wait/io/sql/table/handler`

Os eventos de espera anteriores aparecem mais do que o normal para esse banco de dados Aurora MySQL. Para aprender a ajustar a performance usando eventos de espera no Amazon Aurora, consulte Como ajustar eventos de espera para o Aurora MySQL e Como ajustar eventos de espera para o Aurora PostgreSQL no Guia do usuário do Amazon Aurora. Para saber como ajustar o desempenho usando eventos de espera no RDS para PostgreSQL, consulte Como ajustar eventos de espera para RDS para o PostgreSQL no Guia do usuário do Amazon RDS.

Indicadores relacionados

A seção Indicadores relacionados lista as anomalias contextuais, que são descobertas específicas dentro da anomalia causal. Essas descobertas fornecem informações adicionais sobre os problemas de desempenho.




A tabela de Indicadores relacionados tem duas colunas: Nome do indicador e Cronograma (UTC). Cada linha da tabela corresponde a um indicador específico.

A primeira coluna de cada linha tem as seguintes informações:

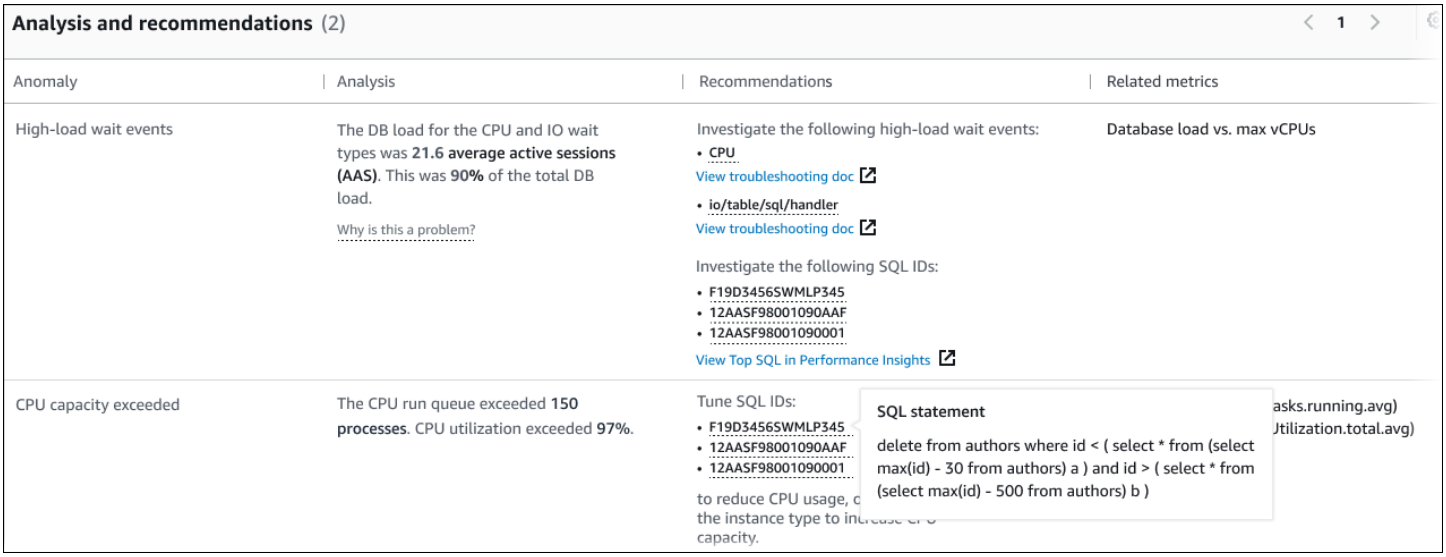
- ***Name***— O nome da métrica. A primeira linha identifica o indicador como tarefas de execução da CPU.
- Atualmente: o valor atual do indicador. Na primeira linha, o valor atual é 162 processos (3x).
- Normalmente — A linha de base dessa métrica para esse banco de dados quando ele está funcionando normalmente. DevOpsO Guru for RDS calcula a linha de base como o valor do 95º percentil em 1 semana de história. A primeira linha indica que 56 processos normalmente estão sendo executados na CPU.
- Contribuindo para: a descoberta associada a esse indicador. Na primeira linha, o indicador de tarefas em execução da CPU está associada à anomalia de capacidade excedida da CPU.

A coluna Cronograma mostra um gráfico de linhas para o indicador. A área sombreada mostra o intervalo de tempo em que o DevOps Guru for RDS designou a descoberta como alta severidade.

### Análise e recomendações

Enquanto a anomalia causal descreve o problema geral, uma anomalia contextual descreve uma descoberta específica que requer investigação. Cada descoberta corresponde a um conjunto de indicadores relacionados.

No exemplo a seguir de uma seção de análise e recomendações, a anomalia de alta carga de banco de dados tem duas descobertas.




A tabela tem as seguintes colunas:

- Anomalia: uma descrição geral dessa anomalia contextual. Neste exemplo, a primeira anomalia são eventos de espera de alta carga, e a segunda é a capacidade da CPU excedida.
- Análise: uma explicação detalhada da anomalia.

  Na primeira anomalia, três tipos de espera contribuem para 90% da carga do banco de dados. Na segunda anomalia, a fila de execução da CPU excedeu 150, o que significa que, a qualquer momento, mais de 150 sessões estavam aguardando tempo de CPU. A utilização da CPU foi superior a 97%, o que significa que, durante o problema, a CPU estava ocupada 97% do tempo. Assim, a CPU estava quase continuamente ocupada, enquanto uma média de 150 sessões esperavam para serem executadas na CPU.
- Recomendações: a resposta sugerida do usuário à anomalia.

  Na primeira anomalia, o DevOps Guru for RDS recomenda que você investigue os eventos de espera e. `cpu` `io/table/sql/handler` Para saber como ajustar o desempenho do seu banco de dados com base nesses eventos, consulte cpu e io/table/sql/handlerno Guia do usuário do Amazon Aurora.

Na segunda anomalia, o DevOps Guru for RDS recomenda que você reduza o consumo de CPU ajustando três instruções SQL. Você pode passar o mouse sobre os links para ver o texto SQL.

- Indicadores relacionados: indicadores que fornecem medidas específicas para a anomalia. Para obter mais informações sobre esses indicadores, consulte Referência de indicadores para Amazon Aurora no Guia do usuário do Amazon Aurora ou Referência de indicadores para Amazon RDS no Guia do usuário do AmazonRDS.

  Na primeira anomalia, o DevOps Guru for RDS recomenda comparar a carga do banco de dados com a CPU máxima da sua instância. Na segunda anomalia, a recomendação é examinar a fila de execução da CPU, a utilização da CPU e a taxa de execução do SQL.

### Visualizar anomalias proativas

Dentro dos insights, você pode visualizar anomalias nos recursos do Amazon RDS. Cada insight proativo fornece detalhes sobre uma anomalia proativa. Em uma página de insights proativos, você pode ver uma visão geral do insight, métricas detalhadas sobre a anomalia e recomendações para evitar problemas futuros. Para ver uma anomalia proativa, acesse a página de insights proativos.

#### Visão geral do insight

A seção Visão geral do insight fornece detalhes sobre por que o insight foi criado. Ela exibe a gravidade do insight, bem como uma descrição da anomalia e o intervalo de tempo no qual a anomalia ocorreu. Ele também lista o número de serviços e aplicativos afetados detectados pelo DevOps Guru.

#### Indicadores

A seção Indicadores fornece gráficos da anomalia. Cada gráfico exibe um limite determinado pelo comportamento básico do recurso, bem como dados do indicador relatados a partir do momento da anomalia.

#### Recomendações para recursos agregados

Esta seção sugere ações que você pode realizar para mitigar os problemas relatados antes que eles se tornem maiores. As ações que você pode realizar são apresentadas na coluna Alteração personalizada recomendada. A lógica por trás das recomendações é apresentada na seção Por que o DevOps Guru está recomendando isso? coluna. Para obter mais informações sobre como responder às recomendações, consulte the section called “Resposta às recomendações”.

### Resposta às recomendações

As recomendações são a parte mais importante do insight. Nesse estágio da análise, você atua para resolver o problema de desempenho. Normalmente, você executa as seguintes etapas:

1. Decida se o problema de desempenho relatado indica um problema real.

   Em alguns casos, um problema pode ser esperado e benigno. Por exemplo, se você sujeitar um banco de dados de teste a uma carga de banco de dados extrema, o DevOps Guru for RDS relata a carga como uma anomalia de desempenho. No entanto, você não precisa corrigir essa anomalia porque é um resultado esperado do seu teste.

   Se você determinar que o problema precisa de uma resposta, vá para a próxima etapa.
2. Decida se deseja implementar a recomendação.

   Na tabela de recomendações, uma coluna mostra as ações recomendadas. Para insights reativos, a coluna é O que recomendamos na página de detalhes da anomalia reativa. Para insights proativos, a coluna é Alteração personalizada recomendada na página de insights proativos.

   DevOpsO Guru for RDS oferece uma lista de recomendações que abrangem vários cenários potencialmente problemáticos. Depois de analisar essa lista, determine qual recomendação é mais relevante para sua situação atual e considere aplicá-la. Se uma recomendação funcionar para a situação, vá para a próxima etapa. Caso contrário, pule a etapa restante e solucione o problema usando técnicas manuais.
3. Execute as ações recomendadas.

   DevOpsO Guru for RDS recomenda que você faça o seguinte:

   - Execute uma ação corretiva específica.

     Por exemplo, o DevOps Guru for RDS pode recomendar que você atualize a capacidade da CPU, ajuste as configurações do pool de aplicativos ou ative o Esquema de Desempenho.
   - Investigue a causa do problema.

     Normalmente, o DevOps Guru for RDS recomenda que você investigue instruções SQL específicas ou eventos de espera. Por exemplo, uma recomendação pode ser investigar o evento de espera `io/table/sql/handler`. Consulte o evento de espera listado em Como ajustar eventos de espera para o Aurora PostgreSQL ou Como ajustar eventos de espera para o Aurora MySQL no Guia do usuário do Amazon Aurora, ou em Como ajustar eventos de

espera para o RDS para PostgreSQL no Guia do usuário do AmazonRDS. Em seguida, execute as ações recomendadas.

> **Important**
>
> Convém testar todas as alterações na instância de teste antes de modificar a instância de produção. Dessa forma, você pode compreender o impacto da alteração.

# Monitoramento de bancos de dados não relacionais usando o Guru DevOps

DevOpsO Guru é capaz de gerar insights para seus bancos de dados não relacionais ou NoSQL que ajudam você a manter seus recursos configurados de acordo com as melhores práticas. Por exemplo, o DevOps Guru pode ajudá-lo a manter o controle do planejamento de capacidade ao prever as necessidades futuras com base no tráfego existente. DevOpsO Guru pode identificar se você está utilizando menos recursos do que os configurados e fornecer recomendações para melhorar a disponibilidade do aplicativo com base no seu histórico de uso. Isso pode ajudar você a reduzir custos desnecessários.

Além do planejamento de capacidade, o DevOps Guru detecta e ajuda você a solucionar problemas operacionais, como limitação, conflitos de transações, falhas de verificação condicional e áreas de melhoria nos parâmetros do SDK. Os bancos de dados geralmente são conectados a vários serviços e recursos, e o DevOps Guru pode correlacionar sua estrutura de aplicativos para análise usando grupos com base em marcação ou agregação. AWS CloudFormation As anomalias podem envolver vários recursos, todos afetados pela mesma solução. DevOps O Guru é capaz de correlacionar diferentes métricas, configurações, registros e eventos de recursos. Por exemplo, o DevOps Guru pode analisar e relacionar dados de uma função Lambda que pode estar lendo ou gravando dados de Amazon DynamoDB uma tabela. Dessa forma, o DevOps Guru monitora vários recursos relacionados para detectar anomalias e fornecer informações úteis para suas soluções de banco de dados.

## Monitorando operações de banco de dados em Amazon DynamoDB

A tabela abaixo mostra exemplos de cenários e insights que o DevOps Guru monitora. Amazon DynamoDB

| Amazon DynamoDB caso de uso | Exemplos | Métricas |
| --- | --- | --- |
| Detecte quando uma grande porcentagem de AccountProvisionedReadCapacityUtilization e AccountProvisionedWriteCapacityUtilization está sendo usada, devido a um grande número de solicitações de leitura e gravação. | Amazon DynamoDB as capacidades de consumo da tabela para solicitações de leitura ou gravação estão atingindo os limites em nível de tabela. | AccountProvisionedReadCapacityUtilization,<br><br>AccountProvisionedWriteCapacityUtilization |
| Detecte falhas de verificação condicional em Amazon DynamoDB solicitações causadas por uma expressão de condição fornecida que não corresponde ao esperado no banco de dados. | As falhas na verificação condicional são causadas por dados incorretos em sua tabela, uma expressão de condição estrita ou condições de corrida. | ConditionalCheckFailedRequests |

## Monitorando operações de banco de dados em Amazon ElastiCache

A tabela abaixo mostra exemplos de cenários e insights que o DevOps Guru monitora. Amazon ElastiCache

| Cenário que o DevOps Guru identifica | CloudWatch métricas monitoradas |
| --- | --- |
| Detecte quando um Amazon ElastiCache cluster está atingindo seu limite de computação para Redis ou Memcached devido às mudanças nas demandas de seus clusters. | CPUUtilization, MotorCPUUtilization, Despejos |

# Integração com o Profiler CodeGuru

Esta seção fornece uma visão geral de como o Amazon DevOps Guru se integra ao Amazon CodeGuru Profiler. Você pode ver as recomendações do CodeGuru Profiler como insights no console do DevOps Guru.

O Amazon DevOps Guru se integra ao Amazon CodeGuru Profiler com uma EventBridge regra gerenciada. CodeGuru O Profiler envia eventos para. EventBridge A regra gerenciada roteia eventos que são enviados com o barramento de eventos padrão. Cada evento de entrada do CodeGuru Profiler é um relatório proativo de anomalias. Para obter mais informações, consulte Trabalhando EventBridge com o CodeGuru Profiler.

DevOpsO Guru suporta eventos de entrada com. EventBridge Um evento indica uma mudança em uma recomendação que o DevOps Guru identificou. CodeGuru O Profiler envia um evento de pulsação a cada 24 horas para mostrar a continuidade do evento. Os eventos contêm informações de recomendação CodeGuru do Profiler, bem como metadados para seus recursos computacionais. Para obter informações sobre o ciclo de vida de um evento, consulte Amazon EventBridge Events.

Quando você configura o DevOps Guru, o DevOps Guru cria a regra EventBridge gerenciada em sua conta que roteia eventos de outro serviço. Essa regra é direcionada para o DevOps Guru. As notificações são enviadas quando há um evento de entrada.

Um barramento de eventos recebe eventos de uma fonte, como o DevOps Guru, e os encaminha para as regras associadas a esse barramento de eventos. Para obter mais informações sobre barramentos de eventos, consulte Barramentos de eventos.

Para obter informações sobre alguns dos parâmetros, consulte EventBridgeEventos da Amazon.

Para receber insights CodeGuru do Profiler no DevOps Guru, você deve ter o seguinte.

- CodeGuru O Profiler deve estar ativado. Para obter informações sobre como ativar o CodeGuru Profiler, consulte Configurando o CodeGuru Profiler.
- DevOpsO Guru deve estar habilitado. Para obter informações sobre como habilitar o DevOps Guru, consulte Habilitar o DevOps Guru.
- Os mesmos recursos devem ser monitorados na mesma região, tanto no CodeGuru Profiler quanto no DevOps Guru.

# Definir aplicativos usando recursos do AWS

O Amazon DevOps Guru agrupa os recursos que estão no limite de cobertura que especifica quais recursos ele analisa para obter informações operacionais. Os recursos são agrupados por recurso em pilhas do AWS CloudFormation ou por recursos com tags. Você escolhe as pilhas ou etiquetas ao configurar o DevOps Guru. Você também pode atualizar as pilhas ou tags posteriormente. Recomendamos que você pense em seus grupos de recursos como aplicativos. Por exemplo, você pode definir todos os recursos que usa para um aplicativo de monitoramento em uma pilha. Ou você pode adicionar a mesma tag a todos os recursos que você usa em um aplicativo de banco de dados, o limite que define quais recursos DevOps o Guru analisa. Todos os recursos da coletânea estão dentro desse limite. Todos os recursos em sua conta que não estejam em sua coletânea de recursos estão fora do limite e não serão analisados. Para obter mais informações sobre os serviços e recursos suportados, consulte os preços do Amazon DevOps Guru.

