aws

Manual do usuário

Console do Developer Tools

Console do Developer Tools: Manual do usuário

Table of Contents

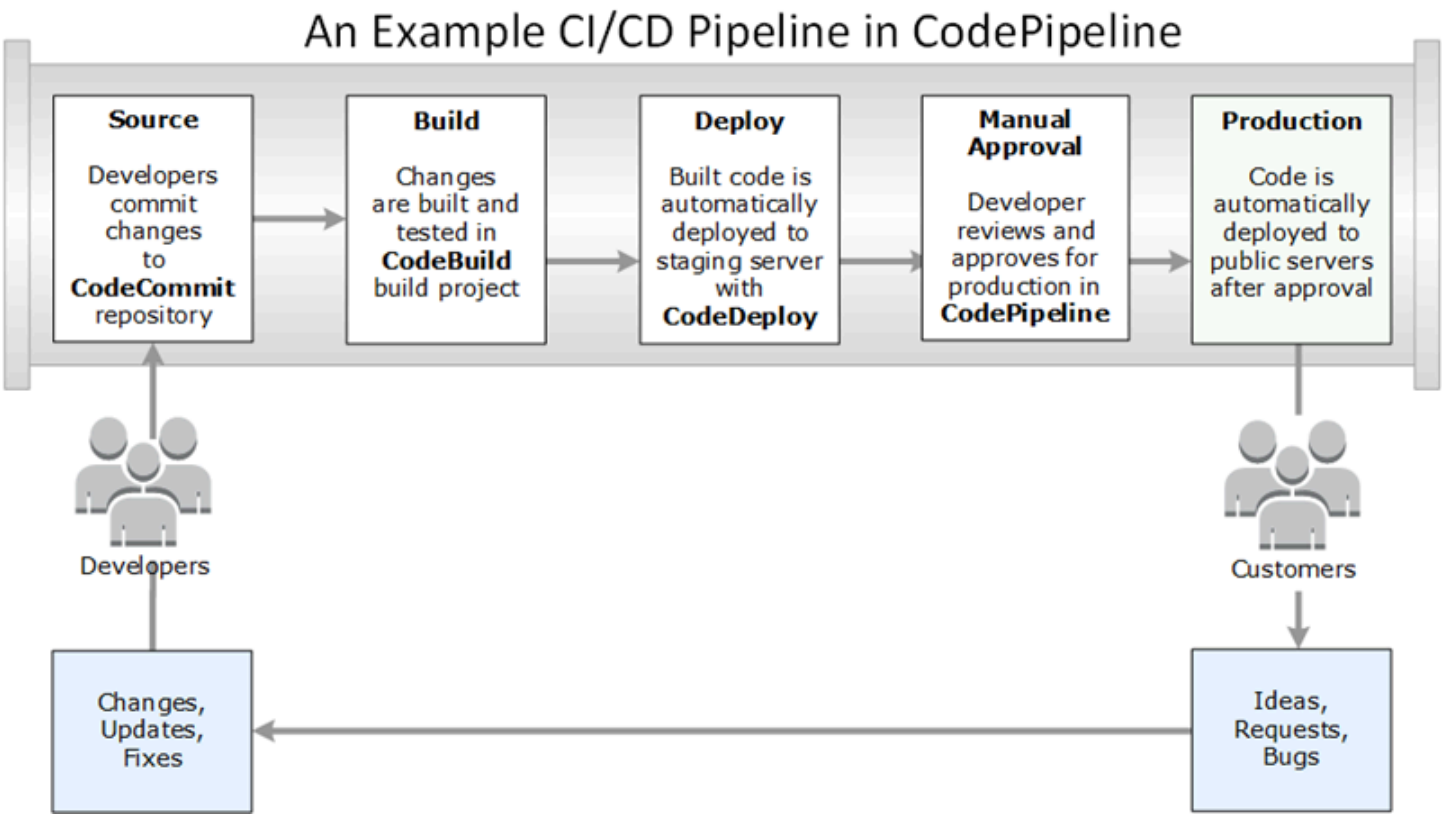
O que é o console do Developer Tools?

O console do Developer Tools oferece um conjunto de serviços e recursos que podem ser usados individual ou coletivamente para ajudá-lo a desenvolver software, individualmente ou em equipe. O Developer Tools pode ajudar a armazenar, compilar, testar e implantar seu software com segurança. Usadas individual ou coletivamente, essas ferramentas fornecem suporte para DevOps, integração contínua e entrega contínua (CI/CD).

O console do Developer Tools inclui os seguintes serviços:

- AWS CodeCommit é um serviço de controle de origem totalmente gerenciado que hospeda repositórios Git privados. Você pode usar repositórios para armazenar e gerenciar ativos (como documentos, código-fonte e arquivos binários) na Nuvem AWS. Os repositórios também armazenam o histórico do projeto, desde a primeira confirmação até as alterações mais recentes. Você pode trabalhar de forma colaborativa no código em repositórios comentando o código e criando solicitações de envio para ajudar a garantir a qualidade do código.
- O AWS CodeBuild é um serviço de compilação totalmente gerenciado que compila o código-fonte, executa testes em unidades e produz artefatos prontos para implantação. Ele fornece ambientes de compilação com pacotes predefinidos para linguagens populares de programação e ferramentas de compilação, como Apache Maven, Gradle, entre outras. Também é possível personalizar ambientes de compilação no CodeBuild para usar suas próprias ferramentas de compilação.
- O AWS CodeDeploy é um serviço de implantação totalmente gerenciado que automatiza implantações de software para serviços de computação, como o Amazon EC2, AWS Lambda e seus servidores locais. Ele pode ajudá-lo a liberar rapidamente novos recursos, evitar tempo de inatividade durante a implantação de aplicativos e lidar com a complexidade da atualização de seus aplicativos.
- O AWS CodePipeline é um serviço de integração contínua e entrega contínua que pode ser usado para modelar, visualizar e automatizar as etapas necessárias para lançar seu software. É possível modelar e configurar rapidamente os diferentes estágios de um processo de lançamento de software. É possível compilar, testar e implantar o código sempre que ocorre uma alteração de código, de acordo com os modelos definidos do processo de lançamento.

Veja um exemplo de como você pode usar os serviços do console do Developer Tools em conjunto para ajudar no desenvolvimento de software.



Neste exemplo, os desenvolvedores criam um repositório no CodeCommit e o usam para desenvolver e colaborar em seu código. Eles criam um projeto de compilação no CodeBuild para criar e testar seu código, e usam o CodeDeploy para implantar seu código em ambientes de teste e produção. Eles precisam iterar rapidamente, e, então, criam um pipeline no CodePipeline para detectar as alterações no repositório do CodeCommit. Essas alterações são compiladas, testes são executados e o código compilado e testado com êxito é implantado no servidor de teste. A equipe adiciona estágios de teste ao pipeline para executar mais testes no servidor de teste, como testes de integração ou carga. Após a conclusão bem-sucedida desses testes, um membro da equipe revisa os resultados e, se satisfeito, aprova manualmente as alterações para produção. O CodePipeline implanta o código testado e aprovado em instâncias de produção.

Este é apenas um exemplo simples de como você pode usar um ou mais dos serviços disponíveis no console do Developer Tools para ajudar a desenvolver software. Cada um dos serviços pode ser personalizado para atender às suas necessidades. Eles oferecem muitas integrações com outros produtos e serviços, na AWS e com outras ferramentas de terceiros. Para obter mais informações, consulte os tópicos a seguir:

- CodeCommit: Integrações de produtos e serviços
- CodeBuild:Usar o CodeBuild com o Jenkins

- CodeDeploy: Integrações de produtos e serviços
- CodePipeline: Integrações de produtos e serviços

Você é um usuário iniciante do ?

Se você é um usuário iniciante de um ou mais dos serviços disponíveis no console do Developer Tools, recomendamos começar lendo os seguintes tópicos:

- Conceitos básicos do CodeCommit
- Conceitos básicos do CodeBuild, Conceitos
- Conceitos básicos do CodeDeploy, Componentes principais
- Conceitos básicos do CodePipeline, Conceitos

Recursos do console do Developer Tools

O console do Developer Tools inclui os seguintes recursos:

- O console do Developer Tools inclui um recurso de gerenciador de notificações que você pode usar para se inscrever em eventos em AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy e AWS CodePipeline. Esse recurso tem sua própria API, o AWS CodeStar Notifications. Você pode usar o recurso de notificações para notificar rapidamente os usuários sobre eventos nos repositórios, projetos de compilação, aplicativos de implantação e pipelines que são mais importantes para seu trabalho. Um gerenciador de notificações ajuda os usuários a saber quais eventos ocorrem em repositórios, compilações, implantações ou pipelines para que possam agir rapidamente, como aprovar alterações ou corrigir erros. Para obter mais informações, consulte O que são notificações?.
- O console do Developer Tools inclui um recurso de conexões que você pode usar para associar seus recursos da AWS a provedores de código-fonte de terceiro. Esse recurso tem sua própria API, o AWS CodeStar Connections. É possível usar o recurso de conexões para configurar uma conexão autorizada com um provedor terceiro e usar o recurso de conexão com outros serviços da AWS. Para obter mais informações, consulte O que são conexões?.

O que são notificações?

O recurso de notificações no Console do Developer Tools é um gerenciador de notificações para inscrição em eventos em AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy e AWS CodePipeline. Ele tem sua própria API, o AWS CodeStar Notifications. Você pode usar o recurso de notificações para notificar rapidamente os usuários sobre eventos nos repositórios, projetos de compilação, aplicativos de implantação e pipelines que são mais importantes para seu trabalho. Um gerenciador de notificações ajuda os usuários a saber quais eventos ocorrem em repositórios, compilações, implantações ou pipelines para que possam agir rapidamente, como aprovar alterações ou corrigir erros.

O que posso fazer com notificações?

Você pode usar o recurso de notificações para criar e gerenciar regras de notificação para notificar os usuários sobre alterações importantes em seus recursos, incluindo:

- Sucessos e falhas de compilação em projetos de compilação do CodeBuild.
- Sucessos e falhas de implantação em aplicações do CodeDeploy.
- Criação de e atualizações em solicitações pull, incluindo comentários em código, em repositórios do CodeCommit.
- Status de aprovação manual e execuções do pipeline no CodePipeline.

Você pode configurar as notificações de forma que elas sejam enviadas para endereços de e-mail de usuários inscritos em um tópico do Amazon SNS. Também é possível integrar esse recurso ao AWS Chatbot e fazer com que as notificações sejam entregues a canais do Slack, ao canal do Microsoft Teams ou a salas de bate-papo do Amazon Chime.

Como as notificações funcionam?

Quando você configura uma regra de notificação para um recurso compatível, como um repositório, projeto de compilação, aplicativo ou pipeline, o recurso de notificações cria uma regra do Amazon EventBridge que monitora os eventos especificados. Quando um evento desse tipo ocorre, a regra de notificação envia notificações aos tópicos do Amazon SNS especificados como destinos para essa regra. Os assinantes desses destinos recebem notificações sobre esses eventos.

Como posso começar a usar notificações?

Para começar, veja alguns tópicos úteis para revisar:

- Saiba mais sobre os conceitos de notificações.
- Configure os recursos necessários para começar a trabalhar com notificações.
- Comece a usar suas primeiras regras de notificação e receba suas primeiras notificações.

Conceitos de notificação

Configurar e usar notificações é mais fácil se você entender os conceitos e termos. Veja alguns conceitos que você deve saber ao usar notificações.

Tópicos

Notificações

Uma notificação é uma mensagem que contém informações sobre eventos que ocorrem nos recursos que você e seus desenvolvedores usam. Você pode configurar notificações para que os usuários de um recurso, como um projeto de compilação, um repositório, um aplicativo de implantação ou um pipeline, recebam e-mails sobre os tipos de evento que você especifica de acordo com a regra de notificação que você cria.

As notificações para o AWS CodeCommit podem conter informações de identidade do usuário, como um nome de exibição ou um endereço de e-mail por meio do uso de tags de sessão. O CodeCommit oferece suporte ao uso de tags de sessão, que são atributos do par de chave/valor que você transmite quando assume uma função do IAM, usa credenciais temporárias ou federa um usuário no AWS Security Token Service (AWS STS). Você também pode associar tags a um usuário do IAM. O CodeCommit incluirá os valores para `displayName` e `emailAddress`no conteúdo de

notificação se essas tags estiverem presentes. Para obter mais informações, consulte Uso de tags para fornecer informações adicionais de identidade no CodeCommit.

> **Important**
>
> As notificações incluem informações específicas ao projeto, como status de compilações, status de implantação, linhas de código que têm comentários e aprovações de pipeline. O conteúdo da notificação pode mudar à medida que novos recursos são adicionados. Como prática recomendada de segurança, você deve revisar regularmente os destinos das regras de notificação e os assinantes do tópico do Amazon SNS. Para obter mais informações, consulte Noções básicas do conteúdo e da segurança das notificações.

Regras de notificação

Uma regra de notificação é um recurso da AWS que você cria para especificar quando e para onde as notificações são enviadas. Ela define:

- As condições nas quais uma notificação é criada. Essas condições são baseadas em eventos que você escolhe, que são específicos ao tipo de recurso. Os tipos de recursos compatíveis incluem projetos de compilação no AWS CodeBuild, aplicativos de implantação no AWS CodeDeploy, pipelines no AWS CodePipeline e repositórios no AWS CodeCommit.
- Os destinos aos quais a notificação é enviada. Você pode especificar até 10 destinos para uma regra de notificação.

As regras de notificação têm escopo para projetos de compilação, aplicativos de implantação, pipelines e repositórios individuais. As regras de notificação têm nomes amigáveis definidos pelo usuário e nomes de recurso da Amazon (ARNs). As regras de notificação devem ser criadas na mesma região da AWS em que está o recurso. Por exemplo, se o projeto de compilação estiver na região Leste dos EUA (Ohio), sua regra de notificação deverá ser criada na região Leste dos EUA (Ohio) também.

Você pode definir até 10 regras de notificação para um recurso.

Eventos

Um evento é uma alteração de estado em um recurso que você deseja monitorar. Cada recurso tem uma lista de tipos de evento que você pode escolher. Ao configurar uma regra de notificação

em um recurso, você especifica os eventos que fazem com que as notificações sejam enviadas. Por exemplo, se você configurar notificações para um repositório no CodeCommit e selecionar Created (Criado) para Pull request (Solicitação pull) e Branches and tags (Ramificações e tags), uma notificação será enviada sempre que um usuário nesse repositório criar uma solicitação pull, uma ramificação ou uma tag Git.

Tipos de detalhes

Ao criar uma regra de notificação, é possível escolher o nível de detalhe ou o tipo de detalhe incluído nas notificações (Full (Completo) ou Basic (Básico)). A configuração Full (Completo) (padrão) inclui todas as informações disponíveis para o evento na notificação, incluindo as informações aprimoradas fornecidas pelos serviços para eventos específicos. A configuração Basic (Básico) inclui apenas um subconjunto das informações disponíveis.

A tabela a seguir lista as informações aprimoradas disponíveis para tipos de evento específicos e descreve as diferenças entre os tipos de detalhes.

Serviço	Evento	Full (Completo) inclui	Basic (Básico) não inclui
CodeCommit	Comentários sobre confirmações Comentários sobre solicitações pull	Todos os detalhes do evento e o conteúdo do comentário, incluindo respostas ou cadeias de comentários. Ele também inclui o número da linha e a linha do código em que o comentário foi feito.	O conteúdo do comentário, número da linha, linha do código ou cadeias de comentário.
CodeCommit	Solicitação pull criada	Todos os detalhes do evento e o número de arquivos que foram adicionados, modificados ou excluídos na solicitação pull em relação	Nenhuma lista de arquivos ou detalhes sobre se a ramificação de origem da solicitação pull adicionou, modificou ou excluiu arquivos.

Serviço	Evento	Full (Completo) inclui	Basic (Básico) não inclui
		à ramificação de destino.	
CodePipeline	Aprovação manual necessária	Todos os detalhes do evento e dados personalizados (se configurados). A notificação também inclui um link para a aprovação necessária no pipeline.	Nenhum link ou dado personalizado.
CodePipeline	Falha na execução da ação Falha na execução do pipeline Falha na execução do estágio	Todos os detalhes do evento e o conteúdo da mensagem de erro para a falha.	Nenhum conteúdo da mensagem de erro.

Destinos

Um destino é um local para receber notificações de regras de notificação. Os tipos de destino permitidos são tópicos do Amazon SNS e clientes do AWS Chatbot configurados para canais do Slack ou do Microsoft Teams. Qualquer usuário inscrito no tópico de destino recebe notificações sobre os eventos que você especificar na regra de notificação.

Se quiser estender o alcance das notificações, você poderá configurar a integração entre as notificações e o AWS Chatbot para que as notificações sejam enviadas para as salas de chat do Amazon Chime. Depois, você poderá selecionar o tópico do Amazon SNS configurado para esse cliente do AWS Chatbot como o destino da regra de notificação. Para obter mais informações, consulte Como integrar notificações com o AWS Chatbot e o Amazon Chime.

Se optar por usar um cliente do AWS Chatbot como destino, você deverá primeiro criar esse cliente no AWS Chatbot. Ao selecionar um cliente do AWS Chatbot como destino para uma regra de notificação, um tópico do Amazon SNS é configurado para esse cliente do AWS Chatbot com todas as políticas necessárias para que as notificações sejam enviadas para o canal do Slack ou do Microsoft Teams. Não é necessário configurar nenhum tópico do Amazon SNS existente para o cliente do AWS Chatbot.

Opte por criar um tópico do Amazon SNS como destino como parte da criação de uma regra de notificação (recomendado). Também é possível escolher um tópico do Amazon SNS existente na mesma região da AWS que a regra de notificação, mas você deve configurá-lo com a política necessária. O tópico do Amazon SNS que você usa para um destino deve estar em sua conta da AWS. Ele também deve estar na mesma região da AWS que a regra de notificação e o recurso da AWS para o qual a regra foi criada.

Por exemplo, se você criar uma regra de notificação para um repositório na região Leste dos EUA (Ohio), o tópico do Amazon SNS também deverá estar nessa região. Se você criar um tópico do Amazon SNS como parte da criação de uma regra de notificação, o tópico será configurado com a política necessária para permitir a publicação de eventos no tópico. Este é o melhor método para trabalhar com destinos e regras de notificação. Se você optar por usar um tópico já existente ou criar um manualmente, será necessário configurá-lo com as permissões necessárias para que os usuários recebam notificações. Para obter mais informações, consulte Configurar tópicos do Amazon SNS para notificações.

> **Note**
>
> Se desejar usar um tópico do Amazon SNS existente em vez de criar um novo, em Targets (Destinos), escolha o ARN. Certifique-se de que o tópico tenha a política de acesso adequada e que a lista de assinantes contenha apenas os usuários que têm permissão para ver informações sobre o recurso. Se o tópico do Amazon SNS já tiver sido usado para notificações do CodeCommit antes de 5 de novembro de 2019, ele terá uma política que permite ao CodeCommit publicar nele e que contém permissões diferentes daquelas exigidas pelo AWS CodeStar Notifications. Não é recomendado usar esses tópicos. Se desejar usar um tópico criado para essa experiência, será necessário adicionar a política exigida para o AWS CodeStar Notifications, além daquela já existente. Para obter mais informações, consulte Configurar tópicos do Amazon SNS para notificações e Noções básicas do conteúdo e da segurança das notificações.

Notificações e AWS CodeStar Notifications

Por ser um recurso do console do Developer Tools, as notificações têm sua própria API, o AWS CodeStar Notifications. Ele também tem seu próprio tipo de recurso da AWS (regras de notificação), permissões e eventos. Os eventos para regras de notificação são registrados no AWS CloudTrail. As ações de API podem ser permitidas ou negadas por meio de políticas do IAM.

Eventos para regras de notificação em repositórios

Categoria	Eventos	IDs de evento

Comentários	Em confirmações
	
	Em solicitações pull
		`codecommit-repository-comments-on-commits`
		
		`codecommit-repository-comments-on-pull-requests`

Aprovações	Status alterado
	
	Substituição de regra
		`codecommit-repository-approvals-status-changed`
		
		`codecommit-repository-approvals-rule-override`

Solicitação pull	Criado
	
	Origem atualizada
	
	Status alterado
	
	Mesclado
		`codecommit-repository-pull-request-created`
		
		`codecommit-repository-pull-request-source-updated`
		
		`codecommit-repository-pull-request-status-changed`
		
		`codecommit-repository-pull-request-merged`

Categoria	Eventos	IDs de evento

Ramificações e tags	Criado
	Deleted (Excluído)
	Atualizado
		`codecommit-repository-branches-and-tags-created`
		`codecommit-repository-branches-and-tags-deleted`
		`codecommit-repository-branches-and-tags-updated`

Eventos para regras de notificação em projetos de compilação

Categoria	Eventos	IDs de evento

Estado da compilação	Reprovada
	Bem-sucedido
	Em andamento
	Interrompida
		`codebuild-project-build-state-failed`
		`codebuild-project-build-state-succeeded`
		`codebuild-project-build-state-in-progress`
		`codebuild-project-build-state-stopped`

Fase da compilação	Falha Bem-sucedida	`codebuild-project-build-phase-failure` `codebuild-project-build-phase-success`

Eventos de regras de notificação em aplicações de implantação

Categoria	Eventos	IDs de evento

Implantação	Reprovada
	Bem-sucedido
	Started
		`codedeploy-application-deployment-failed`
		`codedeploy-application-deployment-succeeded`
		`codedeploy-application-deployment-started`

Eventos para regras de notificação em pipelines

Categoria	Eventos	IDs de evento

Execução da ação	Bem-sucedido
	Reprovada
	Canceled
	Started
		`codepipeline-pipeline-action-execution-succeeded`
		`codepipeline-pipeline-action-execution-failed`
		`codepipeline-pipeline-action-execution-canceled`
		`codepipeline-pipeline-action-execution-started`

Execução do estágio	Started
	Bem-sucedido
	Retomado
	Canceled
	Reprovada
		`codepipeline-pipeline-stage-execution-started`
		`codepipeline-pipeline-stage-execution-succeeded`
		`codepipeline-pipeline-stage-execution-resumed`

Categoria	Eventos	IDs de evento
		codepipeline-pipeline-stage-execution-canceled codepipeline-pipeline-stage-execution-failed
Execução do pipeline	Reprovada Canceled Started Retomado Bem-sucedido Substituído	codepipeline-pipeline-pipeline-execution-failed codepipeline-pipeline-pipeline-execution-canceled codepipeline-pipeline-pipeline-execution-started codepipeline-pipeline-pipeline-execution-resumed codepipeline-pipeline-pipeline-execution-succeeded codepipeline-pipeline-pipeline-execution-superseded
Aprovação manual	Reprovada Necessário Bem-sucedido	codepipeline-pipeline-manual-approval-failed codepipeline-pipeline-manual-approval-needed codepipeline-pipeline-manual-approval-succeeded

Configuração

Se tiver uma política gerenciada para AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy ou AWS CodePipeline aplicada ao usuário ou função do IAM, você terá as permissões necessárias para trabalhar com notificações dentro das limitações das funções e

permissões fornecidas pela política. Por exemplo, os usuários que têm a política gerenciada `AWSCodeBuildAdminAccess`, `AWSCodeCommitFullAccess`, `AWSCodeDeployFullAccess` ou `AWSCodePipeline_FullAccess` aplicada têm acesso administrativo total às notificações.

Para obter mais informações, incluindo exemplos de políticas, consulte Políticas baseadas em identidade.

Se tiver uma dessas políticas aplicada ao usuário ou função do IAM e um projeto de compilação no CodeBuild, um repositório no CodeCommit, uma aplicação de implantação no CodeDeploy ou um pipeline no CodePipeline, você estará pronto para criar sua primeira regra de notificação. Avance para Conceitos básicos das notificações. Caso contrário, consulte os seguintes tópicos:

- CodeBuild: Conceitos básicos do CodeBuild
- CodeCommit: Conceitos básicos do CodeCommit
- CodeDeploy: Tutoriais
- CodePipeline: Conceitos básicos do CodePipeline

Se desejar gerenciar permissões administrativas para notificações para usuários, grupos ou funções do IAM, siga os procedimentos neste tópico para configurar as permissões e os recursos necessários para usar o serviço.

Se desejar usar tópicos do Amazon SNS criados anteriormente para notificações em vez de criar tópicos especificamente para notificações, deverá configurar um tópico do Amazon SNS para usar como destino de uma regra de notificação aplicando uma política que permita que eventos sejam publicados nesse tópico.

> **Note**
>
> Para executar os procedimentos a seguir, você deve estar conectado com uma conta que tenha permissões administrativas. Para obter informações, consulte Criação do seu primeiro usuário administrador e grupo do IAM.

Tópicos

- Criar e aplicar uma política de acesso administrativo a notificações
- Configurar tópicos do Amazon SNS para notificações
- Inscrever usuários em tópicos do Amazon SNS que são destinos

Criar e aplicar uma política de acesso administrativo a notificações

Você pode administrar notificações entrando com um usuário do IAM ou usando uma função que tenha permissões para acessar o serviço e os serviços (AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy ou AWS CodePipeline) para os quais você deseja criar notificações. Você também pode criar suas próprias políticas e aplicá-las a usuários ou grupos.

O procedimento a seguir mostra como configurar um grupo do IAM com permissões para administrar notificações e adicionar usuários do IAM. Se não desejar configurar um grupo, você poderá aplicar essa política diretamente a usuários do IAM ou a uma função do IAM que possa ser assumida pelos usuários. Você também pode usar as políticas gerenciadas para CodeBuild, CodeCommit, CodeDeploy ou CodePipeline, que incluem acesso apropriado à política a recursos de notificação, dependendo do escopo da política.

Para a política abaixo, insira um nome (por exemplo, `AWSCodeStarNotificationsFullAccess`) e uma descrição opcional para essa política. A descrição ajuda você a lembrar do propósito da política (por exemplo, **`This policy provides full access to AWS CodeStar Notifications.`**)

Para usar o editor de políticas JSON para criar uma política

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Políticas.

   Se essa for a primeira vez que escolhe Políticas, a página Bem-vindo às políticas gerenciadas será exibida. Escolha Get Started.
3. Na parte superior da página, escolha Create policy (Criar política).
4. Na seção Editor de políticas, escolha a opção JSON.
5. Insira o seguinte documento de política JSON:

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Sid": "AWSCodeStarNotificationsFullAccess",
       "Effect": "Allow",
       "Action": [
           "codestar-notifications:CreateNotificationRule",
```

```
            "codestar-notifications:DeleteNotificationRule",
            "codestar-notifications:DescribeNotificationRule",
            "codestar-notifications:ListNotificationRules",
            "codestar-notifications:UpdateNotificationRule",
            "codestar-notifications:Subscribe",
            "codestar-notifications:Unsubscribe",
            "codestar-notifications:DeleteTarget",
            "codestar-notifications:ListTargets",
            "codestar-notifications:ListTagsforResource",
            "codestar-notifications:TagResource",
            "codestar-notifications:UntagResource"
        ],
        "Resource": "*"
      }
   ]
}
```

6. Escolha Next (Próximo).

> **Note**
>
> Você pode alternar entre as opções de editor Visual e JSON a qualquer momento. Porém, se você fizer alterações ou escolher Avançar no editor Visual, o IAM poderá reestruturar a política a fim de otimizá-la para o editor visual. Para obter mais informações, consulte Restruturação de política no Manual do usuário do IAM.

7. Na página Revisar e criar, insira um Nome de política e uma Descrição (opcional) para a política que você está criando. Revise Permissões definidas nessa política para ver as permissões que são concedidas pela política.
8. Escolha Create Policy (Criar política) para salvar sua nova política.

Configurar tópicos do Amazon SNS para notificações

A maneira mais fácil de configurar notificações é criar um tópico do Amazon SNS ao criar uma regra de notificação. Você poderá usar um tópico do Amazon SNS existente se ele atender aos seguintes requisitos:

- Ele foi criado na mesma Região da AWS que o recurso (projeto de compilação, aplicação de implantação, repositório ou pipeline) para o qual você deseja criar regras de notificação.

- Ele não foi usado para enviar notificações para o CodeCommit antes de 5 de novembro de 2019. Se tiver sido, ele conterá instruções de política que ativaram essa funcionalidade. É possível optar por usar esse tópico, mas será necessário adicionar a outra política conforme especificado no procedimento. Você não deverá remover a instrução de política existente se um ou mais repositórios ainda estiverem configurados para notificações antes de 5 de novembro de 2019.
- Ele tem uma política que permite ao AWS CodeStar Notifications publicar notificações no tópico.

Para configurar um tópico do Amazon SNS a ser usado como destino para regras de notificação do AWS CodeStar Notifications

1. Faça login no AWS Management Console e abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na barra de navegação, escolha Topics (Tópicos), escolha o tópico que deseja configurar e Edit (Editar).
3. Expanda Access policy (Política de acesso) e, em seguida, escolha Advanced (Avançado).
4. No editor de JSON, adicione a declaração a seguir à política. Inclua o ARN do tópico, a Região da AWS, o ID da Conta da AWS e o nome do tópico.

```
 {
      "Sid": "AWSCodeStarNotifications_publish",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "codestar-notifications.amazonaws.com"
        ]
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-
MyTopicForNotificationRules"
    }
```

A declaração da política deve ser semelhante ao seguinte.

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__default_statement_ID",
```

```
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "SNS:GetTopicAttributes",
        "SNS:SetTopicAttributes",
        "SNS:AddPermission",
        "SNS:RemovePermission",
        "SNS:DeleteTopic",
        "SNS:Subscribe",
        "SNS:ListSubscriptionsByTopic",
        "SNS:Publish",
        "SNS:Receive"
      ],
      "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-
MyTopicForNotificationRules",
      "Condition": {
        "StringEquals": {
          "AWS:SourceOwner": "123456789012"
        }
      }
    },
 {
      "Sid": "AWSCodeStarNotifications_publish",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "codestar-notifications.amazonaws.com"
        ]
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-
MyTopicForNotificationRules"
    }
  ]
}
```

5. Escolha Save changes (Salvar alterações).
6. Se desejar usar um tópico do Amazon SNS criptografado pelo AWS KMS para enviar notificações, você deverá ativar a compatibilidade entre a fonte do evento (AWS CodeStar Notifications) e o tópico criptografado adicionando a instrução a seguir à política da AWS KMS

key. Substitua a Região da AWS (neste exemplo, us-east-2) pela Região da AWS onde a chave foi criada.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "codestar-notifications.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "sns.us-east-2.amazonaws.com"
                }
            }
        }
    ]
}
```

Para obter mais informações, consulte Criptografia em repouso e Como usar condições de políticas com o AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Inscrever usuários em tópicos do Amazon SNS que são destinos

Para que os usuários possam receber notificações, eles deverão estar inscritos no tópico do Amazon SNS que é o destino da regra de notificação. Se os usuários estiverem inscritos por endereço de e-mail, eles deverão confirmar a assinatura antes de receberem notificações. Para enviar notificações a usuários em canais do Slack, canais do Microsoft Teams ou salas de bate-papo do Amazon Chime, consulte Configurar a integração entre notificações e o AWS Chatbot.

Para inscrever usuários em um tópico do Amazon SNS usado para notificações

1. Faça login no AWS Management Console e abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.

2. No painel de navegação, escolha Topics (Tópicos) e escolha o tópico ao qual você deseja inscrever usuários.
3. Em Subscriptions (Assinaturas), selecione Create subscription (Criar assinatura).
4. Em Protocol (Protocolo), selecione Email. Em Endpoint, insira o endereço de e-mail e escolha Create subscription (Criar assinatura).

Conceitos básicos das notificações

A maneira mais fácil de começar a usar notificações é configurar uma regra de notificação em um de seus projetos de compilação, aplicativos de implantação, pipelines ou repositórios.

> **Note**
>
> Na primeira vez que você criar uma regra de notificação, uma função vinculada ao serviço será criada em sua conta. Para obter mais informações, consulte Uso de funções vinculadas ao serviço para AWS CodeStar Notifications..

Tópicos

Pré-requisitos

Siga as etapas em Configuração. Você também precisa de um recurso para o qual cria uma regra de notificação.

- Crie um projeto de compilação no CodeBuild ou use um existente.
- Crie uma aplicação ou use uma aplicação de implantação existente.
- Crie um pipeline no CodePipeline ou use um pipeline existente.
- Create an AWS CodeCommit repository (Crie um repositório do AWS CodeCommit) ou use um repositório existente.

Criar uma regra de notificação para um repositório

É possível criar regras de notificação para enviar notificações sobre eventos de repositório que são importantes para você. As etapas a seguir mostram como configurar uma regra de notificação em um único evento do repositório. Essas etapas são escritas com a suposição de que você tem um repositório configurado em sua conta da AWS.

> **Important**
>
> Se você configurou notificações no CodeCommit antes de 5 de novembro de 2019, os tópicos do Amazon SNS usados para essas notificações conterão uma política que permitirá ao CodeCommit publicar nele e que contém permissões diferentes daquelas exigidas para o AWS CodeStar Notifications. Não é recomendado usar esses tópicos. Se desejar usar um tópico criado para essa experiência, será necessário adicionar a política exigida para o AWS CodeStar Notifications, além daquela já existente. Para obter mais informações, consulte Configurar tópicos do Amazon SNS para notificações e Noções básicas do conteúdo e da segurança das notificações.

1. Abra o console do CodeCommit em https://console.aws.amazon.com/codecommit/.
2. Escolha um repositório na lista e abra-o.
3. Escolha Notify (Notificar) e Create notification rule (Criar regra de notificação). Você também pode escolher Settings (Configurações), Notifications (Notificações) e Create notification rule (Criar regra de notificação).
4. Em Notification name (Nome da notificação), insira um nome para a regra.
5. Em Detail type (Tipo de detalhe), escolha Basic (Básico) se desejar que apenas as informações fornecidas ao Amazon EventBridge sejam incluídas na notificação. Escolha Full (Completo) se desejar incluir as informações fornecidas ao Amazon EventBridge e as informações que possam ser fornecidas pelo serviço de recursos ou pelo gerenciador de notificações.

   Para obter mais informações, consulte Noções básicas do conteúdo e da segurança das notificações.
6. Em Events that trigger notifications (Eventos que acionam notificações), em Branches and tags (Ramificações e tags), selecione Created (Criado).
7. Em Targets (Destinos), escolha Create SNS topic (Criar tópico do SNS).

> **Note**
>
> Quando você cria o tópico como parte da criação da regra de notificação, a política que permite ao CodeCommit publicar eventos no tópico é aplicada a você. O uso de um tópico criado para regras de notificação ajuda a garantir que você inscreva apenas os usuários para os quais deseja enviar notificações sobre esse repositório.

Após o prefixo codestar-notifications-, insira um nome para o tópico e escolha Submit (Enviar).

> **Note**
>
> Se desejar usar um tópico do Amazon SNS existente em vez de criar um novo, em Targets (Destinos), escolha o ARN. Certifique-se de que o tópico tenha a política de acesso adequada e que a lista de assinantes contenha apenas os usuários que têm permissão para ver informações sobre o recurso. Se o tópico do Amazon SNS já tiver sido usado para notificações do CodeCommit antes de 5 de novembro de 2019, ele terá uma política que permite ao CodeCommit publicar nele e que contém permissões diferentes daquelas exigidas pelo AWS CodeStar Notifications. Não é recomendado usar esses tópicos. Se desejar usar um tópico criado para essa experiência, será necessário adicionar a política exigida para o AWS CodeStar Notifications, além daquela já existente. Para obter mais informações, consulte Configurar tópicos do Amazon SNS para notificações e Noções básicas do conteúdo e da segurança das notificações.

8. Escolha Submit (Enviar) e revise a regra de notificação.
9. Inscreva seu endereço de e-mail no tópico do Amazon SNS que acabou de criar. Para obter mais informações, consulte Para inscrever usuários em um tópico do Amazon SNS usado para notificações.
10. Navegue até o repositório e crie uma ramificação de teste da ramificação padrão.
11. Depois de criar a ramificação, a regra de notificação envia uma notificação a todos os assinantes do tópico com informações sobre esse evento.

Criar uma regra de notificação para um projeto de compilação

É possível criar regras de notificação para enviar notificações sobre os eventos no projeto de compilação que são importantes para você. As etapas a seguir mostram como configurar uma regra

de notificação em um único evento do projeto de compilação. Estas etapas são escritas com a suposição de que você tem um projeto de compilação configurado em sua conta da AWS.

1. Abra o console do CodeBuild em.https://console.aws.amazon.com/codebuild/.
2. Escolha um projeto de compilação na lista e abra-o.
3. Escolha Notify (Notificar) e Create notification rule (Criar regra de notificação). Você também pode escolher Settings (Configurações) e Create notification rule (Criar regra de notificação).
4. Em Notification name (Nome da notificação), insira um nome para a regra.
5. Em Detail type (Tipo de detalhe), escolha Basic (Básico) se desejar que apenas as informações fornecidas ao Amazon EventBridge sejam incluídas na notificação. Escolha Full (Completo) se desejar incluir as informações fornecidas ao Amazon EventBridge e as informações que possam ser fornecidas pelo serviço de recursos ou pelo gerenciador de notificações.

   Para obter mais informações, consulte Noções básicas do conteúdo e da segurança das notificações.
6. Em Events that trigger notifications (Eventos que acionam notificações), em Build phase (Fase de compilação), selecione Success (Sucesso).
7. Em Targets (Destinos), escolha Create SNS topic (Criar tópico do SNS).

> **Note**
>
> Quando você cria o tópico como parte da criação da regra de notificação, a política que permite ao CodeBuild publicar eventos no tópico é aplicada a você. O uso de um tópico criado para regras de notificação ajuda a garantir que você inscreva apenas os usuários para os quais deseja enviar notificações sobre esse projeto de compilação.

Após o prefixo codestar-notifications-, insira um nome para o tópico e escolha Submit (Enviar).

> **Note**
>
> Se desejar usar um tópico do Amazon SNS existente em vez de criar um novo, em Targets (Destinos), escolha o ARN. Certifique-se de que o tópico tenha a política de acesso adequada e que a lista de assinantes contenha apenas os usuários que têm permissão para ver informações sobre o recurso. Se o tópico do Amazon SNS já tiver sido usado para notificações do CodeCommit antes de 5 de novembro de 2019, ele

terá uma política que permite ao CodeCommit publicar nele e que contém permissões diferentes daquelas exigidas pelo AWS CodeStar Notifications. Não é recomendado usar esses tópicos. Se desejar usar um tópico criado para essa experiência, será necessário adicionar a política exigida para o AWS CodeStar Notifications, além daquela já existente. Para obter mais informações, consulte Configurar tópicos do Amazon SNS para notificações e Noções básicas do conteúdo e da segurança das notificações.

8. Escolha Submit (Enviar) e revise a regra de notificação.
9. Inscreva seu endereço de e-mail no tópico do Amazon SNS que acabou de criar. Para obter mais informações, consulte Para inscrever usuários em um tópico do Amazon SNS usado para notificações.
10. Navegue até o projeto de compilação e inicie uma compilação.
11. Depois que a fase de compilação for concluída com êxito, a regra de notificação enviará uma notificação a todos os assinantes do tópico com informações sobre esse evento.

Criar uma regra de notificação para uma aplicação de implantação

É possível criar regras de notificação para enviar notificações sobre os eventos em seu aplicativo de implantação que são importantes para você. As etapas a seguir mostram como configurar uma regra de notificação em um único evento do projeto de compilação. Essas etapas são escritas com a suposição de que você tem um aplicativo de implantação configurado em sua conta da AWS.

1. Abra o console do CodeDeploy em https://console.aws.amazon.com/codedeploy/.
2. Escolha um aplicativo na lista e abra-o.
3. Escolha Notify (Notificar) e Create notification rule (Criar regra de notificação). Você também pode escolher Settings (Configurações) e Create notification rule (Criar regra de notificação).
4. Em Notification name (Nome da notificação), insira um nome para a regra.
5. Em Detail type (Tipo de detalhe), escolha Basic (Básico) se desejar que apenas as informações fornecidas ao Amazon EventBridge sejam incluídas na notificação. Escolha Full (Completo) se desejar incluir as informações fornecidas ao Amazon EventBridge e as informações que possam ser fornecidas pelo serviço de recursos ou pelo gerenciador de notificações.

   Para obter mais informações, consulte Noções básicas do conteúdo e da segurança das notificações.

6. Em Events that trigger notifications (Eventos que acionam notificações), em Deployment (Implantação), selecione Succeeded (Com sucesso).
7. Em Targets (Destinos), escolha Create SNS topic (Criar tópico do SNS).

> **Note**
>
> Quando você cria o tópico como parte da criação da regra de notificação, a política que permite ao CodeDeploy publicar eventos no tópico é aplicada a você. O uso de um tópico criado para regras de notificação ajuda a garantir que você assine apenas os usuários para os quais deseja enviar notificações sobre esse aplicativo de implantação.

Após o prefixo codestar-notifications-, insira um nome para o tópico e escolha Submit (Enviar).

> **Note**
>
> Se desejar usar um tópico do Amazon SNS existente em vez de criar um novo, em Targets (Destinos), escolha o ARN. Certifique-se de que o tópico tenha a política de acesso adequada e que a lista de assinantes contenha apenas os usuários que têm permissão para ver informações sobre o recurso. Se o tópico do Amazon SNS já tiver sido usado para notificações do CodeCommit antes de 5 de novembro de 2019, ele terá uma política que permite ao CodeCommit publicar nele e que contém permissões diferentes daquelas exigidas pelo AWS CodeStar Notifications. Não é recomendado usar esses tópicos. Se desejar usar um tópico criado para essa experiência, será necessário adicionar a política exigida para o AWS CodeStar Notifications, além daquela já existente. Para obter mais informações, consulte Configurar tópicos do Amazon SNS para notificações e Noções básicas do conteúdo e da segurança das notificações.

8. Escolha Submit (Enviar) e revise a regra de notificação.
9. Inscreva seu endereço de e-mail no tópico do Amazon SNS que acabou de criar. Para obter mais informações, consulte Para inscrever usuários em um tópico do Amazon SNS usado para notificações.
10. Navegue até o aplicativo de implantação e inicie uma implantação.
11. Depois que a implantação for bem-sucedida, a regra de notificação enviará uma notificação para todos os assinantes de tópico com informações sobre o evento.

Criar uma regra de notificação para um pipeline

É possível criar regras de notificação para enviar notificações sobre os eventos em seu pipeline que são importantes para você. As etapas a seguir mostram como configurar uma regra de notificação em um único evento do pipeline. Essas etapas são escritas com a suposição de que você tem um pipeline configurado em sua conta da AWS.

1. Abra o console do CodePipeline em https://console.aws.amazon.com/codesuite/codepipeline.
2. Escolha um pipeline na lista e abra-o.
3. Escolha Notify (Notificar) e Create notification rule (Criar regra de notificação). Você também pode escolher Settings (Configurações) e Create notification rule (Criar regra de notificação).
4. Em Notification name (Nome da notificação), insira um nome para a regra.
5. Em Detail type (Tipo de detalhe), escolha Basic (Básico) se desejar que apenas as informações fornecidas ao Amazon EventBridge sejam incluídas na notificação. Escolha Full (Completo) se desejar incluir as informações fornecidas ao Amazon EventBridge e as informações que possam ser fornecidas pelo serviço de recursos ou pelo gerenciador de notificações.

   Para obter mais informações, consulte Noções básicas do conteúdo e da segurança das notificações.
6. Em Events that trigger notifications (Eventos que acionam notificações), em Action execution (Execução da ação), selecione Started (Iniciado).
7. Em Targets (Destinos), escolha Create SNS topic (Criar tópico do SNS).

   > **Note**
   >
   > Quando você cria o tópico como parte da criação da regra de notificação, a política que permite ao CodePipeline publicar eventos no tópico é aplicada a você. O uso de um tópico criado para regras de notificação ajuda a garantir que você inscreva apenas os usuários para os quais deseja enviar notificações sobre esse pipeline.

   Após o prefixo codestar-notifications-, insira um nome para o tópico e escolha Submit (Enviar).

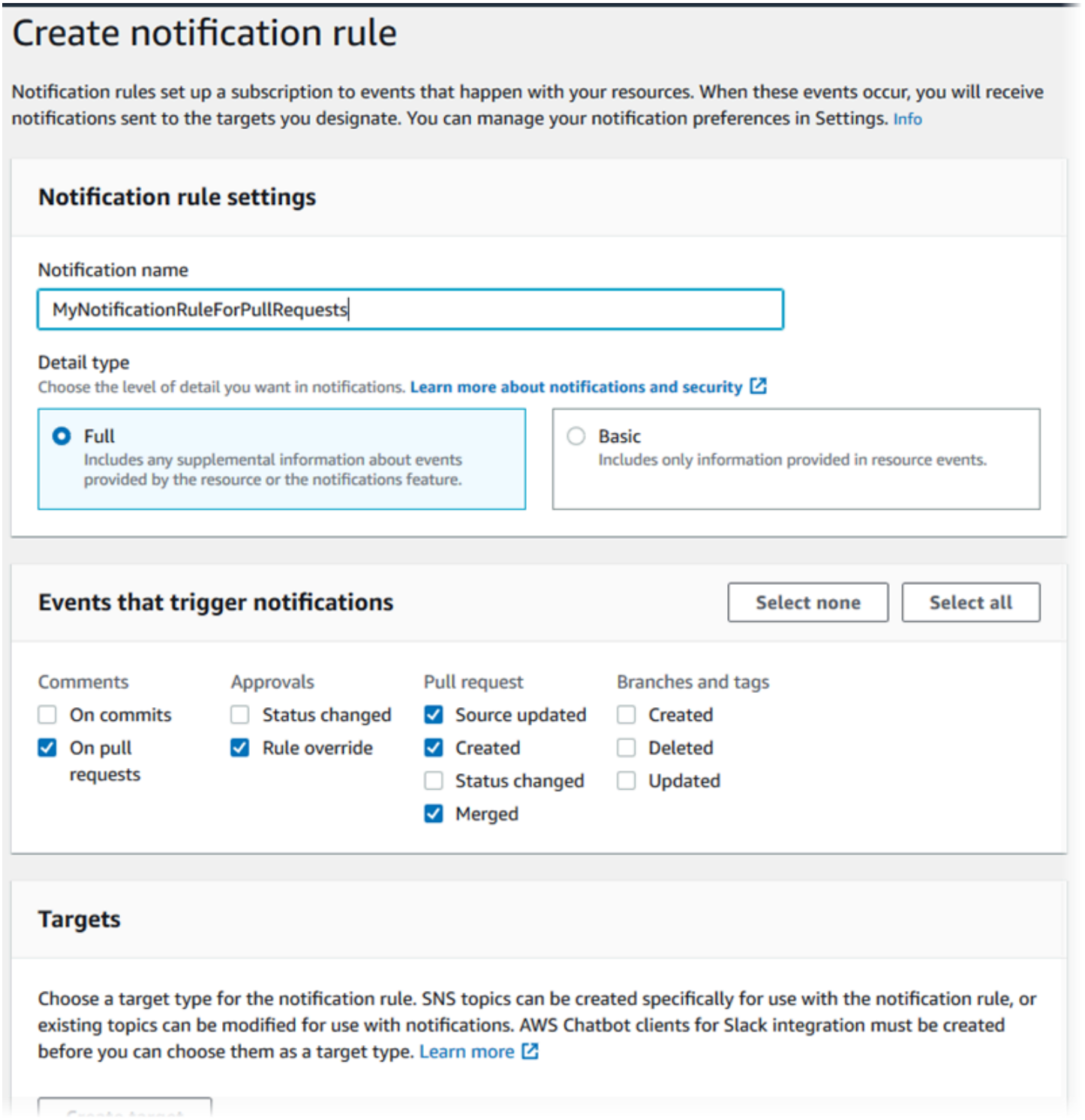
   > **Note**
   >
   > Se desejar usar um tópico do Amazon SNS existente em vez de criar um novo, em Targets (Destinos), escolha o ARN. Certifique-se de que o tópico tenha a política de

acesso adequada e que a lista de assinantes contenha apenas os usuários que têm permissão para ver informações sobre o recurso. Se o tópico do Amazon SNS já tiver sido usado para notificações do CodeCommit antes de 5 de novembro de 2019, ele terá uma política que permite ao CodeCommit publicar nele e que contém permissões diferentes daquelas exigidas pelo AWS CodeStar Notifications. Não é recomendado usar esses tópicos. Se desejar usar um tópico criado para essa experiência, será necessário adicionar a política exigida para o AWS CodeStar Notifications, além daquela já existente. Para obter mais informações, consulte Configurar tópicos do Amazon SNS para notificações e Noções básicas do conteúdo e da segurança das notificações.

8. Escolha Submit (Enviar) e revise a regra de notificação.
9. Inscreva seu endereço de e-mail no tópico do Amazon SNS que acabou de criar. Para obter mais informações, consulte Para inscrever usuários em um tópico do Amazon SNS usado para notificações.
10. Navegue até o pipeline e escolha Release change (Alteração feita no release).
11. Quando a ação é iniciada, a regra de notificação envia uma notificação a todos os assinantes do tópico com informações sobre o evento.

Como trabalhar com regras de notificação

Na regra de notificação, você configura os eventos sobre os quais deseja que os usuários recebam notificações e especifica os destinos que receberão essas notificações. É possível enviar notificações diretamente aos usuários por meio do Amazon SNS ou de clientes do AWS Chatbot configurados para canais Slack ou do Microsoft Teams. Se quiser estender o alcance das notificações, você poderá configurar a integração entre as notificações e o AWS Chatbot para que as notificações sejam enviadas para as salas de chat do Amazon Chime. Para obter mais informações, consulte Destinos e Como integrar notificações com o AWS Chatbot e o Amazon Chime.



É possível usar o console do Developer Tools ou o AWS CLI para criar e gerenciar regras de notificação.

Tópicos

- Criar uma regra de notificação

- Visualizar regras de notificação
- Editar uma regra de notificação
- Habilitar ou desabilitar notificações para uma regra de notificação
- Excluir uma notificação

Criar uma regra de notificação

É possível usar o console do Developer Tools ou o AWS CLI para criar regras de notificação. É possível criar um tópico do Amazon SNS para usar como destino para uma regra de notificação como parte da criação da regra. Se desejar usar um cliente do AWS Chatbot como destino, será necessário criar esse cliente antes de criar a regra. Para obter mais informações, consulte Configurar um cliente do AWS Chatbot para um canal do Slack.

Como criar uma regra de notificação (console)

1. Abra o console do AWS Developer Tools em https://console.aws.amazon.com/codesuite/settings/notifications.
2. Use a barra de navegação para navegar até o recurso.
   - Para o CodeBuild, escolha Build (Compilar), Build projects (Projetos de compilação) e escolha um projeto de compilação.
   - Para o CodeCommit, escolha Source (Origem), Repositories (Repositórios) e escolha um repositório.
   - Para o CodeDeploy, escolha Applications (Aplicações) e escolha uma aplicação.
   - Para o CodePipeline, escolha Pipeline, Pipelines e escolha um pipeline.
3. Na página do recurso, escolha Notify (Notificar) e Create notification rule (Criar regra de notificação). Você também pode acessar a página Settings (Configurações) do recurso, acessar Notifications (Notificações) ou Notification rules (Regras de notificação) e escolher Create notification rule (Criar regra de notificação).
4. Em Notification name (Nome da notificação), insira um nome para a regra.
5. Em Detail type (Tipo de detalhe), escolha Basic (Básico) se desejar que apenas as informações fornecidas ao Amazon EventBridge sejam incluídas na notificação. Escolha Full (Completo) se desejar incluir as informações fornecidas ao Amazon EventBridge e as informações que possam ser fornecidas pelo serviço de recursos ou pelo gerenciador de notificações.

Para obter mais informações, consulte Noções básicas do conteúdo e da segurança das notificações.

6. Em Events that trigger notifications (Eventos que acionam notificações), selecione os eventos para os quais você deseja enviar notificações. Para saber os tipos de evento para um recurso, consulte o seguinte:

   - CodeBuild: Eventos para regras de notificação em projetos de compilação
   - CodeCommit: Eventos para regras de notificação em repositórios
   - CodeDeploy: Eventos de regras de notificação em aplicações de implantação
   - CodePipeline: Eventos para regras de notificação em pipelines

7. Em Targets (Destinos), siga um destes procedimentos:

   - Se você já tiver configurado um recurso para usar com notificações, em Escolher tipo de destino, selecione AWS Chatbot (Slack), AWS Chatbot (Microsoft Teams) ou Tópico do SNS. Em Escolher destino, selecione o nome do cliente (para um cliente Slack ou do Microsoft Teams configurado no AWS Chatbot) ou o nome do recurso da Amazon (ARN) do tópico do Amazon SNS (para tópicos do Amazon SNS já configurados com a política necessária para notificações).
   - Se você não configurou um recurso para usar com notificações, escolha Create target (Criar destino) e selecione SNS topic (Tópico do SNS). Forneça um nome para o tópico após codestar-notifications- e escolha Create (Criar).

   > **Note**
   >
   > - Ao criar o tópico do Amazon SNS como parte da criação da regra de notificação, a política que permite ao recurso publicar eventos no tópico é aplicada para você. O uso de um tópico criado para regras de notificação ajuda a garantir que você inscreva somente os usuários para os quais deseja enviar notificações sobre esse recurso.
   > - Não é possível criar um cliente do AWS Chatbot como parte da criação de uma regra de notificação. Se você escolher AWS Chatbot (Slack) ou AWS Chatbot (Microsoft Teams), será exibido um botão que permitirá configurar um cliente no AWS Chatbot. Ao selecionar essa opção, você abrirá o console do AWS Chatbot. Para obter mais informações, consulte Configurar um cliente do AWS Chatbot para um canal do Slack.

- Se quiser usar um tópico do Amazon SNS existente como destino, você deverá adicionar a política necessária para o AWS CodeStar Notifications além de quaisquer outras políticas que possam existir para esse tópico. Para obter mais informações, consulte Configurar tópicos do Amazon SNS para notificações e Noções básicas do conteúdo e da segurança das notificações.

8. Escolha Submit (Enviar) e revise a regra de notificação.

> **Note**
>
> Os usuários devem se inscrever e confirmar assinaturas do tópico do Amazon SNS que você especificou como destino da regra antes de receberem notificações. Para obter mais informações, consulte Para inscrever usuários em um tópico do Amazon SNS usado para notificações.

Criar uma regra de notificação (AWS CLI)

1. Em um terminal ou prompt de comando, execute o comando create-notification rule para gerar o esqueleto JSON:

```
aws codestar-notifications create-notification-rule --generate-cli-skeleton
 > rule.json
```

É possível nomear o arquivo como você quiser. Neste exemplo, o arquivo é chamado *rule.json*.

2. Abra o arquivo JSON em um editor de texto simples e edite-o para incluir o recurso, os tipos de evento e o destino do Amazon SNS que você deseja para a regra.

O exemplo a seguir mostra uma regra de notificação chamada **MyNotificationRule** para um repositório chamado *MyDemoRepo* em uma conta da AWS com o ID *123456789012*. As notificações com o tipo de detalhe completo são enviadas para um tópico do Amazon SNS chamado *MyNotificationTopic* quando ramificações e tags são criadas.

