aws

Guía del usuario

Consola de Developer Tools

Consola de Developer Tools: Guía del usuario

Table of Contents

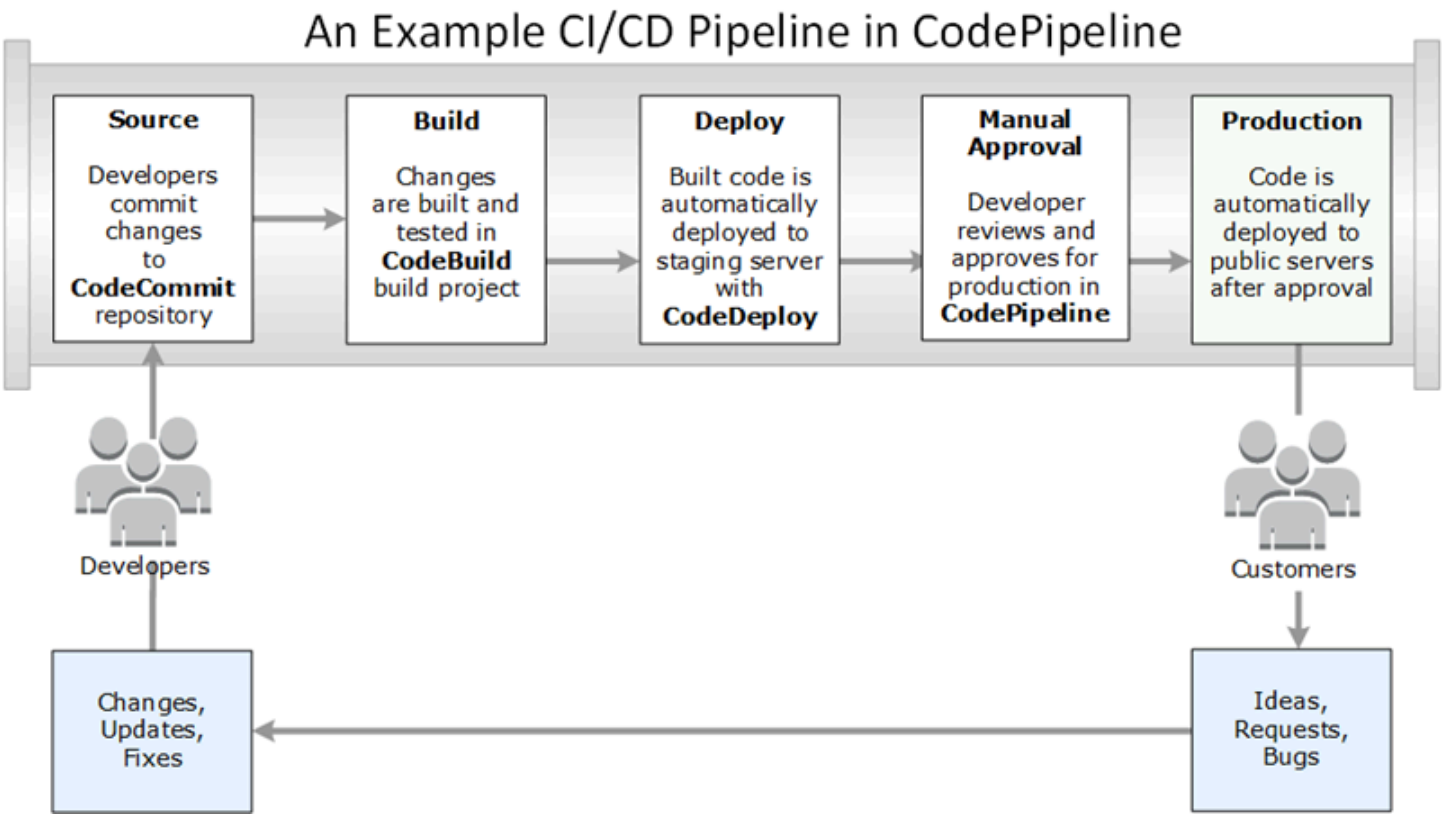
¿Qué es la consola de herramientas para desarrolladores?

La consola de herramientas para desarrolladores contiene un conjunto de servicios y características que puede utilizar individual o colectivamente para facilitar el desarrollo de software, ya sea de forma individual o en equipo. Las herramientas para desarrolladores pueden ayudarle a almacenar, crear, probar e implementar su software de forma segura. Utilizadas individual o colectivamente, estas herramientas proporcionan soporte para DevOps, integración continua y entrega continua (CI/CD).

La consola de herramientas para desarrolladores incluye los siguientes servicios:

- AWS CodeCommit es un servicio de control de código fuente completamente administrado que aloja repositorios Git privados. Puede usar repositorios para almacenar y administrar recursos de forma privada (como documentos, código fuente y archivos binarios) en la Nube de AWS. Sus repositorios almacenan el historial de su proyecto, desde la primera confirmación hasta los últimos cambios. Puede trabajar de forma colaborativa en el código en los repositorios comentando el código y creando solicitudes de extracción para ayudar a garantizar la calidad del código.
- AWS CodeBuild es un servicio de compilación completamente administrado que compila código fuente, ejecuta pruebas unitarias y produce artefactos listos para su implementación. Este servicio proporciona entornos de compilación preconfigurados para lenguajes de programación y herramientas de compilación populares como Apache Maven, Gradle, etc. También puede personalizar entornos de compilación en CodeBuild para utilizar sus propias herramientas de compilación.
- AWS CodeDeploy es un servicio de implementación completamente administrado que automatiza las implementaciones de software para procesar servicios informáticos como Amazon EC2, AWS Lambda y sus servidores en las instalaciones. Puede ayudarle a liberar rápidamente nuevas características, evitar el tiempo de inactividad durante la implementación de aplicaciones y manejar la complejidad de actualizar sus aplicaciones.
- AWS CodePipeline es un servicio continuado de integración y entrega continua que permite modelar, visualizar y automatizar los pasos necesarios para lanzar su software. Puede diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software. Puede compilar, probar e implementar el código cada vez que se produce un cambio en este, de acuerdo con los modelos de procesamiento de la publicación que defina.

A continuación, se muestra un ejemplo de cómo puede utilizar los servicios conjuntos en la consola de herramientas para desarrolladores para facilitar el desarrollo de software.



En este ejemplo, los desarrolladores crean un repositorio en CodeCommit y lo utilizan para desarrollar su código y colaborar en él. Crean un proyecto de compilación en CodeBuild para crear y probar su código, y usan CodeDeploy para implementar su código en entornos de prueba y producción. Desean iterar rápidamente, por lo que crean una canalización en CodePipeline que permite detectar los cambios en el repositorio CodeCommit. Esos cambios se crean, se ejecutan pruebas y el código compilado y probado correctamente se implementa en el servidor de prueba. El equipo añade etapas de prueba a la canalización para ejecutar más pruebas en el servidor provisional, como pruebas de integración o carga. Una vez completadas con éxito esas pruebas, un miembro del equipo revisa los resultados y, si está satisfecho, aprueba manualmente los cambios para la producción. CodePipeline implementa el código probado y aprobado en las instancias de producción.

Se trata solo de un ejemplo sencillo del modo en que puede utilizar uno o varios de los servicios disponibles en la consola de herramientas para desarrolladores para facilitar el desarrollo de software. Cada uno de los servicios se puede personalizar para satisfacer sus necesidades. Ofrecen muchas integraciones con otros productos y servicios, tanto en AWS como con otras herramientas de terceros. Para obtener más información, consulte los siguientes temas:

- CodeCommit: Integraciones de productos y servicios

- CodeBuild: Uso de CodeBuild con Jenkins
- CodeDeploy: Integraciones de productos y servicios
- CodePipeline: Integraciones de productos y servicios

¿Es la primera vez que usa ?

Si es la primera vez que utiliza uno o varios de los servicios disponibles en la consola de herramientas para desarrolladores, se recomienda que lea primero los temas que se indican a continuación:

- Introducción a CodeCommit
- Introducción a CodeBuild, Conceptos
- Introducción a CodeDeploy, Componentes primarios
- Introducción a CodePipeline, Conceptos

Características de la consola de herramientas para desarrolladores

La consola de herramientas para desarrolladores incluye las siguientes características:

- La consola de herramientas para desarrolladores incorpora una característica de administrador de notificaciones que puede utilizar para suscribirse a eventos en AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy y AWS CodePipeline. Esta característica tiene su propia API, AWS CodeStar Notifications. Puede utilizar la función de notificaciones para notificar rápidamente a los usuarios acerca de los eventos en los repositorios, proyectos de compilación, aplicaciones de implementación y canalizaciones que son más importantes para su trabajo. Un administrador de notificaciones ayuda a que los usuarios conozcan los eventos que se producen en repositorios, compilaciones, implementaciones o canalizaciones para que puedan tomar medidas rápidamente, como aprobar cambios o corregir errores. Para obtener más información, consultar ¿Qué son las notificaciones?
- La consola de herramientas para desarrolladores incorpora una característica de conexiones que puede utilizar para asociar sus recursos de AWS con proveedores de código fuente de terceros. Esta característica tiene su propia API, AWS CodeStar Connections. Puede utilizar la característica de conexiones para configurar una conexión autorizada con un proveedor de terceros y utilizar el recurso de conexión con otros servicios de AWS. Para obtener más información, consultar ¿Qué son las conexiones?

¿Qué son las notificaciones?

La característica de notificaciones de la consola de herramientas para desarrolladores es un administrador de notificaciones para suscribirse a eventos en AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy y AWS CodePipeline. Tiene su propia API, AWS CodeStar Notifications. Puede utilizar la función de notificaciones para notificar rápidamente a los usuarios acerca de los eventos en los repositorios, proyectos de compilación, aplicaciones de implementación y canalizaciones que son más importantes para su trabajo. Un administrador de notificaciones ayuda a que los usuarios conozcan los eventos que se producen en repositorios, compilaciones, implementaciones o canalizaciones para que puedan tomar medidas rápidamente, como aprobar cambios o corregir errores.

¿Qué puedo hacer con las notificaciones?

Puede utilizar la función de notificaciones para crear y administrar reglas de notificación para notificar a los usuarios los cambios importantes realizados en sus recursos, entre los que se incluyen:

- errores y éxitos de compilación en los proyectos de compilación de CodeBuild
- errores y éxitos de implementación en aplicaciones CodeDeploy
- creación y actualizaciones de las solicitudes de extracción, incluidos los comentarios sobre el código, en los repositorios de CodeCommit
- estados de aprobación manual y ejecuciones de canalización en CodePipeline

Puede configurar notificaciones para que se envíen a las direcciones de email de los usuarios suscritos a un tema de Amazon SNS. También puede integrar esta característica en AWS Chatbot y enviar notificaciones a los canales de Slack, el canal de Microsoft Teams o las salas de chat de Amazon Chime.

¿Cómo funcionan las notificaciones?

Cuando configura una regla de notificación para un recurso admitido, como, por ejemplo, un repositorio, un proyecto de compilación, una aplicación o una canalización, la característica de notificaciones crea una regla de Amazon EventBridge que monitorea los eventos que especifique. Cuando se produce un evento de ese tipo, la regla de notificación envía notificaciones a los temas de Amazon SNS especificados como destinos para dicha regla. Los suscriptores de dichos destinos reciben notificaciones sobre estos eventos.

¿Cómo empiezo a utilizar las notificaciones?

Para empezar, aquí hay algunos temas útiles para revisar:

- Más información sobre los conceptos para las notificaciones.
- Configure los recursos que necesite para comenzar a utilizar las notificaciones.
- Comience a utilizar sus primeras reglas de notificación y reciba sus primeras notificaciones.

Conceptos de notificación

Configurar y utilizar notificaciones resulta más sencillo si comprende los conceptos y términos. Aquí encontrará algunos conceptos que debe conocer cuando usa las notificaciones.

Temas

- Notificaciones
- Reglas de notificación
- Eventos
- Tipos de detalles
- implementación
- Notificaciones y AWS CodeStar Notifications
- Eventos de reglas de notificación en repositorios
- Eventos de reglas de notificación en proyectos de compilación
- Eventos de reglas de notificación en aplicaciones de implementación
- Eventos de reglas de notificación en canalizaciones

Notificaciones

Una notificación es un mensaje que incluye información sobre los eventos que se producen en los recursos que usted y sus desarrolladores utilizan. Puede configurar notificaciones para que los usuarios de un recurso, como, por ejemplo, un proyecto de compilación, un repositorio, una aplicación de implementación o una canalización, reciban correos electrónicos sobre los tipos de eventos que especifique en función de la regla de notificación que cree.

Las notificaciones para AWS CodeCommit pueden contener información de identidad del usuario, como un nombre de visualización o una dirección de email, mediante el uso de etiquetas de

sesión. CodeCommit admite el uso de etiquetas de sesión, que son atributos de par clave-valor que se pasan cuando asume un rol de IAM, utiliza credenciales temporales o federa un usuario en AWS Security Token Service (AWS STS). También puede asociar etiquetas a un usuario de IAM. CodeCommit incluye los valores de `displayName` y `emailAddress` en el contenido de la notificación en caso de que esas etiquetas estén presentes. Para obtener más información, consulte Uso de etiquetas para proporcionar información adicional de identidad en CodeCommit.

> **Important**
>
> Las notificaciones incluyen información específica del proyecto, como, por ejemplo, estados de compilación, estado de implementación, líneas de código que tienen comentarios y aprobaciones de canalizaciones. El contenido de las notificaciones puede cambiar a medida que se añaden nuevas características. Como práctica recomendada de seguridad, debe revisar regularmente los destinos de las reglas de notificación y los suscriptores del tema de Amazon SNS. Para obtener más información, consulte Descripción del contenido y la seguridad de las notificaciones.

Reglas de notificación

Una regla de notificación es un recurso de AWS que se crea para especificar cuándo y dónde se envían las notificaciones. Define:

- Las condiciones en las que se crea una notificación. Estas condiciones se basan en los eventos que elija, que son específicos del tipo de recurso. Entre los tipos de recursos admitidos, se incluyen proyectos de compilación de AWS CodeBuild, aplicaciones de implementación en AWS CodeDeploy, canalizaciones de AWS CodePipeline y repositorios de AWS CodeCommit.
- Los destinos a los que se envía la notificación. Puede especificar hasta 10 destinos para una regla de notificación.

Las reglas de notificación se aplican a proyectos de compilación individuales, aplicaciones de implementación, canalizaciones y repositorios. Las reglas de notificación tienen nombres fáciles de recordar definidos por el usuario y nombres de recursos de Amazon (ARN). Las reglas de notificación deben crearse en la misma región de AWS en la que existe el recurso. Por ejemplo, si su proyecto de compilación está en la región EE. UU. Este (Ohio), la regla de notificación también debe crearse en la región EE. UU. Este (Ohio).

Puede definir hasta 10 reglas de notificación para un recurso.

Eventos

Un evento es un cambio de estado en un recurso que desea monitorear. Cada recurso tiene una lista de tipos de eventos entre los que puede elegir. Al configurar una regla de notificación en un recurso, usted especifica los eventos que hacen que se envíen notificaciones. Por ejemplo, si configura notificaciones para un repositorio en CodeCommit y selecciona Created (Creado) en Pull request (Solicitud de extracción) y en Branches and tags (Ramificaciones y etiquetas), se envía una notificación cada vez que un usuario de dicho repositorio crea una solicitud de extracción, ramificación o etiqueta de Git.

Tipos de detalles

Al crear una regla de notificación, puede elegir el nivel de detalle o el tipo de detalle que se va a incluir en las notificaciones (Full [Completo] o Basic [Básico]). El valor Full (Completo), que es el predeterminado, incluye toda la información disponible para el evento en la notificación, incluida la información mejorada que proporcionan los servicios para eventos específicos. El valor Basic (Básico) incluye solo un subconjunto de la información disponible.

En la siguiente tabla se muestra la información mejorada disponible para tipos de eventos específicos y se describen las diferencias entre los tipos de detalles.

Servicio	Evento	Full incluye	Basic no incluye
CodeCommit	Comentarios sobre confirmaciones Comentarios sobre solicitudes de extracción	Todos los detalles del evento y el contenido del comentari o, incluidas las respuestas o los hilos de comentarios. También incluye el número de línea y la línea de código sobre la que se realizó el comentario.	El contenido del comentario, el número de línea, la línea de código ni los hilos de comentarios.
CodeCommit	Solicitud de extracció n creada	Todos los detalles del evento y el número de archivos que	Ninguna lista de archivos ni detalles acerca de si la

Servicio	Evento	Full incluye	Basic no incluye
		se agregaron, se modificaron o se eliminaron en la solicitud de extracción en relación con la rama de destino.	rama de origen de la solicitud de extracción ha agregado, modificado o eliminado archivos.
CodePipeline	Requiere aprobación manual	Todos los detalles del evento y los datos personalizados (si están configurados). La notificación también incluye un enlace a la aprobación requerida en la canalización.	No hay datos personalizados ni enlaces.
CodePipeline	Error al ejecutar la acción Error al ejecutar la canalización Error al ejecutar la etapa	Todos los detalles del evento y el contenido del mensaje del error correspondiente.	Ningún contenido de mensaje de error.

implementación

Un destino es una ubicación para recibir notificaciones de reglas de notificación. Los tipos de destinos permitidos son temas de Amazon SNS y clientes de AWS Chatbot configurados para canales de Slack o Microsoft Teams. Todos los usuarios suscritos al destino reciben notificaciones sobre los eventos que especifique en la regla de notificación.

Si desea ampliar el alcance de las notificaciones, puede configurar manualmente la integración entre las notificaciones y AWS Chatbot para que las notificaciones se envíen a las salas de chat de Amazon Chime. A continuación, puede elegir el tema de Amazon SNS que está configurado para

ese cliente de AWS Chatbot como destino de la regla de notificación. Para obtener más información, consulte Para integrar notificaciones en AWS Chatbot y Amazon Chime.

Si decide utilizar un cliente de AWS Chatbot como destino, primero debe crear ese cliente en AWS Chatbot. Cuando se elige un cliente de AWS Chatbot como destino para una regla de notificación, se configura un tema de Amazon SNS para ese cliente de AWS Chatbot con todas las políticas necesarias para que las notificaciones se envíen al canal de Slack o Microsoft Teams. No es necesario configurar ningún tema de Amazon SNS existente para el cliente de AWS Chatbot.

Puede elegir crear un tema de Amazon SNS como destino durante la creación de una regla de notificación (recomendado). También puede elegir un tema de Amazon SNS existente que se encuentre en la misma región de AWS que la regla de notificación, pero debe configurarlo con la política requerida. El tema de Amazon SNS que utilice para un destino debe estar presente en su cuenta de AWS. También debe estar presente en la misma región de AWS que la regla de notificación y que el recurso de AWS para el que se creó la regla.

Por ejemplo, si crea una regla de notificación para un repositorio en la región EE. UU. Este (Ohio), el tema de Amazon SNS también debe existir en dicha región. Si crea un tema de Amazon SNS como parte de la creación de una regla de notificación, el tema se configura con la política necesaria para permitir la publicación de eventos en él. Este es el mejor método para trabajar con destinos y reglas de notificación. Si decide utilizar un tema ya existente o crear uno manualmente, debe configurarlo con los permisos requeridos para que los usuarios reciban notificaciones. Para obtener más información, consulte Configuración de los temas de Amazon SNS para las notificaciones.

> **Note**
>
> Si desea utilizar un tema de Amazon SNS existente en lugar de crear uno nuevo, en Targets (Destinos), elija su ARN. Asegúrese de que el tema tiene la política de acceso adecuada y de que la lista de suscriptores contiene solo aquellos usuarios que tienen permiso para ver información sobre el recurso. Si el tema de Amazon SNS corresponde a uno que se utilizaba para las notificaciones de CodeCommit antes del 5 de noviembre de 2019, contendrá una política que permite a CodeCommit publicar en ella y que contenga permisos distintos a los necesarios para AWS CodeStar Notifications. No se recomienda usar estos temas. Si desea usar uno creado para dicha experiencia, debe agregar la política requerida a AWS CodeStar Notifications además de la que ya existe. Para obtener más información, consulte Configuración de los temas de Amazon SNS para las notificaciones y Descripción del contenido y la seguridad de las notificaciones.

Notificaciones y AWS CodeStar Notifications

Las notificaciones, aunque son una característica de la consola de herramientas para desarrolladores, tienen su propia API, AWS CodeStar Notifications. También tiene su propio tipo de recurso AWS (reglas de notificación), permisos y eventos. Los eventos para las reglas de notificación se registran en AWS CloudTrail. Las acciones de la API se pueden permitir o denegar a través de políticas de IAM.

Eventos de reglas de notificación en repositorios

Categoría	Eventos	Id. de evento
Comentarios	On commits (Sobre confirmaciones)	`codecommit-repository-comments-on-commits`
	On pull requests (Sobre solicitudes de extracción)	`codecommit-repository-comments-on-pull-requests`
Aprobaciones	Status changed (Estado cambiado)	`codecommit-repository-approvals-status-changed`
	Invalidación de reglas	`codecommit-repository-approvals-rule-override`
Pull request (Solicitud de extracción)	Created (Creado)	`codecommit-repository-pull-request-created`
	Source updated (Origen actualizado)	`codecommit-repository-pull-request-source-updated`
	Status changed (Estado cambiado)	`codecommit-repository-pull-request-status-changed`
	Merged (Fusionado)	`codecommit-repository-pull-request-merged`

Categoría	Eventos	Id. de evento

Branches and tags (Ramificaciones y etiquetas)	Created (Creado)
	Deleted (Eliminado)
	Actualizado
		`codecommit-repository-branches-and-tags-created`
		`codecommit-repository-branches-and-tags-deleted`
		`codecommit-repository-branches-and-tags-updated`

Eventos de reglas de notificación en proyectos de compilación

Categoría	Eventos	Id. de evento

Build state (Estado de compilación)	Con error
	Succeeded
	In-progress (En curso)
	Stopped (Detenido)
		`codebuild-project-build-state-failed`
		`codebuild-project-build-state-succeeded`
		`codebuild-project-build-state-in-progress`
		`codebuild-project-build-state-stopped`

Build phase (Fase de compilación)	Error Correcto	`codebuild-project-build-phase-failure` `codebuild-project-build-phase-success`

Eventos de reglas de notificación en aplicaciones de implementación

Categoría	Eventos	Id. de evento

Implementación	Con error
	Succeeded
	Started
		`codedeploy-application-deployment-failed`
		`codedeploy-application-deployment-succeeded`
		`codedeploy-application-deployment-started`

Eventos de reglas de notificación en canalizaciones

Categoría	Eventos	Id. de evento

Action execution (Ejecución de acciones)	Succeeded
	Con error
	Cancelado
	Started
		`codepipeline-pipeline-action-execution-succeeded`
		`codepipeline-pipeline-action-execution-failed`
		`codepipeline-pipeline-action-execution-canceled`
		`codepipeline-pipeline-action-execution-started`

Stage execution (Ejecución de etapas)	Started
	Succeeded
	RESUMED (REANUDADO)
	Cancelado
	Con error
		`codepipeline-pipeline-stage-execution-started`
		`codepipeline-pipeline-stage-execution-succeeded`
		`codepipeline-pipeline-stage-execution-resumed`

Categoría	Eventos	Id. de evento
		`codepipeline-pipeline-stage-execution-canceled` `codepipeline-pipeline-stage-execution-failed`

Pipeline execution (Ejecución de canalizaciones)	Con error
	Cancelado
	Started
	RESUMED (REANUDADO)
	Succeeded
	SUPERSEDED (SUSTITUIDO)
		`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`

Manual approval (Aprobación manual)	Con error
	Needed (Necesario)
	Succeeded
		`codepipeline-pipeline-manual-approval-failed`
		`codepipeline-pipeline-manual-approval-needed`
		`codepipeline-pipeline-manual-approval-succeeded`

Configuración

Si tiene una política administrada para AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy o AWS CodePipeline aplicada a su usuario o rol de IAM, tiene los permisos necesarios para trabajar con notificaciones dentro de las limitaciones de los roles y los permisos

proporcionados por la política. Por ejemplo, los usuarios que tienen aplicadas las políticas `AWSCodeBuildAdminAccess`, `AWSCodeCommitFullAccess`, `AWSCodeDeployFullAccess`, o `AWSCodePipeline_FullAccess` administradas tienen acceso administrativo completo a las notificaciones.

Para obtener más información, incluidos ejemplos de políticas, consulte Políticas basadas en identidades.

Si tiene una de estas políticas aplicada al usuario o al rol de IAM, y un proyecto de compilación en CodeBuild, un repositorio en CodeCommit, una aplicación de implementación en CodeDeploy o una canalización en CodePipeline, está listo para crear la primera regla de notificación. Siga en Introducción a las notificaciones. Si no las tiene, consulte los siguientes temas:

- CodeBuild: Introducción a CodeBuild
- CodeCommit: Introducción a CodeCommit
- CodeDeploy: Tutoriales
- CodePipeline: Introducción al CodePipeline

Si desea administrar usted mismo los permisos administrativos para las notificaciones de usuarios, grupos o roles de IAM, siga los procedimientos de este tema que le permitirán configurar los permisos y los recursos necesarios para utilizar el servicio.

Si desea utilizar temas de Amazon SNS que se hayan creado anteriormente para notificaciones en lugar de crear temas específicos para ellas, debe configurar un tema de Amazon SNS para utilizarlo como destino de una regla de notificación. Para ello, debe aplicar una política que permita publicar eventos en ese tema.

> **Note**
>
> Para realizar los siguientes procedimientos, debe haber iniciado sesión con una cuenta que tenga permisos administrativos. Para obtener más información, consulte Creación del primer grupo y usuario administrador de IAM.

Temas

- Creación y aplicación de una política para el acceso administrativo a notificaciones
- Configuración de los temas de Amazon SNS para las notificaciones

- Suscripción de usuarios a temas de Amazon SNS que son destinos

Creación y aplicación de una política para el acceso administrativo a notificaciones

Puede administrar notificaciones mediante el inicio de sesión con un usuario de IAM o mediante un rol que cuente con los permisos necesarios para acceder al servicio y a los servicios (AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy o AWS CodePipeline) en los que desee crear notificaciones. También puede crear sus propias políticas y aplicarlas a usuarios o grupos.

En el siguiente procedimiento, se muestra cómo configurar un grupo de IAM con permisos para administrar notificaciones y agregar usuarios de IAM. Si no desea configurar un grupo, puede aplicar esta política directamente a los usuarios de IAM o a un rol de IAM que los usuarios puedan asumir. También puede utilizar las políticas administradas para CodeBuild, CodeCommit, CodeDeploy o CodePipeline, que incluyen el acceso adecuado a las características de notificación según el alcance de la política.

En la siguiente política, introduzca un nombre (por ejemplo, `AWSCodeStarNotificationsFullAccess`) y una descripción opcional para esta política. La descripción le ayuda a recordar el propósito de la política (por ejemplo, **`This policy provides full access to AWS CodeStar Notifications.`**)

Para utilizar el editor de política de JSON para crear una política

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la izquierda, elija Policies (Políticas).

   Si es la primera vez que elige Policies (Políticas), aparecerá la página Welcome to Managed Policies (Bienvenido a políticas administradas). Elija Get Started (Comenzar).
3. En la parte superior de la página, seleccione Crear política.
4. En la sección Editor de políticas, seleccione la opción JSON.
5. Ingrese el siguiente 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. Elija Next (Siguiente).

> **Note**
>
> Puede alternar entre las opciones Visual y JSON del editor en todo momento. No obstante, si realiza cambios o selecciona Siguiente en la opción Visual del editor, es posible que IAM reestructure la política, con el fin de optimizarla para el editor visual. Para obtener más información, consulte Reestructuración de política en la Guía del usuario de IAM.

7. En la página Revisar y crear, escriba el Nombre de la política y la Descripción (opcional) para la política que está creando. Revise los Permisos definidos en esta política para ver los permisos que concede la política.
8. Elija Create Policy (Crear política) para guardar la nueva política.

Configuración de los temas de Amazon SNS para las notificaciones

La forma más sencilla de configurar las notificaciones consiste en crear un tema de Amazon SNS cuando crea una regla de notificación. Puede utilizar un tema de Amazon SNS existente si cumple los siguientes requisitos:

- Se creó en la misma Región de AWS que el recurso (proyecto de compilación, aplicación de implementación, repositorio o canalización) para el que desea crear reglas de notificación.
- No se ha utilizado para enviar notificaciones para CodeCommit antes del 5 de noviembre de 2019. Si lo ha hecho, contendrá las instrucciones de política que habilitaron esa funcionalidad. Puede optar por utilizar este tema, pero deberá agregar la política adicional especificada en el procedimiento. No debe quitar la declaración de política existente si uno o varios repositorios siguen configurados para notificaciones anteriores al 5 de noviembre de 2019.
- Tiene una política que permite a AWS CodeStar Notifications publicar notificaciones en el tema.

Para configurar un tema de Amazon SNS para utilizarlo como destino de las reglas de notificación de AWS CodeStar Notifications

1. Inicie sesión en AWS Management Console y abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En la barra de navegación, elija Topics (Temas), elija el tema que desea configurar y, a continuación, elija Edit (Editar).
3. Amplíe Access policy (Política de acceso) y, a continuación, elija Advanced (Avanzado).
4. En el editor JSON, agregue la siguiente instrucción a la política. Incluya el ARN del tema, la Región de AWS, el ID de la Cuenta de AWS y el nombre del tema.

```
 {
      "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"
    }
```

Esta instrucción de política debería ser como esta.

```
{
  "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. Elija Save changes (Guardar cambios).

6. Si desea utilizar un tema de Amazon SNS cifrado con AWS KMS para enviar notificaciones, también debe habilitar la compatibilidad entre la fuente del evento (AWS CodeStar Notifications) y el tema cifrado por medio de la adición de la siguiente instrucción a la política de AWS KMS key. Reemplace la Región de AWS (en este ejemplo, us-east-2) por la Región de AWS donde se creó la clave.

```
{
    "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 obtener más información, consulte Cifrado en reposo y Uso de condiciones de política con AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Suscripción de usuarios a temas de Amazon SNS que son destinos

Antes de que los usuarios puedan recibir notificaciones, deben estar suscritos al tema de Amazon SNS que es el destino de la regla de notificación. Si los usuarios están suscritos por correo electrónico, deben confirmar su suscripción antes de recibir notificaciones. Para enviar notificaciones a los usuarios de canales de Slack, canales de Microsoft Teams o salas de chat de Amazon Chime, consulte Configuración de la integración entre las notificaciones y AWS Chatbot.

Para suscribir a los usuarios a un tema de Amazon SNS utilizado para las notificaciones

1. Inicie sesión en AWS Management Console y abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, elija Topics (Temas) y, a continuación, elija el tema al que quiere suscribir a los usuarios.
3. En Subscriptions (Suscripciones), elija Create subscription (Crear suscripción).
4. En Protocol (Protocolo), elija Email (Correo electrónico). En Endpoint (Punto de enlace), introduzca la dirección de correo electrónico y, a continuación, elija Create subscription (Crear suscripción).

Introducción a las notificaciones

La forma más sencilla de comenzar con las notificaciones es configurar una regla de notificación en uno de sus proyectos de compilación, aplicaciones de implementación, canalizaciones o repositorios.

> **Note**
>
> La primera vez que crea una regla de notificación, se crea un rol vinculado al servicio en su cuenta. Para obtener más información, consulte Uso de roles vinculados a servicios para AWS CodeStar Notifications.

Temas

Requisitos previos

Realice los pasos que se indican en Configuración. También necesita un recurso para el que crear una regla de notificación.

- Cree un proyecto de compilación en CodeBuild o utilice uno ya existente.

- Cree una aplicación o utilice una aplicación de implementación ya existente.
- Cree una canalización en CodePipeline o utilice una ya existente.
- Cree un repositorio de AWS CodeCommit o utilice uno ya existente.

Creación de una regla de notificación para un repositorio

Puede crear reglas de notificación para enviar notificaciones sobre eventos del repositorio que son importantes para usted. En los siguientes pasos se muestra cómo configurar una regla de notificación en un único evento de repositorio. Estos pasos se escriben con la suposición de que tiene un repositorio configurado en su cuenta de AWS.