Você pode definir o limite de cobertura que contém os recursos em seus aplicativos de três maneiras.

- Especifique todos os AWS recursos compatíveis em sua AWS conta e região. Isso faz com que a sua conta e a sua região sejam seu limite de recursos. Com essa opção, o DevOps Guru analisa todos os recursos suportados em sua conta e região. Todos os recursos que estão em uma pilha são agrupados em um aplicativo. Todos os recursos que não estão em uma pilha são agrupados em seu próprio aplicativo.
- Use AWS CloudFormation pilhas para especificar os recursos em seus aplicativos. Uma pilha contém recursos que são gerados usando AWS CloudFormation. No DevOps Guru, você escolhe pilhas na sua conta. Os recursos que você escolhe em cada pilha são agrupados em um aplicativo. Todos os recursos nas pilhas são analisados pelo DevOps Guru para obter informações.
- Use AWS tags para especificar os recursos em seus aplicativos. Uma AWS tag contém uma chave e um valor. No DevOps Guru, escolha uma chave de tag e, opcionalmente, escolha um ou mais valores que estejam emparelhados com essa chave. Você pode usar os valores para agrupar seus recursos em aplicativos.

Para obter mais informações, consulte Atualizando sua cobertura AWS de análise no DevOps Guru.

Tópicos

- Usando tags para identificar recursos em seus aplicativos DevOps Guru

- Usando AWS CloudFormation pilhas para identificar recursos em seus aplicativos DevOps Guru

# Usando tags para identificar recursos em seus aplicativos DevOps Guru

Você pode usar tags para identificar os AWS recursos que o Amazon DevOps Guru analisa e especificar quais recursos são agrupados para monitoramento com a chave de tag e os valores de tag selecionados. Você pode editar essas configurações ao configurar o DevOps Guru ou ao escolher Editar recursos analisados na página Recursos analisados. Depois de selecionar Tags, você escolhe uma chave de tag específica que deseja que o Amazon DevOps Guru monitore. Para analisar todos os recursos na conta e usar valores de tag para agrupar os recursos, selecione Todos os recursos da conta. Para usar valores de tag para especificar os recursos para o DevOps Guru analisar, selecione Escolher valores de tag específicos.

> **Note**
>
> Quando Todos os recursos da conta for selecionado e não existir nenhum valor de tag, os recursos sem a chave de tag serão agrupados e analisados separadamente.

Você usa a chave de uma tag para identificar os recursos e, em seguida, usa valores com essa chave para agrupar recursos em seus aplicativos. Por exemplo, você pode marcar seus recursos com a chave e`devops-guru-applications`, em seguida, usar essa chave com um valor diferente para cada um dos seus aplicativos. Você pode usar os pares `devops-guru-applications/database` de tag chave-valor e `devops-guru-applications/cicd` para identificar três aplicativos em sua conta. `devops-guru-applications/monitoring` Cada aplicativo é composto por recursos relacionados que contêm o mesmo par de tag chave-valor. Você adiciona tags aos seus recursos usando o AWS serviço ao qual elas pertencem. Para obter mais informações, consulte Adicionar AWS tags aos AWS recursos.

Depois de adicionar uma tag aos recursos em seu aplicativo, você pode filtrar seus insights pelas tags dos recursos que os geraram. Para obter mais informações sobre como filtrar seus insights no usando uma tag, consulte Visualizando os DevOps insights do Guru.

Para obter mais informações sobre os serviços e recursos suportados, consulte os preços do Amazon DevOps Guru.

Tópicos


- O que é uma AWS etiqueta?
- Definindo um aplicativo DevOps Guru usando uma tag
- Usando tags com o DevOps Guru
- Adicionar AWS tags aos AWS recursos


## O que é uma AWS etiqueta?

As tags ajudam você a identificar e organizar seus AWS recursos. Muitos AWS serviços oferecem suporte à marcação, então você pode atribuir a mesma tag a recursos de serviços diferentes para indicar que os recursos estão relacionados. Por exemplo, você pode atribuir a mesma tag a um recurso de tabela do Amazon DynamoDB que você atribui a uma função. AWS Lambda Para obter mais informações sobre o uso de tags, consulte o informe Práticas recomendadas de marcação.

Cada AWS etiqueta tem duas partes.

- Uma chave de tag (por exemplo `CostCenter`, `Environment`, `Project` ou `Secret`). As chaves da tag fazem distinção entre maiúsculas e minúsculas.
- Um campo opcional conhecido como um valor de tag (por exemplo, `111122223333`, `Production` ou um nome de equipe). Omitir o valor da tag é o mesmo que usar uma string vazia. Como as chaves de tags, os valores das tags diferenciam maiúsculas de minúsculas.

Juntos, esses são conhecidos como pares de chave-valor.

## Definindo um aplicativo DevOps Guru usando uma tag

Para definir seu aplicativo Amazon DevOps Guru usando uma tag, adicione essa tag aos AWS recursos em sua conta que compõem seu aplicativo. Sua tag contém uma chave e um valor. Recomendamos que você adicione uma tag a cada um dos seus AWS recursos analisados pelo DevOps Guru que tenha a mesma chave. Use um valor diferente na tag para agrupar recursos em seus aplicativos. Por exemplo, você pode atribuir tags com a chave `devops-guru-analysis-boundary` a todos os AWS recursos em seu limite de cobertura. Use valores diferentes com essa chave para identificar aplicativos em sua conta. Você pode usar os valores `containers`, `database`, e `monitoring` para três aplicativos. Para obter mais informações, consulte Atualizando sua cobertura AWS de análise no DevOps Guru.

Se você usar AWS tags para especificar quais recursos analisar, poderá usar tags com apenas uma chave. Você pode emparelhar a chave de suas tags com qualquer valor. Use o valor para agrupar os recursos que contêm sua chave em seus aplicativos operacionais.

> **Important**
>
> Ao criar uma chave, os caracteres da chave podem ser maiúsculos ou minúsculos, à sua escolha. Depois de criada, a chave diferencia entre maiúsculas e minúsculas. Por exemplo, o DevOps Guru trabalha com uma chave nomeada `devops-guru-rds` e uma chave nomeada`DevOps-Guru-RDS`, e elas agem como duas chaves diferentes. Possíveis pares de chave/valor na aplicação podem ser `Devops-Guru-production-application/RDS` ou `Devops-Guru-production-application/containers`.

## Usando tags com o DevOps Guru

Especifique as AWS tags que identificam os AWS recursos que você deseja que o Amazon DevOps Guru analise ou especifique os valores das tags que identificam quais recursos serão agrupados. Esses recursos são seu limite de cobertura de recursos. Você pode escolher uma chave e zero ou mais valores.

Para escolher suas tags

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.
2. Abra o painel de navegação e expanda Configurações.
3. Em Recursos analisados, escolha Editar.
4. Escolha Tags se quiser que o DevOps Guru analise todos os recursos que contêm as tags que você escolher. Escolha uma chave e depois uma das seguintes opções.
   - Todos os recursos da conta — Analise todos os AWS recursos na região e na conta atuais. Os recursos com a chave de tag selecionada são agrupados por valor de tag, se houver. Os recursos sem essa chave de tag são agrupados e analisados separadamente.
   - Escolha valores de tag específicos — Todos os recursos que contêm uma tag com a chave que você escolheu são analisados. DevOpsO Guru agrupa seus recursos em aplicativos de acordo com os valores da sua tag.
5. Escolha Salvar.

## Adicionar AWS tags aos AWS recursos

Ao especificar as AWS tags que identificam os AWS recursos que você deseja que o DevOps Guru analise, escolha tags que tenham recursos associados a elas. Você pode adicionar tags aos seus recursos usando o AWS serviço ao qual cada recurso pertence ou usando o Editor de AWS tags.

- Para gerenciar tags usando o serviço de seus recursos, use o console ou o SDK do serviço ao qual o recurso pertence. AWS Command Line Interface Por exemplo, você pode marcar um recurso de stream do Amazon Kinesis ou um recurso de CloudFront distribuição da Amazon. Esses são dois exemplos de serviços com recursos que podem ser marcados. A maioria dos recursos que o DevOps Guru pode analisar suporta tags. Para obter mais informações, consulte Como marcar seus streams no Amazon Kinesis Developer Guide e Marcar uma distribuição no Amazon Developer Guide. CloudFront  Para saber como adicionar tags a outros tipos de recursos, consulte o guia do usuário ou o guia do desenvolvedor do AWS serviço ao qual eles pertencem.

  > **Note**
  >
  > Ao marcar recursos do Amazon RDS, você deve marcar a instância do banco de dados, e não o cluster.

- Você pode usar o Editor de AWS tags para gerenciar tags por recursos em sua região e por recursos em AWS serviços específicos. Para obter mais informações, consulte o Editor de Tags no Guia do usuário dos Grupos de Recursos e Tags AWS .

Ao adicionar uma tag a um recurso, você pode adicionar somente a chave ou a chave e um valor. Por exemplo, você pode criar uma tag com a chave `devops-guru-` para todos os recursos que fazem parte do seu DevOps aplicativo. Você também pode adicionar uma tag com a chave `devops-guru-` e o valor eRDS, em seguida, adicionar esse par chave-valor somente aos recursos do Amazon RDS em seu aplicativo. Isso é útil se você quiser visualizar insights no console que são gerados somente a partir dos recursos do Amazon RDS em seu aplicativo.

# Usando AWS CloudFormation pilhas para identificar recursos em seus aplicativos DevOps Guru

Você pode usar AWS CloudFormation pilhas para especificar quais AWS recursos você deseja que o DevOps Guru analise. Uma pilha é uma coleção de AWS recursos que são gerenciados como uma única unidade. Os recursos nas pilhas que você escolher compõem seu limite de cobertura

do DevOps Guru. Para cada pilha escolhida, os dados operacionais de seus recursos suportados são analisados em busca de comportamento anômalo. Esses problemas são depois agrupados em anomalias relacionadas para criar insights. Cada insight inclui uma ou mais recomendações para ajudar você a resolvê-los. O número máximo de pilhas que você pode especificar é mil. Para mais informações, consulte Como trabalhar com pilhas no Guia do usuário do AWS CloudFormation e Atualizando sua cobertura AWS de análise no DevOps Guru.

Depois de escolher uma pilha, o DevOps Guru imediatamente começa a analisar qualquer recurso que você adiciona a ela. Se você remover um recurso de uma pilha, ela não será mais analisada.

Se você optar por fazer com que o DevOps Guru analise todos os recursos suportados em sua conta (isso significa que sua AWS conta e região são seu limite de cobertura do DevOps Guru), o DevOps Guru analisa e cria insights para cada recurso suportado em sua conta, incluindo aqueles em pilhas. Um insight criado a partir de anomalias em um recurso que não está em uma pilha é agrupado no nível da conta. Se um insight for criado a partir de anomalias em um recurso que está em uma pilha, ele será agrupado no nível da pilha. Para obter mais informações, consulte Entender como comportamentos anômalos são agrupados em insights.

## Escolhendo pilhas para o DevOps Guru analisar

Especifique os recursos que você deseja que o Amazon DevOps Guru analise escolhendo as AWS CloudFormation pilhas que os criam. Você pode fazer isso usando o AWS Management Console ou o SDK.

Tópicos

- Escolhendo pilhas para o DevOps Guru analisar (console)
- Escolhendo pilhas para o DevOps Guru analisar (DevOpsGuru SDK)

### Escolhendo pilhas para o DevOps Guru analisar (console)

Você pode adicionar AWS CloudFormation pilhas usando o console.

Para escolher as pilhas que contêm os recursos a serem analisados

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.
2. Abra o painel de navegação, e selecione Configurações.
3. Na cobertura da análise do DevOps Guru, escolha Gerenciar.

4. Escolha CloudFormation pilhas se quiser que o DevOps Guru analise os recursos que estão nas pilhas que você escolher e, em seguida, escolha uma das opções a seguir.

   - Todos os recursos: todos os recursos que estão em pilhas na sua conta são analisados. Os recursos em cada pilha são agrupados em seu próprio aplicativo. Os recursos em sua conta que não estejam em uma pilha não são analisados.
   - Selecionar pilhas — Selecione as pilhas que você deseja que o DevOps Guru analise. Os recursos em cada pilha que você seleciona são agrupados em seu próprio aplicativo. Você pode inserir o nome de uma pilha em Localizar pilhas para localizar rapidamente uma pilha específica. Você pode selecionar até 1.000 pilhas.

5. Escolha Salvar.

## Escolhendo pilhas para o DevOps Guru analisar (DevOpsGuru SDK)

Para especificar AWS CloudFormation pilhas usando o Amazon DevOps Guru SDK, use o método. `UpdateResourceCollection` Para obter mais informações, consulte UpdateResourceCollectiona Amazon DevOps Guru API Reference.

# Trabalhando com a Amazon EventBridge

O Amazon DevOps Guru se integra EventBridge à Amazon para notificá-lo sobre determinados eventos relacionados a insights e atualizações de insights correspondentes. Os eventos dos AWS serviços são entregues quase EventBridge em tempo real. É possível criar regras simples para indicar quais eventos são de seu interesse, e quais ações automatizadas devem ser tomadas quando um evento corresponder a uma regra. As ações que podem ser automaticamente acionadas incluem os seguintes exemplos:

- Invocando uma função AWS Lambda
- Invocar um comando de execução do Amazon Elastic Compute Cloud
- Retransmitir o evento para o Amazon Kinesis Data Streams
- Ativar uma máquina de estados do Step Functions
- Notificar sobre um tópico do Amazon SNS ou uma fila do Amazon SQS

Você pode selecionar qualquer um dos seguintes padrões predefinidos para filtrar eventos ou criar uma regra de padrão personalizada para iniciar ações em recursos compatíveis AWS .

- DevOps Guru New Insight Open
- DevOps Associação Guru New Anomaly
- DevOps Gravidade do Guru Insight atualizada
- DevOps Criada nova recomendação do Guru
- DevOps Guru Insight Fechado

# Eventos para DevOps Guru

A seguir estão exemplos de eventos do DevOps Guru. Os eventos são emitidos com base no melhor esforço. Para saber mais sobre padrões de eventos, consulte Introdução à Amazon EventBridge ou Padrões de EventBridge eventos da Amazon.

## DevOpsGuruNovo evento aberto do Insight

Quando o DevOps Guru abre um novo insight, ele envia o seguinte evento.

```
{
```

```
    "version" : "0",
    "id" : "08108845-ef90-00b8-1ad6-2ee5570ac6c4",
    "detail-type" : "DevOps Guru New Insight Open",
    "source" : "aws.devops-guru",
    "account" : "123456789012",
    "time" : "2021-11-01T17:06:10Z",
    "region" : "us-east-1",
    "resources" : [ ],
    "detail" : {
      "insightSeverity" : "high",
      "insightDescription" : "ApiGateway 5XXError Anomalous In Stack TestStack",
      "insightType" : "REACTIVE",
      "anomalies" : [
        {
          "startTime" : "1635786000000",
          "id" : "AL41JDFFQPYlZlXD8cpREkAAAAF83HGGgC9TmTr9lbfJ7sCiISlWMeFCbHY_XXXX",
          "sourceDetails" : [
            {
              "dataSource" : "CW_METRICS",
              "dataIdentifiers" : {
                "period" : "60",
                "stat" : "Average",
                "unit" : "None",
                "name" : "5XXError",
                "namespace" : "AWS/ApiGateway",
                "dimensions" : [
                  {
                    "name" : "ApiName",
                    "value" : "Test API Service"
                  },
                  {
                    "name" : "Stage",
                    "value" : "prod"
                  }
                ]
              }
            }
          ]
        }
      ],
      "accountId" : "123456789012",
      "messageType" : "NEW_INSIGHT",
      "insightUrl" : "https://us-east-1.console.aws.amazon.com/devops-guru/#/insight/
reactive/AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
```

```
      "startTime" : "1635786120000",
      "insightId" : "AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
      "region" : "us-east-1"
    }
  },
```

## Padrão de evento de amostra personalizado para o novo Insight de alta gravidade

As regras usam padrões de evento para selecionar eventos e encaminhá-los para os destinos. A seguir está um exemplo do padrão de eventos do DevOps Guru.

```
{
  "source": [
    "aws.devops-guru"
  ],
  "detail-type": [
    "DevOps Guru New Insight Open"
  ],
  "detail": {
    "insightSeverity": [
          "high"
          ]
  }
}
```

# Atualizando as DevOps configurações do Guru

Você pode atualizar as seguintes configurações do Amazon DevOps Guru:

- Sua cobertura do DevOps Guru. Essa ação define quais recursos da sua conta serão analisados.
- Suas notificações. Isso determina quais tópicos do Amazon Simple Notification Service são usados para notificá-lo sobre eventos importantes do DevOps Guru.
- Atributos para insights aprimorados. Isso inclui detecção de anomalias de log, criptografia e suas configurações de AWS Systems Manager integração. Isso determina se o DevOps Guru exibe dados de log, se você usa chaves de segurança adicionais e se uma OpsItem é criada no Systems Manager OpsCenter para cada nova visão.