```
{
    "Name": "MyNotificationRule",
```

```
    "EventTypeIds": [
        "codecommit-repository-branches-and-tags-created"
    ],
    "Resource": "arn:aws:codecommit:us-east-1:123456789012:MyDemoRepo",
    "Targets": [
        {
            "TargetType": "SNS",
            "TargetAddress": "arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic"
        }
    ],
    "Status": "ENABLED",
    "DetailType": "FULL"
}
```

Salve o arquivo.

3. Usando o arquivo que você acabou de editar, no terminal ou na linha de comando, execute o comando create-notification-rule novamente para criar a regra de notificação.

```
aws codestar-notifications create-notification-rule --cli-input-json
 file://rule.json
```

4. Se houver êxito, o comando retornará o ARN da regra de notificação, semelhante ao seguinte:

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}
```

Como listar tipos de evento para regras de notificação (AWS CLI)

1. Em um terminal ou prompt de comando, execute o comando list-event-types. É possível usar a opção `--filters` para limitar a resposta a um tipo de recurso específico ou a outro atributo. Por exemplo, o comando a seguir retorna uma lista de tipos de evento para aplicações do CodeDeploy.

```
aws codestar-notifications list-event-types --filters
 Name=SERVICE_NAME,Value=CodeDeploy
```

2. O comando gerará uma saída semelhante à seguinte:

```
{
    "EventTypes": [
        {
            "EventTypeId": "codedeploy-application-deployment-succeeded",
            "ServiceName": "CodeDeploy",
            "EventTypeName": "Deployment: Succeeded",
            "ResourceType": "Application"
        },
        {
            "EventTypeId": "codedeploy-application-deployment-failed",
            "ServiceName": "CodeDeploy",
            "EventTypeName": "Deployment: Failed",
            "ResourceType": "Application"
        },
        {
            "EventTypeId": "codedeploy-application-deployment-started",
            "ServiceName": "CodeDeploy",
            "EventTypeName": "Deployment: Started",
            "ResourceType": "Application"
        }
    ]
}
```

Como adicionar uma tag a uma regra de notificação (AWS CLI)

1. Em um terminal ou prompt de comando, execute o comando tag-resource. Por exemplo, use o comando a seguir para adicionar um par de chave/valor de tag que tenha o nome *Team* e o valor *Li_Juan*.

```
aws codestar-notifications tag-resource --arn arn:aws:codestar-notifications:us-
east-1:123456789012:notificationrule/fe1efd35-EXAMPLE --tags Team=Li_Juan
```

2. O comando gerará uma saída semelhante à seguinte:

```
{
    "Tags": {
        "Team": "Li_Juan"
    }
}
```

Visualizar regras de notificação

Você pode usar o console do Developer Tools ou a AWS CLI para visualizar todas as regras de notificação de todos os recursos em uma região da AWS. Você também pode exibir os detalhes de cada regra de notificação. Diferentemente do processo de criação de uma regra de notificação, não é necessário acessar a página de recursos para o recurso em questão.

Como visualizar regras de notificação (console)

1. Abra o console do AWS Developer Tools em https://console.aws.amazon.com/codesuite/settings/notifications.
2. Na barra de navegação, expanda Settings (Configurações) e escolha Notification rules (Regras de notificação).
3. Em Notification rules (Regras de notificação), revise a lista de regras configuradas para os recursos em sua Conta da AWS na Região da AWS à qual você está conectado no momento. Use o seletor para alterar a Região da AWS.
4. Para visualizar os detalhes de uma regra de notificação, escolha-a na lista e escolha View details (Visualizar detalhes). Você também pode simplesmente escolher seu nome na lista.

Como visualizar uma lista de regras de notificação (AWS CLI)

1. Em um terminal ou prompt de comando, execute o comando list-notification-rules para visualizar todas as regras de notificação para a região da AWS especificada.

```
aws codestar-notifications list-notification-rules --region us-east-1
```

2. Se houver êxito, esse comando retornará o ID e o ARN de cada regra de notificação na região da AWS, semelhante ao seguinte:

```
{
    "NotificationRules": [
        {
            "Id": "dc82df7a-EXAMPLE",
            "Arn": "arn:aws:codestar-notifications:us-
east-1:123456789012:notificationrule/dc82df7a-EXAMPLE"
        },
        {
            "Id": "8d1f0983-EXAMPLE",
```

```
            "Arn": "arn:aws:codestar-notifications:us-
east-1:123456789012:notificationrule/8d1f0983-EXAMPLE"
        }
    ]
}
```

Como visualizar detalhes de uma regra de notificação (AWS CLI)

1. Em um terminal ou prompt de comando, execute o comando describe-notification-rule, especificando o ARN da regra de notificação.

```
aws codestar-notifications describe-notification-rule --arn arn:aws:codestar-
notifications:us-east-1:123456789012:notificationrule/dc82df7a-EXAMPLE
```

2. Se houver êxito, o comando gerará uma saída semelhante à seguinte.

```
{
    "LastModifiedTimestamp": 1569199844.857,
    "EventTypes": [
        {
            "ServiceName": "CodeCommit",
            "EventTypeName": "Branches and tags: Created",
            "ResourceType": "Repository",
            "EventTypeId": "codecommit-repository-branches-and-tags-created"
        }
    ],
    "Status": "ENABLED",
    "DetailType": "FULL",
    "Resource": "arn:aws:codecommit:us-east-1:123456789012:MyDemoRepo",
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE",
    "Targets": [
        {
            "TargetStatus": "ACTIVE",
            "TargetAddress": "arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic",
            "TargetType": "SNS"
        }
    ],
    "Name": "MyNotificationRule",
    "CreatedTimestamp": 1569199844.857,
    "CreatedBy": "arn:aws:iam::123456789012:user/Mary_Major"
```

```
}
```

Como visualizar uma lista de tags para uma regra de notificação (AWS CLI)

1. Em um terminal ou prompt de comando, execute o comando list-tags-for-resource para visualizar todas as tags para o ARN de uma regra de notificação especificada.

```
aws codestar-notifications list-tags-for-resource --arn arn:aws:codestar-
notifications:us-east-1:123456789012:notificationrule/fe1efd35-EXAMPLE
```

2. Se houver êxito, o comando gerará uma saída semelhante à seguinte.

```
{
    "Tags": {
        "Team": "Li_Juan"
    }
}
```

Editar uma regra de notificação

É possível editar uma regra de notificação para alterar seu nome, os eventos para os quais ela envia notificações, o tipo de detalhe ou o destino ou destinos para os quais ela envia notificações. É possível usar o console do Developer Tools ou o AWS CLI para editar regras de notificação.

Como editar uma regra de notificação (console)

1. Abra o console do AWS Developer Tools em https://console.aws.amazon.com/codesuite/settings/notifications.
2. Na barra de navegação, expanda Settings (Configurações) e escolha Notification rules (Regras de notificação).
3. Em Notification rules (Regras de notificação), revise as regras configuradas para os recursos em sua conta da AWS na Região da AWS à qual você está conectado no momento. Use o seletor para alterar a Região da AWS.
4. Escolha a regra na lista e escolha Edit (Editar). Faça suas alterações e escolha Submit (Enviar).

Como editar uma regra de notificação (AWS CLI)

1. Em um terminal ou prompt de comando, execute o comando describe-notification-rule para visualizar a estrutura da regra de notificação.
2. Execute o comando update-notification rule para gerar o esqueleto JSON e salve-o em um arquivo.

```
aws codestar-notifications update-notification-rule --generate-cli-skeleton
 > update.json
```

É possível nomear o arquivo como você quiser. Neste exemplo, o arquivo é *update.json*.

3. Abra o arquivo JSON em um editor de texto simples e faça alterações na regra.

O exemplo a seguir mostra uma regra de notificação chamada **MyNotificationRule** para um repositório chamado *MyDemoRepo* em uma conta da AWS com o ID *123456789012*. As notificações são enviadas para um tópico do Amazon SNS chamado *MyNotificationTopic* quando ramificações e tags são criadas. O nome da regra será alterado para *MyNewNotificationRule*.

```
{
    "Name": "MyNewNotificationRule",
    "EventTypeIds": [
        "codecommit-repository-branches-and-tags-created"
    ],
    "Resource": "arn:aws:codecommit:us-east-1:123456789012:MyDemoRepo",
    "Targets": [
        {
            "TargetType": "SNS",
            "TargetAddress": "arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic"
        }
    ],
    "Status": "ENABLED",
    "DetailType": "FULL"
}
```

Salve o arquivo.

4. Usando o arquivo que você acabou de editar, no terminal ou na linha de comando, execute o comando update-notification-rule novamente para atualizar a regra de notificação.

```
aws codestar-notifications update-notification-rule --cli-input-json
 file://update.json
```

5. Se houver êxito, o comando retornará o nome de recurso da Amazon (ARN) da regra de notificação, semelhante ao seguinte:

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}
```

Como remover uma tag de uma regra de notificação (AWS CLI)

1. Em um terminal ou prompt de comando, execute o comando untag-resource. Por exemplo, o comando a seguir remove uma tag com o nome de *Team*.

```
aws codestar-notifications untag-resource --arn arn:aws:codestar-notifications:us-
east-1:123456789012:notificationrule/fe1efd35-EXAMPLE --tag-keys Team
```

2. Se houver êxito, o comando não retorna nada.

Consulte também

- Adicionar ou remover um destino para uma regra de notificação
- Habilitar ou desabilitar notificações para uma regra de notificação
- Eventos

Habilitar ou desabilitar notificações para uma regra de notificação

Quando você cria uma regra de notificação, as notificações são habilitadas por padrão. Não é necessário excluir a regra para impedir que ela envie notificações. Você pode simplesmente alterar seu status de notificação.

Como alterar o status de notificação de uma regra de notificação (console)

1. Abra o console do AWS Developer Tools em https://console.aws.amazon.com/codesuite/settings/notifications.

2. Na barra de navegação, expanda Settings (Configurações) e escolha Notification rules (Regras de notificação).
3. Em Notification rules (Regras de notificação), revise as regras configuradas para os recursos em sua conta da AWS na Região da AWS à qual você está conectado no momento. Use o seletor para alterar a Região da AWS.
4. Localize a regra de notificação que deseja ativar ou desativar e escolha-a para exibir os detalhes.
5. Em Notification status (Status de notificação), escolha o controle deslizante para alterar o status da regra:

   - Sending notifications (Enviando notificações): este é o padrão.
   - Notifications paused (Notificações pausadas): nenhuma notificação é enviada para os destinos especificados.

Como alterar o status de uma regra de notificação (AWS CLI)

1. Siga as etapas em Como editar uma regra de notificação (AWS CLI) para obter o JSON para a regra de notificação.
2. Edite o campo `Status` para `ENABLED` (padrão) ou `DISABLED` (sem notificações) e execute o comando update-notification-rule para alterar o status.

```
"Status": "ENABLED"
```

Excluir uma notificação

Só pode haver 10 regras de notificação configuradas para um recurso, portanto, considere excluir regras que não são mais necessárias. É possível usar o console do Developer Tools ou o AWS CLI para excluir regras de notificação.

> **Note**
>
> Não é possível desfazer a exclusão de uma regra de notificação, mas você pode recriá-la. A exclusão de uma regra de notificação não exclui o destino.

Como excluir uma regra de notificação (console)

1. Abra o console do AWS Developer Tools em https://console.aws.amazon.com/codesuite/settings/notifications.
2. Na barra de navegação, expanda Settings (Configurações) e escolha Notification rules (Regras de notificação).
3. Em Notification rules (Regras de notificação), revise as regras configuradas para os recursos em sua conta da AWS na Região da AWS à qual você está conectado no momento. Use o seletor para alterar a Região da AWS.
4. Escolha a regra de notificação e Delete (Excluir).
5. Digite **`delete`** e, em seguida, escolha Delete (Excluir).

Como excluir uma regra de notificação (AWS CLI)

1. Em um terminal ou prompt de comando, execute o comando delete-notification-rule, especificando o ARN da regra de notificação.

```
aws codestar-notifications delete-notification-rule --arn arn:aws:codestar-
notifications:us-east-1:123456789012:notificationrule/dc82df7a-EXAMPLE
```

2. Se houver êxito, o comando retornará o ARN da regra de notificação excluída, semelhante ao seguinte:

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}
```

Como trabalhar com destinos de regras de notificação

Um destino de regra de notificação é um destino que define para onde você deseja que as notificações sejam enviadas quando as condições do evento de uma regra de notificação são atendidas. É possível selecionar entre tópicos do Amazon SNS e clientes do AWS Chatbot que são configurados para canais do Slack ou do Microsoft Teams. Crie um tópico do Amazon SNS como um destino como parte da criação de uma regra de notificação (recomendado). Também é possível escolher um tópico do Amazon SNS existente na mesma região da AWS que a regra de notificação,

mas você deve configurá-lo com a política necessária. Se optar por usar um cliente do AWS Chatbot como destino, você deverá primeiro criar esse cliente no AWS Chatbot.

Se quiser estender o alcance das notificações, você poderá configurar a integração entre as notificações e o AWS Chatbot para que as notificações sejam enviadas para as salas de chat do Amazon Chime. Depois, você poderá selecionar o tópico do Amazon SNS configurado para esse cliente do AWS Chatbot como o destino da regra de notificação. Para obter mais informações, consulte Como integrar notificações com o AWS Chatbot e o Amazon Chime.

É possível usar o console do Developer Tools ou o AWS CLI para gerenciar destinos de notificação. É possível usar o console ou a AWS CLI para criar e configurar tópicos do Amazon SNS e clientes do AWS Chatbot como destinos. Também é possível configurar a integração entre os tópicos do Amazon SNS configurados como destinos e o AWS Chatbot. Isso permite que você envie notificações para salas de chat do Amazon Chime. Para obter mais informações, consulte Configurar a integração entre notificações e o AWS Chatbot.

Tópicos

- Criar ou configurar um destino de regra de notificação
- Visualizar destinos de regras de notificação
- Adicionar ou remover um destino para uma regra de notificação
- Excluir um destino de regra de notificação

Criar ou configurar um destino de regra de notificação

Os destinos de regra de notificação são tópicos do Amazon SNS ou clientes do AWS Chatbot configurados para canais do Slack ou do Microsoft Teams.

Um cliente do AWS Chatbot deverá ser criado para que você possa selecionar um cliente como destino. Ao selecionar um cliente do AWS Chatbot como destino para uma regra de notificação, um tópico do Amazon SNS é configurado para esse cliente do AWS Chatbot com todas as políticas necessárias para que as notificações sejam enviadas para o canal do Slack ou do Microsoft Teams. Não é necessário configurar nenhum tópico do Amazon SNS existente para o cliente do AWS Chatbot.

Você pode criar destinos de regra de notificação do Amazon SNS no console do Developer Tools ao criar uma regra de notificação. A política que permite que as notificações sejam enviadas para esse tópico é aplicada a você. Esta é a maneira mais fácil de criar um destino para uma regra de notificação. Para obter mais informações, consulte Criar uma regra de notificação.

Se você usar um tópico do Amazon SNS existente, deverá configurá-lo com uma política de acesso que permita que o recurso envie notificações para esse tópico. Para ver um exemplo, consulte Configurar tópicos do Amazon SNS para notificações.

> **Note**
>
> Se desejar usar um tópico do Amazon SNS existente em vez de criar um novo, em Targets (Destinos), escolha o ARN. Certifique-se de que o tópico tenha a política de acesso adequada e que a lista de assinantes contenha apenas os usuários que têm permissão para ver informações sobre o recurso. Se o tópico do Amazon SNS já tiver sido usado para notificações do CodeCommit antes de 5 de novembro de 2019, ele terá uma política que permite ao CodeCommit publicar nele e que contém permissões diferentes daquelas exigidas pelo AWS CodeStar Notifications. Não é recomendado usar esses tópicos. Se desejar usar um tópico criado para essa experiência, será necessário adicionar a política exigida para o AWS CodeStar Notifications, além daquela já existente. Para obter mais informações, consulte Configurar tópicos do Amazon SNS para notificações e Noções básicas do conteúdo e da segurança das notificações.

Se quiser estender o alcance das notificações, você poderá configurar a integração entre as notificações e o AWS Chatbot para que as notificações sejam enviadas para as salas de chat do Amazon Chime. Para obter mais informações, consulte Destinos e Como integrar notificações com o AWS Chatbot e o Amazon Chime.

Para configurar um tópico do Amazon SNS existente para usar como um destino de regra de notificação (console)

1. Faça login no AWS Management Console e abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na barra de navegação, escolha Tópicos. Escolha o tópico e Edit (Editar).
3. Expanda Access policy (Política de acesso) e, em seguida, escolha Advanced (Avançado).
4. No editor de JSON, adicione a declaração a seguir à política. Inclua o ARN do tópico, a Região da AWS, o ID da Conta da AWS e o nome do tópico.

```
{
     "Sid": "AWSCodeStarNotifications_publish",
     "Effect": "Allow",
     "Principal": {
```

```
        "Service": [
          "codestar-notifications.amazonaws.com"
        ]
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-
MyTopicForNotificationRules"
    }
```

A declaração da política deve ser semelhante ao seguinte.

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__default_statement_ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "SNS:GetTopicAttributes",
        "SNS:SetTopicAttributes",
        "SNS:AddPermission",
        "SNS:RemovePermission",
        "SNS:DeleteTopic",
        "SNS:Subscribe",
        "SNS:ListSubscriptionsByTopic",
        "SNS:Publish",
        "SNS:Receive"
      ],
      "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-
MyTopicForNotificationRules",
      "Condition": {
        "StringEquals": {
          "AWS:SourceOwner": "123456789012"
        }
      }
    },
 {
      "Sid": "AWSCodeStarNotifications_publish",
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": [
          "codestar-notifications.amazonaws.com"
        ]
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-
MyTopicForNotificationRules"
    }
  ]
}
```

5. Escolha Save changes (Salvar alterações).
6. Em Subscriptions (Assinaturas), revise a lista de assinantes do tópico. Adicione, edite ou exclua assinantes conforme apropriado para esse destino de regra de notificação. Verifique se a lista de assinantes contém apenas os usuários que têm permissão para ver informações sobre o recurso. Para obter mais informações, consulte Noções básicas do conteúdo e da segurança das notificações.

Como criar um cliente do AWS Chatbot com o Slack para usar como destino

1. Siga as instruções em Configurar o AWS Chatbot com o Slack no Guia do administrador do AWS Chatbot. Ao fazê-lo, considere as seguintes opções para uma integração ideal com notificações:
   - Ao criar uma função do IAM, considere escolher um nome de função que facilite a identificação da finalidade dessa função (por exemplo, **`AWSCodeStarNotifications-Chatbot-Slack-Role`**). Isso pode ajudar a identificar a finalidade da função no futuro.
   - Em SNS topics (Tópicos do SNS), não é necessário escolher um tópico ou uma região da AWS. Ao selecionar o cliente do AWS Chatbot como destino, um tópico do Amazon SNS com todas as permissões necessárias será criado e configurado para o cliente do AWS Chatbot como parte do processo de criação da regra de notificação.
2. Conclua o processo de criação do cliente. Esse cliente estará disponível para ser escolhido como destino durante a criação de regras de notificação. Para obter mais informações, consulte Criar uma regra de notificação.

> **Note**
>
> Não remova o tópico do Amazon SNS do cliente do AWS Chatbot depois de ele ter sido configurado para você. Isso impedirá que notificações sejam enviadas para o Slack.

Como criar um cliente do AWS Chatbot com o Microsoft Teams para usar como destino

1. Siga as instruções em Configurar o AWS Chatbot com o Microsoft Teams no Guia do administrador do AWS Chatbot. Ao fazê-lo, considere as seguintes opções para uma integração ideal com notificações:

   - Ao criar uma função do IAM, considere escolher um nome de função que facilite a identificação da finalidade dessa função (por exemplo, **`AWSCodeStarNotifications-Chatbot-Microsoft-Teams-Role`**). Isso pode ajudar a identificar a finalidade da função no futuro.
   - Em SNS topics (Tópicos do SNS), não é necessário escolher um tópico ou uma região da AWS. Ao selecionar o cliente do AWS Chatbot como destino, um tópico do Amazon SNS com todas as permissões necessárias será criado e configurado para o cliente do AWS Chatbot como parte do processo de criação da regra de notificação.

2. Conclua o processo de criação do cliente. Esse cliente estará disponível para ser escolhido como destino durante a criação de regras de notificação. Para obter mais informações, consulte Criar uma regra de notificação.

> **Note**
>
> Não remova o tópico do Amazon SNS do cliente do AWS Chatbot depois de ele ter sido configurado para você. Isso impedirá que notificações sejam enviadas para o Microsoft Teams.

Visualizar destinos de regras de notificação

Você pode usar o console do Developer Tools, mas não o console do Amazon SNS, para exibir todos os destinos da regra de notificação para todos os recursos em uma região da AWS. Pode também visualizar os detalhes de um destino de regra de notificação.

Para visualizar destinos de regras de notificação (console)

1. Abra o console do AWS Developer Tools em https://console.aws.amazon.com/codesuite/settings/notifications.
2. Na barra de navegação, expanda Settings (Configurações) e escolha Notification rules (Regras de notificação).
3. Em Notification rule targets (Destinos de regras de notificação), revise a lista de destinos usados pelas regras de notificação em sua Conta da AWS na Região da AWS à qual você está conectado no momento. Use o seletor para alterar a Região da AWS. Se o status do destino for exibido como Unreachable (Inacessível), talvez seja necessário investigar. Para obter mais informações, consulte Solução de problemas .

Para visualizar uma lista de destinos de regras de notificação (AWS CLI)

1. Em um terminal ou prompt de comando, execute o comando list-targets para visualizar uma lista de todos os destinos de regras de notificação para a região da AWS especificada:

```
aws codestar-notifications list-targets --region us-east-2
```

2. Se for bem-sucedido, esse comando retornará o ID e o ARN de cada regra de notificação na região da AWS, semelhante ao seguinte:

```
{
    "Targets": [
        {
            "TargetAddress": "arn:aws:sns:us-
east-2:123456789012:MySNSTopicForNotificationRules",
            "TargetType": "SNS",
            "TargetStatus": "ACTIVE"
        },
        {
            "TargetAddress": "arn:aws:chatbot::123456789012:chat-configuration/
slack-channel/MySlackChannelClientForMyDevTeam",
            "TargetStatus": "ACTIVE",
            "TargetType": "AWSChatbotSlack"
        },
        {
            "TargetAddress": "arn:aws:sns:us-
east-2:123456789012:MySNSTopicForNotificationsAboutMyDemoRepo",
            "TargetType": "SNS",
```

```
            "TargetStatus": "ACTIVE"
        }
    ]
}
```

Adicionar ou remover um destino para uma regra de notificação

Você pode editar uma regra de notificação para alterar o destino ou os destinos para os quais ela envia notificações. É possível usar o console do Developer Tools ou a AWS CLI para alterar os destinos de uma regra de notificação.

Para alterar os destinos de uma regra de notificação (console)

1. Abra o console do AWS Developer Tools em https://console.aws.amazon.com/codesuite/settings/notifications.
2. Na barra de navegação, expanda Settings (Configurações) e escolha Notification rules (Regras de notificação).
3. Em Notification rules (Regras de notificação), revise a lista de regras configuradas para os recursos em sua conta da AWS na Região da AWS à qual você está conectado no momento. Use o seletor para alterar a Região da AWS.
4. Escolha a regra e Edit (Editar).
5. Em Targets (Destinos), siga um destes procedimentos:
   - Para adicionar outro destino, selecione Adicionar destino e selecione na lista o tópico do Amazon SNS ou o cliente do AWS Chatbot (Slack) ou AWS Chatbot (Microsoft Teams) que deseja adicionar. Você também pode escolher Create SNS topic (Criar tópico do SNS) para criar um tópico e adicioná-lo como destino. Uma regra de notificação pode ter até 10 destinos.
   - Para remover um destino, escolha Remove target (Remover destino) ao lado do destino que deseja remover.
6. Selecione Submit (Enviar).

Para adicionar um destino a uma regra de notificação (AWS CLI)

1. Em um terminal ou prompt de comando, execute o comando subscribe para adicionar um destino. Por exemplo, o comando a seguir adiciona um tópico do Amazon SNS como um destino para uma regra de notificação.

```
aws codestar-notifications subscribe --arn arn:aws:codestar-
notifications:us-east-1:123456789012:notificationrule/dc82df7a-
EXAMPLE --target TargetType=SNS,TargetAddress=arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic
```

2. Se houver êxito, o comando retornará o ARN da regra de notificação atualizada, semelhante ao seguinte:

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}
```

Para remover um destino de uma regra de notificação (AWS CLI)

1. Em um terminal ou prompt de comando, execute o comando unsubscribe para remover um destino. Por exemplo, o comando a seguir remove um tópico do Amazon SNS como um destino de uma regra de notificação.

```
aws codestar-notifications unsubscribe --arn arn:aws:codestar-
notifications:us-east-1:123456789012:notificationrule/dc82df7a-
EXAMPLE --target TargetType=SNS,TargetAddress=arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic
```

2. Se houver êxito, o comando retornará o ARN da regra de notificação atualizada e informações sobre o destino removido, semelhante ao seguinte:

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
    "TargetAddress": "arn:aws:sns:us-east-1:123456789012:MyNotificationTopic"
}
```

Consulte também

- Editar uma regra de notificação
- Habilitar ou desabilitar notificações para uma regra de notificação

Excluir um destino de regra de notificação

É possível excluir um destino se ele não for mais necessário. Um recurso pode ter somente 10 destinos de regras de notificação configurados para ele, portanto, a exclusão de destinos desnecessários pode ajudar a criar espaço para outros destinos que você queira adicionar a essa regra de notificação.

> **Note**
>
> A exclusão de um destino de regra de notificação remove o destino de todas as regras de notificação configuradas para usá-lo como destino, mas não exclui o destino em si.

Para excluir um destino de regra de notificação (console)

1. Abra o console do AWS Developer Tools em https://console.aws.amazon.com/codesuite/settings/notifications.
2. Na barra de navegação, expanda Settings (Configurações) e escolha Notification rules (Regras de notificação).
3. Em Notification rule targets (Destinos de regras de notificação), revise a lista de destinos configurados para os recursos na sua conta da AWS na Região da AWS à qual você está conectado no momento. Use o seletor para alterar a Região da AWS.
4. Escolha o destino da regra de notificação e Delete (Excluir).
5. Digite **`delete`** e, em seguida, escolha Delete (Excluir).

Para excluir um destino de regra de notificação (AWS CLI)

1. Em um terminal ou prompt de comando, execute o comando delete-target, especificando o ARN do destino. Por exemplo, o comando a seguir exclui um destino que usa um tópico do Amazon SNS.

```
aws codestar-notifications delete-target --target-address arn:aws:sns:us-east-1:123456789012:MyNotificationTopic
```

2. Se for bem-sucedido, o comando não retornará nada. Se não for bem-sucedido, o comando retornará um erro. O erro mais comum informa que o tópico é o destino de uma ou mais regras de notificação.

```
An error occurred (ValidationException) when calling the DeleteTarget operation:
 Unsubscribe target before deleting.
```

É possível usar o parâmetro `--force-unsubscribe-all` para remover o destino de todas as regras de notificação configuradas para usá-lo como destino e, depois, excluir o destino.

```
aws codestar-notifications delete-target --target-address arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic --force-unsubscribe-all
```

Configurar a integração entre notificações e o AWS Chatbot

O AWS Chatbot é um serviço da AWS que permite que equipes de desenvolvimento de software e DevOps usem salas de bate-papo do Amazon Chime, canais do Slack e canais do Microsoft Teams para monitorar e responder a eventos operacionais na Nuvem AWS. É possível configurar a integração entre destinos de regras de notificação e o AWS Chatbot para que as notificações sobre eventos apareçam na sala do Amazon Chime, no canal do Slack ou no canal do Microsoft Teams que você escolher. Para ter mais informações, consulte a Documentação do AWS Chatbot.

Antes de configurar a integração com o AWS Chatbot, é necessário configurar uma regra de notificação e um destino de regra. Para obter mais informações, consulte Configuração e Criar uma regra de notificação. Também é necessário configurar um canal do Slack, um canal do Microsoft Teams ou uma sala de bate-papo do Amazon Chime no AWS Chatbot. Para obter mais informações, consulte a documentação desses serviços.

Tópicos

- Configurar um cliente do AWS Chatbot para um canal do Slack
- Configurar um cliente do AWS Chatbot para um canal do Microsoft Teams
- Configurar clientes para o Slack ou o Amazon Chime manualmente

Configurar um cliente do AWS Chatbot para um canal do Slack

É possível criar regras de notificação que usam um cliente do AWS Chatbot como destino. Se criar um cliente para um canal Slack, você poderá usar esse cliente diretamente como destino no fluxo de trabalho para criar uma regra de notificação. Esta é a maneira mais fácil de configurar as notificações que são exibidas nos canais Slack.

Como criar um cliente do AWS Chatbot com o Slack para usar como destino

1. Siga as instruções em Configurar o AWS Chatbot com o Slack no Guia do administrador do AWS Chatbot. Ao fazê-lo, considere as seguintes opções para uma integração ideal com notificações:

   - Ao criar uma função do IAM, considere escolher um nome de função que facilite a identificação da finalidade dessa função (por exemplo, **`AWSCodeStarNotifications-Chatbot-Slack-Role`**). Isso pode ajudar a identificar a finalidade da função no futuro.
   - Em SNS topics (Tópicos do SNS), não é necessário escolher um tópico ou uma região da AWS. Ao selecionar o cliente do AWS Chatbot como destino, um tópico do Amazon SNS com todas as permissões necessárias será criado e configurado para o cliente do AWS Chatbot como parte do processo de criação da regra de notificação.

2. Conclua o processo de criação do cliente. Esse cliente estará disponível para ser escolhido como destino durante a criação de regras de notificação. Para obter mais informações, consulte Criar uma regra de notificação.

   > **Note**
   >
   > Não remova o tópico do Amazon SNS do cliente do AWS Chatbot depois de ele ter sido configurado para você. Isso impedirá que notificações sejam enviadas para o Slack.

Configurar um cliente do AWS Chatbot para um canal do Microsoft Teams

É possível criar regras de notificação que usam um cliente do AWS Chatbot como destino. Se criar um cliente para um canal do Microsoft Teams, você poderá usar esse cliente diretamente como destino no fluxo de trabalho para criar uma regra de notificação. Essa é a maneira mais fácil de configurar as notificações que são exibidas nos canais do Microsoft Teams.

Como criar um cliente do AWS Chatbot com o Microsoft Teams para usar como destino

1. Siga as instruções em Configurar o AWS Chatbot com o Microsoft Teams no Guia do administrador do AWS Chatbot. Ao fazê-lo, considere as seguintes opções para uma integração ideal com notificações:

   - Ao criar uma função do IAM, considere escolher um nome de função que facilite a identificação da finalidade dessa função (por exemplo, **`AWSCodeStarNotifications-`**

`Chatbot-Microsoft-Teams-Role`). Isso pode ajudar a identificar a finalidade da função no futuro.

- Em SNS topics (Tópicos do SNS), não é necessário escolher um tópico ou uma região da AWS. Ao selecionar o cliente do AWS Chatbot como destino, um tópico do Amazon SNS com todas as permissões necessárias será criado e configurado para o cliente do AWS Chatbot como parte do processo de criação da regra de notificação.

2. Conclua o processo de criação do cliente. Esse cliente estará disponível para ser escolhido como destino durante a criação de regras de notificação. Para obter mais informações, consulte Criar uma regra de notificação.

> **Note**
>
> Não remova o tópico do Amazon SNS do cliente do AWS Chatbot depois de ele ter sido configurado para você. Isso impedirá que notificações sejam enviadas para o Microsoft Teams.

Configurar clientes para o Slack ou o Amazon Chime manualmente

É possível optar por criar a integração entre as notificações e o Slack ou o Amazon Chime diretamente. Este é o único método disponível para configurar notificações para salas de chat do Amazon Chime. Ao configurar essa integração manualmente, você cria um cliente do AWS Chatbot que usa um tópico do Amazon SNS configurado anteriormente como o destino de uma regra de notificação.

Como integrar notificações manualmente com o AWS Chatbot e o Slack

1. Abra o console do AWS Developer Tools em https://console.aws.amazon.com/codesuite/settings/notifications.
2. Selecione Settings (Configurações) e Notification rules (Regras de notificação).
3. Em Notification rule targets (Destinos de regra de notificação), localize e copie o destino.

> **Note**
>
> Você pode configurar mais de uma regra de notificação para usar o mesmo tópico do Amazon SNS como seu destino. Isso pode ajudá-lo a consolidar o sistema de

mensagens, mas também pode ter consequências não intencionais se a lista de assinaturas for específica para uma regra de notificação ou um recurso.

4. Abra o console do AWS Chatbot em https://console.aws.amazon.com/chatbot/.
5. Escolha Configure new client (Configurar novo cliente) e selecione Slack.
6. Selecione Configurar.
7. Faça login no seu espaço de workspace do Slack.
8. Quando for solicitado que você confirme as opções, selecione Allow (Permitir).
9. Escolha Configure new channel (Configurar novo canal).
10. Em Configuration details (Detalhes da configuração), em Configuration name (Nome da configuração), insira um nome para o cliente. Esse é o nome que será exibido na lista de destinos disponíveis para o tipo de destino AWS Chatbot (Slack) quando você criar regras de notificação.
11. Em Configure Slack Channel (Configurar canal do Slack), em Channel type (Tipo de canal), selecione Public (Público) ou Private (Privado), dependendo do tipo de canal ao qual você deseja fazer a integração.
    - Em Public channel (Canal público), escolha o nome do canal do Slack na lista.
    - Em Private channel ID (ID do canal privado), insira o código do canal ou URL.
12. Em IAM permissions (Permissões do IAM), em Role (Função), escolha Create an IAM role using a template (Criar uma função do IAM usando um modelo). Em Policy templates (Modelos de política), escolha Notification permissions (Permissões de notificação). Em Role name (Nome da função), insira um nome para essa função (por exemplo, **`AWSCodeStarNotifications-Chatbot-Slack-Role`**). Em Policy templates (Modelos de política), escolha Notification permissions (Permissões de notificação).
13. Em SNS topics (Tópicos do SNS), em SNS Region (Região do SNS), selecione a Região da AWS na qual criou o destino da regra de notificação. Em SNS topics (Tópicos do SNS), escolha o nome do tópico do Amazon SNS que você configurou como o destino da regra de notificação.

    > **Note**
    >
    > Esta etapa não é necessária se você criar uma regra de notificação usando este cliente como destino.

14. Selecione Configurar.

> **Note**
>
> Se você configurou a integração com um canal privado, é necessário convidar o AWS Chatbot para o canal para poder ver as notificações nesse canal. Para ter mais informações, consulte a Documentação do AWS Chatbot.

15. (Opcional) Para testar a integração, faça uma alteração no recurso que corresponde a um tipo de evento de uma regra de notificação que foi configurada para usar o tópico do Amazon SNS como destino. Por exemplo, caso tenha uma regra de notificação configurada para enviar notificações quando comentários forem inseridos em uma solicitação pull, comente em uma solicitação pull e observe o canal do Slack para ver quando a notificação aparece.

Como integrar notificações com o AWS Chatbot e o Amazon Chime

1. Abra o console do AWS Developer Tools em https://console.aws.amazon.com/codesuite/settings/notifications.
2. Selecione Settings (Configurações) e Notification rules (Regras de notificação).
3. Em Notification rule targets (Destinos de regra de notificação), localize e copie o destino.

> **Note**
>
> Você pode configurar mais de uma regra de notificação para usar o mesmo tópico do Amazon SNS como seu destino. Isso pode ajudá-lo a consolidar o sistema de mensagens, mas também pode ter consequências não intencionais se a lista de assinaturas for específica para uma regra de notificação ou um recurso.

4. No Amazon Chime, abra a sala de chat que deseja configurar para a integração.
5. Escolha o ícone de engrenagem no canto superior direito e escolha Manage webhooks (Gerenciar webhooks).
6. Na caixa de diálogo Manage webhooks (Gerenciar webhooks), escolha New (Novo), insira um nome para o webhook e selecione Create (Criar).
7. Verifique se o webhook é exibido e escolha Copy webhook URL (Copiar URL do webhook).
8. Abra o console do AWS Chatbot em https://console.aws.amazon.com/chatbot/.
9. Escolha Configure new client (Configurar novo cliente) e escolha Amazon Chime.

10. Em Configuration details (Detalhes da configuração), em Configuration name (Nome da configuração), insira um nome para o cliente.
11. Em Webhook URL (URL do webhook), cole o URL. Em Webhook description (Descrição do webhook), forneça uma descrição opcional.
12. Em IAM permissions (Permissões do IAM), em Role (Função), escolha Create an IAM role using a template (Criar uma função do IAM usando um modelo). Em Policy templates (Modelos de política), escolha Notification permissions (Permissões de notificação). Em Role name (Nome da função), insira um nome para essa função (por exemplo, **`AWSCodeStarNotifications-Chatbot-Chime-Role`**).
13. Em SNS topics (Tópicos do SNS), em SNS Region (Região do SNS), selecione a Região da AWS na qual criou o destino da regra de notificação. Em SNS topics (Tópicos do SNS), escolha o nome do tópico do Amazon SNS que você configurou como o destino da regra de notificação.
14. Selecione Configurar.
15. (Opcional) Para testar a integração, faça uma alteração no recurso que corresponde a um tipo de evento de uma regra de notificação que foi configurada para usar o tópico do Amazon SNS como destino. Por exemplo, caso tenha uma regra de notificação configurada para enviar notificações quando comentários forem inseridos em uma solicitação pull, comente em uma solicitação pull e observe a sala de chat do Amazon Chime para ver quando a notificação aparece.

Registro em log de chamadas à API do AWS CodeStar Notifications com o AWS CloudTrail

O AWS CodeStar Connections é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço da AWS. O CloudTrail captura todas as chamadas de API para notificações na forma de eventos. As chamadas capturadas incluem as chamadas do console do Developer Tools e as chamadas de código para as operações de API do AWS CodeStar Notifications. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para notificações. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Com as informações coletadas pelo CloudTrail, você pode determinar a solicitação que foi feita para o AWS CodeStar Notifications, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e outros detalhes.

Para obter mais informações, consulte o Guia do usuário do AWS CloudTrail.

Informações do AWS CodeStar Notifications no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando uma atividade ocorre no AWS CodeStar Notifications, essa atividade é registrada em um evento do CloudTrail com outros eventos de serviços da AWS no Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos em sua Conta da AWS, incluindo eventos para o AWS CodeStar Notifications, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a 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 em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

Todas as ações do AWS CodeStar Notifications são registradas pelo CloudTrail e documentadas na *Referência da API do AWS CodeStar Notifications*. Por exemplo, as chamadas para as ações `CreateNotificationRule`, `Subscribe` e `ListEventTypes` geram entradas nos arquivos de log do CloudTrail.

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

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM).
- 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 serviço da AWS.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas sobre entradas de arquivos de log do

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail 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 de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do `CreateNotificationRule` CloudTrail que demonstra a criação de uma regra de notificação, incluindo as ações e `Subscribe`.

> **Note**
>
> Alguns dos eventos nas entradas do arquivo de log da notificação podem ser provenientes da função vinculada ao serviço AWSServiceRoleForCodeStarNotifications.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/Mary_Major",
        "accountId":"123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName":"Mary_Major"
    },
    "eventTime": "2019-10-07T21:34:41Z",
    "eventSource": "events.amazonaws.com",
    "eventName": "CreateNotificationRule",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "codestar-notifications.amazonaws.com",
    "userAgent": "codestar-notifications.amazonaws.com",
    "requestParameters": {
        "description": "This rule is used to route CodeBuild, CodeCommit, CodePipeline,
 and other Developer Tools notifications to AWS CodeStar Notifications",
        "name": "awscodestarnotifications-rule",
        "eventPattern": "{\"source\":[\"aws.codebuild\",\"aws.codecommit\",
\"aws.codepipeline\"]}"
    },
```

```
    "responseElements": {
        "ruleArn": "arn:aws:events:us-east-1:123456789012:rule/
awscodestarnotifications-rule"
    },
    "requestID": "ff1f309a-EXAMPLE",
    "eventID": "93c82b07-EXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-10-07",
    "recipientAccountId": "123456789012"
}
```

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/Mary_Major",
        "accountId":"123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName":"Mary_Major"
    },
    "eventTime": "2019-10-07T21:34:41Z",
    "eventSource": "events.amazonaws.com",
    "eventName": "Subscribe",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "codestar-notifications.amazonaws.com",
    "userAgent": "codestar-notifications.amazonaws.com",
    "requestParameters": {
        "targets": [
            {
                "arn": "arn:aws:codestar-notifications:us-east-1:::",
                "id": "codestar-notifications-events-target"
            }
        ],
        "rule": "awscodestarnotifications-rule"
    },
    "responseElements": {
        "failedEntryCount": 0,
        "failedEntries": []
    },
    "requestID": "9466cbda-EXAMPLE",
    "eventID": "2f79fdad-EXAMPLE",
    "eventType": "AwsApiCall",
```

```
    "apiVersion": "2015-10-07",
    "recipientAccountId": "123456789012"
}
```

Solução de problemas

As informações a seguir podem ajudá-lo a solucionar problemas comuns com notificações.

Tópicos

- Recebo um erro de permissões quando tento criar uma regra de notificação em um recurso
- Não consigo visualizar regras de notificação
- Não consigo criar regras de notificação
- Estou recebendo notificações de um recurso que não posso acessar
- Não estou recebendo notificações do Amazon SNS
- Estou recebendo notificações duplicadas sobre eventos
- Eu gostaria de entender por que o status de um destino de notificação é exibido como inacessível
- Quero aumentar minhas cotas para notificações e recursos

Recebo um erro de permissões quando tento criar uma regra de notificação em um recurso

Verifique se você tem permissões suficientes. Para obter mais informações, consulte Exemplos de políticas baseadas em identidade.

Não consigo visualizar regras de notificação

Problema: quando você está no console do Developer Tools e escolhe Notifications(Notificações) em Settings (Configurações), um erro de permissões é exibido.

Correções possíveis: talvez você não tenha as permissões necessárias para visualizar notificações. Embora a maioria das políticas gerenciadas para os serviços do AWS Developer Tools, como CodeCommit e CodePipeline, inclua permissões para notificações, os serviços que não são compatíveis com notificações no momento não incluem permissões para exibi-las. Outra possibilidade é que você talvez tenha uma política personalizada aplicada ao seu usuário ou função do IAM que não permite exibir notificações. Para obter mais informações, consulte Exemplos de políticas baseadas em identidade.

Não consigo criar regras de notificação

Talvez você não tenha as permissões necessárias para criar uma regra de notificação. Para obter mais informações, consulte Exemplos de políticas baseadas em identidade.

Estou recebendo notificações de um recurso que não posso acessar

Depois que criar uma regra de notificação e adicionar um destino, o recurso de notificações não validará se o destinatário tem acesso ao recurso. É possível que você receba notificações sobre um recurso que não pode acessar. Se você não conseguir se remover, solicite que seja removido da lista de assinaturas do destino.

Não estou recebendo notificações do Amazon SNS

Para solucionar problemas com o tópico do Amazon SNS, verifique o seguinte:

- Verifique se o tópico do Amazon SNS foi criado na mesma região da AWS que a regra de notificação.
- Verifique se o seu alias de e-mail está inscrito no tópico correto e se você confirmou a assinatura. Para obter mais informações, consulte Como inscrever um endpoint em um tópico do Amazon SNS.
- Verifique se a política do tópico foi editada para permitir que o AWS CodeStar Notifications envie notificações por push para esse tópico. A política do tópico deve incluir uma declaração semelhante à seguinte:

```
{
    "Sid": "AWSCodeStarNotifications_publish",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "codestar-notifications.amazonaws.com"
        ]
    },
    "Action": "SNS:Publish",
    "Resource": "arn:aws:sns:us-east-1:123456789012:MyNotificationTopicName",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012"
        }
    }
```