> **Important**
>
> Si ha configurado las notificaciones de CodeCommit antes del 5 de noviembre de 2019, los temas de Amazon SNS utilizados para esas notificaciones contendrán una política que permite a CodeCommit publicar en ella y que contenga permisos distintos a los necesarios para AWS CodeStar Notifications. No se recomienda usar estos temas. Si desea usar uno creado para dicha experiencia, debe agregar la política requerida a AWS CodeStar Notifications además de la que ya existe. Para obtener más información, consulte Configuración de los temas de Amazon SNS para las notificaciones y Descripción del contenido y la seguridad de las notificaciones.

1. Abra la consola de CodeCommit en https://console.aws.amazon.com/codecommit/.
2. Elija un repositorio de la lista y ábralo.
3. Elija Notify (Notificar) y, a continuación, elija Create notification rule (Crear regla de notificación). También puede elegir Settings (Configuración), elegir Notifications (Notificaciones) y, a continuación, elegir Create notification rule (Crear regla de notificación).
4. En Notification name (Nombre de la notificación), introduzca un nombre para la regla.
5. En Detail type (Tipo de detalle), elija Basic (Básico) si desea que solo la información proporcionada en Amazon EventBridge se incluya en la notificación. Elija Full (Completo) si desea incluir la información proporcionada en Amazon EventBridge y otra información que el servicio de recurso o el administrador de notificaciones podría suministrar.

   Para obtener más información, consulte Descripción del contenido y la seguridad de las notificaciones.

6. En Events that trigger notifications (Eventos que activan notificaciones), en Branches and tags (Ramas y etiquetas), selecciona Created (Creado).
7. En Targets (Destinos), elija Create SNS topic (Crear tema SNS).

> **Note**
>
> Cuando crea el tema como parte de la creación de la regla de notificación, se aplica la política que permite a CodeCommit publicar eventos en el tema. El uso de un tema creado para las reglas de notificación ayuda a garantizar que sólo suscriba a los usuarios que desea recibir notificaciones sobre este repositorio.

Después del prefijo codestar-notifications- escriba un nombre para el tema y, a continuación, elija Submit (Enviar).

> **Note**
>
> Si desea utilizar un tema de Amazon SNS existente en lugar de crear uno nuevo, en Targets (Destinos), elija su ARN. Asegúrese de que el tema tiene la política de acceso adecuada y de que la lista de suscriptores contiene solo aquellos usuarios que tienen permiso para ver información sobre el recurso. Si el tema de Amazon SNS corresponde a uno que se utilizaba para las notificaciones de CodeCommit antes del 5 de noviembre de 2019, contendrá una política que permite a CodeCommit publicar en ella y que contenga permisos distintos a los necesarios para AWS CodeStar Notifications. No se recomienda usar estos temas. Si desea usar uno creado para dicha experiencia, debe agregar la política requerida a AWS CodeStar Notifications además de la que ya existe. Para obtener más información, consulte Configuración de los temas de Amazon SNS para las notificaciones y Descripción del contenido y la seguridad de las notificaciones.

8. Elija Submit (Enviar) y, a continuación, revise la regla de notificación.
9. Suscriba su dirección de email al tema de Amazon SNS que acaba de crear. Para obtener más información, consulte Para suscribir a los usuarios a un tema de Amazon SNS utilizado para las notificaciones.
10. Vaya hasta el repositorio y cree una rama de prueba desde la rama predeterminada.
11. Después de crear la rama, la regla de notificación envía una notificación a todos los suscriptores del tema con información sobre ese evento.

Creación de una regla de notificación para un proyecto de compilación

Puede crear reglas de notificación para enviar notificaciones sobre los eventos del proyecto de compilación que son importantes para usted. En los siguientes pasos se muestra cómo configurar una regla de notificación en un único evento de proyecto de compilación. Estos pasos se escriben con la suposición de que tiene un proyecto de compilación configurado en su cuenta AWS.

1. Abra la consola de CodeBuild en https://console.aws.amazon.com/codebuild/.
2. Elija un proyecto de compilación de la lista y ábralo.
3. Elija Notify (Notificar) y, a continuación, elija Create notification rule (Crear regla de notificación). También puede elegir Settings (Configuración), y, a continuación, elegir Create notification rule (Crear regla de notificación).
4. En Notification name (Nombre de la notificación), introduzca un nombre para la regla.
5. En Detail type (Tipo de detalle), elija Basic (Básico) si desea que solo la información proporcionada en Amazon EventBridge se incluya en la notificación. Elija Full (Completo) si desea incluir la información proporcionada en Amazon EventBridge y otra información que el servicio de recurso o el administrador de notificaciones podría suministrar.

   Para obtener más información, consulte Descripción del contenido y la seguridad de las notificaciones.
6. En Events that trigger notifications (Eventos que activan notificaciones), en Build phase (Fase de compilación), seleccione Success (Correcto).
7. En Targets (Destinos), elija Create SNS topic (Crear tema SNS).

   > **Note**
   >
   > Cuando crea el tema como parte de la creación de la regla de notificación, se aplica la política que permite a CodeBuild publicar eventos en el tema. El uso de un tema creado para reglas de notificación ayuda a garantizar que sólo suscriba a los usuarios que desee que reciban notificaciones sobre este proyecto de compilación.

   Después del prefijo codestar-notifications- escriba un nombre para el tema y, a continuación, elija Submit (Enviar).

> **Note**
>
> Si desea utilizar un tema de Amazon SNS existente en lugar de crear uno nuevo, en Targets (Destinos), elija su ARN. Asegúrese de que el tema tiene la política de acceso adecuada y de que la lista de suscriptores contiene solo aquellos usuarios que tienen permiso para ver información sobre el recurso. Si el tema de Amazon SNS corresponde a uno que se utilizaba para las notificaciones de CodeCommit antes del 5 de noviembre de 2019, contendrá una política que permite a CodeCommit publicar en ella y que contenga permisos distintos a los necesarios para AWS CodeStar Notifications. No se recomienda usar estos temas. Si desea usar uno creado para dicha experiencia, debe agregar la política requerida a AWS CodeStar Notifications además de la que ya existe. Para obtener más información, consulte Configuración de los temas de Amazon SNS para las notificaciones y Descripción del contenido y la seguridad de las notificaciones.

8. Elija Submit (Enviar) y, a continuación, revise la regla de notificación.
9. Suscriba su dirección de email al tema de Amazon SNS que acaba de crear. Para obtener más información, consulte Para suscribir a los usuarios a un tema de Amazon SNS utilizado para las notificaciones.
10. Vaya al proyecto de compilación e inicie una compilación.
11. Una vez completada correctamente la fase de compilación, la regla de notificación envía a todos los suscriptores del tema una notificación con información sobre ese evento.

Creación de una regla de notificación para una aplicación de implementación

Puede crear reglas de notificación para enviar notificaciones sobre los eventos en la aplicación de implementación que son importantes para usted. En los siguientes pasos se muestra cómo configurar una regla de notificación en un único evento de proyecto de compilación. Estos pasos se escriben dando por hecho que tiene una aplicación de implementación configurada en su cuenta de AWS.

1. Abra la consola de CodeDeploy en https://console.aws.amazon.com/codedeploy/.
2. Elija una aplicación de la lista y ábrala.
3. Elija Notify (Notificar) y, a continuación, elija Create notification rule (Crear regla de notificación). También puede elegir Settings (Configuración), y, a continuación, elegir Create notification rule (Crear regla de notificación).

4. En Notification name (Nombre de la notificación), introduzca un nombre para la regla.
5. En Detail type (Tipo de detalle), elija Basic (Básico) si desea que solo la información proporcionada en Amazon EventBridge se incluya en la notificación. Elija Full (Completo) si desea incluir la información proporcionada en Amazon EventBridge y otra información que el servicio de recurso o el administrador de notificaciones podría suministrar.

   Para obtener más información, consulte Descripción del contenido y la seguridad de las notificaciones.

6. En Events that trigger notifications (Eventos que desencadenan notificaciones), en Deployment (Implementación), seleccione Succeeded (Correcto).
7. En Targets (Destinos), elija Create SNS topic (Crear tema SNS).

> **Note**
>
> Cuando crea el tema como parte de la creación de la regla de notificación, se aplica la política que permite a CodeDeploy publicar eventos en el tema. El uso de un tema creado para las reglas de notificación ayuda a garantizar que sólo suscriba a los usuarios que quiere que reciban notificaciones sobre esta aplicación de implementación.

Después del prefijo codestar-notifications- escriba un nombre para el tema y, a continuación, elija Submit (Enviar).

> **Note**
>
> Si desea utilizar un tema de Amazon SNS existente en lugar de crear uno nuevo, en Targets (Destinos), elija su ARN. Asegúrese de que el tema tiene la política de acceso adecuada y de que la lista de suscriptores contiene solo aquellos usuarios que tienen permiso para ver información sobre el recurso. Si el tema de Amazon SNS corresponde a uno que se utilizaba para las notificaciones de CodeCommit antes del 5 de noviembre de 2019, contendrá una política que permite a CodeCommit publicar en ella y que contenga permisos distintos a los necesarios para AWS CodeStar Notifications. No se recomienda usar estos temas. Si desea usar uno creado para dicha experiencia, debe agregar la política requerida a AWS CodeStar Notifications además de la que ya existe. Para obtener más información, consulte Configuración de los temas de Amazon SNS para las notificaciones y Descripción del contenido y la seguridad de las notificaciones.

8. Elija Submit (Enviar) y, a continuación, revise la regla de notificación.
9. Suscriba su dirección de email al tema de Amazon SNS que acaba de crear. Para obtener más información, consulte Para suscribir a los usuarios a un tema de Amazon SNS utilizado para las notificaciones.
10. Desplácese hasta la aplicación de implementación e inicie una implementación.
11. Una vez que la implementación se realiza correctamente, la regla de notificación envía una notificación a todos los suscriptores del tema con información sobre el evento.

Creación de una regla de notificación para una canalización

Puede crear reglas de notificación para enviar notificaciones sobre los eventos de la canalización que son importantes para usted. En los siguientes pasos se muestra cómo configurar una regla de notificación en un único evento de canalización. Estos pasos se escriben dando por hecho que tiene una canalización configurada en su cuenta AWS.

1. Abra la consola de CodePipeline en https://console.aws.amazon.com/codepipeline/.
2. Elija una canalización de la lista y ábrala.
3. Elija Notify (Notificar) y, a continuación, elija Create notification rule (Crear regla de notificación). También puede elegir Settings (Configuración), y, a continuación, elegir Create notification rule (Crear regla de notificación).
4. En Notification name (Nombre de la notificación), introduzca un nombre para la regla.
5. En Detail type (Tipo de detalle), elija Basic (Básico) si desea que solo la información proporcionada en Amazon EventBridge se incluya en la notificación. Elija Full (Completo) si desea incluir la información proporcionada en Amazon EventBridge y otra información que el servicio de recurso o el administrador de notificaciones podría suministrar.

   Para obtener más información, consulte Descripción del contenido y la seguridad de las notificaciones.
6. En Events that trigger notifications (Eventos que activan notificaciones), en Action execution (Ejecución de acciones), seleccione Started (Iniciado).
7. En Targets (Destinos), elija Create SNS topic (Crear tema SNS).

> **Note**
>
> Cuando crea el tema como parte de la creación de la regla de notificación, se aplica la política que permite a CodePipeline publicar eventos en el tema. El uso de un tema

creado para reglas de notificación ayuda a garantizar que sólo suscribe a los usuarios que quiere que reciban notificaciones sobre esta canalización.

Después del prefijo codestar-notifications- escriba un nombre para el tema y, a continuación, elija Submit (Enviar).

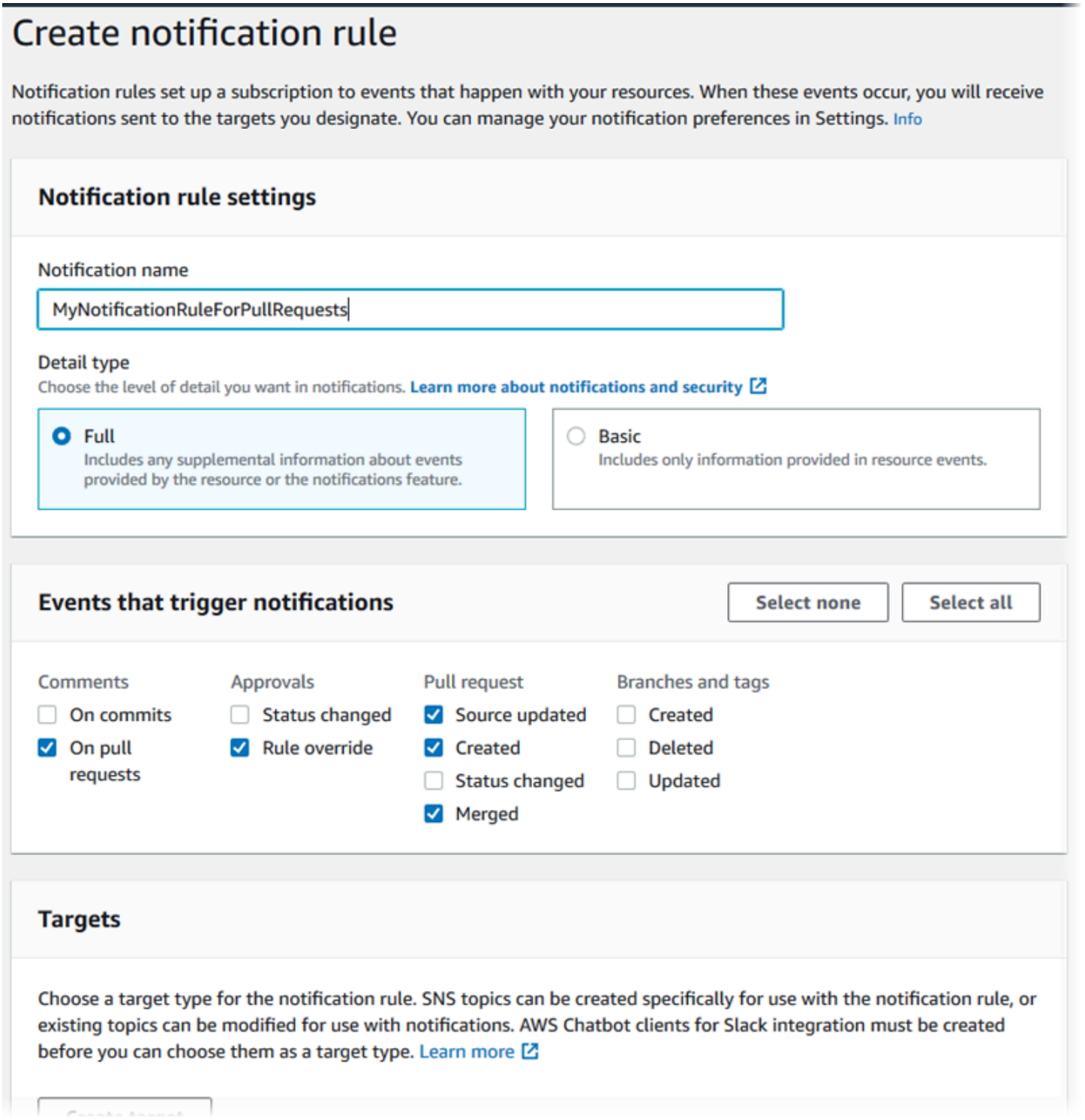
> **Note**
>
> Si desea utilizar un tema de Amazon SNS existente en lugar de crear uno nuevo, en Targets (Destinos), elija su ARN. Asegúrese de que el tema tiene la política de acceso adecuada y de que la lista de suscriptores contiene solo aquellos usuarios que tienen permiso para ver información sobre el recurso. Si el tema de Amazon SNS corresponde a uno que se utilizaba para las notificaciones de CodeCommit antes del 5 de noviembre de 2019, contendrá una política que permite a CodeCommit publicar en ella y que contenga permisos distintos a los necesarios para AWS CodeStar Notifications. No se recomienda usar estos temas. Si desea usar uno creado para dicha experiencia, debe agregar la política requerida a AWS CodeStar Notifications además de la que ya existe. Para obtener más información, consulte Configuración de los temas de Amazon SNS para las notificaciones y Descripción del contenido y la seguridad de las notificaciones.

8. Elija Submit (Enviar) y, a continuación, revise la regla de notificación.
9. Suscriba su dirección de email al tema de Amazon SNS que acaba de crear. Para obtener más información, consulte Para suscribir a los usuarios a un tema de Amazon SNS utilizado para las notificaciones.
10. Vaya a la canalización y, a continuación, elija Release change (Cambio de versión).
11. Cuando se inicia la acción, la regla de notificación envía una notificación a todos los suscriptores del tema con información sobre el evento.

Uso de las reglas de notificación

Una regla de notificación es aquella en la que puede configurar los eventos sobre los que desea que los usuarios reciban notificaciones y especificar los destinos que reciben dichas notificaciones. Puede enviar notificaciones directamente a los usuarios a través de Amazon SNS o a través de clientes de AWS Chatbot configurados para canales de Slack o Microsoft Teams. Si desea ampliar el alcance de las notificaciones, puede configurar manualmente la integración entre las notificaciones

y AWS Chatbot para que las notificaciones se envíen a las salas de chat de Amazon Chime. Para obtener más información, consulte implementación y Para integrar notificaciones en AWS Chatbot y Amazon Chime.



Puede utilizar la consola de herramientas para desarrolladores o la AWS CLI para crear y administrar reglas de notificación.

Temas

Creación de una regla de notificación

Puede utilizar la consola de herramientas para desarrolladores o la AWS CLI para crear reglas de notificación. Puede crear un tema de Amazon SNS para utilizarlo como destino de una regla de notificación durante la creación de la regla. Si desea utilizar un cliente de AWS Chatbot como destino, debe crearlo antes de crear la regla. Para obtener más información, consulte Configuración de un cliente de AWS Chatbot para un canal de Slack.

Para crear una regla de notificación (consola)

1. Abra la consola de las herramientas para desarrolladores de AWS en https://console.aws.amazon.com/codesuite/settings/notifications.
2. Utilice la barra de navegación para desplazarse hasta el recurso.
   - En CodeBuild, elija Build (Compilar). Luego, elija Build projects (Compilar proyectos) y elija un proyecto de compilación.
   - En CodeCommit, elija Source (Fuente), Luego, elija Repositories (Repositorios) y elija un repositorio.
   - En CodeDeploy, elija Applications (Aplicaciones) y elija una aplicación.
   - En CodePipeline, elija Pipeline (Canalización). Luego, elija Pipelines (Canalizaciones) y elija una canalización.
3. En la página de recursos, elija Notify (Notificar) y, a continuación, elija Create notification rule (Crear regla de notificación). También puede ir a la página Settings (Configuración) del recurso, ir a Notifications (Notificaciones) o Notification rules (Reglas de notificación) y elegir Create notification rule (Crear regla de notificación).
4. En Notification name (Nombre de la notificación), introduzca un nombre para la regla.

5. En Detail type (Tipo de detalle), elija Basic (Básico) si desea que solo la información proporcionada en Amazon EventBridge se incluya en la notificación. Elija Full (Completo) si desea incluir la información proporcionada en Amazon EventBridge y otra información que el servicio de recurso o el administrador de notificaciones podría suministrar.

   Para obtener más información, consulte Descripción del contenido y la seguridad de las notificaciones.

6. En Events that trigger notifications (Eventos que activan notificaciones), seleccione los eventos para los que desea enviar notificaciones. Para obtener información sobre los tipos de evento de un recurso, consulte lo siguiente:

   - CodeBuild: Eventos de reglas de notificación en proyectos de compilación
   - CodeCommit: Eventos de reglas de notificación en repositorios
   - CodeDeploy: Eventos de reglas de notificación en aplicaciones de implementación
   - CodePipeline: Eventos de reglas de notificación en canalizaciones

7. En Targets (Destinos), realice una de las siguientes operaciones:

   - Si ya ha configurado un recurso para utilizarlo con notificaciones, en Elegir tipo de destino, elija AWSChatbot (Slack), AWS Chatbot (Microsoft Teams) o Tema de SNS. En Elegir destino, elija el nombre del cliente (para un cliente de Slack o Microsoft Teams configurado en AWS Chatbot) o el nombre de recurso de Amazon (ARN) del tema de Amazon SNS (para los temas de Amazon SNS ya configurados con la política necesaria para las notificaciones).
   - Si no ha configurado un recurso para utilizarlo con notificaciones, elija Create target (Crear destino) y, a continuación, elija SNS topic (Tema de SNS). Indique el nombre del tema después de codestar-notifications- y, a continuación, elija Create (Crear).

   > **Note**
   >
   > - Si crea el tema de Amazon SNS durante la creación de la regla de notificación, se aplica la política que permite a la característica de notificaciones publicar eventos en el tema. El uso de un tema creado para las reglas de notificación lo ayuda a garantizar que solo suscriba a los usuarios que desea recibir notificaciones sobre este recurso.
   > - No se puede crear un cliente de AWS Chatbot durante la creación de una regla de notificación. Si elige AWS Chatbot (Slack) o AWS Chatbot (Microsoft Teams), aparecerá un botón que lo llevará a configurar un cliente en AWS Chatbot. Mediante

la elección de esa opción, se abrirá la consola de AWS Chatbot. Para obtener más información, consulte Configuración de un cliente de AWS Chatbot para un canal de Slack.

- Si desea utilizar un tema de Amazon SNS ya existente como destino, debe agregar la política necesaria para AWS CodeStar Notifications además de otras políticas que puedan existir para ese tema. Para obtener más información, consulte Configuración de los temas de Amazon SNS para las notificaciones y Descripción del contenido y la seguridad de las notificaciones.

8. Elija Submit (Enviar) y, a continuación, revise la regla de notificación.

> **Note**
>
> Los usuarios deben suscribirse al tema de Amazon SNS que usted haya especificado como destino de la regla y confirmar su suscripción antes de recibir las notificaciones. Para obtener más información, consulte Para suscribir a los usuarios a un tema de Amazon SNS utilizado para las notificaciones.

Para crear una regla de notificación (AWS CLI)

1. En un terminal o símbolo del sistema, ejecute el comando create-notification rule para generar el esqueleto JSON.

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

Puede asignar al archivo el nombre que desee. En este ejemplo, el archivo se denomina *rule.json*.

2. Abra el archivo JSON en un editor de texto sin formato y edítelo para incluir el recurso, los tipos de eventos y el destino de Amazon SNS que desea para la regla.

En el siguiente ejemplo, se muestra una regla de notificación denominada **MyNotificationRule** para un repositorio denominado *MyDemoRepo* en una cuenta de AWS con el ID *123456789012*. Las notificaciones con el tipo de detalle completo se envían a un

tema de Amazon SNS denominado *MyNotificationTopic* cuando se crean las ramas y las etiquetas.

```
{
    "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"
}
```

Guarde el archivo.

3. Mediante el archivo que acaba de modificar, en el terminal o línea de comandos, vuelva a ejecutar el comando create-notification-rule para crear la regla de notificación.

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

4. Si se ejecuta correctamente, el comando devuelve el ARN de la regla de notificación, similar a lo siguiente.

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

Para mostrar los tipos de eventos de las reglas de notificación (AWS CLI)

1. Ejecute el comando list-event-types en un terminal o en la línea de comandos. Puede utilizar la opción `--filters` para delimitar los resultados a un tipo de recurso específico u otro atributo.

Por ejemplo, lo siguiente devuelve una lista de tipos de eventos para las aplicaciones de CodeDeploy.

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

2. El resultado de este comando debería ser similar al siguiente.

```
{
    "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"
        }
    ]
}
```

Para añadir una etiqueta a una regla de notificación (AWS CLI)

1. Ejecute el comando tag-resource en un terminal o en la línea de comandos. Por ejemplo, utilice el siguiente comando para agregar un par de clave-valor de etiqueta que tenga el nombre *Team* y el 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. El resultado de este comando debería ser similar al siguiente.

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

Visualización de las reglas de notificación

Puede utilizar la consola de herramientas para desarrolladores o la AWS CLI para ver todas las reglas de notificación de todos los recursos de una región de AWS. También puede ver los detalles de cada regla de notificación. A diferencia del proceso de creación de una regla de notificación, no tiene que ir a la página de recursos del recurso.

Para ver las reglas de notificación (consola)

1. Abra la consola de las herramientas para desarrolladores de AWS en https://console.aws.amazon.com/codesuite/settings/notifications.
2. En la barra de navegación, amplíe Settings (Configuración) y, a continuación, elija Notification rules (Reglas de notificación).
3. En Notification rules (Reglas de notificación), revise la lista de reglas configuradas para los recursos en su Cuenta de AWS de la Región de AWS en la que ha iniciado sesión actualmente. Utilice el selector para cambiar la Región de AWS.
4. Para ver los detalles de una regla de notificación, elíjala en la lista y, a continuación, elija View details (Ver detalles). También puede simplemente elegir su nombre en la lista.

Para ver una lista de reglas de notificación (AWS CLI)

1. En un terminal o símbolo del sistema, ejecute el comando list-notification-rules para ver una lista de todas las reglas de notificación para la región de AWS especificada.

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

2. Si se ejecuta correctamente, este comando devuelve el ID y el ARN de cada regla de notificación de la región de AWS, similar a lo siguiente.

```
{
    "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"
        }
    ]
}
```

Para ver los detalles de una regla de notificación (AWS CLI)

1. En un terminal o símbolo del sistema, ejecute el comando describe-notification-rule, especificando el ARN de la regla de notificación.

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

2. Si se ejecuta correctamente, el comando devolverá información similar a la siguiente.

```
{
    "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"
}
```

Para ver una lista de las etiquetas de una regla de notificación (AWS CLI)

1. En un terminal o símbolo del sistema, ejecute el comando list-tags-for-resource para ver todas las etiquetas de un ARN de regla de notificación determinado.

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

2. Si se ejecuta correctamente, este comando proporciona información similar a la siguiente.

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

Edición de una regla de notificación

Puede editar una regla de notificación para cambiar su nombre, los eventos para los que envía notificaciones, el tipo de detalle o el destino o los destinos a los que envía notificaciones. Puede utilizar la consola de herramientas para desarrolladores o la AWS CLI para editar reglas de notificación.

Para editar una regla de notificación (consola)

1. Abra la consola de las herramientas para desarrolladores de AWS en https://console.aws.amazon.com/codesuite/settings/notifications.
2. En la barra de navegación, amplíe Settings (Configuración) y, a continuación, elija Notification rules (Reglas de notificación).

3. En Notification rules (Reglas de notificación), revise las reglas configuradas para los recursos en su cuenta de AWS en la Región de AWS en la que ha iniciado sesión actualmente. Utilice el selector para cambiar la Región de AWS.
4. Elija la regla de la lista y, a continuación, elija Edit (Editar). Realice sus cambios y, a continuación, elija Submit (Enviar).

Para editar una regla de notificación (AWS CLI)

1. En un terminal o símbolo del sistema, ejecute el comando describe-notification-rule para ver la estructura de la regla de notificación.
2. Ejecute el comando update-notification rule para generar el esqueleto JSON y guárdelo en un archivo.

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

Puede asignar al archivo el nombre que desee. En este ejemplo, el archivo es*update.json*.

3. Abra el archivo JSON en un editor de texto sin formato y realice cambios en la regla.

En el siguiente ejemplo, se muestra una regla de notificación denominada **MyNotificationRule** para un repositorio denominado *MyDemoRepo* en una cuenta de AWS con el ID *123456789012*. Cuando se crean ramas y etiquetas, las notificaciones se envían a un tema de Amazon SNS denominado *MyNotificationTopic*. El nombre de la regla se cambia a *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"
}
```

Guarde el archivo.

4. Mediante el archivo que acaba de modificar en el terminal o línea de comandos, vuelva a ejecutar el comando update-notification-rule para actualizar la regla de notificación.

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

5. Si se ejecuta correctamente, el comando devuelve el nombre de recurso de Amazon (ARN) de la regla de notificación, similar a lo siguiente.

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

Para eliminar una etiqueta de una regla de notificación (AWS CLI)

1. Ejecute el comando untag-resource en un terminal o en la línea de comandos. Por ejemplo, el siguiente comando elimina una etiqueta cuyo nombre es *Team*.

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

2. Si se ejecuta correctamente, este comando no devuelve nada.

Véase también

- Agregado o eliminación de un destino para una regla de notificación
- Habilitación o desactivación de notificaciones para una regla de notificación
- Eventos

Habilitación o desactivación de notificaciones para una regla de notificación

Al crear una regla de notificación, las notificaciones se habilitan de forma predeterminada. No es necesario eliminar la regla para evitar que envíe notificaciones. Simplemente puede cambiar su estado de notificación.

Para cambiar el estado de notificación de una regla de notificación (consola)

1. Abra la consola de las herramientas para desarrolladores de AWS en https://console.aws.amazon.com/codesuite/settings/notifications.
2. En la barra de navegación, amplíe Settings (Configuración) y, a continuación, elija Notification rules (Reglas de notificación).
3. En Notification rules (Reglas de notificación), revise las reglas configuradas para los recursos en su cuenta de AWS en la Región de AWS en la que ha iniciado sesión actualmente. Utilice el selector para cambiar la Región de AWS.
4. Busque la regla de notificación que desee habilitar o deshabilitar y selecciónela para mostrar sus detalles.
5. En Notification status (Estado de notificación), seleccione el control deslizante para cambiar el estado de la regla:
   - Sending notifications (Envío de notificaciones): este es el valor predeterminado.
   - Notifications paused (Notificaciones en pausa): no se envían notificaciones a los destinos especificados.

Para cambiar el estado de notificación de una regla de notificación (AWS CLI)

1. Siga los pasos de Para editar una regla de notificación (AWS CLI) para obtener el JSON para la regla de notificación.
2. Edite el campo `Status` a `ENABLED` (predeterminado) o `DISABLED` (sin notificaciones) y, a continuación, ejecute el comando update-notification-rule para cambiar el estado.

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

Eliminación de una regla de notificación

Solo puede haber 10 reglas de notificación configuradas para un recurso, así que considere la posibilidad de eliminar las reglas que ya no necesite. Puede utilizar la consola de herramientas para desarrolladores o la AWS CLI para eliminar reglas de notificación.

> **Note**
>
> No puede deshacer la eliminación de una regla de notificación, pero puede volver a crearla. Al eliminar una regla de notificación no se elimina el destino.

Para eliminar una regla de notificación (consola)

1. Abra la consola de las herramientas para desarrolladores de AWS en https://console.aws.amazon.com/codesuite/settings/notifications.
2. En la barra de navegación, amplíe Settings (Configuración) y, a continuación, elija Notification rules (Reglas de notificación).
3. En Notification rules (Reglas de notificación), revise las reglas configuradas para los recursos en su cuenta de AWS en la Región de AWS en la que ha iniciado sesión actualmente. Utilice el selector para cambiar la Región de AWS.
4. Elija la regla de notificación y, a continuación, elija Delete (Eliminar).
5. Escriba **`delete`** y seleccione Delete (Eliminar).

Para eliminar una regla de notificación (AWS CLI)

1. En un terminal o símbolo del sistema, ejecute el comando delete-notification-rule, especificando el ARN de la regla de notificación.

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

2. Si se ejecuta correctamente, el comando devuelve el ARN de la regla de notificación eliminada, similar a lo siguiente.

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

```
}
```

Uso de los destinos de reglas de notificación

Un destino de regla de notificación es un destino que define adónde desea que se envíen las notificaciones cuando se cumplen las condiciones de evento de una regla de notificación. Puede elegir entre temas de Amazon SNS y clientes de AWS Chatbot configurados para los canales de Slack o Microsoft Teams. Puede crear un tema de Amazon SNS como destino durante la creación de una regla de notificación (recomendado). También puede elegir un tema de Amazon SNS existente que se encuentre en la misma región de AWS que la regla de notificación, pero debe configurarlo con la política requerida. Si decide utilizar un cliente de AWS Chatbot como destino, primero debe crear ese cliente en AWS Chatbot.

Si desea ampliar el alcance de las notificaciones, puede configurar manualmente la integración entre las notificaciones y AWS Chatbot para que las notificaciones se envíen a las salas de chat de Amazon Chime. A continuación, puede elegir el tema de Amazon SNS configurado para ese cliente de AWS Chatbot como destino de la regla de notificación. Para obtener más información, consulte Para integrar notificaciones en AWS Chatbot y Amazon Chime.

Puede utilizar la consola de herramientas para desarrolladores o la AWS CLI para administrar reglas de notificación. Puede utilizar la consola o la AWS CLI para crear y configurar temas de Amazon SNS y clientes de AWS Chatbot como destinos. También puede configurar la integración entre los temas de Amazon SNS que configure como destinos y AWS Chatbot. Esto te permite enviar notificaciones a las salas de chat de Amazon Chime. Para obtener más información, consulte Configuración de la integración entre las notificaciones y AWS Chatbot.

Temas

- Creación o configuración de un destino de regla de notificación
- Visualización de destinos de reglas de notificación
- Agregado o eliminación de un destino para una regla de notificación
- Eliminación de un destino de regla de notificación

Creación o configuración de un destino de regla de notificación

Los destinos de reglas de notificación son temas de Amazon SNS o clientes de AWS Chatbot configurados para canales de Slack o Microsoft Teams.

El cliente de AWS Chatbot debe haberse creado antes de seleccionarlo como destino. Cuando se elige un cliente de AWS Chatbot como destino para una regla de notificación, se configura un tema de Amazon SNS para ese cliente de AWS Chatbot con todas las políticas necesarias para que las notificaciones se envíen al canal de Slack o Microsoft Teams. No es necesario configurar ningún tema de Amazon SNS existente para el cliente de AWS Chatbot.

Puede crear destinos de reglas de notificación de Amazon SNS en la consola de herramientas para desarrolladores cuando cree una regla de notificación. La política que permite enviar notificaciones a ese tema se aplica para usted. Esta es la forma más fácil de crear un destino para una regla de notificación. Para obtener más información, consulte Creación de una regla de notificación.

Si utiliza un tema de Amazon SNS ya existente, debe configurarlo con una política de acceso que permita que el recurso envíe notificaciones a ese tema. Para ver un ejemplo, consulte Configuración de los temas de Amazon SNS para las notificaciones.

> **Note**
>
> Si desea utilizar un tema de Amazon SNS existente en lugar de crear uno nuevo, en Targets (Destinos), elija su ARN. Asegúrese de que el tema tiene la política de acceso adecuada y de que la lista de suscriptores contiene solo aquellos usuarios que tienen permiso para ver información sobre el recurso. Si el tema de Amazon SNS corresponde a uno que se utilizaba para las notificaciones de CodeCommit antes del 5 de noviembre de 2019, contendrá una política que permite a CodeCommit publicar en ella y que contenga permisos distintos a los necesarios para AWS CodeStar Notifications. No se recomienda usar estos temas. Si desea usar uno creado para dicha experiencia, debe agregar la política requerida a AWS CodeStar Notifications además de la que ya existe. Para obtener más información, consulte Configuración de los temas de Amazon SNS para las notificaciones y Descripción del contenido y la seguridad de las notificaciones.

Si desea ampliar el alcance de las notificaciones, puede configurar manualmente la integración entre las notificaciones y AWS Chatbot para que las notificaciones se envíen a las salas de chat de Amazon Chime. Para obtener más información, consulte implementación y Para integrar notificaciones en AWS Chatbot y Amazon Chime.

Para configurar un tema de Amazon SNS ya existente para utilizarlo como destino de regla de notificación (consola)

1. Inicie sesión en AWS Management Console y abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En la barra de navegación, elija Topics. Elija el tema y, a continuación, seleccione Edit (Editar).
3. Amplíe Access policy (Política de acceso) y, a continuación, elija Advanced (Avanzado).
4. En el editor JSON, agregue la siguiente instrucción a la política. Incluya el ARN del tema, la Región de AWS, el ID de la Cuenta de AWS y el nombre del tema.