Tópicos


- Atualizar as configurações da sua conta de gerenciamento
- Atualizando sua cobertura AWS de análise no DevOps Guru
- Atualizando suas notificações no DevOps Guru
- Filtrando suas notificações do DevOps Guru
- Atualizando AWS Systems Manager a integração no DevOps Guru
- Atualizando a detecção de anomalias de log no DevOps Guru
- Atualizando as configurações de criptografia no DevOps Guru


## Atualizar as configurações da sua conta de gerenciamento

Você pode configurar o DevOps Guru para contas em sua organização. Se você não registrou um administrador delegado, pode fazer isso escolhendo Registrar administrador delegado. Para obter mais informações sobre como registrar um administrador delegado, consulte Enable DevOps Guru.

## Atualizando sua cobertura AWS de análise no DevOps Guru

Você pode atualizar quais AWS recursos em sua conta o DevOps Guru analisa. Para tanto, navegue até a página Recursos analisados no console e escolha Editar. Para obter mais informações, consulte Visualizar recursos analisados.

# Atualizando suas notificações no DevOps Guru

Configure tópicos do Amazon Simple Notification Service que são usados para notificá-lo sobre eventos importantes do Amazon DevOps Guru. Você pode escolher entre uma lista de nomes de tópicos que já existem em sua AWS conta, inserir o nome de um novo tópico que o DevOps Guru cria em sua conta ou inserir o Amazon Resource Name (ARN) de um tópico existente em AWS qualquer conta em sua região. Se você especificar o ARN de um tópico que não está na sua conta, você deve conceder permissão para o DevOps Guru acessar esse tópico adicionando uma política do IAM a ele. Para obter mais informações, consulte permissões para os tópicos do Amazon SNS. Você pode definir até dois tópicos.

DevOpsO Guru envia notificações para as seguintes atualizações:

- Um novo insight foi criado.
- Uma nova anomalia foi adicionada a um insight.
- A gravidade do insight foi atualizada de `Low` ou `Medium` para `High`.
- O status do insight mudou de contínuo para resolvido.
- Uma recomendação para um insight foi identificada.

DevOpsO Guru também envia notificações se uma chave de AWS CloudFormation pilha ou tag selecionada for inválida quando você estiver tentando adicionar recursos à sua conta do Guru. DevOps

Você pode optar por receber notificações do Amazon SNS para todos os tipos de atualização de um problema ou receber notificações do Amazon SNS somente quando o problema for aberto, encerrado ou tiver uma alteração na gravidade. Por padrão, você recebe notificações para todas as atualizações.

Para atualizar suas notificações, primeiro navegue até a página de notificações e escolha entre adicionar, remover ou atualizar as configurações dos tópicos de notificação do Amazon SNS.

Tópicos

- Navegue até as configurações de notificação no console do DevOps Guru
- Adicionando tópicos de notificação do Amazon SNS no console do DevOps Guru
- Removendo tópicos de notificação do Amazon SNS no console do DevOps Guru
- Atualizar as configurações de notificação do Amazon SNS

- Permissões adicionadas ao seu tópico do Amazon SNS

## Navegue até as configurações de notificação no console do DevOps Guru

Para atualizar as notificações, primeiro você deve navegar até a seção de configurações de notificação.

Para navegar até a seção de configurações de notificação

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.
2. Selecione Configurações no painel de navegação.

   A página de Configurações inclui a seção Notificações que contém informações sobre tópicos configurados do Amazon SNS.

## Adicionando tópicos de notificação do Amazon SNS no console do DevOps Guru

Para adicionar um tópico de notificação do Amazon SNS no console do DevOps Guru

1. the section called “Navegue até as configurações de notificação no console do DevOps Guru”.
2. Escolha Adicionar notificação.
3. Para adicionar um tópico do Amazon SNS, siga um dos procedimentos abaixo.

   - Escolha Gerar um novo tópico do SNS usando e-mail. Depois, em Especificar o endereço de e-mail, informe o endereço de e-mail no qual você deseja receber notificações. Para inserir endereços de e-mail adicionais, escolha Adicionar novo e-mail.
   - Escolha Usar um tópico SNS existente. Em seguida, em Escolha um tópico na sua AWS conta, escolha o tópico que você deseja usar.
   - Escolha Usar um ARN de tópico do SNS existente para especificar um tópico existente de outra conta. Depois, em Inserir um ARN para um tópico, insira o ARN do tópico. O ARN é o nome do recurso da Amazon do tópico. Você pode especificar um tópico em uma conta diferente. Se você usar um tópico em outra conta, deverá adicionar uma política de atributos ao tópico. Para obter mais informações, consulte permissões para os tópicos do Amazon SNS.
4. Escolha Salvar.

## Removendo tópicos de notificação do Amazon SNS no console do DevOps Guru

Para remover tópicos do Amazon SNS no console do DevOps Guru

1. the section called “Navegue até as configurações de notificação no console do DevOps Guru”.
2. Escolha Selecionar tópico existente.
3. No menu suspenso, selecione o tópico que você deseja remover.
4. Escolha Remover.
5. Escolha Salvar.

## Atualizar as configurações de notificação do Amazon SNS

Há dois tipos de configurações de notificação para tópicos DevOps de notificação do Amazon SNS no Guru. Você pode optar por receber notificações de todos os níveis de gravidade ou somente notificações com níveis de gravidade Alta e Média. Você também pode escolher entre receber notificações para todos os tipos de atualização ou apenas alguns tipos de atualização.

Quando você escolhe receber notificações do Amazon SNS para todos os tipos de atualizações do problema, o DevOps Guru envia notificações para as seguintes atualizações:

- Um novo insight foi criado.
- Uma nova anomalia foi adicionada a um insight.
- A gravidade do insight foi atualizada de `Low` ou `Medium` para `High`.
- O status do insight mudou de contínuo para resolvido.
- Uma recomendação para um insight foi identificada.

Por padrão, você recebe somente notificações de nível de gravidade Alta e Média e recebe notificações para todos os tipos de atualizações.

Para atualizar as configurações de notificação para tópicos de notificação do Amazon SNS

1. the section called “Navegue até as configurações de notificação no console do DevOps Guru”.
2. Escolha Selecionar tópico existente.
3. No menu suspenso, selecione o tópico que você deseja atualizar.

4. Escolha Todos os níveis de gravidade para receber notificações com níveis de gravidade Alta, Média e Baixa, ou escolha Somente Alta e Média para receber notificações com níveis de gravidade Alta e Média.
5. Escolha Notify me on all updates to the insight (Notifique-me sobre todas as atualizações do insight) ou escolha Notify me when an insight is opened or closed, or the severity level changes from Low or Medium to High (Notifique-me quando um insight for aberto ou fechado, ou se o nível de severidade mudar de Baixo ou Médio para Alto).
6. Escolha Salvar.

## Permissões adicionadas ao seu tópico do Amazon SNS

Um tópico do Amazon SNS é um recurso que contém uma política de recursos AWS Identity and Access Management (IAM). Quando você especifica um tópico aqui, o DevOps Guru acrescenta as seguintes permissões à sua política de recursos.

```
{
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
    }
  }
}
```

Essas permissões são necessárias para que o DevOps Guru publique notificações usando um tópico. Se você preferir não ter essas permissões no tópico, você pode removê-las com segurança e o tópico continuará funcionando como antes de você escolhê-lo. No entanto, se essas permissões anexadas forem removidas, o DevOps Guru não poderá usar o tópico para gerar notificações.

# Filtrando suas notificações do DevOps Guru

Você pode filtrar suas notificações do DevOps Guru usando the section called “Atualizar as configurações de notificação do Amazon SNS” ou usando uma política de filtro de assinatura do Amazon SNS.

Tópicos

- Filtrar notificações com uma política de filtro de assinaturas do Amazon SNS
- Exemplo de notificação filtrada do Amazon SNS para o Amazon Guru DevOps

## Filtrar notificações com uma política de filtro de assinaturas do Amazon SNS

Você pode criar uma política de filtro de assinatura do Amazon Simple Notification Service (Amazon SNS) para reduzir o número de notificações que você recebe do Amazon Guru. DevOps

Use uma política de filtro para especificar os tipos de notificação que você recebe. Você pode filtrar suas mensagens do Amazon SNS usando as seguintes palavras-chave.

- `NEW_INSIGHT`: receber uma notificação quando um novo insight for criado.
- `CLOSED_INSIGHT`: receber uma notificação quando um insight existente for fechado.
- `NEW_RECOMMENDATION`: receber uma notificação quando uma nova recomendação for criada a partir de um insight.
- `NEW_ASSOCIATION`: receber uma notificação quando uma nova anomalia for detectada a partir de um insight.
- `CLOSED_ASSOCIATION`: receber uma notificação quando uma anomalia existente for fechada.
- `SEVERITY_UPGRADED`: receber uma notificação quando a gravidade de um insight for atualizada

Para obter mais informações sobre como criar uma política de filtro de assinatura do Amazon SNS, consulte Amazon SNS subscription filter policies (Políticas de filtro de assinatura do Amazon SNS) no Guia do desenvolvedor do Amazon Simple Notification Service. Em sua política de filtro, você especifica uma das palavras-chave com o `MessageType` da política. Por exemplo, apareceria o seguinte em um filtro que especifica que o tópico do Amazon SNS só entregará notificações quando for detectada uma nova anomalia a partir de um insight.

```
{
```

```
  "MessageType":["NEW_ ASSOCIATION"]
}
```

## Exemplo de notificação filtrada do Amazon SNS para o Amazon Guru DevOps

A seguir, um exemplo de notificação do Amazon Simple Notification Service (Amazon SNS) de um tópico do Amazon SNS com uma política de filtro. O `MessageType` está configurado como `NEW_ASSOCIATION`, portanto, envia notificações somente quando uma nova anomalia é detectada a partir de um insight.

```
{
      "accountId": "123456789012",
      "region": "us-east-1",
      "messageType": "NEW_ASSOCIATION",
      "insightId": "ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-Function duration due to increased number of invocations",
      "insightUrl": "https://us-east-1.console.aws.amazon.com/devops-guru/insight/
reactive/ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightType": "REACTIVE",
      "insightDescription": "At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-Function had\n an increased duration anomaly possibly caused by
 the Lambda function invocation increase. DevOps Guru has detected this is a repeated
 insight. DevOps Guru treats repeated insights as 'Low Severity'.",
      "startTime": 1628767500000,
      "startTimeISO": "2023-03-29T22:00:00Z",
      "anomalies": [
        {
          "id": "AG2n8ljW74BoI1CHu-m_oAgAAAF7Ohu24N4Yro69ZSdUtn_alzPH7VTpaL30JXiF",
          "startTime": 1628767500000,
          "startTimeISO": "2023-03-29T22:00:00Z",
          "openTime": 1680127740000,
          "openTimeISO": "2023-03-29T22:09:00Z",
          "sourceDetails": [
            {
              "dataSource": "CW_METRICS",
              "dataIdentifiers": {
                "namespace": "AWS/SQS",
                "name": "ApproximateAgeOfOldestMessage",
                "stat": "Maximum",
                "unit": "None",
```

```
                "period": "60",
                "dimensions": "{\"QueueName\":\"FindingNotificationsDLQ\"}"
              }
            }
          ],
          "associatedResourceArns":[
           "arn:aws:sns:us-east-1:123456789012:DevOpsGuru-insights-sns"
          ]
        }
      ],
      "resourceCollection":{
      "cloudFormation":{
         "stackNames":[
            "CapstoneNotificationPublisherEcsApplicationInfrastructure"
          ]
        }
      }
}
```

# Atualizando AWS Systems Manager a integração no DevOps Guru

Você pode habilitar a criação de um OpsItem para cada nova visão em AWS Systems Manager OpsCenter. OpsCenter é um sistema centralizado no qual você pode visualizar, investigar e revisar itens de trabalho operacionais (OpsItems). O OpsItems for your insights pode ajudá-lo a gerenciar o trabalho que aborda o comportamento anômalo que desencadeou a criação de cada insight. Para obter mais informações, consulte AWS Systems Manager OpsCentere Trabalhando com OpsItem no Guia AWS Systems Manager do Usuário.

> **Note**
>
> Se você alterar a chave ou o valor do campo de tag de um OpsItem, o DevOps Guru não poderá atualizá-lo. OpsItem Por exemplo, se você alterar a tag de um OpsItem de `"aws:RequestTag/DevOps-GuruInsightSsmOpsItemRelated": "true"` para outra coisa, o DevOps Guru não poderá atualizá-la. OpsItem

Para gerenciar sua integração com o Systems Manager

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.
2. Selecione Configurações no painel de navegação.

3. Na AWS Systems Manager integração, selecione Enable DevOps Guru para criar uma AWS OpstItem entrada OpsCenter para cada insight, a fim de OpsItem criar uma para cada nova visão. Desmarque-a para parar de OpsItem criar uma para cada nova visão.

Você é cobrado pelo OpsItems criado em sua conta. Para obter mais informações, consulte Definição de preço do AWS Systems Manager.

## Atualizando a detecção de anomalias de log no DevOps Guru

Para gerenciar suas configurações de detecção de anomalias do log

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.
2. Selecione Configurações no painel de navegação.
3. Em Detecção de anomalias de log, selecione Ativar detecção de anomalias de log concedendo permissões ao DevOps Guru para exibir dados de log associados a um insight. para que o DevOps Guru exiba dados de registro relacionados a insights.

## Atualizando as configurações de criptografia no DevOps Guru

Você pode atualizar as configurações de criptografia para usar chaves AWS próprias ou chaves gerenciadas pelo AWS KMS cliente. Ao mudar para uma nova AWS KMS chave gerenciada pelo cliente a partir de uma AWS KMS chave gerenciada pelo cliente existente, o DevOps Guru começa automaticamente a criptografar os metadados recém-ingeridos usando a nova chave. Os dados históricos permanecerão criptografados com a AWS KMS chave gerenciada pelo cliente configurada anteriormente.

> **Note**
>
> Se você revogar a concessão ou desativar ou excluir a AWS KMS chave anterior, o DevOps Guru não poderá acessar nenhum dos dados criptografados por essa chave e você poderá vê-los `AccessDeniedException` ao realizar uma operação de leitura.

Para gerenciar suas configurações de criptografia

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.

2. Selecione Configurações no painel de navegação.
3. Na seção Criptografia, escolha Editar criptografia.
4. Selecione o tipo de criptografia que você gostaria de usar para proteger seus dados. Você pode usar uma chave AWS própria padrão, escolher uma chave gerenciada pelo cliente existente ou criar uma nova AWS KMS chave gerenciada pelo cliente.
5. Escolha Salvar.

A criptografia é uma parte importante da segurança do DevOps Guru. Para obter mais informações, consulte the section called “Proteção de dados”.

# Visualizar notificações

Existem diferentes tipos de notificações no DevOps Guru.

Tópicos


- Novo insight
- Insight fechado
- Nova associação
- Nova recomendação
- Gravidade atualizada
- Falha na validação de recursos


As seções nesta página mostram exemplos de cada tipo de notificação.