```
}
```

Para obter mais informações, consulte Configurar tópicos do Amazon SNS para notificações.

Estou recebendo notificações duplicadas sobre eventos

Estes são os motivos mais comuns para receber várias notificações:

- Várias regras de notificação que incluem o mesmo tipo de evento foram configuradas para um recurso e você está inscrito nos tópicos do Amazon SNS que são os destinos dessas regras. Para resolver esse problema, cancele a assinatura de um dos tópicos ou edite as regras de notificação para remover a duplicação.
- Um ou mais destinos da regra de notificação estão integrados ao AWS Chatbot e você está recebendo notificações na caixa de entrada de e-mail e em um canal do Slack, em um canal do Microsoft Teams ou em uma sala de chat do Amazon Chime. Para resolver esse problema, considere a possibilidade de cancelar assinatura de seu endereço de e-mail do tópico do Amazon SNS que é o destino da regra e usar o canal do Slack, o canal do Microsoft Teams ou a sala de bate-papo do Amazon Chime para visualizar notificações.

Eu gostaria de entender por que o status de um destino de notificação é exibido como inacessível

Os destinos têm dois status possíveis: Active (Ativo) e Unreachable (Inacessível). Unreachable (Inacessível) indica que as notificações foram enviadas para um destino e que a entrega não foi bem-sucedida. As notificações continuam a ser enviadas para esse destino e, se houver êxito, o status será redefinido como Active (Ativo).

O destino de uma regra de notificação pode ficar indisponível por um dos seguintes motivos:

- O recurso (tópico do Amazon SNS ou cliente do AWS Chatbot) foi excluído. Escolha outro destino para a regra de notificação.
- O tópico do Amazon SNS é criptografado e a política necessária para tópicos criptografados está ausente ou a chave do AWS KMS foi excluída. Para obter mais informações, consulte Configurar tópicos do Amazon SNS para notificações.
- O tópico do Amazon SNS não tem a política necessária para notificações. As notificações não podem ser enviadas para um tópico do Amazon SNS a menos que ele tenha a política. Para obter mais informações, consulte Configurar tópicos do Amazon SNS para notificações.

- O serviço de suporte do destino (Amazon SNS ou AWS Chatbot) pode estar com problemas.

Quero aumentar minhas cotas para notificações e recursos

No momento, não é possível alterar nenhuma cota. Consulte Cotas para notificações.

Cotas para notificações

A tabela a seguir lista as cotas (também chamadas de limites) para notificações no console do Developer Tools. Para ter informações sobre os limites que podem ser alterados, consulte AWS service quotas (Cotas de serviço da AWS).

Recurso	Limite padrão
Número máximo de regras de notificação em uma conta da AWS	1000
Número máximo de destinos para uma regra de notificação	10
Número máximo de regras de notificação para um recurso	10

O que são conexões?

Você pode usar o recurso de conexões no console do Developer Tools para conectar AWS recursos, como AWS CodePipeline repositórios de código externos. Esse recurso tem sua própria API, a referência da API AWS CodeStar Connections. Cada conexão é um recurso que você pode fornecer aos AWS serviços para se conectarem a um repositório de terceiros, como BitBucket. Por exemplo, você pode adicionar a conexão para CodePipeline que ela acione seu pipeline quando uma alteração de código for feita em seu repositório de código de terceiros. Cada conexão é nomeada e associada a um nome do recurso da Amazon (ARN) exclusivo que é usado para fazer referência à conexão.

O que posso fazer com as conexões?

Você pode usar conexões para integrar recursos de provedores de terceiros com seus recursos da AWS em ferramentas de desenvolvedor, como:

- Conecte-se a um provedor terceirizado, como o Bitbucket, e use a conexão de terceiros como uma integração de origem com seus AWS recursos, como CodePipeline.
- Gerencie uniformemente o acesso à sua conexão em todos os seus recursos ao CodeBuild criar projetos, CodeDeploy aplicativos e pipelines CodePipeline para seu provedor terceirizado.
- Use um ARN de conexão em seus modelos de pilha para CodeBuild criar projetos, CodeDeploy aplicativos e pipelines CodePipeline, sem a necessidade de referenciar segredos ou parâmetros armazenados.

Para quais provedores de terceiros posso criar conexões?

As conexões podem associar seus AWS recursos aos seguintes repositórios de terceiros:

- Bitbucket Cloud
- GitHub
- GitHub Nuvem corporativa
- GitHub Servidor corporativo
- GitLab
- GitLab instalação autogerenciada (para Enterprise Edition ou Community Edition)

Para obter uma visão geral do fluxo de trabalho de conexões, consulte Fluxo de trabalho para criar ou atualizar conexões.

As etapas para criar conexões para um tipo de provedor de nuvem GitHub, como, são diferentes das etapas para um tipo de provedor instalado, como GitHub Enterprise Server. Para obter as etapas de alto nível para criar uma conexão por tipo de provedor, consulte Trabalhar com conexões.

> **Note**
>
> Para usar conexões na Europa (Milão) Região da AWS, você deve:
>
> 1. Instalar uma aplicação específica da região.
> 2. Habilitar a região.
>
> Essa aplicação específica da região é compatível com conexões na região Europa (Milão). Ela é publicada no site do provedor externo e é separada da aplicação existente que permite

conexões para outras regiões. Ao instalar essa aplicação, você autoriza provedores externos a compartilhar seus dados somente com o serviço dessa região, mas pode revogar as permissões a qualquer momento ao desinstalá-la.
O serviço não processará nem armazenará seus dados, a menos que você habilite a região. Ao habilitar essa região, você concede ao nosso serviço permissões para processar e armazenar seus dados.
Mesmo que a região não esteja habilitada, provedores externos ainda poderão compartilhar seus dados com nosso serviço se a aplicação específica da região permanecer instalada. Portanto, desinstale a aplicação depois de desabilitar a região. Para obter mais informações, consulte Habilitar uma região.

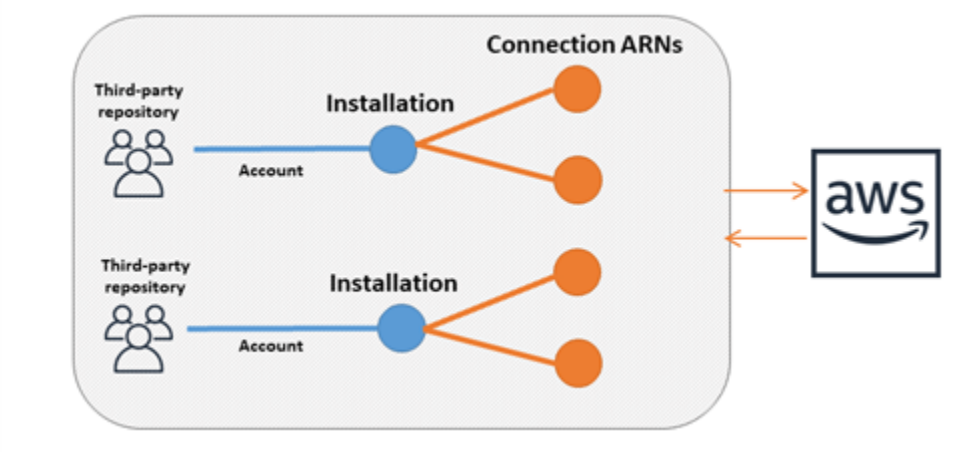
O que Serviços da AWS se integra às conexões?

Você pode usar conexões para integrar seu repositório de terceiros a outros Serviços da AWS. Para visualizar as integrações de serviços para conexões, consulte Integrações de produtos e serviços com o AWS CodeStar Connections.

Como funcionam as conexões?

Antes de criar uma conexão, você deve primeiro instalar ou fornecer acesso à aplicação de autenticação da AWS em sua conta de terceiros. Depois que uma conexão é instalada, ela pode ser atualizada para usar essa instalação. Ao criar uma conexão, você deve fornecer acesso ao recurso da AWS em sua conta de terceiros. Isso permite que a conexão acesse conteúdo, como repositórios de origem, na conta de terceiros, em nome de seus AWS recursos. Em seguida, você pode compartilhar essa conexão com outras pessoas Serviços da AWS para fornecer conexões OAuth seguras entre os recursos.

Se você quiser criar uma conexão com um tipo de provedor instalado, como o GitHub Enterprise Server, primeiro crie um recurso de host usando AWS Management Console o.



As conexões são de propriedade de Conta da AWS quem as cria. As conexões são identificadas por um ARN que contém um ID de conexão. O ID da conexão é um UUID que não pode ser alterado nem remapeado. Excluir e restabelecer uma conexão resulta em um novo ID de conexão e, portanto, em um novo ARN de conexão. Isso significa que os ARNs de conexão nunca são reutilizados.

Uma conexão recém-criada está em um estado `Pending`. Um processo de handshake de terceiros (fluxo OAuth) é necessário para concluir a configuração da conexão e para que ela se mova de `Pending` para um estado `Available`. Depois que isso for concluído, uma conexão é `Available` e pode ser usada com AWS serviços, como CodePipeline.

Um host recém-criado está em um estado `Pending`. Um processo de registro de terceiros (fluxo OAuth) é necessário para concluir a configuração do host e para que ela se mova de `Pending` para um estado `Available`. Depois que isso for concluído, um host será `Available` e poderá ser usado para conexões com tipos de provedores instalados.

Para obter uma visão geral do fluxo de trabalho de conexões, consulte Fluxo de trabalho para criar ou atualizar conexões. Consulte uma visão geral do fluxo de trabalho de criação de host para provedores instalados em Fluxo de trabalho para criar ou atualizar um host. Para obter as etapas de alto nível para criar uma conexão por tipo de provedor, consulte Trabalhar com conexões.

Recursos globais em AWS CodeStar conexões

Conexões são recursos globais, o que significa que o recurso é replicado em todas as Regiões da AWS.

Embora o formato do ARN da conexão reflita o nome da região onde ele foi criado, o recurso não está restrito a nenhuma região. A região onde o recurso de conexão foi criado é a região onde as atualizações de dados de recursos de conexão são controladas. Exemplos de operações de API que

controlam atualizações para dados de recursos de conexão incluem criar uma conexão, atualizar uma instalação, excluir uma conexão ou marcar uma conexão.

Recursos de host para conexões não são recursos disponíveis globalmente. Use recursos de host somente na região em que eles foram criados.

- Você só precisa criar uma conexão uma vez; depois, você pode usá-la em qualquer Região da AWS.
- Se a região onde a conexão foi criada estiver tendo problemas, isso afetará APIs que controlam dados de recursos de conexão, mas você ainda poderá usar a conexão com êxito em todas as outras regiões.
- Quando você lista recursos de conexão no console ou CLI, a lista mostra todos os recursos de conexão associados à sua conta em todas as regiões.
- Quando você lista os recursos do host no console ou na CLI, a lista mostra os recursos do host associados à sua conta somente na região selecionada.
- Quando uma conexão com um recurso de host associado é listada ou exibida com a CLI, a saída retorna o ARN do host independentemente da região da CLI configurada.

Fluxo de trabalho para criar ou atualizar um host

Ao criar uma conexão com um provedor instalado, primeiro crie um host.

Os hosts podem ter os seguintes estados:

- `Pending`: um host `pending` foi criado e deve ser configurado (movido para `available`) antes de poder ser usado.
- `Available`: você pode usar ou passar um host `available` para sua conexão.

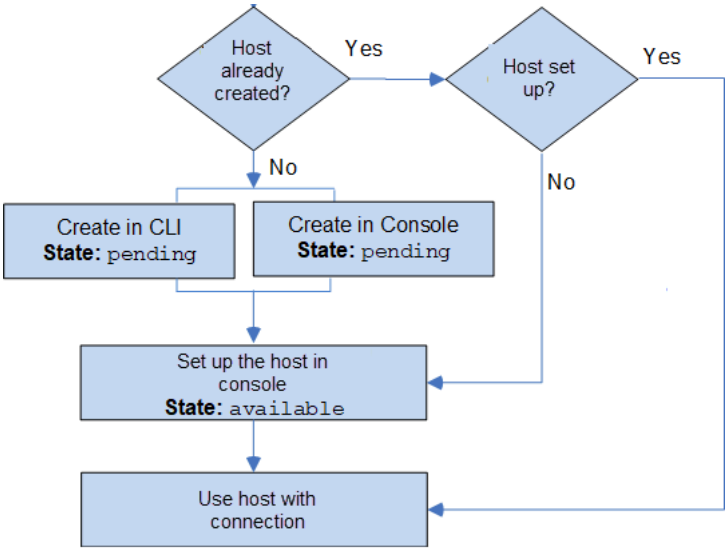
Fluxo de trabalho: criar ou atualizar um host com a CLI, o SDK ou o AWS CloudFormation

Você usa a CreateHostAPI para criar um host usando o AWS Command Line Interface (AWS CLI), SDK ou AWS CloudFormation. Após ser criado, o host fica em um estado `pending`. Conclua o processo usando a opção Configurar no console.

Fluxo de trabalho: criar ou atualizar um host com o console

Se você estiver criando uma conexão com um tipo de provedor instalado, como GitHub Enterprise Server ou GitLab autogerenciado, primeiro crie um host. Se você estiver se conectando a um tipo de provedor de nuvem, como Bitbucket, ignore a criação do host e continue criando uma conexão.

Use o console para configurar o host e alterar seu status de `pending` para `available`.



Fluxo de trabalho para criar ou atualizar conexões

Ao criar uma conexão, você também cria ou usa uma instalação existente para o handshake de autenticação com o provedor de terceiros.

As conexões podem ter um dos seguintes status:

- `Pending`: uma conexão `pending` é uma conexão que deve ser concluída (movida para `available`) antes que possa ser usada.
- `Available`: você pode usar ou passar uma conexão `available` para outros recursos e usuários na sua conta.
- `Error`: uma conexão que tem um estado `error` é repetida automaticamente. Ela não poderá ser usada até se tornar `available`.

Fluxo de trabalho: Criando ou atualizando uma conexão com a CLI, SDK ou AWS CloudFormation

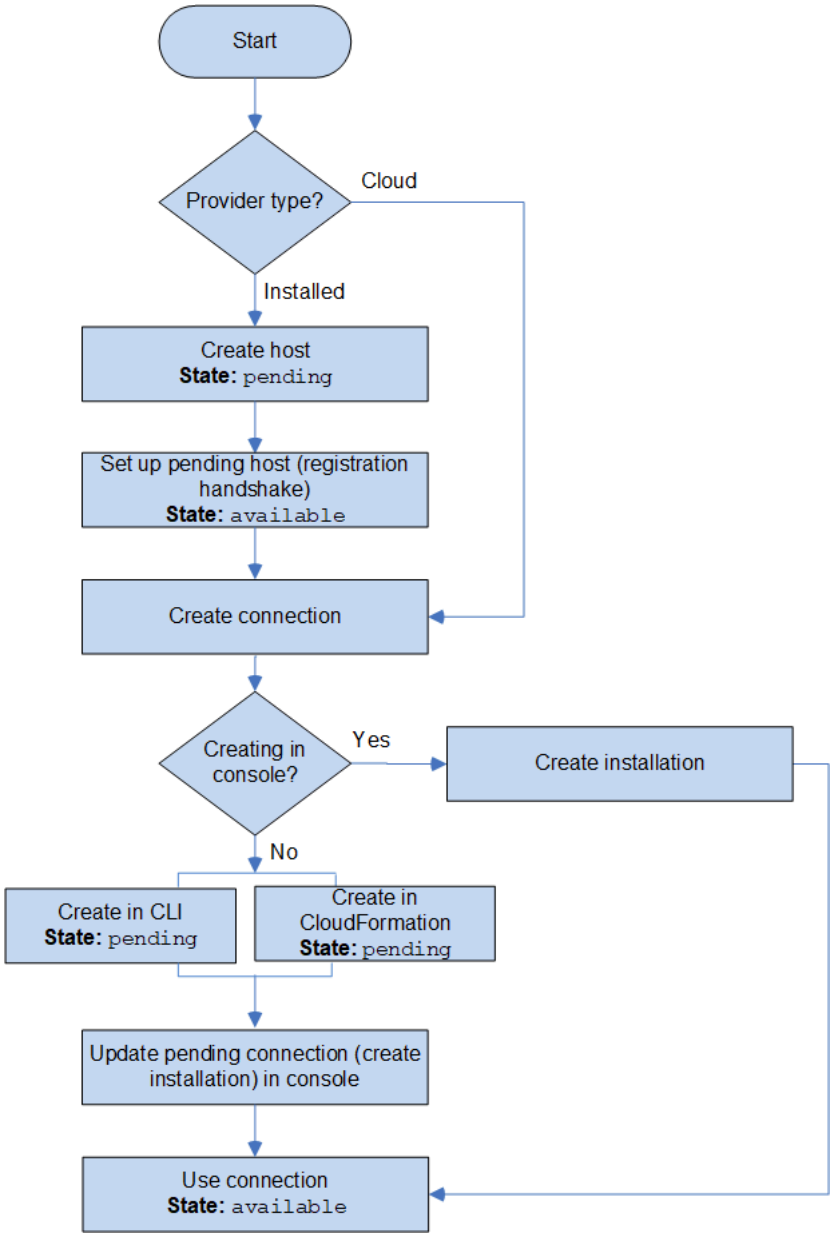
Você usa a CreateConnectionAPI para criar uma conexão usando AWS Command Line Interface (AWS CLI), SDK ou AWS CloudFormation. Após ser criada, a conexão está em um estado `pending`. Você deve então concluir o processo usando a opção Set up pending connection (Configurar conexão pendente do console. O console solicita que você crie uma instalação ou use uma

instalação existente para a conexão. Em seguida, use o console para concluir o handshake e mover a conexão para um estado `available` escolhendo Complete connection (Concluir conexão) no console.

Fluxo de trabalho: criação ou atualização de uma conexão com o console

Se você estiver criando uma conexão com um tipo de provedor instalado, como o GitHub Enterprise Server, primeiro crie um host. Se você estiver se conectando a um tipo de provedor de nuvem, como Bitbucket, ignore a criação do host e continue criando uma conexão.

Para criar ou atualizar uma conexão usando o console, use a página de ação de CodePipeline edição no console para escolher seu provedor terceirizado. O console solicita que você crie uma instalação ou use uma instalação existente para a conexão e, em seguida, use o console para criar a conexão. O console conclui o handshake e move a conexão de `pending` automaticamente para um estado `available`.



O que devo fazer para começar a usar conexões?

Para começar, veja alguns tópicos úteis para revisar:

- Saiba mais sobre os conceitos de conexões.
- Configure os recursos necessários para começar a trabalhar com conexões.
- Comece a configurar suas primeiras conexões e conecte-as a um recurso.

Conceitos de conexões

Configurar e usar o recurso de notificações é mais fácil quando você compreende os conceitos e termos. Veja alguns conceitos que você deve saber ao usar conexões no console do Developer Tools:

instalação

Uma instância da aplicação AWS em uma conta de terceiros. A instalação da aplicação AWS CodeStar Connector permite que a AWS acesse recursos na conta de terceiros. Uma instalação só poderá ser editada no site do provedor de terceiros.

conexão

Um recurso da AWS usado para conectar repositórios de origem de terceiros a outros serviços da AWS.

repositório de terceiros

Um repositório que é fornecido por um serviço ou empresa que não faz parte da AWS. Por exemplo, um repositório BitBucket é um repositório de terceiros.

tipo de provedor

Um serviço ou empresa que fornece o repositório de origem de terceiros ao qual você deseja se conectar. Você conecta seu recursos da AWS a tipos de provedores externos. Um tipo de provedor em que o repositório de origem está instalado na rede e a infraestrutura é um tipo de provedor instalado. Por exemplo, o GitHub Enterprise Server é um tipo de provedor instalado.

host

Um recurso que representa a infraestrutura em que um provedor de terceiros está instalado. As conexões usam o host para representar o servidor em que seu provedor de terceiros está instalado, como o GitHub Enterprise Server. Você cria um host para todas as conexões a esse tipo de fornecedor.

> **Note**
>
> Ao usar o console para criar uma conexão com o GitHub Enterprise Server, o console cria um recurso de host para você como parte do processo.

AWS CodeStar Conexões, provedores e versões compatíveis

Este capítulo fornece informações sobre os provedores e as versões compatíveis AWS CodeStar com o Connections.

Tópicos

Tipo de provedor compatível com o Bitbucket

Você pode usar o AWS CodeStar aplicativo com o Atlassian Bitbucket Cloud.

Não há suporte a tipos de provedores instalados do Bitbucket, como o Bitbucket Server.

Tipo de provedor compatível com GitHub o GitHub Enterprise Cloud

Você pode usar o AWS Conector para GitHub aplicativos com GitHub o GitHub Enterprise Cloud.

Tipo e versões de provedor compatíveis com o GitHub Enterprise Server

Você pode usar o AWS CodeStar aplicativo com versões compatíveis do GitHub Enterprise Server. Para ver uma lista das versões com suporte, consulte https://enterprise.github.com/releases/.

> **Important**
>
> AWS CodeStar O Connections não oferece suporte a versões obsoletas do GitHub Enterprise Server. Por exemplo, o AWS CodeStar Connections não oferece suporte ao GitHub Enterprise Server versão 2.22.0 devido a um problema conhecido na versão. Para conectar, atualize para a versão 2.22.1 ou a versão mais recente disponível.

Tipo de provedor compatível para GitLab

Você pode usar conexões com GitLab. Para ter mais informações, consulte Crie uma conexão com GitLab.

Tipo de provedor compatível para GitLab autogerenciamento

Você pode usar conexões com instalação GitLab autogerenciada (para Enterprise Edition ou Community Edition). Para ter mais informações, consulte Crie uma conexão com o GitLab autogerenciado.

Integrações de produtos e serviços com o AWS CodeStar Connections

O AWS CodeStar Connections é integrado a vários serviços e produtos e serviços de parceiros da AWS Use as informações nas seções a seguir para ajudar a configurar conexões para se integrar aos produtos e aos serviços que você usa.

Os recursos relacionados a seguir podem ajudar você à medida que trabalha com este serviço.

Tópicos

- Amazon CodeGuru Reviewer
- Amazon CodeWhisperer
- Amazon SageMaker
- AWS App Runner
- AWS CloudFormation
- AWS CodePipeline
- AWS CodeStar
- Service Catalog
- AWS Proton

Amazon CodeGuru Reviewer

CodeGuru Reviewer é um serviço para monitorar o código de seu repositório. Você pode usar conexões para associar o repositório de terceiros que tem o código-fonte a ser analisado. Para ver um tutorial em que você aprende a configurar o CodeGuru Reviewer para monitorar o código-fonte em um repositório do GitHub, a fim de que ele possa criar recomendações que melhorem o código, consulte Tutorial: monitor source code in a GitHub repository (Tutorial: Monitorar o código-fonte em um repositório do GitHub) no Guia do usuário do Amazon CodeGuru Reviewer.

Amazon CodeWhisperer

O Amazon CodeWhisperer é um serviço para analisar o código do repositório. O CodeWhisperer analisa o código e fornece recomendações de código em tempo real. Para ver as etapas para configurar uma personalização no CodeWhisperer em que você acessa a fonte de dados usando uma conexão, consulte Criar sua personalização no Guia do usuário do Amazon CodeWhisperer.

Amazon SageMaker

O Amazon SageMaker é um serviço para criar, treinar e implantar modelos de linguagem de machine learning. Para ver um tutorial em que você configura uma conexão com o repositório do GitHub, consulte Passo a passo do projeto SageMaker MLOps usando repositórios Git de terceiros no Guia do desenvolvedor do Amazon SageMaker.

AWS App Runner

O AWS App Runner é um serviço que fornece um modo rápido, simples e econômico de fazer implantações usando o código-fonte ou uma imagem de contêiner diretamente em uma aplicação Web escalável e segura na Nuvem AWS. Você pode implantar o código da aplicação usando seu repositório com um pipeline automático de integração e entrega do App Runner. Você pode usar conexões para implantar o código-fonte em um serviço do App Runner usando um repositório privado do GitHub. Para obter mais informações, consulte Source code repository providers (Provedores de repositório de código-fonte) no Guia do desenvolvedor do AWS App Runner.

AWS CloudFormation

O AWS CloudFormation é um serviço que ajuda você a modelar e configurar seus recursos da AWS para despender menos tempo gerenciando esses recursos e mais tempo se concentrando em seus aplicativos executados AWS. Você cria um modelo que descreve todos os recursos da AWS desejados (como funções do Amazon EC2 e tabelas do Amazon RDS), e o CloudFormation cuida do provisionamento e da configuração desses recursos para você. Para ter mais informações, consulte Registrar sua conta para publicar extensões do CloudFormation no Guia do usuário da interface da linha de comando do CloudFormation.

AWS CodePipeline

O CodePipeline é um serviço de entrega contínua que pode ser usado para modelar, visualizar e automatizar as etapas necessárias para lançar seu software. Você pode usar conexões para configurar um repositório de terceiros para ações do CodePipeline.

Saiba mais:

- Consulte a página de referência de configuração de ações do CodePipeline para ver a ação `CodeStarSourceConnection`. Para ver os parâmetros de configuração e um exemplo de trecho JSON/YAML, consulte CodeStarSourceConnection no Guia do usuário do AWS CodePipeline.
- Para visualizar um tutorial de conceitos básicos que cria um pipeline com um repositório de origem de terceiros, consulte Conceitos básicos sobre conexões.

AWS CodeStar

O AWS CodeStar é um serviço baseado em nuvem para criar, gerenciar e trabalhar com projetos de desenvolvimento de software na AWS. Você pode desenvolver, projetar e implantar aplicativos na AWS rapidamente com um projeto do AWS CodeStar. É possível usar conexões para configurar seus repositórios de terceiros para os pipelines nos projetos do AWS CodeStar. Para ver um tutorial em que você cria um projeto do AWS CodeStar com uma conexão com um repositório do GitHub, consulte Criar um link para o seu repositório no Guia do usuário do AWS CodeStar.

Service Catalog

O Service Catalog permite que as organizações criem e gerenciem catálogos de produtos aprovados para uso na AWS.

Quando você autoriza uma conexão entre sua Conta da AWS e um provedor de repositório externo, como GitHub, GitHub Enterprise ou BitBucket, a conexão permite que você sincronize produtos do Service Catalog com arquivos de modelo gerenciados por meio de repositórios de terceiros.

Para obter mais informações, consulte Sincronizar produtos do Service Catalog com arquivos de modelo do GitHub, GitHub Enterprise ou Bitbucket no Guia do usuário do Service Catalog.

AWS Proton

AWS Proton é um serviço baseado em nuvem para implantação na infraestrutura de nuvem. É possível usar conexões para criar um link direcionado a repositórios de terceiros para os recursos em seus modelos do AWS Proton. Para obter mais informações, consulte Create a link to your repository (Criar um link para seu repositório) no Guia do usuário do AWS Proton.

Configuração de conexões

Conclua as tarefas nesta seção para configurar a criação e o uso do recurso de conexões no console do Developer Tools.

Tópicos

Cadastrar para AWS

Cadastrar-se em uma Conta da AWS

Se você ainda não tem uma Conta da AWS, siga as etapas a seguir para criar uma.

Para se cadastrar em uma Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se cadastra em uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário administrativo e use somente o usuário raiz para realizar as tarefas que exigem acesso do usuário raiz.

A AWS envia um e-mail de confirmação depois que o processo de cadastramento é concluído. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Crie um usuário administrador

Depois de se cadastrar em uma Conta da AWS, proteja seu Usuário raiz da conta da AWS, habilite o AWS IAM Identity Center e crie um usuário administrativo para não usar o usuário raiz em tarefas cotidianas.

Proteger seu Usuário raiz da conta da AWS

1. Faça login no AWS Management Console como o proprietário da conta ao escolher a opção Usuário raiz e inserir o endereço de e-mail da Conta da AWS. Na próxima página, digite sua 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. Ative a autenticação multifator (MFA) para o usuário raiz.c

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

Criar um usuário administrativo

1. Habilitar o IAM Identity Center.

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

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

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configure user access with the default Diretório do Centro de Identidade do IAM no Guia do usuário do AWS IAM Identity Center.

Login como usuário administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda com o login utilizando um usuário do Centro de Identidade do IAM, consulte Fazer login no portal de acesso da AWS, no Guia do usuário do Início de Sessão da AWS.

Criar e aplicar uma política com permissões para criar conexões

Para usar o editor de políticas JSON para criar uma política

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Policies (Políticas).

   Se essa for a primeira vez que você escolhe Políticas, a página Bem-vindo às políticas gerenciadas será exibida. Escolha Conceitos básicos.

3. Na parte superior da página, escolha Criar política.
4. Na seção Editor de políticas, escolha a opção JSON.
5. Insira o seguinte documento de política JSON:

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "codestar-connections:CreateConnection",
               "codestar-connections:DeleteConnection",
               "codestar-connections:GetConnection",
               "codestar-connections:ListConnections",
               "codestar-connections:GetInstallationUrl",
               "codestar-connections:GetIndividualAccessToken",
               "codestar-connections:ListInstallationTargets",
               "codestar-connections:StartOAuthHandshake",
               "codestar-connections:UpdateConnectionInstallation",
               "codestar-connections:UseConnection"
           ],
           "Resource": [
               "*"
           ]
       }
   ]
}
```

6. Escolha Próximo.

> **Note**
>
> É possível alternar entre as opções de editor Visual e JSON a qualquer momento. Porém, se você fizer alterações ou escolher Próximo no editor Visual, o IAM poderá reestruturar a política a fim de otimizá-la para o editor visual. Para obter mais informações, consulte Restruturação de política no Guia do usuário do IAM.

7. Na página Revisar e criar, insira um Nome de política e uma Descrição (opcional) para a política que você está criando. Revise Permissões definidas nessa política para ver as permissões que são concedidas pela política.

8. Escolha Criar política para salvar sua nova política.

Conceitos básicos sobre conexões

A maneira mais fácil de começar a usar conexões é configurar uma conexão que associe seu repositório de origem de terceiro aos recursos da AWS. Se quisesse conectar seu pipeline a uma fonte da AWS, como CodeCommit, você se conectaria a ela como uma ação de origem. No entanto, se você tiver um repositório externo, será necessário criar uma conexão para associar seu repositório ao pipeline. Neste tutorial, você configura uma conexão com seu repositório do Bitbucket e seu pipeline.

Nesta seção, você usa conexões com:

- AWS CodePipeline: nestas etapas, você cria um pipeline com seu repositório do Bitbucket como a origem do pipeline.
- Amazon CodeGuru Reviewer: em seguida, associe o repositório do Bitbucket às suas ferramentas de feedback e análise no CodeGuru Reviewer.

Tópicos

Pré-requisitos

Antes de começar, conclua as etapas em Configuração. Você também precisa de um repositório de origem de terceiro a ser conectado aos seus serviços da AWS e permitir que a conexão gerencie a autenticação para você. Por exemplo, talvez você queira conectar um repositório do Bitbucket aos seus serviços da AWS que se integram aos repositórios de origem.

- Crie um repositório do Bitbucket com sua conta Bitbucket.
- Tenha suas credenciais do Bitbucket em mãos. Ao usar o AWS Management Console para configurar uma conexão, você é avisado para entrar com suas credenciais do Bitbucket.

Etapa 1: Editar o arquivo de origem

Quando você cria seu repositório do Bitbucket, um arquivo `README.md` está incluído, o qual você deverá editar.

1. Faça login no seu repositório do Bitbucket e escolha Source (Origem).
2. Selecione o arquivo `README.md` e escolha Edit (Editar) na parte superior da página. Exclua o texto existente e adicione o texto a seguir.

   ```
   This is a Bitbucket repository!
   ```

3. Escolha Commit (Confirmar).

   Certifique-se de que o arquivo `README.md` esteja no nível raiz do repositório.

Etapa 2: Criar o pipeline

Nesta seção, você criará um pipeline com as seguintes ações:

- Um estágio de origem com uma conexão com seu repositório do Bitbucket e ação.
- Um estágio de compilação com uma ação de compilação AWS CodeBuild.

Criar um pipeline com o assistente

1. Faça login no console do CodePipeline em https://console.aws.amazon.com/codesuite/codepipeline.
2. Na página Welcome (Bem-vindo), Getting started (Conceitos básicos) ou Pipelines, selecione Create pipeline (Criar pipeline).
3. Em Step 1: Choose pipeline settings (Etapa 1: selecionar as configurações do pipeline), em Pipeline name (Nome do pipeline), insira **`MyBitbucketPipeline`**.
4. Em Service role (Função do serviço), selecione New service role (Nova função de serviço).

   > **Note**
   >
   > Se você optar por usar sua função de serviço do CodePipeline existente, certifique-se de ter adicionado a permissão do IAM `codestar-connections:UseConnection` à

sua política de função de serviço. Para obter instruções sobre a função de serviço do CodePipeline, consulte Adicionar permissões à função de serviço do CodePipeline.

5. Em Configurações avançadas mantenha os padrões. Em Artifact store (Armazenamento de artefatos), selecione Default location (Local padrão) para usar o armazenamento de artefatos padrão, como o bucket de artefatos do Amazon S3 designado como padrão, para o pipeline na região que você selecionou.

> **Note**
>
> Este não é o bucket de origem para seu código-fonte. Este é o armazenamento de artefatos para o pipeline. Um armazenamento de artefatos separado, como um bucket do S3, é necessário para cada pipeline.

   Escolha Next (Próximo).

6. Na página Step 2: Add source stage (Etapa 2: Adicionar um estágio de origem), adicione um estágio de origem:

   a. Em Source provider (Provedor de origem), escolha Bitbucket.

   b. Em Connection (Conexão), escolha Connect to Bitbucket (Conectar a Bitbucket).

   c. Na página Connect to Bitbucket (Conectar ao Bitbucket), em Connection name (Nome da conexão), digite o nome da conexão que deseja criar. O nome ajuda você a identificar essa conexão posteriormente.

      Em Bitbucket apps (Aplicações do Bitbucket), escolha Install a new app (Instalar uma nova aplicação).

   d. Na página de instalação do aplicativo, uma mensagem mostra que o aplicativo do AWS CodeStar está tentando se conectar à sua conta do Bitbucket. Escolha Grant access (Conceder acesso). Depois de autorizar a conexão, seus repositórios no Bitbucket serão detectados, e você poderá optar por associar um ao seu recurso da AWS.

   e. O ID de conexão para sua nova instalação é exibido. Escolha Complete connection (Conexão completa). Você retornará ao console do CodePipeline.

   f. Em Repository name (Nome do repositório), selecione o nome do seu repositório do Bitbucket.

   g. Em Branch name (Nome da ramificação), escolha a ramificação para seu repositório.

h. Assegure-se de que a opção Iniciar o pipeline na alteração do código-fonte esteja selecionada.

i. Em Formato do artefato de saída, selecione uma das seguintes opções: CodePipeline padrão.

- Selecione CodePipeline padrão a fim de usar o formato zip padrão para artefatos no pipeline.
- Selecione Clone completo para incluir metadados do Git sobre o repositório de artefatos no pipeline. Isso só é possível com ações do CodeBuild.

Escolha Next (Próximo).

7. Em Add build stage (Adicionar estágio de compilação), adicione um estágio de compilação:

a. Em Build provider (Provedor de compilação), escolha AWS CodeBuild. Permita que Region (Região) seja definida para a região do pipeline.

b. Escolha Create project (Criar projeto).

c. Em Project name (Nome do projeto), insira um nome para esse projeto de compilação.

d. Em Environment image (Imagem do ambiente), escolha Managed image (Imagem gerenciada). Para Operating system, selecione Ubuntu.

e. Em Runtime (Tempo de execução), selecione Standard (Padrão). Em Imagem, selecione aws/codebuild/standard:5.0.

f. Em Service role (Função de serviço), selecione New service role (Nova função de serviço).

g. Em Buildspec, para Build specifications (Especificações da compilação), escolha Insert build commands (Inserir comandos de compilação). Selecione Switch to editor (Alternar para o editor) e cole o seguinte em Build commands (Comandos de compilação):

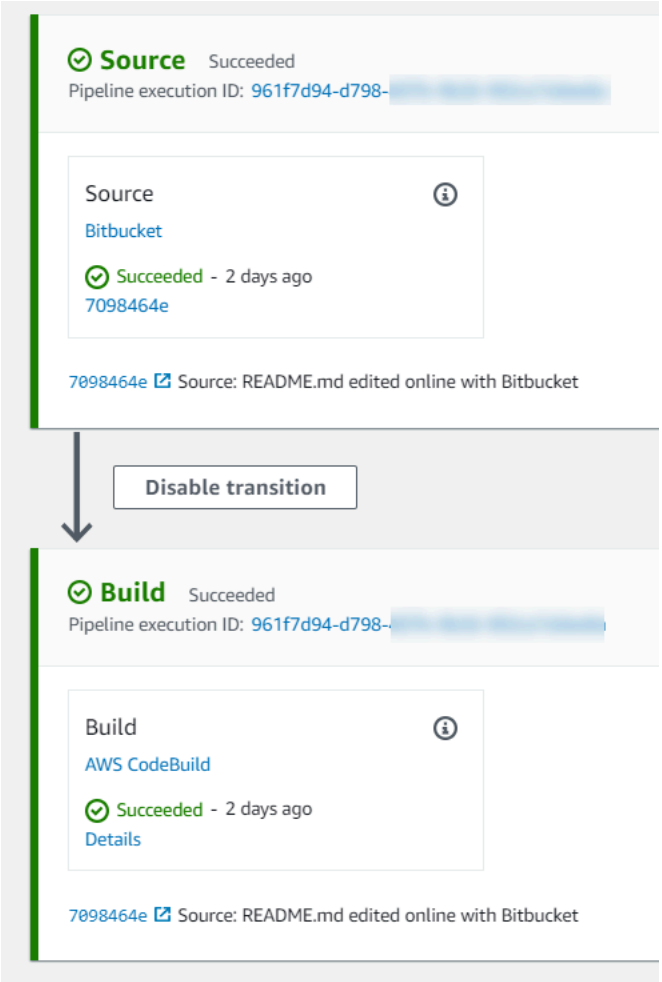
```
version: 0.2

phases:
  install:
    #If you use the Ubuntu standard image 2.0 or later, you must specify
 runtime-versions.
    #If you specify runtime-versions and use an image other than Ubuntu
 standard image 2.0, the build fails.
    runtime-versions:
      nodejs: 12
      # name: version
```

```
    #commands:
      # - command
      # - command
  pre_build:
    commands:
      - ls -lt
      - cat README.md
  # build:
    #commands:
      # - command
      # - command
  #post_build:
    #commands:
      # - command
      # - command
#artifacts:
  #files:
    # - location
    # - location
  #name: $(date +%Y-%m-%d)
  #discard-paths: yes
  #base-directory: location
#cache:
  #paths:
    # - paths
```

h. Escolha Continue to CodePipeline (Continuar para CodePipeline). Isso retornará para o console do CodePipeline e criará um projeto do CodeBuild que usa seus comandos de compilação para configuração. O projeto de compilação usa uma função de serviço para gerenciar permissões de serviço da AWS. Essa etapa pode levar alguns minutos.

i. Escolha Next (Próximo).

8. Na página Step 4: Add deploy stage (Etapa 4: adicionar estágio de implantação), escolha Skip deploy stage (Ignorar estágio de implantação) e aceite a mensagem de aviso ao clicar novamente em Skip (Ignorar). Escolha Next (Próximo).
9. Em Step 5: Review (Etapa 5: revisar), escolha Create pipeline (Criar pipeline).
10. Quando seu pipeline é criado com êxito, uma execução de pipeline é iniciada.



11. Em seu estágio de construção bem-sucedido, escolha Details (Detalhes).

    Em Execution details (Detalhes da execução), visualize a saída de compilação do CodeBuild. Os comandos geram o conteúdo do arquivo `README.md` da seguinte forma:

```
This is a Bitbucket repository!
```

```
35 [Container] 2020/06/05 19:14:51 Running command cat README.md
36 This is a Bitbucket repository!
37 [Container] 2020/06/05 19:14:51 Phase complete: PRE_BUILD State: SUCCEEDED
38 [Container] 2020/06/05 19:14:51 Phase context status code:  Message:
39 [Container] 2020/06/05 19:14:51 Entering phase BUILD
40 [Container] 2020/06/05 19:14:51 Phase complete: BUILD State: SUCCEEDED
41 [Container] 2020/06/05 19:14:51 Phase context status code:  Message:
42 [Container] 2020/06/05 19:14:51 Entering phase POST_BUILD
43 [Container] 2020/06/05 19:14:51 Phase complete: POST_BUILD State: SUCCEEDED
44 [Container] 2020/06/05 19:14:51 Phase context status code:  Message:
```

Etapa 3: Associe seu repositório ao CodeGuru Reviewer

Depois de criar uma conexão, você poderá usar essa conexão para todos os seus recursos da AWS na mesma conta. Por exemplo, você pode usar a mesma conexão Bitbucket para uma ação de origem do CodePipeline em um pipeline e a análise de confirmação do repositório no CodeGuru Reviewer.

1. Faça login no console do CodeGuru Reviewer.
2. Em CodeGuru Reviewer, escolha Associate repository (Repositório associado).

   O assistente de uma página é aberto.
3. Em Select source provider (Selecionar provedor de origem), escolha Bitbucket.
4. Em Conectar ao Bitbucket (com o AWS CodeStar connections), selecione a conexão que você criou para o pipeline.
5. Em Local do repositório, escolha o nome do repositório do Bitbucket e escolha Associar.

   Você pode continuar a configurar revisões de código. Para obter mais informações, consulte Conectar ao Bitbucket para associar um repositório ao CodeGuru Reviewer no Manual do usuário do Amazon CodeGuru Reviewer.

Trabalhar com conexões

As conexões são configurações usadas para conectar recursos da AWS a repositórios de código externos. Cada conexão é um recurso que pode ser fornecido a serviços, como AWS CodePipeline a conexão com um repositório de terceiros, como o Bitbucket. Por exemplo, você pode adicionar a conexão para CodePipeline que ela acione seu pipeline quando uma alteração de código for feita em seu repositório de código de terceiros. Você também pode conectar seus AWS recursos a um tipo de provedor instalado, como o GitHub Enterprise Server.

Se você quiser criar uma conexão com um tipo de provedor instalado, como o GitHub Enterprise Server, o console cria um host para você. Um host é um recurso que você cria para representar o servidor em que seu provedor está instalado. Para ter mais informações, consulte Como trabalhar com hosts.

Ao criar uma conexão, você usa um assistente no console para instalar o AWS CodeStar aplicativo com seu provedor terceirizado e associá-lo a uma nova conexão. Se você já instalou o AWS CodeStar aplicativo, pode usá-lo.

> **Note**
>
> Para usar conexões na Europa (Milão) Região da AWS, você deve:
>
> 1. Instalar uma aplicação específica da região.
> 2. Habilitar a região.
>
> Essa aplicação específica da região é compatível com conexões na região Europa (Milão). Ela é publicada no site do provedor externo e é separada da aplicação existente que permite conexões para outras regiões. Ao instalar essa aplicação, você autoriza provedores externos a compartilhar seus dados somente com o serviço dessa região, mas pode revogar as permissões a qualquer momento ao desinstalá-la.
> O serviço não processará nem armazenará seus dados, a menos que você habilite a região. Ao habilitar essa região, você concede ao nosso serviço permissões para processar e armazenar seus dados.
> Mesmo que a região não esteja habilitada, provedores externos ainda poderão compartilhar seus dados com nosso serviço se a aplicação específica da região permanecer instalada. Portanto, desinstale a aplicação depois de desabilitar a região. Para obter mais informações, consulte Habilitar uma região.

Para obter mais informações sobre conexões, consulte a referência da API AWS CodeStar Connections. Para obter mais informações sobre a ação de CodePipeline origem do Bitbucket, consulte CodestarConnectionSourceo Guia do AWS CodePipeline usuário.

Para criar ou anexar uma política ao seu usuário ou função AWS Identity and Access Management (IAM) com as permissões necessárias para usar AWS CodeStar conexões, consulteConexões de código da AWS referência de permissões. Dependendo de quando sua função CodePipeline de serviço foi criada, talvez seja necessário atualizar suas permissões para oferecer suporte às AWS CodeStar conexões. Para obter instruções, consulte Atualizar a função de serviço no Manual do usuário do AWS CodePipeline .

Tópicos

- Criar uma conexão
- Criar uma conexão com o Bitbucket
- Crie uma conexão com GitHub

- Crie uma conexão com o GitHub Enterprise Server
- Crie uma conexão com GitLab
- Crie uma conexão com o GitLab autogerenciado
- Atualizar uma conexão pendente
- Listar Conexões
- Excluir uma conexão
- Recursos de conexões de tags
- Visualizar detalhes da conexão

Criar uma conexão

Você pode criar conexões para os seguintes tipos de provedores de terceiros:

- Para criar uma conexão com o Bitbucket, consulte Criar uma conexão com o Bitbucket.
- Para criar uma conexão com GitHub nossa GitHub Enterprise Cloud, consulteCrie uma conexão com GitHub.
- Para criar uma conexão com o GitHub Enterprise Server, incluindo a criação do seu recurso de host, consulteCrie uma conexão com o GitHub Enterprise Server.
- Para criar uma conexão com GitLab, consulteCrie uma conexão com GitLab.

Criar uma conexão com o Bitbucket

Você pode usar o AWS Management Console ou o AWS Command Line Interface (AWS CLI) para criar uma conexão com um repositório hospedado em bitbucket.org.

Antes de começar

- Você já deve ter criado uma conta com o Bitbucket.
- Você já deve ter criado um repositório de código no bitbucket.org.

> **Note**
>
> Você pode criar conexões para um repositório do Bitbucket Cloud. Não há suporte a tipos de provedores instalados do Bitbucket, como o Bitbucket Server. Consulte AWS CodeStar Conexões, provedores e versões compatíveis.

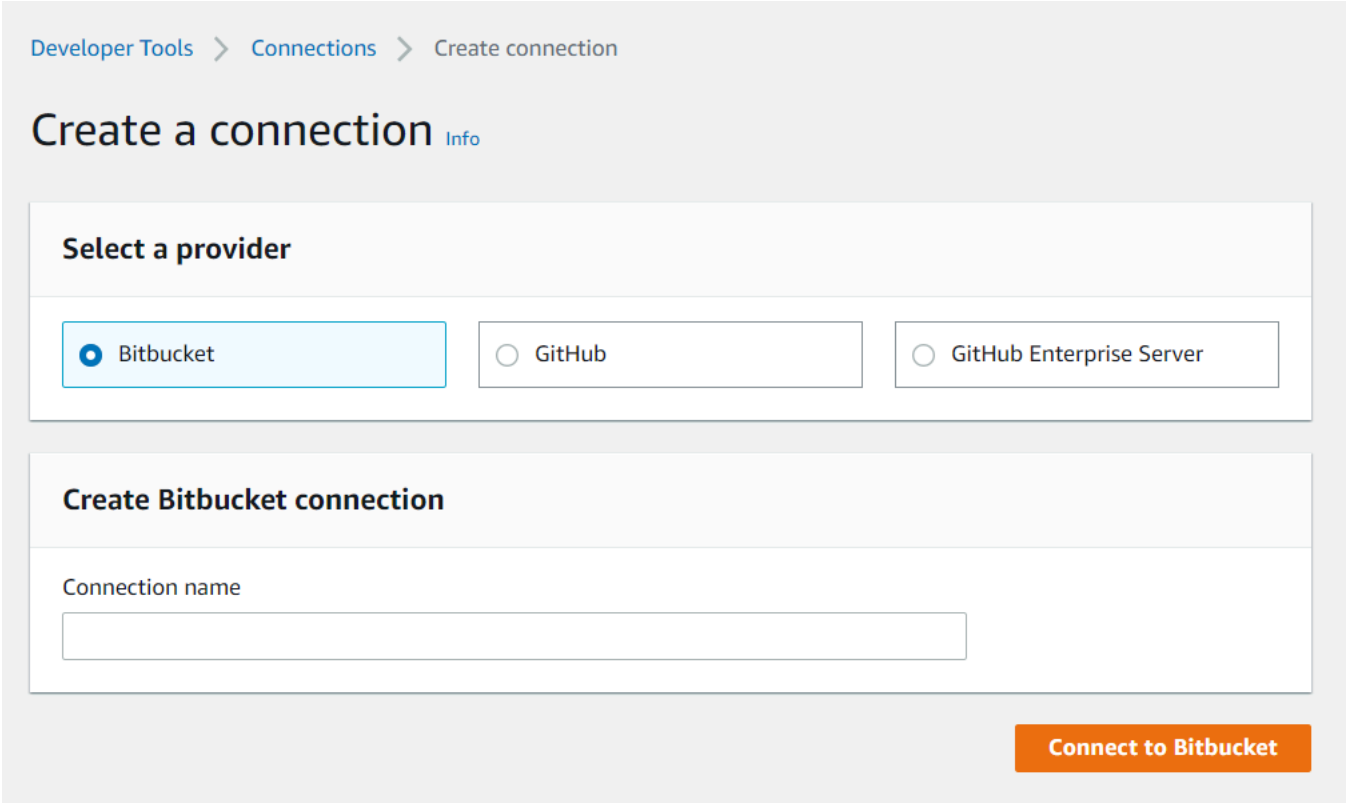
> **Note**
>
> As conexões fornecem acesso somente a repositórios pertencentes à conta do Bitbucket usada para criar a conexão.
> Se a aplicação estiver sendo instalada em um espaço de trabalho do Bitbucket, você precisará de permissões Administer workspace (Administrar o espaço de trabalho). Caso contrário, a opção de instalar a aplicação não será exibida.

Tópicos

Criar uma conexão com o Bitbucket (console)

Etapa 1: criar uma conexão

1. Faça login no e abra AWS Management Console o console do AWS Developer Tools emhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Escolha Settings > Connections (Configurações > Conexões) e, em seguida, escolha Create connection (Criar conexão).
3. Para criar uma conexão com um repositório do Bitbucket, em Select a provider (Selecione um provedor), escolha Bitbucket. Em Connection name (Nome da conexão), digite o nome da conexão que você deseja criar. Selecione Connect to Bitbucket (Conectar ao Bitbucket) e prossiga para a Etapa 2.