```
 {
      "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"
    }
```

Esta instrucción de política debería ser como esta.

```
{
  "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. Elija Save changes (Guardar cambios).
6. En Subscriptions (Suscripciones), revise la lista de suscriptores de temas. Añada, edite o elimine suscriptores según corresponda para este destino de regla de notificación. Asegúrese de que la lista de suscriptores contiene sólo aquellos usuarios que tienen permiso para ver información sobre el recurso. Para obtener más información, consulte Descripción del contenido y la seguridad de las notificaciones.

Para crear un cliente de AWS Chatbot con Slack para usarlo como destino

1. Siga las instrucciones que se muestran en Configuración de AWS Chatbot con Slack en la Guía del administrador de AWS Chatbot. Al hacerlo, estudie las siguientes opciones para realizar una integración óptima con las notificaciones:

- Cuando se crea un rol de IAM, es conveniente elegir un nombre de rol que permita identificar fácilmente el propósito de este rol (por ejemplo, **`AWSCodeStarNotifications-Chatbot-Slack-Role`**). Esto puede ayudarle a identificar el propósito del rol en el futuro.
- En SNS topics (Temas de SNS), no tiene que elegir un tema o una región de AWS. Cuando se elige el cliente de AWS Chatbot como destino, se crea un tema de Amazon SNS con todos los permisos necesarios y se configura para el cliente de AWS Chatbot durante el proceso de creación de las reglas de notificación.

2. Complete el proceso de creación del cliente. Este cliente estará disponible para que pueda elegirlo como destino al crear reglas de notificación. Para obtener más información, consulte Creación de una regla de notificación.

> **Note**
>
> No elimine el tema de Amazon SNS del cliente de AWS Chatbot después de configurarlo. Si lo hace, impedirá que las notificaciones se envíen a Slack.

Para crear un cliente de AWS Chatbot con Microsoft Teams para usarlo como destino

1. Siga las instrucciones que se muestran en Configuración de AWS Chatbot con Microsoft Teams en la Guía del administrador de AWS Chatbot. Al hacerlo, estudie las siguientes opciones para realizar una integración óptima con las notificaciones:

   - Cuando se crea un rol de IAM, es conveniente elegir un nombre de rol que permita identificar fácilmente el propósito de este rol (por ejemplo, **`AWSCodeStarNotifications-Chatbot-Microsoft-Teams-Role`**). Esto puede ayudarle a identificar el propósito del rol en el futuro.
   - En SNS topics (Temas de SNS), no tiene que elegir un tema o una región de AWS. Cuando se elige el cliente de AWS Chatbot como destino, se crea un tema de Amazon SNS con todos los permisos necesarios y se configura para el cliente de AWS Chatbot durante el proceso de creación de las reglas de notificación.

2. Complete el proceso de creación del cliente. Este cliente estará disponible para que pueda elegirlo como destino al crear reglas de notificación. Para obtener más información, consulte Creación de una regla de notificación.

> **Note**
>
> No elimine el tema de Amazon SNS del cliente de AWS Chatbot después de configurarlo. Si lo hace, impedirá que las notificaciones se envíen a Microsoft Teams.

Visualización de destinos de reglas de notificación

Puede utilizar la consola de herramientas para desarrolladores, en lugar de la consola de Amazon SNS, para ver todos los destinos de la regla de notificación de todos los recursos de una región de AWS. También puede ver los detalles de un destino de regla de notificación.

Para ver los destinos de reglas de notificación (consola)

1. Abra la consola de las herramientas para desarrolladores de AWS en https://console.aws.amazon.com/codesuite/settings/notifications.
2. En la barra de navegación, amplíe Settings (Configuración) y, a continuación, elija Notification rules (Reglas de notificación).
3. En Notification rule targets (Destinos de reglas de notificación), revise la lista de destinos utilizados por las reglas de notificación en su Cuenta de AWS de la Región de AWS en la que ha iniciado sesión actualmente. Utilice el selector para cambiar la Región de AWS. Si el estado del destino aparece como Unreachable (Ilocalizable), es posible que deba investigar los motivos. Para obtener más información, consulte Solución de problemas .

Para ver una lista de destinos de reglas de notificación (AWS CLI)

1. En un terminal o símbolo del sistema, ejecute el comando list-targets para ver una lista de todos los destinos de reglas de notificación para la región de AWS especificada:

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

2. Si se ejecuta correctamente, este comando devuelve el ID y el ARN de cada regla de notificación de la región de AWS, similar a lo siguiente:

```
{
    "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"
        }
    ]
}
```

Agregado o eliminación de un destino para una regla de notificación

Puede editar una regla de notificación para cambiar el destino o los destinos a los que se envían notificaciones. Puede utilizar la consola de herramientas para desarrolladores o la AWS CLI para cambiar los destinos de una regla de notificación.

Para cambiar los destinos de una regla de notificación (consola)

1. Abra la consola de las herramientas para desarrolladores de AWS en https://console.aws.amazon.com/codesuite/settings/notifications.
2. En la barra de navegación, amplíe Settings (Configuración) y, a continuación, elija Notification rules (Reglas de notificación).
3. En Notification rules (Reglas de notificación), revise la lista de reglas configuradas para los recursos en su AWS de la Región de AWS en la que ha iniciado sesión actualmente. Utilice el selector para cambiar la Región de AWS.
4. Elija la regla y, a continuación, elija Edit (Editar).
5. En Targets (Destinos), realice una de las siguientes operaciones:

- Para añadir otro destino, elija Agregar destino y, a continuación, elija en la lista el tema de Amazon SNS o el cliente de AWS Chatbot (Slack) o AWS Chatbot (Microsoft Teams) que desee añadir. También puede elegir Create SNS topic (Crear tema SNS) para crear un tema y agregarlo como destino. Una regla de notificación puede tener hasta 10 destinos.
- Para eliminar un destino, elija Remove target (Eliminar destino) junto al destino que desea eliminar.

6. Elija Submit (Enviar).

Para añadir un destino a una regla de notificación (AWS CLI)

1. En un terminal o símbolo del sistema, ejecute el comando subscribe para agregar un destino. Por ejemplo, el siguiente comando agrega un tema de Amazon SNS como destino para una regla de notificación.

```
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. Si se ejecuta correctamente, el comando devuelve el ARN de la regla de notificación actualizada, similar a lo siguiente.

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

Para eliminar un destino de una regla de notificación (AWS CLI)

1. En una terminal o símbolo del sistema, ejecute el comando unsubscribe para eliminar un destino. Por ejemplo, el siguiente comando elimina un tema de Amazon SNS como destino para una regla de notificación.

```
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. Si se ejecuta correctamente, el comando devuelve el ARN de la regla de notificación actualizada e información sobre el destino eliminado, similar a lo siguiente.

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

Véase también

- Edición de una regla de notificación
- Habilitación o desactivación de notificaciones para una regla de notificación

Eliminación de un destino de regla de notificación

Puede eliminar un destino si ya no es necesario. Un recurso solo puede tener 10 destinos de reglas de notificación configurados, de modo que la eliminación de destinos innecesarios puede ayudar a crear espacio para otros destinos que tal vez desee agregar a dicha regla de notificación.

> **Note**
>
> La eliminación de un destino de regla de notificación elimina el destino de todas las reglas de notificación configuradas para utilizarlo como destino, pero no elimina el destino en sí.

Para eliminar un destino de regla de notificación (consola)

1. Abra la consola de las herramientas para desarrolladores de AWS en https://console.aws.amazon.com/codesuite/settings/notifications.
2. En la barra de navegación, amplíe Settings (Configuración) y, a continuación, elija Notification rules (Reglas de notificación).
3. En Notification rule targets (Destinos de reglas de notificación), revise la lista de destinos configurados para los recursos en su cuenta de AWS de la Región de AWS en la que ha iniciado sesión actualmente. Utilice el selector para cambiar la Región de AWS.
4. Elija el destino de la regla de notificación y, a continuación, elija Delete (Eliminar).
5. Escriba **`delete`** y seleccione Delete (Eliminar).

Para eliminar un destino de regla de notificación (AWS CLI)

1. En un terminal o símbolo del sistema, ejecute el comando delete-target, especificando el ARN del destino. Por ejemplo, el siguiente comando elimina un destino que utiliza un tema de Amazon SNS.

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

2. Si se ejecuta correctamente, el comando no devuelve nada. Si no se ejecuta correctamente, el comando devuelve un error. El error más común es que el tema sea el destino de una o varias reglas de notificación.

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

   Puede utilizar el parámetro `--force-unsubscribe-all` para eliminar el destino de todas las reglas de notificación configuradas para utilizarlo como destino y, a continuación, eliminar el destino.

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

Configuración de la integración entre las notificaciones y AWS Chatbot

AWS Chatbot es un servicio de AWS que permite a los equipos de desarrollo de software y DevOps utilizar las salas de chat de Amazon Chime, los canales de Slack y los canales de Microsoft Teams para monitorizar eventos operativos en la Nube de AWS y responder a ellos. Puede configurar la integración entre los destinos de reglas de notificación y AWS Chatbot para que las notificaciones sobre los eventos aparezcan en la sala de chat de Amazon Chime, en el canal de Slack o en el canal de Microsoft Teams que elija. Para obtener más información, consulte la documentación de AWS Chatbot.

Antes de configurar la integración con AWS Chatbot, debe configurar una regla de notificación y un destino de regla. Para obtener más información, consulte Configuración y Creación de una regla de notificación. También debe configurar un canal de Slack, un canal de Microsoft Teams o una sala de chat de Amazon Chime en AWS Chatbot. Para obtener más información, consulte la documentación de estos servicios.

Temas

Configuración de un cliente de AWS Chatbot para un canal de Slack

Puede crear reglas de notificación que utilicen un cliente de AWS Chatbot como destino. Si crea un cliente para un canal de Slack, puede utilizarlo directamente como destino en el flujo de trabajo para crear una regla de notificación. Esta es la forma más fácil de configurar las notificaciones que aparecen en los canales de Slack.

Para crear un cliente de AWS Chatbot con Slack para usarlo como destino

1. Siga las instrucciones que se muestran en Configuración de AWS Chatbot con Slack en la Guía del administrador de AWS Chatbot. Al hacerlo, estudie las siguientes opciones para realizar una integración óptima con las notificaciones:

   - Cuando se crea un rol de IAM, es conveniente elegir un nombre de rol que permita identificar fácilmente el propósito de este rol (por ejemplo, **`AWSCodeStarNotifications-Chatbot-Slack-Role`**). Esto puede ayudarle a identificar el propósito del rol en el futuro.
   - En SNS topics (Temas de SNS), no tiene que elegir un tema o una región de AWS. Cuando se elige el cliente de AWS Chatbot como destino, se crea un tema de Amazon SNS con todos los permisos necesarios y se configura para el cliente de AWS Chatbot durante el proceso de creación de las reglas de notificación.

2. Complete el proceso de creación del cliente. Este cliente estará disponible para que pueda elegirlo como destino al crear reglas de notificación. Para obtener más información, consulte Creación de una regla de notificación.

> **Note**
>
> No elimine el tema de Amazon SNS del cliente de AWS Chatbot después de configurarlo. Si lo hace, impedirá que las notificaciones se envíen a Slack.

Configuración de un cliente de AWS Chatbot para un canal de Microsoft Teams

Puede crear reglas de notificación que utilicen un cliente de AWS Chatbot como destino. Si crea un cliente para un canal de Microsoft Teams, puede utilizarlo directamente como destino en el flujo de trabajo para crear una regla de notificación. Esta es la forma más fácil de configurar las notificaciones que aparecen en los canales de Microsoft Teams.

Para crear un cliente de AWS Chatbot con Microsoft Teams para usarlo como destino

1. Siga las instrucciones que se muestran en Configuración de AWS Chatbot con Microsoft Teams en la Guía del administrador de AWS Chatbot. Al hacerlo, estudie las siguientes opciones para realizar una integración óptima con las notificaciones:

   - Cuando se crea un rol de IAM, es conveniente elegir un nombre de rol que permita identificar fácilmente el propósito de este rol (por ejemplo, **`AWSCodeStarNotifications-Chatbot-Microsoft-Teams-Role`**). Esto puede ayudarle a identificar el propósito del rol en el futuro.
   - En SNS topics (Temas de SNS), no tiene que elegir un tema o una región de AWS. Cuando se elige el cliente de AWS Chatbot como destino, se crea un tema de Amazon SNS con todos los permisos necesarios y se configura para el cliente de AWS Chatbot durante el proceso de creación de las reglas de notificación.

2. Complete el proceso de creación del cliente. Este cliente estará disponible para que pueda elegirlo como destino al crear reglas de notificación. Para obtener más información, consulte Creación de una regla de notificación.

   > **Note**
   >
   > No elimine el tema de Amazon SNS del cliente de AWS Chatbot después de configurarlo. Si lo hace, impedirá que las notificaciones se envíen a Microsoft Teams.

Configuración manual de clientes para Slack o Amazon Chime

Puede elegir crear la integración entre las notificaciones y Slack o Amazon Chime directamente. Este es el único método disponible para configurar notificaciones en las salas de chat de Amazon Chime. Cuando configura esta integración de forma manual, se crea un cliente de AWS Chatbot que utiliza un tema de Amazon SNS configurado previamente como destino para una regla de notificación.

Para integrar notificaciones manualmente en AWS Chatbot y Slack

1. Abra la consola de las herramientas para desarrolladores de AWS en https://console.aws.amazon.com/codesuite/settings/notifications.
2. Elija Settings (Configuración) y, a continuación, elija Notification rules (Reglas de notificación).
3. En Notification rule targets (Destinos de regla de notificación), busque y copie el destino.

   > **Note**
   >
   > Puede configurar más de una regla de notificación para utilizar el mismo tema de Amazon SNS que su destino. Esto puede ayudarle a consolidar la mensajería, pero puede tener consecuencias no deseadas si la lista de suscripciones está destinada a un recurso o regla de notificación.

4. Abra la consola de AWS Chatbot en https://console.aws.amazon.com/chatbot/.
5. Elija Configure new client (Configurar nuevo cliente) y, a continuación, seleccione Slack.
6. Elija Configure.
7. Inicie sesión en su espacio de trabajo de Slack.
8. Si se le pide que confirme las opciones, elija Allow (Permitir).
9. Elija Configure new channel (Configurar nuevo canal).
10. En Configuration details (Detalles de configuración), escriba el nombre para el cliente en Configuration name (Nombre de configuración). Este es el nombre que aparecerá en la lista de destinos disponibles para el tipo de destino de AWS Chatbot (Slack) cuando se crean reglas de notificación.
11. En Configure Slack Channel (Configurar canal de Slack), en Channel type (Tipo de canal), elija Public (Público) o Private (Privado), en función del tipo de canal que desee integrar.

    - En Public channel (Canal público), elija el nombre del canal Slack de la lista.
    - En Private channel ID (ID de canal privado), introduzca el código de canal o la URL.

12. En IAM permissions (Permisos de IAM), en Role (Rol), elija Create an IAM role using a template (Crear un rol de IAM con una plantilla). En Policy template (Plantillas de políticas), elija Notification permissions (Permisos de notificación). En Role name (Nombre del rol), introduzca un nombre para este rol (por ejemplo, **`AWSCodeStarNotifications-Chatbot-Slack-Role`**). En Policy template (Plantillas de políticas), elija Notification permissions (Permisos de notificación).

13. En SNS topics (Temas de SNS), en SNS Region (Región de SNS), elija la Región de AWS en la que creó el destino de regla de notificación. En SNS topics (Temas de SNS), elija el nombre del tema de Amazon SNS que ha configurado como el destino de regla de notificación.

    > **Note**
    >
    > Este paso no es necesario si va a crear una regla de notificación utilizando este cliente como destino.

14. Elija Configure.

    > **Note**
    >
    > Si configuró la integración con un canal privado, debe invitar a AWS Chatbot a ese canal para poder ver las notificaciones que aparecen en él. Para obtener más información, consulte la documentación de AWS Chatbot.

15. (Opcional) Para probar la integración, realice un cambio en el recurso que coincida con un tipo de evento de una regla de notificación configurada para utilizar el tema de Amazon SNS como destino. Por ejemplo, si tiene una regla de notificación configurada para enviar notificaciones cuando se realizan comentarios sobre una solicitud de extracción, realice un comentario sobre una solicitud de extracción y, a continuación, vea el canal de Slack en el navegador para ver cuándo aparece la notificación.

Para integrar notificaciones en AWS Chatbot y Amazon Chime

1. Abra la consola de las herramientas para desarrolladores de AWS en https://console.aws.amazon.com/codesuite/settings/notifications.
2. Elija Settings (Configuración) y, a continuación, elija Notification rules (Reglas de notificación).
3. En Notification rule targets (Destinos de regla de notificación), busque y copie el destino.

    > **Note**
    >
    > Puede configurar más de una regla de notificación para utilizar el mismo tema de Amazon SNS que su destino. Esto puede ayudarle a consolidar la mensajería, pero también puede tener consecuencias no deseadas si la lista de suscripciones está destinada a un recurso o regla de notificación.

4. En Amazon Chime, abra la sala de chat que desea configurar para la integración.
5. Elija el icono de engranaje en la esquina superior derecha y, a continuación, seleccione Manage webhooks (Administrar webhooks).
6. En el cuadro de diálogo Manage webhooks (Administrar webhooks), elija New (Nuevo), escriba un nombre para el webhook y a continuación elija Create (Crear).
7. Compruebe que aparece el webhook y, a continuación, elija Copy webhook URL (Copiar URL del webhook).
8. Abra la consola de AWS Chatbot en https://console.aws.amazon.com/chatbot/.
9. Elija Configure new client (Configurar nuevo cliente) y, a continuación, elija Amazon Chime.
10. En Configuration details (Detalles de configuración), escriba el nombre para el cliente en Configuration name (Nombre de configuración).
11. En Webhook URL (URL de webhook), pegue la URL. En Webhook description (descripción de Webhook), proporcione una descripción opcional.
12. En IAM permissions (Permisos de IAM), en Role (Rol), elija Create an IAM role using a template (Crear un rol de IAM con una plantilla). En Policy template (Plantillas de políticas), elija Notification permissions (Permisos de notificación). En Role name (Nombre del rol), introduzca un nombre para este rol (por ejemplo, **`AWSCodeStarNotifications-Chatbot-Chime-Role`**).
13. En SNS topics (Temas de SNS), en SNS Region (Región de SNS), elija la Región de AWS en la que creó el destino de regla de notificación. En SNS topics (Temas de SNS), elija el nombre del tema de Amazon SNS que ha configurado como el destino de regla de notificación.
14. Elija Configure.
15. (Opcional) Para probar la integración, realice un cambio en el recurso que coincida con un tipo de evento de una regla de notificación configurada para utilizar el tema de Amazon SNS como destino. Por ejemplo, si tiene una regla de notificación configurada para enviar notificaciones cuando se realizan comentarios sobre una solicitud de extracción, realice un comentario sobre una de ellas y, a continuación, consulte la sala de chat de Amazon Chime para comprobar cuándo aparece la notificación.

Registro de llamadas a la API de AWS CodeStar Notifications con AWS CloudTrail

AWS CodeStar Notifications se integra a AWS CloudTrail, un servicio que proporciona un registro de las acciones que realiza un usuario, un rol o un servicio de AWS. CloudTrail captura todas las

llamadas a la API para las notificaciones en forma de eventos. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de herramientas para desarrolladores y las llamadas de código a las operaciones de la API de AWS CodeStar Notifications. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos para las notificaciones. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Event history (Historial de eventos). Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a AWS CodeStar Notifications, la dirección IP desde la cual se realizó, quién la realizó y cuándo, etc.

Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Información sobre AWS CodeStar Notifications en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando la crea. Cuando se produce una actividad en AWS CodeStar Notifications, dicha actividad se registra en un evento de CloudTrail junto con los eventos de los demás servicios de AWS en Event history (Historial de eventos). Puede ver, buscar y descargar los últimos eventos de la Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de eventos de CloudTrail.

Para el registro continuo de los eventos de su Cuenta de AWS, incluidos los eventos de AWS CodeStar Notifications, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recibir archivos de registro de CloudTrail de varias cuentas

CloudTrail registra todas las acciones de AWS CodeStar Notifications y se documentan en la *Referencia de la API de AWS CodeStar Notifications*. Por ejemplo, las llamadas a las

acciones `CreateNotificationRule`, `Subscribe` y `ListEventTypes` generan entradas en los archivos de registros de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el elemento userIdentity de CloudTrail.

Descripción de las entradas de los archivos de registro de

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la creación de una regla de notificación, incluidas las acciones `CreateNotificationRule` y `Subscribe`.

> **Note**
>
> Algunos de los eventos de las entradas del archivo de registros de notificaciones podrían proceder del rol vinculado a servicios 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"
}
```

Solución de problemas

La siguiente información puede ayudarle a solucionar problemas habituales con las notificaciones.

Temas

- Aparece un error de permisos cuando intento crear una regla de notificación en un recurso.
- No se pueden visualizar las reglas de notificación
- No puedo crear reglas de notificación.
- Recibo notificaciones para un recurso al que no puedo tener acceso.
- No recibo notificaciones de Amazon SNS
- Recibo notificaciones duplicadas sobre eventos.
- Quiero comprender por qué el estado de un destino de notificación se muestra como “Unreachable” (Ilocalizable)
- Quiero aumentar mis cuotas de notificaciones y recursos

Aparece un error de permisos cuando intento crear una regla de notificación en un recurso.

Asegúrese de que tiene permisos suficientes. Para obtener más información, consulte Ejemplos de políticas basadas en identidades.

No se pueden visualizar las reglas de notificación

Problema: cuando se encuentra en la consola de herramientas para desarrolladores y elige Notificaciones (Notificaciones) en la pestaña Settings (Configuración), aparecerá un error de permisos.

Soluciones posibles: es posible que no cuente con los permisos necesarios para ver las notificaciones. Si bien la mayoría de las políticas administradas para los servicios de las herramientas para desarrolladores de AWS, como CodeCommit y CodePipeline, incluyen permisos para las notificaciones, los servicios que actualmente no admiten notificaciones tampoco tienen permisos para verlas. Otra posibilidad es que tenga una política personalizada aplicada a su usuario o rol de IAM que no le permita ver las notificaciones. Para obtener más información, consulte Ejemplos de políticas basadas en identidades.

No puedo crear reglas de notificación.

Es posible que no tenga los permisos necesarios para crear una regla de notificación. Para obtener más información, consulte Ejemplos de políticas basadas en identidades.

Recibo notificaciones para un recurso al que no puedo tener acceso.

Cuando crea una regla de notificación y agrega un destino, la característica de notificaciones no valida si el destinatario tiene acceso al recurso. Es posible que reciba notificaciones sobre un recurso al que no puede tener acceso. Si no puede eliminarse usted mismo, solicite que le eliminen de la lista de suscripciones del destino.

No recibo notificaciones de Amazon SNS

Para solucionar problemas con el tema de Amazon SNS, verifique lo siguiente:

- Asegúrese de que el tema de Amazon SNS se creó en la misma región de AWS que la regla de notificación.

- Asegúrese de que su alias de correo electrónico está suscrito al tema correcto y de que ha confirmado la suscripción. Para obtener más información, consulte Suscripción de un punto de enlace a un tema de Amazon SNS.
- Compruebe que la política del tema se ha editado para permitir a AWS CodeStar Notifications enviar notificaciones push a dicho tema. La política de temas debe incluir una instrucción similar a la siguiente:

```
{
    "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 obtener más información, consulte Configuración de los temas de Amazon SNS para las notificaciones.

Recibo notificaciones duplicadas sobre eventos.

Estas son las razones más comunes para recibir notificaciones múltiples:

- Se han configurado varias reglas de notificación que incluyen el mismo tipo de evento para un recurso y está suscrito a los temas de Amazon SNS que son los destinos de dichas reglas. Para solucionar este problema, cancele la suscripción a uno de los temas o edite las reglas de notificación para eliminar la duplicación.
- Uno o varios destinos de reglas de notificación están integrados en AWS Chatbot y usted recibe notificaciones tanto en la bandeja de entrada de su email como en un canal de Slack, en un canal de Microsoft Teams o en la sala de chat de Amazon Chime. Para solucionar este problema, tenga en cuenta la posibilidad de cancelar la suscripción de su dirección de email al tema de

Amazon SNS, que es el destino de la regla, y usar el canal de Slack, el canal de Microsoft Teams o la sala de chat de Amazon Chime para ver las notificaciones.

Quiero comprender por qué el estado de un destino de notificación se muestra como “Unreachable” (Ilocalizable)

Los destinos tienen dos estados posibles: Active (Activo) o Unreachable (Ilocalizable). Unreachable (Ilocalizable) indica que las notificaciones se enviaron a un destino y que la entrega no se realizó correctamente. Las notificaciones se siguen enviando a ese destino y, si se entregan correctamente, el estado se restablece a Active (Activo).

Es posible que el destino de una regla de notificación no esté disponible por alguno de los siguientes motivos:

- Se ha eliminado el recurso (tema de Amazon SNS o cliente de AWS Chatbot). Elija otro destino para la regla de notificación.
- El tema de Amazon SNS está cifrado y falta la política necesaria para los temas cifrados o se ha eliminado la clave de AWS KMS. Para obtener más información, consulte Configuración de los temas de Amazon SNS para las notificaciones.
- El tema de Amazon SNS no tiene la política necesaria para las notificaciones. Las notificaciones no se pueden enviar a un tema de Amazon SNS a menos que este tenga la política. Para obtener más información, consulte Configuración de los temas de Amazon SNS para las notificaciones.
- Es posible que haya algún problema en este momento en el servicio de soporte del destino (Amazon SNS o AWS Chatbot).

Quiero aumentar mis cuotas de notificaciones y recursos

Actualmente no se puede cambiar ninguna cuota. Consulte Cuotas para las notificaciones.

Cuotas para las notificaciones

En la siguiente tabla se enumeran las cuotas (también denominadas límites) de las notificaciones en la consola de herramientas para desarrolladores. Para obtener más información acerca de los límites que pueden cambiarse, consulte Cuotas de servicio de AWS.

Resource	Límite predeterminado
Número máximo de reglas de notificación de una cuenta de AWS.	1 000
Número máximo de destinos de una regla de notificación.	10
Número máximo de reglas de notificación de un recurso.	10

¿Qué son las conexiones?

Puede utilizar la función de conexiones de la consola de Developer Tools para conectar AWS recursos, por ejemplo, AWS CodePipeline a repositorios de código externos. Esta función tiene su propia API, la API de referencia de AWS CodeStar Connections. Cada conexión es un recurso que puedes asignar a AWS los servicios para que se conecten a un repositorio de terceros, por ejemplo BitBucket. Por ejemplo, puedes añadir la conexión para CodePipeline que active tu canalización cuando se realice un cambio de código en tu repositorio de código de terceros. Cada conexión recibe un nombre y se asocia a un nombre de recurso de Amazon (ARN) único que se utiliza para hacer referencia a la conexión.

¿Qué puedo hacer con las conexiones?

Puede utilizar las conexiones para integrar los recursos de proveedores de terceros a sus recursos de AWS en herramientas para desarrolladores, incluso:

- Conéctate a un proveedor externo, como Bitbucket, y utiliza la conexión de terceros como fuente de integración con tus AWS recursos, por ejemplo. CodePipeline
- Gestiona de manera uniforme el acceso a tu conexión a todos tus recursos y CodeBuild crea proyectos, CodeDeploy aplicaciones y canalizaciones CodePipeline para tu proveedor externo.
- Usa un ARN de conexión en tus plantillas de pila para CodeBuild crear proyectos, CodeDeploy aplicaciones y canalizaciones CodePipeline, sin necesidad de hacer referencia a los secretos o parámetros almacenados.

¿Para qué proveedores de terceros puedo crear conexiones?

Las conexiones pueden asociar tus AWS recursos con los siguientes repositorios de terceros:

- Bitbucket Cloud
- GitHub
- GitHub Nube empresarial
- GitHub Servidor empresarial
- GitLab
- GitLab instalación autogestionada (para Enterprise Edition o Community Edition)

Para obtener información general acerca del flujo de trabajo de las conexiones, consulte Flujo de trabajo para crear o actualizar conexiones.

Los pasos para crear conexiones para un tipo de proveedor de nube, por ejemplo GitHub, son diferentes de los pasos para un tipo de proveedor instalado, como GitHub Enterprise Server. Para conocer los pasos de alto nivel necesarios para crear una conexión por tipo de proveedor, consulte Trabajar con conexiones.

> **Note**
>
> Para usar conexiones en Europa (Milán) Región de AWS, debe:
>
> 1. Instalar una aplicación específica de la región
> 2. Habilitar la región
>
> Esta aplicación específica de la región está disponible en la región Europa (Milán). Se publica en el sitio del proveedor externo y es independiente de la aplicación existente que admite conexiones para otras regiones. Al instalar esta aplicación, autoriza a los proveedores externos a compartir sus datos con el servicio únicamente para esta región, y puede revocar los permisos en cualquier momento desinstalando la aplicación.
> El servicio no procesará ni almacenará sus datos a menos que habilite la región. Al habilitar esta región, otorga a nuestro servicio permisos para procesar y almacenar sus datos.
> Aunque la región no esté habilitada, los proveedores externos pueden compartir sus datos con nuestro servicio si la aplicación específica de la región permanece instalada, así que

asegúrese de desinstalar la aplicación una vez que deshabilite la región. Para obtener más información, consulte Habilitar una región.