## Novo insight

As notificações de novos insights contêm as seguintes informações:

```
{
   "accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-4",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"DevOps Guru has detected this is a repeated insight. DevOps
 Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680148920000,
   "startTimeISO": "2023-03-30T04:02:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime": 1680148800000,
         "startTimeISO": "2023-03-30T04:00:00Z",
```

```
         "openTime": 1680148920000,
         "openTimeISO": "2023-03-30T04:02:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
                  "name":"ApproximateAgeOfOldestMessage",
                  "namespace":"AWS/SQS",
                  "period":"60",
                  "stat":"Maximum",
                  "unit":"None",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        },
   }
}
```

# Insight fechado

As notificações de insights fechados contêm as seguintes informações:

```
{
"accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"CLOSED_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "DynamoDB table writes are under utilized in mock-stack",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription":"DynamoDB table writes are under utilized",
```

```
    "insightSeverity":"medium",
    "startTime": 1670612400000,
    "startTimeISO": "2022-12-09T19:00:00Z",
    "endTime": 1679994000000,
    "endTimeISO": "2023-03-28T09:00:00Z",
    "anomalies":[
       {
          "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
          "startTime": 1665428400000,
          "startTimeISO": "2022-10-10T19:00:00Z",
          "endTime": 1679986800000,
          "endTimeISO": "2023-03-28T07:00:00Z",
          "openTime": 1670612400000,
          "openTimeISO": "2022-12-09T19:00:00Z",
          "closeTime": 1679994000000,
          "closeTimeISO": "2023-03-28T09:00:00Z",
          "description":"Empty receives while messages are available",
          "anomalyResources":[
             {
                "type":"AWS::SQS::Queue",
                "name":"SampleQueue"
             }
          ],
          "sourceDetails":[
             {
                "dataSource":"CW_METRICS",
                "dataIdentifiers":{
                "name":"NumberOfEmptyReceives",
                   "namespace":"AWS/SQS",
                   "period":"60",
                   "stat":"Sum",
                   "unit":"COUNT",
                   "dimensions":"{\"QueueName\":\"SampleQueue\"}"
                }
             }
           ],
         "associatedResourceArn": [
             "arn:aws:sqs:us-east-1:123456789101:SampleQueue"
         ]
       }
    ],
    "resourceCollection":{
         "cloudFormation":{
             "stackNames":[
```

```
                "SampleApplication"
            ]
        }
    }
}
```

# Nova associação

As notificações de novas associações contêm as seguintes informações:

```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_ASSOCIATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-GetOneFunction duration due to increased number of
 invocations",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-GetOneFunction had\nan increased duration anomaly possibly
 caused by the Lambda function invocation increase. DevOps Guru has detected this is a
 repeated insight. DevOps Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680127200000,
   "startTimeISO": "2023-03-29T22:00:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime":1672945500000,
         "startTimeISO": "2023-03-29T22:00:00Z",
         "openTime": 1680127740000,
         "openTimeISO": "2023-03-29T22:09:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
               "namespace":"AWS/SQS",
                  "name":"ApproximateAgeOfOldestMessage",
                  "stat":"Maximum",
                  "unit":"None",
```

```
                  "period":"60",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

# Nova recomendação

As notificações de novas recomendações contêm as seguintes informações:

```
{
   "accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"NEW_RECOMMENDATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "Recreation of AWS SDK Service Clients",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription": "Usually for a given service you can create one [AWS SDK
 service client](https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/creating-
clients.html) and reuse that client across your entire service.\n\nWhen instead you
 create a new AWS SDK service client for each call (e.g. for DynamoDB) it\u0027s
 generally a waste of CPU time.",
   "insightSeverity":"medium",
   "startTime": 1680125893576,
   "startTimeISO": "2023-03-29T21:38:13.576Z",
   "recommendations":[
      {
         "name":"Tune Availability Zones of your Lambda Function",
```

```
        "description":"Based on your configurations, we recommend that you set
 SampleFunction to be deployed in at least 3 Availability Zones to maintain Multi
 Availability Zone Redundancy.",
        "reason":"Lambda Function SampleFunction is currently only deployed to 2
 unique Availability zones in a region with 7 total Availability zones.",
        "link":"https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html",
        "relatedAnomalies":[
           {
              "sourceDetails":{
                   "cloudWatchMetrics":null
              },
              "resources":[
                 {
                    "name":"SampleFunction",
                    "type":"AWS::Lambda::Function"
                 }
              ],
              "associatedResourceArns": [
                 "arn:aws:lambda:arn:123456789101:SampleFunction"
              ]
           }
        ]
     }
  ],
  "resourceCollection": {
       "cloudFormation": {
       "stackNames":[
           "SampleApplication"
        ]
     }
  }
}
```

# Gravidade atualizada

As notificações de atualizações de gravidade contêm as seguintes informações:

```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"SEVERITY_UPGRADED",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
```

```
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-11",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
   "insightType":"REACTIVE",
   "insightDescription": "DevOps Guru has detected this is a repeated insight. DevOps
 Guru will treat future occurrences of this insight as 'Low Severity' for the next 7
 days.",
   "insightSeverity":"high",
   "startTime": 1680127320000,
   "startTimeISO": "2023-03-29T22:02:00Z",
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

# Falha na validação de recursos

Você pode usar AWS CloudFormation pilhas e AWS tags para filtrar e identificar os AWS recursos que você deseja que o DevOps Guru analise. Quando você escolhe uma pilha ou tag inválida para o DevOps Guru identificar recursos, o DevOps Guru cria uma notificação. `SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE` Isso pode acontecer quando a tag ou o nome da pilha que você especifica não tem recursos associados a ela. Para aproveitar ao máximo os métodos de filtragem do DevOps Guru, escolha pilhas e tags que tenham recursos associados a elas.

```
{
    "accountId":"123456789101",
    "region":"eu-west-1",
    "messageType":"SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE",
    "ResourceFilterType": "Tags",
    "InvalidResourceNames": [
         "Devops-Guru-tag-key-tag-value"
    ],
    "awsInsightSource": "aws.devopsguru"
}
```

# Visualizando recursos analisados pelo DevOps Guru

DevOpsO Guru fornece uma lista de nomes de recursos e seus limites de aplicativos em análise usando a `ListMonitoredResources` ação. Essas informações são coletadas da Amazon CloudWatch e de outros AWS serviços usando a função vinculada ao serviço DevOps Guru. AWS CloudTrail

Observe que, mesmo que um usuário não tenha permissão explícita para acessar o APIs de outro serviço, como AWS Lambda o Amazon RDS, o DevOps Guru ainda fornece uma lista de recursos desse serviço, desde que a `ListMonitoredResources` ação seja permitida.

Tópicos


- Atualizando sua cobertura AWS de análise no DevOps Guru
- Remover a visualização de recursos analisados para usuários


## Atualizando sua cobertura AWS de análise no DevOps Guru

Você pode atualizar quais AWS recursos em sua conta o DevOps Guru analisa. Os recursos analisados compõem o limite de cobertura do DevOps Guru. Quando você especifica o limite, seus recursos são agrupados em aplicativos. Você tem quatro opções de cobertura limite.

- Escolha que o DevOps Guru analise todos os recursos suportados em sua conta. Todos os recursos da sua conta que estão em uma pilha são agrupados em um aplicativo. Se você tiver várias pilhas em sua conta, os recursos de cada pilha formarão seu próprio aplicativo. Se algum recurso de sua conta não estiver em uma pilha, ele será agrupado em um aplicativo próprio.
- Especifique os recursos escolhendo AWS CloudFormation pilhas que definem esses recursos. Se você fizer isso, o DevOps Guru analisará cada recurso especificado nas pilhas que você escolher. Se um recurso de sua conta não for definido por uma pilha que você escolher, ele não será analisado. Para mais informações, consulte Como trabalhar com pilhas no Guia do usuário do AWS CloudFormation e Determine a cobertura para o DevOps Guru.
- Especifique os recursos usando AWS tags. DevOpsO Guru analisa todos os recursos em sua conta e região ou todos os recursos que contêm a chave de tag que você escolher. Os recursos são agrupados com base nos valores de tag selecionados. Para obter mais informações, consulte Usando tags para identificar recursos em seus aplicativos DevOps Guru.
- Especifique que nenhum recurso seja analisado para que você pare de incorrer em cobranças decorrentes da análise de recursos.

> **Note**
>
> Se você atualizar sua cobertura para parar de analisar recursos, poderá continuar incorrendo em pequenas cobranças se analisar os insights existentes gerados pelo DevOps Guru no passado. Essas cobranças estão associadas às chamadas de API usadas para recuperar e exibir informações de insights. Para obter mais informações, consulte os preços do Amazon DevOps Guru.

DevOpsO Guru oferece suporte a todos os recursos associados aos serviços suportados. Para obter mais informações sobre os serviços e recursos suportados, consulte os preços do Amazon DevOps Guru.

Para gerenciar sua cobertura de análise do DevOps Guru

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.
2. Expanda Recursos analisados no painel de navegação.
3. Escolha Editar.
4. Escolha uma das seguintes opções de cobertura.

   - Escolha Todos os recursos da conta se quiser que o DevOps Guru analise todos os recursos suportados em sua AWS conta e região. Se você escolher essa opção, sua AWS conta será o limite de cobertura da análise de recursos. Todos os recursos de cada pilha da sua conta são agrupados em um aplicativo próprio. Todos os recursos restantes que não estão em uma pilha são agrupados em um aplicativo próprio.
   - Escolha CloudFormation pilhas se quiser que o DevOps Guru analise os recursos que estão nas pilhas que você escolher e, em seguida, escolha uma das opções a seguir.
     - Todos os recursos: todos os recursos que estão em pilhas na sua conta são analisados. Os recursos em cada pilha são agrupados em seu próprio aplicativo. Os recursos em sua conta que não estejam em uma pilha não são analisados.
     - Selecionar pilhas — Selecione as pilhas que você deseja que o DevOps Guru analise. Os recursos em cada pilha que você seleciona são agrupados em seu próprio aplicativo. Você pode inserir o nome de uma pilha em Localizar pilhas para localizar rapidamente uma pilha específica. Você pode selecionar até 1.000 pilhas.

Para obter mais informações, consulte Usando AWS CloudFormation pilhas para identificar recursos em seus aplicativos DevOps Guru.

- Escolha Tags se quiser que o DevOps Guru analise todos os recursos que contêm as tags que você escolher. Escolha uma chave e depois uma das seguintes opções.
  - Todos os recursos da conta: analise todos os recursos na região e na conta atuais. Os recursos com a chave de tag selecionada são agrupados por valor de tag, se houver. Os recursos sem essa chave de tag são agrupados e analisados separadamente.
  - Escolha valores de tag específicos — Todos os recursos que contêm uma tag com a chave que você escolheu são analisados. DevOpsO Guru agrupa seus recursos em aplicativos de acordo com os valores da sua tag.

  Para obter mais informações, consulte Usando tags para identificar recursos em seus aplicativos DevOps Guru.
- Escolha Nenhum se você não quiser que o DevOps Guru analise nenhum recurso. Essa opção desativa o DevOps Guru para que você pare de incorrer em cobranças decorrentes da análise de recursos.

5. Escolha Salvar.

## Remover a visualização de recursos analisados para usuários

Mesmo que um usuário não tenha permissão explícita para acessar o APIs de outro serviço, como Lambda ou Amazon RDS DevOps, o Guru ainda fornece uma lista de recursos desse serviço, desde que a ação seja permitida. `ListMonitoredResources` Para mudar esse comportamento, você pode atualizar sua política AWS do IAM para negar essa ação.

```
{
            "Sid": "DenyListMonitoredResources",
            "Effect": "Deny",
            "Action": [
                "devops-guru:ListMonitoredResources"
            ]
}
```

# Melhores práticas no DevOps Guru

As melhores práticas a seguir podem ajudar você a entender, diagnosticar e corrigir comportamentos anômalos detectados pelo Amazon Guru. DevOps Use as melhores práticas Entendendo os insights no console do DevOps Guru para resolver problemas operacionais detectados pelo DevOps Guru.

- Na visualização do cronograma de um insight, veja primeiro os indicadores destacados. Eles geralmente são indicadores-chave do problema.
- Use CloudWatch a Amazon para visualizar métricas que ocorreram imediatamente antes da primeira métrica destacada em um insight para identificar quando e como o comportamento mudou. Vocês podem me ajudar a diagnosticar o problema?
- Para recursos do Amazon RDS, veja os indicadores do Performance Insights. Ao correlacionar os indicadores do contador com a carga do banco de dados, você pode obter informações detalhadas sobre problemas de desempenho. Para obter mais informações, consulte Análise de anomalias de desempenho com o DevOps Guru para Amazon RDS.
- Muitas vezes, várias dimensões do mesmo indicador podem ser anômalas. Veja as dimensões na exibição gráfica para obter uma compreensão mais profunda do problema.
- Veja na seção de eventos de um insight os eventos de implantação ou infraestrutura que aconteceram na época em que o insight foi criado. Saber quais eventos ocorreram quando o comportamento anômalo de um insight aconteceu pode ajudá-lo a entender e diagnosticar o problema.
- Procure tíquetes em seu sistema operacional que aconteceram no mesmo momento em busca de pistas.
- Em uma visão geral, leia as recomendações e acesse os links nas recomendações. Eles geralmente têm etapas de solução de problemas que podem ajudá-lo a diagnosticar e resolver problemas rapidamente.
- Não ignore os insights resolvidos, a menos que você já tenha resolvido o problema. Uma vez por dia, analise novos insights, mesmo que tenham sido resolvidos. Tente entender a causa raiz por trás do maior número de insights possível. Procure um padrão que possa ser o sinal de um problema sistêmico. Se um problema sistêmico não for resolvido, ele poderá causar problemas mais sérios no futuro. Corrigir problemas transitórios agora pode ajudar a evitar incidentes futuros e mais sérios.

# Segurança no Amazon DevOps Guru

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon DevOps Guru, consulte AWS Services in Scope by Compliance Program .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o DevOps Guru. Os tópicos a seguir mostram como configurar o DevOps Guru para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros serviços da AWS que ajudam você a monitorar e proteger seus recursos do DevOps Guru.

Tópicos


- Proteção de dados no Amazon DevOps Guru
- Identity and Access Management para Amazon DevOps Guru
- DevOpsGuru de registro e monitoramento
- DevOpsGuru e interface VPC endpoints ()AWS PrivateLink
- Segurança de infraestrutura em DevOps Guru
- Resiliência no Amazon DevOps Guru

# Proteção de dados no Amazon DevOps Guru

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no Amazon DevOps Guru. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Data Privacy FAQ. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o DevOps Guru ou outro Serviços da AWS usando o console, a API ou AWS SDKs. AWS CLI Quaisquer dados inseridos em tags ou em campos de texto de formato livre

usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

## Criptografia de dados no DevOps Guru

A criptografia é uma parte importante da segurança do DevOps Guru. Algumas criptografias, como aquelas de dados em trânsito, são fornecidas por padrão e não requerem qualquer ação por parte do cliente. Outras criptografias, como aquelas de dados em repouso, podem ser configuradas durante a criação ou compilação do projeto.

- Criptografia de dados em trânsito: toda a comunicação entre clientes e o DevOps Guru e entre o DevOps Guru e suas dependências posteriores é protegida usando TLS e autenticada usando o processo de assinatura Signature Version 4. Todos os endpoints do DevOps Guru usam certificados gerenciados por. AWS Private Certificate Authority Para obter mais informações, consulte Processo de assinatura do Signature versão 4 e O que é o ACM PCA?.
- Criptografia de dados em repouso: para todos os AWS recursos analisados pelo DevOps Guru, as CloudWatch métricas, os dados, os recursos e os AWS CloudTrail eventos da Amazon são armazenados usando o Amazon S3 IDs, o Amazon DynamoDB e o Amazon Kinesis. Se AWS CloudFormation as pilhas forem usadas para definir os recursos analisados, os dados da pilha também serão coletados. DevOpsO Guru usa as políticas de retenção de dados do Amazon S3, DynamoDB e Kinesis. Os dados armazenados no Kinesis podem ser retidos por até um ano, dependendo das políticas definidas. Os dados armazenados no Amazon S3 e no DynamoDB são armazenados por um ano.

  Os dados armazenados são criptografados usando os recursos de data-at-rest criptografia do Amazon S3, do DynamoDB e do Kinesis.