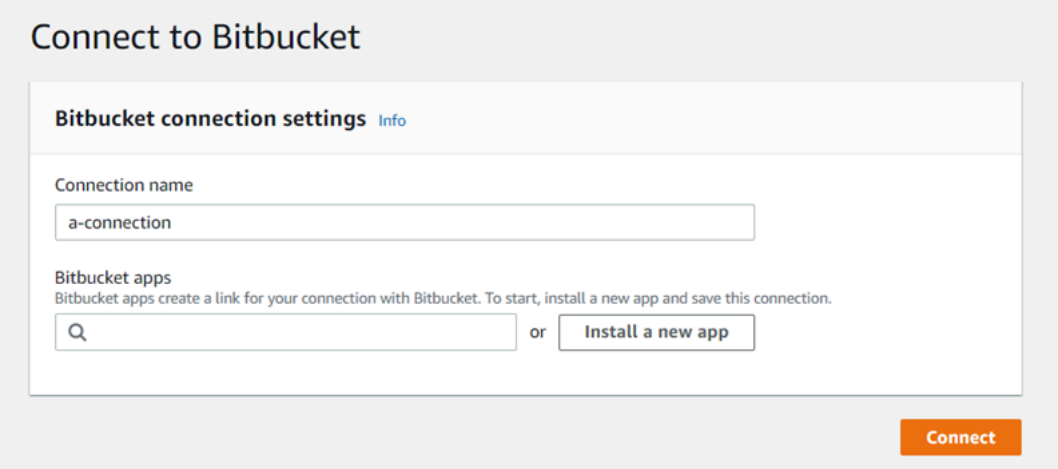


Etapa 2: Conectar ao Bitbucket

1. Seu nome de conexão é exibido na página de configurações de Connect to Bitbucket (Conectar ao Bitbucket).

   Em Bitbucket apps (Aplicações do Bitbucket), escolha uma instalação de aplicação ou Install a new app (Instalar uma nova aplicação) para criar uma.

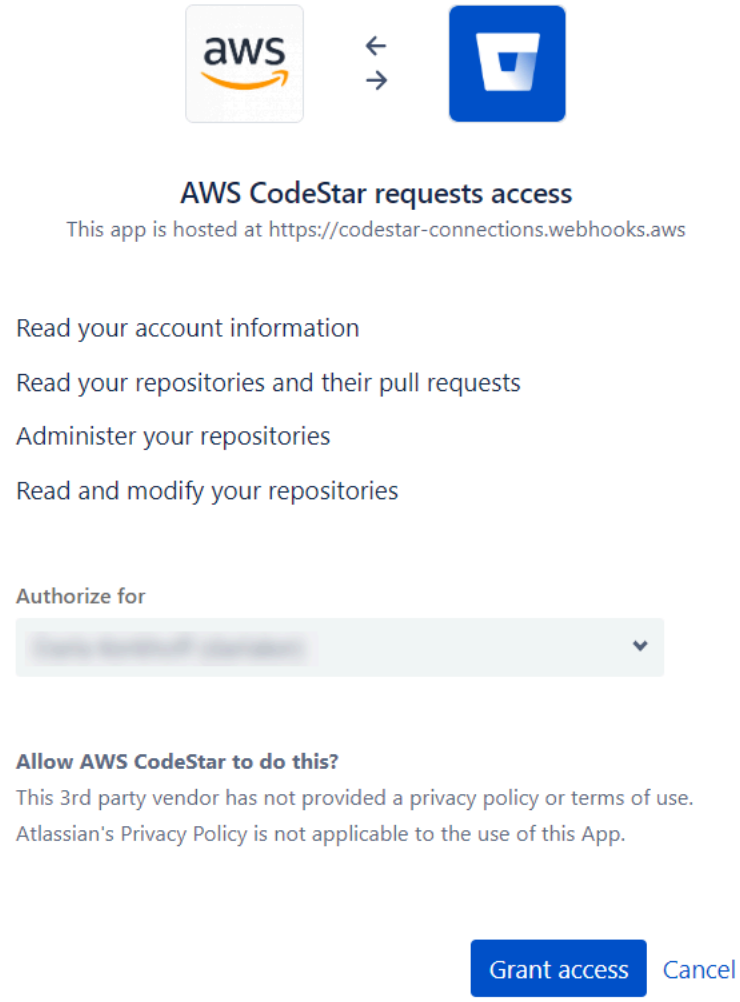
   > **Note**
   >
   > A aplicação é instalada apenas uma vez para cada espaço de trabalho ou conta do Bitbucket. Se você já instalou a aplicação Bitbucket, escolha-a e vá para a última etapa nesta seção.



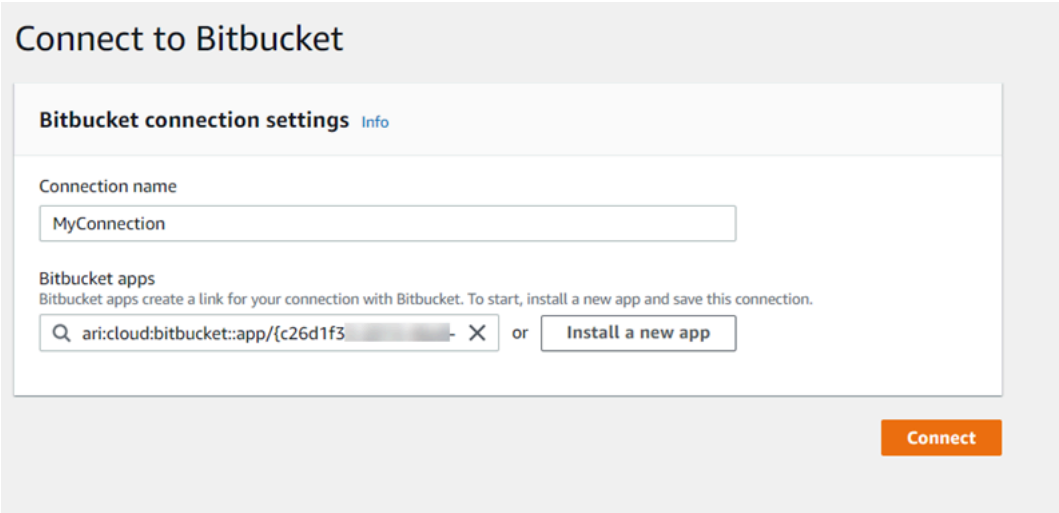
2. Se a página de login do Bitbucket for exibida, faça login com suas credenciais e escolha a opção de continuar.
3. Na página de instalação do aplicativo, uma mensagem mostra que o AWS CodeStar aplicativo está tentando se conectar à sua conta do Bitbucket.

   Se você estiver usando um espaço de trabalho do Bitbucket, altere a opção Authorize for (Autorizar para) do espaço de trabalho. Somente os espaços de trabalho nos quais você tem acesso de administrador serão exibidos.

   Escolha Conceder acesso.



4. Em Bitbucket apps (Aplicações do Bitbucket), o ID de conexão para a nova instalação é exibido. Selecione Conectar. A conexão criada é exibida na lista de conexões.



Criar uma conexão com o Bitbucket (CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para criar uma conexão.

Para fazer isso, use o comando create-connection.

> **Important**
>
> Uma conexão criada por meio do AWS CLI ou AWS CloudFormation está no `PENDING` status por padrão. Depois de criar uma conexão com a CLI ou AWS CloudFormation, use o console para editar a conexão e definir seu status. `AVAILABLE`

Para criar uma conexão com o Bitbucket

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o create-connection comando, especificando `--provider-type` e `--connection-name` para sua conexão. Neste exemplo, o nome do provedor de terceiros é `Bitbucket` e o nome da conexão especificada é `MyConnection`.

   ```
   aws codestar-connections create-connection --provider-type Bitbucket --connection-name MyConnection
   ```

   Se tiver êxito, esse comando gerará as informações do ARN de conexão semelhantes às seguintes.

   ```
   {
       "ConnectionArn": "arn:aws:codestar-connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f"
   }
   ```

2. Use o console para concluir a conexão. Para ter mais informações, consulte Atualizar uma conexão pendente.

Crie uma conexão com GitHub

Você pode usar o AWS Management Console ou o AWS Command Line Interface (AWS CLI) para criar uma conexão com GitHub.

Antes de começar

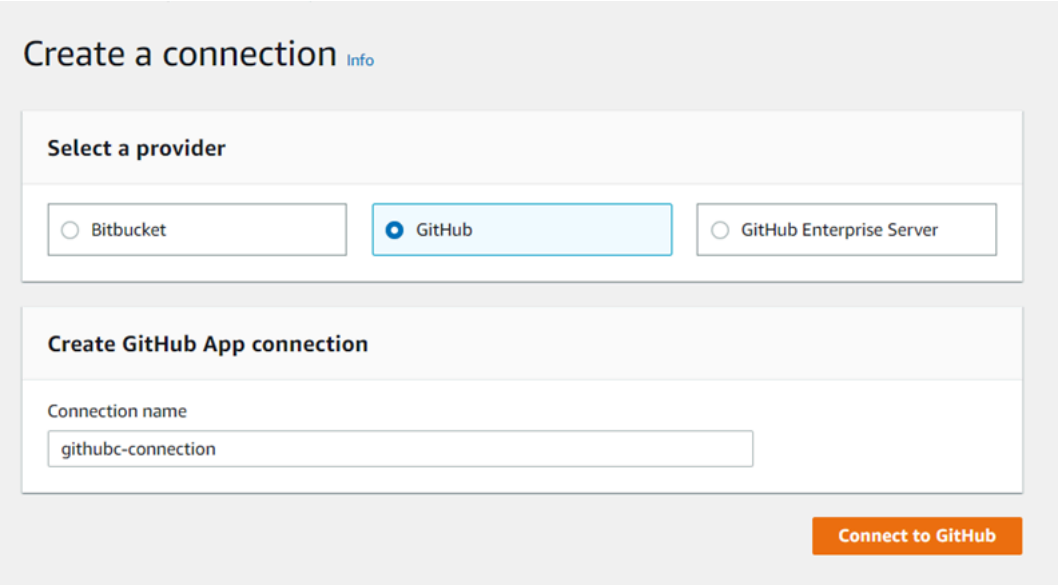
- Você já deve ter criado uma conta com GitHub.
- Você já deve ter criado seu repositório de código de terceiros.

> **Note**
>
> Para criar a conexão, você deve ser o proprietário GitHub da organização. Para repositórios que não estão em uma organização, você deve ser o proprietário do repositório.

Tópicos

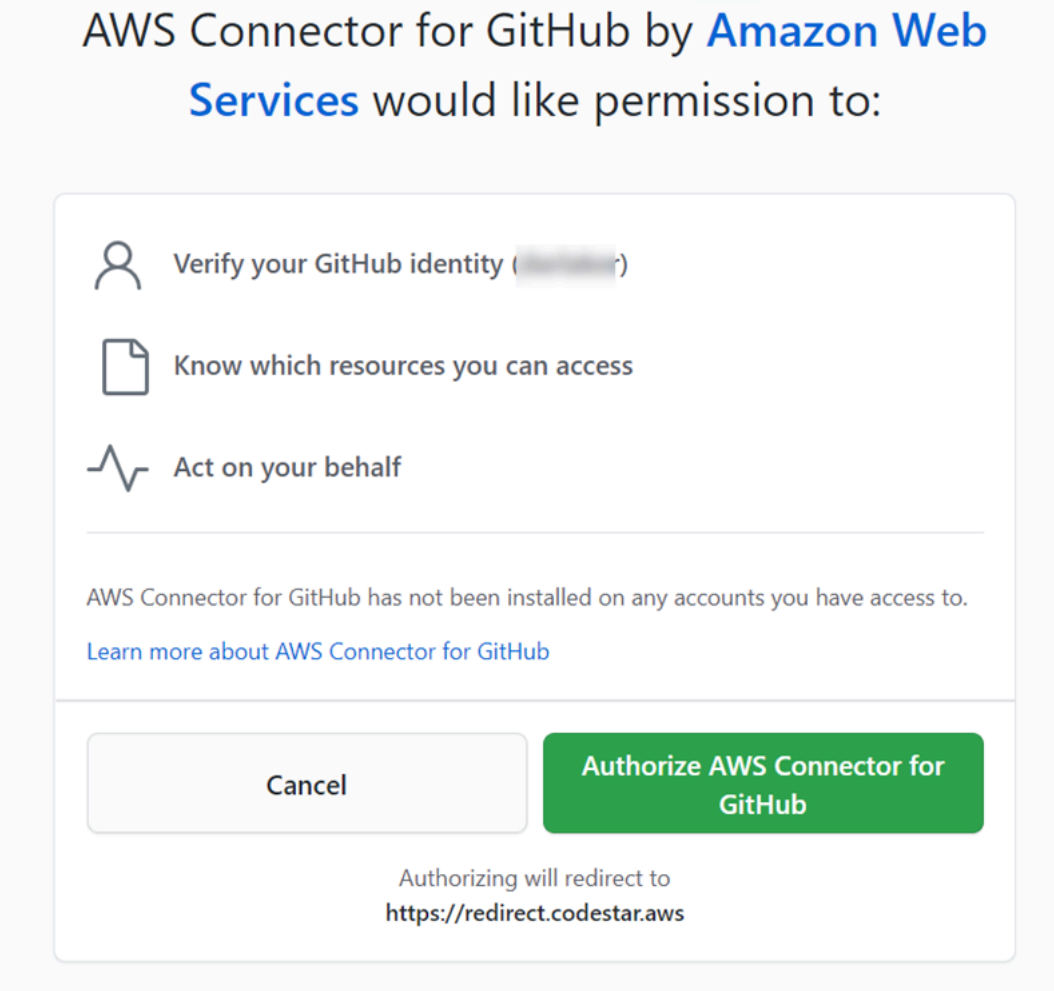
Crie uma conexão com GitHub (console)

1. Faça login no e abra AWS Management Console o console do Developer Tools emhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Escolha Settings > Connections (Configurações > Conexões) e, em seguida, escolha Create connection (Criar conexão).
3. Para criar uma conexão com um repositório GitHub ou com o GitHub Enterprise Cloud, em Selecionar um provedor, escolha GitHub. Em Connection name (Nome da conexão), digite o nome da conexão que você deseja criar. Escolha Connect GitHub to e vá para a Etapa 2.

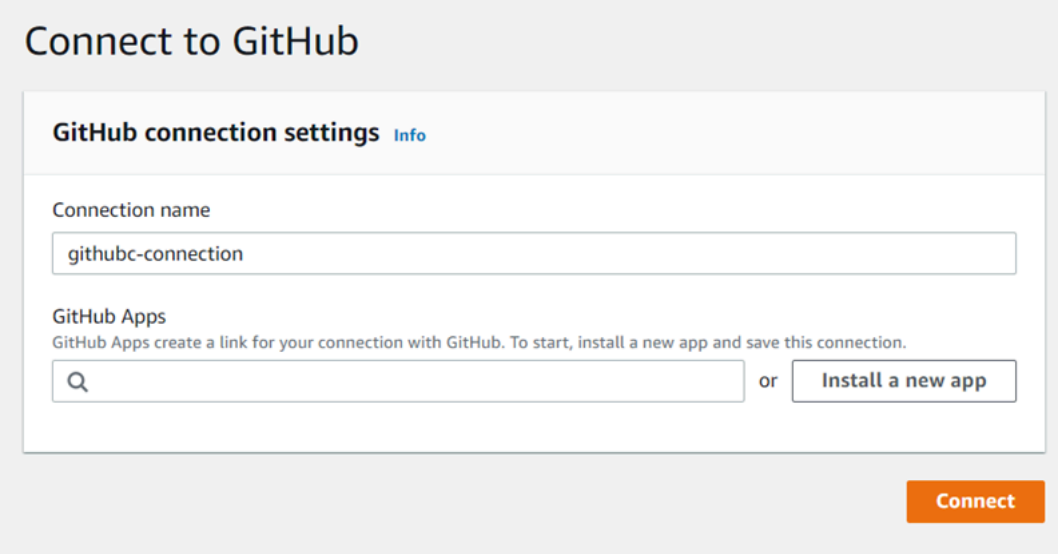


Para criar uma conexão com GitHub

1. Nas configurações de GitHub conexão, o nome da conexão aparece em Nome da conexão. Escolha Connect to GitHub. A página de solicitação de acesso será exibida.



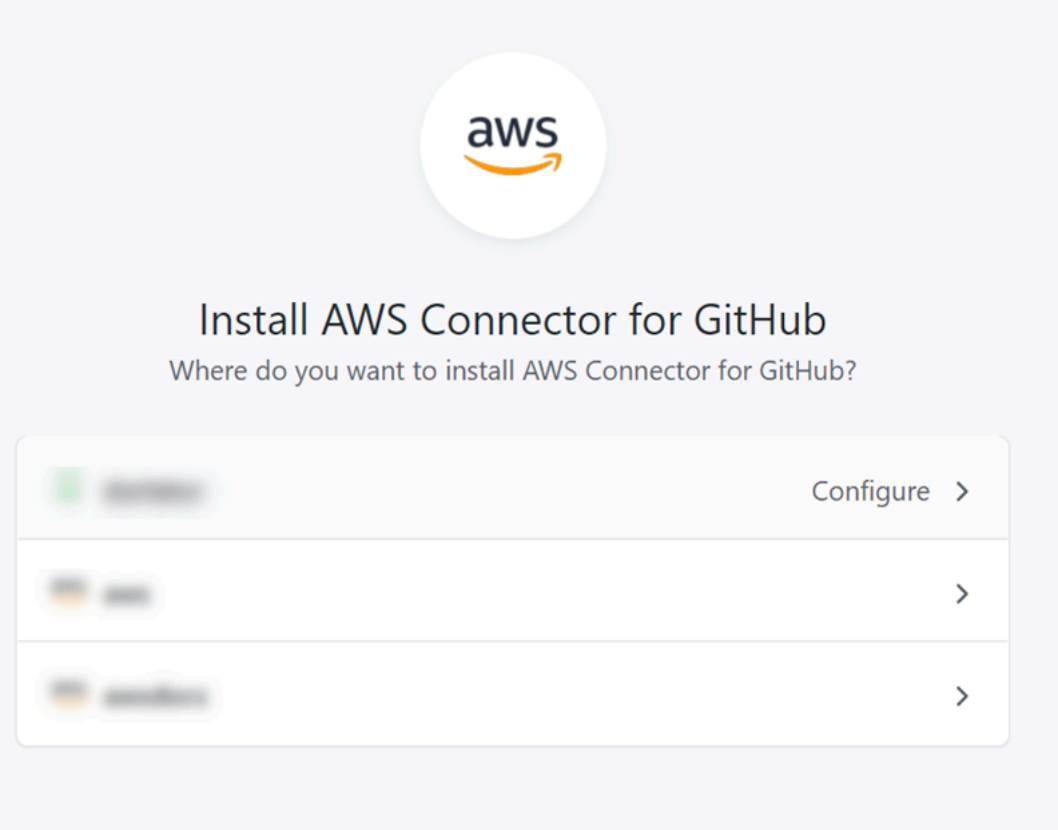
2. Escolha Autorizar AWS conector para GitHub. A página de conexão é exibida e mostra o campo GitHub Aplicativos.



3. Em GitHub Aplicativos, escolha uma instalação de aplicativo ou escolha Instalar um novo aplicativo para criar um.

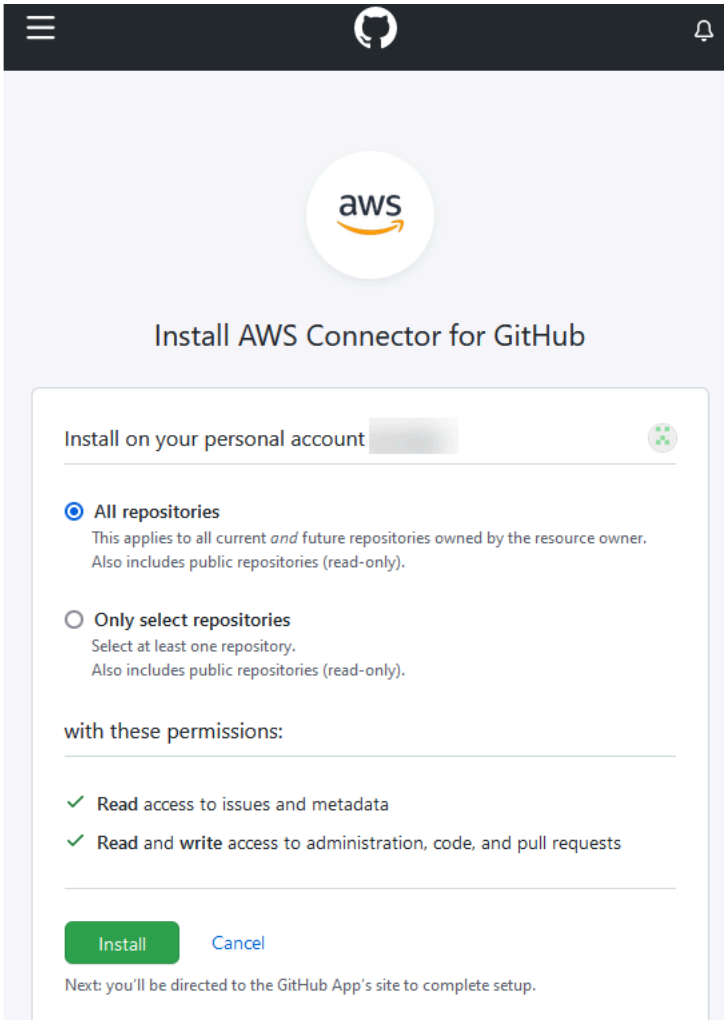
> **Note**
>
> Você instala uma aplicação para todas as suas conexões com um provedor específico. Se você já instalou o GitHub aplicativo AWS Connector for, escolha-o e pule esta etapa.

4. Na GitHub página Install AWS Connector for, escolha a conta na qual você deseja instalar o aplicativo.



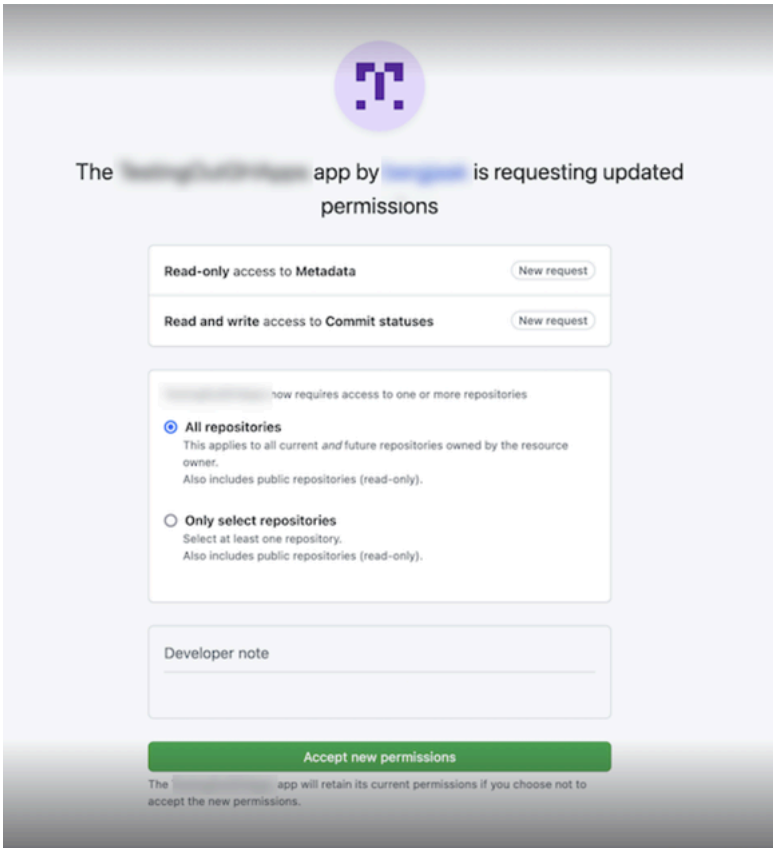
> **Note**
>
> Você só instala o aplicativo uma vez para cada GitHub conta. Se você instalou a aplicação anteriormente, poderá escolher Configure (Configurar) para prosseguir para uma página de modificação para a instalação da aplicação ou usar o botão Back (Voltar) para retornar ao console.

5. Na GitHub página Install AWS Connector for, deixe os padrões e escolha Instalar.



Após essa etapa, uma página de permissões atualizada pode ser exibida em GitHub.

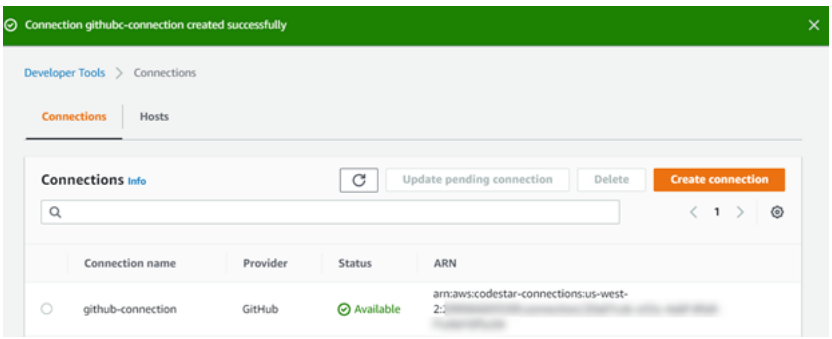
6. Se uma página for exibida mostrando que há permissões atualizadas para o GitHub aplicativo AWS Connector for, escolha Aceitar novas permissões.



7. Você retornará à GitHub página Connect to. O ID de conexão da sua nova instalação aparece em GitHubAplicativos. Selecione Conectar.

Visualizar sua conexão criada

- A conexão criada é exibida na lista de conexões.



Crie uma conexão com GitHub (CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para criar uma conexão com GitHub.

Para fazer isso, use o comando create-connection.

> **Important**
>
> Uma conexão criada por meio do AWS CLI ou AWS CloudFormation está no `PENDING` status por padrão. Depois de criar uma conexão com a CLI ou AWS CloudFormation, use o console para editar a conexão e definir seu status. `AVAILABLE`

Para criar uma conexão com GitHub

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o create-connection comando, especificando `--provider-type` e `--connection-name` para sua conexão. Neste exemplo, o nome do provedor de terceiros é `GitHub` e o nome da conexão especificada é `MyConnection`.

   ```
   aws codestar-connections create-connection --provider-type GitHub --connection-name
    MyConnection
   ```

   Se tiver êxito, esse comando gerará as informações do ARN de conexão semelhantes às seguintes.

   ```
   {
       "ConnectionArn": "arn:aws:codestar-connections:us-west-2:account_id:connection/
   aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f"
   }
   ```

2. Use o console para concluir a conexão. Para ter mais informações, consulte Atualizar uma conexão pendente.

Crie uma conexão com o GitHub Enterprise Server

Você usa conexões para associar seus AWS recursos a um repositório de terceiros. Você pode usar o AWS Management Console ou o AWS Command Line Interface (AWS CLI) para criar uma conexão com o GitHub Enterprise Server.

As conexões fornecem acesso somente aos repositórios pertencentes à conta do GitHub Enterprise Server que são usados durante a criação da conexão para autorizar a instalação do GitHub aplicativo.

Antes de começar

- Você já deve ter uma instância do GitHub Enterprise Server e um repositório nela.
- Você precisa ser administrador da instância do GitHub Enterprise Server para criar GitHub aplicativos e criar um recurso de host, conforme mostrado nesta seção.

> **Important**
>
> Quando você configura seu host para o GitHub Enterprise Server, um VPC endpoint para dados de eventos de webhooks é criado para você. Se você criou seu host antes de 24 de novembro de 2020 e deseja usar endpoints de PrivateLink webhook VPC, primeiro exclua seu host e depois crie um novo host.

Tópicos

Crie uma conexão com o GitHub Enterprise Server (console)

Para criar uma conexão com o GitHub Enterprise Server, você fornece informações sobre onde o GitHub Enterprise Server está instalado e autoriza a criação da conexão com suas credenciais GitHub Enterprise.

Tópicos

Crie sua conexão com o GitHub Enterprise Server (console)

Para criar uma conexão com o GitHub Enterprise Server, tenha o URL do servidor e as credenciais do GitHub Enterprise em mãos.

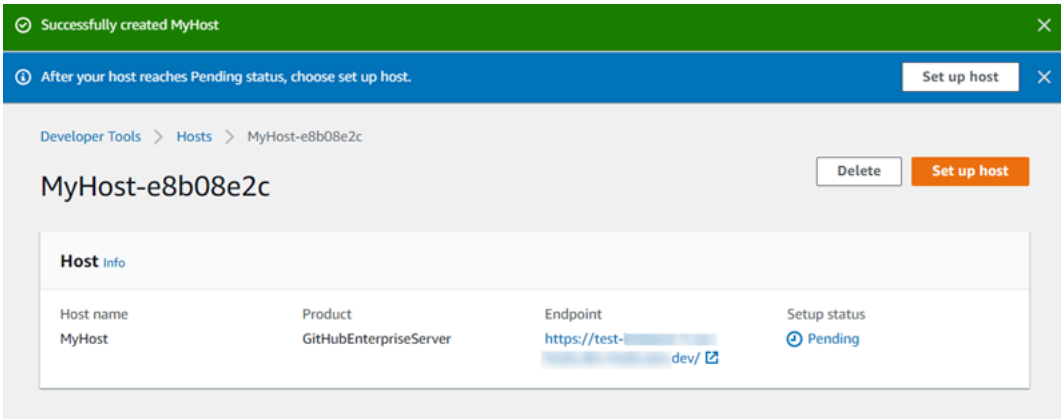
Para criar um host

1. Faça login no e abra AWS Management Console o console do AWS Developer Tools emhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Na guia Hosts, escolha Create host (Criar host).

3. Em Host name (Nome do host), insira o nome que deseja usar para o host.
4. Em Selecionar um provedor, escolha uma das seguintes opções:
   - GitHub Servidor corporativo
   - GitLab autogerenciado
5. Em URL, insira o endpoint da infraestrutura em que seu provedor está instalado.
6. Se seu servidor estiver configurado em uma Amazon VPC e você quiser se conectar com sua VPC, escolha Use a VPC (Usar uma VPC). Caso contrário, escolha No VPC.
7. Se você tiver iniciado sua instância em uma Amazon VPC e quiser se conectar à sua VPC, escolhaUse a VPC (Usar uma VPC) e conclua as operações a seguir.
   a. Em VPC ID (ID da VPC), escolha o ID da sua VPC. Escolha a VPC para a infraestrutura onde a instância está instalada ou uma VPC com acesso à instância por meio da VPN ou do Direct Connect.
   b. Se você tiver uma VPC privada configurada e tiver configurado a instância para executar a validação de TLS usando uma autoridade de certificação não pública, será necessário inserir o ID do certificado em Certificado TLS. O valor do certificado TLS é a chave pública do certificado.
8. Escolha Create host (Criar host).
9. Depois que a página de detalhes do host for exibida, o status do host será alterado quando o host for criado.

> **Note**
>
> Se a configuração do host incluir uma configuração de VPC, aguarde vários minutos pelo provisionamento de componentes de rede do host.

Aguarde até que seu host atinja um status Pending (Pendente) e, em seguida, conclua a configuração. Para ter mais informações, consulte Configurar um host pendente.

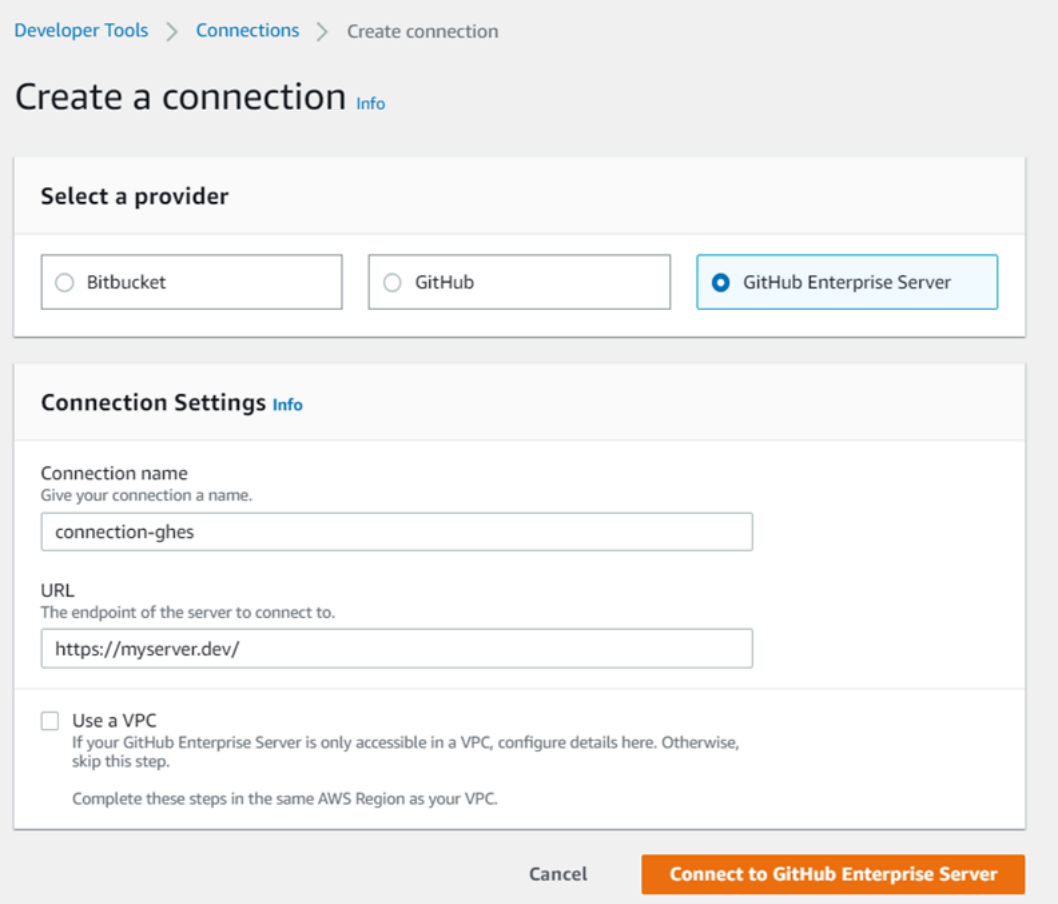


Etapa 2: Crie sua conexão com o GitHub Enterprise Server (console)

1. Faça login no AWS Management Console e abra o console do Developer Tools emhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Escolha Settings > Connections (Configurações > Conexões) e, em seguida, escolha Create connection (Criar conexão).
3. Para criar uma conexão com um repositório instalado do GitHub Enterprise Server, escolha GitHub Enterprise Server.

Conecte-se ao servidor GitHub corporativo

1. Em Connection name (Nome da conexão), informe um nome para a conexão.



2. Em URL, insira o endpoint do seu servidor.

> **Note**
>
> Se a URL fornecida já tiver sido usada para configurar um GitHub Enterprise Server para uma conexão, você será solicitado a escolher o ARN do recurso de host que foi criado anteriormente para esse endpoint.

3. (Opcional) Se você tiver iniciado o servidor em uma Amazon VPC e quiser se conectar à VPC, escolha Usar uma VPC e faça o indicado a seguir.

   a. Em VPC ID (ID da VPC), escolha o ID da sua VPC. Certifique-se de escolher a VPC para a infraestrutura em que sua instância do GitHub Enterprise Server está instalada ou uma VPC com acesso à sua instância do GitHub Enterprise Server por meio de VPN ou Direct Connect.

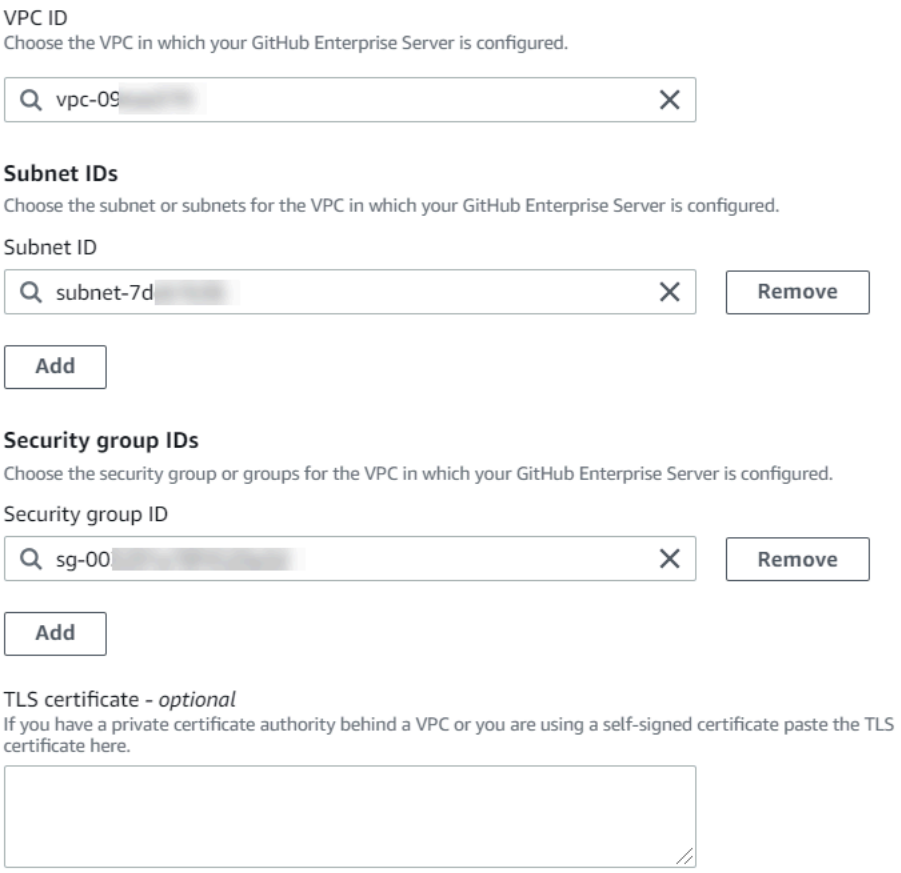
   b. Em Subnet ID (ID da sub-rede), escolha Add (Adicionar). No campo, escolha o ID da sub-rede que você deseja usar para seu host. Você pode escolher até 10 sub-redes.

Certifique-se de escolher a sub-rede para a infraestrutura em que sua instância do GitHub Enterprise Server está instalada ou uma sub-rede com acesso à sua instância instalada do GitHub Enterprise Server por meio de VPN ou Direct Connect.

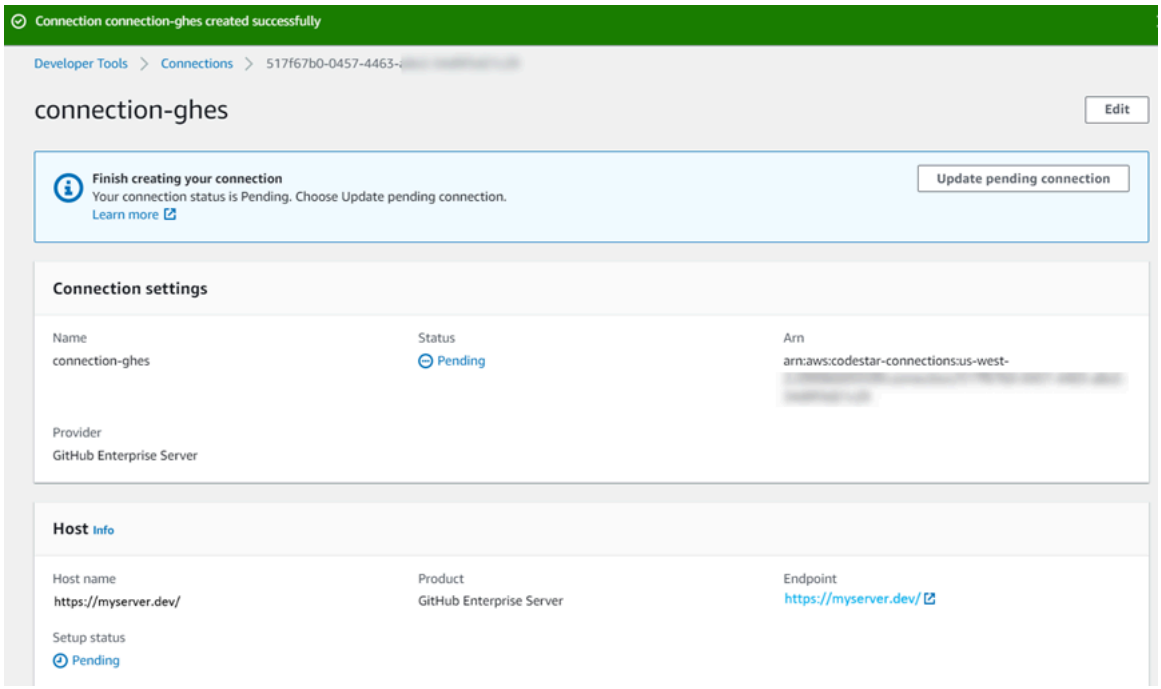
c. Em Security group IDs (IDs de grupos de segurança), escolha Add (Adicionar). No campo, escolha o grupo de segurança que você deseja usar para seu host. Você pode criar até 10 grupos de segurança.

   Certifique-se de escolher o grupo de segurança para a infraestrutura em que sua instância do GitHub Enterprise Server está instalada ou um grupo de segurança com acesso à sua instância instalada do GitHub Enterprise Server por meio de VPN ou Direct Connect.

d. Se você tiver uma VPC privada configurada e tiver configurado sua instância do GitHub Enterprise Server para realizar a validação de TLS usando uma autoridade de certificação não pública, em Certificado TLS, insira seu ID de certificado. O valor do certificado TLS deve ser a chave pública do certificado.

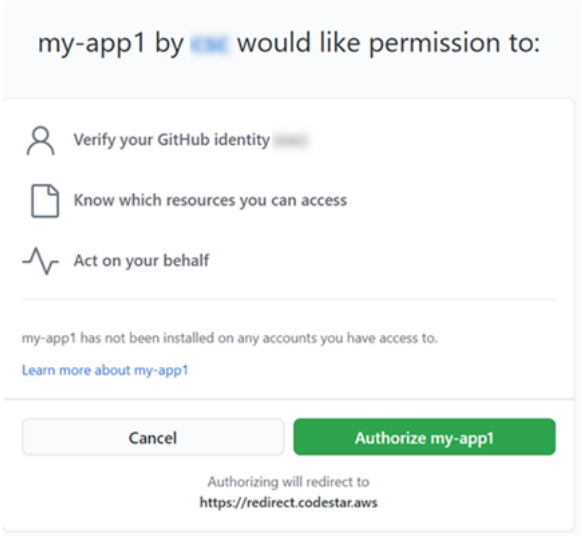


4. Escolha Connect to GitHub Enterprise Server. A conexão criada é mostrada com um status Pending (Pendente). Um recurso de host é criado para a conexão com as informações do servidor fornecidas. Para o nome do host, o URL é usado.
5. Selecione Update pending connection (Atualizar conexão pendente).



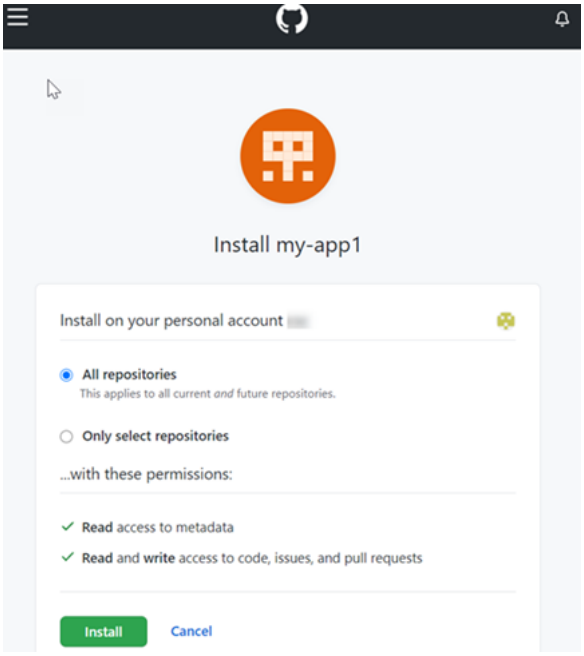
6. Se solicitado, na página de login do GitHub Enterprise, faça login com suas credenciais do GitHub Enterprise.
7. Na página Criar GitHub aplicativo, escolha um nome para seu aplicativo.

8. <app-name>Na página de GitHub autorização, escolha Autorizar.



9. Na página de instalação do aplicativo, uma mensagem mostra que o aplicativo AWS CodeStar Connector está pronto para ser instalado. Se você tiver várias organizações, poderá ser solicitado a escolher a organização onde deseja instalar a aplicação.

   Escolha as configurações do repositório em que deseja instalar a aplicação. Escolha Instalar.



10. A página de conexão mostra a conexão criada em um status Available (Disponível).

Crie uma conexão com o GitHub Enterprise Server (CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para criar uma conexão.

Para fazer isso, use os comandos create-host e create-connection.

> **Important**
>
> Uma conexão criada por meio do AWS CLI ou AWS CloudFormation está no `PENDING` status por padrão. Depois de criar uma conexão com a CLI ou AWS CloudFormation, use o console para editar a conexão e definir seu status. `AVAILABLE`

Etapa 1: Para criar um host para o GitHub Enterprise Server (CLI)

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o create-host comando, especificando o `--name` `--provider-type`, e `--provider-endpoint` para sua conexão. Neste exemplo, o nome do provedor de terceiros é `GitHubEnterpriseServer` e o endpoint é `my-instance.dev`.

```
aws codestar-connections create-host --name MyHost --provider-type
 GitHubEnterpriseServer --provider-endpoint "https://my-instance.dev"
```

Se o comando for bem-sucedido, ele retornará as informações de nome do recurso da Amazon (ARN) do host semelhantes às mostradas a seguir.

```
{
    "HostArn": "arn:aws:codestar-connections:us-west-2:account_id:host/My-
Host-28aef605"
}
```

Após esta etapa, o host estará no status `PENDING`.

2. Use o console para concluir a configuração do host e mova o host para um status `Available`. Para ter mais informações, consulte Configurar um host pendente.

Etapa 2: configurar um host pendente no console

1. Faça login no AWS Management Console e abra o console do Developer Tools emhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Use o console para concluir a configuração do host e mova o host para um status `Available`. Consulte Configurar um host pendente.

Etapa 3: Para criar uma conexão para o GitHub Enterprise Server (CLI)

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o create-connection comando, especificando `--host-arn` e `--connection-name` para sua conexão.

```
aws codestar-connections create-connection --host-arn arn:aws:codestar-
connections:us-west-2:account_id:host/MyHost-234EXAMPLE --connection-name
 MyConnection
```

Se tiver êxito, esse comando gerará as informações do ARN de conexão semelhantes às seguintes.

```
{
    "ConnectionArn": "arn:aws:codestar-connections:us-west-2:account_id:connection/
aEXAMPLE-8aad"
}
```

2. Use o console para configurar a conexão pendente. Para ter mais informações, consulte Atualizar uma conexão pendente.

Etapa 4: Para concluir uma conexão para o GitHub Enterprise Server no console

1. Faça login no AWS Management Console e abra o console do Developer Tools emhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Use o console para configurar a conexão pendente e mover a conexão para um status de `Available`. Para ter mais informações, consulte Atualizar uma conexão pendente.

Crie uma conexão com GitLab

Você pode usar o AWS Management Console ou o AWS Command Line Interface (AWS CLI) para criar uma conexão com um repositório hospedado em gitlab.com.

> **Note**
>
> Ao autorizar a instalação dessa conexão GitLab, você concede ao nosso serviço permissões para processar seus dados e pode revogar as permissões a qualquer momento desinstalando o aplicativo.

Antes de começar

- Você já deve ter criado uma conta com GitLab.

> **Note**
>
> As conexões fornecem acesso à conta usada para criar e autorizar a conexão.

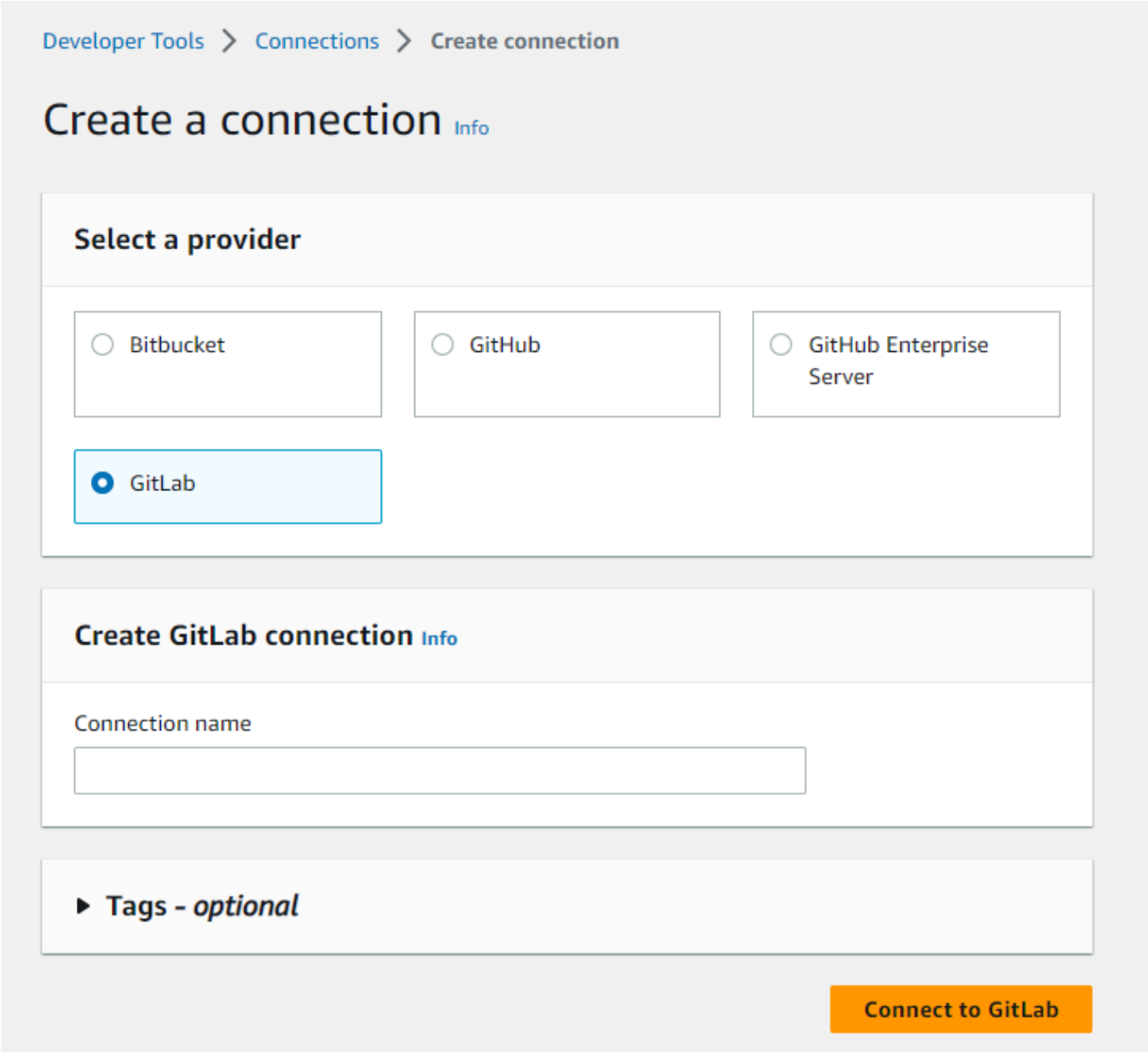
> **Note**
>
> Você pode criar conexões nas quais você tem a função de Proprietário e GitLab, em seguida, a conexão pode ser usada com o repositório com recursos como CodePipeline. Para repositórios em grupos, você não precisa ser o proprietário do grupo.