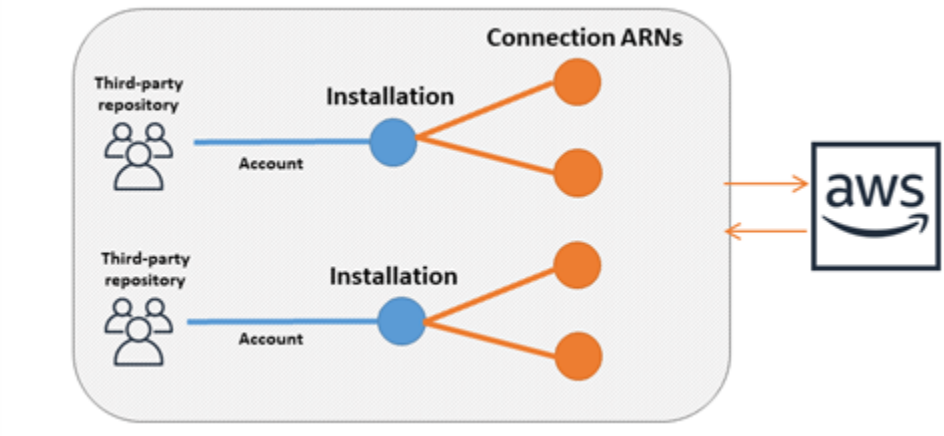
¿Qué se Servicios de AWS integra con las conexiones?

Puede utilizar las conexiones para integrar su repositorio de terceros con otros Servicios de AWS. Para ver las integraciones de servicios para las conexiones, consulte Integraciones de productos y servicios con AWS CodeStar Connections.

¿Cómo funcionan las conexiones?

Para poder crear una conexión, primero debe instalar la aplicación de autenticación de AWS en su cuenta de terceros o conceder acceso a ella. Una vez que la conexión se instaló, se puede actualizar para utilizar la instalación. Cuando crea una conexión, concede acceso al recurso de AWS de su cuenta de terceros. Esto permite que la conexión acceda al contenido, como los repositorios de fuentes, de la cuenta de terceros, en nombre de tus AWS recursos. A continuación, puedes compartir esa conexión con otras Servicios de AWS para proporcionar conexiones OAuth seguras entre los recursos.

Si desea crear una conexión a un tipo de proveedor instalado, como GitHub Enterprise Server, primero debe crear un recurso de host mediante. AWS Management Console



Las conexiones son propiedad de quien Cuenta de AWS las crea. Las conexiones se identifican mediante un ARN que contiene un ID de conexión. El ID de conexión es un UUID (identificador único universal) que no se puede cambiar ni remapear. Cuando se elimina y se restablece una conexión, se obtiene un ID de conexión nuevo y, por lo tanto, un ARN de conexión nuevo. Esto significa que los ARN de conexión nunca se reutilizan.

Una conexión recién creada se encuentra en estado `Pending`. Se requiere un proceso de protocolo de enlace de terceros (flujo de OAuth) para completar la configuración de la conexión y para que el estado de la conexión pase de `Pending` a `Available`. Una vez completado esto, la conexión se utiliza `Available` y se puede utilizar con AWS servicios, como CodePipeline.

Un alojamiento recién creado se encuentra en un estado `Pending`. Se requiere un proceso de registro de terceros para completar la configuración del alojamiento y para que el estado del alojamiento pase de `Pending` a `Available`. Una vez que se completa este paso, un alojamiento está `Available` y se puede utilizar para conexiones con tipos de proveedores instalados.

Para obtener información general acerca del flujo de trabajo de las conexiones, consulte Flujo de trabajo para crear o actualizar conexiones. Para obtener información general sobre el flujo de trabajo de creación de hosts para proveedores instalados, consulte Flujo de trabajo para crear o actualizar un host. Para conocer los pasos de alto nivel necesarios para crear una conexión por tipo de proveedor, consulte Trabajar con conexiones.

Recursos globales en AWS CodeStar Connections

Las conexiones son recursos globales, lo que significa que el recurso se replica en todas las regiones de Regiones de AWS.

Si bien el formato de ARN de conexión refleja el nombre de la región donde se creó, el recurso no se limita a ninguna región. La región donde se creó el recurso de conexión es la región donde se controlan las actualizaciones de los datos de los recursos de conexión. Entre los ejemplos de operaciones de la API que controlan las actualizaciones de los datos de los recursos de conexión se incluyen la creación de una conexión, la actualización de una instalación, la eliminación de una conexión o el etiquetado de una conexión.

Los recursos de alojamiento para conexiones no son recursos que están disponibles en todo el mundo. Los recursos de alojamiento solo se utilizan en la región donde se crearon.

- Solo tiene que crear una conexión una vez y, después, puede utilizarla en cualquier Región de AWS.
- Si la región donde se creó la conexión presenta problemas, las API que controlan los datos de los recursos de conexión se ven afectadas; sin embargo, usted puede seguir utilizando la conexión de forma correcta en todas las demás regiones.
- Cuando enumera los recursos de conexión en la consola o la CLI, la lista muestra todos los recursos de conexión asociados a su cuenta en todas las regiones.

- Cuando enumera los recursos de alojamiento en la consola o la CLI, la lista muestra los recursos de alojamiento asociados a su cuenta solo en la región seleccionada.
- Cuando una conexión con un recurso de alojamiento asociado se muestra o se visualiza con la CLI, la salida devuelve el ARN del alojamiento independientemente de la región de la CLI configurada.

Flujo de trabajo para crear o actualizar un host

Cuando cree una conexión para un proveedor instalado, cree primero un host.

Los hosts pueden tener los siguientes estados:

- `Pending`: un host `pending` es un host que se ha creado y se debe configurar (moverse a `available`) para poderse utilizar.
- `Available`: puede usar o transferir un host `available` a su conexión.

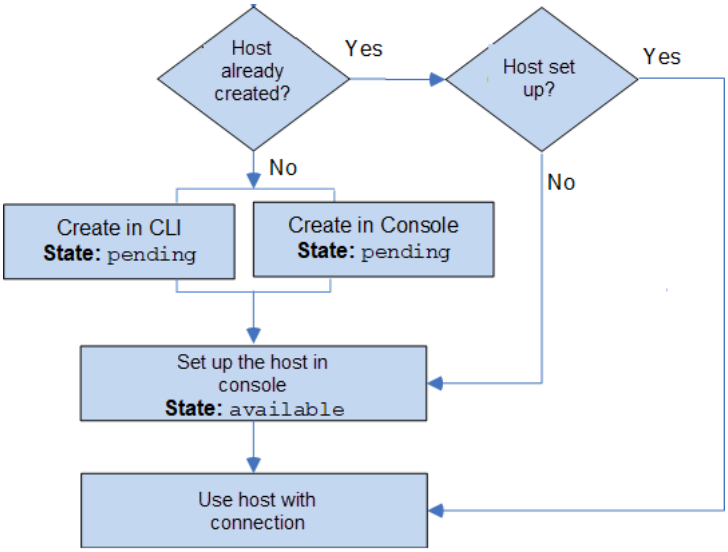
Flujo de trabajo: la creación o actualización de un host con la CLI, el SDK o AWS CloudFormation

Utiliza la CreateHostAPI para crear un host mediante AWS Command Line Interface (AWS CLI), el SDK o AWS CloudFormation. Una vez creada, el host se encuentra en estado `pending`. El proceso se completa mediante la opción Configurar de la consola.

Flujo de trabajo: creación o actualización de un host con la consola

Si va a crear una conexión a un tipo de proveedor instalado, como GitHub Enterprise Server o GitLab autogestionado, primero debe crear un host. Si se conecta a un tipo de proveedor de la nube, como Bitbucket, debe omitir la creación del alojamiento y continuar creando una conexión.

Utilice la consola para configurar el host y cambiar su estado de `pending` a `available`.



Flujo de trabajo para crear o actualizar conexiones

Cuando crea una conexión, también crea o utiliza una instalación existente para el protocolo de enlace de autenticación con el proveedor de terceros.

Las conexiones pueden tener los siguientes estados:

- `Pending`: una conexión `pending` es aquella que debe completarse (pasar a `available`) antes de utilizarse.
- `Available`: puede utilizar o pasar una conexión `available` a otros recursos y usuarios de su cuenta.
- `Error`: una conexión que tiene un estado `error` se vuelve a intentar de forma automática. No se puede utilizar hasta que esté `available`.

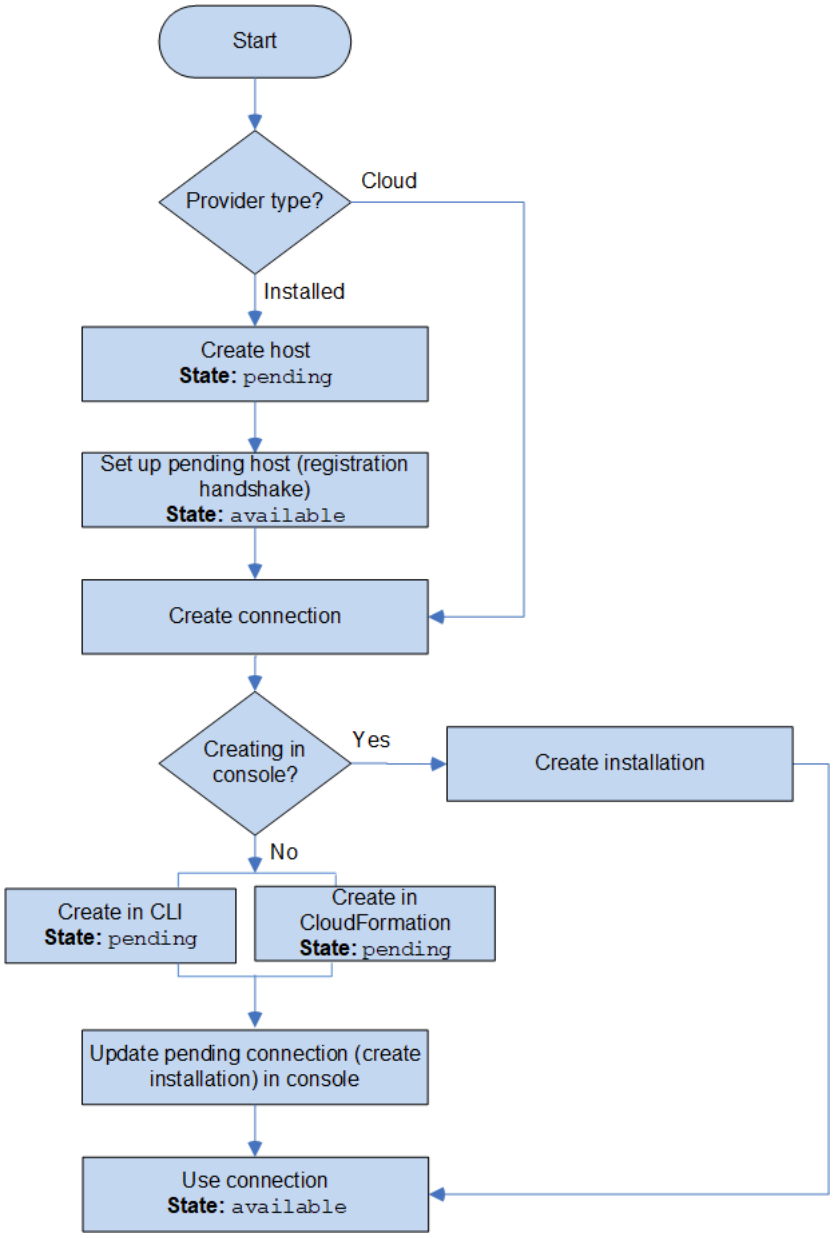
Flujo de trabajo: la creación o la actualización de una conexión con la CLI, el SDK o AWS CloudFormation

Utiliza la CreateConnectionAPI para crear una conexión mediante AWS Command Line Interface (AWS CLI), el SDK o AWS CloudFormation. Una vez creada, la conexión se encuentra en estado `pending`. El proceso se completa mediante la opción de la consola Set up pending connection (Configurar conexión pendiente). La consola solicita que se cree una instalación o que se utilice una instalación existente para la conexión. Luego, se utiliza la consola para completar el protocolo de enlace y cambiar el estado de la conexión a `available` con la opción Complete connection (Completar conexión) de la consola.

Flujo de trabajo: creación o actualización de una conexión con la consola

Si va a crear una conexión a un tipo de proveedor instalado, como GitHub Enterprise Server, primero debe crear un host. Si se conecta a un tipo de proveedor de la nube, como Bitbucket, debe omitir la creación del alojamiento y continuar creando una conexión.

Para crear o actualizar una conexión mediante la consola, utilice la página de acciones de CodePipeline edición de la consola para elegir su proveedor externo. La consola solicita que se cree una instalación o se utilice una instalación existente para la conexión y que luego, se utilice la consola para crear la conexión. La consola completa el protocolo de enlace y el estado de la conexión pasa de `pending` a `available` de forma automática.



¿Cómo comienzo a utilizar las conexiones?

Para empezar, aquí hay algunos temas útiles para revisar:

- Obtenga información acerca de los conceptos de las conexiones.
- Configure los recursos que necesita para comenzar a trabajar con las conexiones.
- Comience con sus primeras conexiones y conéctelas a un recurso.

Conceptos de conexiones

La configuración y el uso de la característica de conexiones resultan más sencillos si comprende los conceptos y los términos. A continuación, se muestran algunos conceptos que debe conocer cuando utiliza conexiones en la consola de herramientas para desarrolladores:

instalación

Se trata de una instancia de la aplicación de AWS en una cuenta de terceros. La instalación de la aplicación AWS CodeStar Connector permite a AWS acceder a recursos en la cuenta de terceros. Una instalación solo se puede editar en el sitio web del proveedor de terceros.

conexión

Se trata de un recurso de AWS utilizado para conectar repositorios de origen de terceros a otros servicios de AWS.

repositorio de terceros

Se trata de un repositorio proporcionado por un servicio o una empresa que no forma parte de AWS. Por ejemplo, un repositorio de Bitbucket es un repositorio de terceros.

tipo de proveedor

Se trata de un servicio o una empresa que proporciona el repositorio de origen de terceros al que desea conectarse. Conecte sus recursos de AWS a tipos de proveedores externos. Un tipo de proveedor donde el repositorio de origen está instalado en la red y la infraestructura es un tipo de proveedor instalado. Por ejemplo, GitHub Enterprise Server es un tipo de proveedor instalado.

host

Se trata de un recurso que representa la infraestructura en la que está instalado un proveedor de terceros. Las conexiones utilizan el alojamiento para representar el servidor donde está instalado

el proveedor de terceros, como GitHub Enterprise Server. Crea un alojamiento para todas las conexiones a ese tipo de proveedor.

> **Note**
>
> Cuando utiliza la consola para crear una conexión a GitHub Enterprise Server, la consola crea un recurso de alojamiento para usted como parte del proceso.

AWS CodeStar Conexiones, proveedores y versiones compatibles

En este capítulo se proporciona información sobre los proveedores y las versiones compatibles con AWS CodeStar Connections.

Temas

Tipo de proveedor compatible con Bitbucket

Puedes usar la AWS CodeStar aplicación con Atlassian Bitbucket Cloud.

Los tipos de proveedores de Bitbucket instalados, como Bitbucket Server, no son compatibles.

Tipo de proveedor compatible con Enterprise Cloud GitHub GitHub

Puede usar la GitHub aplicación AWS Connector para aplicaciones con GitHub GitHub Enterprise Cloud.

Tipos y versiones de proveedor compatibles para GitHub Enterprise Server

Puede usar la AWS CodeStar aplicación con las versiones compatibles de GitHub Enterprise Server. Para obtener una lista de las versiones compatibles, consulte https://enterprise.github.com/releases/.

> **Important**
>
> AWS CodeStar Connections no admite las versiones obsoletas de GitHub Enterprise Server. Por ejemplo, AWS CodeStar Connections no es compatible con la versión 2.22.0 de GitHub Enterprise Server debido a un problema conocido en la versión. Para conectarse, actualice a la versión 2.22.1 o a la última versión disponible.

Tipo de proveedor compatible para GitLab

Puede utilizar conexiones con GitLab. Para obtener más información, consulte Cree una conexión a GitLab.

Tipo de proveedor compatible para la GitLab autogestión

Puede usar conexiones con una instalación GitLab autogestionada (para Enterprise Edition o Community Edition). Para obtener más información, consulte Cree una conexión a una red GitLab autogestionada.

Integraciones de productos y servicios con AWS CodeStar Connections

AWS CodeStar Connections se integra con diversos servicios de AWS, así como productos y servicios de socios. La información de las siguientes secciones puede ayudarle a configurar conexiones para la integración con los productos y servicios que utilice.

Los recursos relacionados siguientes pueden serle de ayuda cuando trabaje con este servicio.

Temas

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

Amazon CodeGuru Reviewer

Revisor de CodeGuru es un servicio para supervisar el código de su repositorio. Puede utilizar las conexiones para asociar el repositorio de terceros que tiene el código que desea revisar. Para ver un tutorial en el que se aprende a configurar Revisor de CodeGuru para que supervise el código fuente en un repositorio de GitHub de modo que pueda crear recomendaciones que mejoren el código, consulte Tutorial: monitor source code in a GitHub repository (Tutorial: supervisar el código fuente en un repositorio de GitHub) en la Guía del usuario de Revisor de Amazon CodeGuru.

Amazon CodeWhisperer

Amazon CodeWhisperer es un servicio para revisar el código del repositorio. CodeWhisperer revisa el código y le ofrece recomendaciones de código en tiempo real. Para conocer los pasos necesarios para configurar una personalización en CodeWhisperer en la que se accede al origen de datos mediante una conexión, consulte Creación de una personalización en la Guía del usuario de Amazon CodeWhisperer.

Amazon SageMaker

Amazon SageMaker es un servicio para crear, entrenar e implementar modelos de lenguaje de machine learning. Para ver un tutorial en el que puede configurar una conexión al repositorio de GitHub, consulte Tutorial del proyecto MLOps de SageMaker sobre el uso de repositorios Git de terceros en la Guía para desarrolladores de Amazon SageMaker.

AWS App Runner

AWS App Runner es un servicio que proporciona una forma rápida, sencilla y rentable de implementar desde el código fuente o una imagen de contenedor directamente hacia una aplicación web escalable y segura en la Nube de AWS. Puede implementar el código de la aplicación desde su repositorio con una canalización de integración y entrega automática de App Runner. Puede utilizar las conexiones para implementar su código fuente en un servicio de App Runner desde un repositorio privado de GitHub. Para obtener más información, consulte Source code repository providers (Proveedores de repositorios de código fuente) en la Guía para desarrolladores de AWS App Runner.

AWS CloudFormation

AWS CloudFormation es un servicio que le ayuda a modelar y configurar sus recursos de AWS, por lo que podrá dedicar menos tiempo a la administración de dichos recursos y más tiempo a

centrarse en las aplicaciones que se ejecutan en AWS. Puede crear una plantilla que describa todos los recursos de AWS que desea (como instancias de Amazon EC2 o instancias de base de datos de Amazon RDS) y CloudFormation se encargará del aprovisionamiento y la configuración de dichos recursos. Para obtener más información, consulte Registro de la cuenta para publicar extensiones de CloudFormation en la Guía del usuario de la interfaz de línea de comandos de CloudFormation.

AWS CodePipeline

CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para lanzar su software. Puede utilizar las conexiones para configurar un repositorio de terceros para las acciones de origen de CodePipeline.

Más información:

- Consulte la página de referencia de configuración de la acción CodePipeline para la acción `CodeStarSourceConnection`. Para ver los parámetros de configuración y un fragmento de código JSON/YAML de ejemplo, consulte CodeStarSourceConnection en la Guía del usuario de AWS CodePipeline.
- Para ver un tutorial de introducción que crea una canalización con un repositorio de origen de terceros, consulte Introducción a las conexiones.

AWS CodeStar

AWS CodeStar es un servicio basado en la nube para crear, administrar y trabajar con proyectos de desarrollo de software en AWS. Puede desarrollar, compilar e implementar aplicaciones rápidamente en AWS con un proyecto de AWS CodeStar. Puede utilizar las conexiones para configurar los repositorios de terceros para las conexiones de los proyectos de AWS CodeStar. Para ver un tutorial en el que se crea un proyecto de AWS CodeStar con una conexión a un repositorio de GitHub, consulte Crear un enlace al repositorio en la Guía del usuario de AWS CodeStar.

Service Catalog

Service Catalog permite a las organizaciones crear y administrar catálogos de productos aprobados para su uso en AWS.

Cuando autoriza una conexión entre su Cuenta de AWS y un proveedor de repositorios externo, como GitHub, GitHub Enterprise o BitBucket, la conexión le permite sincronizar los productos de Service Catalog con archivos de plantilla que se administran a través de repositorios de terceros.

Para obtener más información, consulte Syncing Service Catalog products to template files from GitHub, GitHub Enterprise, or Bitbucket (Sincronización de los productos de Service Catalog con archivos de plantilla de GitHub, GitHub Enterprise o Bitbucket) en la Guía del usuario de Service Catalog.

AWS Proton

AWS Proton es un servicio basado en la nube que se implementa en una infraestructura de nube. Puede utilizar las conexiones para crear un enlace a sus repositorios de terceros para los recursos de sus plantillas para AWS Proton. Para obtener más información, consulte Create a link to your repository (Crear un enlace a su repositorio) en la Guía del usuario de AWS Proton.

Configuración de conexiones

Complete las tareas de esta sección para configurar la creación y el uso de la característica de conexiones en la consola de herramientas para desarrolladores.

Temas

- Registrarse en AWS
- Creación y aplicación de una política con permisos para crear conexiones

Registrarse en AWS

Registro para obtener una Cuenta de AWS

Si no dispone de una Cuenta de AWS, siga estos pasos para crear una.

Cómo registrarse en una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Al registrarse en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario administrativo y utilice únicamente el usuario raíz para realizar tareas que requieran acceso de usuario raíz.

AWS le enviará un correo electrónico de confirmación luego de completar el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Crear un usuario administrativo

Después de registrarse para obtener una Cuenta de AWS, proteja su Usuario raíz de la cuenta de AWS, habilite AWS IAM Identity Center y cree un usuario administrativo para no utilizar el usuario raíz en las tareas cotidianas.

Protección de su Usuario raíz de la cuenta de AWS

1. Inicie sesión en la AWS Management Console como propietario de cuenta, elija Usuario raíz e ingrese el email de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In.
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario raíz de la Cuenta de AWS (consola) en la Guía del usuario de IAM.

Creación de un usuario administrativo

1. Activar IAM Identity Center

   Para ver las instrucciones, consulte Enabling AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.
2. En IAM Identity Center, conceda acceso administrativo a un usuario administrativo.

   Para ver un tutorial sobre el uso del Directorio de IAM Identity Center como origen de identidades, consulte Configure user access with the default Directorio de IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.

Cómo iniciar sesión como usuario administrativo

- Para iniciar sesión con el usuario del IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario del IAM Identity Center.

Para obtener ayuda para iniciar sesión con un usuario del IAM Identity Center, consulte Iniciar sesión en el portal de acceso de AWS en la Guía del Usuario de AWS Sign-In.

Creación y aplicación de una política con permisos para crear conexiones

Para utilizar el editor de política de JSON para crear una política

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la izquierda, seleccione Políticas.

   Si es la primera vez que elige Políticas, aparecerá la página Bienvenido a políticas administradas. Elija Comenzar.
3. En la parte superior de la página, seleccione Crear política.
4. En la sección Editor de políticas, seleccione la opción JSON.
5. Ingrese el siguiente 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. Elija Siguiente.

> **Note**
>
> Puede alternar entre las opciones Visual y JSON del editor en todo momento. No obstante, si realiza cambios o selecciona Siguiente en la opción Visual del editor, es posible que IAM reestructure la política, con el fin de optimizarla para el editor visual. Para obtener más información, consulte Reestructuración de política en la Guía del usuario de IAM.

7. En la página Revisar y crear, introduzca el Nombre de la política y la Descripción (opcional) para la política que está creando. Revise los Permisos definidos en esta política para ver los permisos que concede la política.
8. Elija Create Policy (Crear política) para guardar la nueva política.

Introducción a las conexiones

La forma más sencilla de comenzar a utilizar las conexiones es configurar una conexión que asocie su repositorio de origen de terceros a sus recursos de AWS. Si desea conectar la canalización a un origen de AWS, como CodeCommit, se conectará a este como una acción de origen. Sin embargo, si tiene un repositorio externo, debe crear una conexión para asociar el repositorio a la canalización. En este tutorial, configurará una conexión con su repositorio de Bitbucket y su canalización.

En esta sección, utilizará conexiones con lo siguiente:

- AWS CodePipeline: en estos pasos, crea una canalización con su repositorio de Bitbucket como origen de canalización.
- Amazon CodeGuru Reviewer: luego, asocia su repositorio de Bitbucket a las herramientas de comentarios y análisis de CodeGuru Reviewer.

Temas

- Paso 3: Asociar el repositorio a CodeGuru Reviewer

Requisitos previos

Antes de comenzar, complete los pasos de Configuración. También necesita un repositorio de origen de terceros que desee conectar a los servicios de AWS y permitir que la conexión administre la autenticación por usted. Por ejemplo, es posible que desee conectar un repositorio de Bitbucket a sus servicios de AWS que se integran a repositorios de origen.

- Cree un repositorio de Bitbucket con su cuenta de Bitbucket.
- Tenga listas las credenciales de Bitbucket. Cuando utiliza la AWS Management Console para configurar una conexión, se le pide que inicie sesión con sus credenciales de Bitbucket.

Paso 1: Editar archivo de origen

Cuando crea el repositorio de Bitbucket, se incluye un archivo `README.md` predeterminado, el cual usted editará.

1. Inicie sesión en su repositorio de Bitbucket y elija Source (Origen).
2. Elija el archivo `README.md` y elija Edit (Editar) en la parte superior de la página. Elimine el texto existente y agregue el siguiente texto.

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

3. Elija Commit (Confirmar).

   Asegúrese de que el archivo `README.md` está en el nivel raíz del repositorio.

Paso 2: Crear la canalización

En esta sección, debe crear una canalización con las siguientes acciones:

- una etapa de origen con una conexión a la acción y el repositorio de Bitbucket
- una etapa de compilación con una acción de compilación de AWS CodeBuild

Para crear una canalización con el asistente

1. Inicie sesión en la consola de CodePipeline en https://console.aws.amazon.com/codepipeline/.

2. En la página Welcome (Bienvenido), Getting Started (Introducción) o en la página Pipelines (Canalizaciones), elija Create pipeline (Crear canalización).
3. En Step 1: Choose pipeline settings (Paso 1: Elegir configuración de canalización), en Pipeline name (Nombre de canalización), escriba **`MyBitbucketPipeline`**.
4. En Service role (Rol de servicio), elija New service role (Nuevo rol de servicio).

   > **Note**
   >
   > Si, en cambio, elige utilizar la función de servicio de CodePipeline existente, asegúrese de haber agregado el permiso de IAM `codestar-connections:UseConnection` a la política de la función de servicio. Para obtener instrucciones acerca de la función de servicio de CodePipeline, consulte Agregar permisos a la función de servicio de CodePipeline.

5. Para Configuración avanzada deje los valores predeterminados. En Artifact store (Almacén de artefactos), elija Default location (Ubicación predeterminada) para utilizar el almacén de artefactos predeterminado, como el bucket de artefacto de Amazon S3 que se estableció como predeterminado, para la canalización en la región que seleccionó para esta.

   > **Note**
   >
   > Este no es el bucket de origen para su código fuente. Este es el almacén de artefactos de la canalización. Cada canalización debe tener su propio almacén de artefactos independiente, como un bucket de S3.

   Elija Next (Siguiente).
6. En la página Step 2: Add source stage (Paso 2: Agregar etapa de origen), agregue una etapa de origen:

   a. En Source provider (Proveedor de origen), elija Bitbucket.
   b. En Connection (Conexión), elija Connect to Bitbucket (Conectarse a Bitbucket).
   c. En la página Connect to Bitbucket (Conectarse a Bitbucket), en Connection name (Nombre de la conexión), ingrese el nombre de la conexión que desea crear. El nombre le ayudará a identificar esta conexión más adelante.

En Bitbucket apps (Aplicaciones de Bitbucket), elija Install a new app (Instalar una aplicación nueva).

d. En la página de instalación de la aplicación, aparece un mensaje que indica que la aplicación de AWS CodeStar está intentando conectarse a su cuenta de Bitbucket. Elija Grant access (Conceder acceso). Después de autorizar la conexión, se detectan sus repositorios en Bitbucket y puede elegir asociar uno a su recurso de AWS.

e. Se muestra el ID de conexión de la nueva instalación. Elija Complete connection (Completar conexión). Volverá a la consola de CodePipeline.

f. En Repository name (Nombre del repositorio), elija el nombre de su repositorio de Bitbucket.

g. En Branch name (Nombre de ramificación), elija la ramificación para su repositorio.

h. Asegúrese de que la opción Iniciar la canalización en el cambio del código fuente está seleccionada.

i. En Formato de artefacto de salida, elija una de las siguientes opciones: CodePipeline predeterminado.

- Elija CodePipeline predeterminado para usar el formato zip predeterminado para los artefactos en la canalización.
- Elija Clonación completa para incluir en la canalización los metadatos de Git sobre el repositorio para artefactos. Esto solo se admite para las acciones de CodeBuild.

Elija Next (Siguiente).