  Chaves gerenciadas pelo cliente: o DevOps Guru oferece suporte à criptografia de conteúdo do cliente e metadados confidenciais, como anomalias de registro geradas a partir de CloudWatch registros com chaves gerenciadas pelo cliente. Esse recurso oferece a opção de adicionar uma camada de segurança autogerenciada para ajudar você a atender aos requisitos regulatórios e de conformidade da sua organização. Para obter informações sobre como habilitar chaves gerenciadas pelo cliente em suas configurações do DevOps Guru, consultethe section called “Atualizar a criptografia”.

  Como você tem controle total dessa camada de criptografia, você pode realizar tarefas como:

  - Estabelecer e manter as políticas de chave

- Estabelecer e manter subsídios e IAM policies
- Habilitar e desabilitar políticas de chaves
- Alternar os materiais de criptografia de chave
- Adicionar etiquetas
- Criar réplicas de chaves
- Chaves de agendamento para exclusão

Para obter mais informações, consulte Chaves gerenciadas pelo cliente no Guia do AWS Key Management Service desenvolvedor.

> **Note**
>
> DevOpsO Guru ativa automaticamente a criptografia em repouso usando chaves AWS próprias para proteger metadados confidenciais sem nenhum custo. No entanto, AWS KMS cobranças são cobradas pelo uso de uma chave gerenciada pelo cliente. Para obter mais informações sobre preços, consulte os AWS Key Management Service preços.

## Como o DevOps Guru usa subsídios em AWS KMS

DevOpsO Guru exige uma concessão para usar sua chave gerenciada pelo cliente.

Quando você opta por habilitar a criptografia com uma chave gerenciada pelo cliente, o DevOps Guru cria uma concessão em seu nome enviando uma CreateGrant solicitação para AWS KMS. As concessões AWS KMS são usadas para dar ao DevOps Guru acesso a uma AWS KMS chave na conta de um cliente.

DevOpsO Guru exige que a concessão use sua chave gerenciada pelo cliente para as seguintes operações internas:

- Envie DescribeKey solicitações para verificar se AWS KMS a ID simétrica da chave KMS gerenciada pelo cliente inserida ao criar um rastreador ou uma coleção de cercas geográficas é válida.
- Envie GenerateDataKey solicitações AWS KMS para gerar chaves de dados criptografadas pela chave gerenciada pelo cliente.
- Envie solicitações de descriptografia para AWS KMS descriptografar as chaves de dados criptografadas para que elas possam ser usadas para criptografar seus dados.

É possível revogar o acesso à concessão, ou remover o acesso do serviço à chave gerenciada pelo cliente a qualquer momento. Se você fizer isso, o DevOps Guru não poderá acessar nenhum dos dados criptografados pela chave gerenciada pelo cliente, o que afeta as operações que dependem desses dados. Por exemplo, se você tentar obter informações criptografadas de anomalias de log que o DevOps Guru não consegue acessar, a operação retornará um AccessDeniedException erro.

## Monitorando suas chaves de criptografia no DevOps Guru

Ao usar uma chave gerenciada pelo AWS KMS cliente com seus recursos do DevOps Guru, você pode usar AWS CloudTrail nossos CloudWatch registros para rastrear solicitações enviadas pelo DevOps Guru. AWS KMS

## Criar uma chave gerenciada pelo cliente

Você pode criar uma chave simétrica gerenciada pelo cliente usando o AWS Management Console ou o. AWS KMS APIs

Para criar uma chave gerenciada pelo cliente, consulte Como criar chaves KMS de criptografia simétrica.

### Política de chave

As políticas de chaves controlam o acesso à chave gerenciada pelo cliente. Cada chave gerenciada pelo cliente deve ter exatamente uma política de chaves, que contém declarações que determinam quem pode usar a chave e como pode usá-la. Ao criar a chave gerenciada pelo cliente, é possível especificar uma política de chave. Para obter mais informações, consulte Autenticação e controle de acesso AWS KMS no Guia do AWS Key Management Service desenvolvedor.

Para usar sua chave gerenciada pelo cliente com seus recursos do DevOps Guru, as seguintes operações de API devem ser permitidas na política de chaves:

- `kms:CreateGrant`: adiciona uma concessão a uma chave gerenciada pelo cliente. Concede acesso de controle a uma AWS KMS chave especificada, o que permite o acesso às operações de concessão exigidas pelo DevOps Guru. Para obter mais informações sobre o uso de subsídios, consulte o Guia do AWS Key Management Service desenvolvedor.

Isso permite que o DevOps Guru faça o seguinte:

- Ligue GenerateDataKey para gerar uma chave de dados criptografada e armazená-la, porque a chave de dados não é usada imediatamente para criptografar.

- Chamar o Decrypt para usar a chave de dados criptografada armazenada para acessar dados criptografados.
- Configure uma entidade principal aposentada para permitir que o serviço para RetireGrant.
- Use kms: DescribeKey para fornecer detalhes da chave gerenciada pelo cliente para permitir que o DevOps Guru valide a chave.

A declaração a seguir inclui exemplos de declarações de política que você pode adicionar ao DevOps Guru:

```
"Statement" : [
  {
    "Sid" : "Allow access to principals authorized to use DevOps Guru",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [
      "kms:DescribeKey",
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "devops-guru.Region.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
      }
  },
  {
    "Sid": "Allow access for key administrators",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
     },
    "Action" : [
      "kms:*"
     ],
    "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
  },
  {
    "Sid" : "Allow read-only access to key metadata to the account",
    "Effect" : "Allow",
```

```
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:root"
      },
      "Action" : [
        "kms:Describe*",
        "kms:Get*",
        "kms:List*"
      ],
      "Resource" : "*"
    }
  ]
```

## Privacidade do tráfego

Você pode melhorar a segurança de sua análise de recursos e geração de insights configurando o DevOps Guru para usar uma interface VPC endpoint. Para fazer isso, você não precisa de um gateway da Internet, de um dispositivo NAT ou de um gateway privado virtual. Também não é necessário configurá-lo PrivateLink, embora seja recomendado. Para obter mais informações, consulte DevOpsGuru e interface VPC endpoints ()AWS PrivateLink. Para obter mais informações sobre endpoints de VPC, consulte PrivateLink e AWS PrivateLinkComo acessar os serviços da AWS por meio de. PrivateLink

# Identity and Access Management para Amazon DevOps Guru

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do DevOps Guru. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticação com identidades
- Gerenciar o acesso usando políticas
- DevOpsAtualizações do Guru para políticas AWS gerenciadas e funções vinculadas a serviços
- Como o Amazon DevOps Guru funciona com o IAM

- Políticas baseadas em identidade para o Amazon Guru DevOps
- Usando funções vinculadas a serviços para o Guru DevOps
- Referência de permissões do Amazon DevOps Guru
- permissões para os tópicos do Amazon SNS
- Permissões para tópicos AWS KMS criptografados do Amazon SNS
- Solução de problemas de identidade e acesso ao Amazon DevOps Guru

## Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no DevOps Guru.

Usuário do serviço — Se você usa o serviço DevOps Guru para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do DevOps Guru para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador. Se você não conseguir acessar um recurso no DevOps Guru, consulteSolução de problemas de identidade e acesso ao Amazon DevOps Guru.

Administrador de serviços — Se você é responsável pelos recursos do DevOps Guru em sua empresa, provavelmente tem acesso total ao DevOps Guru. É seu trabalho determinar quais recursos e recursos do DevOps Guru seus usuários do serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar o IAM com o DevOps Guru, consulteComo o Amazon DevOps Guru funciona com o IAM.

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao DevOps Guru. Para ver exemplos de políticas baseadas em identidade do DevOps Guru que você pode usar no IAM, consulte. Políticas baseadas em identidade para o Amazon Guru DevOps

## Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator da AWS no IAM no Guia do usuário do IAM.

### Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do Usuário do IAM.

### Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, é recomendável usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Guia do Usuário do AWS IAM Identity Center .

## Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso para usuários do IAM no Guia do usuário do IAM.

## Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode alternar de um usuário para uma função do IAM (console). Você pode assumir uma função chamando uma

operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Guia do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados a serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia do usuário do IAM.

## Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

### Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

### Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

### Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o AWS WAF Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

## Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.
- Políticas de controle de recursos (RCPs) — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do

usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

### Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

## DevOpsAtualizações do Guru para políticas AWS gerenciadas e funções vinculadas a serviços

Veja detalhes sobre atualizações nas políticas AWS gerenciadas e na função vinculada ao serviço do DevOps Guru desde que esse serviço começou a rastrear essas mudanças. Para alertas automáticos sobre mudanças nesta página, assine o feed RSS do DevOps GuruHistórico de documentos do Amazon DevOps Guru.

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonDevOpsGuruConsoleFullAccess - Atualizar para uma política existente | A política gerenciada pelo `AmazonDevOpsGuruFullAccess` agora oferece suporte às assinaturas do Amazon SNS. | 9 de agosto de 2023 |
| AmazonDevOpsGuruReadOnlyAccess: atualização para uma política existente | A política gerenciada pelo `AmazonDevOpsGuruReadOnlyAccess` agora é compatível com acesso somente leitura às listas de assinatura do Amazon SNS. | 9 de agosto de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonDevOpsGuruServiceRolePolicy: atualizar para uma política existente. | A função `AWSServiceRoleForDevOpsGuru` vinculada ao serviço agora dá suporte ao acesso às ações GET do API Gateway em REST. APIs | 11 de janeiro de 2023 |
| AmazonDevOpsGuruServiceRolePolicy: atualizar para uma política existente. | A função vinculada ao serviço do `AWSServiceRoleForDevOpsGuru` agora oferece suporte a várias ações do Amazon Simple Storage Service e Service Quotas. | 19 de outubro de 2022 |
| AmazonDevOpsGuruFullAccess: atualização para uma política existente | A política gerenciada `AmazonDevOpsGuruFullAccess` . agora oferece suporte ao acesso à CloudWatch `FilterLogEvents` ação. | 30 de agosto de 2022 |
| AmazonDevOpsGuruConsoleFullAccess: atualização para uma política existente | A política `AmazonDevOpsGuruConsoleFullAccess` gerenciada agora dá suporte ao acesso à CloudWatch `FilterLogEvents` ação. | 30 de agosto de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonDevOpsGuruReadOnlyAccess: atualização para uma política existente | A política `AmazonDevOpsGuruReadOnlyAccess` gerenciada agora oferece suporte ao acesso somente de leitura à ação CloudWatch `FilterLogEvents` . | 30 de agosto de 2022 |
| AmazonDevOpsGuruServiceRolePolicy: atualizar para uma política existente. | A função `AWSServiceRoleForDevOpsGuru` vinculada ao serviço agora oferece suporte às ações de CloudWatch registros `FilterLogEvents` `DescribeLogGroups` , e. `DescribeLogStreams` | 12 de julho de 2022 |
| Políticas baseadas em identidade para o DevOps Guru — Nova política gerenciada. | A política `AmazonDevOpsGuruConsoleFullAccess` foi adicionada. | 16 de dezembro de 2021 |
| AmazonDevOpsGuruServiceRolePolicy: atualizar para uma política existente. | A função vinculada ao serviço do `AWSServiceRoleForDevOpsGuru` agora dá suporte a ações do Performance Insights `DescribeMetricsKeys` e do Amazon RDS `DescribeDBInstances` . | 1º de dezembro de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonDevOpsGuruReadOnlyAccess: atualização para uma política existente | A política gerenciada pelo `AmazonDevOpsGuruReadOnlyAccess` agora dá suporte ao acesso somente leitura às ações do Amazon RDS `DescribeDBInstances` . | 1º de dezembro de 2021 |
| AmazonDevOpsGuruFullAccess: atualização para uma política existente | A política gerenciada pelo `AmazonDevOpsGuruFullAccess` agora dá suporte com o acesso às ações do Amazon RDS do `DescribeDBInstances` . | 1º de dezembro de 2021 |
| Políticas baseadas em identidade para o Amazon Guru DevOps: nova política adicionada. | A função vinculada ao serviço do `AWSServiceRoleForDevOpsGuru` agora dá suporte ao acesso às ações do Amazon RDS `DescribeDBInstances` e do Performance Insights `GetResourceMetrics` .<br><br>A política `AmazonDevOpsGuruOrganizationsAccess` gerenciada fornece acesso ao DevOps Guru dentro de uma organização. | 16 de novembro de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonDevOpsGuruServiceRolePolicy: atualizar para uma política existente. | A função vinculada ao serviço do `AWSServiceRoleForDevOpsGuru` agora dá suporte ao AWS Organizations. | 4 de novembro de 2021 |
| AmazonDevOpsGuruServiceRolePolicy: atualizar para uma política existente. | A função vinculada ao serviço do `AWSServiceRoleForDevOpsGuru` agora contém novas condições nas ações `ssm:CreateOpsItem` e `ssm:AddTagsToResource`. | 11 de outubro de 2021 |
| Permissões de função vinculadas ao serviço para o Guru DevOps: atualizar para uma política existente. | A função vinculada ao serviço do `AWSServiceRoleForDevOpsGuru` agora contém novas condições nas ações `ssm:CreateOpsItem` e `ssm:AddTagsToResource`. | 14 de junho de 2021 |
| AmazonDevOpsGuruReadOnlyAccess: atualização para uma política existente | A política `AmazonDevOpsGuruReadOnlyAccess` gerenciada agora permite acesso somente para leitura às ações AWS Identity and Access Management `GetRole` e ao DevOps Guru `DescribeFeedback`. | 14 de junho de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonDevOpsGuruReadOnlyAccess: atualização para uma política existente | A política `AmazonDevOpsGuruReadOnlyAccess` gerenciada agora permite acesso somente de leitura ao DevOps Guru e às ações `GetCostEstimation` . `StartCostEstimation` | 27 de abril de 2021 |
| AmazonDevOpsGuruServiceRolePolicy - Atualizar para uma política existente | A `AWSServiceRoleForDevOpsGuru` função agora permite acesso às ações AWS Systems Manager `AddTagsToResource` e ao Amazon EC2 Auto Scaling. `DescribeAutoScalingGroups` | 27 de abril de 2021 |
| DevOpsO Guru começou a monitorar as mudanças | DevOpsO Guru começou a monitorar as mudanças em suas políticas AWS gerenciadas. | 10 de dezembro de 2020 |

## Como o Amazon DevOps Guru funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao DevOps Guru, saiba quais recursos do IAM estão disponíveis para uso com o DevOps Guru.

Recursos do IAM que você pode usar com o Amazon DevOps Guru

| Recurso do IAM | DevOpsSuporte do Guru |
| --- | --- |
| Políticas baseadas em identidade | Sim |

| Recurso do IAM | DevOpsSuporte do Guru |
| --- | --- |
| Políticas baseadas em recurso | Não |
| Ações de políticas | Sim |
| Recursos de políticas | Sim |
| Chaves de condição de políticas | Sim |
| ACLs | Não |
| ABAC (tags em políticas) | Não |
| Credenciais temporárias | Sim |
| Permissões de entidade principal | Sim |
| Perfis de serviço | Não |
| Funções vinculadas ao serviço | Sim |

Para ter uma visão de alto nível de como o DevOps Guru e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

## Políticas baseadas em identidade para o Guru DevOps

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem

ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para o Guru DevOps

Para ver exemplos de políticas baseadas em identidade do DevOps Guru, consulte. Políticas baseadas em identidade para o Amazon Guru DevOps

## Políticas baseadas em recursos dentro do Guru DevOps

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

## Ações políticas para o DevOps Guru

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do DevOps Guru, consulte Ações definidas pelo Amazon DevOps Guru na Referência de autorização de serviço.

As ações políticas no DevOps Guru usam o seguinte prefixo antes da ação:

```
aws
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [
      "aws:action1",
      "aws:action2"
         ]
```

Para ver exemplos de políticas baseadas em identidade do DevOps Guru, consulte. Políticas baseadas em identidade para o Amazon Guru DevOps

## Recursos políticos para o DevOps Guru

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do DevOps Guru e seus ARNs, consulte Recursos definidos pelo Amazon DevOps Guru na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo Amazon DevOps Guru.

Para ver exemplos de políticas baseadas em identidade do DevOps Guru, consulte. Políticas baseadas em identidade para o Amazon Guru DevOps

## Chaves de condições de política para o DevOps Guru

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do DevOps Guru, consulte Chaves de condição do Amazon DevOps Guru na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo Amazon DevOps Guru.