Tópicos

Crie uma conexão com GitLab (console)

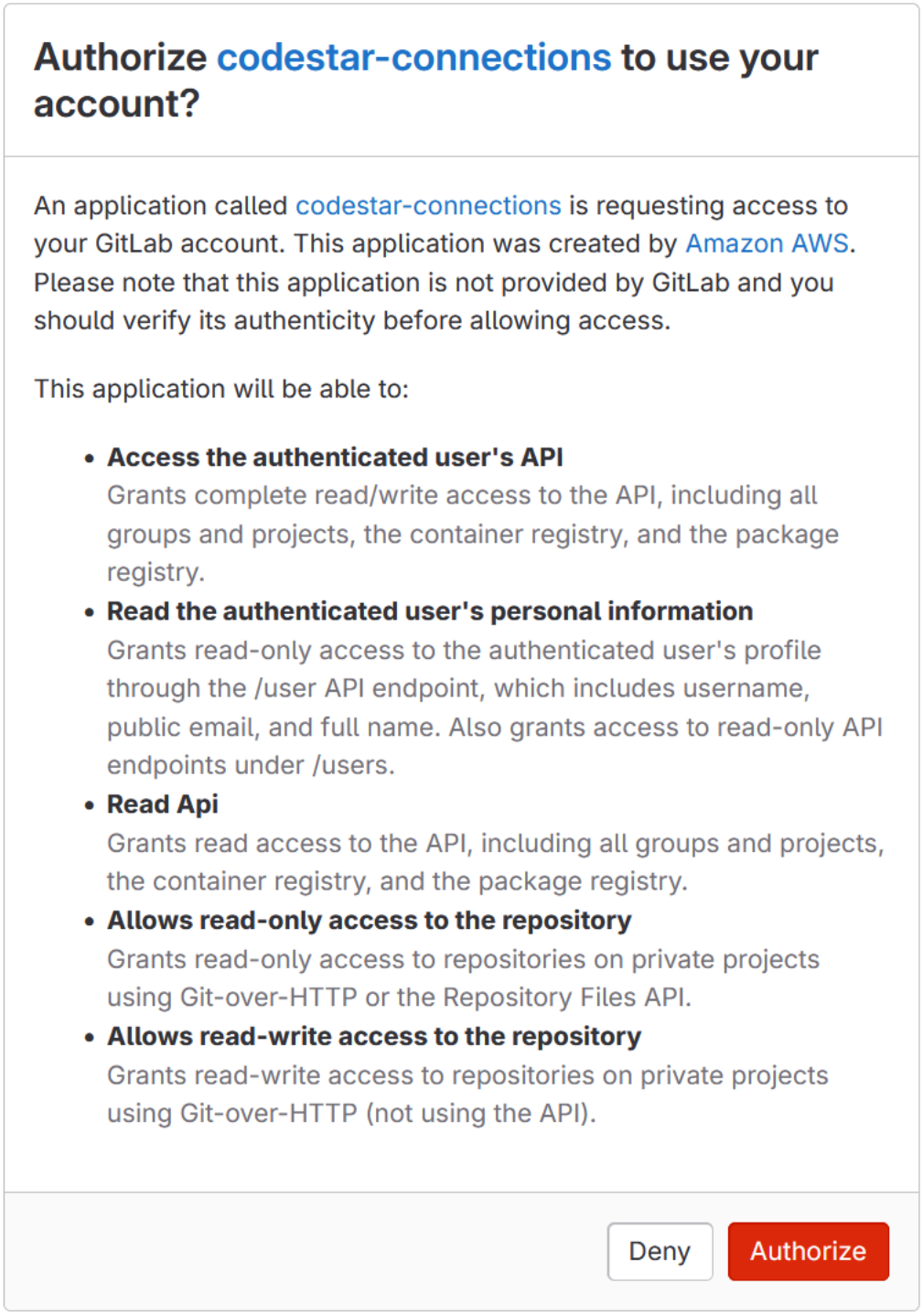
Etapa 1: criar uma conexão

1. Faça login no e AWS Management Console, em seguida, abra o console do AWS Developer Tools emhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Selecione Configurações > Conexões e escolha Conexões. Escolha Criar conexão.
3. Para criar uma conexão com um GitLab repositório, em Selecionar um provedor, escolha GitLab. Em Connection name (Nome da conexão), digite o nome da conexão que você deseja criar. Escolha Connect to GitLab.



4. Quando a página de login for GitLab exibida, faça login com suas credenciais e escolha Entrar.
5. Uma página de autorização é exibida com uma mensagem solicitando autorização para a conexão acessar sua GitLab conta.

   Escolha Authorize.



6. O navegador retorna à página do console de conexões. Em Criar GitLab conexão, a nova conexão é mostrada em Nome da conexão.
7. Escolha Connect to GitLab.

Depois que a conexão for criada com êxito, um banner de êxito será exibido. Os detalhes da conexão são mostrados na página Configurações da conexão.

Crie uma conexão com GitLab (CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para criar uma conexão.

Para fazer isso, use o comando create-connection.

> **Important**
>
> Uma conexão criada por meio do AWS CLI ou AWS CloudFormation está no `PENDING` status por padrão. Depois de criar uma conexão com a CLI ou AWS CloudFormation, use o console para editar a conexão e definir seu status. `AVAILABLE`

Para criar uma conexão com GitLab

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o create-connection comando, especificando `--provider-type` e `--connection-name` para sua conexão. Neste exemplo, o nome do provedor de terceiros é `GitLab` e o nome da conexão especificada é `MyConnection`.

   ```
   aws codestar-connections create-connection --provider-type GitLab --connection-name
    MyConnection
   ```

   Se tiver êxito, esse comando gerará as informações do ARN de conexão semelhantes às seguintes.

   ```
   {
       "ConnectionArn": "arn:aws:codestar-connections:us-west-2:account_id:connection/
   aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f"
   }
   ```

2. Use o console para concluir a conexão. Para ter mais informações, consulte Atualizar uma conexão pendente.

Crie uma conexão com o GitLab autogerenciado

Você pode criar conexões para GitLab Enterprise Edition ou GitLab Community Edition com uma instalação autogerenciada.

Você pode usar o AWS Management Console ou o AWS Command Line Interface (AWS CLI) para criar uma conexão e um host para GitLab autogerenciamento.

> **Note**
>
> Ao autorizar esse aplicativo de conexão como GitLab autogerenciado, você concede ao nosso serviço permissões para processar seus dados e pode revogar as permissões a qualquer momento desinstalando o aplicativo.

Antes de criar uma conexão GitLab autogerenciada, você deve criar um host para usar na conexão, conforme detalhado nessas etapas. Consulte uma visão geral do fluxo de trabalho de criação de host para provedores instalados em Fluxo de trabalho para criar ou atualizar um host.

Se preferir, você poderá configurar o host com uma VPC. Consulte mais informações sobre a configuração de rede e VPC para o recurso de host nos pré-requisitos da VPC em (Opcional) Pré-requisitos: configuração de rede ou da Amazon VPC para sua conexão e Solução de problemas de configuração da VPC para seu host.

Antes de começar

- Você já deve ter criado uma conta GitLab e ter a GitLab Enterprise Edition ou a GitLab Community Edition com uma instalação autogerenciada. Consulte mais informações em https://docs.gitlab.com/ee/subscriptions/self_managed/.

  > **Note**
  >
  > As conexões fornecem acesso à conta usada para criar e autorizar a conexão.

> **Note**
>
> Você pode criar conexões com um repositório no qual você tem a função de Proprietário e GitLab, em seguida, a conexão pode ser usada com recursos como CodePipeline. Para repositórios em grupos, você não precisa ser o proprietário do grupo.

- Você já deve ter criado um token de acesso GitLab pessoal (PAT) somente com a seguinte permissão reduzida: api. Consulte mais informações em https://docs.gitlab.com/ee/user/profile/personal_access_tokens.html. Somente o PAT usado por um administrador pode ser usado.

> **Note**
>
> O PAT é usado para autorizar o host e não é armazenado ou usado pelas conexões. Para configurar um host, é possível criar um PAT temporário e, depois de configurar o host, você pode excluir o PAT.

Tópicos

Crie uma conexão com o GitLab autogerenciado (console)

Use essas etapas para criar um host e uma conexão GitLab autogerenciada no console. Consulte considerações sobre a configuração de um host em uma VPC em (Opcional) Pré-requisitos: configuração de rede ou da Amazon VPC para sua conexão.

> **Note**
>
> Você cria um host para uma única instalação GitLab autogerenciada e, em seguida, pode gerenciar uma ou mais conexões GitLab autogerenciadas com esse host.

Etapa 1: criar o host

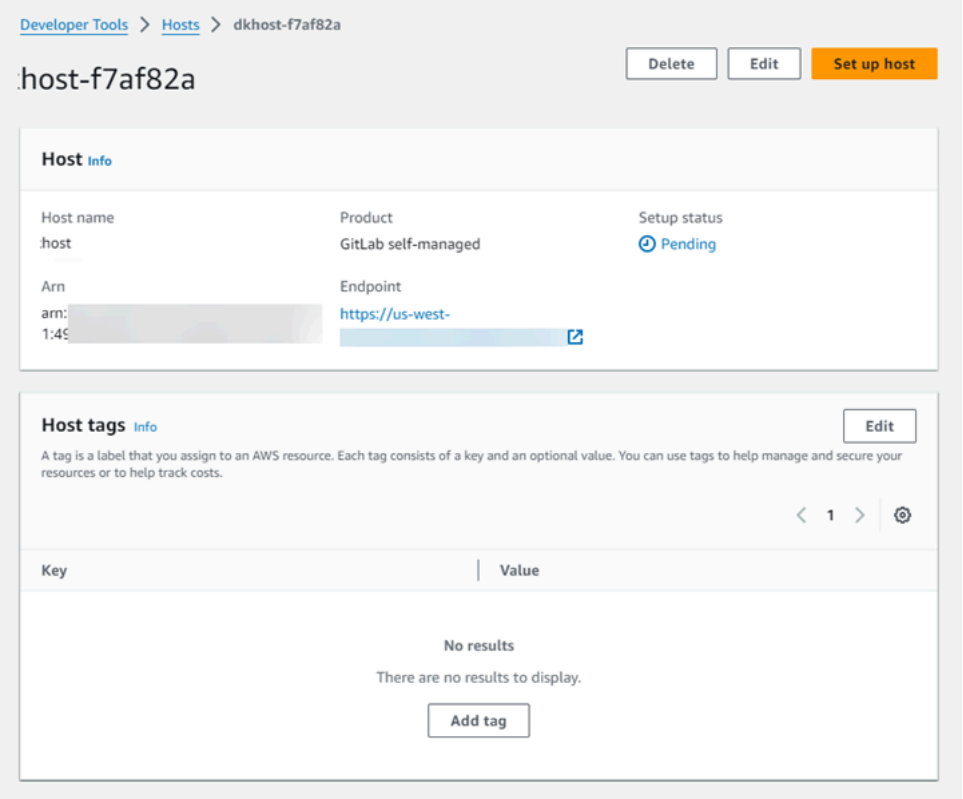
1. Faça login no e AWS Management Console, em seguida, abra o console do AWS Developer Tools emhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Na guia Hosts, escolha Create host (Criar host).
3. Em Host name (Nome do host), insira o nome que deseja usar para o host.
4. Em Selecionar um provedor, escolha GitLabautogerenciado.
5. Em URL, insira o endpoint da infraestrutura em que seu provedor está instalado.
6. Se seu servidor estiver configurado em uma Amazon VPC e você quiser se conectar com sua VPC, escolha Use a VPC (Usar uma VPC). Caso contrário, escolha No VPC.
7. (Opcional) Se você tiver iniciado o host em uma Amazon VPC e quiser se conectar à VPC, escolha Usar uma VPC e faça o indicado a seguir.

   a. Em VPC ID (ID da VPC), escolha o ID da sua VPC. Escolha a VPC para a infraestrutura onde o host está instalado ou uma VPC com acesso à instância por meio da VPN ou do Direct Connect.

   b. Se você tiver uma VPC privada configurada e tiver configurado o host para executar a validação de TLS usando uma autoridade de certificação não pública, será necessário inserir o ID do certificado em Certificado TLS. O valor do certificado TLS é a chave pública do certificado.
8. Escolha Create host (Criar host).
9. Depois que a página de detalhes do host for exibida, o status do host será alterado quando o host for criado.

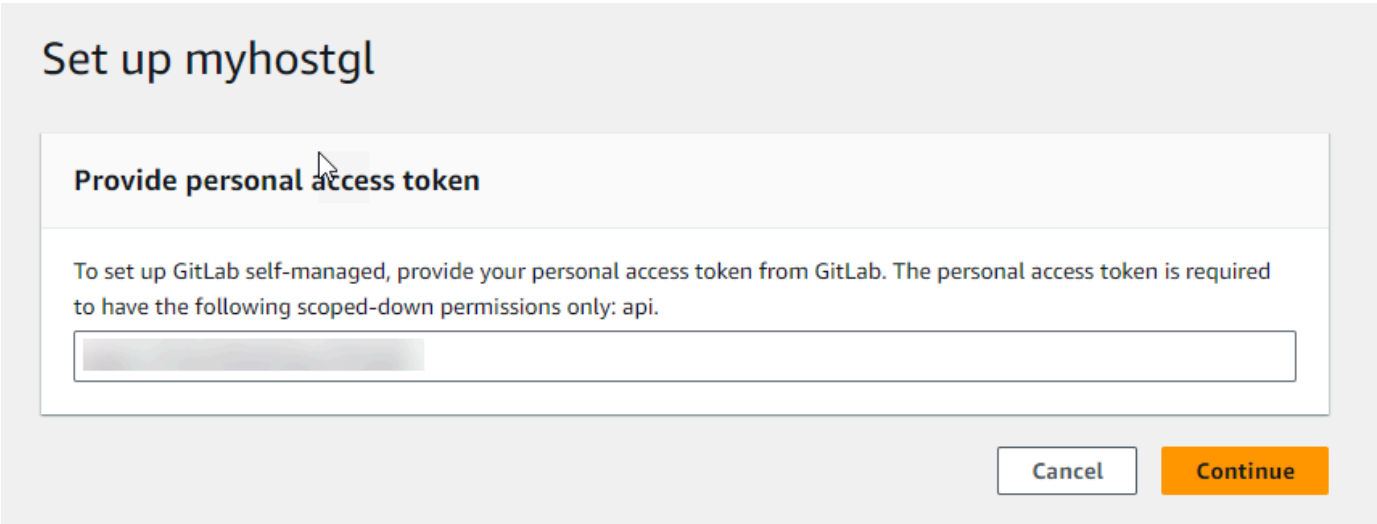
> **Note**
>
> Se a configuração do host incluir uma configuração de VPC, aguarde vários minutos pelo provisionamento de componentes de rede do host.

Aguarde até que seu host atinja um status Pending (Pendente) e, em seguida, conclua a configuração. Para ter mais informações, consulte Configurar um host pendente.

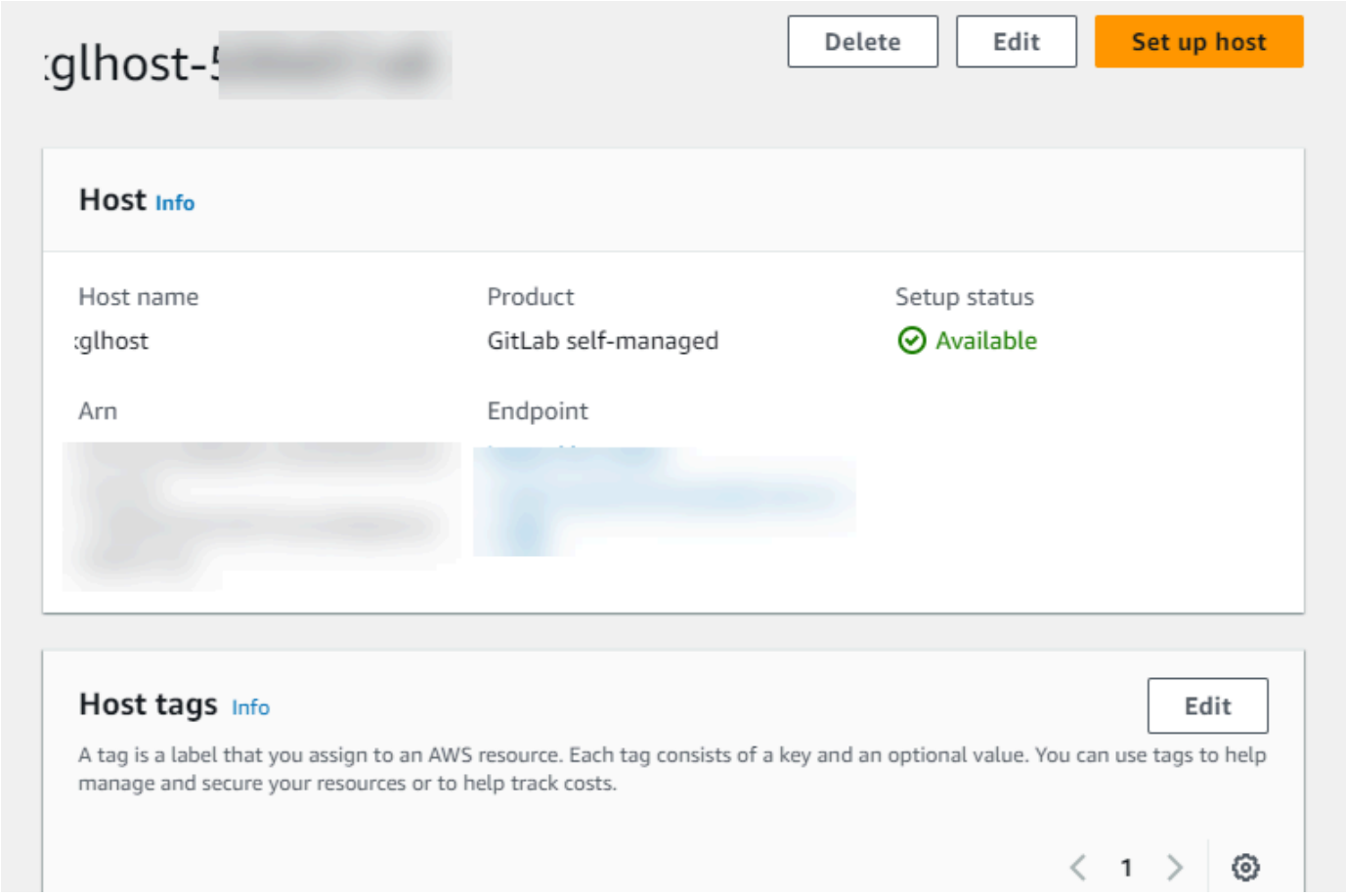


Etapa 2: configurar o host pendente

1. Escolha Configurar host.
2. Uma página Configurar ***host_name*** é exibida. Em Fornecer token de acesso pessoal, forneça GitLab ao PAT somente a seguinte permissão com escopo reduzido: api.

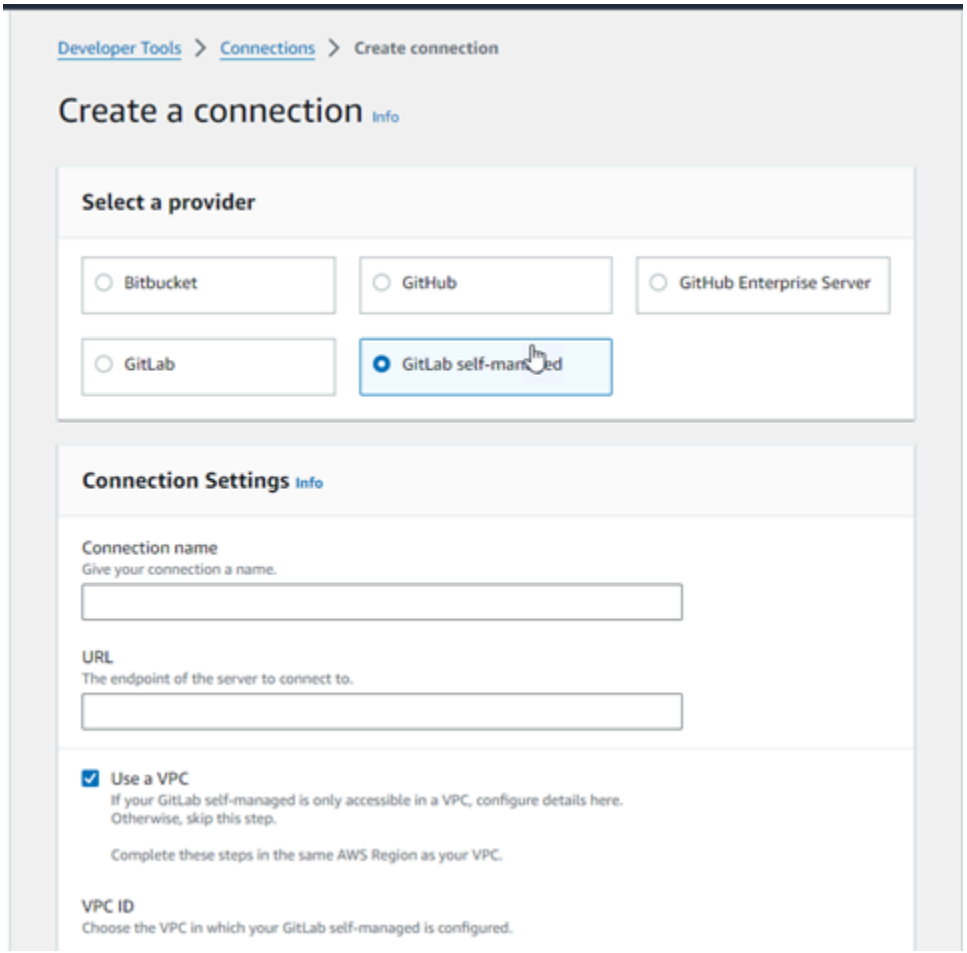


3. Depois que o host for registrado com êxito, a página de detalhes do host será exibida e mostrará que o status do host é Available (Disponível).



Etapa 3: criar uma conexão

1. Faça login no e AWS Management Console, em seguida, abra o console do AWS Developer Tools emhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Selecione Configurações > Conexões e escolha Conexões. Escolha Criar conexão.
3. Para criar uma conexão com um GitLab repositório, em Selecionar um provedor, escolha GitLab autogerenciado. Em Connection name (Nome da conexão), digite o nome da conexão que você deseja criar.



4. Em URL, insira o endpoint do seu servidor.
5. Se você tiver iniciado seu servidor em uma Amazon VPC e quiser se conectar à sua VPC, escolhaUse a VPC (Usar uma VPC) e conclua as operações a seguir.

   a. Em VPC ID (ID da VPC), escolha o ID da sua VPC. Escolha a VPC para a infraestrutura onde o host está instalado ou uma VPC com acesso ao host por meio da VPN ou do Direct Connect.

   b. Em Subnet ID (ID da sub-rede), escolha Add (Adicionar). No campo, escolha o ID da sub-rede que você deseja usar para seu host. Você pode escolher até 10 sub-redes.

      Escolha a sub-rede para a infraestrutura onde o host está instalado ou uma sub-rede com acesso ao host instalado por meio da VPN ou do Direct Connect.

   c. Em Security group IDs (IDs de grupos de segurança), escolha Add (Adicionar). No campo, escolha o grupo de segurança que você deseja usar para seu host. Você pode criar até 10 grupos de segurança.

Escolha o grupo de segurança para a infraestrutura onde o host está instalado ou um grupo de segurança com acesso ao host instalado por meio da VPN ou do Direct Connect.

d. Se você tiver uma VPC privada configurada e tiver configurado o host para executar a validação de TLS usando uma autoridade de certificação não pública, será necessário inserir o ID do certificado em Certificado TLS. O valor do certificado TLS deve ser a chave pública do certificado.

6. Escolha Conectar ao GitLab autogerenciado. A conexão criada é mostrada com um status Pending (Pendente). Um recurso de host é criado para a conexão com as informações do servidor fornecidas. Para o nome do host, o URL é usado.
7. Selecione Update pending connection (Atualizar conexão pendente).
8. Quando a página de login for GitLab exibida, faça login com suas credenciais e escolha Entrar.
9. Uma página de autorização é exibida com uma mensagem solicitando autorização para a conexão acessar sua GitLab conta.

   Escolha Authorize.
10. O navegador retorna à página do console de conexões. Em Criar GitLab conexão, a nova conexão é mostrada em Nome da conexão.
11. Escolha Conectar ao GitLab autogerenciado.

    Depois que a conexão for criada com êxito, um banner de êxito será exibido. Os detalhes da conexão são mostrados na página Configurações da conexão.

Crie uma conexão com o GitLab autogerenciado (CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para criar um host e uma conexão GitLab autogerenciados.

Para fazer isso, use os comandos create-host e create-connection.

> **Important**
>
> Uma conexão criada por meio do AWS CLI ou AWS CloudFormation está no `PENDING` status por padrão. Depois de criar uma conexão com a CLI ou AWS CloudFormation, use o console para editar a conexão e definir seu status. `AVAILABLE`

Etapa 1: Para criar um host para GitLab autogerenciamento (CLI)

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o create-host comando, especificando o `--name`--`provider-type`, e `--provider-endpoint` para sua conexão. Neste exemplo, o nome do provedor de terceiros é `GitLabSelfManaged` e o endpoint é `my-instance.dev`.

   ```
   aws codestar-connections create-host --name MyHost --provider-type
    GitLabSelfManaged --provider-endpoint "https://my-instance.dev"
   ```

   Se o comando for bem-sucedido, ele retornará as informações de nome do recurso da Amazon (ARN) do host semelhantes às mostradas a seguir.

   ```
   {
       "HostArn": "arn:aws:codestar-connections:us-west-2:account_id:host/My-
   Host-28aef605"
   }
   ```

   Após esta etapa, o host estará no status `PENDING`.

2. Use o console para concluir a configuração do host e mova o host para um status de `Available` na etapa a seguir.

Etapa 2: configurar um host pendente no console

1. Faça login no AWS Management Console e abra o console do Developer Tools emhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Use o console para concluir a configuração do host e mova o host para um status `Available`. Consulte Configurar um host pendente.

Etapa 3: Para criar uma conexão GitLab autogerenciada (CLI)

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o create-connection comando, especificando `--host-arn` e `--connection-name` para sua conexão.

```
aws codestar-connections create-connection --host-arn arn:aws:codestar-
connections:us-west-2:account_id:host/MyHost-234EXAMPLE --connection-name
 MyConnection
```

Se tiver êxito, esse comando gerará as informações do ARN de conexão semelhantes às seguintes.

```
{
    "ConnectionArn": "arn:aws:codestar-connections:us-west-2:account_id:connection/
aEXAMPLE-8aad"
}
```

2. Use o console para configurar a conexão pendente na etapa a seguir.

Etapa 4: Para concluir uma conexão GitLab autogerenciada no console

1. Faça login no AWS Management Console e abra o console do Developer Tools emhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Use o console para configurar a conexão pendente e mover a conexão para um status de `Available`. Para ter mais informações, consulte Atualizar uma conexão pendente.

Atualizar uma conexão pendente

Uma conexão criada por meio do AWS Command Line Interface (AWS CLI) ou AWS CloudFormation está no `PENDING` status por padrão. Depois de criar uma conexão com o AWS CLI ou AWS CloudFormation, use o console para atualizar a conexão e definir seu status`AVAILABLE`.

> **Note**
>
> É necessário usar o console para atualizar uma conexão pendente. Não é possível atualizar uma conexão pendente usando o AWS CLI.

Na primeira vez que o console for usado para adicionar uma nova conexão a um provedor de terceiros, será necessário concluir o handshake OAuth com o provedor de terceiros usando a instalação associada à conexão.

É possível usar o console do Developer Tools para concluir uma conexão pendente.

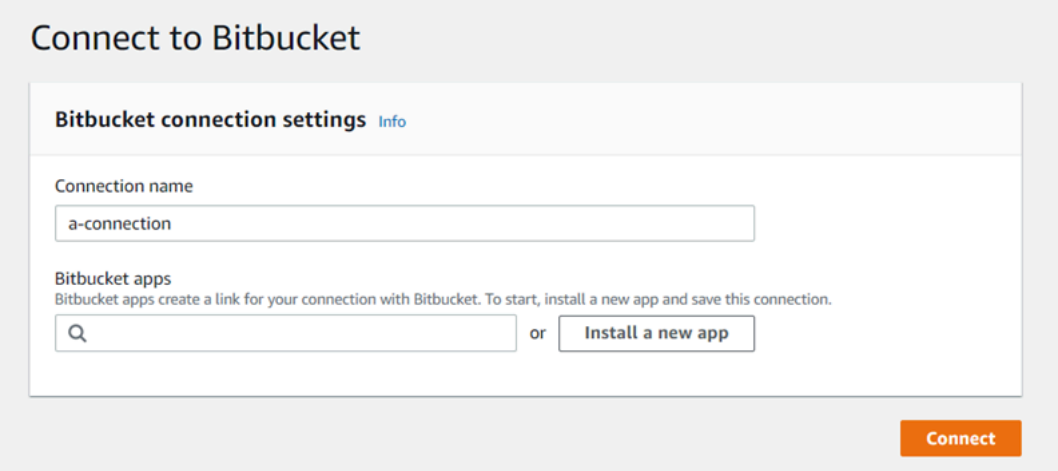
Como concluir uma conexão

1. Abra o console do AWS Developer Tools emhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Escolha Settings > Connections (Configurações > Conexão).

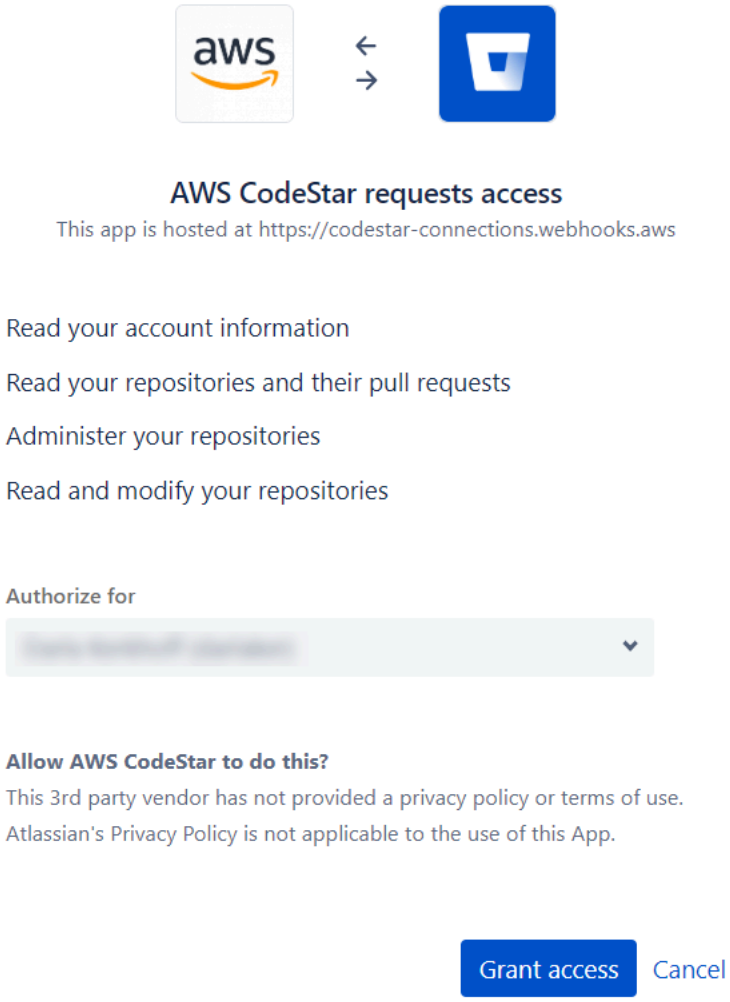
   Os nomes de todas as conexões associadas à sua AWS conta são exibidos.
3. Em Nome, escolha o nome da conexão pendente a ser atualizado.

   A opção Update a pending connection (Atualizar uma conexão pendente) é habilitada quando uma conexão é escolhida com o status Pending (Pendente).
4. Escolha Update a pending connection (Atualizar uma conexão pendente).
5. Na página Connect to Bitbucket (Conectar ao Bitbucket), em Connection name (Nome da conexão), verifique o nome da sua conexão.

   Em Bitbucket apps (Aplicações do Bitbucket), escolha uma instalação de aplicação ou Install a new app (Instalar uma nova aplicação) para criar uma.



6. Na página de instalação do aplicativo, uma mensagem mostra que o AWS CodeStar aplicativo está tentando se conectar à sua conta do Bitbucket. Escolha Conceder acesso.



7. O ID de conexão para sua nova instalação é exibido. Escolha Complete connection (Conexão completa).

Listar Conexões

É possível usar o console do Developer Tools ou o comando list-connections na AWS Command Line Interface (AWS CLI) para visualizar uma lista de conexões na conta.

Listar conexões (console)

Para listar conexões

1. Abra o console do Developer Tools em https://console.aws.amazon.com/codesuite/settings/connections.
2. Escolha Settings > Connections (Configurações > Conexão).

3. Visualize o nome, o status e o ARN das conexões.

Listar conexões (CLI)

Você pode usar o AWS CLI para listar suas conexões com repositórios de código de terceiros. Para uma conexão associada a um recurso do host, como conexões com o GitHub Enterprise Server, a saída também retorna o ARN do host.

Para fazer isso, use o comando list-connections.

Para listar conexões

- Abra um terminal (Linux, macOS ou Unix) ou prompt de comando (Windows) e use o AWS CLI para executar o comando. list-connections

```
aws codestar-connections list-connections --provider-type Bitbucket
--max-results 5 --next-token: next-token
```

Este comando retorna a seguinte saída.

```
{
     "Connections": [
         {
             "ConnectionName": "my-connection",
             "ProviderType": "Bitbucket",
             "Status": "PENDING",
             "ARN": "arn:aws:codestar-connections:us-west-2:account_id:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
             "OwnerAccountId": "account_id"
         },
         {
             "ConnectionName": "my-other-connection",
             "ProviderType": "Bitbucket",
             "Status": "AVAILABLE",
             "ARN": "arn:aws:codestar-connections:us-west-2:account_id:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
             "OwnerAccountId": "account_id"
          },
      ],
     "NextToken": "next-token"
}
```

Excluir uma conexão

É possível usar o console do Developer Tools ou o comando delete-connection na AWS Command Line Interface (AWS CLI) para excluir uma conexão.

Tópicos

Excluir uma conexão (console)

Excluir uma conexão

1. Abra o console do Developer Tools em https://console.aws.amazon.com/codesuite/settings/connections.
2. Escolha Settings > Connections (Configurações > Conexão).
3. Em Nome da conexão, escolha o nome da conexão a ser excluída.
4. Escolha Delete.
5. Digite **`delete`** no campo para confirmar e escolha Excluir.

> **Important**
>
> Esta ação não pode ser desfeita.

Excluir uma conexão (CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para excluir uma conexão.

Para fazer isso, use o comando delete-connection.

> **Important**
>
> Após a execução do comando, a conexão é excluída. Nenhuma caixa de diálogo de confirmação é exibida. É possível criar uma nova conexão, mas o Nome de recurso da Amazon (ARN) nunca é reutilizado.

Excluir uma conexão

- Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o delete-connection comando, especificando o ARN da conexão que você deseja excluir.

  ```
  aws codestar-connections delete-connection --connection-arn arn:aws:codestar-connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f
  ```

  Esse comando não retorna nada.

Recursos de conexões de tags

Uma tag é um rótulo de atributo personalizado que você atribui ou AWS atribui a um AWS recurso. Cada AWS tag tem duas partes:

- Uma chave de tag (por exemplo `CostCenter`, `Environment` ou `Project`). Chaves de 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 chaves de tag, os valores das tags diferenciam maiúsculas de minúsculas.

Juntos, são conhecidos como pares de chave/valor.

Você pode usar o console ou a CLI para marcar recursos.

É possível marcar os seguintes tipos de recursos no CodeConnections:

- Conexões
- Hosts

Essas etapas pressupõem que você já tenha instalado uma versão recente do AWS CLI ou atualizado para a versão atual. Para obter mais informações, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface .

Além de identificar, organizar e rastrear seu recurso com tags, você pode usar tags nas políticas AWS Identity and Access Management (IAM) para ajudar a controlar quem pode visualizar e interagir

com seu recurso. Para obter exemplos de políticas de acesso baseadas em tags, consulte Usando tags para controlar o acesso aos recursos do AWS CodeStar Connections.

Tópicos

- Marcar recursos (console)
- Recursos de tag (CLI)

Marcar recursos (console)

É possível usar o console para adicionar, atualizar ou remover tags em um recurso de conexões.

Tópicos

- Adicionar tags a um recurso de conexões (console)
- Visualizar tags para um recurso de conexões (console)
- Editar tags para um recurso de conexões (console)
- Remover tags de um recurso de conexões (console)

Adicionar tags a um recurso de conexões (console)

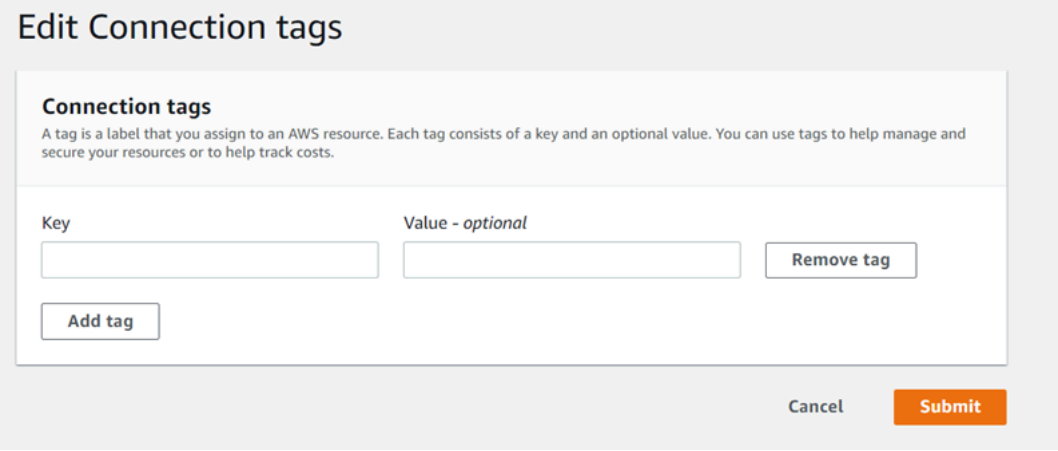
Você pode usar o console para adicionar tags a uma conexão ou a um host existente.

> **Note**
>
> Quando você cria uma conexão para um provedor instalado, como o GitHub Enterprise Server, e um recurso de host também é criado para você, as tags durante a criação são adicionadas somente à conexão. Isso permite que você marque um host separadamente se quiser reutilizá-lo para uma nova conexão. Se quiser adicionar tags ao host, use as etapas aqui.

Para adicionar etiquetas a uma conexão

1. Faça login no console do . No painel de navegação, escolha Settings (Configurações).
2. Em Settings (Configurações), escolha Connections (Conexões). Escolha a guia Connections (Conexões).
3. Escolha a conexão que deseja editar. A página de configurações de conexão é exibida.

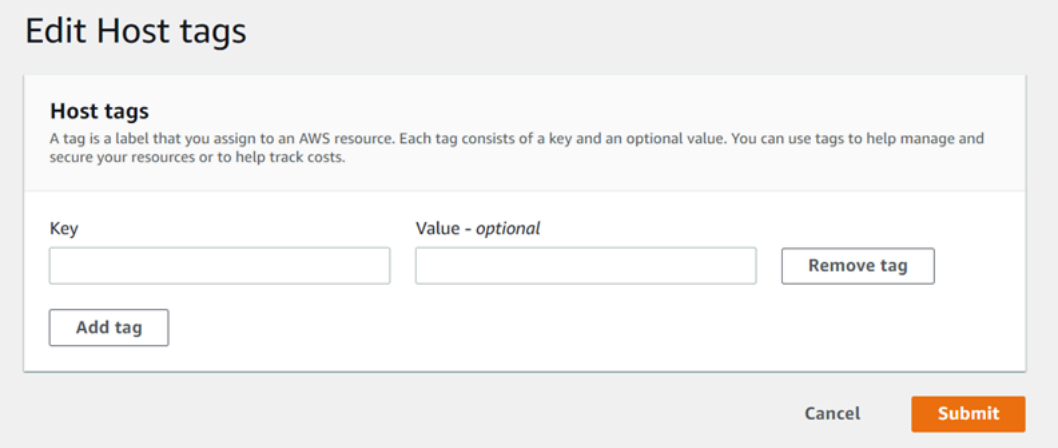
4. Em Connection tags (Tags da conexão), escolha Edit (Editar). A página Edit Connection tags (Editar tags da conexão) é exibida.
5. Nos campos Key (Chave) e Value (Valor), insira um par de chaves para cada conjunto de tags que você deseja adicionar. (O campo Value (Valor) é opcional.) Por exemplo, em Key (Chave), insira **`Project`**. Em Valor, informe **`ProjectA`**.



6. (Opcional) Escolha Add tag (Adicionar tag) para adicionar mais linhas e inserir mais tags.
7. Selecione Enviar. As tags são listadas em configurações da conexão.

Para adicionar etiquetas a um host

1. Faça login no console do . No painel de navegação, escolha Settings (Configurações).
2. Em Settings (Configurações), escolha Connections (Conexões). Escolha a guia Hosts.
3. Selecione o host que deseja editar. A página de configurações do host é exibida.
4. Em Host tags (Tags do host), escolha Edit (Editar). A página Host tags (Tags do host) é exibida.
5. Nos campos Key (Chave) e Value (Valor), insira um par de chaves para cada conjunto de tags que você deseja adicionar. (O campo Value (Valor) é opcional.) Por exemplo, em Key (Chave), insira **`Project`**. Em Valor, informe **`ProjectA`**.



6. (Opcional) Escolha Add tag (Adicionar tag) para adicionar mais linhas e inserir mais tags para um host.
7. Selecione Enviar. As tags são listadas nas configurações do host.

Visualizar tags para um recurso de conexões (console)

Você pode usar o console para visualizar as tags para recursos existentes.

Para visualizar etiquetas de uma conexão

1. Faça login no console do . No painel de navegação, escolha Settings (Configurações).
2. Em Settings (Configurações), escolha Connections (Conexões). Escolha a guia Connections (Conexões).
3. Escolha a conexão que deseja visualizar. A página de configurações de conexão é exibida.
4. Em Connection tags (Tags da conexão), visualize as tags para a conexão nas colunas Key (Chave) e Value (Valor).

Para visualizar etiquetas de um host

1. Faça login no console do . No painel de navegação, escolha Settings (Configurações).
2. Em Settings (Configurações), escolha Connections (Conexões). Escolha a guia Hosts.
3. Escolha o host que deseja visualizar.
4. Em Host tags (Tags do host), visualize as tags para o host nas colunas Key (Chave) e Value (Valor).

Editar tags para um recurso de conexões (console)

Você pode usar o console para editar tags que foram adicionadas a recursos de conexões.

Para editar etiquetas de uma conexão

1. Faça login no console do . No painel de navegação, escolha Settings (Configurações).
2. Em Settings (Configurações), escolha Connections (Conexões). Escolha a guia Connections (Conexões).
3. Escolha a conexão que deseja editar. A página de configurações de conexão é exibida.
4. Em Connection tags (Tags da conexão), escolha Edit (Editar). A página Connection tags (Tags da conexão) é exibida.
5. Nos campos Key (Chave) e Value (Valor), atualize os valores em cada campo conforme necessário. Por exemplo, para a chave **`Project`**, em Value (Valor), altere **`ProjectA`** para **`ProjectB`**.
6. Selecione Enviar.

Para editar etiquetas de um host

1. Faça login no console do . No painel de navegação, escolha Settings (Configurações).
2. Em Settings (Configurações), escolha Connections (Conexões). Escolha a guia Hosts.
3. Selecione o host que deseja editar. A página de configurações do host é exibida.
4. Em Host tags (Tags do host), escolha Edit (Editar). A página Host tags (Tags do host) é exibida.
5. Nos campos Key (Chave) e Value (Valor), atualize os valores em cada campo conforme necessário. Por exemplo, para a chave **`Project`**, em Value (Valor), altere **`ProjectA`** para **`ProjectB`**.
6. Selecione Enviar.

Remover tags de um recurso de conexões (console)

Você pode usar o console para remover tags de recursos de conexão. Ao remover tags do recurso associado, as tags são excluídas.

Para remover etiquetas de uma conexão

1. Faça login no console do . No painel de navegação, escolha Settings (Configurações).

2. Em Settings (Configurações), escolha Connections (Conexões). Escolha a guia Connections (Conexões).
3. Escolha a conexão que deseja editar. A página de configurações de conexão é exibida.
4. Em Connection tags (Tags da conexão), escolha Edit (Editar). A página Connection tags (Tags da conexão) é exibida.
5. Ao lado da chave e do valor para cada tag que você deseja excluir, escolha Remove tag (Remover tag).
6. Selecione Enviar.

Para remover etiquetas de um host

1. Faça login no console do . No painel de navegação, escolha Settings (Configurações).
2. Em Settings (Configurações), escolha Connections (Conexões). Escolha a guia Hosts.
3. Selecione o host que deseja editar. A página de configurações do host é exibida.
4. Em Host tags (Tags do host), escolha Edit (Editar). A página Host tags (Tags do host) é exibida.
5. Ao lado da chave e do valor para cada tag que você deseja excluir, escolha Remove tag (Remover tag).
6. Selecione Enviar.

Recursos de tag (CLI)

É possível usar a CLI para adicionar, atualizar ou remover tags em um recurso de conexões.

Tópicos

- Adicionar tags a um recurso de conexões (CLI)
- Visualizar tags para um recurso de conexões (CLI)
- Editar tags para um recurso de conexões (CLI)
- Remover tags de um recurso de conexões (CLI)

Adicionar tags a um recurso de conexões (CLI)

Você pode usar o AWS CLI para marcar recursos em conexões.

No terminal ou na linha de comando, execute o comando tag-resource, especificando o nome de recurso da Amazon (ARN) do recurso no qual você deseja incluir tags e a chave e o valor da tag que você deseja adicionar. É possível adicionar mais de uma tag.

Para adicionar etiquetas a uma conexão

1. Obtenha o ARN para o seu recurso. Use o comando list-connections mostrado em Listar Conexões para obter o ARN da conexão.
2. No terminal ou na linha de comando, execute o comando tag-resource.

   Por exemplo, use o comando a seguir para marcar uma conexão com duas tags, uma chave de tag chamada Projeto com o valor de tag de Projecta e uma chave de tag chamada ReadOnlycom o valor de tag true.

   ```
   aws codestar-connections tag-resource --resource-arn arn:aws:codestar-
   connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f --
   tags Key=Project,Value=ProjectA Key=IscontainerBased,Value=true
   ```

   Se houver êxito, o comando não retornará nada.

Para adicionar etiquetas a um host

1. Obtenha o ARN para o seu recurso. Use o comando list-hosts mostrado em Listar hosts para obter o ARN do host.
2. No terminal ou na linha de comando, execute o comando tag-resource.

   Por exemplo, use o comando a seguir para marcar um host com duas tags, uma chave de tag chamada Projeto com o valor de tag de Projecta e uma chave de tag chamada IscontainerBasedcom o valor de tag true.

   ```
   aws codestar-connections tag-resource --resource-arn arn:aws:codestar-
   connections:us-west-2:account_id:host/My-Host-28aef605 --tags
    Key=Project,Value=ProjectA Key=IscontainerBased,Value=true
   ```

   Se houver êxito, o comando não retornará nada.

Visualizar tags para um recurso de conexões (CLI)

Você pode usar o AWS CLI para visualizar as AWS tags de um recurso de conexões. Se não foram adicionadas tags, a lista retornará vazia. Use o comando list-tags-for-resource para visualizar tags adicionadas a uma conexão ou um host.