7. En Add build stage (Añadir etapa de compilación), añada una etapa de compilación:

a. En Build provider (Proveedor de compilación), elija AWS CodeBuild. En el campo Region (Región) conserve el valor predeterminado de la región de la canalización.

b. Elija Create project (Crear proyecto).

c. En Project name (Nombre de proyecto), escriba un nombre para este proyecto de compilación.

d. En Environment image (Imagen de entorno), elija Managed image (Imagen administrada). En Operating system (Sistema operativo), elija Ubuntu.

e. En Runtime, elija Standard (Estándar). En Imagen, elija aws/codebuild/standard:5.0.

f. En Service role (Rol de servicio), elija New service role (Nuevo rol de servicio).

g. En Buildspec, para Build specifications (Especificaciones de la compilación), elija Insert build commands (Insertar comandos de compilación). Elija Switch to editor (Cambiar a editor) y pegue lo siguiente en Build commands (Comandos de compilación):

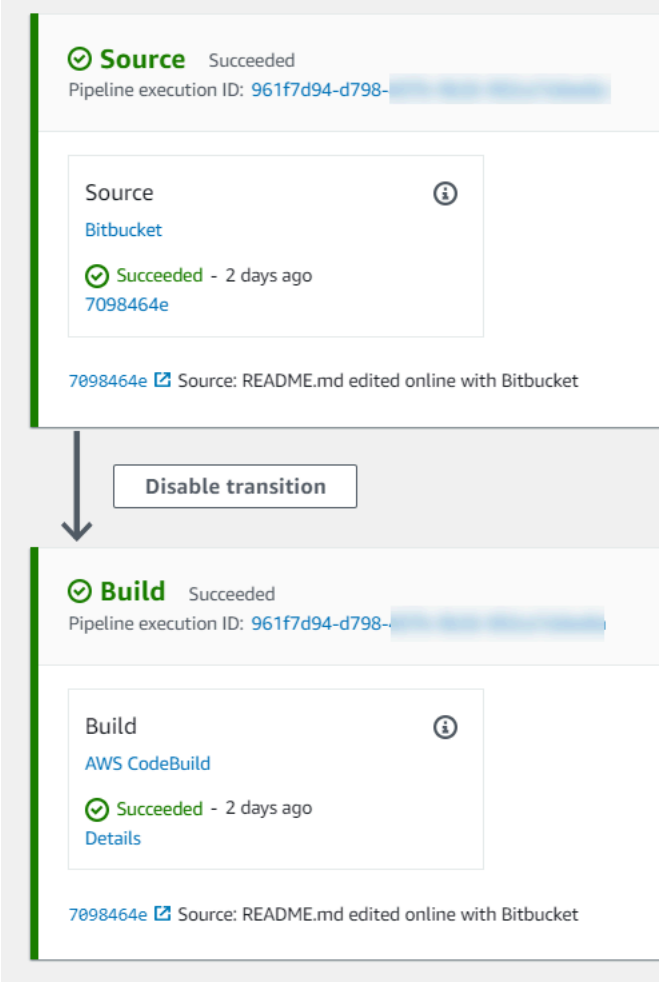
```
version: 0.2

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. Elija Continue to CodePipeline (Continuar en CodePipeline). Esto vuelve a la consola de CodePipeline y crea un proyecto de CodePipeline que utiliza los comandos de compilación

para la configuración. El proyecto de compilación utiliza una función de servicio para administrar los permisos del servicio de AWS. Es posible que este paso tarde un par de minutos.

i. Elija Next (Siguiente).

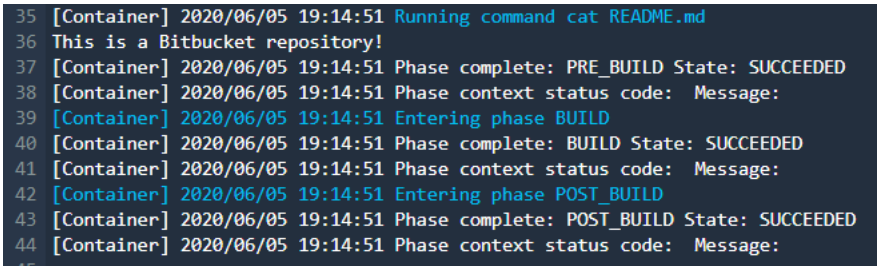
8. En la página Step 4: Add deploy stage (Paso 4: Añadir etapa de implementación), elija Skip deploy stage (Omitir etapa de implementación) y, a continuación, acepte el mensaje de advertencia eligiendo Skip (Omitir) una vez más. Elija Next (Siguiente).
9. En Step 5: Review (Paso 5: Revisar), seleccione Create pipeline (Crear canalización).
10. Cuando su canalización se crea correctamente, se inicia la ejecución de una canalización.



11. En la etapa de compilación exitosa, elija Details (Detalles).

    En Execution details (Detalles de ejecución), vea la salida de la compilación de CodeBuild. Los comandos generan el contenido del archivo `README.md` de la siguiente manera:

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



Paso 3: Asociar el repositorio a CodeGuru Reviewer

Después de crear una conexión, puede utilizar esa conexión para todos los recursos de AWS en la misma cuenta. Por ejemplo, puede utilizar la misma conexión de Bitbucket para una acción de origen de CodePipeline en una canalización y el análisis de confirmación del repositorio en CodeGuru Reviewer.

1. Inicie sesión en la consola de CodeGuru Reviewer.
2. En CodeGuru Reviewer, elija Associate repository (Asociar repositorio).

   Se abre el asistente de una página.
3. En Select source provider (Seleccionar el proveedor de origen), elija Bitbucket.
4. En Conectarse a Bitbucket (con AWS CodeStar Connections), elija la conexión que creó para su canalización.
5. En Repository location (Ubicación del repositorio), elija el nombre de su repositorio de Bitbucket y elija Associate (Asociar).

   Puede continuar configurando revisiones de código. Para obtener más información, consulte Conexión a Bitbucket para asociar un repositorio a CodeGuru Reviewer en la Guía del usuario de Amazon CodeGuru Reviewer.

Trabajar con conexiones

Las conexiones son configuraciones que se utilizan para conectar recursos de AWS a repositorios de código externos. Cada conexión es un recurso que se puede asignar a servicios como la conexión AWS CodePipeline a un repositorio de terceros, como Bitbucket. Por ejemplo, puedes añadir la conexión para CodePipeline que active tu canalización cuando se realice un cambio de código en tu repositorio de código de terceros. También puedes conectar tus AWS recursos a un tipo de proveedor instalado, como GitHub Enterprise Server.

Si desea crear una conexión a un tipo de proveedor instalado, como GitHub Enterprise Server, la consola crea un host para usted. Un alojamiento es un recurso que se crea para representar el servidor donde está instalado el proveedor. Para obtener más información, consulte Trabajo con alojamientos.

Al crear una conexión, se utiliza un asistente en la consola para instalar la AWS CodeStar aplicación con un proveedor externo y asociarla a una nueva conexión. Si ya ha instalado la AWS CodeStar aplicación, puede utilizarla.

> **Note**
>
> Para utilizar conexiones en Europa (Milán) Región de AWS, debe:
>
> 1. Instalar una aplicación específica de la región
> 2. Habilitar la región
>
> Esta aplicación específica de la región está disponible en la región Europa (Milán). Se publica en el sitio del proveedor externo y es independiente de la aplicación existente que admite conexiones para otras regiones. Al instalar esta aplicación, autoriza a los proveedores externos a compartir sus datos con el servicio únicamente para esta región, y puede revocar los permisos en cualquier momento desinstalando la aplicación.
> El servicio no procesará ni almacenará sus datos a menos que habilite la región. Al habilitar esta región, otorga a nuestro servicio permisos para procesar y almacenar sus datos. Aunque la región no esté habilitada, los proveedores externos pueden compartir sus datos con nuestro servicio si la aplicación específica de la región permanece instalada, así que asegúrese de desinstalar la aplicación una vez que deshabilite la región. Para obtener más información, consulte Habilitar una región.

Para obtener más información sobre las conexiones, consulta la referencia de la API de AWS CodeStar conexiones. Para obtener más información sobre la acción CodePipeline fuente de Bitbucket, consulta CodestarConnectionSourcela Guía del AWS CodePipeline usuario.

Para crear o adjuntar una política a tu usuario o rol AWS Identity and Access Management (de IAM) con los permisos necesarios para usar AWS CodeStar las conexiones, consulta. AWS CodeConnections referencia de permisos En función de cuándo se creó su función de CodePipeline servicio, es posible que necesite actualizar sus permisos para admitir AWS CodeStar las conexiones.

Para conocer las instrucciones, consulte Actualización de la función de servicio en la Guía del usuario de AWS CodePipeline .

Temas

Crear una conexión de

Puede crear conexiones con los siguientes tipos de proveedores de terceros:

- Para crear una conexión a Bitbucket, consulte Creación de una conexión a Bitbucket.
- Para crear una conexión a Enterprise Cloud GitHub o GitHub Enterprise Cloud, consulteCree una conexión a GitHub.
- Para crear una conexión a GitHub Enterprise Server, incluida la creación de su recurso de host, consulteCree una conexión a GitHub Enterprise Server.
- Para crear una conexión a GitLab, consulteCree una conexión a GitLab.

Creación de una conexión a Bitbucket

Puedes usar AWS Management Console o AWS Command Line Interface (AWS CLI) para crear una conexión a un repositorio alojado en bitbucket.org.

Antes de empezar

- Debe haber creado una cuenta con Bitbucket.

- Debe haber creado un repositorio de código en bitbucket.org.

> **Note**
>
> Puede crear conexiones a un repositorio de Bitbucket Cloud. Los tipos de proveedores de Bitbucket instalados, como Bitbucket Server, no son compatibles. Consulte AWS CodeStar Conexiones, proveedores y versiones compatibles.

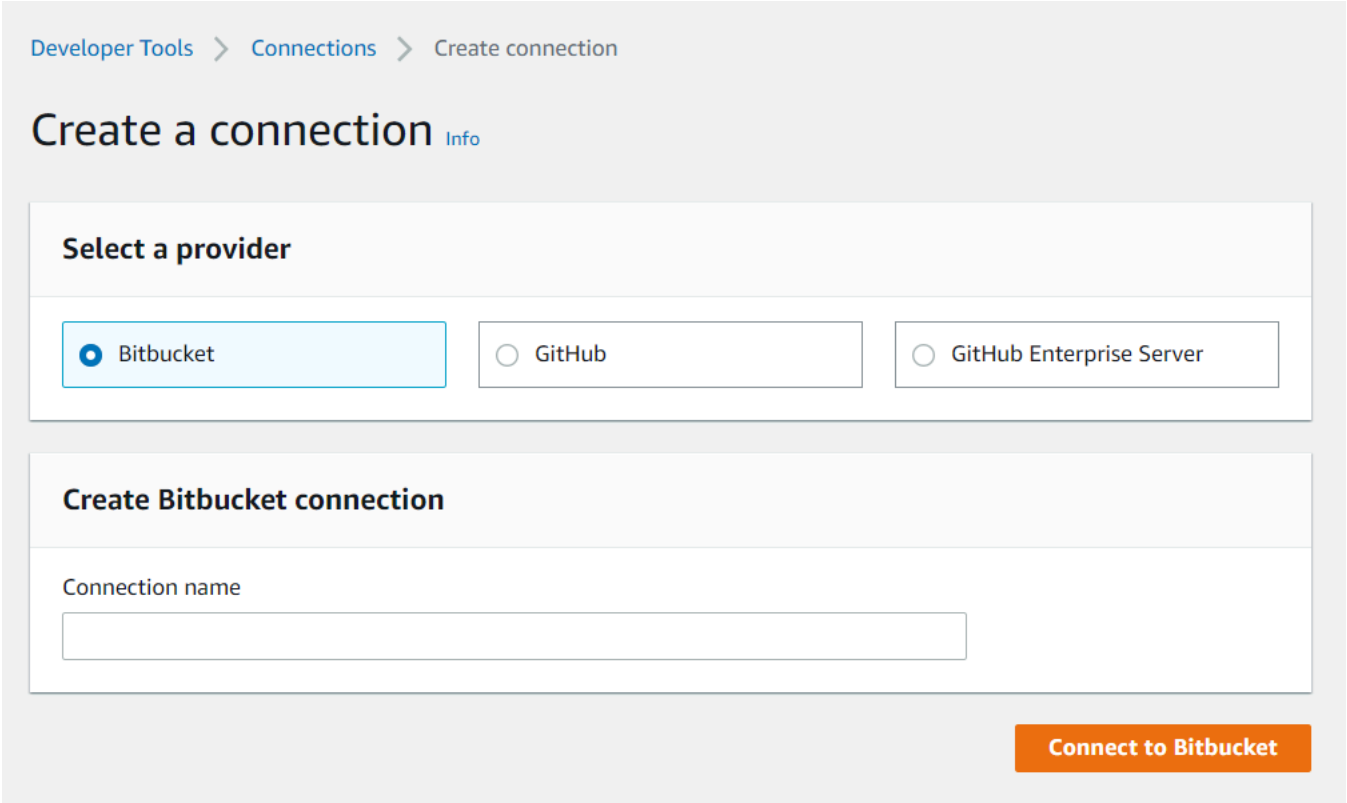
> **Note**
>
> Las conexiones solo brindan acceso a los repositorios que pertenecen a la cuenta que se utilizó para crear la conexión.
> Si la aplicación se va a instalar en un espacio de trabajo de Bitbucket, necesita permisos Administer workspace (Administrar espacio de trabajo). De lo contrario, no se mostrará la opción de instalar la aplicación.

Temas

Creación de una conexión a Bitbucket (consola)

Paso 1: Crear una conexión

1. Inicia sesión en y abre la AWS Management Console consola de herramientas para AWS desarrolladores en. https://console.aws.amazon.com/codesuite/settings/connections
2. Elija Settings > Connections (Configuración > Conexiones) y, luego, elija Create connection (Crear conexión).
3. Para crear una conexión a un repositorio de Bitbucket, en Select a provider (Seleccionar un proveedor), elija Bitbucket. En Connection name (Nombre de la conexión), ingrese el nombre de la conexión que desea crear. Elija Connect to Bitbucket (Conectarse a Bitbucket) y continúe con el paso 2.

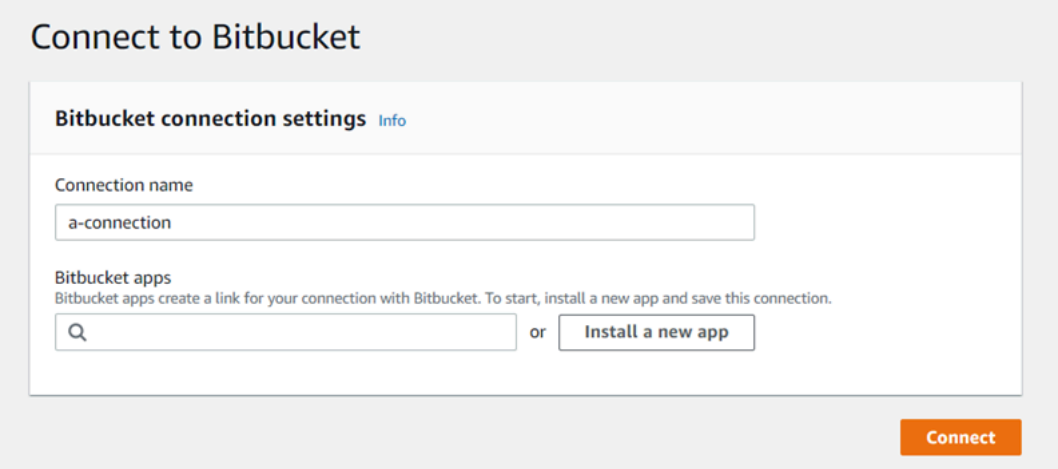


Paso 2: Conectarse a Bitbucket

1. En la página de configuración Connect to Bitbucket(Conectarse a Bitbucket), se mostrará el nombre de la conexión.

   En Bitbucket apps (Aplicaciones de Bitbucket), elija la instalación de una aplicación o elija Install a new app (Instalar una aplicación nueva) para crear una.

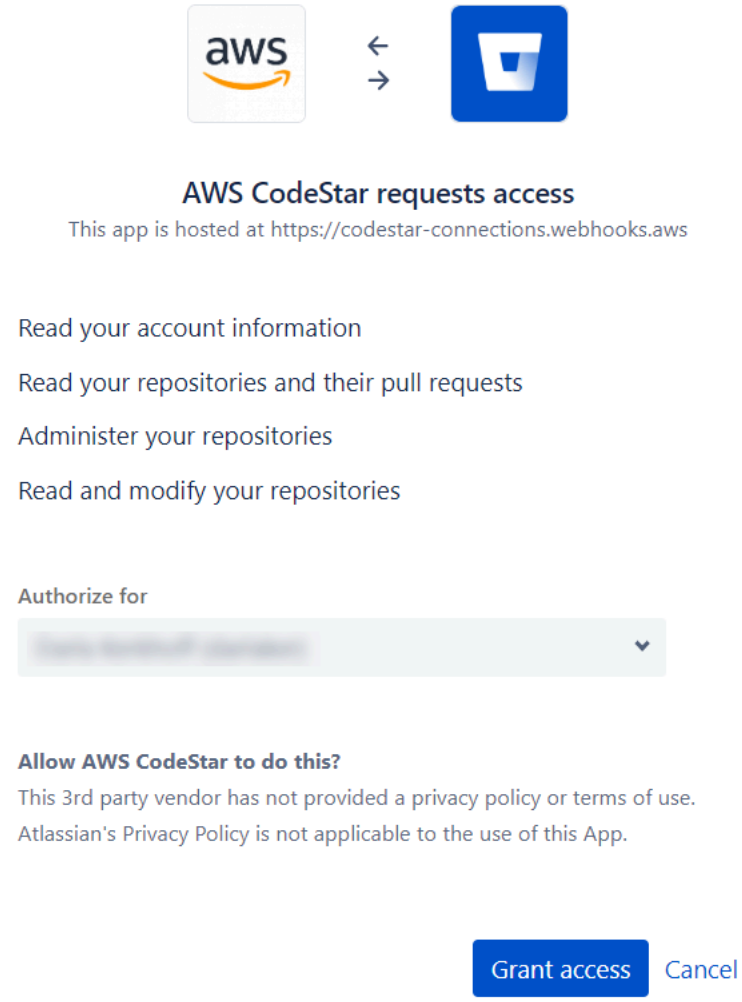
   > **Note**
   >
   > Solo instale la aplicación una vez para cada espacio de trabajo o cuenta de Bitbucket. Si ya ha instalado la aplicación de Bitbucket, elíjala y diríjase al último paso de esta sección.



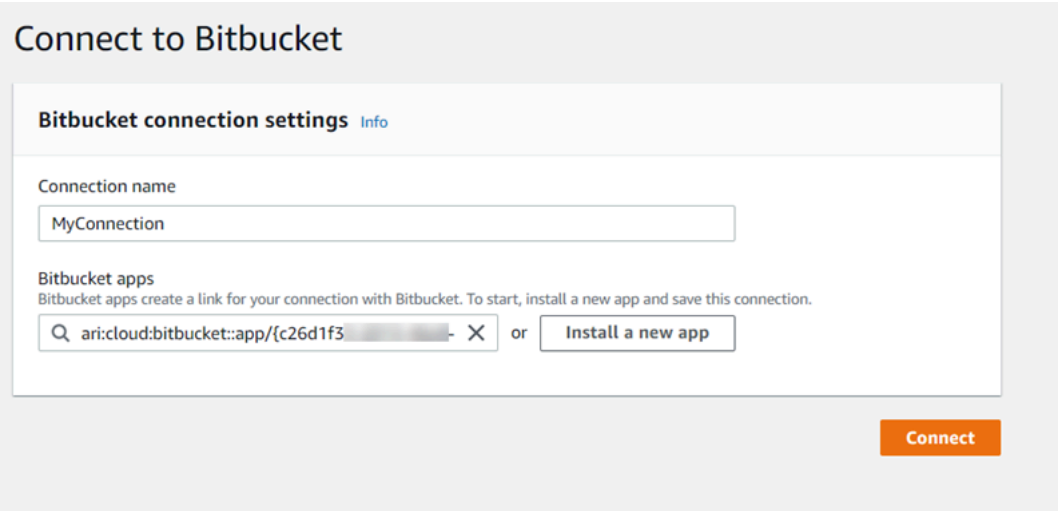
2. Si se muestra la página de inicio de sesión de Bitbucket, inicie sesión con sus credenciales y luego elija continuar.
3. En la página de instalación de la aplicación, aparece un mensaje que indica que la AWS CodeStar aplicación está intentando conectarse a tu cuenta de Bitbucket.

   Si utiliza un espacio de trabajo de Bitbucket, cambie la opción Authorize for (Autorizar para) para el espacio de trabajo. Solo se mostrarán los espacios de trabajo en los que tenga acceso de administrador.

   Elija Grant access (Conceder acceso).



4. En Bitbucket apps (Aplicaciones de Bitbucket), se muestra el ID de conexión de la instalación nueva. Elija Conectar. La conexión creada se muestra en la lista de conexiones.



Creación de una conexión a Bitbucket (CLI)

Puedes usar el AWS Command Line Interface (AWS CLI) para crear una conexión.

Para ello, utilice el comando create-connection.

> **Important**
>
> Una conexión creada a través del AWS CLI o AWS CloudFormation está en `PENDING` estado de forma predeterminada. Después de crear una conexión con la CLI o AWS CloudFormation, utilice la consola para editar la conexión y establecer su estado`AVAILABLE`.

Para crear una conexión a Bitbucket

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice el AWS CLI para ejecutar el create-connection comando, especificando el `--provider-type` y `--connection-name` para la conexión. En este ejemplo, el nombre del proveedor de terceros es `Bitbucket` y el nombre especificado para la conexión es `MyConnection`.

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

   Si se ejecuta correctamente, este comando devuelve la información del ARN de la conexión, que será similar a lo siguiente.

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

2. Utilice la consola para completar la conexión. Para obtener más información, consulte Actualización de una conexión pendiente.

Cree una conexión a GitHub

Puede usar el AWS Management Console o el AWS Command Line Interface (AWS CLI) para crear una conexión a GitHub.

Antes de empezar

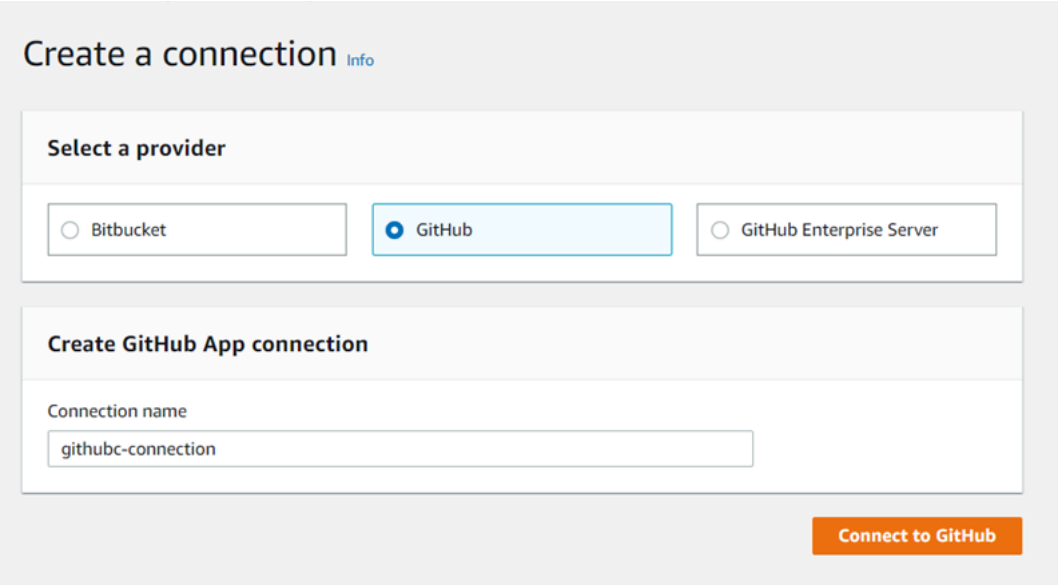
- Debe haber creado ya una cuenta con GitHub.
- Debe haber creado su repositorio de código de terceros.

> **Note**
>
> Para crear la conexión, debe ser el propietario de la GitHub organización. Para los repositorios que no pertenecen a una organización, debe ser el propietario del repositorio.

Temas

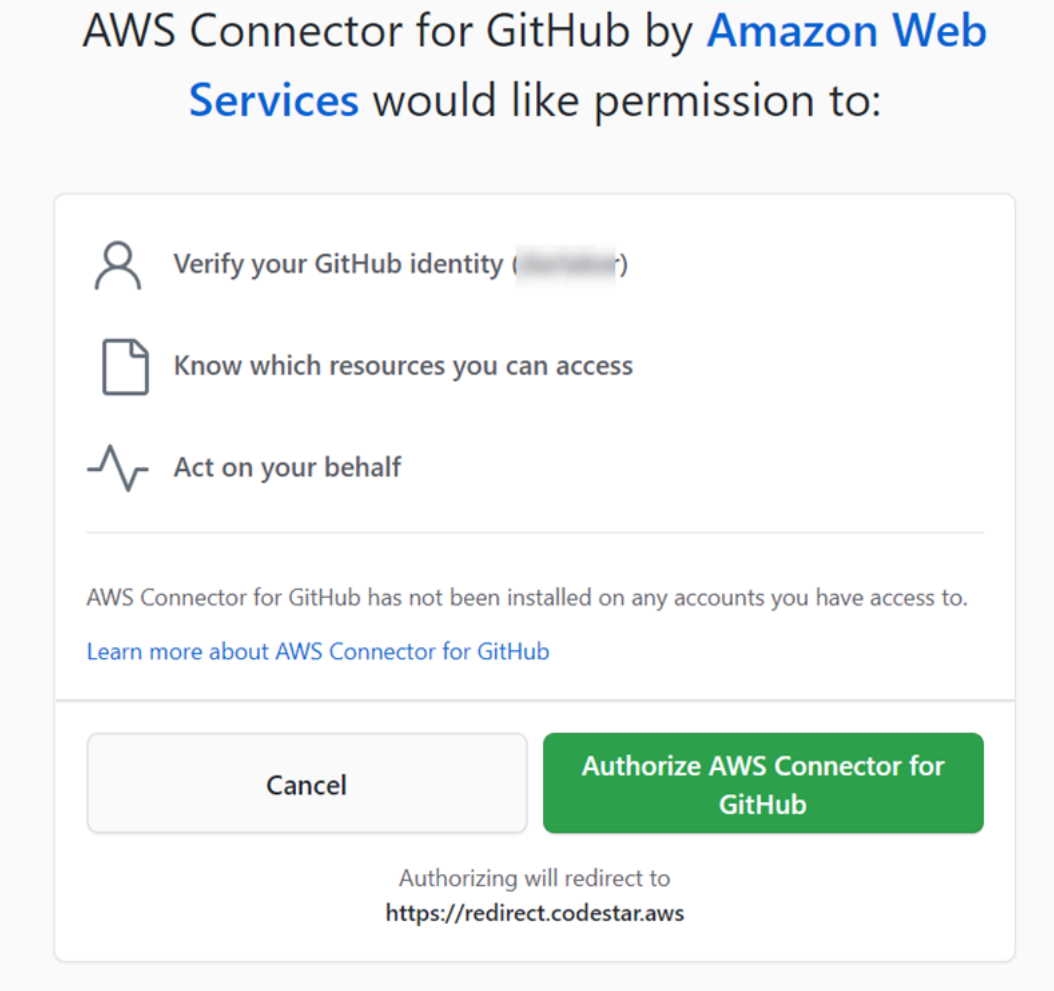
Crea una conexión a GitHub (consola)

1. Inicie sesión en y abra la AWS Management Console consola de Herramientas para desarrolladores enhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Elija Settings > Connections (Configuración > Conexiones) y, luego, elija Create connection (Crear conexión).
3. Para crear una conexión a un repositorio GitHub o a un repositorio de GitHub Enterprise Cloud, en Seleccione un proveedor, elija GitHub. En Nombre de la conexión, introduzca el nombre de la conexión que desea crear. Selecciona Conectar a GitHub y continúa con el paso 2.

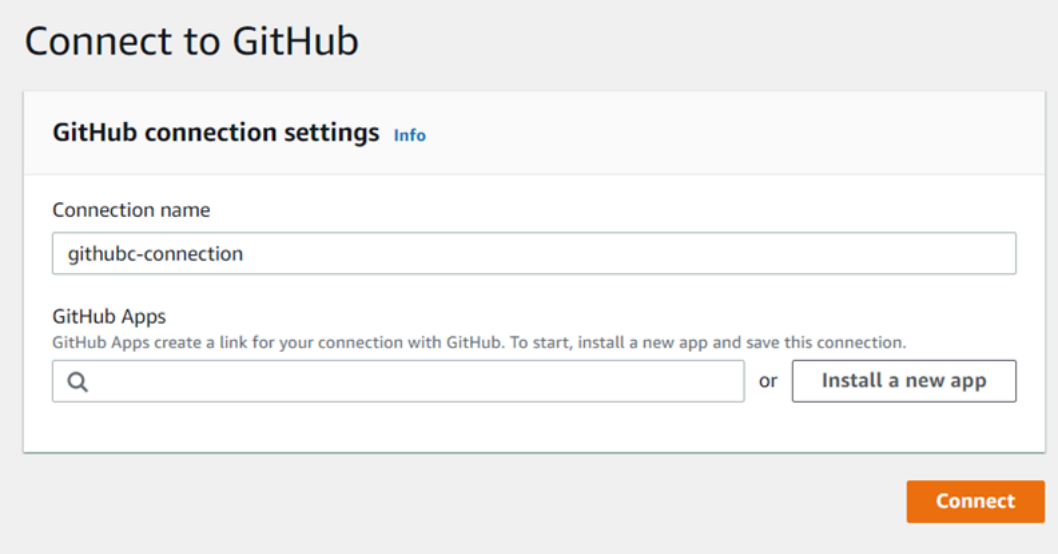


Para crear una conexión a GitHub

1. En la configuración de la GitHub conexión, el nombre de la conexión aparece en Nombre de la conexión. Elija Connect to (Conectar a GitHub). Aparece la página de solicitud de acceso.



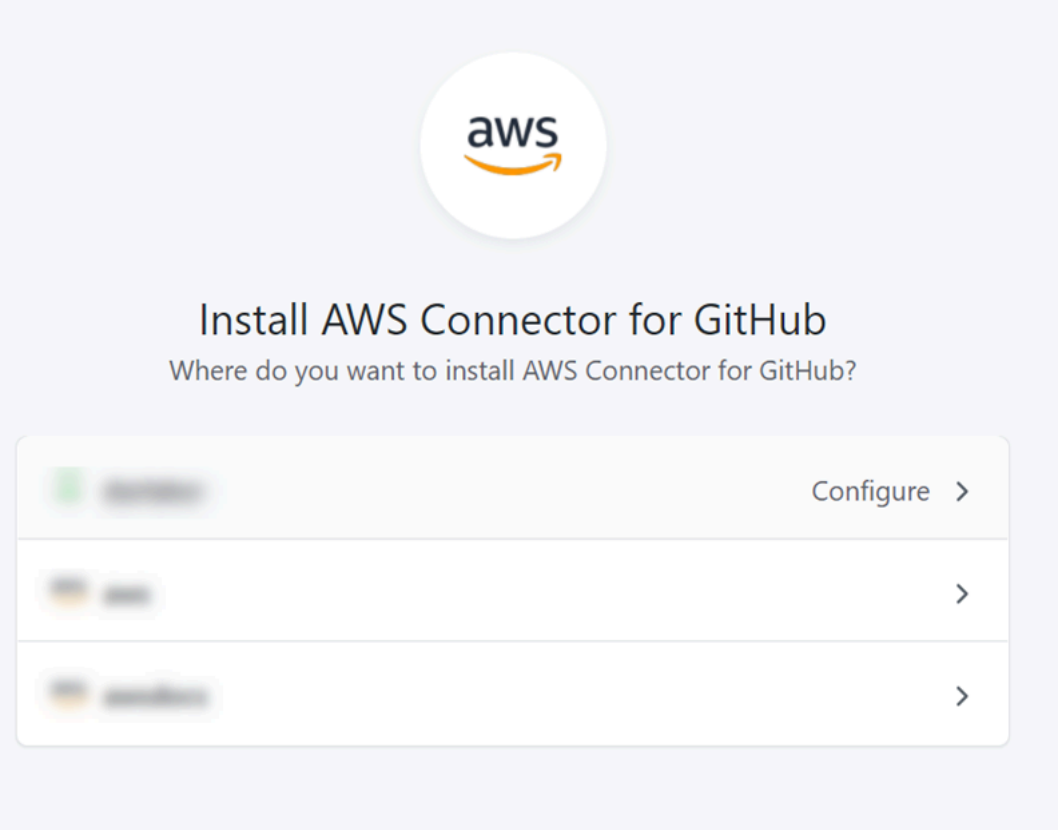
2. Seleccione Autorizar AWS conector para GitHub. Aparece la página de conexión y muestra el campo GitHub Aplicaciones.



3. En GitHub Aplicaciones, selecciona la instalación de una aplicación o selecciona Instalar una nueva aplicación para crear una.

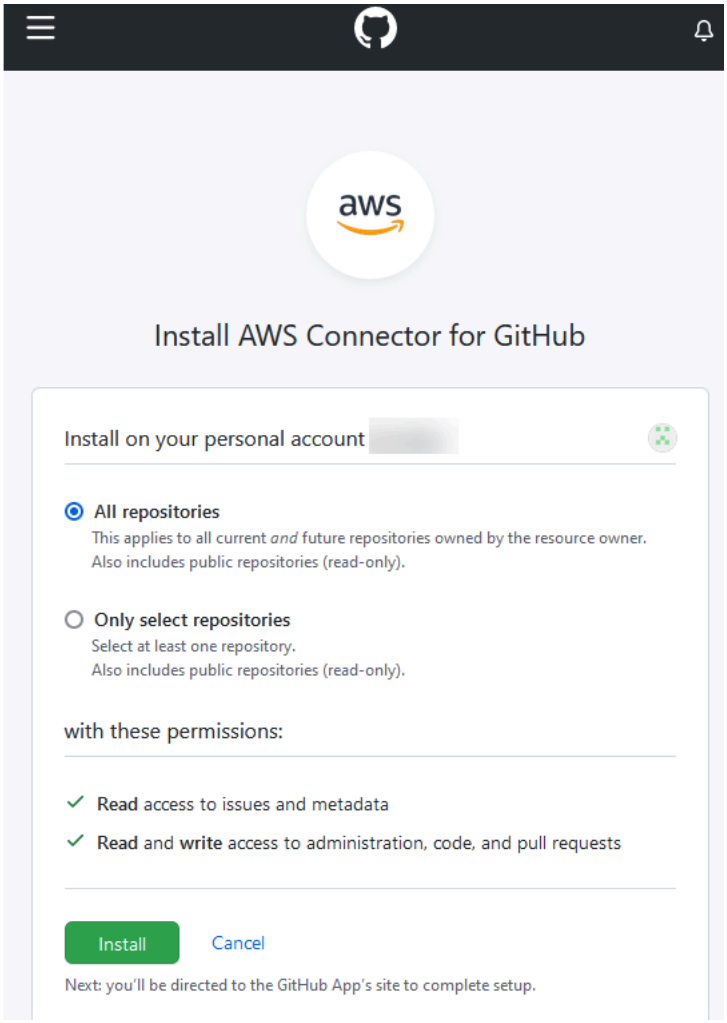
> **Note**
>
> Se instala una aplicación para todas las conexiones a un proveedor en particular. Si ya ha instalado el AWS conector para la GitHub aplicación, elíjalo y omita este paso.

4. En la GitHub página Instalar el AWS conector para, elige la cuenta en la que quieres instalar la aplicación.



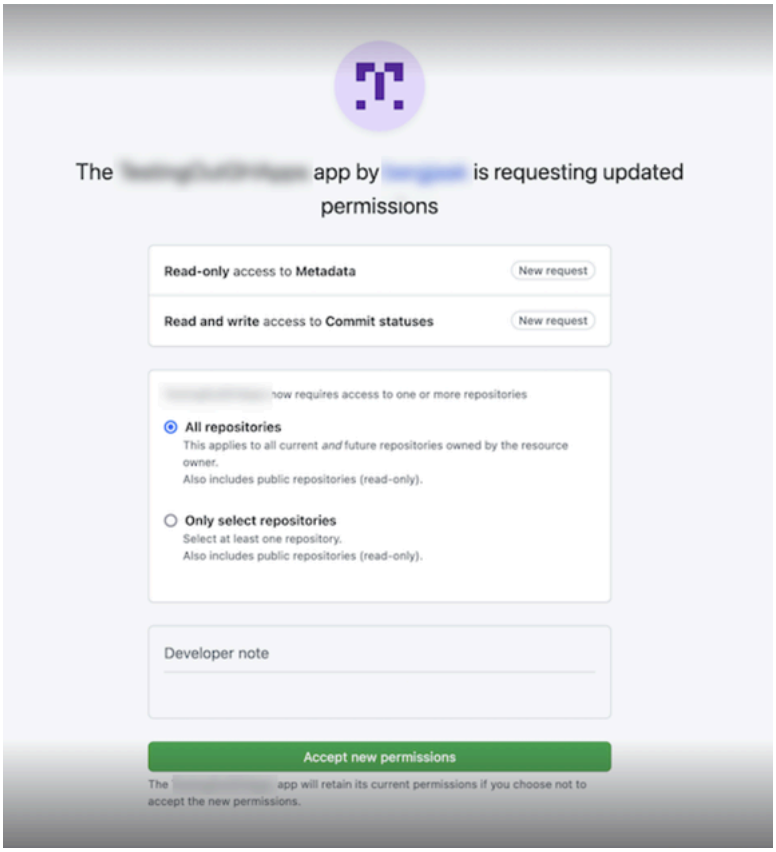
> **Note**
>
> Solo instalas la aplicación una vez para cada GitHub cuenta. Si instaló la aplicación previamente, puede elegir Configurar para dirigirse a una página de modificación para la instalación de la aplicación o puede utilizar el botón Atrás para volver a la consola.

5. En la GitHub página Instalar el AWS conector para, deja los valores predeterminados y selecciona Instalar.



Tras este paso, es posible que aparezca una página de permisos actualizada GitHub.

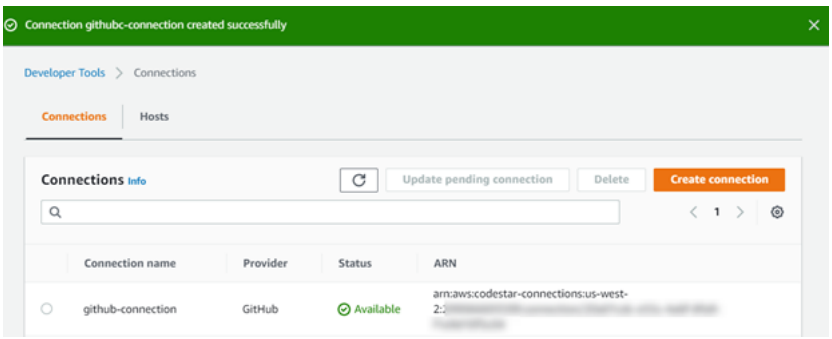
6. Si aparece una página en la que se indica que hay permisos actualizados para la GitHub aplicación AWS Connector for, seleccione Aceptar nuevos permisos.



7. Volverá a la GitHub página Conectar a. El identificador de conexión de la nueva instalación aparece en GitHubAplicaciones. Elija Conectar.

Visualización de la conexión creada

- La conexión creada se muestra en la lista de conexiones.



Crear una conexión a GitHub (CLI)

Puede usar AWS Command Line Interface (AWS CLI) para crear una conexión a GitHub.

Para ello, utilice el comando create-connection.

> **Important**
>
> Una conexión creada a través del AWS CLI o AWS CloudFormation está en `PENDING` estado de forma predeterminada. Después de crear una conexión con la CLI o AWS CloudFormation, utilice la consola para editar la conexión y establecer su estado`AVAILABLE`.

Para crear una conexión a GitHub

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice el AWS CLI para ejecutar el create-connection comando, especificando el `--provider-type` y `--connection-name` para la conexión. En este ejemplo, el nombre del proveedor de terceros es `GitHub` y el nombre especificado para la conexión es `MyConnection`.

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

   Si se ejecuta correctamente, este comando devuelve la información del ARN de la conexión, que será similar a lo siguiente.

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

2. Utilice la consola para completar la conexión. Para obtener más información, consulte Actualización de una conexión pendiente.

Cree una conexión a GitHub Enterprise Server

Las conexiones se utilizan para asociar AWS los recursos a un repositorio de terceros. Puede usar AWS Management Console o AWS Command Line Interface (AWS CLI) para crear una conexión a GitHub Enterprise Server.

Las conexiones solo proporcionan acceso a los repositorios propiedad de la cuenta de GitHub Enterprise Server que se utiliza durante la creación de la conexión para autorizar la instalación de la GitHub aplicación.

Antes de empezar

- Debe tener ya una instancia de GitHub Enterprise Server y un repositorio en ella.
- Debe ser administrador de la instancia de GitHub Enterprise Server para poder crear GitHub aplicaciones y crear un recurso de host, como se muestra en esta sección.

> **Important**
>
> Al configurar el host para GitHub Enterprise Server, se crea automáticamente un punto de enlace de VPC para los datos de eventos de webhooks. Si creaste tu host antes del 24 de noviembre de 2020 y quieres usar los puntos de enlace de PrivateLink webhook de VPC, primero debes eliminar tu host y, después, crear uno nuevo.

Temas

- Crea una conexión a GitHub Enterprise Server (consola)
- Crear una conexión a GitHub Enterprise Server (CLI)

Crea una conexión a GitHub Enterprise Server (consola)

Para crear una conexión con GitHub Enterprise Server, debe proporcionar información sobre dónde está instalado su GitHub Enterprise Server y autorizar la creación de la conexión con sus credenciales de GitHub Enterprise.

Temas

- Cree su conexión a GitHub Enterprise Server (consola)

Cree su conexión a GitHub Enterprise Server (consola)

Para crear una conexión a GitHub Enterprise Server, tenga preparadas la URL del servidor y las credenciales GitHub empresariales.

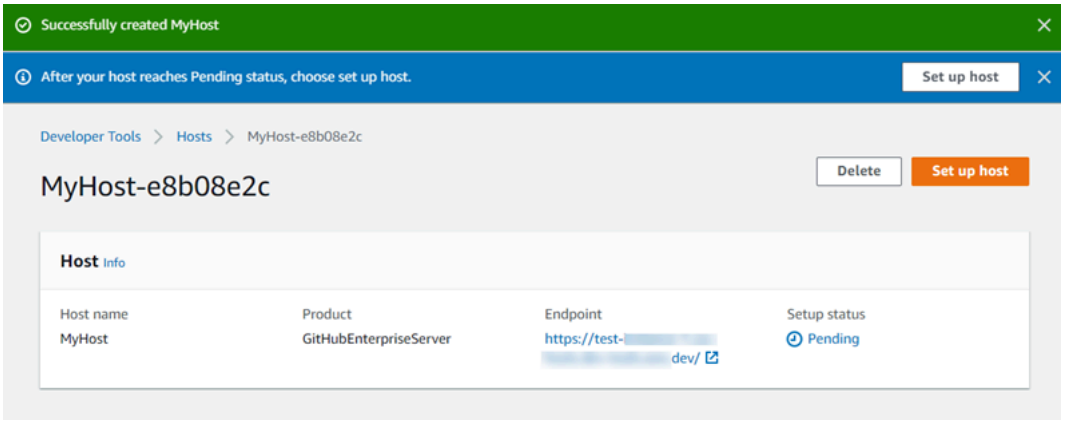
Para crear un alojamiento

1. Inicie sesión en y abra la AWS Management Console consola de herramientas para AWS desarrolladores enhttps://console.aws.amazon.com/codesuite/settings/connections.
2. En la pestaña Hosts (Alojamientos), elija Create host (Crear alojamiento).

3. En Host name (Nombre del alojamiento), ingrese el nombre que desea utilizar para el alojamiento.
4. En Seleccionar un proveedor, elija una de las siguientes opciones:
   - GitHub Servidor empresarial
   - GitLab autogestionado
5. En URL, ingrese el punto de enlace de la infraestructura donde está instalado el proveedor.
6. Si su servidor está configurado en una Amazon VPC y desea conectarse a su VPC, elija Use a VPC (Utilizar una VPC). En caso contrario, elija No VPC.
7. Si lanzó su instancia en una Amazon VPC y desea conectarse a su VPC, elija Use a VPC (Utilizar una VPC) y complete lo siguiente.
   a. En VPC ID (ID de la VPC), elija el ID de su VPC. Asegúrese de elegir la VPC para la infraestructura donde está instalada su instancia o una VPC con acceso a la instancia a través de VPN o Direct Connect.
   b. Si tiene una VPC privada configurada y ha configurado su instancia para realizar la validación de TLS mediante una entidad de certificación no pública, introduzca el ID de su certificado en Certificado TLS. El valor del certificado TLS es la clave pública del certificado.
8. Elija Create host (Crear alojamiento).
9. Una vez que se muestra la página de detalles del alojamiento, el estado del alojamiento cambia a medida que se crea el alojamiento.

> **Note**
>
> Si la configuración del alojamiento incluye una configuración de VPC, espere varios minutos para el aprovisionamiento de los componentes de red del alojamiento.

Espere a que el alojamiento alcance un estado Pendiente y, luego, complete la configuración. Para obtener más información, consulte Configuración de un alojamiento pendiente.

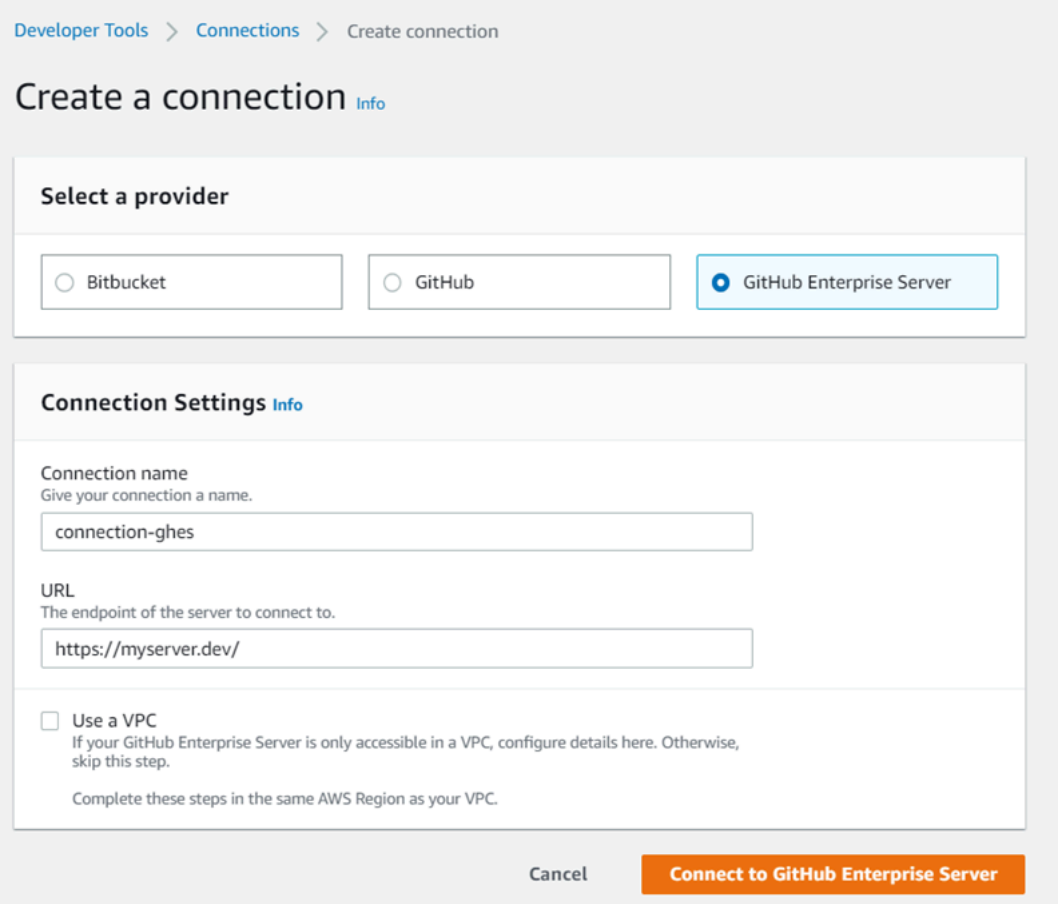


Paso 2: Cree su conexión a GitHub Enterprise Server (consola)

1. Inicie sesión en la consola de Herramientas para desarrolladores AWS Management Console y ábrala enhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Elija Settings > Connections (Configuración > Conexiones) y, luego, elija Create connection (Crear conexión).
3. Para crear una conexión a un repositorio de GitHub Enterprise Server instalado, elija GitHub Enterprise Server.

Conectarse a GitHub Enterprise Server

1. En Connection name (Nombre de la conexión), ingrese el nombre para la conexión.



2. En URL, ingrese el punto de enlace para el servidor.

> **Note**
>
> Si la URL proporcionada ya se ha utilizado para configurar un servidor GitHub empresarial para una conexión, se le pedirá que elija el ARN del recurso de host que se creó anteriormente para ese punto final.

3. (Opcional) Si ha lanzado su servidor en una Amazon VPC y desea conectarse a su VPC, elija Utilizar una VPC y complete lo siguiente.

   a. En VPC ID (ID de la VPC), elija el ID de su VPC. Asegúrese de elegir la VPC para la infraestructura en la que está instalada la instancia de GitHub Enterprise Server o una VPC con acceso a la instancia de GitHub Enterprise Server a través de VPN o Direct Connect.

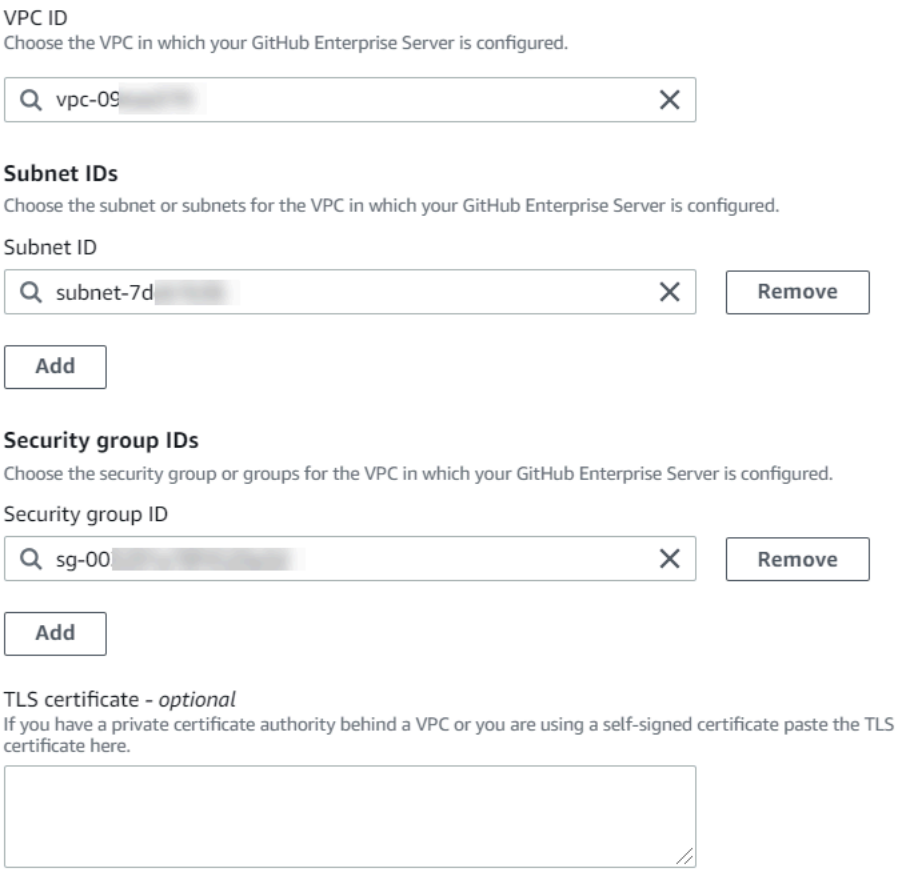
   b. En Subnet ID (ID de la subred), elija Add (Agregar). En el campo, elija el ID de la subred que desea utilizar para el alojamiento. Puede elegir hasta 10 subredes.

Asegúrese de elegir la subred para la infraestructura en la que está instalada la instancia de GitHub Enterprise Server o una subred con acceso a la instancia de GitHub Enterprise Server instalada a través de VPN o Direct Connect.

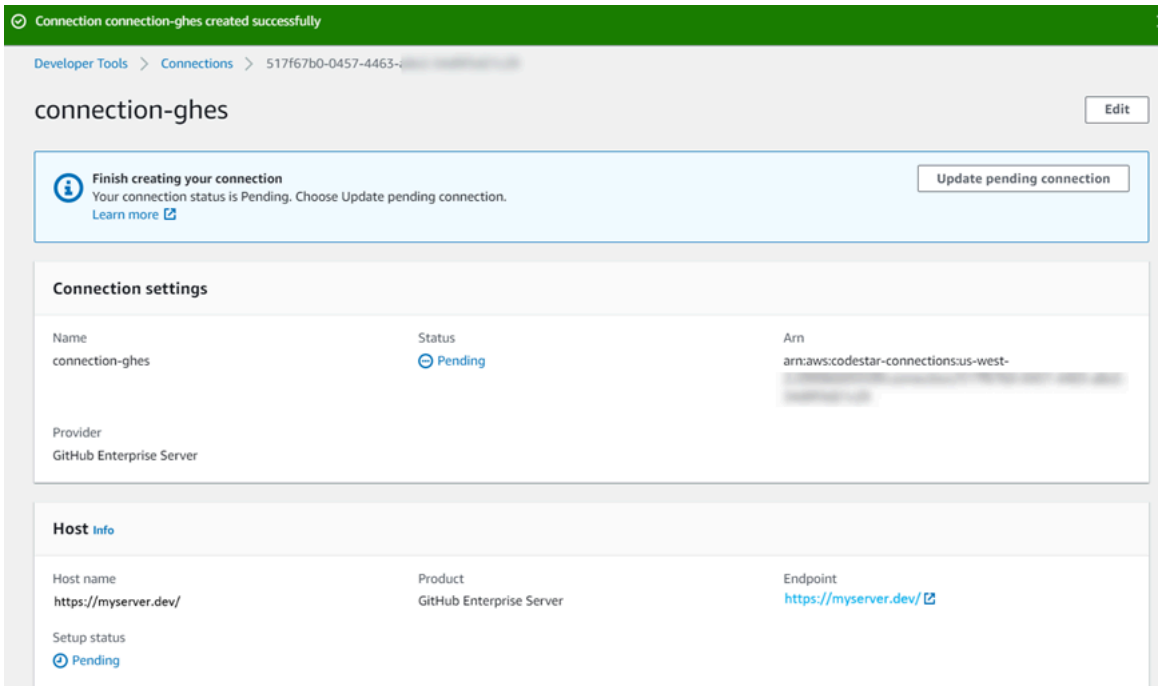
c. En Security group IDs (ID del grupo de seguridad), elija Add (Agregar). En el campo, elija el grupo de seguridad que desea utilizar para el alojamiento. Puede elegir hasta 10 grupos de seguridad.

   Asegúrese de elegir el grupo de seguridad para la infraestructura en la que está instalada la instancia de GitHub Enterprise Server o un grupo de seguridad con acceso a la instancia de GitHub Enterprise Server instalada a través de VPN o Direct Connect.

d. Si tiene configurada una VPC privada y ha configurado su instancia de GitHub Enterprise Server para realizar la validación de TLS mediante una entidad de certificación no pública, introduzca su ID de certificado en el certificado TLS. El valor del certificado TLS debe ser la clave pública del certificado.

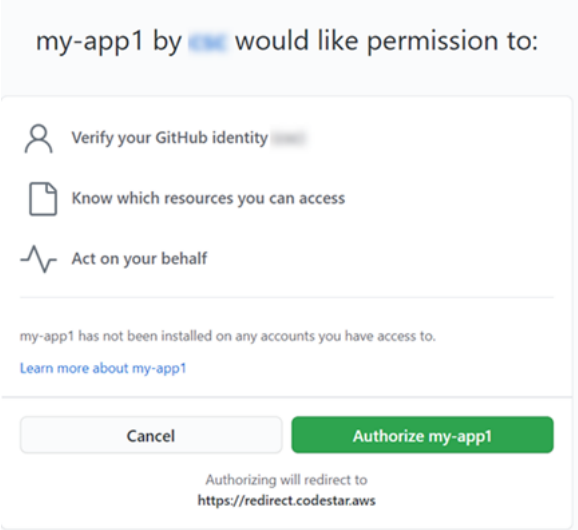


4. Elija Connect to GitHub Enterprise Server. La conexión creada se muestra con un estado Pendiente. Se crea un recurso de alojamiento para la conexión con la información del servidor que usted proporcionó. Se utiliza la URL para el nombre del alojamiento.
5. Elija Update pending connection (Actualizar conexión pendiente).



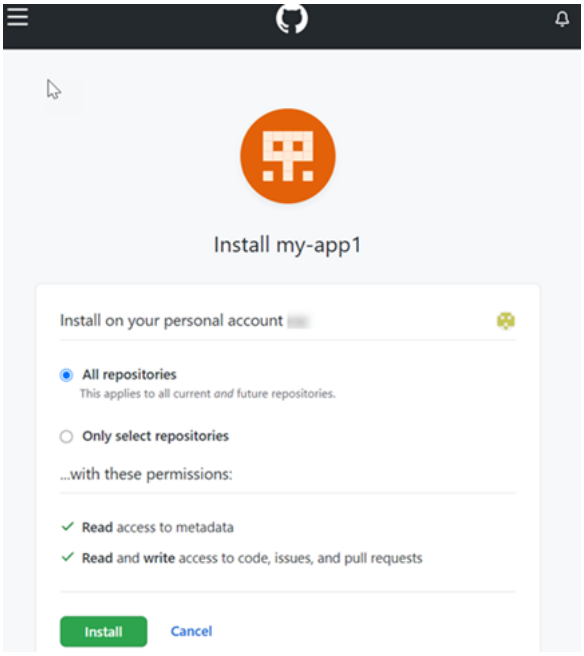
6. Si se te solicita, en la página de inicio de sesión de GitHub Enterprise, inicia sesión con tus credenciales de GitHub Enterprise.
7. En la página Crear GitHub aplicación, elige un nombre para la aplicación.

8. En la página de GitHub autorización, selecciona Autorizar<app-name>.



9. En la página de instalación de la aplicación, aparece un mensaje que indica que la aplicación AWS CodeStar Connector está lista para instalarse. Si tiene varias organizaciones, es posible que deba elegir la organización en la que desea instalar la aplicación.

   Elija la configuración del repositorio donde desea instalar la aplicación. Elija Instalar.



10. La página de conexión muestra la conexión creada en un estado Disponible.

Crear una conexión a GitHub Enterprise Server (CLI)

Puede usar AWS Command Line Interface (AWS CLI) para crear una conexión.

Para ello, utilice los comandos create-host y create-connection.

> **Important**
>
> Una conexión creada a través del AWS CLI o AWS CloudFormation está en `PENDING` estado de forma predeterminada. Después de crear una conexión con la CLI o AWS CloudFormation, utilice la consola para editar la conexión y establecer su estado`AVAILABLE`.

Paso 1: Crear un host para GitHub Enterprise Server (CLI)

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice el AWS CLI para ejecutar el create-host comando, especificando el `--name`--`provider-type`, y `--provider-endpoint` para la conexión. En este ejemplo, el nombre del proveedor de terceros es `GitHubEnterpriseServer` y el punto de conexión es `my-instance.dev`.

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

Si se ejecuta correctamente, este comando devuelve la información del nombre de recurso de Amazon (ARN) del alojamiento, que será similar a lo siguiente.

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

Después de este paso, el alojamiento se encuentra en estado `PENDING`.

2. Utilice la consola para completar la configuración del alojamiento y que el estado del alojamiento cambie a `Available`. Para obtener más información, consulte Configuración de un alojamiento pendiente.

Paso 2: Configurar un host pendiente en la consola

1. Inicie sesión en la consola de Herramientas para desarrolladores AWS Management Console y ábrala enhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Utilice la consola para completar la configuración del alojamiento y que el estado del alojamiento cambie a `Available`. Consulte Configuración de un alojamiento pendiente.

Paso 3: Para crear una conexión para GitHub Enterprise Server (CLI)

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice el AWS CLI para ejecutar el create-connection comando, especificando el `--host-arn` y `--connection-name` para la conexión.

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

Si se ejecuta correctamente, este comando devuelve la información del ARN de la conexión, que será similar a lo siguiente.

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