Para ver exemplos de políticas baseadas em identidade do DevOps Guru, consulte. Políticas baseadas em identidade para o Amazon Guru DevOps

## Listas de controle de acesso (ACLs) no DevOps Guru

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

## Controle de acesso baseado em atributos (ABAC) com o Guru DevOps

Oferece compatibilidade com ABAC (tags em políticas): não

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

## Usando credenciais temporárias com DevOps o Guru

Compatível com credenciais temporárias: sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS "Trabalhe com o IAM" no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil do IAM (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

## Permissões principais entre serviços para DevOps o Guru

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

## Funções de serviço para o DevOps Guru

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper a funcionalidade do DevOps Guru. Edite as funções de serviço somente quando o DevOps Guru fornecer orientação para fazer isso.

### Funções vinculadas a serviços para o Guru DevOps

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

## Políticas baseadas em identidade para o Amazon Guru DevOps

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do DevOps Guru. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo DevOps Guru, incluindo o formato de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para o Amazon DevOps Guru na Referência de autorização de serviço. ARNs

Tópicos

- Práticas recomendadas de política
- Usando o console do DevOps Guru
- Permitir que os usuários visualizem suas próprias permissões
- Políticas gerenciadas (predefinidas) pela AWS para DevOps o Guru

## Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do DevOps Guru em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.

- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

## Usando o console do DevOps Guru

Para acessar o console do Amazon DevOps Guru, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do DevOps Guru em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console do DevOps Guru, anexe também o DevOps Guru `AmazonDevOpsGuruReadOnlyAccess` ou a política `AmazonDevOpsGuruFullAccess` AWS gerenciada às entidades. Para obter informações, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

## Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

## Políticas gerenciadas (predefinidas) pela AWS para DevOps o Guru

AWS aborda muitos casos de uso comuns fornecendo políticas autônomas do IAM que são criadas e administradas pela AWS. Essas políticas AWS gerenciadas concedem as permissões necessárias para casos de uso comuns, para que você não precise investigar quais permissões são necessárias. Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

Para criar e gerenciar funções de serviço do DevOps Guru, você também deve anexar a política AWS gerenciada chamada. `IAMFullAccess`

Você também pode criar suas próprias políticas personalizadas do IAM para permitir permissões para ações e recursos do DevOps Guru. Você pode anexar essas políticas personalizadas a usuários ou grupos do que exijam essas permissões.

As políticas AWS gerenciadas a seguir, que você pode anexar aos usuários em sua conta, são específicas do DevOps Guru.

Tópicos

- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruOrganizationsAccess

### AmazonDevOpsGuruFullAccess

`AmazonDevOpsGuruFullAccess`— Fornece acesso total ao DevOps Guru, incluindo permissões para criar tópicos do Amazon SNS, acessar métricas da CloudWatch Amazon e AWS CloudFormation acessar pilhas. Aplique isso somente aos usuários de nível administrativo aos quais você deseja conceder controle total sobre o Guru. DevOps

A política `AmazonDevOpsGuruFullAccess` contém a seguinte declaração.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
```

```
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruConsoleFullAccess

`AmazonDevOpsGuruConsoleFullAccess`— Fornece acesso total ao DevOps Guru, incluindo permissões para criar tópicos do Amazon SNS, acessar métricas da CloudWatch Amazon e AWS CloudFormation acessar pilhas. Essa política tem permissões adicionais de insights de desempenho para que você possa visualizar análises detalhadas relacionadas a instâncias anômalas do banco de dados Aurora do Amazon RDS no console. Aplique isso somente aos usuários de nível administrativo aos quais você deseja conceder controle total sobre o Guru. DevOps

A política `AmazonDevOpsGuruConsoleFullAccess` contém a seguinte declaração.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "devops-guru:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
```

```
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PerformanceInsightsMetricsDataAccess",
            "Effect": "Allow",
            "Action": [
                "pi:GetResourceMetrics",
                "pi:DescribeDimensionKeys"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
```

```
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruReadOnlyAccess

`AmazonDevOpsGuruReadOnlyAccess`— Concede acesso somente para leitura ao DevOps Guru e recursos relacionados em outros serviços. AWS Aplique essa política aos usuários aos quais você deseja conceder a capacidade de visualizar insights, mas não de fazer nenhuma atualização no limite de cobertura de análise do DevOps Guru, nos tópicos do Amazon SNS ou na integração com o Systems Manager. OpsCenter

A política `AmazonDevOpsGuruReadOnlyAccess` contém a seguinte declaração.

```
    {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:DescribeAccountHealth",
                "devops-guru:DescribeAccountOverview",
                "devops-guru:DescribeAnomaly",
                "devops-guru:DescribeEventSourcesConfig",
                "devops-guru:DescribeFeedback",
                "devops-guru:DescribeInsight",
                "devops-guru:DescribeResourceCollectionHealth",
                "devops-guru:DescribeServiceIntegration",
                "devops-guru:GetCostEstimation",
                "devops-guru:GetResourceCollection",
                "devops-guru:ListAnomaliesForInsight",
                "devops-guru:ListEvents",
                "devops-guru:ListInsights",
                "devops-guru:ListAnomalousLogGroups",
                "devops-guru:ListMonitoredResources",
                "devops-guru:ListNotificationChannels",
```

```
                "devops-guru:ListRecommendations",
                "devops-guru:SearchInsights",
                "devops-guru:StartCostEstimation"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
```

```
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruOrganizationsAccess

`AmazonDevOpsGuruOrganizationsAccess`— Fornece aos administradores do Organizations acesso à visualização de várias contas do DevOps Guru em uma organização. Aplique essa política aos usuários de nível administrativo da sua organização para os quais você deseja conceder acesso total ao DevOps Guru dentro de uma organização. Você pode aplicar essa política na conta de gerenciamento da sua organização e na conta de administrador delegado do DevOps Guru. Você pode se inscrever `AmazonDevOpsGuruReadOnlyAccess` ou, `AmazonDevOpsGuruFullAccess` em adição a esta política, fornecer acesso somente para leitura ou acesso total ao DevOps Guru.

A política `AmazonDevOpsGuruOrganizationsAccess` contém a seguinte declaração.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDevOpsGuruOrganizationsAccess",
   "Effect": "Allow",
   "Action": [
    "devops-guru:DescribeOrganizationHealth",
    "devops-guru:DescribeOrganizationResourceCollectionHealth",
    "devops-guru:DescribeOrganizationOverview",
```

```
    "devops-guru:ListOrganizationInsights",
    "devops-guru:SearchOrganizationInsights"
   ],
   "Resource": "*"
  },
  {
   "Sid": "OrganizationsDataAccess",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListAccounts",
    "organizations:ListChildren",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListRoots"
   ],
   "Resource": "arn:aws:organizations::*:"
  },
  {
   "Sid": "OrganizationsAdminDataAccess",
   "Effect": "Allow",
   "Action": [
    "organizations:DeregisterDelegatedAdministrator",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "devops-guru.amazonaws.com"
     ]
    }
   }
  }
 ]
}
```

# Usando funções vinculadas a serviços para o Guru DevOps

O Amazon DevOps Guru usa funções AWS Identity and Access Management vinculadas a serviços (IAM). Uma função vinculada a serviços é um tipo exclusivo de função do IAM vinculada diretamente ao DevOps Guru. As funções vinculadas ao serviço são predefinidas pelo DevOps Guru e incluem todas as permissões que o serviço exige para chamar a AWS CloudTrail Amazon CloudWatch,, e o AWS X-Ray AWS Organizations em seu nome. AWS CodeDeploy

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

Você só pode excluir um perfil vinculado a serviço depois de excluir os recursos relacionados. Isso protege seus recursos do DevOps Guru porque você não pode remover inadvertidamente a permissão para acessar os recursos.

## Permissões de função vinculadas ao serviço para o Guru DevOps

DevOpsO Guru usa a função vinculada ao serviço chamada. `AWSServiceRoleForDevOpsGuru` Essa é uma política AWS gerenciada com permissões específicas que o DevOps Guru precisa executar em sua conta.

A função vinculada ao serviço `AWSServiceRoleForDevOpsGuru` confia no seguinte serviço para assumir a função:

- `devops-guru.amazonaws.com`

A política de permissões de função `AmazonDevOpsGuruServiceRolePolicy` permite que o DevOps Guru conclua as seguintes ações nos recursos especificados.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "autoscaling:DescribeAutoScalingGroups",
    "cloudtrail:LookupEvents",
```

```
    "cloudwatch:GetMetricData",
    "cloudwatch:ListMetrics",
    "cloudwatch:DescribeAnomalyDetectors",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:ListDashboards",
    "cloudwatch:GetDashboard",
    "cloudformation:GetTemplate",
    "cloudformation:ListStacks",
    "cloudformation:ListStackResources",
    "cloudformation:DescribeStacks",
    "cloudformation:ListImports",
    "codedeploy:BatchGetDeployments",
    "codedeploy:GetDeploymentGroup",
    "codedeploy:ListDeployments",
    "config:DescribeConfigurationRecorderStatus",
    "config:GetResourceConfigHistory",
    "events:ListRuleNamesByTarget",
    "xray:GetServiceGraph",
    "organizations:ListRoots",
    "organizations:ListChildren",
    "organizations:ListDelegatedAdministrators",
    "pi:GetResourceMetrics",
    "tag:GetResources",
    "lambda:GetFunction",
    "lambda:GetFunctionConcurrency",
    "lambda:GetAccountSettings",
    "lambda:ListProvisionedConcurrencyConfigs",
    "lambda:ListAliases",
    "lambda:ListEventSourceMappings",
    "lambda:GetPolicy",
    "ec2:DescribeSubnets",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingPolicies",
    "sqs:GetQueueAttributes",
    "kinesis:DescribeStream",
    "kinesis:DescribeLimits",
    "dynamodb:DescribeTable",
    "dynamodb:DescribeLimits",
    "dynamodb:DescribeContinuousBackups",
    "dynamodb:DescribeStream",
    "dynamodb:ListStreams",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "rds:DescribeDBInstances",
```

```
    "rds:DescribeDBClusters",
    "rds:DescribeOptionGroups",
    "rds:DescribeDBClusterParameters",
    "rds:DescribeDBInstanceAutomatedBackups",
    "rds:DescribeAccountAttributes",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "s3:GetBucketNotification",
    "s3:GetBucketPolicy",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketTagging",
    "s3:GetBucketWebsite",
    "s3:GetIntelligentTieringConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:ListAllMyBuckets",
    "s3:ListStorageLensConfigurations",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListRequestedServiceQuotaChangeHistory",
    "servicequotas:ListServiceQuotas"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowPutTargetsOnASpecificRule",
   "Effect": "Allow",
   "Action": [
    "events:PutTargets",
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
  },
  {
   "Sid": "AllowCreateOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:CreateOpsItem"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAddTagsToOpsItem",
   "Effect": "Allow",
   "Action": [
```

```
    "ssm:AddTagsToResource"
   ],
   "Resource": "arn:aws:ssm:*:*:opsitem/*"
  },
  {
   "Sid": "AllowAccessOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:GetOpsItem",
    "ssm:UpdateOpsItem"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated": "true"
    }
   }
  },
  {
   "Sid": "AllowCreateManagedRule",
   "Effect": "Allow",
   "Action": "events:PutRule",
   "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
  },
  {
   "Sid": "AllowAccessManagedRule",
   "Effect": "Allow",
   "Action": [
    "events:DescribeRule",
    "events:ListTargetsByRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
  },
  {
   "Sid": "AllowOtherOperationsOnManagedRule",
   "Effect": "Allow",
   "Action": [
    "events:DeleteRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
```

```
    "Condition": {
     "StringEquals": {
      "events:ManagedBy": "devops-guru.amazonaws.com"
     }
    }
   },
   {
    "Sid": "AllowTagBasedFilterLogEvents",
    "Effect": "Allow",
    "Action": [
     "logs:FilterLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/DevOps-Guru-Analysis": "true"
     }
    }
   },
   {
    "Sid": "AllowAPIGatewayGetIntegrations",
    "Effect": "Allow",
    "Action": "apigateway:GET",
    "Resource": [
     "arn:aws:apigateway:*::/restapis/??????????",
     "arn:aws:apigateway:*::/restapis/*/resources",
     "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
    ]
   }
  ]
}
```

## Criação de uma função vinculada a serviços para o Guru DevOps

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria um insight na AWS Management Console, na ou na AWS API AWS CLI, o DevOps Guru cria a função vinculada ao serviço para você.

> **Important**
>
> Essa função vinculada ao serviço pode aparecer em sua conta se você tiver concluído uma ação em outro serviço que usa os recursos suportados por essa função; por exemplo, ela pode aparecer se você adicionou o DevOps Guru a um repositório do. AWS CodeCommit

## Editando uma função vinculada ao serviço para o Guru DevOps

DevOpsO Guru não permite que você edite a função vinculada ao `AWSServiceRoleForDevOpsGuru` 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 função vinculada ao serviço para o Guru DevOps

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. Porém, você deve se desassociar de todos os repositórios antes de poder exclui-la manualmente.

> **Note**
>
> Se o serviço DevOps Guru 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.

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

# Referência de permissões do Amazon DevOps Guru

Você pode usar chaves AWS de condição abrangentes em suas políticas do DevOps Guru para expressar condições. Para obter uma lista, consulte Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

Você especifica as ações no campo `Action` das políticas. Para especificar uma ação, use o prefixo `devops-guru:` seguido pelo nome da operação API (por exemplo, `devops-guru:SearchInsights` e `devops-guru:ListAnomalies`). Para especificar várias ações em uma única declaração, separe-as com vírgulas (por exemplo, `"Action": [ "devops-guru:SearchInsights", "devops-guru:ListAnomalies" ]`).

Usando caracteres curinga

Você especifica um nome do recurso da Amazon (ARN), com ou sem um caractere curinga (*), como o valor do recurso no campo `Resource` das políticas. Você pode usar um curinga para especificar várias ações ou recursos. Por exemplo, `devops-guru:*` especifica todas as ações do DevOps Guru e `devops-guru:List*` especifica todas as ações do DevOps Guru que começam com a palavra. `List` O exemplo a seguir se refere a todos os insights com um identificador exclusivo universal (Universally Unique Identifier, UUID) que começa com `12345`.