Para visualizar etiquetas de uma conexão

1. Obtenha o ARN para o seu recurso. Use o comando list-connections mostrado em Listar Conexões para obter o ARN da conexão.
2. No terminal ou na linha de comando, execute o comando list-tags-for-resource. Por exemplo, use o comando a seguir para visualizar uma lista de chaves e valores de tag para uma conexão.

```
aws codestar-connections list-tags-for-resource --resource-arn arn:aws:codestar-
connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f
```

   Esse comando retorna as tags associadas ao recurso. Este exemplo mostra dois pares de chave e valor retornados para uma conexão.

```
{
    "Tags": [
        {
            "Key": "Project",
            "Value": "ProjectA"
        },
        {
            "Key": "ReadOnly",
            "Value": "true"
        }
    ]
}
```

Para visualizar etiquetas de um host

1. Obtenha o ARN para o seu recurso. Use o comando list-hosts mostrado em Listar hosts para obter o ARN do host.
2. No terminal ou na linha de comando, execute o comando list-tags-for-resource. Por exemplo, use o comando a seguir para visualizar uma lista de chaves e valores de tag para um host.

```
aws codestar-connections list-tags-for-resource --resource-arn arn:aws:codestar-
connections:us-west-2:account_id:host/My-Host-28aef605
```

Esse comando retorna as tags associadas ao recurso. Este exemplo mostra dois pares de chave e valor retornados para um host.

```
{
    "Tags": [
        {
            "Key": "IscontainerBased",
            "Value": "true"
        },
        {
            "Key": "Project",
            "Value": "ProjectA"
        }
    ]
}
```

Editar tags para um recurso de conexões (CLI)

Você pode usar o AWS CLI para editar uma tag para um recurso. Você pode alterar o valor para uma chave existente ou adicionar outra chave.

No terminal ou na linha de comando, execute o comando tag-resource, especificando o ARN do recurso em que você deseja atualizar uma tag e especifique a chave e o valor da tag a ser atualizada.

Quando você editar tags, todas as chaves de tag não especificadas serão mantidas, enquanto qualquer outra coisa com a mesma chave, mas um novo valor, será atualizada. Novas chaves que são adicionadas com o comando edit são adicionadas como um novo par chave-valor.

Para editar etiquetas de uma conexão

1. Obtenha o ARN para o seu recurso. Use o comando list-connections mostrado em Listar Conexões para obter o ARN da conexão.
2. No terminal ou na linha de comando, execute o comando tag-resource.

   Neste exemplo, o valor da chave `Project` é alterado para `ProjectB`.

```
aws codestar-connections tag-resource --resource-arn arn:aws:codestar-
connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f --
tags Key=Project,Value=ProjectB
```

Se houver êxito, o comando não retornará nada. Para verificar as tags associadas à conexão, execute o comando list-tags-for-resource.

Para editar etiquetas de um host

1. Obtenha o ARN para o seu recurso. Use o comando list-hosts mostrado em Listar hosts para obter o ARN do host.
2. No terminal ou na linha de comando, execute o comando tag-resource.

   Neste exemplo, o valor da chave `Project` é alterado para `ProjectB`.

   ```
   aws codestar-connections tag-resource --resource-arn arn:aws:codestar-
   connections:us-west-2:account_id:host/My-Host-28aef605 --tags
    Key=Project,Value=ProjectB
   ```

   Se houver êxito, o comando não retornará nada. Para verificar as tags associadas ao host, execute o comando list-tags-for-resource.

Remover tags de um recurso de conexões (CLI)

Siga estas etapas para usar o AWS CLI para remover uma tag de um recurso. Ao remover tags do recurso associado, as tags são excluídas.

> **Note**
>
> Se você excluir um recurso de conexão, todas as associações de tags serão removidas do recurso excluído. Não é necessário remover tags antes de excluir um recurso de conexão.

No terminal ou na linha de comando, execute o comando untag-resource, especificando o ARN do recurso de onde você deseja remover tags e a chave da tag a ser removida. Por exemplo, para remover várias tags em uma conexão com as chaves de tag *`Project`* e *`ReadOnly`*, use o comando a seguir.

```
aws codestar-connections untag-resource --resource-arn arn:aws:codestar-connections:us-
west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f --tag-
keys Project ReadOnly
```

Se houver êxito, o comando não retornará nada. Para verificar as tags associadas ao recurso, execute o comando list-tags-for-resource. A saída mostra que todas as tags foram removidas.

```
{
    "Tags": []
}
```

Visualizar detalhes da conexão

É possível usar o console do Developer Tools ou o comando get-connection na AWS Command Line Interface (AWS CLI) para visualizar os detalhes de uma conexão. Para usar o AWS CLI, você já deve ter instalado uma versão recente do AWS CLI ou atualizado para a versão atual. Para obter mais informações, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface .

Para visualizar uma conexão (console)

1. Abra o console do Developer Tools em https://console.aws.amazon.com/codesuite/settings/connections.
2. Escolha Settings > Connections (Configurações > Conexão).
3. Escolha o botão ao lado da conexão que você deseja visualizar e escolha View details (Visualizar detalhes).
4. As seguintes informações são exibidas para sua conexão:

   - O nome da conexão.
   - O tipo de provedor para a sua conexão.
   - O status da conexão.
   - O ARN da conexão.
   - Se a conexão foi criada para um provedor instalado, como o GitHub Enterprise Server, as informações do host associadas à conexão.
   - Se a conexão foi criada para um provedor instalado, como o GitHub Enterprise Server, as informações do endpoint associadas ao host da conexão.

5. Se a conexão estiver no status Pending (Pendente), para concluir a conexão, selecione Update pending connection (Atualizar conexão pendente). Para obter mais informações, consulte Atualizar uma conexão pendente.

Para visualizar uma conexão (CLI)

- No terminal ou na linha de comando, execute o comando get-connection. Por exemplo, use o comando a seguir para visualizar detalhes para uma conexão com o valor de ARN `arn:aws:codestar-connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f`.

```
aws codestar-connections get-connection --connection-arn arn:aws:codestar-
connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f
```

Se o comando for bem-sucedido, os detalhes da conexão serão retornados.

Exemplo de saída para uma conexão ao Bitbucket:

```
{
    "Connection": {
        "ConnectionName": "MyConnection",
        "ConnectionArn": "arn:aws:codestar-connections:us-
west-2:account_id:connection/cdacd948-EXAMPLE",
        "ProviderType": "Bitbucket",
        "OwnerAccountId": "account_id",
        "ConnectionStatus": "AVAILABLE"
    }
}
```

Exemplo de saída para uma GitHub conexão:

```
{
    "Connection": {
        "ConnectionName": "MyGitHubConnection",
        "ConnectionArn": "arn:aws:codestar-connections:us-
west-2:account_id:connection/ebcd4a13-EXAMPLE",
        "ProviderType": "GitHub",
        "OwnerAccountId": "account_id",
        "ConnectionStatus": "AVAILABLE"
    }
```

```
}
```

Exemplo de saída para uma conexão com o GitHub Enterprise Server:

```
{
    "Connection": {
        "ConnectionName": "MyConnection",
        "ConnectionArn": "arn:aws:codestar-connections:us-
west-2:account_id:connection/2d178fb9-EXAMPLE",
        "ProviderType": "GitHubEnterpriseServer",
        "OwnerAccountId": "account_id",
        "ConnectionStatus": "PENDING",
        "HostArn": "arn:aws:codestar-connections:us-west-2:account_id:host/sdfsdf-
EXAMPLE"
    }
}
```

Como trabalhar com hosts

Para criar uma conexão com um tipo de provedor instalado, como o GitHub Enterprise Server, crie primeiro um host usando o AWS Management Console. Um host é um recurso que você cria para representar a infraestrutura em que seu provedor está instalado. Em seguida, você cria uma conexão usando esse host. Para obter mais informações, consulte Trabalhar com conexões.

Por exemplo, você cria um host para sua conexão para que o aplicativo de terceiros para seu provedor possa ser registrado para representar sua infraestrutura. Você cria um host para um tipo de provedor e, em seguida, todas as conexões a esse tipo de provedor utilizam esse host.

Quando você usa o console para criar uma conexão com um tipo de provedor instalado, como o GitHub Enterprise Server, o console cria seu recurso de host para você.

Tópicos

- Criar um host
- Configurar um host pendente
- Listar hosts
- Editar um host
- Excluir um host

- Visualizar detalhes do host

Criar um host

Você pode usar o AWS Management Console ou a AWS Command Line Interface (AWS CLI) para criar uma conexão com um repositório de código de terceiros instalado na sua infraestrutura. Por exemplo, você pode ter o GitHub Enterprise Server em execução como uma máquina virtual em uma instância do Amazon EC2. Antes de criar uma conexão com o GitHub Enterprise Server, crie um host a ser usado para a conexão.

Consulte uma visão geral do fluxo de trabalho de criação de host para provedores instalados em Fluxo de trabalho para criar ou atualizar um host.

Antes de começar

- (Opcional) Se quiser criar o host com uma VPC, você já deverá ter criado uma rede ou uma nuvem privada virtual (VPC).
- Você já deve ter criado a instância e, se planeja se conectar com a VPC, também já deve ter iniciado o host na VPC.

> **Note**
>
> Cada VPC só pode estar associada a um host por vez.

Se preferir, você poderá configurar o host com uma VPC. Consulte mais informações sobre a configuração de rede e VPC para o recurso de host nos pré-requisitos da VPC em (Opcional) Pré-requisitos: configuração de rede ou da Amazon VPC para sua conexão e Solução de problemas de configuração da VPC para seu host.

Para usar o console a fim de criar um host e uma conexão com o GitHub Enterprise Server, consulte Crie sua conexão com o GitHub Enterprise Server (console). O console cria seu host para você.

Para usar o console a fim de criar um host e uma conexão com o GitLab autogerenciado, consulte Crie uma conexão com o GitLab autogerenciado. O console cria seu host para você.

(Opcional) Pré-requisitos: configuração de rede ou da Amazon VPC para sua conexão

Se a sua infraestrutura estiver configurada com uma conexão de rede, ignore esta seção.

Se o seu host só for acessível em uma VPC, siga estes requisitos da VPC antes de continuar.

Requisitos da VPC

Você pode optar por criar o host com uma VPC. Veja a seguir os requisitos gerais da VPC, dependendo da VPC que você configurou para sua instalação.

- Você pode configurar uma VPC pública com sub-redes públicas e privadas. Você poderá usar a VPC padrão para a sua Conta da AWS se não tiver blocos ou sub-redes CIDR preferenciais.
- Se você tiver uma VPC privada configurada e tiver configurado sua instância do GitHub Enterprise Server para executar a validação de TLS usando uma autoridade de certificação não pública, será necessário fornecer o certificado TLS para seu recurso de host.
- Quando o AWS CodeStar Connections cria o host, o endpoint da VPC (PrivateLink) para webhooks é criado para você. Para obter mais informações, consulte Conexões do AWS CodeStar Connections e endpoints da VPC de interface (AWS PrivateLink).
- Configuração do grupo de segurança:
  - Os grupos de segurança usados durante a criação do host precisam de regras de entrada e saída que permitem que a interface de rede se conecte à instância do GitHub Enterprise Server
  - Os grupos de segurança anexados à instância do GitHub Enterprise Server (que não fazem parte da configuração do host) precisam de acesso de entrada e saída a partir das interfaces de rede criadas por conexões.
- As sub-redes da VPC devem residir em zonas de disponibilidade diferentes na região. As zonas de disponibilidade são locais distintos e isolados de falhas em outras zonas de disponibilidade. Cada sub-rede deve residir inteiramente dentro de uma zona de disponibilidade e não pode abranger zonas.

Para obter mais informações sobre como trabalhar com VPCs e sub-redes, consulte Dimensionamento da VPC e sub-rede para IPv4 no Manual do usuário da Amazon VPC.

Informações da VPC que você forneceu para a configuração do host

Ao criar o recurso de host para suas conexões na próxima etapa, forneça o seguinte:

- ID da VPC: o ID da VPC para o servidor em que sua instância do GitHub Enterprise Server está instalada ou uma VPC que tenha acesso à instância do GitHub Enterprise Server instalada por meio de VPN ou Direct Connect.

- ID ou IDs de sub-rede: o ID da sub-rede do servidor em que sua instância do GitHub Enterprise Server está instalada ou uma sub-rede com acesso à instância do GitHub Enterprise Server instalada por meio de VPN ou Direct Connect.
- Grupo ou grupos de segurança: o grupo de segurança do servidor em que sua instância do GitHub Enterprise Server está instalada ou um grupo de segurança com acesso à instância do GitHub Enterprise Server instalada por meio de VPN ou Direct Connect.
- Endpoint: tenha o endpoint do servidor pronto e continue até a próxima etapa.

Para obter mais informações sobre como solucionar problemas de VPC ou conexões de host, consulte Solução de problemas de configuração da VPC para seu host.

Requisitos de permissão

No processo de criação do host, o AWS CodeStar Connections cria recursos de rede em seu nome para facilitar a conectividade da VPC. Isso inclui uma interface de rede do AWS Codestar Connections para consultar dados do host e um endpoint da VPC ou PrivateLink para que o host envie dados de eventos por meio de webhooks ao AWS CodeStar Connections. Para criar esses recursos de rede, verifique se a função usada para criar o host tem as permissões a seguir:

```
ec2:CreateNetworkInterface
ec2:CreateTags
ec2:DescribeDhcpOptions
ec2:DescribeNetworkInterfaces
ec2:DescribeSubnets
ec2:DeleteNetworkInterface
ec2:DescribeVpcs
ec2:CreateVpcEndpoint
ec2:DeleteVpcEndpoints
ec2:DescribeVpcEndpoints
```

Para obter mais informações sobre como solucionar problemas de permissões ou conexões de host em uma VPC, consulte Solução de problemas de configuração da VPC para seu host.

Para obter mais informações sobre VPC endpoint do webhook, consulte Conexões do AWS CodeStar Connections e endpoints da VPC de interface (AWS PrivateLink).

Tópicos

- Criar um host para uma conexão (console)

- Criar um host para uma conexão (CLI)

Criar um host para uma conexão (console)

Para conexões de instalações, como com o GitHub Enterprise Server ou o GitLab autogerenciado, você deve usar um host para representar o endpoint da infraestrutura em que o provedor de terceiros está instalado.

Para saber mais sobre as considerações sobre a configuração de um host em uma VPC, consulte Crie uma conexão com o GitLab autogerenciado.

Para usar o console a fim de criar um host e uma conexão com o GitHub Enterprise Server, consulte Crie sua conexão com o GitHub Enterprise Server (console). O console cria seu host para você.

Para usar o console a fim de criar um host e uma conexão com o GitLab autogerenciado, consulte Crie uma conexão com o GitLab autogerenciado. O console cria seu host para você.

> **Note**
>
> Você só deve criar um host uma vez por conta do GitHub Enterprise Server ou do GitLab autogerenciado. Todas as suas conexões com uma conta específica do GitHub Enterprise Server ou do GitLab autogerenciado usarão o mesmo host.

Criar um host para uma conexão (CLI)

Você pode usar a AWS Command Line Interface (AWS CLI) para criar um host para conexões instaladas.

> **Note**
>
> Você só cria um host uma vez por conta do GitHub Enterprise Server. Todas as suas conexões com uma conta específica do GitHub Enterprise Server usarão o mesmo host.

Você usa um host para representar o endpoint da infraestrutura em que seu provedor de terceiros está instalado. Para criar um host com a CLI, use o comando create-host. Concluída a criação do host, o host estará no status Pending (Pendente). Você então deve configurar o host para movê-lo para um status Available (Disponível). Depois que o host estiver disponível, conclua as etapas para criar uma conexão.

> **Important**
>
> Um host criado por meio da AWS CLI permanece no status `Pending` por padrão. Depois de criar um host com a CLI, use o console do para configurar o host e tornar seu status `Available`.

Para usar o console a fim de criar um host e uma conexão com o GitHub Enterprise Server, consulte Crie sua conexão com o GitHub Enterprise Server (console). O console cria seu host para você.

Para usar o console a fim de criar um host e uma conexão com o GitLab autogerenciado, consulte Crie uma conexão com o GitLab autogerenciado. O console cria seu host para você.

Configurar um host pendente

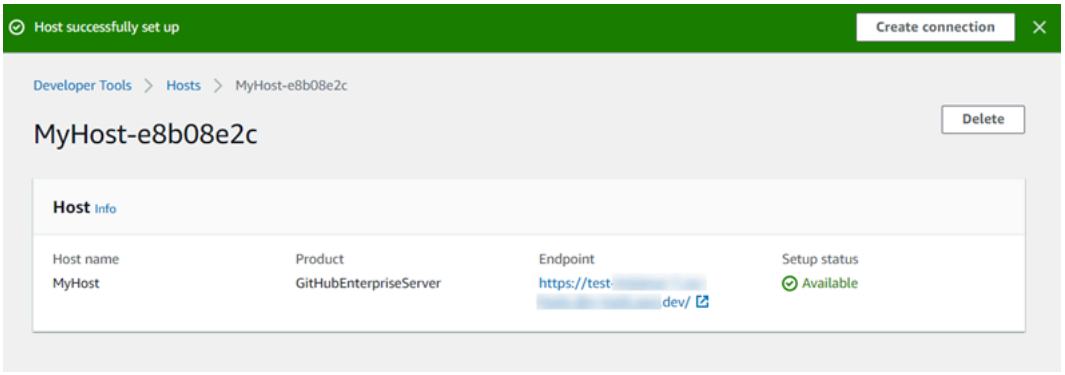
Um host criado por meio da AWS Command Line Interface (AWS CLI) ou SDK permanece no status `Pending` por padrão. Depois de criar uma conexão com o console, a AWS CLI ou o SDK, use o console para atualizar o host e tornar seu status `Available`.

Você já deve ter criado um host Para obter mais informações, consulte Criar um host.

Para configurar um host pendente

Depois que o host é criado, ele está em um status Pending (Pendente). Para mover o host de Pending (Pendente) para Available (Disponível), conclua estas etapas. Esse processo executa um handshake com o provedor terceiro para registrar a aplicação de conexão da AWS no host.

1. Depois que seu host atingir o status Pending (Pendente) no console do AWS Developer Tools, selecione Set up host (Configurar host).
2. Se você estiver criando um host para o GitLab autogerenciado, será exibida uma página de Configuração. Em Fornecer token de acesso pessoal, forneça ao PAT do GitLab somente a seguinte permissão de escopo reduzido: api.
3. Na página de login do provedor instalado de terceiros, como o GitHub EnterpriseServer, faça login com as credenciais da sua conta, se solicitado.
4. Na página de instalação da aplicação, em GitHub App name (Nome da aplicação do GitHub), insira um nome para a aplicação que deseja instalar para seu host. Escolha Create GitHub App (Criar aplicação do GitHub).
5. Depois que o host for registrado com êxito, a página de detalhes do host será exibida e mostrará que o status do host é Available (Disponível).



6. Você pode continuar criando sua conexão depois que o host estiver disponível. No banner de sucesso, escolha Create connection (Criar conexão). Conclua as etapas em Create a connection (Criar uma conexão).

Listar hosts

É possível usar o console do Developer Tools ou o comando list-connections na AWS Command Line Interface (AWS CLI) para visualizar uma lista de conexões na conta.

Listar hosts (console)

Para listar hosts

1. Abra o console do Developer Tools em https://console.aws.amazon.com/codesuite/settings/connections.
2. Escolha a guia Hosts. Visualize o nome, o status e o ARN dos hosts.

Listar hosts (CLI)

Você pode usar a AWS CLI para listar seus hosts para conexões de provedores de terceiros instalados.

Para fazer isso, use o comando list-hosts.

Para listar hosts

- Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows) e use a AWS CLI para executar o comando list-hosts.

```
aws codestar-connections list-hosts
```

Este comando retorna a seguinte saída.

```
{
    "Hosts": [
        {
            "Name": "My-Host",
            "HostArn": "arn:aws:codestar-connections:us-west-2:account_id:host/My-
Host-28aef605",
            "ProviderType": "GitHubEnterpriseServer",
            "ProviderEndpoint": "https://my-instance.test.dev",
            "Status": "AVAILABLE"
        }
    ]
}
```

Editar um host

Você pode editar as configurações de host para um host no status `Pending`. Você pode editar o nome do host, URL ou configuração da VPC.

Não é possível usar o mesmo URL para mais de um host.

> **Note**
>
> Para saber mais sobre as considerações sobre a configuração de um host em uma VPC, consulte (Opcional) Pré-requisitos: configuração de rede ou da Amazon VPC para sua conexão.

Para editar um host

1. Abra o console do Developer Tools em https://console.aws.amazon.com/codesuite/settings/connections.
2. Escolha Settings > Connections (Configurações > Conexão).
3. Escolha a guia Hosts.

   Os hosts associados à sua conta da AWS e criados na região da AWS selecionada são exibidos.

4. Para editar o nome do host, insira um novo valor em Name (Nome).
5. Para editar o endpoint do host, insira um novo valor em URL.
6. Para editar a configuração da VPC do host, insira novos valores em VPC ID (ID da VPC).
7. Selecione Edit host (Editar host).
8. As configurações atualizadas são exibidas. Selecione Set up Pending host (Configurar host pendente).

Excluir um host

É possível usar o console do Developer Tools ou o comando delete-host na AWS Command Line Interface (AWS CLI) para excluir um host.

Tópicos

- Excluir um host (console)
- Excluir um host (CLI)

Excluir um host (console)

Para excluir um host

1. Abra o console do Developer Tools em https://console.aws.amazon.com/codesuite/settings/connections.
2. Escolha a guia Hosts. Em Name (Nome), escolha o nome do host que você deseja excluir.
3. Escolha Delete (Excluir).
4. Digite **`delete`** no campo para confirmar e escolha Excluir.

> **Important**
>
> Esta ação não pode ser desfeita.

Excluir um host (CLI)

Você pode usar a AWS Command Line Interface (AWS CLI) para excluir um host.

Para fazer isso, use o comando delete-host.

> **Important**
>
> Para poder excluir um host, primeiro é necessário excluir todas as conexões associadas a ele.
> Após a execução do comando, o host é excluído. Nenhuma caixa de diálogo de confirmação é exibida.

Para excluir um host

- Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use a AWS CLI para executar o comando delete-host, especificando o nome do recurso da Amazon (ARN) do host que deseja excluir.

  ```
  aws codestar-connections delete-host --host-arn "arn:aws:codestar-connections:us-west-2:account_id:host/My-Host-28aef605"
  ```

  Esse comando não retorna nada.

Visualizar detalhes do host

É possível usar o console do Developer Tools ou o comando get-host na AWS Command Line Interface (AWS CLI) para visualizar os detalhes de um host.

Para visualizar detalhes de um host (console)

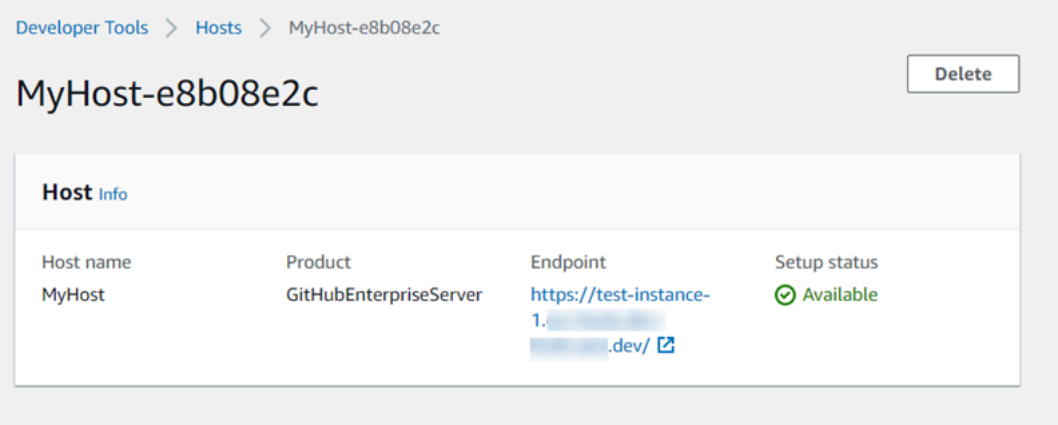
1. Faça login no AWS Management Console e abra o console do Developer Tools em https://console.aws.amazon.com/codesuite/settings/connections.
2. Escolha Settings > Connections (Configurações > Conexões) e, em seguida, escolha a guia Hosts.
3. Escolha o botão ao lado do host que você deseja visualizar e escolha View details (Visualizar detalhes).
4. As seguintes informações são exibidas para o seu host:

   - O nome do host.
   - O tipo de provedor para a sua conexão.
   - O endpoint da infraestrutura em que seu provedor está instalado.

- O status de configuração do seu host. Um host pronto para uma conexão está no status Available (Disponível). Se o host foi criado, mas a configuração não foi concluída, o host pode estar em um status diferente.

  Os seguintes status estão disponíveis:

  - PENDING (PENDENTE): a criação do host foi concluída e ele está pronto para iniciar a configuração registrando a aplicação do provedor no host.
  - AVAILABLE (DISPONÍVEL): a criação e a configuração do host foram concluídas e ele está disponível para uso com conexões.
  - ERROR (ERRO): ocorreu um erro durante a criação ou o registro do host.
  - VPC_CONFIG_VPC_INITIALIZING: a configuração da VPC para o host está sendo criada.
  - VPC_CONFIG_VPC_FAILED_INITIALIZATION: a configuração da VPC para o host encontrou um erro e falhou.
  - VPC_CONFIG_VPC_AVAILABLE: a configuração da VPC para o host foi concluída e está disponível.
  - VPC_CONFIG_VPC_DELETING: a configuração da VPC para o host está sendo excluída.



5. Para excluir o host, escolha Delete (Excluir).
6. Se o host estiver no status Pending (Pendente), escolha Set up host (Configurar host) para concluir a configuração. Para obter mais informações, consulte Configurar um host pendente.

Para visualizar detalhes do host (CLI)

- Abra um terminal (Linux, macOS ou Unix) ou prompt de comando (Windows) e use a AWS CLI para executar o comando get-host, especificando o nome do recurso da Amazon (ARN) do host para o qual você deseja visualizar os detalhes.

```
aws codestar-connections get-host --host-arn arn:aws:codestar-connections:us-
west-2:account_id:host/My-Host-28aef605
```

Este comando retorna a seguinte saída.

```
{
    "Name": "MyHost",
    "Status": "AVAILABLE",
    "ProviderType": "GitHubEnterpriseServer",
    "ProviderEndpoint": "https://test-instance-1.dev/"
}
```

Trabalhar com configurações de sincronização para repositórios vinculados

Em AWS CodeStar Conexões, você usa uma conexão para associar AWS recursos a um repositório de terceiros GitHub, como Bitbucket Cloud, GitHub Enterprise Server e. GitLab Usando o tipo de `CFN_STACK_SYNC` sincronização, você pode criar uma configuração de sincronização, que permite AWS sincronizar conteúdo de um repositório Git para atualizar um recurso específico. AWS AWS CloudFormation se integra às conexões para que você possa usar o Git sync para gerenciar seus arquivos de modelo e parâmetros em um repositório vinculado com o qual você sincroniza.

Depois de criar uma conexão, você pode usar a CLI de conexões ou o AWS CloudFormation console para criar o link do repositório e a configuração de sincronização.

- Link de repositório: um link de repositório cria uma associação entre a conexão e um repositório Git externo. O link de repositório permite que a sincronização Git monitore e sincronize as alterações nos arquivos em um repositório Git especificado.
- Configuração de sincronização: use a configuração de sincronização para sincronizar conteúdo de um repositório Git para atualizar um recurso específico. AWS

Para obter mais informações, consulte a Referência da API AWS CodeStar Connections.

Para ver um tutorial que orienta você na criação de uma configuração de sincronização para uma AWS CloudFormation pilha usando o AWS CloudFormation console, consulte Como trabalhar com o AWS CloudFormation Git sync no Guia CloudFormation do Usuário.

Tópicos

- Trabalhar com links de repositório
- Trabalhar com configurações de sincronização

Trabalhar com links de repositório

Um link de repositório cria uma associação entre a conexão e um repositório Git externo. O link do repositório permite que o Git sync monitore e sincronize as alterações nos arquivos em um repositório Git especificado com uma pilha. AWS CloudFormation

Para obter mais informações sobre links de repositórios, consulte a referência da API AWS CodeStar Connections.

Tópicos

- Criar um link de repositório
- Atualizar um link de repositório
- Listar links de repositório
- Excluir um link de repositório
- Visualizar os detalhes do link de repositório

Criar um link de repositório

Você pode usar o create-repository-link comando no AWS Command Line Interface (AWS CLI) para criar um link entre sua conexão e o repositório externo para sincronizar.

Antes de criar um link de repositório, você já deve ter criado seu repositório externo com seu provedor terceirizado, como. GitHub

Como criar um link de repositório

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o create-repository-link comando. Especifique o ARN da conexão associada, o ID do proprietário e o nome do repositório.

```
aws codestar-connections create-repository-link --connection-arn  arn:aws:codestar-
connections:us-east-1:account_id:connection/001f5be2-a661-46a4-b96b-4d277cac8b6e --
owner-id account_id --repository-name MyRepo
```

2. Este comando retorna a seguinte saída.

```
{
    "RepositoryLinkInfo": {
        "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
        "OwnerId": "account_id",
        "ProviderType": "GitHub",
        "RepositoryLinkArn": "arn:aws:codestar-connections:us-
east-1:account_id:repository-link/be8f2017-b016-4a77-87b4-608054f70e77",
        "RepositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
        "RepositoryName": "MyRepo",
        "Tags": []
    }
}
```

Atualizar um link de repositório

Você pode usar o update-repository-link comando no AWS Command Line Interface (AWS CLI) para atualizar um link de repositório especificado.

É possível atualizar as seguintes informações para o link do repositório:

- `--connection-arn`
- `--owner-id`
- `--repository-name`

É possível atualizar um link de repositório quando quiser alterar a conexão associada ao repositório. Para usar uma conexão diferente, é necessário especificar o ARN da conexão. Para ver as etapas para visualizar o ARN da conexão, consulte Visualizar detalhes da conexão.

Como atualizar um link de repositório

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o update-repository-link comando, especificando o valor a ser atualizado para

o link do repositório. Por exemplo, o comando a seguir atualiza a conexão associada ao ID do link de repositório. Ele especifica o novo ARN da conexão com o parâmetro `--connection`.

```
aws codestar-connections update-repository-link --repository-link-id
 6053346f-8a33-4edb-9397-10394b695173 --connection-arn arn:aws:codestar-
connections:us-east-1:account_id:connection/aEXAMPLE-f055-4843-adef-4ceaefcb2167
```

2. Este comando retorna a seguinte saída.

```
{
    "RepositoryLinkInfo": {
        "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/aEXAMPLE-f055-4843-adef-4ceaefcb2167",
        "OwnerId": "owner_id",
        "ProviderType": "GitHub",
        "RepositoryLinkArn": "arn:aws:codestar-connections:us-
east-1:account_id:repository-link/6053346f-8a33-4edb-9397-10394b695173",
        "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
        "RepositoryName": "MyRepo",
        "Tags": []
    }
}
```

Listar links de repositório

Você pode usar o list-repository-links comando no AWS Command Line Interface (AWS CLI) para listar os links do repositório da sua conta.

Como listar links de repositório

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o list-repository-links comando.

```
aws codestar-connections list-repository-links
```

2. Este comando retorna a seguinte saída.

```
{
    "RepositoryLinks": [
        {
```

```
            "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/001f5be2-a661-46a4-b96b-4d277cac8b6e",
            "OwnerId": "owner_id",
            "ProviderType": "GitHub",
            "RepositoryLinkArn": "arn:aws:codestar-connections:us-
east-1:account_id:repository-link/6053346f-8a33-4edb-9397-10394b695173",
            "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "RepositoryName": "MyRepo",
            "Tags": []
        }
    ]
}
```

Excluir um link de repositório

Você pode usar o delete-repository-link comando no AWS Command Line Interface (AWS CLI) para excluir um link do repositório.

Para poder excluir um link de repositório, primeiro é necessário excluir todas as configurações de sincronização associadas a ele.

> **Important**
>
> Após a execução do comando, o link de repositório é excluído. Nenhuma caixa de diálogo de confirmação é exibida. É possível criar um link de repositório, mas o nome do recurso da Amazon (ARN) não é reutilizado.

Como excluir um link de repositório

- Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o delete-repository-link comando, especificando o ID do link do repositório a ser excluído.

  ```
  aws codestar-connections delete-repository-link --repository-link-id
   6053346f-8a33-4edb-9397-10394b695173
  ```

  Esse comando não retorna nada.

Visualizar os detalhes do link de repositório

Você pode usar o get-repository-link comando no AWS Command Line Interface (AWS CLI) para ver detalhes sobre um link de repositório.

Como visualizar os detalhes do link de repositório

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o get-repository-link comando, especificando o ID do link do repositório.

```
aws codestar-connections get-repository-link --repository-link-id
 6053346f-8a33-4edb-9397-10394b695173
```

2. Este comando retorna a seguinte saída.

```
{
    "RepositoryLinkInfo": {
        "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
        "OwnerId": "owner_id",
        "ProviderType": "GitHub",
        "RepositoryLinkArn": "arn:aws:codestar-connections:us-
east-1:account_id:repository-link/be8f2017-b016-4a77-87b4-608054f70e77",
        "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
        "RepositoryName": "MyRepo",
        "Tags": []
    }
}
```

Trabalhar com configurações de sincronização

Uma configuração de sincronização cria uma associação entre uma conexão e um repositório especificados. Use a configuração de sincronização para sincronizar conteúdo de um repositório Git para atualizar um recurso especificado da AWS .

Para obter mais informações sobre conexões, consulte a referência da API AWS CodeStar Connections.

Tópicos

- Criar uma configuração de sincronização

- Atualizar uma configuração de sincronização
- Listar configurações de sincronização
- Excluir uma configuração de sincronização
- Visualizar detalhes da configuração de sincronização

Criar uma configuração de sincronização

Você pode usar o create-repository-link comando no AWS Command Line Interface (AWS CLI) para criar um link entre sua conexão e o repositório externo para sincronizar.

Para criar uma configuração de sincronização, é necessário já ter criado um link de repositório entre a conexão e o repositório de terceiros.

Como criar uma configuração de sincronização

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o create-repository-link comando. Especifique o ARN da conexão associada, o ID do proprietário e o nome do repositório. O comando a seguir cria uma configuração de sincronização com um tipo de sincronização para um recurso no AWS CloudFormation. Também especifica a ramificação do repositório e o arquivo de configuração no repositório. Neste exemplo, o recurso é uma pilha denominada **`mystack`**.

```
aws codestar-connections create-sync-configuration --branch main --config-file
 filename --repository-link-id be8f2017-b016-4a77-87b4-608054f70e77 --resource-name
 mystack --role-arn arn:aws:iam::account_id:role/myrole --sync-type CFN_STACK_SYNC
```

2. Este comando retorna a seguinte saída.

```
{
    "SyncConfiguration": {
        "Branch": "main",
        "ConfigFile": "filename",
        "OwnerId": "account_id",
        "ProviderType": "GitHub",
        "RepositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
        "RepositoryName": "MyRepo",
        "ResourceName": "mystack",
        "RoleArn": "arn:aws:iam::account_id:role/myrole",
        "SyncType": "CFN_STACK_SYNC"
```

```
    }
```

Atualizar uma configuração de sincronização

É possível usar o comando update-sync-configuration na AWS Command Line Interface (AWS CLI) para atualizar uma configuração de sincronização especificada.

É possível atualizar as seguintes informações para a configuração de sincronização:

- `--branch`
- `--config-file`
- `--repository-link-id`
- `--resource-name`
- `--role-arn`

Como atualizar uma configuração de sincronização

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o update-sync-configuration comando, especificando o valor que você deseja atualizar, junto com o nome do recurso e o tipo de sincronização. Por exemplo, o comando a seguir atualiza o nome da ramificação associado à configuração de sincronização com o parâmetro `--branch`.

```
aws codestar-connections update-sync-configuration --sync-type CFN_STACK_SYNC --
resource-name mystack --branch feature-branch
```

2. Este comando retorna a seguinte saída.

```
{
    "SyncConfiguration": {
        "Branch": "feature-branch",
        "ConfigFile": "filename.yaml",
        "OwnerId": "owner_id",
        "ProviderType": "GitHub",
        "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
        "RepositoryName": "MyRepo",
        "ResourceName": "mystack",
        "RoleArn": "arn:aws:iam::account_id:role/myrole",
```

```
        "SyncType": "CFN_STACK_SYNC"
    }
```

Listar configurações de sincronização

É possível usar o comando list-sync-configurations na AWS Command Line Interface (AWS CLI) para listar os links de repositório para a conta.

Como listar links de repositório

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o list-sync-configurations comando, especificando o tipo de sincronização e o ID do link do repositório.

```
aws codestar-connections list-sync-configurations --repository-link-id
 6053346f-8a33-4edb-9397-10394b695173  --sync-type CFN_STACK_SYNC
```

2. Este comando retorna a seguinte saída.

```
{
    "SyncConfigurations": [
        {
            "Branch": "main",
            "ConfigFile": "filename.yaml",
            "OwnerId": "owner_id",
            "ProviderType": "GitHub",
            "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "RepositoryName": "MyRepo",
            "ResourceName": "mystack",
            "RoleArn": "arn:aws:iam::account_id:role/myrole",
            "SyncType": "CFN_STACK_SYNC"
        }
    ]
}
```

Excluir uma configuração de sincronização

É possível usar o comando delete-sync-configuration na AWS Command Line Interface (AWS CLI) para excluir uma configuração de sincronização.

> **Important**
>
> Após a execução do comando, a configuração de sincronização é excluída. Nenhuma caixa de diálogo de confirmação é exibida. É possível criar uma configuração de sincronização, mas o nome do recurso da Amazon (ARN) não é reutilizado.

Como excluir uma configuração de sincronização

- Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o delete-sync-configuration comando, especificando o tipo de sincronização e o nome do recurso para a configuração de sincronização que você deseja excluir.

  ```
  aws codestar-connections delete-sync-configuration --sync-type CFN_STACK_SYNC --
  resource-name mystack
  ```

  Esse comando não retorna nada.

Visualizar detalhes da configuração de sincronização

Você pode usar o get-sync-configuration comando no AWS Command Line Interface (AWS CLI) para ver os detalhes de uma configuração de sincronização.

Como visualizar detalhes de uma configuração de sincronização

1. Abra um terminal (Linux, macOS ou Unix) ou um prompt de comando (Windows). Use o AWS CLI para executar o get-sync-configuration comando, especificando o ID do link do repositório.

   ```
   aws codestar-connections get-sync-configuration --sync-type CFN_STACK_SYNC --
   resource-name mystack
   ```

2. Este comando retorna a seguinte saída.

   ```
   {
       "SyncConfiguration": {
           "Branch": "main",
           "ConfigFile": "filename",
           "OwnerId": "owner_id",
           "ProviderType": "GitHub",
           "RepositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
   ```

```
        "RepositoryName": "MyRepo",
        "ResourceName": "mystack",
        "RoleArn": "arn:aws:iam::account_id:role/myrole",
        "SyncType": "CFN_STACK_SYNC"
    }
}
```

Registrar em log chamadas de API do Conexões de código da AWS com o AWS CloudTrail

O Conexões de código da AWS é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço da AWS. O CloudTrail captura todas as chamadas de API para notificações na forma de eventos. As chamadas capturadas incluem as chamadas do console de ferramentas do desenvolvedor e as chamadas de código para as operações de API do Conexões de código da AWS.

Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon Simple Storage Service (Amazon S3), incluindo eventos para notificações. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Ao usar as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita ao Conexões de código da AWS, o endereço IP do qual a solicitação foi feita, quem a fez e quando ela foi feita, além de outros detalhes.

Para obter mais informações, consulte o Guia do usuário do AWS CloudTrail.

Informações do Conexões de código da AWS no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre uma atividade no Conexões de código da AWS, essa atividade é registrada em um evento do CloudTrail com outros eventos de produtos da AWS em Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da AWS. Para obter mais informações, consulte o tópico sobre como Visualizar eventos com o histórico de eventos do CloudTrail, no Guia do usuário do AWS CloudTrail.

Para obter um registro contínuo de eventos na conta da AWS, incluindo eventos do Conexões de código da AWS, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a 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 em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail.

Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do AWS CloudTrail:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões
- Recebimento de arquivos de log do CloudTrail de várias contas

Todas as ações do Conexões de código da AWS são registradas pelo CloudTrail e documentadas na Referência de API do Conexões de código da AWS. Por exemplo, as chamadas para as ações `CreateConnection`, `DeleteConnection` e `GetConnection` geram entradas nos arquivos de log do CloudTrail.

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

- Se a solicitação foi feita com credenciais de raiz ou outras credenciais do IAM.
- 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 serviço da AWS.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas sobre entradas de arquivos de log do

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `CreateConnection`.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/Mary_Major",
        "accountId":"123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName":"Mary_Major"
    },
    "eventTime": "2020-04-21T01:09:48Z",
    "eventSource": "codestar-connections.amazonaws.com",
    "eventName": "CreateConnection",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "IP",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/80.0.3987.163 Safari/537.36",
    "requestParameters": {
        "providerType": "Bitbucket",
        "connectionName": "my-connection"
    },
    "responseElements": {
        "connectionArn": "arn:aws:codestar-connections:us-
west-2:123456789012:connection/7EXAMPLE-5da1-4867-960c-4918175ea3ce"
    },
    "requestID": "ac1fbc15-a84f-4568-9f90-f05f1a57749c",
    "eventID": "7548f5b0-7ecf-430f-84bf-72e364644359",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Conexões do AWS CodeStar Connections e endpoints da VPC de interface (AWS PrivateLink)

É possível estabelecer uma conexão privada entre a VPC e o AWS CodeStar Connections criando um endpoint da VPC da interface. Os endpoints de interface são ativados por AWS PrivateLink, uma tecnologia que permite acessar de forma privada as APIs do AWS CodeStar Connections sem um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão do AWS Direct

Connect. As instâncias na VPC não precisam de endereços IP públicos para se comunicar com APIs do AWS CodeStar Connections, pois o tráfego entre a VPC e o AWS CodeStar Connections não sai da rede da Amazon.

Cada endpoint de interface é representado por uma ou mais interfaces de rede elástica nas sub-redes.

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

Considerações sobre os endpoints da VPC do AWS CodeStar Connections

Antes de configurar um endpoint da VPC de interface para AWS CodeStar Connections, leia Interface endpoints (Endpoints de interface) no Guia do usuário da Amazon VPC.

O AWS CodeStar Connections é compatível com chamadas para todas as ações de API da sua VPC.

Os endpoints da VPC são compatíveis em todas as regiões do AWS CodeStar Connections.

Conceitos de endpoints da VPC

Veja a seguir os principais conceitos de VPC endpoints:

VPC endpoint

O ponto de entrada na VPC que permite que você se conecte de forma privada a um serviço. A seguir estão os diferentes tipos de endpoints da VPC. Crie o tipo de VPC endpoint necessário para o serviço compatível.

- Endpoints da VPC para ações do AWS CodeStar Connections
- Endpoints da VPC para webhooks do AWS CodeStar Connections

AWS PrivateLink

Uma tecnologia que fornece conectividade privada entre VPCs e serviços.

Endpoints da VPC para ações do AWS CodeStar Connections

É possível gerenciar endpoints da VPC para o serviço AWS CodeStar Connections.

Criar endpoints da VPC de interface para ações do AWS CodeStar Connections

É possível criar um endpoint da VPC para o serviço AWS CodeStar Connections usando o console da Amazon VPC ou a AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Criar um endpoint de interface no Guia do usuário da Amazon VPC.

Para começar a usar conexões com a VPC, crie um endpoint da VPC de interface para o AWS CodeStar Connections. Ao criar um endpoint da VPC para o AWS CodeStar Connections, selecione AWS Services (Serviços da AWS), e em Service Name (Nome do serviço), selecione:

- com.amazonaws.***region***.codestar-connections.api: essa opção cria um endpoint da VPC para operações de API do AWS CodeStar Connections. Por exemplo, selecione essa opção se os usuários utilizarem a CLI da AWS, a API do AWS CodeStar Connections ou os AWS SDKs para interagir com o AWS CodeStar Connections para operações, como `CreateConnection`, `ListConnections` e `CreateHost`.

Para a opção Enable DNS name (Ativar nome de DNS), se você selecionar o DNS privado para o endpoint, poderá fazer solicitações de API para o AWS CodeStar Connections usando seu nome DNS padrão para a região, por exemplo, `codestar-connections.us-east-1.amazonaws.com`.

> **Important**
>
> O DNS privado é ativado por padrão para endpoints criados para serviços da AWS e serviços de parceiros do AWS Marketplace.

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

Criar uma política de endpoint da VPC para ações do AWS CodeStar Connections

É possível anexar uma política ao endpoint da VPC que controla o acesso ao AWS CodeStar Connections. Essa política especifica as seguintes informações:

- A entidade principal que pode executar ações.
- As ações que podem ser executadas.
- Os recursos sobre os quais as ações podem ser realizadas.

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

> **Note**
>
> O endpoint com.amazonaws.*region*.codestar-connections.webhooks não oferece suporte a políticas.