```
}
```

2. Utilice la consola para configurar la conexión pendiente. Para obtener más información, consulte Actualización de una conexión pendiente.

Paso 4: Para completar una conexión para GitHub Enterprise Server en la consola

1. Inicie sesión en la consola de Herramientas para desarrolladores AWS Management Console y ábrala enhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Use la consola para configurar la conexión pendiente y mover la conexión a un estado `Available`. Para obtener más información, consulte Actualización de una conexión pendiente.

Cree una conexión a GitLab

Puedes usar el AWS Management Console o el AWS Command Line Interface (AWS CLI) para crear una conexión a un repositorio alojado en gitlab.com.

> **Note**
>
> Al autorizar la instalación de esta conexión GitLab, concedes a nuestro servicio permisos para procesar tus datos y puedes revocar los permisos en cualquier momento desinstalando la aplicación.

Antes de empezar

- Debe haber creado ya una cuenta con. GitLab

> **Note**
>
> Las conexiones solo dan acceso a la cuenta que se utilizó para crear y autorizar la conexión.

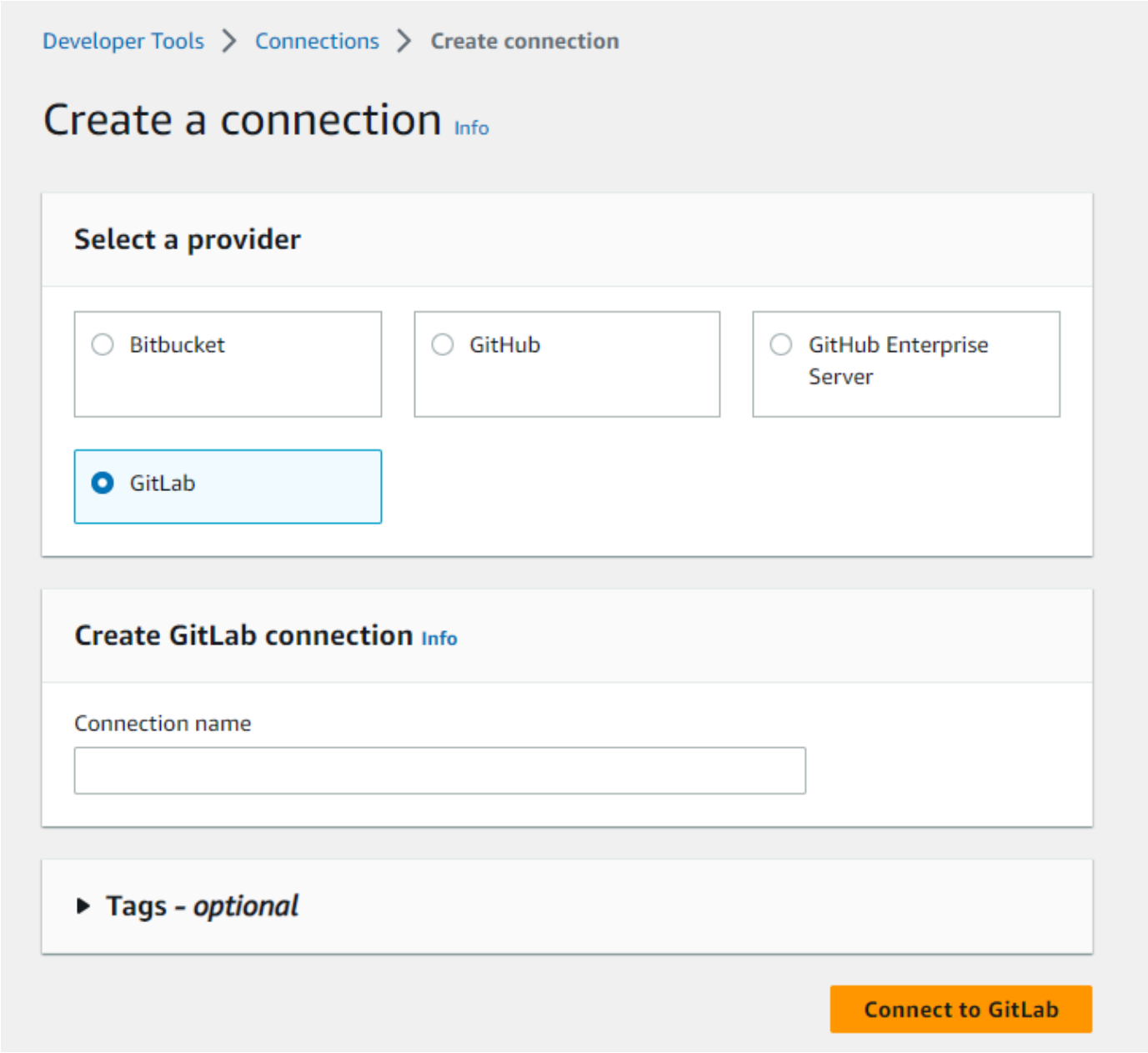
> **Note**
>
> Puede crear conexiones en las que tenga el rol de propietario y GitLab, a continuación, la conexión se puede utilizar con el repositorio con recursos como CodePipeline: En el caso de los repositorios en grupos, no es necesario que sea el propietario del grupo.

Temas

Cree una conexión a GitLab (consola)

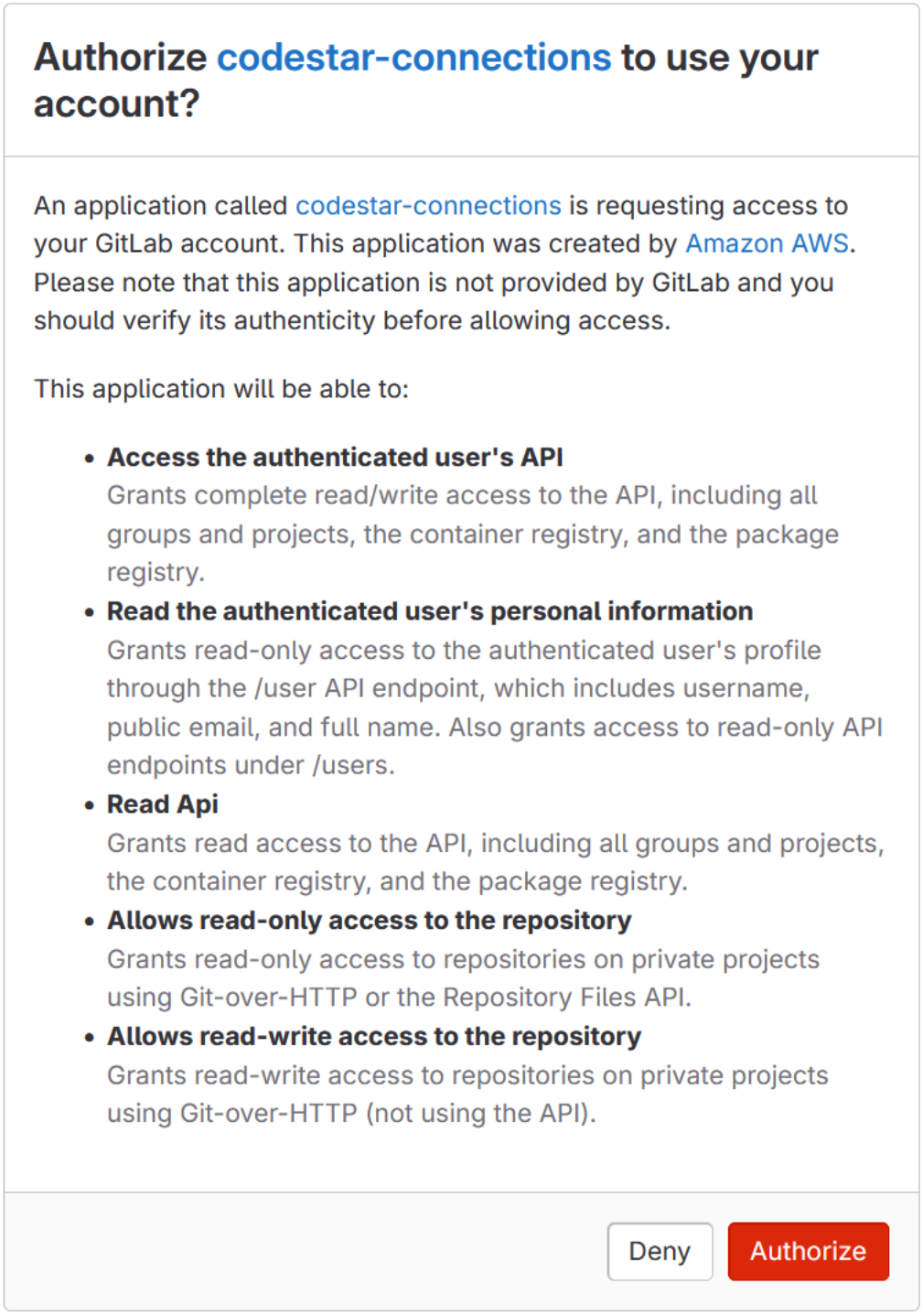
Paso 1: Crear una conexión

1. Inicie sesión en y AWS Management Console, a continuación, abra la consola de Herramientas para AWS desarrolladores enhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Elija Configuración y, a continuación, elija Conexiones. Seleccione Crear conexión.
3. Para crear una conexión a un GitLab repositorio, en Seleccione un proveedor, elija GitLab. En Nombre de la conexión, introduzca el nombre de la conexión que desea crear. Selecciona Conectar a GitLab.



4. Cuando aparezca la página de inicio de GitLab sesión, inicia sesión con tus credenciales y, a continuación, selecciona Iniciar sesión.
5. Aparece una página de autorización con un mensaje en la que se solicita la autorización de la conexión para acceder a tu GitLab cuenta.

   Seleccione Autorizar.



6. El navegador vuelve a la página de la consola de conexiones. En Crear GitLab conexión, la nueva conexión se muestra en el nombre de la conexión.
7. Selecciona Conectar a GitLab.

Cuando la conexión se haya creado correctamente, se mostrará el banner de realización correcta. Los detalles de la conexión se muestran en la página Ajustes de conexión.

Crear una conexión a GitLab (CLI)

Puede usar AWS Command Line Interface (AWS CLI) para crear una conexión.

Para ello, utilice el comando create-connection.

> **Important**
>
> Una conexión creada a través del AWS CLI o AWS CloudFormation está en `PENDING` estado de forma predeterminada. Después de crear una conexión con la CLI o AWS CloudFormation, utilice la consola para editar la conexión y establecer su estado`AVAILABLE`.

Para crear una conexión a GitLab

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice el AWS CLI para ejecutar el create-connection comando, especificando el `--provider-type` y `--connection-name` para la conexión. En este ejemplo, el nombre del proveedor de terceros es `GitLab` y el nombre especificado para la conexión es `MyConnection`.

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

   Si se ejecuta correctamente, este comando devuelve la información del ARN de la conexión, que será similar a lo siguiente.

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

2. Utilice la consola para completar la conexión. Para obtener más información, consulte Actualización de una conexión pendiente.

Cree una conexión a una red GitLab autogestionada

Puede crear conexiones para GitLab Enterprise Edition o GitLab Community Edition con una instalación autogestionada.

Puede usar AWS Management Console o AWS Command Line Interface (AWS CLI) para crear una conexión y hospedarla de forma GitLab autogestionada.

> **Note**
>
> Al autorizar esta aplicación de conexión como GitLab autogestionada, concedes a nuestro servicio permisos para procesar tus datos y puedes revocar los permisos en cualquier momento desinstalando la aplicación.

Antes de crear una conexión GitLab autogestionada, debe crear un host para utilizarlo en la conexión, tal y como se detalla en estos pasos. Para obtener información general sobre el flujo de trabajo de creación de hosts para proveedores instalados, consulte Flujo de trabajo para crear o actualizar un host.

Si lo desea, puede configurar su host con una VPC. Para obtener más información acerca de la configuración de la VPC y la red para su recurso de host, consulte los requisitos previos de la VPC en (Opcional) Requisitos previos: configuración de red o Amazon VPC para la conexión y Solución de problemas de la configuración de una VPC para el alojamiento.

Antes de empezar

- Debe haber creado ya una cuenta GitLab y disponer de GitLab Enterprise Edition o GitLab Community Edition con una instalación autogestionada. Para obtener más información, consulte https://docs.gitlab.com/ee/subscriptions/self_managed/.

  > **Note**
  >
  > Las conexiones solo dan acceso a la cuenta que se utilizó para crear y autorizar la conexión.

> **Note**
>
> Puede crear conexiones a un repositorio en el que tenga el rol de propietario y GitLab, a continuación, utilizar la conexión con recursos como CodePipeline: En el caso de los repositorios en grupos, no es necesario que sea el propietario del grupo.

- Debe haber creado ya un token de acceso GitLab personal (PAT) únicamente con el siguiente permiso limitado: api. Para obtener más información, consulte https://docs.gitlab.com/ee/user/profile/personal_access_tokens.html. Solo se puede usar el PAT utilizado por un administrador.

> **Note**
>
> Su PAT se utiliza para autorizar el host y las conexiones no la almacenan ni lo utilizan de ningún otro modo. Para configurar un host, puede crear un PAT temporal y, después de configurar el host, puede eliminarlo.

Temas

- Cree una conexión GitLab autogestionada (consola)
- Crear una conexión a la red GitLab autogestionada (CLI)

Cree una conexión GitLab autogestionada (consola)

Siga estos pasos para crear un host y una conexión GitLab autogestionada en la consola. Para obtener información acerca de las consideraciones de la configuración de un host en una VPC, consulte (Opcional) Requisitos previos: configuración de red o Amazon VPC para la conexión.

> **Note**
>
> Cree un host para una única instalación GitLab autogestionada y, a continuación, podrá administrar una o más conexiones GitLab autogestionadas a ese host.

Paso 1: Crear el host

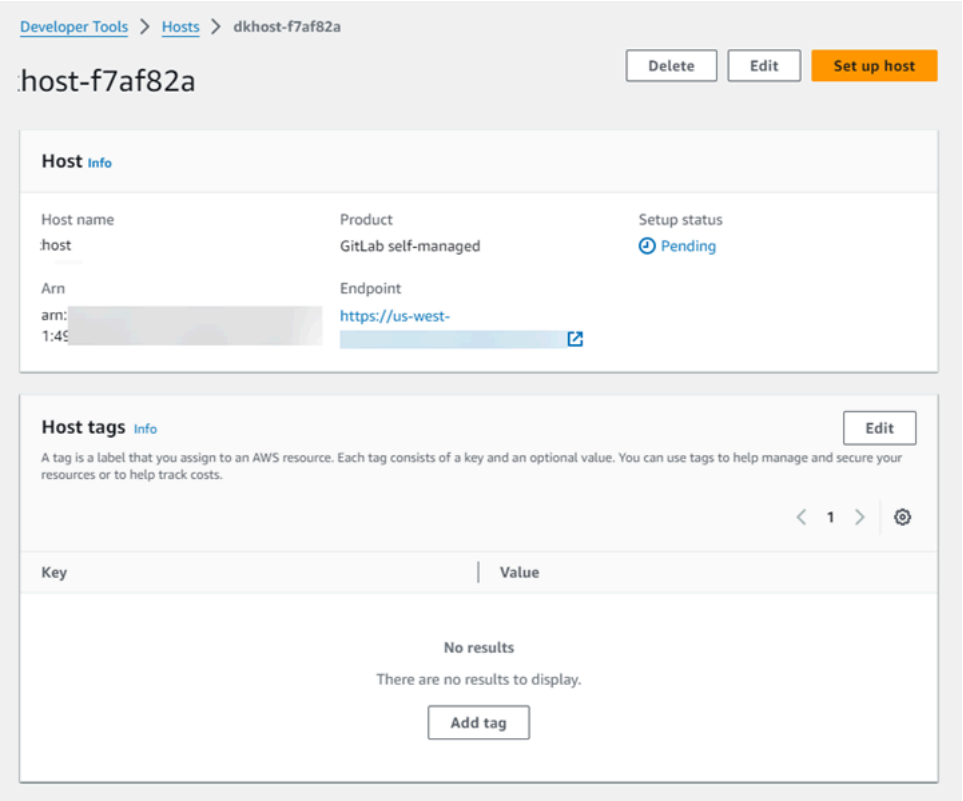
1. Inicie sesión en y AWS Management Console, a continuación, abra la consola de Herramientas para AWS desarrolladores en. https://console.aws.amazon.com/codesuite/settings/connections
2. En la pestaña Hosts (Alojamientos), elija Create host (Crear alojamiento).
3. En Host name (Nombre del alojamiento), ingrese el nombre que desea utilizar para el alojamiento.
4. En Seleccione un proveedor, elija GitLabautogestionado.
5. En URL, ingrese el punto de enlace de la infraestructura donde está instalado el proveedor.
6. Si su servidor está configurado en una Amazon VPC y desea conectarse a su VPC, elija Use a VPC (Utilizar una VPC). En caso contrario, elija No VPC.
7. (Opcional) Si ha lanzado su host en una Amazon VPC y desea conectarse a su VPC, elija Utilizar una VPC y complete lo siguiente.

   a. En VPC ID (ID de la VPC), elija el ID de su VPC. Asegúrese de elegir la VPC para la infraestructura donde está instalado su host o una VPC con acceso a la instancia a través de VPN o Direct Connect.

   b. Si tiene una VPC privada configurada y ha configurado su host para realizar la validación de TLS mediante una entidad de certificación no pública, introduzca el ID de su certificado en Certificado TLS. El valor del certificado TLS es la clave pública del certificado.
8. Elija Create host (Crear alojamiento).
9. Una vez que se muestra la página de detalles del alojamiento, el estado del alojamiento cambia a medida que se crea el alojamiento.

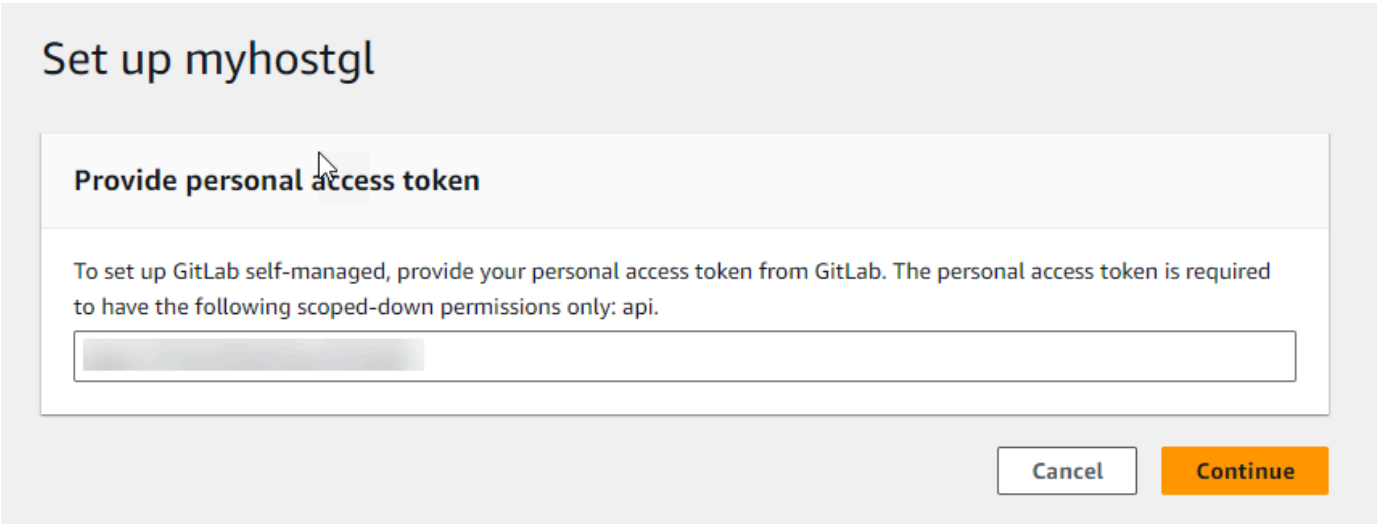
> **Note**
>
> Si la configuración del alojamiento incluye una configuración de VPC, espere varios minutos para el aprovisionamiento de los componentes de red del alojamiento.

Espere a que el alojamiento alcance un estado Pendiente y, luego, complete la configuración. Para obtener más información, consulte Configuración de un alojamiento pendiente.

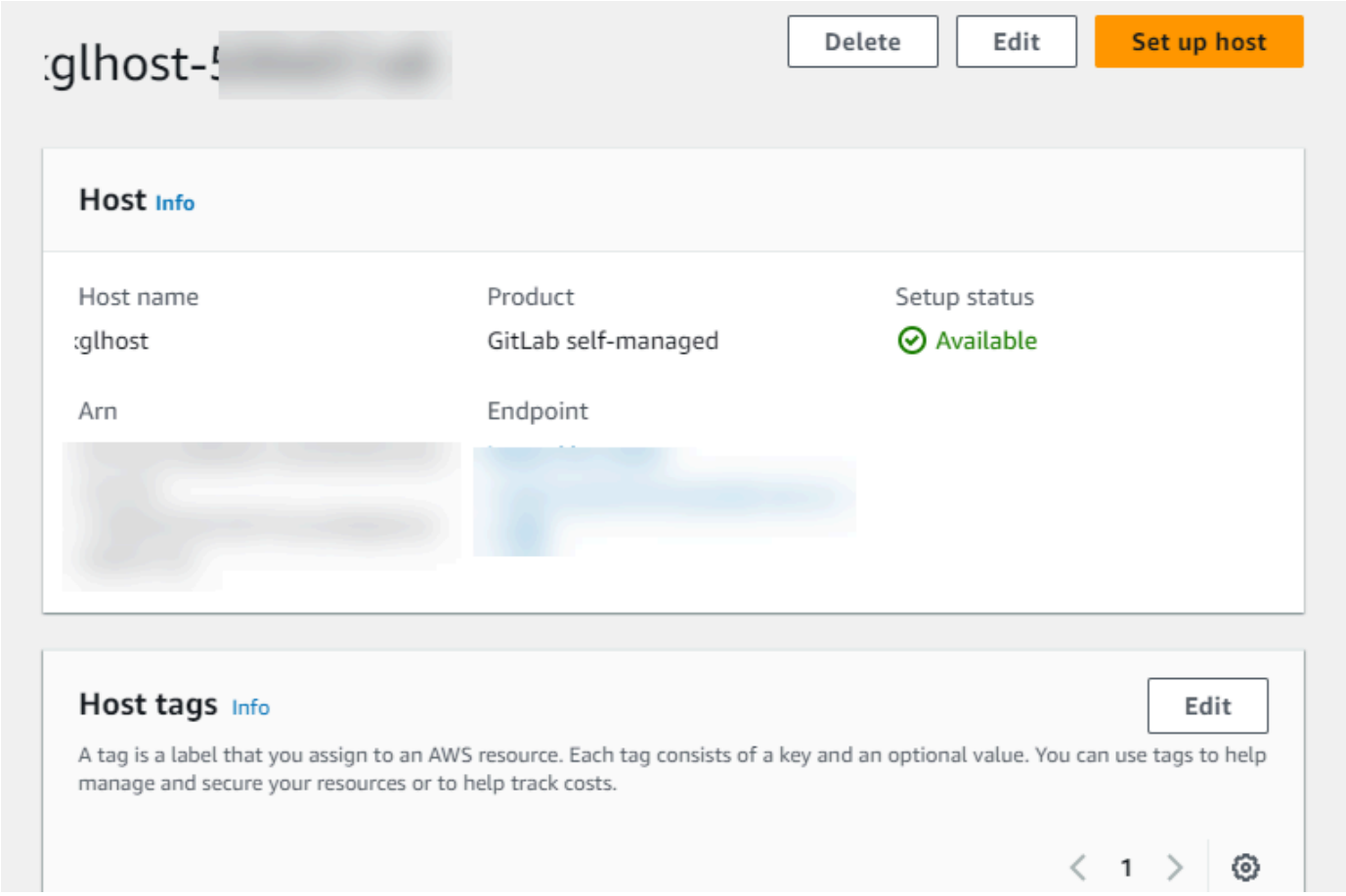


Paso 2: Configurar su host pendiente

1. Elija Configurar host.
2. Aparece la página Configurar ***`host_name`***. En Proporcionar un token de acceso personal, proporciona a tu GitLab PAT únicamente el siguiente permiso limitado: api.

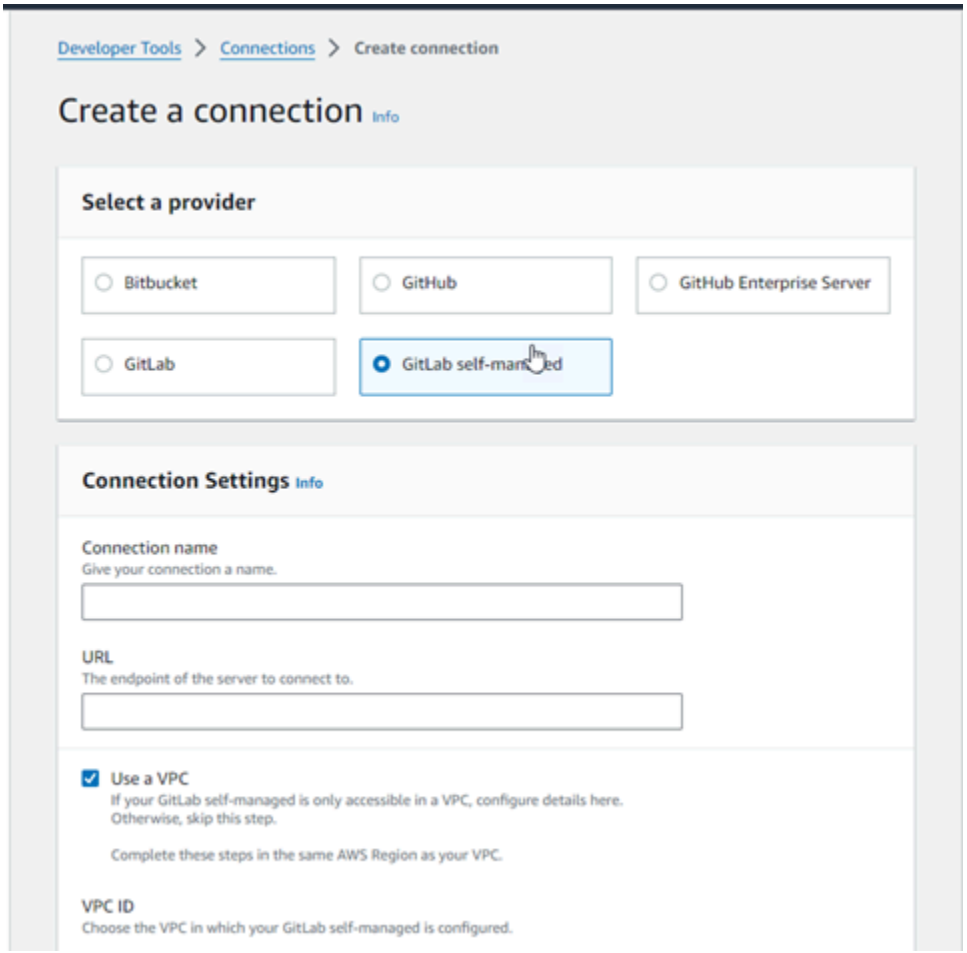


3. Una vez que el alojamiento se registró correctamente, aparece la página de detalles del alojamiento y muestra que el estado del alojamiento es Disponible.



Paso 3: Crear una conexión

1. Inicie sesión en y AWS Management Console, a continuación, abra la consola de Herramientas para AWS desarrolladores enhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Elija Configuración y, a continuación, elija Conexiones. Seleccione Crear conexión.
3. Para crear una conexión a un GitLab repositorio, en Seleccione un proveedor, elija GitLab autogestionado. En Nombre de la conexión, introduzca el nombre de la conexión que desea crear.



4. En URL, ingrese el punto de conexión para el servidor.
5. Si lanzó su servidor en una Amazon VPC y desea conectarse a su VPC, elija Use a VPC (Utilizar una VPC) y complete lo siguiente.

   a. En VPC ID (ID de la VPC), elija el ID de su VPC. Asegúrese de elegir la VPC para la infraestructura donde está instalado su host o una VPC con acceso al host a través de VPN o Direct Connect.

   b. En Subnet ID (ID de la subred), elija Add (Agregar). En el campo, elija el ID de la subred que desea utilizar para el alojamiento. Puede elegir hasta 10 subredes.

      Asegúrese de elegir la subred para la infraestructura donde está instalado su host o una subred con acceso al host instalado a través de VPN o Direct Connect.

   c. En Security group IDs (ID del grupo de seguridad), elija Add (Agregar). En el campo, elija el grupo de seguridad que desea utilizar para el alojamiento. Puede elegir hasta 10 grupos de seguridad.

Asegúrese de elegir el grupo de seguridad para la infraestructura en la que está instalado su host o un grupo de seguridad con acceso a su host instalado a través de VPN o Direct Connect.

d. Si tiene una VPC privada configurada y ha configurado su host para realizar la validación de TLS mediante una entidad de certificación no pública, introduzca el ID de su certificado en Certificado TLS. El valor del certificado TLS debe ser la clave pública del certificado.

6. Elige Conectar para GitLab autogestionarse. La conexión creada se muestra con un estado Pendiente. Se crea un recurso de alojamiento para la conexión con la información del servidor que usted proporcionó. Se utiliza la URL para el nombre del alojamiento.
7. Elija Update pending connection (Actualizar conexión pendiente).
8. Cuando aparezca la página de inicio de GitLab sesión, inicia sesión con tus credenciales y, a continuación, selecciona Iniciar sesión.
9. Aparece una página de autorización con un mensaje en la que se solicita la autorización de la conexión para acceder a tu GitLab cuenta.

   Seleccione Autorizar.
10. El navegador vuelve a la página de la consola de conexiones. En Crear GitLab conexión, la nueva conexión se muestra en el nombre de la conexión.
11. Elige Conectar para GitLab autogestionarse.

    Cuando la conexión se haya creado correctamente, se mostrará el banner de realización correcta. Los detalles de la conexión se muestran en la página Ajustes de conexión.

Crear una conexión a la red GitLab autogestionada (CLI)

Puede usar el AWS Command Line Interface (AWS CLI) para crear un host y una conexión de forma GitLab autogestionada.

Para ello, utilice los comandos create-host y create-connection.

> **Important**
>
> Una conexión creada a través del AWS CLI o AWS CloudFormation está en `PENDING` estado de forma predeterminada. Después de crear una conexión con la CLI o AWS CloudFormation, utilice la consola para editar la conexión y establecer su estado`AVAILABLE`.

Paso 1: Crear un host para GitLab autogestión (CLI)

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice el AWS CLI para ejecutar el create-host comando, especificando el `--name--provider-type`, y `--provider-endpoint` para la conexión. En este ejemplo, el nombre del proveedor de terceros es `GitLabSelfManaged` y el punto de conexión es `my-instance.dev`.

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

   Si se ejecuta correctamente, este comando devuelve la información del nombre de recurso de Amazon (ARN) del alojamiento, que será similar a lo siguiente.

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

   Después de este paso, el alojamiento se encuentra en estado `PENDING`.

2. Utilice la consola para completar la configuración del host y mover el host a un que el estado del alojamiento cambie a estado `Available` en el siguiente paso.

Paso 2: Configurar un host pendiente en la consola

1. Inicie sesión en la consola de Herramientas para desarrolladores AWS Management Console y ábrala enhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Utilice la consola para completar la configuración del alojamiento y que el estado del alojamiento cambie a `Available`. Consulte Configuración de un alojamiento pendiente.

Paso 3: Para crear una conexión GitLab autogestionada (CLI)

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice el AWS CLI para ejecutar el create-connection comando, especificando el `--host-arn` y `--connection-name` para la conexión.

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

Si se ejecuta correctamente, este comando devuelve la información del ARN de la conexión, que será similar a lo siguiente.

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

2. Utilice la consola para configurar la conexión pendiente en el siguiente paso.

Paso 4: Para completar una conexión GitLab autogestionada en la consola

1. Inicie sesión en la consola de herramientas para desarrolladores AWS Management Console y ábrala enhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Use la consola para configurar la conexión pendiente y mover la conexión a un estado `Available`. Para obtener más información, consulte Actualización de una conexión pendiente.

Actualización de una conexión pendiente

Una conexión creada a través de AWS Command Line Interface (AWS CLI) o AWS CloudFormation que está en `PENDING` estado de forma predeterminada. Tras crear una conexión con AWS CLI o AWS CloudFormation, utilice la consola para actualizar la conexión y establecer su estado`AVAILABLE`.

> **Note**
>
> Se debe utilizar la consola para actualizar una conexión pendiente. No se puede actualizar una conexión pendiente mediante la AWS CLI.

La primera vez que utilice la consola para agregar una nueva conexión a un proveedor de terceros, deberá completar el protocolo de enlace OAuth con el proveedor de terceros utilizando la instalación asociada a la conexión.

Puede utilizar la consola de Developer Tools para completar una conexión pendiente.

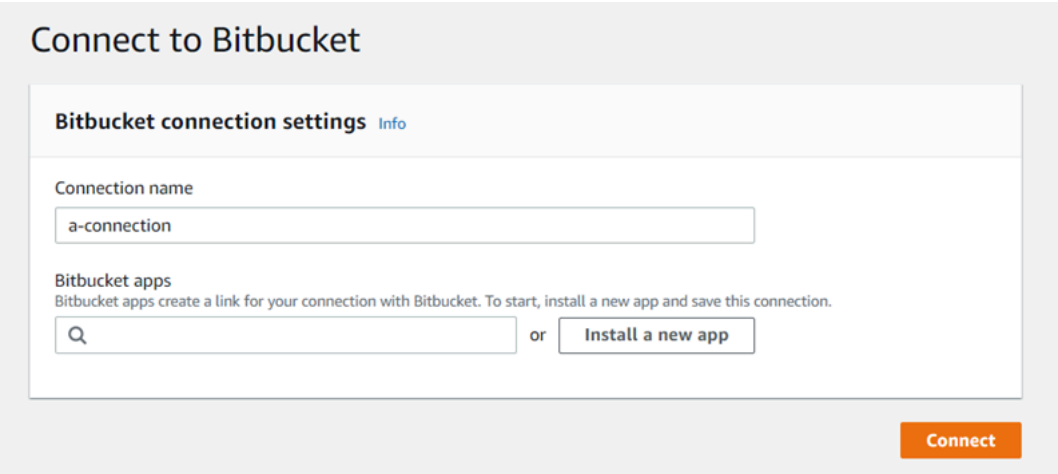
Para completar una conexión

1. Abra la consola de herramientas para AWS desarrolladores enhttps://console.aws.amazon.com/codesuite/settings/connections.
2. Elija Settings > Connections (Configuración > Conexiones).

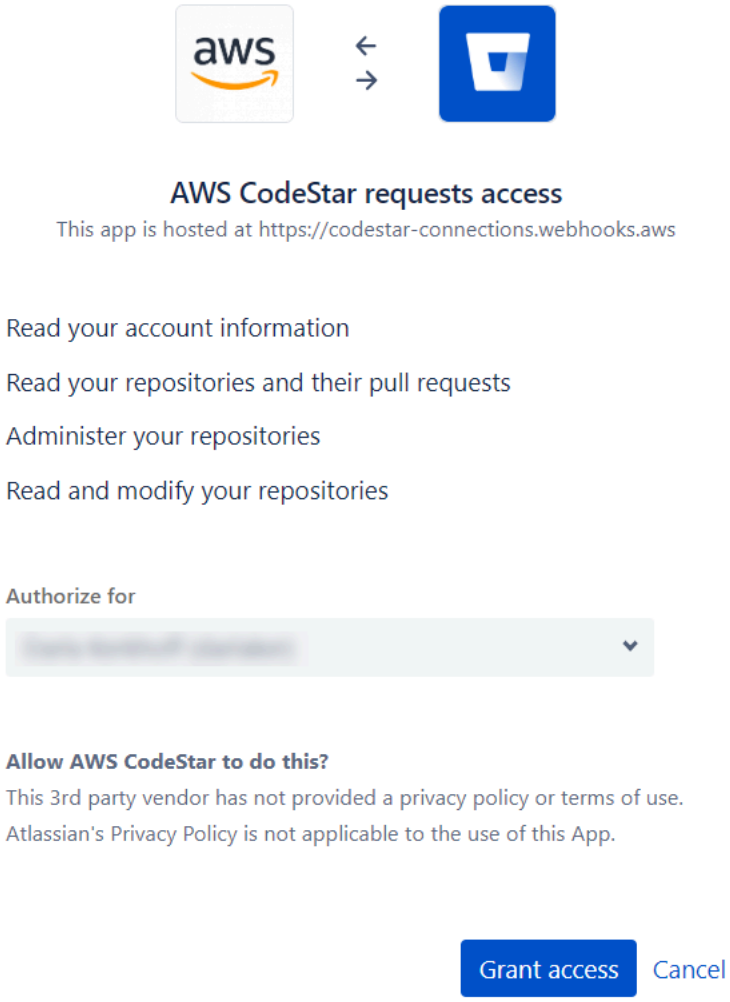
   Se muestran los nombres de todas las conexiones asociadas a su AWS cuenta.
3. En Nombre, elija el nombre de la conexión pendiente que desee actualizar.

   Update a pending connection (Actualizar una conexión pendiente) se habilita cuando se elige una conexión con un estado Pendiente.
4. Elija Update a pending connection (Actualizar una conexión pendiente).
5. En la página Connect to Bitbucket (Conectarse a Bitbucket), en Connection name (Nombre de la conexión), verifique el nombre de su conexión.

   En Bitbucket apps (Aplicaciones de Bitbucket), elija la instalación de una aplicación o elija Install a new app (Instalar una aplicación nueva) para crear una.



6. En la página de instalación de la aplicación, aparece un mensaje que indica que la AWS CodeStar aplicación está intentando conectarse a tu cuenta de Bitbucket. Elija Grant access (Conceder acceso).



7. Se muestra el ID de conexión de la nueva instalación. Elija Complete connection (Completar conexión).

Mostrar conexiones

Puede utilizar la consola de Developer Tools o el comando list-connections de AWS Command Line Interface (AWS CLI) para ver una lista con las conexiones de su cuenta.

Mostrar conexiones (consola)

Para mostrar las conexiones

1. Abra la consola de herramientas para desarrolladores en https://console.aws.amazon.com/codesuite/settings/connections.
2. Elija Settings > Connections (Configuración > Conexiones).

3. Consulte el nombre, el estado y el ARN de las conexiones.

Mostrar conexiones (CLI)

Puedes usarla AWS CLI para enumerar tus conexiones a repositorios de código de terceros. Para una conexión asociada a un recurso de host, como las conexiones a GitHub Enterprise Server, la salida devuelve además el ARN del host.

Para ello, utilice el comando list-connections.

Para mostrar las conexiones

- Abre una terminal (Linux, macOS o Unix) o una línea de comandos (Windows) y usa la AWS CLI para ejecutar el list-connections comando.

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

Este comando devuelve la siguiente salida.