```
arn:aws:devops-guru:us-east-2:123456789012:insight:12345*
```

Você pode usar a tabela a seguir como referência ao configurar o Autenticação com identidades e escrever políticas de permissões que você pode anexar a uma identidade do IAM (políticas baseadas em identidade).

DevOpsOperações da API Guru e permissões necessárias para ações

`AddNotificationChannel`

Ação: `devops-guru:AddNotificationChannel`

Necessário para adicionar um canal de notificação do DevOps Guru. Um canal de notificação é usado para notificá-lo quando o DevOps Guru gera uma visão que contém informações sobre como melhorar suas operações.

Recurso: `*`

`RemoveNotificationChannel`

`devops-guru:RemoveNotificationChannel`

Necessário para remover um canal de notificação do DevOps Guru. Um canal de notificação é usado para notificá-lo quando o DevOps Guru gera uma visão que contém informações sobre como melhorar suas operações.

Recurso: *

`ListNotificationChannels`

Ação: `devops-guru:ListNotificationChannels`

Necessário para retornar uma lista de canais de notificação configurados para o DevOps Guru. Cada canal de notificação é usado para notificá-lo quando o DevOps Guru gera uma visão que contém informações sobre como melhorar suas operações. O único tipo de notificação suportado é o Amazon Simple Notification Service.

Recurso: *

`UpdateResourceCollectionFilter`

Ação: `devops-guru:UpdateResourceCollectionFilter`

Necessário para atualizar a lista de AWS CloudFormation pilhas usadas para especificar quais AWS recursos em sua conta são analisados pelo DevOps Guru. A análise gera insights que incluem recomendações, métricas e eventos operacionais que você pode usar para melhorar o desempenho de suas operações. Esse método também cria as funções do IAM necessárias para você usar CodeGuru OpsAdvisor.

Recurso: *

`GetResourceCollectionFilter`

Ação: `devops-guru:GetResourceCollectionFilter`

É necessário retornar a lista de AWS CloudFormation pilhas usadas para especificar quais AWS recursos em sua conta são analisados pelo DevOps Guru. A análise gera insights que incluem recomendações, métricas e eventos operacionais que você pode usar para melhorar o desempenho de suas operações.

Recurso: *

`ListInsights`

Ação: `devops-guru:ListInsights`

Obrigatório para retornar uma lista de insights em sua AWS conta. Você pode especificar quais insights são retornados por horário de início, status (`ongoing` ou `any`) e tipo (`reactive` ou `predictive`).

Recurso: *

`DescribeInsight`

Ação: `devops-guru:DescribeInsight`

necessário para retornar detalhes sobre um insight que você especifica usando sua ID.

Recurso: *

`SearchInsights`

Ação: `devops-guru:SearchInsights`

Obrigatório para retornar uma lista de insights em sua AWS conta. Você pode especificar quais insights são retornados por horário de início, filtros e tipo (`reactive` ou `predictive`).

Recurso: *

`ListAnomalies`

Ação: `devops-guru:ListAnomalies`

necessário para retornar uma lista das anomalias que pertencem a um insight que você especifica usando sua ID.

Recurso: *

`DescribeAnomaly`

Ação: `devops-guru:DescribeAnomaly`

necessário para retornar detalhes sobre uma anomalia que você especifica usando sua ID.

Recurso: *

`ListEvents`

Ação: `devops-guru:ListEvents`

Necessário retornar uma lista dos eventos emitidos pelos recursos que são avaliados pelo DevOps Guru. Você pode usar filtros para especificar quais eventos são retornados.

Recurso: *

`ListRecommendations`

Ação: `devops-guru:ListRecommendations`

necessário para retornar uma lista das recomendações especificadas de um insight. Cada recomendação inclui uma lista de métricas e uma de eventos relacionados às recomendações.

Recurso: *

`DescribeAccountHealth`

Ação: `devops-guru:DescribeAccountHealth`

Necessário para retornar o número de insights reativos abertos, o número de insights preditivos abertos e o número de métricas analisadas em sua AWS conta. Use esses números para avaliar a integridade das operações em sua AWS conta.

Recurso: *

`DescribeAccountOverview`

Ação: `devops-guru:DescribeAccountOverview`

necessário para retornar o que aconteceu durante um intervalo de tempo: o número de insights reativos abertos que foram criados, o número de insights preditivos abertos que foram criados e o tempo médio de recuperação (Mean Time To Recover, MTTR) de todos os insights reativos que foram fechados.

Recurso: *

`DescribeResourceCollectionHealthOverview`

Ação: `devops-guru:DescribeResourceCollectionHealthOverview`

Necessário para retornar o número de insights preditivos abertos, insights reativos abertos e tempo médio de recuperação (MTTR) para todos os insights de cada AWS CloudFormation pilha especificada no Guru. DevOps

Recurso: *

`DescribeIntegratedService`

Ação: `devops-guru:DescribeIntegratedService`

Necessário para retornar o status de integração dos serviços que podem ser integrados ao DevOps Guru. O único serviço que pode ser integrado ao DevOps Guru é AWS Systems Manager o que pode ser usado para criar um insight OpsItem para cada geração.

Recurso: *

`UpdateIntegratedServiceConfig`

Ação: `devops-guru:UpdateIntegratedServiceConfig`

Necessário para ativar ou desativar a integração com um serviço que pode ser integrado ao DevOps Guru. O único serviço que pode ser integrado ao DevOps Guru é o Systems Manager, que pode ser usado para criar um insight OpsItem para cada geração.

Recurso: *

## permissões para os tópicos do Amazon SNS

Use as informações deste tópico somente se quiser configurar o Amazon DevOps Guru para entregar notificações aos tópicos do Amazon SNS pertencentes a outra conta. AWS

Para que o DevOps Guru envie notificações para um tópico do Amazon SNS pertencente a uma conta diferente, você deve anexar uma política ao tópico do Amazon SNS que DevOps conceda ao Guru permissões para enviar notificações a ele. Se você configurar o DevOps Guru para entregar notificações aos tópicos do Amazon SNS pertencentes à mesma conta que você usa DevOps para o Guru, DevOps o Guru adicionará uma política aos tópicos para você.

Depois de anexar uma política para configurar permissões para um tópico do Amazon SNS em outra conta, você pode adicionar o tópico do Amazon SNS no Guru. DevOps Você também pode atualizar sua política do Amazon SNS com um canal de notificação para torná-la mais segura.

> **Note**
>
> DevOpsAtualmente, o Guru só oferece suporte ao acesso entre contas na mesma região.

Tópicos


- Configurar permissões para um tópico do Amazon SNS em outra conta
- Adicionar um tópico do Amazon SNS de outra conta
- Atualizar sua política do Amazon SNS com um canal de notificação (recomendado)


## Configurar permissões para um tópico do Amazon SNS em outra conta

Adicionar permissões como um perfil do IAM

Para usar um tópico do Amazon SNS de outra conta após fazer login com um perfil do IAM, você deve anexar uma política ao tópico do Amazon SNS que deseja usar. Para anexar uma política a um tópico do Amazon SNS de outra conta enquanto usa um perfil do IAM, você precisa ter as seguintes permissões para esse recurso da conta como parte do seu perfil do IAM:

- sns: CreateTopic
- sns: GetTopicAttributes
- sns: SetTopicAttributes
- sns:Publish

Anexar a seguinte política ao tópico do Amazon SNS que você deseja usar. Para a `Resource` chave, *`topic-owner-account-id`* é o ID da conta do proprietário do tópico, *`topic-sender-account-id`* é o ID da conta do usuário que configurou o DevOps Guru e *`devops-guru-role`* é a função do IAM do usuário individual envolvido. Você deve substituir os valores apropriados por *`region-id`* (por exemplo,`us-west-2`) *`my-topic-name`* e.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EnableDevOpsGuruServicePrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "Service": "region-id.devops-guru.amazonaws.com"
            },
            "Condition": {
                "StringEquals": {
```

```
                    "AWS:SourceAccount": "topic-sender-account-id"
                }
            }
        },
        {
            "Sid": "EnableAccountPrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "AWS": ["arn:aws:iam::topic-sender-account-id:role/devops-guru-role"]
            }
        }
    ]
}
```

Adicionar permissões como um usuário do IAM

Para usar um tópico do SNS de outra conta como usuário do IAM, anexe a política a seguir ao tópico do Amazon SNS que você deseja usar. Para a `Resource` chave, *`topic-owner-account-id`* é o ID da conta do proprietário do tópico, *`topic-sender-account-id`* é o ID da conta do usuário que configurou o DevOps Guru e *`devops-guru-user-name`* é o usuário individual do IAM envolvido. Você deve substituir os valores apropriados por *`region-id`* (por exemplo,`us-west-2`) *`my-topic-name`* e.

> **Note**
>
> Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EnableDevOpsGuruServicePrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
```

```
            "Principal": {
                "Service": "region-id.devops-guru.amazonaws.com"
            },
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "topic-sender-account-id"
                }
            }
        },
        {
            "Sid": "EnableAccountPrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "AWS": ["arn:aws:iam::topic-sender-account-id:user/devops-guru-user-
name"]
            }
        }
    ]
 }
```

## Adicionar um tópico do Amazon SNS de outra conta

Depois de configurar as permissões para um tópico do Amazon SNS em outra conta, você pode adicionar esse tópico do Amazon SNS às DevOps suas configurações de notificação do Guru. Você pode adicionar o tópico do Amazon SNS usando o console AWS CLI ou o DevOps Guru.

- Ao usar o console, você deve selecionar a opção Usar um ARN de tópico do SNS para especificar um tópico existente para usar um tópico de outra conta.
- Ao usar a AWS CLI operação add-notification-channel, você deve especificar o que está `TopicArn` dentro do `NotificationChannelConfig` objeto.

Adicionar um tópico do Amazon SNS de outra conta usando o console

1. Abra o console do Amazon DevOps Guru em https://console.aws.amazon.com/devops-guru/.
2. Abra o painel de navegação e escolha Configurações.
3. Vá para a seção Notificações e escolha Editar.
4. Escolha Adicionar tópico do SNS.

5. Escolha Usar um ARN do tópico do SNS para especificar um tópico existente.
6. Insira o ARN do tópico do Amazon SNS que você deseja usar. Você já deve ter configurado as permissões para esse tópico anexando uma política a ele.
7. (Opcional) Escolha Configuração de notificação para editar as configurações de frequência de notificação.
8. Escolha Salvar.

Depois de adicionar o tópico do Amazon SNS às suas configurações de notificação, o DevOps Guru usa esse tópico para notificá-lo sobre eventos importantes, como quando um novo insight é criado.

## Atualizar sua política do Amazon SNS com um canal de notificação (recomendado)

Depois de adicionar um tópico, recomendamos que você torne sua política mais segura especificando permissões somente para o canal de notificação do DevOps Guru que contém seu tópico.

Atualizar seu tópico do Amazon SNS com um canal de notificação (recomendado)

1. Execute o AWS CLI comando `list-notification-channels` DevOps Guru na sua conta da qual você deseja enviar notificações.

```
aws devops-guru list-notification-channels
```

2. Na resposta do `list-notification-channels`, anote o ID do canal que contém o ARN do seu tópico do Amazon SNS. O ID do canal é um guia.

   Por exemplo, na resposta a seguir, o ID do canal para o tópico com o ARN `arn:aws:sns:`*`region-id`*`:`*`111122223333`*`:`*`topic-name`* é *`e89be5f7-989d-4c4c-b1fe-e7145037e531`*

```
{
  "Channels": [
    {
      "Id": "e89be5f7-989d-4c4c-b1fe-e7145037e531",
      "Config": {
      "Sns": {
          "TopicArn": "arn:aws:sns:region-id:111122223333:topic-name"
        },
      "Filters": {
```

```
            "MessageTypes": ["CLOSED_INSIGHT", "NEW_INSIGHT", "SEVERITY_UPGRADED"],
            "Severities": ["HIGH", "MEDIUM"]
          }
        }
      }
    ]
}
```

3. Acesse a política que você criou em outra conta usando o ID do proprietário do tópico em the section called “Configurar permissões para um tópico do Amazon SNS em outra conta”. Na declaração da política do `Condition`, adicione a linha que especifica o `SourceArn`. O ARN contém seu ID de região (por exemplo,`us-east-1`), o número da AWS conta do remetente do tópico e o ID do canal que você anotou.

   Sua declaração `Condition` atualizada tem a seguinte aparência.

```
"Condition" : {
  "StringEquals" : {
    "AWS:SourceArn": "arn:aws:devops-guru:us-
east-1:111122223333:channel/e89be5f7-989d-4c4c-b1fe-e7145037e531",
    "AWS:SourceAccount": "111122223333"
   }
 }
```

Se `AddNotificationChannel` não conseguir adicionar seu tópico do SNS, verifique se sua política do IAM tem as seguintes permissões.

```
{
     "Version": "2012-10-17",
     "Statement": [{
           "Sid": "DevOpsGuruTopicPermissions",
           "Effect": "Allow",
           "Action": [
                 "sns:CreateTopic",
                 "sns:GetTopicAttributes",
                 "sns:SetTopicAttributes",
                 "sns:Publish"
           ],
           "Resource": "arn:aws:sns:region-id:account-id:my-topic-name"
     }]
}
```

## Permissões para tópicos AWS KMS criptografados do Amazon SNS

O tópico do Amazon SNS especificado por você pode ser criptografado pelo AWS Key Management Service. Para permitir que o DevOps Guru trabalhe com tópicos criptografados, você deve primeiro criar uma AWS KMS key e depois adicionar a seguinte declaração à política da chave KMS. Para obter mais informações, consulte Criptografia de mensagens publicadas no Amazon SNS com o AWS KMS, Identificadores de chave KeyId () no Guia do usuário e Criptografia de dados AWS KMS no Guia do desenvolvedor do Amazon Simple Notification Service.

```
{
  "Version": "2012-10-17",
  "Id": "your-kms-key-policy",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> DevOpsAtualmente, o Guru oferece suporte a tópicos criptografados para uso em uma única conta. No momento, o uso de um tópico criptografado em várias contas não é suportado.

## Solução de problemas de identidade e acesso ao Amazon DevOps Guru

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o DevOps Guru e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação no DevOps Guru
- Quero dar acesso programático aos usuários
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do DevOps Guru

## Não estou autorizado a realizar uma ação no DevOps Guru

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda.