Exemplo: política de endpoint da VPC para ações do AWS CodeStar Connections

Veja a seguir um exemplo de política de endpoint para o AWS CodeStar Connections. Quando anexada a um endpoint, essa política concede acesso às ações do AWS CodeStar Connections para todas as entidades principais em todos os recursos.

```
{
  "Statement": [
    {
      "Sid": "GetConnectionOnly",
      "Principal": "*",
      "Action": [
        "codestar-connections:GetConnection"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Endpoints da VPC para webhooks do AWS CodeStar Connections

O AWS CodeStar Connections cria endpoints de webhook quando você cria ou exclui um host com configuração de VPC. O nome do endpoint é com.amazonaws.***region***.codestar-connections.webhooks.

Com o endpoint da VPC para webhooks do GitHub, os hosts podem enviar dados de eventos via webhooks para seus serviços integrados da AWS pela rede da Amazon.

> **Important**
>
> Quando você configura seu host para o GitHub Enterprise Server, o AWS CodeStar Connections cria um endpoint da VPC para dados de eventos de webhooks para você. Se você criou seu host antes de 24 de novembro de 2020 e deseja usar os endpoints webhook do VPC PrivateLink, é necessário excluir seu host primeiro e, em seguida, criar um novo host.

O AWS CodeStar Connections gerencia o ciclo de vida desses endpoints. Para excluir o endpoint, você deve excluir o recurso de host correspondente.

Como os endpoints de webhooks para hosts do AWS CodeStar Connections são usados

O endpoint do webhook é onde os webhooks de repositórios de terceiro são enviados para processamento no AWS CodeStar Connections. Um webhook descreve uma ação do cliente. Quando você executa um `git push`, o endpoint do webhook recebe um webhook do provedor detalhando o push. Por exemplo, o AWS CodeStar Connections pode notificar o CodePipeline para iniciar seu pipeline.

Para provedores de nuvem, como hosts do Bitbucket ou GitHub Enterprise Server que não usam uma VPC, o endpoint da VPC do webhook não se aplica porque os provedores estão enviando webhooks para o AWS CodeStar Connections onde a rede da Amazon não é usada.

Solução de problemas de conexões

As informações a seguir podem ajudar você a solucionar problemas comuns de conexões com recursos no AWS CodeBuild, AWS CodeDeploy e AWS CodePipeline.

Tópicos

- Não consigo criar uma conexão para o meu host
- Solução de problemas de configuração da VPC para seu host
- Solução de problemas de endpoints da VPC de webhook (PrivateLink) para conexões do GitHub Enterprise Server
- Solução de problemas para hosts criados antes de 24 de novembro de 2020
- Não é possível criar a conexão para um repositório do GitHub
- Editar as permissões da aplicação de conexão do GitHub Enterprise Server
- Erro de conexão com o GitHub: “Ocorreu um problema, verifique se os cookies estão habilitados no seu navegador” ou “O proprietário da organização deve instalar a aplicação do GitHub”.
- Quero aumentar meus limites para conexões

Não consigo criar conexões

Talvez você não tenha permissões para criar uma conexão. Para obter mais informações, consulte Permissões e exemplos para Conexões de código da AWS.

Recebo um erro de permissões quando tento criar ou concluir uma conexão

A seguinte mensagem de erro pode ser retornada quando você tenta criar ou exibir uma conexão no console do CodePipeline.

User: *`username`* is not authorized to perform: *`permission`* on resource: *`connection-ARN`* (O usuário <nome de usuário> não está autorizado a realizar: <permissão> no recurso: <ARN da conexão>).

Se essa mensagem for exibida, verifique se você tem permissões suficientes.

As permissões para criar e exibir conexões na AWS Command Line Interface(AWS CLI) ou no AWS Management Console são apenas parte das permissões necessárias para criar e concluir conexões no console. As permissões necessárias para simplesmente visualizar, editar ou criar uma conexão e, em seguida, concluir a conexão pendente devem ser reduzidas para usuários que só precisam executar determinadas tarefas. Para obter mais informações, consulte Permissões e exemplos para Conexões de código da AWS.

Recebo um erro de permissões quando tento usar uma conexão

Uma ou ambas as mensagens de erro a seguir poderão ser retornadas se você tentar usar uma conexão no console do CodePipeline, mesmo que você tenha as permissões para listar, obter e criar permissões.

Não foi possível autenticar sua conta.

User: *username* is not authorized to perform: codestar-connections:UseConnection on resource: *connection-ARN* (O usuário: <nome de usuário> não está autorizado a realizar: codestar-connections:UseConnection no recurso <ARN da conexão>).

Se isso ocorrer, verifique se você tem permissões suficientes.

Verifique se você tem as permissões necessárias para usar uma conexão, incluindo listar os repositórios disponíveis no local do provedor. Para obter mais informações, consulte Permissões e exemplos para Conexões de código da AWS.

A conexão não está no estado disponível ou não está mais pendente

Se o console exibir uma mensagem informando que uma conexão não está em um estado disponível, escolha Complete connection (Conexão concluída).

Se você optar por concluir a conexão e uma mensagem informando que a conexão não está em um estado pendente for exibida, você poderá cancelar a solicitação porque a conexão já está em um estado disponível.

Adicionar permissões do GitClone para conexões

Quando você usa uma conexão do AWS CodeStar em uma ação de origem e uma ação do CodeBuild, há duas maneiras para passar o artefato de entrada para a compilação:

- O padrão: a ação de origem produz um arquivo zip que contém o código que o CodeBuild obtém por download.
- Clone do Git: o código-fonte pode ser obtido por download diretamente para o ambiente de compilação.

  O modo de clone do Git permite que você interaja com o código-fonte como um repositório Git em funcionamento. Para utilizar este modo, você deve conceder permissões de ambiente para o CodeBuild utilizar a conexão.

Para adicionar permissões à política de função de serviço do CodeBuild, crie uma política gerenciada pelo cliente anexada à sua função de serviço do CodeBuild. As etapas a seguir criam uma política em que a permissão `UseConnection` é especificada no campo `action` e o nome do recurso da Amazon (ARN) da conexão é especificado no campo `Resource`.

Para usar o console para adicionar as permissões do UseConnection

1. Para localizar o ARN da conexão para o pipeline, abra o pipeline e escolha o ícone (i) na ação de origem. O painel Configuração é aberto e o ARN da conexão aparece ao lado de ConnectionArn. Você adiciona o ARN da conexão à sua política de função de serviço do CodeBuild.
2. Para localizar sua função de serviço do CodeBuild, abra o projeto de compilação usado no pipeline e navegue até a guia Build details (Detalhes da compilação).
3. Na seção Environment (Ambiente), escolha o link Service role (Função de serviço). Isso abre o console do AWS Identity and Access Management (IAM), onde você pode adicionar uma nova política que concede acesso à sua conexão.
4. No console do IAM, escolha Attach policies (Anexar políticas) e selecione Create policy (Criar política).

   Use o seguinte exemplo de modelo de política. Adicione o ARN da sua conexão conexão no campo `Resource`, conforme mostrado neste exemplo.

   ```
   {
       "Version": "2012-10-17",
       "Statement": [
           {
               "Effect": "Allow",
               "Action": "codestar-connections:UseConnection",
               "Resource": "insert connection ARN here"
           }
       ]
   }
   ```

   Na guia JSON, cole sua política.
5. Escolha Review policy (Revisar política). Insira um nome para a política (por exemplo, **`connection-permissions`**) e escolha Create policy (Criar política).
6. Retorne à página Attach Permissions (Anexar permissões) da função de serviço, atualize a lista de políticas e selecione a política que acabou de criar. Escolha Attach policies (Anexar políticas).

O host não está no estado disponível

Se o console exibir uma mensagem informando que um host não está em um estado `Available`, escolha Set up host (Configurar host).

A primeira etapa para a criação do host resulta no host criado agora em um estado `Pending`. Para mover o host para um estado `Available`, você deve optar por configurar o host no console. Para obter mais informações, consulte Configurar um host pendente.

> **Note**
>
> Você não pode usar a AWS CLI para configurar um host `Pending`.

Solução de problemas de um host com erros de conexão

Conexões e hosts poderão entrar no estado de erro se a aplicação do GitHub subjacente for excluída ou modificada. Hosts e conexões no estado de erro não podem ser recuperados e o host deve ser recriado.

- Ações como alterar a chave pem da aplicação ou alterar o nome da aplicação (após a criação inicial) farão com que o host e todas as conexões associadas entrem no estado de erro.

Se o console ou a CLI retornar um host ou uma conexão relacionada a um host com um estado `Error`, talvez você precise executar a seguinte etapa:

- Exclua e recrie o recurso do host e reinstale a aplicação de registro do host. Para obter mais informações, consulte Criar um host.

Não consigo criar uma conexão para o meu host

Para criar uma conexão ou host, as condições a seguir são necessárias.

- Seu host deve estar no estado AVAILABLE (DISPONÍVEL). Para obter mais informações, consulte
- As conexões devem ser criadas na mesma região que o host.

Solução de problemas de configuração da VPC para seu host

Ao criar um recurso de host, você deve fornecer informações de conexão de rede ou VPC para a infraestrutura em que sua instância do GitHub Enterprise Server está instalada. Para solucionar problemas de configuração da VPC ou sub-rede para o host, use as informações de exemplo da VPC mostradas aqui como referência.

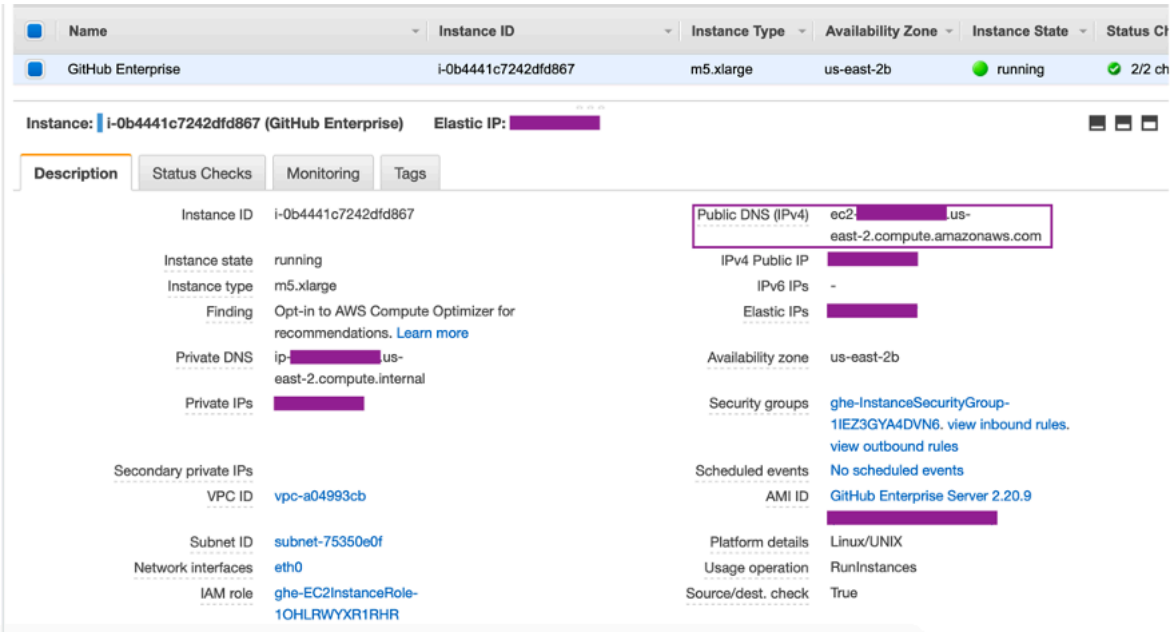
> **Note**
>
> Use esta seção para solucionar problemas relacionados à configuração de host do GitHub Enterprise Server em uma Amazon VPC. Para solucionar problemas relacionados à conexão configurada para usar o endpoint do webhook para VPC (PrivateLink), consulte Solução de problemas de endpoints da VPC de webhook (PrivateLink) para conexões do GitHub Enterprise Server.

Para este exemplo, você usaria o seguinte processo para configurar a VPC e o servidor em que sua instância do GitHub Enterprise Server será instalada:

1. Crie uma VPC. Para obter mais informações, consulte https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#Create-VPC.
2. Crie uma sub-rede na VPC. Para obter mais informações, consulte https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#AddaSubnet.
3. Inicie uma instância na VPC. Para obter mais informações, consulte https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#VPC_Launch_Instance.

> **Note**
>
> Cada VPC pode ser associada somente a um host (instância do GitHub Enterprise Server) por vez.

A imagem a seguir mostra uma instância do EC2 iniciada usando a AMI do GitHub Enterprise.



Ao usar uma VPC para uma conexão do GitHub Enterprise Server, você deve fornecer as seguintes informações para sua infraestrutura ao configurar seu host:

- ID da VPC: a VPC para o servidor em que sua instância do GitHub Enterprise Server está instalada ou uma VPC que tenha acesso à instância do GitHub Enterprise Server instalada por meio de VPN ou Direct Connect.
- ID ou IDs de sub-rede: a sub-rede do servidor em que sua instância do GitHub Enterprise Server está instalada ou uma sub-rede com acesso à instância do GitHub Enterprise Server instalada por meio de VPN ou Direct Connect.
- Grupo ou grupos de segurança: o grupo de segurança do servidor em que sua instância do GitHub Enterprise Server está instalada ou um grupo de segurança com acesso à instância do GitHub Enterprise Server instalada por meio de VPN ou Direct Connect.
- Endpoint: tenha o endpoint do servidor pronto e continue até a próxima etapa.

Para obter mais informações sobre como trabalhar com VPCs e sub-redes, consulte Dimensionamento da VPC e sub-rede para IPv4 no Manual do usuário da Amazon VPC.

Tópicos

- Não consigo obter um host no estado pendente
- Não consigo obter um host no estado disponível
- Minha conexão/host estava funcionando e parou de funcionar agora

- Não consigo excluir minhas interfaces de rede

Não consigo obter um host no estado pendente

Se o host entrar no estado VPC_CONFIG_FAILED_INITIALIZATION, a causa provavelmente é um problema com a VPC, sub-redes ou grupos de segurança que você selecionou para o host.

- A VPC, as sub-redes e os grupos de segurança devem pertencer à conta que cria o host.
- As sub-redes e grupos de segurança devem pertencer à VPC selecionada.
- Cada sub-rede deve estar em uma zona de disponibilidade diferente.
- O usuário que está criando o host deve ter as seguintes permissões do IAM:

```
ec2:CreateNetworkInterface
ec2:CreateTags
ec2:DescribeDhcpOptionsec2:DescribeNetworkInterfaces
ec2:DescribeSubnets
ec2:DeleteNetworkInterface
ec2:DescribeVpcs
ec2:CreateVpcEndpoint
ec2:DeleteVpcEndpoints
ec2:DescribeVpcEndpoints
```

Não consigo obter um host no estado disponível

Se você não conseguir concluir a configuração da aplicação AWS CodeStar Connections para seu host, pode ser devido a um problema com suas configurações de VPC ou sua instância do GitHub Enterprise Server.

- Se você não estiver usando uma autoridade de certificação pública, será necessário fornecer um certificado TLS ao host usado pela instância do GitHub Enterprise. O valor do certificado TLS deve ser a chave pública do certificado.
- É necessário ser um administrador da instância do GitHub Enterprise Server para criar aplicações do GitHub.

Minha conexão/host estava funcionando e parou de funcionar agora

Se uma conexão/host estava funcionando antes e não está funcionando agora, isso pode ser devido a uma alteração de configuração em sua VPC ou a aplicação GitHub foi modificada. Verifique o seguinte:

- O grupo de segurança anexado ao recurso de host que você criou para sua conexão foi alterado ou não tem mais acesso ao GitHub Enterprise Server. AWS O CodeStar Connections requer um grupo de segurança que tenha conectividade com a instância do GitHub Enterprise Server.
- O IP do servidor DNS foi alterado recentemente. Você pode verificar isso consultando as opções de DHCP anexadas à VPC especificada no recurso de host criado para sua conexão. Observe que se você migrou recentemente do AmazonProvidedDNS para um servidor DNS personalizado ou começou a usar um novo servidor DNS personalizado, o host/conexão deixaria de funcionar. Para corrigir isso, exclua seu host existente e recrie-o, o que armazenaria as configurações de DNS mais recentes em nosso banco de dados.
- As configurações de ACLs de rede foram alteradas e não estão mais permitindo conexões HTTP para a sub-rede onde sua infraestrutura do GitHub Enterprise Server está localizada.
- Configurações da aplicação AWS CodeStar Connections em seu GitHub Enterprise Server foram alteradas. Modificações em qualquer uma das configurações, como URLs ou segredos de aplicações, podem interromper a conectividade entre a instância do GitHub Enterprise Server instalada e o AWS CodeStar Connections.

Não consigo excluir minhas interfaces de rede

Se você não conseguir detectar suas interfaces de rede, verifique o seguinte:

- As interfaces de rede criadas pelo AWS CodeStar Connections só podem ser excluídas com a remoção do próprio host. Elas não podem ser excluídas manualmente pelo usuário.
- Você deve ter as seguintes permissões:

```
ec2:DescribeNetworkInterfaces
ec2:DeleteNetworkInterface
```

Solução de problemas de endpoints da VPC de webhook (PrivateLink) para conexões do GitHub Enterprise Server

Quando você cria um host com a configuração da VPC, o endpoint da VPC do webhook é criado para você.

> **Note**
>
> Use esta seção para solucionar problemas relacionados à conexão configurada para usar o endpoint do webhook para VPC (PrivateLink). Para solucionar problemas relacionados à configuração de host do GitHub Enterprise Server em uma Amazon VPC, consulte Solução de problemas de configuração da VPC para seu host.

Quando você cria uma conexão com um tipo de provedor instalado e especifica que seu servidor está configurado em uma VPC, o AWS CodeStar Connections cria seu host e o endpoint da VPC (PrivateLink) para webhooks é criado para você. Isso permite que o host envie dados de eventos via webhooks para seus serviços integrados da AWS pela rede da Amazon. Para obter mais informações, consulte Conexões do AWS CodeStar Connections e endpoints da VPC de interface (AWS PrivateLink).

Tópicos

- Não consigo excluir meus endpoints da VPC do webhook

Não consigo excluir meus endpoints da VPC do webhook

O AWS Codestar Connections gerencia o ciclo de vida dos endpoints da VPC do webhook para o seu host. Se desejar excluir o endpoint, faça isso excluindo o recurso de host correspondente.

- Os endpoints da VPC do webhook (PrivateLink) criados pelo AWS CodeStar Connections só podem ser excluídos com a exclusão do host. Eles não podem ser excluídos manualmente.
- Você deve ter as seguintes permissões:

```
ec2:DescribeNetworkInterfaces
ec2:DeleteNetworkInterface
```

Solução de problemas para hosts criados antes de 24 de novembro de 2020

A partir de 24 de novembro de 2020, quando o AWS CodeStar Connections configura seu host, o suporte a uma endpoint da VPC (PrivateLink) adicional é configurado para você. Para hosts criados antes desta atualização, use esta seção de solução de problemas.

Para obter mais informações, consulte Conexões do AWS CodeStar Connections e endpoints da VPC de interface (AWS PrivateLink).

Tópicos

- Tenho um host criado antes de 24 de novembro de 2020 e quero usar endpoints da VPC (PrivateLink) para webhooks
- Não consigo obter um host no estado disponível (erro da VPC)

Tenho um host criado antes de 24 de novembro de 2020 e quero usar endpoints da VPC (PrivateLink) para webhooks

Quando você configura seu host para o GitHub Enterprise Server, o endpoint do webhook é criado para você. As conexões agora usam endpoints webhook do VPC PrivateLink. Se você criou seu host antes de 24 de novembro de 2020 e deseja usar os endpoints webhook do VPC PrivateLink, é necessário excluir seu host primeiro e, em seguida, criar um novo host.

Não consigo obter um host no estado disponível (erro da VPC)

Se seu host foi criado antes de 24 de novembro de 2020 e você não consegue concluir a configuração da aplicação AWS CodeStar Connections para seu host, pode ser devido a um problema com suas configurações de VPC ou sua instância do GitHub Enterprise Server.

Sua VPC precisará de um gateway NAT (ou acesso de saída à Internet) para que sua instância do GitHub Enterprise Server possa enviar tráfego de rede de saída para webhooks do GitHub.

Não é possível criar a conexão para um repositório do GitHub

Problema:

Como uma conexão com um repositório do GitHub usa o AWS Connector para GitHub, você precisa de permissões de proprietário da organização ou permissões de administrador para o repositório para criar a conexão.

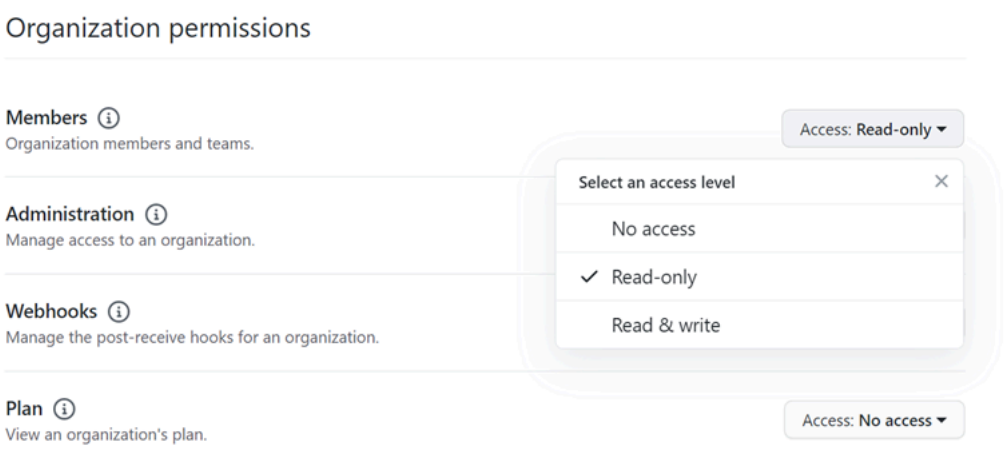
Correções possíveis: para obter informações sobre níveis de permissão de um repositório do GitHub, consulte https://docs.github.com/en/free-pro-team@latest/github/setting-up-and-managing-organizations-and-teams/permission-levels-for-an-organization.

Editar as permissões da aplicação de conexão do GitHub Enterprise Server

Se você instalou a aplicação para GitHub Enterprise Server em ou antes de 23 de dezembro de 2020, talvez seja necessário conceder à aplicação acesso somente leitura aos membros da organização. Se você for o proprietário da aplicação GitHub, siga estas etapas para editar as permissões para a aplicação que foi instalada quando o host foi criado.

> **Note**
>
> Você deve concluir essas etapas em sua instância do GitHub Enterprise Server e ser o proprietário da aplicação GitHub.

1. No GitHub Enterprise Server, na opção suspensa em sua foto de perfil, escolha Settings (Configurações).
2. Escolha Developer settings (Configurações do desenvolvedor) e, em seguida, GitHub Apps (Aplicações do GitHub).
3. Na lista de aplicações, escolha o nome da aplicação para sua conexão e escolha Permissions and events (Permissões e eventos) na exibição de configurações.
4. Em Organization permissions (Permissões da organização), em Members (Membros), escolha Read-only (Somente leitura) na lista suspensa Access (Acesso).



5. Em Add a note to users (Adicionar uma nota para os usuários), adicione uma descrição do motivo da atualização. Escolha Save changes (Salvar alterações).

Erro de conexão com o GitHub: “Ocorreu um problema, verifique se os cookies estão habilitados no seu navegador” ou “O proprietário da organização deve instalar a aplicação do GitHub”.

Problema:

Para criar a conexão para um repositório do GitHub, você deve ser o proprietário da organização do GitHub. Para repositórios que não estão em uma organização, você deve ser o proprietário do repositório. Quando uma conexão é criada por alguém que não seja o proprietário da organização, é criada uma solicitação para o proprietário da organização e um dos seguintes erros é exibido:

Ocorreu um problema, verifique se os cookies estão habilitados em seu navegador

OU

O proprietário da organização deve instalar a aplicação do GitHub

Correções possíveis: para repositórios em uma organização do GitHub, o proprietário da organização deve criar a conexão com o repositório do GitHub. Para repositórios que não estão em uma organização, você deve ser o proprietário do repositório.

Quero aumentar meus limites para conexões

É possível solicitar um aumento para determinados limites no AWS CodeStar Connections. Para obter mais informações, consulte Cotas para conexões.

Cotas para conexões

As seguintes tabelas listam as cotas (também chamadas de limites) para conexões no console do Developer Tools.

As cotas nesta tabela se aplicam por Região da AWS e podem ser aumentadas. Para solicitar um aumento, use o Console da Central de Suporte. Para obter mais informações sobre Região da AWS e cotas que podem ser alteradas, consulte AWS service quotas.

> **Note**
>
> É necessário habilitar a Região da AWS da Europa (Milão) para usá-la. Para obter mais informações, consulte Habilitar uma região.

Recurso	Limite padrão
Número máximo de conexões por Conta da AWS	250

As cotas na tabela são fixadas e não podem ser alteradas.

Recurso	Limite padrão
Máximo de caracteres nos nomes de conexões	32 caracteres
Número máximo de hosts por Conta da AWS	50
Número máximo de links de repositório	100
Número máximo de configurações de sincronização de pilha do AWS CloudFormation	100
Número máximo de configurações de sincronização por link de repositório	100
Número máximo de configurações de sincronização por ramificação	50

Endereços IP para adicionar à sua lista de permissões

Se você implementar a filtragem de IP ou permitir determinados endereços IP nas instâncias do Amazon EC2, adicione os endereços IP a seguir à sua lista de permissões. Isso permite conexões com provedores, como o GitHub Bitbucket.

A tabela a seguir lista os endereços IP para conexões no console do Developer Tools por Região da AWS.

> **Note**
>
> Para usar a região Europa (Milão), primeiro é necessário habilitá-la. Para obter mais informações, consulte Habilitar uma região.

Região	Endereços IP
Oeste dos EUA (Oregon) (us-west-2)	35.160.210.199, 54.71.206.108, 54.71.36.205
Leste dos EUA (Norte da Virgínia) (us-east-1)	3.216.216.90, 3.216.243.220, 3.217.241.85
Europa (Irlanda) (eu-west-1)	34.242.64.82, 52.18.37.201, 54.77.75.62
Leste dos EUA (Ohio) (us-east-2)	18.217.188.190, 18.218.158.91, 18.220.4.80
Ásia-Pacífico (Singapura) (ap-southeast-1)	18.138.171.151, 18.139.22.70, 3.1.157.176
Ásia-Pacífico (Sydney) (ap-southeast-2)	13.236.59.253, 52.64.166.86, 54.206.1.112
Ásia Pacific (Tóquio) (ap-northeast-1)	52.196.132.231, 54.95.133.227, 18.181.13.91
Europa (Frankfurt) (eu-central-1)	18.196.145.164, 3.121.252.59, 52.59.104.195
Ásia-Pacífico (Seul) (ap-northeast-2)	13.125.8.239, 13.209.223.177, 3.37.200.23
Ásia-Pacífico (Mumbai) (ap-south-1)	13.234.199.152, 13.235.29.220, 35.154.23 0.124
América do Sul (São Paulo) (sa-east-1)	18.229.77.26, 54.233.226.52, 54.233.207.69
Canadá (Central) (ca-central-1)	15.222.219.210, 35.182.166.138, 99.79.111 .198
Europa (Londres) (eu-west-2)	3.9.97.205, 35.177.150.185, 35.177.200.225

Região	Endereços IP
Oeste dos EUA (Norte da Califórnia) (us-west-1)	52.52.16.175, 52.8.63.87
Europa (Paris) (eu-west-3)	35.181.127.138, 35.181.145.22, 35.181.20.200
UE (Estocolmo) (eu-north-1)	13.48.66.148, 13.48.8.79, 13.53.78.182
UE (Milão) (eu-south-1)	18.102.28.105, 18.102.35.130, 18.102.8.116

Segurança de recursos do console do Developer Tools

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada 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 isto 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 de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos compliance programs AWS. Para saber mais sobre os programas de conformidade que se aplicam às AWS CodeStar notificações e AWS CodeStar conexões, consulte AWS Serviços no escopo por programa de conformidade.
- 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.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS CodeStar Notificações e AWS CodeStar Conexões. Os tópicos a seguir mostram como configurar AWS CodeStar notificações e AWS CodeStar conexões para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos de AWS CodeStar Notificações e AWS CodeStar Conexões.

Para obter mais informações sobre segurança dos serviços no console do Developer Tools, consulte:

- CodeBuild Segurança
- CodeCommit Segurança
- CodeDeploy Segurança
- CodePipeline Segurança

Noções básicas do conteúdo e da segurança das notificações

As notificações fornecem informações sobre recursos para os usuários inscritos nos destinos da regra de notificação que você configurar. Essas informações podem incluir detalhes sobre recursos do Developer Tools, incluindo conteúdo do repositório, status da compilação, status de implantação e execuções de pipeline.

Por exemplo, você pode configurar uma regra de notificação para um repositório CodeCommit para incluir comentários em commits ou pull requests. Se esse for o caso, as notificações enviadas em resposta a essa regra podem conter a linha ou as linhas de código às quais o comentário faz referência. Da mesma forma, você pode configurar uma regra de notificação para um projeto de compilação CodeBuild para incluir sucessos ou falhas em estados e fases de compilação. As notificações enviadas em resposta a essa regra conterão essas informações.

Você pode configurar uma regra de notificação para um pipeline CodePipeline para incluir informações sobre aprovações manuais, e as notificações enviadas em resposta a essa regra podem conter o nome da pessoa que fornece a aprovação. Você pode configurar uma regra de notificação para um aplicativo CodeDeploy para indicar o sucesso da implantação, e as notificações enviadas em resposta a essa regra podem conter informações sobre o destino da implantação.

As notificações podem incluir informações específicas ao projeto, como status de compilações, linhas de código que contêm comentários e aprovações de pipeline. Para ajudar a garantir a segurança do seu projeto, certifique-se de revisar regularmente os destinos das regras de notificação e a lista de assinantes dos tópicos do Amazon SNS especificados como destinos. Além disso, o conteúdo das notificações enviadas em resposta a eventos pode mudar à medida que recursos adicionais são adicionados aos serviços subjacentes. Essa alteração pode ocorrer sem aviso prévio para as regras de notificação já existentes. Considere revisar o conteúdo das mensagens de notificação periodicamente para ajudar a mantê-lo informado sobre o que está sendo enviado, bem como para quem está sendo enviado.

Para obter mais informações sobre os tipos de evento disponíveis para regras de notificação, consulte Conceitos de notificação.

Você pode optar por limitar os detalhes incluídos nas notificações apenas ao que está incluído em um evento. Isso é o que é chamado de tipo de detalhe Basic (Básico). Esses eventos contêm exatamente as mesmas informações enviadas à Amazon EventBridge e à Amazon CloudWatch Events.

Os serviços de console do Developer Tools CodeCommit, como, podem optar por adicionar informações sobre alguns ou todos os seus tipos de eventos nas mensagens de notificação além do que está disponível em um evento. Essas informações adicionais podem ser adicionadas a qualquer momento para aprimorar os tipos de eventos atuais ou complementar os tipos de eventos futuros. Você pode optar por incluir qualquer informação complementar sobre o evento, se disponível, na notificação, escolhendo o tipo de detalhe Full (Completo). Para ter mais informações, consulte Tipos de detalhes.

Proteção de dados no AWS CodeStar Notifications e no AWS CodeStar Connections

O modelo de responsabilidade compartilhada da AWS aplica-se à proteção de dados no AWS CodeStar Notifications e no AWS CodeStar Connections. Conforme descrito nesse modelo, AWS é responsável por proteger a infraestrutura global que executa todas as Nuvem AWS. Você é responsável por manter o controle sobre seu 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 Perguntas Frequentes sobre Privacidade de Dados.. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS LGPD e Modelo de Responsabilidade Compartilhada no AWSBlog de Segurança.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da Conta da AWS e configure as contas de usuário 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 [multi-factor authentication]) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e atividade do usuário logando com AWS CloudTrail.
- Use as soluções de criptografia AWS, juntamente com todos os controles de segurança padrão em 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 140-2 ao acessar AWS por meio de uma interface de linha de comando ou uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Padrão Federal de Processamento de Informações (Federal Information Processing Standard, ou FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de email dos seus clientes, em marcações ou campos de formato livre, como um campo Name. Isso também vale para o uso do AWS CodeStar Notifications e do AWS CodeStar Connections ou de outros Serviços da AWS com o console, a API, a AWS CLI ou os AWS SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais na URL para validar a solicitação a esse servidor.

Gerenciamento de identidade e acesso para AWS CodeStar notificações e AWS CodeStar conexões

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) a usar os recursos de AWS CodeStar Notificações e AWS CodeStar Conexões. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Solução de problemas de AWS CodeStar notificações e AWS CodeStar conexões: identidade e acesso
- Uso de funções vinculadas ao serviço para AWS CodeStar Notifications.
- Uso de funções vinculadas ao serviço do Conexões de código da AWS
- Políticas gerenciadas pela AWS para o Conexões de código da AWS

Público

A forma como você usa o AWS Identity and Access Management (IAM) é diferente, dependendo do trabalho que você faz em AWS CodeStar Notificações e AWS CodeStar Conexões.

Usuário do serviço — Se você usa o serviço de AWS CodeStar Notificações e AWS CodeStar Conexões para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões necessárias. À medida que você usa mais recursos de AWS CodeStar Notificações e AWS CodeStar Conexões para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso em AWS CodeStar Notificações e AWS CodeStar conexões, consulteSolução de problemas de AWS CodeStar notificações e AWS CodeStar conexões: identidade e acesso.

Administrador de serviços — Se você é responsável pelos recursos de AWS CodeStar Notificações e AWS CodeStar Conexões em sua empresa, provavelmente tem acesso total às AWS CodeStar Notificações e AWS CodeStar Conexões. É seu trabalho determinar quais recursos e recursos de AWS CodeStar Notificações e AWS CodeStar Conexões seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com AWS CodeStar notificações e AWS CodeStar conexões, consulteComo os recursos no console do Developer Tools funcionam com o IAM.

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso às AWS CodeStar notificações e AWS CodeStar conexões. Para ver exemplos de políticas baseadas em identidade de AWS CodeStar Notificações e AWS CodeStar Conexões que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade

Autenticando 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 uma 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 em 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 assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça 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 AWS IAM Identity Center do usuário. Usar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Usuário raiz da conta da AWS

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 pode 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.

Grupos e usuários 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, recomendamos depender de 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, recomendamos alternar as chaves de acesso. Para mais informações, consulte Alterne 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 IAMAdmins e atribuir 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 Quando criar um usuário do IAM (em vez de um perfil) 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. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM 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, você pode 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 pelo mesmo. Para mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM

Identity Center 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 assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: você pode usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) acesse recursos na sua conta de uma conta diferente. 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 saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em recurso 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 aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de 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 Encaminhar sessões de acesso.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para 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 assumir 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 pode editar as permissões para perfis vinculados ao serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciamento do 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 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 funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a 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 funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de política do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais 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.

Como os recursos no console do Developer Tools funcionam com o IAM

Antes de usar o IAM para gerenciar o acesso a recursos no console do Developer Tools, você deve entender quais recursos do IAM estão disponíveis para uso com ele. Para ter uma visão de alto nível de como as notificações e outros AWS serviços funcionam com o IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Tópicos

- Políticas baseadas em identidade no console do Developer Tools.
- AWS CodeStar Políticas baseadas em recursos de notificações e AWS CodeStar conexões
- Autorização baseada em tags do
- Perfis do IAM

Políticas baseadas em identidade no console do Developer Tools.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. AWS CodeStar Notificações e AWS CodeStar conexões oferecem suporte a ações, recursos e chaves de condição específicos. Para saber mais sobre todos os elementos usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

Ações

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 você pode usar 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. Há também algumas operações que 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.

As ações de política para notificações no console do Developer Tools usam o seguinte prefixo antes da ação: `codestar-notifications and codestar-connections`. Por exemplo, para conceder permissão a alguém para visualizar todas as regras de notificação em sua conta, inclua a `codestar-notifications:ListNotificationRules` ação na política relacionada. As declarações de política devem incluir um `NotAction` elemento `Action` ou. AWS CodeStar Notificações e AWS CodeStar conexões definem seu próprio conjunto de ações que descrevem as tarefas que você pode executar com esse serviço.

Para especificar várias ações de AWS CodeStar Notificações em uma única instrução, separe-as com vírgulas da seguinte maneira.

```
"Action": [
      "codestar-notifications:action1",
      "codestar-notifications:action2"
```

Para especificar várias Conexões de código da AWS ações em uma única declaração, separe-as com vírgulas da seguinte maneira.

```
"Action": [
      "codestar-connections:action1",
      "codestar-connections:action2"
```

Você também pode especificar várias ações utilizando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `List`, inclua a ação a seguir:

```
"Action": "codestar-notifications:List*"
```

AWS CodeStar As ações da API de notificações incluem:

- `CreateNotificationRule`

- DeleteNotificationRule
- DeleteTarget
- DescribeNotificationRule
- ListEventTypes
- ListNotificationRules
- ListTagsForResource
- ListTargets
- Subscribe
- TagResource
- Unsubscribe
- UntagResource
- UpdateNotificationRule

Conexões de código da AWS As ações da API incluem o seguinte:

- CreateConnection
- DeleteConnection
- GetConnection
- ListConnections
- ListTagsForResource
- TagResource
- UntagResource

As seguintes ações somente de permissões são necessárias Conexões de código da AWS para concluir o handshake de autenticação:

- GetIndividualAccessToken
- GetInstallationUrl
- ListInstallationTargets
- StartOAuthHandshake
- UpdateConnectionInstallation

A seguinte ação somente de permissões é necessária Conexões de código da AWS para usar uma conexão:

- `UseConnection`

A seguinte ação somente de permissões é necessária Conexões de código da AWS para transmitir uma conexão a um serviço:

- `PassConnection`

Para ver uma lista de ações de AWS CodeStar notificações e AWS CodeStar conexões, consulte Ações definidas por AWS CodeStar notificações e Ações definidas por AWS CodeStar conexões no Guia do usuário do IAM.

Recursos

AWS CodeStar Notificações e AWS CodeStar conexões não oferecem suporte à especificação de ARNs de recursos em uma política.

Chaves de condição

AWS CodeStar As notificações e AWS CodeStar conexões definem seus próprios conjuntos de chaves de condição e também oferecem suporte ao uso de algumas chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Todas as ações de AWS CodeStar notificações oferecem suporte à chave de `codestar-notifications:NotificationsForResource` condição. Para ter mais informações, consulte Exemplos de políticas baseadas em identidade.

Conexões de código da AWS defina as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter mais informações, consulte Conexões de código da AWS referência de permissões.

Chaves de condição	Descrição
`codestar-connections:BranchName`	Filtra o acesso pelo nome da ramificação do repositório de terceiros.

Chaves de condição	Descrição
`codestar-connections:FullRepositoryId`	Filtra o acesso pelo repositório que é passado na solicitação. Aplica-se somente a solicitações `UseConnection` para acesso a um repositório específico
`codestar-connections:InstallationId`	Filtra o acesso pelo ID de terceiros (como o ID de instalação da aplicação Bitbucket) que é usado para atualizar uma conexão. Permite restringir quais instalações de aplicações de terceiros podem ser usadas para estabelecer uma conexão
`codestar-connections:OwnerId`	Filtra o acesso pelo proprietário ou ID da conta do provedor de terceiros
`codestar-connections:PassedToService`	Filtra o acesso pelo serviço ao qual o principal tem permissão para passar uma conexão
`codestar-connections:ProviderAction`	Filtra o acesso pela ação do provedor em uma solicitação `UseConnection` , como `ListRepositories` .
`codestar-connections:ProviderPermissionsRequired`	Filtra o acesso pelo tipo de permissões de provedor de terceiros
`codestar-connections:ProviderType`	Filtra o acesso pelo tipo de provedor de terceiros passado na solicitação
`codestar-connections:ProviderTypeFilter`	Filtra o acesso pelo tipo de provedor de terceiros usado para filtrar resultados
`codestar-connections:RepositoryName`	Filtra o acesso pelo nome do repositório de terceiros.

Exemplos

Para ver exemplos de políticas baseadas em identidade de AWS CodeStar Notificações e AWS CodeStar Conexões, consulte. Exemplos de políticas baseadas em identidade

AWS CodeStar Políticas baseadas em recursos de notificações e AWS CodeStar conexões

AWS CodeStar Notificações e AWS CodeStar conexões não oferecem suporte a políticas baseadas em recursos.

Autorização baseada em tags do

Você pode anexar tags aos recursos de AWS CodeStar Notificações e AWS CodeStar Conexões ou passar tags em uma solicitação. Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as chaves de condição `codestar-notifications and codestar-connections:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`. Para obter mais informações sobre estratégias de marcação, consulte Recursos de marcação AWS. Para obter mais informações sobre a marcação de recursos de AWS CodeStar notificações e AWS CodeStar conexões, consulteRecursos de conexões de tags.

Para visualizar exemplos de políticas baseadas em identidade para limitar o acesso a um recurso baseado em tags desse recurso, consulte Usando tags para controlar o acesso aos recursos do AWS CodeStar Connections.

Perfis do IAM

Uma função do IAM é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usar credenciais temporárias

Você pode usar credenciais temporárias para fazer login com federação e assumir uma função do IAM ou uma função entre contas. Você obtém credenciais de segurança temporárias chamando operações de AWS STS API, como AssumeRoleou GetFederationToken.

AWS CodeStar Notificações e AWS CodeStar conexões oferecem suporte ao uso de credenciais temporárias.

Perfis vinculados ao serviço

As funções vinculadas ao serviço permitem que AWS os serviços acessem recursos em outros serviços para concluir uma ação em seu nome. Os perfis vinculados a serviço aparecem na sua

conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados a serviço.

AWS CodeStar As notificações oferecem suporte a funções vinculadas a serviços. Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço de AWS CodeStar Notificações e AWS CodeStar Conexões, consulte. Uso de funções vinculadas ao serviço para AWS CodeStar Notifications.

AWS CodeStar O Connections não oferece suporte a funções vinculadas a serviços.

Conexões de código da AWS referência de permissões

As tabelas a seguir listam cada operação de Conexões de código da AWS API, as ações correspondentes para as quais você pode conceder permissões e o formato do ARN do recurso a ser usado para conceder permissões. As Conexões de código da AWS APIs são agrupadas em tabelas com base no escopo das ações permitidas por essa API. Consulte-o ao escrever políticas de permissões que você pode anexar a uma identidade do IAM (políticas baseadas em identidade).

Quando você cria uma política de permissões, você especifica as ações no campo `Action` da política. Você especifica o valor do recurso no campo `Resource` da política como um ARN, com ou sem um caractere curinga (*).

Para expressar condições nas suas políticas de conexão, use as chaves de condição descritas aqui e listadas em Chaves de condição. Você também pode usar teclas de condição AWS-wide. Para obter uma lista completa AWS de chaves gerais, consulte Chaves disponíveis no Guia do usuário do IAM.

Para especificar uma ação, use o `codestar-connections:` prefixo seguido do nome da operação da API (por exemplo, `codestar-connections:ListConnections` ou `codestar-connections:CreateConnection`).

Uso de curingas

Para especificar várias ações ou recursos, use um caractere curinga (*) no seu ARN. Por exemplo, `codestar-connections:*` especifica todas as Conexões de código da AWS ações e `codestar-connections:Get*` especifica todas as Conexões de código da AWS ações que começam com a palavra. `Get` O exemplo a seguir concede acesso a todos os repositórios com nomes que começam com `MyConnection`.

```
arn:aws:codestar-connections:us-west-2:account-ID:connection/*
```

Você pode usar curingas apenas com os recursos de *conexão* listados na tabela a seguir. Você não pode usar curingas com recursos *region* ou *account-id*. Para obter mais informações sobre curingas, consulte Identificadores do IAM, no Manual do usuário do IAM.

Tópicos

Permissões para gerenciar conexões

Uma função ou usuário designado para usar o SDK AWS CLI ou para visualizar, criar ou excluir conexões deve ter permissões limitadas ao seguinte.

> **Note**
>
> Não é possível concluir nem usar uma conexão no console somente com as permissões a seguir. É necessário adicionar as permissões em Permissões para concluir conexões.

```
codestar-connections:CreateConnection
codestar-connections:DeleteConnection
codestar-connections:GetConnection
codestar-connections:ListConnections
```

AWS CodeStar Notificações e AWS CodeStar conexões exigiam permissões para ações de gerenciamento de conexões

CreateConnection

Ação/Ações: `codestar-connections:CreateConnection`

Necessária para usar a CLI ou o console para criar uma conexão.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

DeleteConnection

Ação/Ações: `codestar-connections:DeleteConnection`

Necessária para usar a CLI ou o console para excluir uma conexão.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetConnection

Ação/Ações: `codestar-connections:GetConnection`

Necessária para usar a CLI ou o console para visualizar detalhes de uma conexão.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListConnections

Ação/Ações: `codestar-connections:ListConnections`

Necessária para usar a CLI ou o console para listar todas as conexões na conta.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Estas operações oferecem suporte às seguintes chaves de condição:

Ação	Chaves de condição
`codestar-connections:CreateConnection`	`codestar-connections:ProviderType`

Ação	Chaves de condição
`codestar-connections:DeleteConnection`	N/D
`codestar-connections:GetConnection`	N/D
`codestar-connections:ListConnections`	`codestar-connections:ProviderTypeFilter`

Permissões para gerenciamento de hosts

Uma função ou usuário designado para usar o SDK AWS CLI ou para visualizar, criar ou excluir hosts deve ter permissões limitadas ao seguinte.

> **Note**
>
> Não é possível concluir nem usar uma conexão no host somente com as permissões a seguir. É necessário adicionar as permissões em Permissões para configurar hosts.

```
codestar-connections:CreateHost
codestar-connections:DeleteHost
codestar-connections:GetHost
codestar-connections:ListHosts
```

AWS CodeStar Notificações e AWS CodeStar conexões exigiam permissões para ações de gerenciamento de hosts

CreateHost

Ação/Ações: `codestar-connections:CreateHost`

Necessária para usar a CLI ou o console para criar um host.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

DeleteHost

Ação/Ações: `codestar-connections:DeleteHost`

Necessária para usar a CLI ou o console para excluir um host.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

GetHost

Ação/Ações: `codestar-connections:GetHost`

Necessária para usar a CLI ou o console para visualizar detalhes de um host.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

ListHosts

Ação/Ações: `codestar-connections:ListHosts`

Necessária para usar a CLI ou o console para listar todos os hosts na conta.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

Estas operações oferecem suporte às seguintes chaves de condição:

Ação	Chaves de condição
`codestar-connections:CreateHost`	`codestar-connections:ProviderType`
`codestar-connections:DeleteHost`	N/D
`codestar-connections:GetHost`	N/D
`codestar-connections:ListHosts`	`codestar-connections:ProviderTypeFilter`

Permissões para concluir conexões

Uma função ou um usuário designado para gerenciar conexões no console deve ter as permissões necessárias para concluir uma conexão no console e criar uma instalação, o que inclui autorizar o

handshake para o provedor e criar instalações para conexões a serem usadas. Use as permissões a seguir além das permissões acima.

As seguintes operações do IAM são usadas pelo console ao executar um handshake baseado em navegador. `ListInstallationTargets`, `GetInstallationUrl`, `StartOAuthHandshake`, `UpdateConnectionInstallation` e `GetIndividualAccessToken` são permissões de políticas do IAM. Elas não são ações de API.

```
codestar-connections:GetIndividualAccessToken
codestar-connections:GetInstallationUrl
codestar-connections:ListInstallationTargets
codestar-connections:StartOAuthHandshake
codestar-connections:UpdateConnectionInstallation
```

Com base nisso, as permissões a seguir são necessárias para usar, criar, atualizar ou excluir uma conexão no console.

```
codestar-connections:CreateConnection
codestar-connections:DeleteConnection
codestar-connections:GetConnection
codestar-connections:ListConnections
codestar-connections:UseConnection
codestar-connections:ListInstallationTargets
codestar-connections:GetInstallationUrl
codestar-connections:StartOAuthHandshake
codestar-connections:UpdateConnectionInstallation
codestar-connections:GetIndividualAccessToken
```

Conexões de código da AWS permissões necessárias para ações para concluir conexões

GetIndividualAccessToken

Ação/Ações: `codestar-connections:GetIndividualAccessToken`

Necessária para usar o console para concluir a conexão. Esta é apenas uma permissão de política do IAM, e não uma ação de API.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetInstallationUrl

Ação/Ações: `codestar-connections:GetInstallationUrl`

Necessária para usar o console para concluir a conexão. Esta é apenas uma permissão de política do IAM, e não uma ação de API.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListInstallationTargets

Ação/Ações: `codestar-connections:ListInstallationTargets`

Necessária para usar o console para concluir a conexão. Esta é apenas uma permissão de política do IAM, e não uma ação de API.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Iniciar para AuthHandshake

Ação/Ações: `codestar-connections:StartOAuthHandshake`

Necessária para usar o console para concluir a conexão. Esta é apenas uma permissão de política do IAM, e não uma ação de API.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

UpdateConnectionInstallation

Ação/Ações: `codestar-connections:UpdateConnectionInstallation`

Necessária para usar o console para concluir a conexão. Esta é apenas uma permissão de política do IAM, e não uma ação de API.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Estas operações oferecem suporte às chaves de condição a seguir.

Ação	Chaves de condição
codestar-connections:GetIndividualAccessToken	codestar-connections:ProviderType
codestar-connections:GetInstallationUrl	codestar-connections:ProviderType
codestar-connections:ListInstallationTargets	N/D
codestar-connections:StartOAuthHandshake	codestar-connections:ProviderType
codestar-connections:UpdateConnectionInstallation	codestar-connections:InstallationId

Permissões para configurar hosts

Uma função ou um usuário designado para gerenciar conexões no console deve ter as permissões necessárias para concluir uma conexão no console, o que inclui autorizar o handshake para o provedor e instalar a aplicação host. Use as permissões a seguir além das permissões para hosts acima.

As seguintes operações do IAM são usadas pelo console ao executar um registro de host baseado em navegador. `RegisterAppCode` e `StartAppRegistrationHandshake` são permissões de políticas do IAM. Elas não são ações de API.

```
codestar-connections:RegisterAppCode
codestar-connections:StartAppRegistrationHandshake
```

Com base nisso, as permissões a seguir são necessárias para usar, criar, atualizar ou excluir uma conexão no console que requer um host (como os tipos de provedor instalados).

```
codestar-connections:CreateConnection
codestar-connections:DeleteConnection
codestar-connections:GetConnection
codestar-connections:ListConnections
```

```
codestar-connections:UseConnection
codestar-connections:ListInstallationTargets
codestar-connections:GetInstallationUrl
codestar-connections:StartOAuthHandshake
codestar-connections:UpdateConnectionInstallation
codestar-connections:GetIndividualAccessToken
codestar-connections:RegisterAppCode
codestar-connections:StartAppRegistrationHandshake
```

Conexões de código da AWS permissões necessárias para ações para concluir a configuração do host

RegisterAppCode

Ação/Ações: `codestar-connections:RegisterAppCode`

Necessária para usar o console para concluir a configuração do host. Esta é apenas uma permissão de política do IAM, e não uma ação de API.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

StartAppRegistrationHandshake

Ação/Ações: `codestar-connections:StartAppRegistrationHandshake`

Necessária para usar o console para concluir a configuração do host. Esta é apenas uma permissão de política do IAM, e não uma ação de API.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

Estas operações oferecem suporte às chaves de condição a seguir.

Transmitir uma conexão para um serviço

Quando uma conexão é passada para um serviço (por exemplo, quando um ARN de conexão é fornecido em uma definição de pipeline para criar ou atualizar um pipeline), o usuário deve ter a `codestar-connections:PassConnection` permissão.

Conexões de código da AWS permissões necessárias para passar uma conexão

PassConnection

Ação/Ações: `codestar-connections:PassConnection`

Necessária para passar uma conexão para um serviço.

Recurso:`arn:aws:codestar-connections:`*region*`:`*account-id*`:connection/`*connection-id*

Esta operação também é compatível com a seguinte chave de condição:

- `codestar-connections:PassedToService`

Valores compatíveis com chaves de condição

Chave	Provedores de ação válidos
`codestar-connections:PassedToService`	• `codeguru-reviewer` • `codepipeline.amazonaws.com` • `proton.amazonaws.com`

Usar uma conexão

Quando um serviço como CodePipeline usa uma conexão, a função de serviço deve ter a `codestar-connections:UseConnection` permissão para uma determinada conexão.

Para gerenciar conexões no console, a política do usuário deve ter a permissão `codestar-connections:UseConnection`.

Conexões de código da AWS ação necessária para usar uma conexão

UseConnection

Ação/Ações: `codestar-connections:UseConnection`

Necessária para usar uma conexão.

Recurso:`arn:aws:codestar-connections:`*region*`:`*account-id*`:connection/`*connection-id*

Esta operação também é compatível com as seguintes chaves de condição:

- `codestar-connections:BranchName`

- codestar-connections:FullRepositoryId
- codestar-connections:OwnerId
- codestar-connections:ProviderAction
- codestar-connections:ProviderPermissionsRequired
- codestar-connections:RepositoryName

Valores compatíveis com chaves de condição

Chave	Provedores de ação válidos
codestar-connections:FullRepositoryId	O nome do usuário e o nome de um repositório, como my-owner/my-repository . Compatível somente quando a conexão está sendo usada para acessar um repositório específico.
codestar-connections:ProviderPermissionsRequired	read_only ou read_write
codestar-connections:ProviderAction	GetBranch , ListRepositories , ListOwners , ListBranches , StartUploadArchiveToS3 , GitPush, GitPull, GetUploadArchiveToS3Status , CreatePullRequestDiffComment , GetPullRequest , ListBranchCommits , ListCommitFiles , ListPullRequestComments , ListPullRequestCommits . Para obter mais informações, consulte a próxima seção.

As chaves de condição necessárias para algumas funcionalidades podem mudar ao longo do tempo. Recomendamos que você use codestar-connections:UseConnection para controlar o acesso a uma conexão, a menos que seus requisitos de controle de acesso exijam permissões diferentes.

Tipos de acesso suportados para **`ProviderAction`**

Quando uma conexão é usada por um AWS serviço, isso resulta na realização de chamadas de API para seu provedor de código-fonte. Por exemplo, um serviço pode listar repositórios para uma conexão Bitbucket chamando a `https://api.bitbucket.org/2.0/repositories/`*`username`* API.

A `ProviderAction` chave de condição permite restringir quais APIs em um provedor podem ser chamadas. Como o caminho da API pode ser gerado dinamicamente e o caminho varia de provedor para provedor, o valor `ProviderAction` é mapeado em um nome de ação abstrata em vez do URL da API. Isso permite que você escreva políticas que têm o mesmo efeito, independentemente do tipo de provedor para a conexão.

A seguir estão os tipos de acesso concedidos para cada um dos valores `ProviderAction` compatíveis: A seguir são mostradas permissões de políticas do IAM. Elas não são ações de API.

Conexões de código da AWS tipos de acesso suportados para **`ProviderAction`**

GetBranch

Ação/Ações: `codestar-connections:GetBranch`

Necessária para acessar informações sobre uma ramificação, como a confirmação mais recente para essa ramificação

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListRepositories

Ação/Ações: `codestar-connections:ListRepositories`

Necessária para acessar uma lista de repositórios públicos e privados, incluindo detalhes sobre esses repositórios, que pertencem a um proprietário.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListOwners

Ação/Ações: `codestar-connections:ListOwners`

Necessária para acessar uma lista de proprietários aos quais a conexão tem acesso.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListBranches

Ação/Ações: `codestar-connections:ListBranches`

Necessária para acessar a lista de ramificações que existem em um determinado repositório.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

StartUploadArchiveToS3

Ação/Ações: `codestar-connections:StartUploadArchiveToS3`

Necessária para ler o código-fonte e fazer seu upload para o Amazon S3.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GitPush

Ação/Ações: `codestar-connections:GitPush`

Necessária para gravar em um repositório usando o Git.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GitPull

Ação/Ações: `codestar-connections:GitPull`

Necessária para ler de um repositório usando o Git.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetUploadArchiveToStatus do S3

Ação/Ações: `codestar-connections:GetUploadArchiveToS3Status`

Necessária para acessar o status de um upload, incluindo quaisquer mensagens de erro, iniciado por `StartUploadArchiveToS3`.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

CreatePullRequestDiffComment

Ação/Ações: `codestar-connections:CreatePullRequestDiffComment`

Necessária para acessar comentários em uma solicitação pull.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetPullRequest

Ação/Ações: `codestar-connections:GetPullRequest`

Necessária para visualizar solicitações pull para um repositório.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListBranchCommits

Ação/Ações: `codestar-connections:ListBranchCommits`

Necessária para visualizar uma lista de confirmações para uma ramificação de repositório.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListCommitFiles

Ação/Ações: `codestar-connections:ListCommitFiles`

Necessária para visualizar uma lista de arquivos para uma confirmação.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListPullRequestComments

Ação/Ações: `codestar-connections:ListPullRequestComments`

Necessária para visualizar uma lista de comentários para uma solicitação pull.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListPullRequestCommits

Ação/Ações: `codestar-connections:ListPullRequestCommits`

Necessária para visualizar uma lista de confirmações para uma solicitação pull.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Permissões compatíveis para marcar recursos de conexão

As operações do IAM a seguir são usadas na marcação de recursos de conexão.