```
{
     "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"
}
```

Eliminar una conexión

Puede utilizar la consola de herramientas para desarrolladores o el comando delete-connection en la AWS Command Line Interface (AWS CLI) para eliminar una conexión.

Temas

Eliminación de una conexión (consola)

Para eliminar una conexión

1. Abra la consola de herramientas para desarrolladores en https://console.aws.amazon.com/codesuite/settings/connections.
2. Elija Settings > Connections (Configuración > Conexiones).
3. En Nombre de la conexión, elija el nombre de la conexión que desea eliminar.
4. Elija Eliminar.
5. Escriba **`delete`** en el campo para confirmar y elija Eliminar.

> **Important**
>
> Esta acción no se puede deshacer.

Eliminación de una conexión (CLI)

Puede usar el AWS Command Line Interface (AWS CLI) para eliminar una conexión.

Para ello, utilice el comando delete-connection.

> **Important**
>
> Después de ejecutar el comando, se elimina la conexión. No se muestra ningún cuadro de diálogo de confirmación. Puede crear una nueva conexión, pero el nombre de recurso de Amazon (ARN) no se reutiliza nunca.

Para eliminar una conexión

- Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice el AWS CLI para ejecutar el delete-connection comando, especificando el ARN de la conexión que desea eliminar.

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

  Este comando no devuelve nada.

Etiquetado de recursos de conexiones

Una etiqueta es una etiqueta de atributo personalizada que usted o AWS asigna a un AWS recurso. Cada AWS etiqueta consta de dos partes:

- Una clave de etiqueta (por ejemplo, `CostCenter`, `Environment` o `Project`). Las claves de etiqueta distinguen entre mayúsculas y minúsculas.
- Un campo opcional que se denomina valor de etiqueta (por ejemplo, `111122223333` o `Production`o el nombre de un equipo). Omitir el valor de etiqueta es lo mismo que utilizar una cadena vacía. Al igual que las claves de etiqueta, los valores de etiqueta distinguen entre mayúsculas y minúsculas.

En conjunto, se conocen como pares clave-valor.

Puede utilizar la consola o la CLI para etiquetar recursos.

Puede etiquetar los siguientes tipos de recursos de CodeConnections:

- Conexiones
- Anfitriones

En estos pasos se presupone que ya ha instalado una versión reciente de la versión actual AWS CLI o que la ha actualizado a ella. Para obtener más información, consulte Instalar la AWS CLI en la Guía del usuario de AWS Command Line Interface .

Además de identificar, organizar y realizar un seguimiento del recurso mediante etiquetas, puede utilizarlas en las políticas AWS Identity and Access Management (de IAM) para controlar quién puede

ver el recurso e interactuar con él. Para ver ejemplos de políticas de acceso basadas en etiquetas, consulte Uso de etiquetas para controlar el acceso a los recursos de AWS CodeStar Connections.

Temas

- Etiquetado de recursos (consola)
- Etiquetado de recursos (CLI)

Etiquetado de recursos (consola)

Puede utilizar la consola para agregar, actualizar o eliminar etiquetas en un recurso de conexiones.

Temas

- Agregado de etiquetas a un recurso de conexiones (consola)
- Visualización de etiquetas de un recurso de conexiones (consola)
- Edición de etiquetas de un recurso de conexiones (consola)
- Eliminación de etiquetas de un recurso de conexiones (consola)

Agregado de etiquetas a un recurso de conexiones (consola)

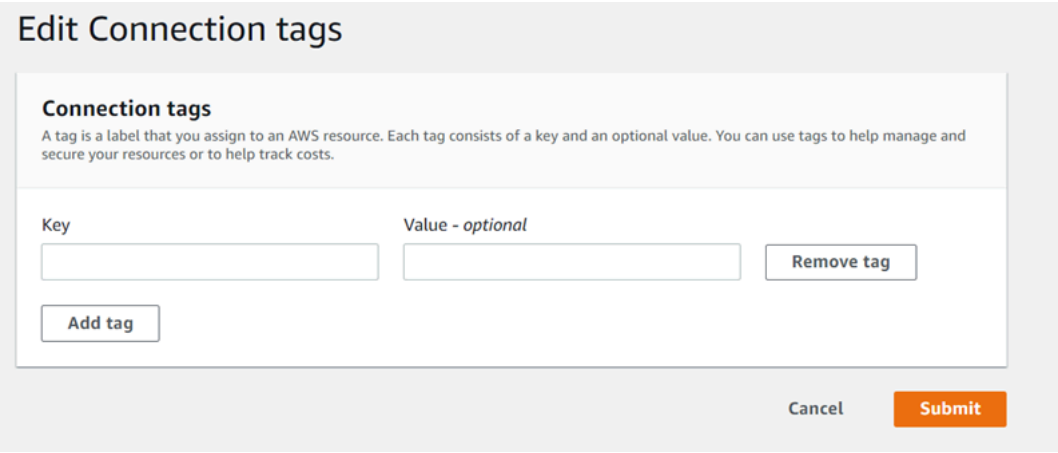
Puede utilizar la consola para agregar etiquetas a una conexión o un alojamiento existente.

> **Note**
>
> Al crear una conexión para un proveedor instalado, como GitHub Enterprise Server, y también se crea un recurso de host para usted, las etiquetas durante la creación solo se agregan a la conexión. Esto permite etiquetar un alojamiento por separado si desea reutilizarlo para una conexión nueva. Si desea agregar etiquetas al alojamiento, siga los pasos a continuación.

Para agregar etiquetas para una conexión

1. Inicie sesión en la consola de . En el panel de navegación, seleccione Configuración.
2. En Settings (Configuración), elija Connections (Conexiones). Elija la pestaña Connections (Conexiones).
3. Elija la conexión que desea editar. Se muestra la página de configuración de conexión.

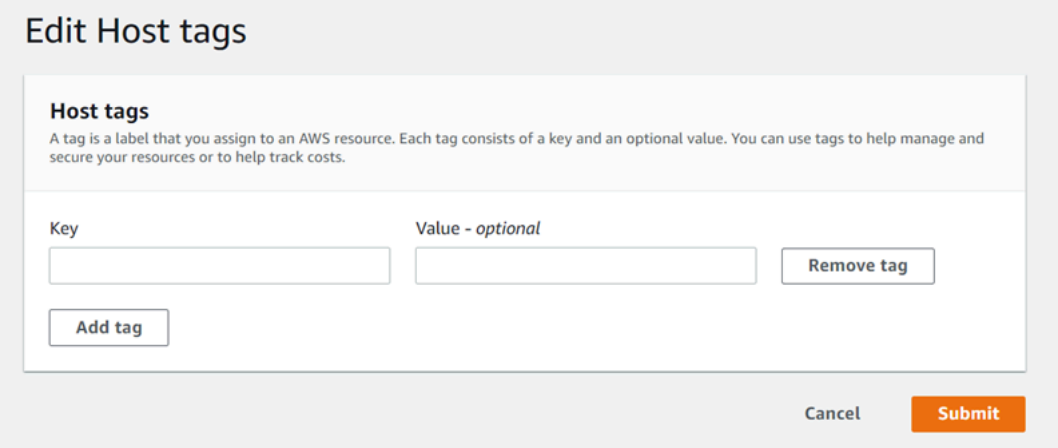
4. En Connection tags (Etiquetas de conexión), elija Edit (Editar). Se muestra la página Edit Connection tags (Editar etiquetas de conexión).
5. En los campos Key (Clave) y Value (Valor), escriba un par de claves para cada conjunto de etiquetas que desea añadir. (El campo Value (Valor) es opcional). Por ejemplo, en Key (Clave), escriba **`Project`**. En Valor, escriba **`ProjectA`**.



6. (Opcional) ElijaAdd tag (Añadir etiqueta) para añadir más filas y escribir más etiquetas.
7. Elija Enviar. Las etiquetas se encuentran en la configuración de la conexión.

Para agregar etiquetas para un alojamiento

1. Inicie sesión en la consola de . En el panel de navegación, seleccione Configuración.
2. En Settings (Configuración), elija Connections (Conexiones). Elija la pestaña Hosts (Alojamientos).
3. Elija el alojamiento que desea editar. Se muestra la página de configuración de alojamiento.
4. En Host tags (Etiquetas del alojamiento), elija Edit (Editar). Se muestra la página Host tags (Etiquetas del alojamiento).
5. En los campos Key (Clave) y Value (Valor), escriba un par de claves para cada conjunto de etiquetas que desea añadir. (El campo Value (Valor) es opcional). Por ejemplo, en Key (Clave), escriba **`Project`**. En Valor, escriba **`ProjectA`**.



6. (Opcional) Elija Add tag (Agregar etiqueta) para agregar más filas e ingresar más etiquetas para un alojamiento.
7. Elija Enviar. Las etiquetas se encuentran en la configuración del alojamiento.

Visualización de etiquetas de un recurso de conexiones (consola)

Puede utilizar la consola para ver las etiquetas de recursos existentes.

Para ver etiquetas de una conexión

1. Inicie sesión en la consola de . En el panel de navegación, seleccione Configuración.
2. En Settings (Configuración), elija Connections (Conexiones). Elija la pestaña Connections (Conexiones).
3. Elija la conexión que desea ver. Se muestra la página de configuración de conexión.
4. En Connection tags (Etiquetas de conexión), puede ver las etiquetas de la conexión en las columnas Key (Clave) y Value (Valor).

Para ver etiquetas de un alojamiento

1. Inicie sesión en la consola de . En el panel de navegación, seleccione Configuración.
2. En Settings (Configuración), elija Connections (Conexiones). Elija la pestaña Hosts (Alojamientos).
3. Elija el alojamiento que desea ver.
4. En Host tags (Etiquetas del alojamiento), puede ver las etiquetas del alojamiento en las columnas Key (Clave) y Value (Valor).

Edición de etiquetas de un recurso de conexiones (consola)

Puede utilizar la consola para editar las etiquetas que se han agregado a los recursos de conexiones.

Para editar etiquetas de una conexión

1. Inicie sesión en la consola de . En el panel de navegación, seleccione Configuración.
2. En Settings (Configuración), elija Connections (Conexiones). Elija la pestaña Connections (Conexiones).
3. Elija la conexión que desea editar. Se muestra la página de configuración de conexión.
4. En Connection tags (Etiquetas de conexión), elija Edit (Editar). Se muestra la página Connection tags (Etiquetas de conexión).
5. En los campos Key (Clave) y Value (Valor), actualice los valores que sean necesarios. Por ejemplo, para la clave **`Project`**, en Value (Valor), cambie **`ProjectA`** a **`ProjectB`**.
6. Elija Enviar.

Para editar etiquetas de un alojamiento

1. Inicie sesión en la consola de . En el panel de navegación, seleccione Configuración.
2. En Settings (Configuración), elija Connections (Conexiones). Elija la pestaña Hosts (Alojamientos).
3. Elija el alojamiento que desea editar. Se muestra la página de configuración de alojamiento.
4. En Host tags (Etiquetas del alojamiento), elija Edit (Editar). Se muestra la página Host tags (Etiquetas del alojamiento).
5. En los campos Key (Clave) y Value (Valor), actualice los valores que sean necesarios. Por ejemplo, para la clave **`Project`**, en Value (Valor), cambie **`ProjectA`** a **`ProjectB`**.
6. Elija Enviar.

Eliminación de etiquetas de un recurso de conexiones (consola)

Puede utilizar la consola para eliminar etiquetas de recursos de conexiones. Cuando se quitan etiquetas del recurso asociado, las etiquetas se eliminan.

Para eliminar etiquetas de una conexión

1. Inicie sesión en la consola de . En el panel de navegación, seleccione Configuración.
2. En Settings (Configuración), elija Connections (Conexiones). Elija la pestaña Connections (Conexiones).
3. Elija la conexión que desea editar. Se muestra la página de configuración de conexión.
4. En Connection tags (Etiquetas de conexión), elija Edit (Editar). Se muestra la página Connection tags (Etiquetas de conexión).
5. Junto a la clave y el valor de cada etiqueta que desea eliminar, elija Remove tag (Quitar etiqueta).
6. Elija Enviar.

Para eliminar etiquetas de un alojamiento

1. Inicie sesión en la consola de . En el panel de navegación, seleccione Configuración.
2. En Settings (Configuración), elija Connections (Conexiones). Elija la pestaña Hosts (Alojamientos).
3. Elija el alojamiento que desea editar. Se muestra la página de configuración de alojamiento.
4. En Host tags (Etiquetas del alojamiento), elija Edit (Editar). Se muestra la página Host tags (Etiquetas del alojamiento).
5. Junto a la clave y el valor de cada etiqueta que desea eliminar, elija Remove tag (Quitar etiqueta).
6. Elija Enviar.

Etiquetado de recursos (CLI)

Puede utilizar la CLI para ver, agregar, actualizar o eliminar etiquetas de un recurso de conexiones.

Temas

- Agregado de etiquetas a un recurso de conexiones (CLI)
- Visualización de etiquetas de un recurso de conexiones (CLI)
- Edición de etiquetas para un recurso de conexiones (CLI)
- Eliminación de etiquetas de un recurso de conexiones (CLI)

Agregado de etiquetas a un recurso de conexiones (CLI)

Puede utilizarlas AWS CLI para etiquetar los recursos de las conexiones.

En el terminal o la línea de comandos, ejecute el comando tag-resource especificando el nombre de recurso de Amazon (ARN) del recurso al que desea agregar etiquetas, y la clave y el valor de la etiqueta que desee agregar. Puede agregar varias etiquetas.

Para agregar etiquetas para una conexión

1. Obtenga el ARN para su recurso. Utilice el comando list-connections que se muestra en Mostrar conexiones para obtener el ARN de la conexión.
2. En un terminal o en la línea de comandos, ejecute el comando tag-resource.

   Por ejemplo, utilice el siguiente comando para etiquetar una conexión con dos etiquetas, una clave de etiqueta denominada Project con el valor de etiqueta de ProjectA y una clave de etiqueta denominada ReadOnlytrue.

   ```
   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
   ```

   Si se ejecuta correctamente, este comando no devuelve nada.

Para agregar etiquetas para un alojamiento

1. Obtenga el ARN para su recurso. Utilice el comando list-hosts que se muestra en Enumeración de alojamientos para obtener el ARN del alojamiento.
2. En un terminal o en la línea de comandos, ejecute el comando tag-resource.

   Por ejemplo, utilice el siguiente comando para etiquetar un anfitrión con dos etiquetas, una clave de etiqueta denominada Project con el valor de etiqueta de ProjectA y una clave de etiqueta denominada IscontainerBasedtrue.

   ```
   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
   ```

Si se ejecuta correctamente, este comando no devuelve nada.

Visualización de etiquetas de un recurso de conexiones (CLI)

Puede utilizar la AWS CLI para ver las AWS etiquetas de un recurso de conexiones. Si no se han añadido etiquetas, la lista obtenida está vacía. Utilice el comando list-tags-for-resource para ver las etiquetas que se han agregado a una conexión o un alojamiento.

Para ver etiquetas de una conexión

1. Obtenga el ARN para su recurso. Utilice el comando list-connections que se muestra en Mostrar conexiones para obtener el ARN de la conexión.
2. En un terminal o en la línea de comandos, ejecute el comando list-tags-for-resource. Por ejemplo, utilice el siguiente comando para ver una lista de claves de etiqueta y valores de etiqueta para una conexión.

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

Este comando devuelve las etiquetas asociadas al recurso. Este ejemplo muestra dos pares clave-valor devueltos para una conexión.

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

Para ver etiquetas de un alojamiento

1. Obtenga el ARN para su recurso. Utilice el comando list-hosts que se muestra en Enumeración de alojamientos para obtener el ARN del alojamiento.
2. En un terminal o en la línea de comandos, ejecute el comando list-tags-for-resource. Por ejemplo, utilice el siguiente comando para ver una lista de claves de etiqueta y valores de etiqueta para un alojamiento.

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

   Este comando devuelve las etiquetas asociadas al recurso. Este ejemplo muestra dos pares clave-valor devueltos para un alojamiento.

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

Edición de etiquetas para un recurso de conexiones (CLI)

Puede utilizarla AWS CLI para editar la etiqueta de un recurso. Puede cambiar el valor de una clave existente o añadir otra clave.

En el terminal o la línea de comandos, ejecute el comando tag-resource especificando el ARN del recurso cuya etiqueta desee actualizar y especifique la clave y el valor de la etiqueta.

Cuando se editan etiquetas, todas las claves de etiquetas no especificadas se conservarán, mientras que todo lo que tenga la misma clave y un valor nuevo se actualizará. Las claves nuevas que se agregan con el comando de edición se agregan como un par clave-valor nuevo.

Para editar etiquetas de una conexión

1. Obtenga el ARN para su recurso. Utilice el comando list-connections que se muestra en Mostrar conexiones para obtener el ARN de la conexión.
2. En un terminal o en la línea de comandos, ejecute el comando tag-resource.

   En este ejemplo, el valor de la clave `Project` cambia a `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
   ```