O erro do exemplo a seguir ocorre quando o usuário `mateojackson` tenta usar o console para visualizar detalhes sobre um recurso fictício do *`my-example-widget`*, mas não tem as permissões fictícias do `aws:GetWidget`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 aws:GetWidget on resource: my-example-widget
```

Neste caso, Mateo pede ao administrador para atualizar suas políticas e permitir o acesso ao recurso *`my-example-widget`* usando a ação `aws:GetWidget`.

## Quero dar acesso programático aos usuários

Os usuários precisam de acesso programático se quiserem interagir com pessoas AWS fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| Identidade da força de trabalho<br><br>(Usuários gerenciados no Centro de Identidade do IAM) | Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs | Siga as instruções da interface que deseja utilizar.<br><br>• Para o AWS CLI, consulte Configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS |

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| | | Command Line Interface usuário.<br>• Para AWS SDKs, ferrament as e AWS APIs, consulte a autenticação do IAM Identity Center no Guia de referênci a de ferramentas AWS SDKs e ferramentas. |
| IAM | Use credenciais temporári as para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs | Siga as instruções em Como usar credenciais temporárias com AWS recursos no Guia do usuário do IAM. |

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| IAM | (Não recomendado)<br>Use credenciais de longo prazo para assinar solicitaç ões programáticas para o AWS CLI, AWS SDKs, ou. AWS APIs | Siga as instruções da interface que deseja utilizar.<br>• Para isso AWS CLI, consulte Autenticação usando credenciais de usuário do IAM no Guia do AWS Command Line Interface usuário.<br>• Para ferramentas AWS SDKs e ferramentas, consulte Autenticar usando credenciais de longo prazo no Guia de referência de ferramentas AWS SDKs e ferramentas.<br>• Para isso AWS APIs, consulte Gerenciamento de chaves de acesso para usuários do IAM no Guia do usuário do IAM. |

## Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o DevOps Guru.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no DevOps Guru. No entanto, a ação exige que o serviço tenha

permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do DevOps Guru

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o DevOps Guru oferece suporte a esses recursos, consulteComo o Amazon DevOps Guru funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

# DevOpsGuru de registro e monitoramento

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do DevOps Guru e de suas outras soluções da AWS. A AWS fornece as seguintes ferramentas de monitoramento para observar o DevOps Guru, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. Você pode coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas EC2 instâncias da Amazon e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.
- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem no qual as chamadas foram feitas e quando elas ocorreram. Para mais informações, consulte o Guia do usuário do AWS CloudTrail.

Tópicos


- DevOpsGuru do monitoramento com a Amazon CloudWatch
- Registrando chamadas de API do Amazon DevOps Guru com AWS CloudTrail


## DevOpsGuru do monitoramento com a Amazon CloudWatch

Você pode monitorar o DevOps Guru usando CloudWatch, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. Essas estatísticas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como a aplicação web ou o serviço está se saindo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

Para o DevOps Guru, você pode rastrear métricas para obter insights e métricas para seu uso do DevOps Guru. Talvez você queira prestar atenção ao grande número de soluções criadas pela `Insights` para ajudar você a determinar se suas soluções operacionais estão apresentando um

comportamento anômalo. Ou talvez você queira observar o uso do DevOps Guru para ajudar a controlar seus custos.

O serviço DevOps Guru relata as seguintes métricas no `AWS/DevOps-Guru` namespace.

Tópicos


- Métricas de insight
- DevOpsMétricas de uso do Guru


## Métricas de insight

Você pode usar CloudWatch para rastrear uma métrica para mostrar quantos insights são criados em sua AWS conta. Você pode especificar a `Type` dimensão para rastrear `proactive` ou `reactive`insights. Não especifique uma dimensão se quiser rastrear todos os insights.

Métricas

| Métrica | Descrição |
| --- | --- |
| `Insight` | O número de insights criados em uma AWS conta.<br>Dimensões válidas: `Type`<br>Estatísticas válidas: Sample Count, Sum<br>Unidades: contagem |

A dimensão a seguir é compatível com a `Insight` métrica DevOps Guru.

Dimensões

| Dimensão | Descrição |
| --- | --- |
| `Type` | Esse é o tipo do insight. Não especifique uma dimensão para a métrica do `Insights` se quiser rastrear todos os insights. Os valores válidos são `proactive` , `reactive`. |

## DevOpsMétricas de uso do Guru

Você pode usar CloudWatch para rastrear seu uso do Amazon DevOps Guru.

Métricas

| Métrica | Descrição |
| --- | --- |
| `CallCount` | O número de chamadas feitas por um dos seguintes métodos do DevOps Guru.<br>• `ListInsights`<br>• `ListAnomaliesForInsight`<br>• `ListRecommendations`<br>• `ListEvents`<br>• `SearchInsights`<br>• `DescribeInsight`<br>• `DescribeAnomaly`<br><br>Dimensões válidas: `Service`, `Class`, `Type`, `Resource`<br><br>Estatísticas válidas: Sample Count, Sum<br><br>Unidades: contagem |

As dimensões a seguir são compatíveis com as métricas de uso do DevOps Guru.

Dimensões

| Dimensão | Descrição |
| --- | --- |

| Dimensão | Descrição |
| --- | --- |
| `Service` | Este é o nome do serviço da AWS que contém o recurso. Por exemplo, para o DevOps Guru, esse valor é`DevOps-Guru` . |
| `Class` | Essa é a classe do recurso que é rastreado. DevOpsO Guru usa essa dimensão com o valor`None`. |
| `Type` | Esse é o tipo de recurso que é rastreado. DevOpsO Guru usa essa dimensão com o valor`API`. |
| `Resource` | Esse é o nome da operação DevOps Guru. Os valores válidos são: `ListInsights` , `ListAnomaliesForInsight` , `ListRecommendations` , `ListEvents` , `SearchInsights` , `DescribeInsight` , `DescribeAnomaly` . |

## Registrando chamadas de API do Amazon DevOps Guru com AWS CloudTrail

O Amazon DevOps Guru é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no DevOps Guru. CloudTrail captura chamadas de API para o DevOps Guru como eventos. As chamadas capturadas incluem chamadas do console do DevOps Guru e chamadas de código para as operações da API do DevOps Guru. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para DevOps o Guru. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao DevOps Guru, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

### DevOpsInformações sobre o Guru em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre no DevOps Guru, essa atividade é registrada em um CloudTrail evento junto com outros eventos de AWS serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em

sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos do DevOps Guru, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

DevOpsO Guru suporta o registro de todas as suas ações como eventos em arquivos de CloudTrail log. Para obter mais informações, consulte Ações na referência da API DevOps Guru.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário da raiz ou do .
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

## Entendendo as entradas do arquivo de log do DevOps Guru

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante.

CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `UpdateResourceCollection` ação.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAAAAAAAEXAMPLE:TestSession",
    "arn": "arn:aws:sts::123456789012:assumed-role/TestRole/TestSession",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/TestRole",
        "accountId": "123456789012",
        "userName": "sample-user-name"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-12-03T15:29:51Z"
      }
    }
  },
  "eventTime": "2020-12-01T16:14:31Z",
  "eventSource": "devops-guru.amazonaws.com",
  "eventName": "UpdateResourceCollection",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "sample-ip-address",
  "userAgent": "aws-internal/3 aws-sdk-java/1.11.901
 Linux/4.9.217-0.3.ac.206.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.275-b01
 java/1.8.0_275 vendor/Oracle_Corporation",
  "requestParameters": {
    "Action": "REMOVE",
    "ResourceCollection": {
      "CloudFormation": {
        "StackNames": [
          "*"
```

```
        ]
      }
    }
  },
  "responseElements": null,
  "requestID": " cb8c167e-EXAMPLE ",
  "eventID": " e3c6f4ce-EXAMPLE ",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

# DevOpsGuru e interface VPC endpoints ()AWS PrivateLink

Você pode usar VPC endpoints ao ligar para o Amazon Guru. DevOps APIs Quando você usa endpoints da VPC, suas chamadas de API ficam mais seguras porque estão contidas em sua VPC e não acessam a Internet. Para obter mais informações, consulte Ações na referência de API do Amazon DevOps Guru.

Você estabelece uma conexão privada entre sua VPC e o DevOps Guru criando uma interface VPC endpoint. Os endpoints de interface são alimentados por AWS PrivateLinkuma tecnologia que permite que você acesse o DevOps Guru de forma privada APIs sem um gateway de internet, dispositivo NAT, conexão VPN ou conexão do AWS Direct Connect. As instâncias em sua VPC não precisam de endereços IP públicos para se comunicar com DevOps o Guru. APIs O tráfego entre sua VPC e o DevOps Guru não sai da rede Amazon.

Cada endpoint de interface é representado por uma ou mais Interfaces de Rede Elástica nas sub-redes.

Para obter mais informações, consulte Interface VPC endpoints (AWS PrivateLink) no Guia do usuário da Amazon VPC.

## Considerações sobre os endpoints DevOps Guru VPC

Antes de configurar uma interface VPC endpoint para o DevOps Guru, certifique-se de revisar as propriedades e limitações do endpoint da interface no Guia do usuário da Amazon VPC.

DevOpsO Guru suporta fazer chamadas para todas as suas ações de API a partir de sua VPC.

## Criação de uma interface VPC endpoint para o Guru DevOps

Você pode criar um VPC endpoint para o serviço DevOps Guru usando o console Amazon VPC ou o (). AWS Command Line Interface AWS CLI Para obter mais informações, consulte Criar um endpoint de interface no Guia do usuário da Amazon VPC.

Crie um VPC endpoint para o DevOps Guru usando o seguinte nome de serviço:

- com.amazonaws. *region*.devops-guru

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API ao DevOps Guru usando seu nome DNS padrão para a região, por exemplo,. `devops-guru.us-east-1.amazonaws.com`

Para mais informações, consulte Acessar um serviço por um endpoint de interface no Guia do usuário da Amazon VPC.

## Criação de uma política de VPC endpoint para o Guru DevOps

Você pode anexar uma política de endpoint ao seu VPC endpoint que controla o acesso ao Guru. DevOps Essa política especifica as seguintes informações:

- A entidade principal que pode realizar ações.
- As ações que podem ser realizadas.
- Os recursos aos quais as ações podem ser aplicadas.

Para mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Guia do usuário da Amazon VPC.

Exemplo: política de VPC endpoint para ações do Guru DevOps

Veja a seguir um exemplo de uma política de endpoint para o DevOps Guru. Quando anexada a um endpoint, essa política concede acesso às ações listadas do DevOps Guru para todos os diretores de todos os recursos.

```
{
   "Statement":[
      {
         "Principal":"*",
```

```
            "Effect":"Allow",
            "Action":[
               "devops-guru:AddNotificationChannel",
               "devops-guru:ListInsights",
               "devops-guru:ListRecommendations"
            ],
            "Resource":"*"
         }
      ]
}
```

# Segurança de infraestrutura em DevOps Guru

Como um serviço gerenciado, o Amazon DevOps Guru é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o DevOps Guru pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

# Resiliência no Amazon DevOps Guru

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. DevOpsO Guru opera em várias zonas de disponibilidade e armazena dados e metadados de artefatos no Amazon S3

e no Amazon DynamoDB. Seus dados criptografados são armazenados com redundância em várias instalações e diversos dispositivos em cada instalação, fazendo com que sejam altamente disponíveis e altamente duráveis.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

# Cotas e limites para o Amazon DevOps Guru

A tabela a seguir lista a cota atual no Amazon DevOps Guru. Essa cota é para cada AWS região compatível com cada AWS conta.

## Notificações

| | |
|---|---|
| Número máximo de tópicos do Amazon Simple Notification Service que você pode especificar de uma vez | 2 |

## AWS CloudFormation pilhas

| | |
|---|---|
| Número máximo de AWS CloudFormation pilhas que você pode especificar | 1000 |

## DevOpsLimites de monitoramento de recursos do Guru

| Descrição do recurso | Limite | Pode ser aumentada |
|---|---|---|
| Limite padrão para o monitoramento das filas do Amazon Simple Queue Service (Amazon SQS) | 100* | Sim** |

*Para novas contas do DevOps Guru criadas em ou após 29 de junho de 2023 e para contas existentes que estavam ativas na mesma data e têm menos de 100 filas do Amazon SQS.

**Para solicitar uma alteração nesse limite, entre em contato Suporte em https://aws.amazon.com/contact-us. Você pode solicitar um limite de monitoramento de filas do Amazon SQS de 100, 500, 1.000, 5.000 ou 10.000.

# DevOpsCotas do Guru para criar, implantar e gerenciar uma API

As cotas fixas a seguir se aplicam à criação, implantação e gerenciamento de uma API no DevOps Guru, usando o console do AWS CLI API Gateway ou a API REST do API Gateway e suas. SDKs

Para obter uma lista de todos os DevOps Gurus APIs, consulte Amazon DevOps Guru Actions.

| Cota padrão | Pode ser aumentada | |
|---|---|---|
| 20 solicitações a cada 1 segundo por conta | Sim | |

# Histórico de documentos do Amazon DevOps Guru

A tabela a seguir descreve a documentação desta versão do DevOps Guru.

- Versão da API: mais recente
- Última atualização de documentação: 9 de agosto de 2023

| Alteração | Descrição | Data |
| --- | --- | --- |
| Atualizações da política gerenciada | As assinaturas do Amazon SNS e o acesso à lista de assinaturas foram adicionados à política do `AmazonDevOpsGuruConsoleFullAccess`. O acesso à lista de assinaturas também foi adicionado à política do `AmazonDevOpsGuruReadOnlyAccess`. Para obter mais informações, consulte Políticas baseadas em identidade para o Amazon DevOps Guru. | 9 de agosto de 2023 |
| Chaves de criptografia gerenciadas pelo cliente | DevOpsO Guru agora oferece suporte à criptografia com o uso AWS KMS de chaves gerenciadas pelo cliente. Para obter mais informações, consulte Proteção de dados no DevOps Guru. | 5 de julho de 2023 |
| DevOpsO Guru for RDS suporta RDS PostgreSQL | DevOpsO Guru for RDS pode detectar gargalos de desempenho e outros insights nos bancos de dados | 30 de março de 2023 |

| | | |
|---|---|---|
| | PostgreSQL. Para obter mais informações, consulte Benefícios do DevOps Guru para RDS. | |
| DevOpsO Guru for RDS oferece suporte a insights proativos | DevOpsO Guru for RDS publica insights proativos com recomendações para ajudá-lo a resolver problemas em seus bancos de dados Aurora antes que eles se tornem problemas maiores. Para obter mais informações, consulte Trabalhando com anomalias no DevOps Guru for RDS. | 28 de fevereiro de 2023 |
| Página de recursos analisados | Uma nova página no console do DevOps Guru lista os recursos em sua conta que são analisados pelo DevOps Guru. Para obter mais informações, consulte Visualização de recursos analisados pelo DevOps Guru. | 20 de outubro de 2022 |
| Novas configurações de notificação | Agora, você pode escolher se deseja receber todas as notificações ou receber apenas notificações para determinadas gravidades e eventos. Para mais informaçõ es, consulte Como atualizar as configurações do Amazon SNS. | 30 de setembro de 2022 |

| | | |
|---|---|---|
| Adição da análise de anomalias de log às políticas gerenciadas | AWS as políticas gerenciadas do DevOps Guru foram atualizadas no console do IAM para dar suporte ao acesso à ação CloudWatch . `FilterLogEvents` Para obter mais informações, consulte Atualizações do DevOps Guru sobre políticas AWS gerenciadas e funções vinculadas a serviços. | 30 de agosto de 2022 |
| Análise de anomalias de log adicionada | Você pode ver informações detalhadas sobre grupos de registros relacionados a insights no console do DevOps Guru. Também há uma função expandida vinculada a serviços disponível para descrever CloudWatch registros e fluxos. Para obter mais informações, consulte Compreendendo os insights no console do DevOps Guru e as atualizações do DevOps Guru para políticas AWS gerenciadas e funções vinculadas a serviços. | 12 de julho de 2022 |

| | | |
|---|---|---|
| CodeGuru Integração com o Profiler | DevOpsO Guru agora se integra ao Amazon CodeGuru Profiler com uma EventBridge regra gerenciada. Cada evento de entrada do CodeGuru Profiler é um relatório proativo de anomalias. Para obter mais informações, consulte Integração com o CodeGuru Profiler. | 7 de março de 2022 |
| Função vinculada ao serviço e atualizações de política gerenciadas | Políticas expandidas disponíveis no console do IAM. As mudanças permitem que o DevOps Guru ofereça suporte à integração aprimorada com o Amazon Relational Database Service (Amazon RDS). Para obter mais informações, consulte Usando funções vinculadas a serviços e políticas AWS gerenciadas (predefinidas) para o Guru. DevOps | 21 de dezembro de 2021 |
| Nova política gerenciada adicionada | A política `AmazonDevOpsGuruConsoleFullAccess` foi adicionada. Para obter mais informações, consulte Políticas baseadas em identidade para o Amazon DevOps Guru. | 6 de dezembro de 2021 |

| | | |
|---|---|---|
| Support para definir seu aplicativo com AWS tags | Agora você pode usar AWS tags para identificar os recursos que você deseja que o DevOps Guru analise, identificar os recursos em seus aplicativos e filtrar insights no console. Para mais informações, consulte Usar tags para identificar recursos em suas aplicações. | 1º de dezembro de 2021 |
| Função vinculada ao serviço e atualizações de política gerenciadas | Políticas expandidas disponíveis no console do IAM. As mudanças permitem que o DevOps Guru ofereça suporte à integração aprimorada com o Amazon Relational Database Service (Amazon RDS). Para obter mais informações, consulte Usando funções vinculadas a serviços e políticas AWS gerenciadas (predefinidas) para o Guru. DevOps | 1º de dezembro de 2021 |
| Suporte do Amazon RDS | DevOpsO Guru agora fornece análises e insights abrangentes para os recursos do Amazon Relational Database Service (Amazon RDS) em seu aplicativo. Para obter mais informações, consulte Trabalhando com anomalias no DevOps Guru para Amazon RDS. | 1º de dezembro de 2021 |

| | | |
|---|---|---|
| EventBridge Integração com a Amazon | DevOpsO Guru agora se integra EventBridge para notificá-lo sobre certos eventos relacionados aos seus insights do DevOps Guru. Para obter mais informações, consulte Trabalhando com EventBridge. | 18 de novembro de 2021 |
| AWS política gerenciada adicionada | Nova política AWS gerenciada adicionada. A `AmazonDevOpsGuruOrganizationsAccess` política fornece acesso ao DevOps Guru dentro de uma organização. Para mais informações, consulte políticas baseadas em identidade. | 16 de novembro de 2021 |
| Atualização da política de função vinculada ao serviço | Política expandida disponível no console do IAM. A mudança permite que o DevOps Guru ofereça suporte à visualização de várias contas. Para mais informações, consulte Como usar funções vinculadas a serviços. | 4 de novembro de 2021 |
| Suporte a contas cruzadas | Agora, você pode visualizar insights e métricas em várias contas de sua organização. Para obter mais informações, consulte O que é o Amazon DevOps Guru. | 4 de novembro de 2021 |

| | | |
|---|---|---|
| Versão de disponibilidade geral | O Amazon DevOps Guru agora está disponível ao público em geral (GA). | 4 de maio de 2021 |
| Novo tópico | Agora você pode gerar uma estimativa de custo mensal para o DevOps Guru analisar seus recursos. Para obter mais informações, consulte Estimar seus custos do Amazon DevOps Guru. | 27 de abril de 2021 |
| Suporte para endpoint da VPC | Agora você pode usar endpoints da VPC para melhorar a segurança de sua análise de recursos e geração de insights. Para obter mais informações, consulte DevOpsGuru e interface VPC endpoints AWS PrivateLink (). | 15 de abril de 2021 |
| Novo tópico | Um novo tópico sobre como monitorar o DevOps Guru com a Amazon CloudWatch foi adicionado. Para obter mais informações, consulte Monitoring DevOps Guru with Amazon CloudWatch. | 11 de dezembro de 2020 |
| Versão prévia | Esta é a versão prévia do Guia do usuário do Amazon DevOps Guru. | 1º de dezembro de 2020 |

# AWS Glossário

Para obter a AWS terminologia mais recente, consulte o AWS glossário na Glossário da AWS Referência.

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.