```
codestar-connections:ListTagsForResource
codestar-connections:TagResource
codestar-connections:UntagResource
```

Conexões de código da AWS ações necessárias para marcar recursos de conexão

ListTagsForResource

Ação/Ações: `codestar-connections:ListTagsForResource`

Necessária para visualizar uma lista de tags associadas ao recurso de conexão.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*, `arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

TagResource

Ação/Ações: `codestar-connections:TagResource`

Necessária para marcar um recurso de conexão.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*, `arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

UntagResource

Ação/Ações: `codestar-connections:UntagResource`

Necessária para remover tags de um recurso de conexão.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*, `arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

Transmitir uma conexão a um link de repositório

Quando um link de repositório é fornecido em uma configuração de sincronização, o usuário deve ter a permissão `codestar-connections:PassRepository` para o ARN/recurso do link de repositório.

Conexões de código da AWS permissões necessárias para passar uma conexão

PassRepository

Ação/Ações: `codestar-connections:PassRepository`

Necessário para transmitir um link de repositório para uma configuração de sincronização.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:repository-link/`*`repository-link-id`*

Esta operação também é compatível com a seguinte chave de condição:

- `codestar-connections:PassedToService`

Valores compatíveis com chaves de condição

Chave	Provedores de ação válidos
`codestar-connections:PassedToService`	• `cloudformation.sync.codeconnections.amazonaws.com`

Chave de condição compatível para links de repositório

As operações para links de repositório e recursos de configuração de sincronização são compatíveis com a seguinte chave de condição:

- `codestar-connections:Branch`

  Filtra o acesso pelo nome da ramificação que é passado na solicitação.

Ações compatíveis com a chave de condição

Chave	Valores válidos
`codestar-connections:Branch`	As seguintes ações são compatíveis com essa chave de condição: • CreateSyncConfiguration • UpdateSyncConfiguration • GetRepositorySyncStatus

Exemplos de políticas baseadas em identidade

Por padrão, os usuários e funções do IAM que têm uma das políticas gerenciadas para AWS CodeCommit AWS CodeBuild AWS CodeDeploy,, ou AWS CodePipeline aplicada têm permissões para conexões, notificações e regras de notificação que se alinham à intenção dessas políticas. Por exemplo, usuários ou funções do IAM que têm uma das políticas de acesso total (AWSCodeCommitFullAccessAWSCodeBuildAdminAccess, AWSCodeDeployFullAccess, ou AWSCodePipeline_FullAccess) aplicada a eles também têm acesso total às notificações e às regras de notificação criadas para os recursos desses serviços.

Outros usuários e funções do IAM não têm permissão para criar ou modificar recursos de AWS CodeStar Notificações e AWS CodeStar Conexões. Eles também não podem realizar tarefas usando a AWS API AWS Management Console AWS CLI, ou. Um administrador do IAM deve criar políticas do IAM que concedam a usuários e funções permissão para executar operações da API nos recursos necessários especificados. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

Permissões e exemplos de AWS CodeStar notificações

As declarações e exemplos de políticas a seguir podem ajudar você a gerenciar AWS CodeStar as notificações.

Permissões relacionadas a notificações em políticas gerenciadas de acesso total

As políticas AWSCodeCommitFullAccessAWSCodeBuildAdminAccess, AWSCodeDeployFullAccess, e AWSCodePipeline_FullAccessgerenciadas incluem as seguintes declarações para permitir acesso total às notificações no console do Developer Tools. Os usuários com uma dessas políticas gerenciadas aplicadas também podem criar e gerenciar tópicos do Amazon SNS para notificações, inscrever e cancelar a inscrição de usuários em tópicos e listar tópicos para escolher como destinos para regras de notificação.

> **Note**
>
> Na política gerenciada, a chave de condição `codestar-notifications:NotificationsForResource` terá um valor específico para o tipo de recurso do serviço. Por exemplo, na política de acesso total para CodeCommit, o valor `éarn:aws:codecommit:*`.

```
    {
        "Sid": "CodeStarNotificationsReadWriteAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:CreateNotificationRule",
            "codestar-notifications:DescribeNotificationRule",
            "codestar-notifications:UpdateNotificationRule",
            "codestar-notifications:DeleteNotificationRule",
            "codestar-notifications:Subscribe",
            "codestar-notifications:Unsubscribe"
        ],
        "Resource": "*",
        "Condition" : {
            "StringLike" : {"codestar-notifications:NotificationsForResource" :
"arn:aws:<vendor-code>:*"}
        }
    },
    {
        "Sid": "CodeStarNotificationsListAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:ListNotificationRules",
            "codestar-notifications:ListTargets",
            "codestar-notifications:ListTagsforResource",
```

```
            "codestar-notifications:ListEventTypes"
        ],
        "Resource": "*"
    },
    {
        "Sid": "CodeStarNotificationsSNSTopicCreateAccess",
        "Effect": "Allow",
        "Action": [
            "sns:CreateTopic",
            "sns:SetTopicAttributes"
        ],
        "Resource": "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
        "Sid": "SNSTopicListAccess",
        "Effect": "Allow",
        "Action": [
            "sns:ListTopics"
        ],
        "Resource": "*"
    },
    {
        "Sid": "CodeStarNotificationsChatbotAccess",
        "Effect": "Allow",
        "Action": [
            "chatbot:DescribeSlackChannelConfigurations",
            "chatbot:ListMicrosoftTeamsChannelConfigurations"
          ],
       "Resource": "*"
    }
```

Permissões relacionadas a notificações em políticas gerenciadas somente leitura

As políticas AWSCodeCommitReadOnlyAccessAWSCodeBuildReadOnlyAccess,, AWSCodeDeployReadOnlyAccess, e AWSCodePipeline_ReadOnlyAccessgerenciadas incluem as seguintes declarações para permitir acesso somente para leitura às notificações. Por exemplo, elas podem exibir notificações de recursos no console do Developer Tools, mas não podem criar, gerenciar ou se inscrever neles.

> **Note**
>
> Na política gerenciada, a chave de condição `codestar-notifications:NotificationsForResource` terá um valor específico para o tipo de recurso do serviço. Por exemplo, na política de acesso total para CodeCommit, o valor é `arn:aws:codecommit:*`.

```
  {
       "Sid": "CodeStarNotificationsPowerUserAccess",
       "Effect": "Allow",
       "Action": [
           "codestar-notifications:DescribeNotificationRule"
       ],
       "Resource": "*",
       "Condition" : {
           "StringLike" : {"codestar-notifications:NotificationsForResource" :
"arn:aws:<vendor-code>:*"}
       }
   },
   {
       "Sid": "CodeStarNotificationsListAccess",
       "Effect": "Allow",
       "Action": [
           "codestar-notifications:ListNotificationRules",
           "codestar-notifications:ListEventTypes",
           "codestar-notifications:ListTargets"
       ],
       "Resource": "*"
   }
```

Permissões relacionadas a notificações em outras políticas gerenciadas

As políticas AWSCodeBuildDeveloperAccessgerenciadas AWSCodeCommitPowerUserAWSCodeBuildDeveloperAccess,, e incluem as seguintes declarações para permitir que os desenvolvedores com uma dessas políticas gerenciadas aplicadas criem, editem e assinem notificações. Elas não podem excluir regras de notificação ou gerenciar tags para recursos.

> **Note**
>
> Na política gerenciada, a chave de condição `codestar-notifications:NotificationsForResource` terá um valor específico para o tipo de recurso do serviço. Por exemplo, na política de acesso total para CodeCommit, o valor é `arn:aws:codecommit:*`.

```
    {
        "Sid": "CodeStarNotificationsReadWriteAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:CreateNotificationRule",
            "codestar-notifications:DescribeNotificationRule",
            "codestar-notifications:UpdateNotificationRule",
            "codestar-notifications:Subscribe",
            "codestar-notifications:Unsubscribe"
        ],
        "Resource": "*",
        "Condition" : {
            "StringLike" : {"codestar-notifications:NotificationsForResource" :
"arn:aws:<vendor-code>:*"}
        }
    },
    {
        "Sid": "CodeStarNotificationsListAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:ListNotificationRules",
            "codestar-notifications:ListTargets",
            "codestar-notifications:ListTagsforResource",
            "codestar-notifications:ListEventTypes"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SNSTopicListAccess",
        "Effect": "Allow",
        "Action": [
            "sns:ListTopics"
        ],
        "Resource": "*"
```

```
    },
    {
        "Sid": "CodeStarNotificationsChatbotAccess",
        "Effect": "Allow",
        "Action": [
            "chatbot:DescribeSlackChannelConfigurations",
            "chatbot:ListMicrosoftTeamsChannelConfigurations"
          ],
       "Resource": "*"
    }
```

Exemplo: uma política em nível de administrador para gerenciar notificações AWS CodeStar

Neste exemplo, você quer conceder a um usuário do IAM em sua AWS conta acesso total às AWS CodeStar notificações para que o usuário possa revisar os detalhes das regras de notificação e listar as regras de notificação, os alvos e os tipos de eventos. Você também deseja permitir que o usuário adicione, atualize e exclua regras de notificação. Essa é uma política de acesso total, equivalente às permissões de notificação incluídas como parte das políticas AWSCodeBuildAdminAccess, AWSCodeCommitFullAccess, AWSCodeDeployFullAccess, e AWSCodePipeline_FullAccessgerenciadas. Como essas políticas gerenciadas, você só deve anexar esse tipo de declaração de política a usuários, grupos ou funções do IAM que exijam acesso administrativo total às notificações e regras de notificação em toda a sua AWS conta.

> **Note**
>
> Essa política contém a permissão `CreateNotificationRule`. Qualquer usuário com essa política aplicada ao usuário ou função do IAM poderá criar regras de notificação para todo e qualquer tipo de recurso suportado pelas AWS CodeStar notificações na AWS conta, mesmo que esse usuário não tenha acesso a esses recursos por si só. Por exemplo, um usuário com essa política pode criar uma regra de notificação para um CodeCommit repositório sem ter permissões para acessar a CodeCommit si mesmo.

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

```
            "codestar-notifications:CreateNotificationRule",
            "codestar-notifications:DeleteNotificationRule",
            "codestar-notifications:DescribeNotificationRule",
            "codestar-notifications:ListNotificationRules",
            "codestar-notifications:UpdateNotificationRule",
            "codestar-notifications:Subscribe",
            "codestar-notifications:Unsubscribe",
            "codestar-notifications:DeleteTarget",
            "codestar-notifications:ListTargets",
            "codestar-notifications:ListTagsforResource",
            "codestar-notifications:TagResource",
            "codestar-notifications:UntagResource"
        ],
        "Resource": "*"
      }
   ]
}
```

Exemplo: uma política em nível de colaborador para o uso de notificações AWS CodeStar

Neste exemplo, você deseja conceder acesso ao day-to-day uso de AWS CodeStar notificações, como criar e assinar notificações, mas não a ações mais destrutivas, como excluir regras ou alvos de notificação. Isso equivale ao acesso fornecido nas políticas AWSCodeCommitPowerUsergerenciadas AWSCodeBuildDeveloperAccessAWSCodeDeployDeveloperAccess, e.

> **Note**
>
> Essa política contém a permissão `CreateNotificationRule`. Qualquer usuário com essa política aplicada ao usuário ou função do IAM poderá criar regras de notificação para todo e qualquer tipo de recurso suportado pelas AWS CodeStar notificações na AWS conta, mesmo que esse usuário não tenha acesso a esses recursos por si só. Por exemplo, um usuário com essa política pode criar uma regra de notificação para um CodeCommit repositório sem ter permissões para acessar a CodeCommit si mesmo.

```
{
    "Version": "2012-10-17",
    "Sid": "AWSCodeStarNotificationsPowerUserAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-notifications:CreateNotificationRule",
```

```
            "codestar-notifications:DescribeNotificationRule",
            "codestar-notifications:ListNotificationRules",
            "codestar-notifications:UpdateNotificationRule",
            "codestar-notifications:Subscribe",
            "codestar-notifications:Unsubscribe",
            "codestar-notifications:ListTargets",
            "codestar-notifications:ListTagsforResource"
        ],
        "Resource": "*"
        }
    ]
}
```

Exemplo: uma read-only-level política para o uso de AWS CodeStar notificações

Neste exemplo, você deseja conceder a um usuário do IAM em sua conta acesso somente leitura a regras de notificação, destinos e tipos de evento em sua conta da AWS . Este exemplo mostra como você pode criar uma política que permite visualizar esses itens. Isso equivale às permissões incluídas como parte das AWSCodeBuildReadOnlyAccesspolíticas AWSCodePipeline_ReadOnlyAccessgerenciadas e. AWSCodeCommitReadOnly

```
{
    "Version": "2012-10-17",
    "Id": "CodeNotification__ReadOnly",
    "Statement": [
        {
            "Sid": "Reads_API_Access",
            "Effect": "Allow",
            "Action": [
                "CodeNotification:DescribeNotificationRule",
                "CodeNotification:ListNotificationRules",
                "CodeNotification:ListTargets",
                "CodeNotification:ListEventTypes"
            ],
            "Resource": "*"
        }
    ]
}
```

Permissões e exemplos para Conexões de código da AWS

As declarações de políticas e os exemplos a seguir podem ajudar você a gerenciar o Conexões de código da AWS.

Para obter informações sobre como criar uma política baseada em identidade do IAM usando esses documentos de política JSON de exemplo, consulte Criação de políticas na guia JSON no Manual do usuário do IAM.

Exemplo: uma política para criar Conexões de código da AWS com a CLI e visualizar com o console

Uma função ou usuário designado para usar o SDK AWS CLI ou para visualizar, criar, marcar ou excluir conexões deve ter permissões limitadas ao seguinte.

> **Note**
>
> Não é possível concluir uma conexão no console somente com as permissões a seguir. É necessário adicionar as permissões na próxima seção.

Para usar o console a fim de visualizar uma lista de conexões disponíveis, visualizar tags e usar uma conexão, use a política a seguir.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "ConnectionsFullAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-connections:CreateConnection",
            "codestar-connections:DeleteConnection",
            "codestar-connections:UseConnection",
            "codestar-connections:GetConnection",
            "codestar-connections:ListConnections",
            "codestar-connections:TagResource",
            "codestar-connections:ListTagsForResource",
            "codestar-connections:UntagResource"
        ],
        "Resource": "*"
      }
   ]
```

```
}
```

Exemplo: uma política para criar Conexões de código da AWS com o console

Uma função ou um usuário designado para gerenciar conexões no console deve ter as permissões necessárias para concluir uma conexão no console e criar uma instalação, o que inclui autorizar o handshake para o provedor e criar instalações para conexões a serem usadas. `UseConnection` também deve ser adicionada para usar a conexão no console. Use a política a seguir para visualizar, usar, criar, marcar ou excluir uma conexão no console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "codestar-connections:CreateConnection",
                "codestar-connections:DeleteConnection",
                "codestar-connections:GetConnection",
                "codestar-connections:ListConnections",
                "codestar-connections:GetInstallationUrl",
                "codestar-connections:GetIndividualAccessToken",
                "codestar-connections:ListInstallationTargets",
                "codestar-connections:StartOAuthHandshake",
                "codestar-connections:UpdateConnectionInstallation",
                "codestar-connections:UseConnection",
                "codestar-connections:TagResource",
                "codestar-connections:ListTagsForResource",
                "codestar-connections:UntagResource"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Exemplo: uma política em nível de administrador para gerenciar Conexões de código da AWS

Neste exemplo, você deseja conceder acesso total a um usuário do IAM em sua AWS conta para que ele CodeConnections possa adicionar, atualizar e excluir conexões. Essa é uma política de acesso total, equivalente à política AWSCodePipeline_FullAccessgerenciada. Assim como essa

política gerenciada, você só deve anexar esse tipo de declaração de política a usuários, grupos ou funções do IAM que exijam acesso administrativo total às conexões em sua AWS conta.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "ConnectionsFullAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-connections:CreateConnection",
            "codestar-connections:DeleteConnection",
            "codestar-connections:UseConnection",
            "codestar-connections:GetConnection",
            "codestar-connections:ListConnections",
            "codestar-connections:ListInstallationTargets",
            "codestar-connections:GetInstallationUrl",
            "codestar-connections:StartOAuthHandshake",
            "codestar-connections:UpdateConnectionInstallation",
            "codestar-connections:GetIndividualAccessToken",
            "codestar-connections:TagResource",
            "codestar-connections:ListTagsForResource",
            "codestar-connections:UntagResource"
        ],
        "Resource": "*"
     }
   ]
}
```

Exemplo: uma política em nível de colaborador para usar Conexões de código da AWS

Neste exemplo, você deseja conceder acesso ao day-to-day uso de CodeConnections, como criar e visualizar detalhes de conexões, mas não a ações mais destrutivas, como excluir conexões.

```
{
    "Version": "2012-10-17",
    "Sid": "AWSCodeStarConnectionsPowerUserAccess",
        "Effect": "Allow",
        "Action": [
            "codestar-connections:CreateConnection",
            "codestar-connections:UseConnection",
            "codestar-connections:GetConnection",
            "codestar-connections:ListConnections",
```

```
            "codestar-connections:ListInstallationTargets",
            "codestar-connections:GetInstallationUrl",
            "codestar-connections:GetIndividualAccessToken",
            "codestar-connections:StartOAuthHandshake",
            "codestar-connections:UpdateConnectionInstallation",
            "codestar-connections:ListTagsForResource"
        ],
        "Resource": "*"
        }
    ]
}
```

Exemplo: uma read-only-level política para usar Conexões de código da AWS

Neste exemplo, você quer conceder a um usuário do IAM em sua conta acesso somente de leitura às conexões em sua AWS conta. Este exemplo mostra como você pode criar uma política que permite visualizar esses itens.

```
{
    "Version": "2012-10-17",
    "Id": "Connections__ReadOnly",
    "Statement": [
        {
            "Sid": "Reads_API_Access",
            "Effect": "Allow",
            "Action": [
            "codestar-connections:GetConnection",
            "codestar-connections:ListConnections",
            "codestar-connections:ListInstallationTargets",
            "codestar-connections:GetInstallationUrl",
            "codestar-connections:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo: uma política de escopo reduzido para uso Conexões de código da AWS com um repositório especificado

No exemplo a seguir, o cliente quer que a função CodeBuild de serviço acesse o repositório Bitbucket especificado. A política sobre a função CodeBuild de serviço:

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "codestar-connections:UseConnection"
        ],
        "Resource": "arn:aws:codestar-connections:us-
west-2:connection:3dee99b9-172f-4ebe-a257-722365a39557",
        "Condition": {"ForAllValues:StringEquals": {"codestar-
connections:FullRepositoryId": "myrepoowner/myreponame"}}
    }
}
```

Exemplo: uma política para usar uma conexão com CodePipeline

No exemplo a seguir, um administrador deseja que os usuários usem uma conexão com CodePipeline o. A política anexada ao usuário:

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "codestar-connections:PassConnection"
        ],
        "Resource": "arn:aws:codestar-connections:us-west-2:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
        "Condition": {"ForAllValues:StringEquals": {"codestar-
connections:PassedToService": "codepipeline.amazonaws.com"}}
    }
}
```

Exemplo: use uma função CodeBuild de serviço para operações de leitura do Bitbucket com Conexões de código da AWS

No exemplo a seguir, o cliente quer que a função CodeBuild de serviço realize operações de leitura no Bitbucket, independentemente do repositório. A política sobre a função CodeBuild de serviço:

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

```
        "Effect": "Allow",
        "Action": [
            "codestar-connections:UseConnection"
        ],
        "Resource": "arn:aws:codestar-connections:us-west-2:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
        "Condition": {"ForAllValues:StringEquals": {"codestar-
connections:ProviderPermissionsRequired": "read_only"}}
    }
}
```

Exemplo: limitar a função de CodeBuild serviço de realizar operações com Conexões de código da AWS

No exemplo a seguir, o cliente deseja impedir que a função de CodeBuild serviço execute uma operação como`CreateRepository`. A política sobre a função CodeBuild de serviço:

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "codestar-connections:UseConnection"
        ],
        "Resource": "arn:aws:codestar-connections:us-west-2:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
        "Condition": {"ForAllValues:StringNotEquals": {"codestar-
connections:ProviderPermissionsRequired": "CreateRepository"}}
    }
}
```

Usando tags para controlar o acesso aos recursos do AWS CodeStar Connections

As etiquetas podem ser anexadas ao recurso ou passadas na solicitação para serviços que comportem etiquetas. Em CodeConnections, os recursos podem ter tags e algumas ações podem incluir tags. Ao criar uma política do IAM, você poderá usar chaves de condição de tag para controlar o seguinte:

- Quais usuários podem executar ações em um recurso de pipeline, com base nas tags que o recurso já tem.

- Quais tags podem ser transmitidas na solicitação de uma ação.
- Se chaves de tags específicas podem ser usadas em uma solicitação.

Os exemplos a seguir demonstram como especificar condições de tag em políticas para usuários do CodeConnections .

Example 1: Permitir ações com base em tags na solicitação

A política a seguir concede aos usuários permissão para criar conexões no CodeConnections.

Para fazer isso, ela permitirá as ações `CreateConnection` e `TagResource` se a solicitação especificar uma tag denominada `Project` com o valor `ProjectA`. (A `aws:RequestTag` chave de condição é usada para controlar quais tags podem ser transmitidas em uma solicitação do IAM.) A `aws:TagKeys` condição garante que a chave de tag faça diferenciação de letras maiúsculas e minúsculas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codestar-connections:CreateConnection",
        "codestar-connections:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Project": "ProjectA"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["Project"]
        }
      }
    }
  ]
}
```

Example 2: Permitir ações com base em tags de recursos

A política a seguir concede aos usuários permissão para executar ações e receber informações sobre recursos no CodeConnections.

Para fazer isso, ela permitirá ações específicas se o pipeline tiver uma tag denominada `Project` com o valor `ProjectA`. (A `aws:RequestTag` chave de condição é usada para controlar quais tags podem ser transmitidas em uma solicitação do IAM.) A `aws:TagKeys` condição garante que a chave de tag faça diferenciação de letras maiúsculas e minúsculas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codestar-connections:CreateConnection",
        "codestar-connections:DeleteConnection",
        "codestar-connections:ListConnections"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "ProjectA"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["Project"]
        }
      }
    }
  ]
}
```

Uso de notificações e conexões no console

A experiência de notificações é incorporada aos CodePipeline consoles CodeBuild CodeCommit, CodeDeploy,, e, bem como no console de Ferramentas do Desenvolvedor, na própria barra de navegação de Configurações. Para acessar notificações nos consoles, é necessário ter uma das políticas gerenciadas para esses serviços aplicada ou um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos de AWS CodeStar Notificações e AWS CodeStar Conexões em sua AWS conta. Se você criar uma política baseada

em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis do IAM) com essa política. Para obter mais informações sobre como conceder acesso a AWS CodeBuild, AWS CodeCommit, e AWS CodeDeploy AWS CodePipeline, incluindo acesso a esses consoles, consulte os tópicos a seguir:

- CodeBuild: Usando políticas baseadas em identidade para CodeBuild
- CodeCommit: Usando políticas baseadas em identidade para CodeCommit
- AWS CodeDeploy: Gerenciamento de identidade e acesso para AWS CodeDeploy
- CodePipeline: Controle de acesso com políticas do IAM

AWS CodeStar As notificações não têm nenhuma política AWS gerenciada. Para fornecer acesso à funcionalidade de notificação, é necessário aplicar uma das políticas gerenciadas a um dos serviços listados anteriormente ou criar políticas com o nível de permissão que deseja conceder a usuários ou entidades e anexar essas políticas aos usuários, aos grupos ou às funções que exigem essas permissões. Para obter mais informações e exemplo, consulte o seguinte:

- Exemplo: uma política em nível de administrador para gerenciar notificações AWS CodeStar
- Exemplo: uma política em nível de colaborador para o uso de notificações AWS CodeStar
- Exemplo: uma read-only-level política para o uso de AWS CodeStar notificações.

AWS CodeStar As conexões não têm nenhuma política AWS gerenciada. Você usa as permissões e combinações de permissões para acesso, como as permissões detalhadas em Permissões para concluir conexões.

Para mais informações, consulte:

- Exemplo: uma política em nível de administrador para gerenciar Conexões de código da AWS
- Exemplo: uma política em nível de colaborador para usar Conexões de código da AWS
- Exemplo: uma read-only-level política para usar Conexões de código da AWS

Você não precisa permitir permissões de 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 às ações que correspondem à operação da API que você está tentando executar.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite 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": "*"
        }
    ]
}
```

Solução de problemas de AWS CodeStar notificações e AWS CodeStar conexões: identidade e acesso

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com notificações e o IAM.

Tópicos

Sou administrador e quero permitir que outros usuários tenham acesso a notificações

Para permitir que outras pessoas acessem AWS CodeStar Notificações e AWS CodeStar Conexões, você deve criar uma entidade do IAM (usuário ou função) para a pessoa ou o aplicativo que precisa de acesso. Elas usarão as credenciais dessa entidade para acessar a AWS. Em seguida, você deve anexar uma política à entidade que conceda a ela as permissões corretas em AWS CodeStar Notificações e AWS CodeStar Conexões.

Para começar a usar imediatamente, consulte Criar os primeiros usuário e grupo delegados pelo IAM no Guia do usuário do IAM.

Para obter informações específicas sobre AWS CodeStar notificações, consultePermissões e exemplos de AWS CodeStar notificações.

Criei um tópico do Amazon SNS e o adicionei como um destino de regra de notificação, mas não estou recebendo e-mails sobre eventos

Para receber notificações sobre eventos, você deve ter um tópico do Amazon SNS válido inscrito como um destino para a regra de notificação, e seu endereço de e-mail deve estar inscrito no tópico do Amazon SNS. Para solucionar problemas com o tópico do Amazon SNS, verifique o seguinte:

- Certifique-se de que o tópico do Amazon SNS esteja na mesma AWS região da regra de notificação.

- Verifique se o seu alias de e-mail está inscrito no tópico correto e se você confirmou a assinatura. Para obter mais informações, consulte Como inscrever um endpoint em um tópico do Amazon SNS.
- Verifique se a política do tópico foi modificada para permitir que AWS CodeStar as notificações enviem notificações para esse tópico. A política do tópico deve incluir uma declaração semelhante à seguinte:

```
{
    "Sid": "AWSCodeStarNotifications_publish",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "codestar-notifications.amazonaws.com"
        ]
    },
    "Action": "SNS:Publish",
    "Resource": "arn:aws:sns:us-east-1:123456789012:MyNotificationTopicName",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012"
        }
    }
}
```

  Para ter mais informações, consulte Configuração.

Quero permitir que pessoas fora da minha AWS conta acessem meus recursos de AWS CodeStar Notificações e AWS CodeStar Conexões

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode 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 AWS CodeStar as Notificações e AWS CodeStar Conexões oferecem suporte a esses recursos, consulteComo os recursos no console do Developer Tools funcionam 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 usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Uso de funções vinculadas ao serviço para AWS CodeStar Notifications.

O AWS CodeStar Notifications usa funções vinculadas ao serviço do AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao AWS CodeStar Notifications. As funções vinculadas ao serviço são predefinidas pelo AWS CodeStar Notifications e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome. Essa função é criada na primeira vez que você cria uma regra de notificação. Não é necessário criar a função.

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

Para excluir uma função vinculada ao serviço, primeiro é necessário excluir os recursos relacionados. Isso protege seus recursos do AWS CodeStar Notifications, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros produtos que oferecem suporte a funções vinculadas a serviços, consulte Serviços da AWS que funcionam com o IAM.

Uso de permissões de funções vinculadas ao serviço para AWS CodeStar Notifications

O AWS CodeStar Notifications usa a função vinculada ao serviço AWSServiceRoleForCodeStarNotifications para recuperar informações sobre eventos que ocorrem em sua cadeia de ferramentas e enviar notificações para os destinos especificados.

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

- `codestar-notifications.amazonaws.com`

A política de permissões da função permite que o AWS CodeStar Notifications conclua as seguintes ações nos recursos especificados:

- Ação: `PutRule` em `CloudWatch Event rules that are named awscodestar-notifications-*`
- Ação: `DescribeRule` em `CloudWatch Event rules that are named awscodestar-notifications-*`
- Ação: `PutTargets` em `CloudWatch Event rules that are named awscodestar-notifications-*`
- Ação: `CreateTopic` para `create Amazon SNS topics for use with AWS CodeStar Notifications with the prefix CodeStarNotifications-`
- Ação: `GetCommentsForPullRequests` em `all comments on all pull requests in all CodeCommit repositories in the AWS account`
- Ação: `GetCommentsForComparedCommit` em `all comments on all commits in all CodeCommit repositories in the AWS account`
- Ação: `GetDifferences` em `all commits in all CodeCommit repositories in the AWS account`
- Ação: `GetCommentsForComparedCommit` em `all comments on all commits in all CodeCommit repositories in the AWS account`
- Ação: `GetDifferences` em `all commits in all CodeCommit repositories in the AWS account`
- Ação: `DescribeSlackChannelConfigurations` em `all AWS Chatbot clients in the AWS account`

- Ação: `UpdateSlackChannelConfiguration` em `all AWS Chatbot clients in the AWS account`
- Ação: `ListActionExecutions` em `all actions in all pipelines in the AWS account`
- Ação: `GetFile` em `all files in all CodeCommit repositories in the AWS account unless otherwise tagged`

Veja essas ações na declaração de política para a função vinculada ao serviço AWSServiceRoleForCodeStarNotifications.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "events:PutTargets",
                "events:PutRule",
                "events:DescribeRule"
            ],
            "Resource": "arn:aws:events:*:*:rule/awscodestarnotifications-*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "sns:CreateTopic"
            ],
            "Resource": "arn:aws:sns:*:*:CodeStarNotifications-*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "codecommit:GetCommentsForPullRequest",
                "codecommit:GetCommentsForComparedCommit",
                "codecommit:GetDifferences",
                "chatbot:DescribeSlackChannelConfigurations",
                "chatbot:UpdateSlackChannelConfiguration",
                "codepipeline:ListActionExecutions"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
```

```
        {
            "Action": [
                "codecommit:GetFile"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:ResourceTag/ExcludeFileContentFromNotifications": "true"
                }
            },
            "Effect": "Allow"
        }
    ]
}
```

Você deve configurar permissões para permitir que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de Função Vinculadas ao Serviço no Guia do Usuário do IAM.

Criação de uma função vinculada ao serviço para o AWS CodeStar Notifications

Não é necessário criar manualmente um perfil vinculado ao serviço. Você pode usar o console do Developer Tools ou a API CreateNotificationRule pelos SDKs para criar uma regra de notificação. Você também pode chamar a API diretamente. Independentemente do método usado, a função vinculada ao serviço é criada para você.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você pode usar esse mesmo processo para recriar a função na sua conta. Você pode usar o console do Developer Tools ou a API CreateNotificationRule pelos SDKs para criar uma regra de notificação. Você também pode chamar a API diretamente. Independentemente do método usado, a função vinculada ao serviço é criada para você.

Edição de uma função vinculada ao serviço para o AWS CodeStar Notifications

Depois que criar uma função vinculada ao serviço, você não poderá alterar o nome da função, pois várias entidades podem fazer referência a ela. No entanto, é possível usar o IAM para editar a descrição da função. Para obter mais informações, consulte Editando uma Função Vinculada ao Serviço no Guia do Usuário do IAM.

Exclusão de uma função vinculada ao serviço para o AWS CodeStar Notifications

Se você não precisar mais usar um recurso ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. É necessário limpar os recursos de sua função vinculada ao serviço antes de excluí-la. Para o AWS CodeStar Notifications, isso significa excluir todas as regras de notificação que usam o perfil de serviço em sua conta da AWS.

> **Note**
>
> Se o serviço AWS CodeStar Notifications estiver usando a função ao mesmo tempo que você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir recursos do AWS CodeStar Notifications usados por AWSServiceRoleForCodeStarNotifications

1. Abra o console do AWS Developer Tools em https://console.aws.amazon.com/codesuite/settings/notifications.

   > **Note**
   >
   > As regras de notificação são aplicáveis à região da AWS em que são criadas. Se você tiver regras de notificação em mais de uma região da AWS, use o seletor para alterar a Região da AWS.

2. Escolha todas as regras de notificação que aparecem na lista e escolha Delete (Excluir).
3. Repita essas etapas em todas as regiões da AWS em que você criou regras de notificação.

Para usar o IAM para excluir a função vinculada ao serviço

Use o console do IAM, a AWS CLI ou a API da AWS Identity and Access Management para excluir a função vinculada ao serviço AWSServiceRoleForCodeStarNotifications. Para obter mais informações, consulte Deleting a Service-Linked Role no IAM User Guide.

Regiões compatíveis com funções vinculadas ao serviço do AWS CodeStar Notifications

O AWS CodeStar Notifications é compatível com perfis vinculados a serviços em todas as regiões da AWS em que o serviço está disponível. Para obter mais informações, consulte AWS Regions and Endpoints e AWS CodeStar Notifications.

Uso de funções vinculadas ao serviço do Conexões de código da AWS

Conexões de código da AWS usa AWS Identity and Access Management perfis vinculados ao serviço (IAM). A função vinculada ao serviço é um tipo exclusivo de perfil do IAM vinculada diretamente ao Conexões de código da AWS. As funções vinculadas a serviços são predefinidas pelo Conexões de código da AWS e incluem todas as permissões que o serviço exige para chamar outros serviços da AWS em seu nome. Esse perfil é criado na primeira vez que você cria uma conexão. Não é necessário criar a função.

Uma função vinculada ao serviço facilita a configuração do Conexões de código da AWS porque não é necessário adicionar as permissões manualmente. O Conexões de código da AWS define as permissões de suas funções vinculadas ao serviço e, a não ser que definido em contrário, somente o Conexões de código da AWS pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Para excluir uma função vinculada ao serviço, primeiro é necessário excluir os recursos relacionados. Isso protege seus recursos do Conexões de código da AWS, pois você não pode remover por engano as permissões de acesso aos recursos.

Para obter informações sobre outros produtos que oferecem suporte a funções vinculadas a serviços, consulte Serviços da AWS que funcionam com o IAM.

Permissões de função vinculada ao serviço Conexões de código da AWS

O Conexões de código da AWS usa o perfil vinculado ao serviço AWSServiceRoleForGitSync para usar a sincronização Git com repositórios conectados baseados em Git.

O perfil vinculado ao serviço AWSServiceRoleForGitSync confia nos seguintes serviços para assumir o perfil:

- `repository.sync.codeconnections.amazonaws.com`

A política de permissões de perfil vinculado ao serviço AWSGitSyncServiceRolePolicy permite que o Conexões de código da AWS conclua as seguintes ações nos recursos especificados:

- Ação: concede permissões para que os usuários criem conexões com repositórios externos baseados em Git e usem a sincronização Git com esses repositórios.

Você deve configurar permissões para permitir que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de Função Vinculadas ao Serviço no Guia do Usuário do IAM.

Crie uma função vinculada ao serviço para o Conexões de código da AWS

Não é necessário criar manualmente um perfil vinculado ao serviço. Você cria o perfil ao criar um recurso para o projeto sincronizado com o Git com a API CreateRepositoryLink.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você pode usar esse mesmo processo para recriar a função na sua conta.

Editar uma função vinculada ao serviço para o Conexões de código da AWS

Depois que criar uma função vinculada ao serviço, você não poderá alterar o nome da função, pois várias entidades podem fazer referência a ela. No entanto, é possível usar o IAM para editar a descrição da função. Para obter mais informações, consulte Editando uma Função Vinculada ao Serviço no Guia do Usuário do IAM.

Excluir uma função vinculada ao serviço para o Conexões de código da AWS

Se você não precisar mais usar um recurso ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. É necessário limpar os recursos de sua função vinculada ao serviço antes de excluí-la. Isso significa excluir todas as conexões que usem o perfil de serviço na conta da AWS.

> **Note**
>
> Se o serviço Conexões de código da AWS estiver usando a função quando você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Como excluir recursos do Conexões de código da AWS utilizados por AWSServiceRoleForGitSync

1. Abra o console do Developer Tools e escolha Configurações.
2. Escolha todas as conexões que aparecem na lista e escolha Excluir.
3. Repita essas etapas em todas as regiões da AWS em que você criou conexões.

Para usar o IAM para excluir a função vinculada ao serviço

Use o console do IAM, a AWS CLI ou a API do AWS Identity and Access Management para excluir o perfil vinculado ao serviço AWSServiceRoleForGitSync. Para obter mais informações, consulte Deleting a Service-Linked Role no IAM User Guide.

Regiões compatíveis com funções vinculadas ao serviço do Conexões de código da AWS

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

Políticas gerenciadas pela AWS para o Conexões de código da AWS

Uma política gerenciada AWS é uma política independente criada e administrada por AWS. As políticas gerenciadas AWS são criadas para fornecer permissões a vários casos de uso comuns e permitir a atribuição de permissões a usuários, grupos e perfis.

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

Você não pode alterar as permissões definidas em políticas gerenciadas AWS. Se AWS atualiza as permissões definidas em um política gerenciada por AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política estiver vinculada. É provável que AWS atualize uma política gerenciada por AWS quando um novo AWS service (Serviço da AWS) for lançado, ou novas operações de API forem disponibilizadas para os serviços existentes.

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

Política gerenciada da AWS: AWSGitSyncServiceRolePolicy

Não é possível anexar a AWSGitSyncServiceRolePolicy às entidades do IAM. Essa política é anexada a uma função vinculada ao serviço que permite que o Conexões de código da AWS realize ações em seu nome. Para obter mais informações, consulte Uso de funções vinculadas ao serviço do Conexões de código da AWS.

Essa política permite que os clientes acessem repositórios baseados em Git para uso com conexões. Os clientes acessarão esses recursos depois de usar a API CreateRepositoryLink.

Detalhes da permissão

Esta política inclui as seguintes permissões.

- `codestar-connections`: concede permissões para que os usuários criem conexões com repositórios externos baseados em Git.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AccessGitRepos",
   "Effect": "Allow",
   "Action": [
    "codestar-connections:UseConnection"
   ],
   "Resource": "arn:aws:codestar-connections:*:*:connection/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  }
 ]
```

```
}
```

Atualizações Conexões de código da AWS para políticas gerenciadas por AWS

Visualizar detalhes sobre atualizações em políticas gerenciadas pela AWS para o Conexões de código da AWS desde o início do rastreio das alterações pelo serviço. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed de RSS na página Histórico do documento do Conexões de código da AWS.

Alteração	Descrição	Data
AWSGitSyncServiceRolePolicy: nova política	O Conexões de código da AWS adicionou a política. Concede permissões para permitir que os usuários do Conexões de código da AWS usem a sincronização Git com repositórios conectados baseados em Git.	26 de novembro de 2023
O Conexões de código da AWS iniciou o rastreamento das alterações	O Conexões de código da AWS começou a monitorar as alterações para as políticas gerenciadas da AWS.	26 de novembro de 2023

Validação de conformidade para AWS CodeStar notificações e AWS CodeStar conexões

AWS CodeStar Notificações e AWS CodeStar conexões não estão no escopo de nenhum programa de AWS conformidade.

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte AWS serviços no escopo por programa de conformidade. Para obter informações gerais, consulte Programas de conformidade da AWS.

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Como baixar relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar AWS CodeStar Notificações e AWS CodeStar Conexões é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade da sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos focados em segurança e conformidade em. AWS
- AWS recursos de conformidade — essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Config— Esse AWS serviço avalia se suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Esse AWS serviço fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.

Resiliência no AWS CodeStar Notifications e no AWS CodeStar Connections

A infraestrutura global da AWS é criada com base em regiões da AWS e zonas de disponibilidade. As regiões da AWS As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, as quais são conectadas com baixa latência, alto throughput e redes altamente redundantes. Com as zonas de disponibilidade, você pode projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre regiões e zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

- As regras de notificação são específicas da Região da AWS em que são criadas. Se você tiver regras de notificação em mais de uma Região da AWS, use o seletor de região para revisar regras de notificação em cada Região da AWS.

- O AWS CodeStar Notifications depende de tópicos do Amazon Simple Notification Service (Amazon SNS) como destinos de regras de notificação. As informações sobre seus tópicos do Amazon SNS e destinos da regra de notificação podem ser armazenadas em uma região da AWS fora da região em que você configurou a regra de notificação.

Segurança da infraestrutura no AWS CodeStar Notifications e no AWS CodeStar Connections

Como recursos de um serviço gerenciado, o AWS CodeStar Notifications e o AWS CodeStar Connections são protegidos pelos procedimentos de segurança da rede globais da AWS, os quais estão descritos no whitepaper Amazon Web Services: Overview of security processes.

Você usa chamadas de API publicadas pela AWS para acessar o AWS CodeStar Notifications e o AWSCodeStar Conexões via rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.0 ou posterior. Os clientes também devem ter suporte a conjuntos de criptografia com perfect forward secrecy (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos suporta esses modos.

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.

Tráfego entre recursos do Conexões de código da AWS entre regiões

Se você usar o recurso de conexões para ativar a conexão de seus recursos, você concorda e nos instrui a armazenar e processar informações associadas a esses recursos de conexão em Regiões da AWS fora das Regiões da AWS onde você está usando o serviço subjacente, exclusivamente em conexão com, e com o único propósito de fornecer conexão com esses recursos em regiões diferentes daquela em que o recurso foi criado.

Para obter mais informações, consulte Recursos globais em AWS CodeStar conexões.

> **Note**
>
> Se você usar o recurso de conexões para habilitar a conexão de seus recursos em regiões que não precisam ser habilitadas primeiro, armazenaremos e processaremos as informações conforme detalhado nos tópicos anteriores.

Para conexões estabelecidas em regiões que primeiro devem ser habilitadas, como a região Europa (Milão), armazenaremos e processaremos somente as informações dessa conexão nessa região.

Histórico do documento

A tabela a seguir descreve a documentação desta versão do console do Developer Tools.

- Versão da API do AWS CodeStar Notifications: 15/10/2019
- Versão da API do AWS CodeStar Connections: 01/12/2019

Alteração	Descrição	Data
Suporte ao GitLab autogerenciado	Suporte adicionado para configurar conexões e hosts de recursos da AWS para interagir com o GitLab autogerenciado. Consulte mais informações em Workflow to create or update a host e Create a connection to GitLab self-managed.	28 de dezembro de 2023
Novos links de repositório e configurações de sincronização para conexões	Foram adicionadas informações sobre como configurar links de repositório e configurações de sincronização. Use a configuração de sincronização para sincronizar conteúdo de um repositório Git para atualizar os recursos de pilha do AWS CloudFormation. Para obter mais informações, consulte Working with repository links e Working with sync configurations.	27 de novembro de 2023
Suporte para conexões de perfil vinculado ao serviço	Foi adicionado suporte à configuração de conexões para usar sincronização	26 de novembro de 2023

	Git com repositórios Git. Para obter mais informaçõ es, consulte Using service-l inked roles for AWS CodeStar Connections e Managed policies.	
Suporte para grupos do GitLab	Suporte adicionado para configurar conexões de recursos da AWS para interagir com grupos do GitLab. Para receber mais informações, consulte Criar uma conexão e Criar uma conexão com o GitHub.	15 de setembro de 2023
Novo tipo de provedor do GitLab	Agora você pode criar conexões com o GitLab. Para receber mais informações, consulte Criar uma conexão e Criar uma conexão com o GitHub.	10 de agosto de 2023
Novo tipo de destino para regras de notificação	Agora é possível escolher clientes do AWS Chatbot configurados para canais do Microsoft Teams como destino para regras de notificação. Para obter mais informações, consulte Criar uma regra de notificação e Como trabalhar com destinos de regra de notificação.	17 de maio de 2023

As conexões estão disponíveis na região Europa (Milão)	Informações adicionadas para conexões na região Europa (Milão). Para obter mais informações, consulte Tráfego entre recursos de conexões do AWS CodeStar entre regiões.	17 de maio de 2023
Adição da resolução de problemas para erros de conexão com permissões de repositório	Ao criar uma conexão com um repositório em uma organização do GitHub, você deve ser o proprietário da organização do GitHub. Para obter mais informações, consulte Connections error when connecting to GitHub (Erro de conexão com o GitHub).	29 de agosto de 2022
Adição de informações para marcação de recursos de host	Agora você pode marcar hosts usando o console e a CLI. Para ter mais informações, consulte Marcar recursos no AWS CodeStar Connections.	19 de abril de 2021
Compatibilidade com endpoint da VPC para conexões	É possível usar VPC endpoints com o Connections. Para ter mais informações, consulte AWS CodeStar Connections e endpoints de VPC da interface (AWS PrivateLink).	24 de novembro de 2020

Novos tipos de provedores GitHub e GitHub Enterprise Cloud	Agora você pode criar conexões para o GitHub e o GitHub Enterprise Cloud. Para obter mais informações, consulte Criar uma conexão e Criar uma conexão com o GitHub.	30 de setembro de 2020
Adição do tipo de provedor GitHub Enterprise Server e recursos de host	Informações sobre o recurso de host para conexões foram adicionadas a este guia. Agora você pode criar conexões para o GitHub Enterprise Server. Para obter mais informações, consulte Criar uma conexão e Como trabalhar com hosts. Esta é a versão disponibi lizada para o público em geral do recurso de conexões no Manual do usuário do console do Developer Tools.	29 de junho de 2020

Adição de informações sobre uso e marcação de conexões	Informações sobre o recurso de conexões no console foram adicionadas a este guia. Você pode exibir conceitos, etapas para começar, uma referênci a de permissões que inclui políticas de exemplo e etapas para criar, exibir e marcar conexões. Para ter mais informações, consulte O que são conexões, Conceitos de conexões, Conceitos básicos de conexões, Criar uma conexão, Marcar recursos no AWS CodeStar Connectio ns, Segurança, Cotas para conexões, Solução de problemas e Chamadas da API do AWS CodeStar Connections com o AWS CloudTrail. Para exibir uma lista de ações adicionais do provedor (ações somente de permissões), consulte Ações para ProviderType.	28 de junho de 2020
Novo tipo de destino para regras de notificação	Agora é possível escolher clientes do AWS Chatbot configurados para canais Slack como destino para regras de notificação. Para obter mais informações, consulte Criar uma regra de notificação e Como trabalhar com destinos de regra de notificação.	2 de abril de 2020

Notificações adicionadas sobre eventos adicionais do AWS CodeCommit	Agora você pode configurar notificações para eventos relacionados a aprovações de solicitação pull. Para obter mais informações, consulte Eventos para regras de notificação em repositórios e Como trabalhar com solicitações pull no CodeCommit.	10 de fevereiro de 2020
Notificações disponíveis em duas regiões da AWS adicionais	O console do Developer Tools agora oferece suporte a notificações nas regiões Oriente Médio (Bahrein) e Ásia-Pacífico (Hong Kong). Para ter mais informações, consulte Notificações do AWS CodeStar na Referência geral da AWS.	5 de fevereiro de 2020
Adição de suporte para tópicos criptografados do Amazon SNS	Adição de orientações para o uso de tópicos criptografados do Amazon SNS como alvos de notificações. Para obter mais informações, consulte Configuração de tópicos do Amazon SNS para notificações.	4 de fevereiro de 2020

As notificações podem incluir informações de etiqueta de sessão para o CodeCommit	Agora as notificações para o CodeCommit podem conter informações de identidade do usuário, como um nome de exibição ou um endereço de e-mail por meio do uso de tags de sessão. Para obter mais informações, consulte Conceitos e Uso de tags para fornecer informações de identidade no CodeCommit.	19 de dezembro de 2019
Lançamento inicial	Esta é a versão inicial do Manual do usuário do console do Developer Tools.	5 de novembro de 2019

Glossário da AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

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.