   Si se ejecuta correctamente, este comando no devuelve nada. Para verificar las etiquetas asociadas a la conexión, ejecute el comando list-tags-for-resource.

Para editar etiquetas de un alojamiento

1. Obtenga el ARN para su recurso. Utilice el comando list-hosts que se muestra en Enumeración de alojamientos para obtener el ARN del alojamiento.
2. En un terminal o en la línea de comandos, ejecute el comando tag-resource.

   En este ejemplo, el valor de la clave `Project` cambia a `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
   ```

   Si se ejecuta correctamente, este comando no devuelve nada. Para verificar las etiquetas asociadas al alojamiento, ejecute el comando list-tags-for-resource.

Eliminación de etiquetas de un recurso de conexiones (CLI)

Siga estos pasos para usar el AWS CLI para eliminar una etiqueta de un recurso. Cuando se quitan etiquetas del recurso asociado, las etiquetas se eliminan.

> **Note**
>
> Si elimina un recurso de conexión, todas las asociaciones de etiquetas se quitarán del recurso eliminado. No es necesario quitar las etiquetas antes de eliminar un recurso de conexión.

En el terminal o la línea de comandos, ejecute el comando untag-resource especificando el ARN del recurso cuyas etiquetas desea quitar y la clave de la etiqueta que desea quitar. Por ejemplo, para eliminar varias etiquetas de una conexión con las teclas de etiquetas *Project* y *ReadOnly*, utilice el siguiente comando.

```
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
```

Si se ejecuta correctamente, este comando no devuelve nada. Para ver las etiquetas asociadas al recurso, ejecute el comando list-tags-for-resource. El resultado indica que se han eliminado todas las etiquetas.

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

Visualización de los detalles de la conexión

Puede utilizar la consola de herramientas para desarrolladores o el comando get-connection en la AWS Command Line Interface (AWS CLI) para ver los detalles de una conexión. Para utilizar el AWS CLI, debe haber instalado ya una versión reciente del AWS CLI o haber actualizado a la versión actual. Para obtener más información, consulte Instalar la AWS CLI en la Guía del usuario de AWS Command Line Interface .

Para ver una conexión (consola)

1. Abra la consola de herramientas para desarrolladores en https://console.aws.amazon.com/codesuite/settings/connections.
2. Elija Settings > Connections (Configuración > Conexiones).
3. Elija el botón situado junto a la conexión que desea ver y, luego, elija View details (Ver detalles).

4. Aparecerá la siguiente información de la conexión:

   - Aparecerá el nombre de la conexión.
   - Se mostrará el tipo de proveedor de la conexión.
   - Aparecerá el estado de la conexión.
   - Aparecerá el ARN de la conexión.
   - Si la conexión se creó para un proveedor instalado, como GitHub Enterprise Server, la información del host asociada a la conexión.
   - Si la conexión se creó para un proveedor instalado, como GitHub Enterprise Server, la información del punto final asociada al host de la conexión.

5. Si la conexión está en estado Pendiente, para completar la conexión, elija Update pending connection (Actualizar conexión pendiente). Para obtener más información, consulte Actualización de una conexión pendiente.

Para ver una conexión (CLI)

- En el terminal o la línea de comandos, ejecute el comando get-connection. Por ejemplo, utilice el siguiente comando para ver los detalles de una conexión con el 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
```

  Si se ejecuta correctamente, el comando devolverá los detalles de las conexiones.

  Ejemplo de salida de una conexión de Bitbucket:

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

```
}
```

Ejemplo de salida para una GitHub conexión:

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

Ejemplo de salida para una conexión de 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"
    }
}
```

Trabajo con alojamientos

Para crear una conexión a un tipo de proveedor instalado, como GitHub Enterprise Server, primero debe crear un alojamiento mediante la AWS Management Console. Un alojamiento es un recurso que se crea para representar la infraestructura donde está instalado el proveedor. Luego, se crea una conexión con ese alojamiento. Para obtener más información, consulte Trabajar con conexiones.

Por ejemplo, se crea un alojamiento para la conexión de modo que la aplicación de terceros para el proveedor se pueda registrar para representar la infraestructura. Se crea un alojamiento para un tipo de proveedor y, luego, todas las conexiones a ese tipo de proveedor utilizan ese alojamiento.

Cuando utiliza la consola para crear una conexión a un tipo de proveedor instalado, como GitHub Enterprise Server, la consola crea un recurso de alojamiento para usted.

Temas

Creación de un alojamiento

Puede utilizar la AWS Management Console o la AWS Command Line Interface (AWS CLI) para crear una conexión a un repositorio de código de terceros instalado en la infraestructura. Por ejemplo, es posible que GitHub Enterprise Server se esté ejecutando como una máquina virtual en una instancia de Amazon EC2. Antes de crear una conexión a GitHub Enterprise Server, cree un alojamiento para utilizar con la conexión.

Para obtener información general sobre el flujo de trabajo de creación de hosts para proveedores instalados, consulte Flujo de trabajo para crear o actualizar un host.

Antes de empezar

- (Opcional) Si desea crear su host con una VPC, debe haber creado ya una red o una nube virtual privada (VPC).
- Debe haber creado la instancia y, si planea conectarse a su VPC, debe haber lanzado su host en la VPC.

> **Note**
>
> Cada VPC solo se puede asociar a un host a la vez.

Si lo desea, puede configurar su host con una VPC. Para obtener más información acerca de la configuración de la VPC y la red para su recurso de host, consulte los requisitos previos de la VPC en (Opcional) Requisitos previos: configuración de red o Amazon VPC para la conexión y Solución de problemas de la configuración de una VPC para el alojamiento.

Si desea utilizar la consola para crear un host y una conexión a GitHub Enterprise Server, consulte Cree su conexión a GitHub Enterprise Server (consola). La consola crea un alojamiento para usted.

Si desea utilizar la consola para crear un host y una conexión a GitLab autoadministrado, consulte Cree una conexión a una red GitLab autogestionada. La consola crea un alojamiento para usted.

(Opcional) Requisitos previos: configuración de red o Amazon VPC para la conexión

Si su infraestructura está configurada con una conexión de red, puede omitir esta sección.

Si solo se puede acceder a su host en una VPC, siga estos requisitos de la VPC antes de continuar.

Requisitos de la VPC

Si lo desea, puede elegir crear su host con una VPC. A continuación se encuentran los requisitos generales de la VPC, los cuales dependen de la VPC que haya configurado para la instalación.

- Puede configurar una VPC pública con subredes públicas y privadas. Si no tiene subredes ni bloques de CIDR preferidos, puede utilizar la VPC predeterminada para su cuenta de Cuenta de AWS.
- Si tiene una VPC privada configurada y ha configurado la instancia de GitHub Enterprise Server para realizar la validación de TLS mediante una entidad de certificación no pública, debe proporcionar el certificado TLS para el recurso de alojamiento.
- Cuando AWS CodeStar Connections crea el alojamiento, se crea el punto de conexión de VPC (PrivateLink) para webhooks. Para obtener más información, consulte AWS CodeStar Connections y puntos de conexión de VPC de la interfaz (AWS PrivateLink).
- Configuración del grupo de seguridad:
  - Los grupos de seguridad utilizados durante la creación del alojamiento necesitan reglas de entrada y de salida que permitan que la interfaz de red se conecte a la instancia de GitHub Enterprise Server.
  - Los grupos de seguridad adjuntos a la instancia de GitHub Enterprise Server (que no forman parte de la configuración del alojamiento) necesitan acceso de entrada y de salida de las interfaces de red creadas por las conexiones.

- Las subredes de la VPC deben residir en diferentes zonas de disponibilidad de su región. Las zonas de disponibilidad son ubicaciones diferentes que están aisladas en caso de que se produzca un error en otras zonas de disponibilidad. Cada subred debe residir enteramente en una zona de disponibilidad y no puede abarcar otras zonas.

Para obtener más información acerca de cómo trabajar con las VPC y las subredes, consulte Tamaño de la subred y la VPC para una dirección IPv4 en la Guía del usuario de Amazon VPC.

Información de la VPC que se proporciona para la configuración del alojamiento

Cuando crea el recurso de alojamiento para las conexiones en el siguiente paso, debe proporcionar lo siguiente:

- ID de la VPC: se trata del ID de la VPC del servidor donde está instalada la instancia de GitHub Enterprise Server o de una VPC con acceso a la instancia instalada de GitHub Enterprise Server a través de VPN o Direct Connect.
- el ID o los ID de la subred: se trata del ID de la subred del servidor donde está instalada la instancia de GitHub Enterprise Server o de una subred con acceso a la instancia instalada de GitHub Enterprise Server a través de VPN o Direct Connect.
- grupo o grupos de seguridad: se trata del grupo de seguridad del servidor donde está instalada la instancia de GitHub Enterprise Server o de un grupo de seguridad con acceso a la instancia instalada de GitHub Enterprise Server a través de VPN o Direct Connect.
- punto de enlace: tenga listo el punto de enlace del servidor y continúe con el siguiente paso.

Para obtener más información, incluida la solución de problemas de conexiones de alojamiento o de la VPC, consulte Solución de problemas de la configuración de una VPC para el alojamiento.

Requisitos del permiso

Como parte del proceso de creación del host, AWS CodeStar Connections crea recursos de red en su nombre para facilitar la conectividad de la VPC. Esto incluye una interfaz de red para AWS Codestar Connections para consultar los datos en el host y un punto de conexión de VPC o PrivateLink para que el host envíe datos de eventos a AWS CodeStar Connections a través de webhooks. Para poder crear estos recursos de red, asegúrese de que el rol que ha utilizado para crear el host tenga los siguientes permisos:

```
ec2:CreateNetworkInterface
ec2:CreateTags
```

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

Para obtener más información acerca de la solución de problemas de permisos o conexiones de alojamiento en una VPC, consulte Solución de problemas de la configuración de una VPC para el alojamiento.

Para obtener más información acerca del punto de enlace de la VPC de webhook, consulte AWS CodeStar Connections y puntos de conexión de VPC de la interfaz (AWS PrivateLink).

Temas

- Creación de un alojamiento para una conexión (consola)
- Creación de un host para una conexión (CLI)

Creación de un alojamiento para una conexión (consola)

Para conexiones para instalaciones, como con GitHub Enterprise Server o con GitLab autoadministrado, utilice un host para representar el punto de conexión de la infraestructura donde está instalado el proveedor de terceros.

Para obtener información acerca de las consideraciones de la configuración de un alojamiento en una VPC, consulte Cree una conexión a una red GitLab autogestionada.

Si desea utilizar la consola para crear un host y una conexión a GitHub Enterprise Server, consulte Cree su conexión a GitHub Enterprise Server (consola). La consola crea un alojamiento para usted.

Si desea utilizar la consola para crear un host y una conexión a GitLab autoadministrado, consulte Cree una conexión a una red GitLab autogestionada. La consola crea un alojamiento para usted.

> **Note**
>
> Solo cree un host una vez por cuenta de GitHub Enterprise Server o GitLab autoadministrado. Todas las conexiones a una cuenta específica de GitHub Enterprise Server o GitLab autoadministrado utilizarán el mismo host.

Creación de un host para una conexión (CLI)

Puede utilizar la AWS Command Line Interface (AWS CLI) para crear un alojamiento para las conexiones instaladas.

> **Note**
>
> Solo cree un alojamiento una vez por cuenta de GitHub Enterprise Server. Todas las conexiones a una cuenta específica de GitHub Enterprise Server utilizarán el mismo alojamiento.

Se utiliza un alojamiento para representar el punto de enlace de la infraestructura donde está instalado el proveedor de terceros. Para crear un alojamiento con la CLI, utilice el comando create-host. Una vez que termine de crear el alojamiento, este estará en estado Pendiente. Luego, configure el alojamiento para que su estado cambie a Disponible. Una vez que el alojamiento esté disponible, complete los pasos para crear una conexión.

> **Important**
>
> Un alojamiento creado mediante la AWS CLI está en estado `Pending` de forma predeterminada. Después de crear un alojamiento con la CLI, utilice la consola para configurar el alojamiento de manera que su estado cambie a `Available`.

Si desea utilizar la consola para crear un host y una conexión a GitHub Enterprise Server, consulte Cree su conexión a GitHub Enterprise Server (consola). La consola crea un alojamiento para usted.

Si desea utilizar la consola para crear un host y una conexión a GitLab autoadministrado, consulte Cree una conexión a una red GitLab autogestionada. La consola crea un alojamiento para usted.

Configuración de un alojamiento pendiente

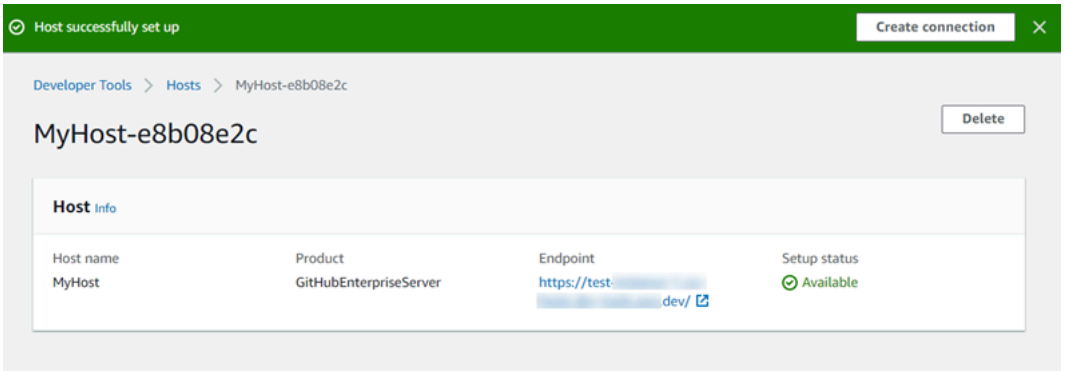
Un alojamiento creado a través de la AWS Command Line Interface (AWS CLI) o el SDK está en estado `Pending` de forma predeterminada. Después de crear una conexión con la consola, la AWS CLI o el SDK, utilice la consola para configurar el alojamiento de manera que su estado cambie a `Available`.

Debe haber creado un alojamiento. Para obtener más información, consulte Create a host (Crear un alojamiento).

Para configurar un alojamiento pendiente

Una vez creado el alojamiento, se encuentra en un estado Pendiente. Para que el estado del alojamiento pase de Pendiente a Disponible, complete estos pasos. Este proceso lleva a cabo un protocolo de enlace con el proveedor de terceros para registrar la aplicación de conexión de AWS en el host.

1. Una vez que el host alcance el estado Pendiente en la consola de herramientas para desarrolladores de AWS, elija Set up host (Configurar host).
2. Si estás creando un host para GitLab autoadministrado, aparecerá una página Configuración. En Proporcionar token de acceso personal, proporcione a su PAT de GitLab únicamente el siguiente permiso limitado: api.
3. En la página de inicio de sesión del proveedor de terceros instalado, como la página de inicio de GitHub Enterprise Server, inicie sesión con las credenciales de su cuenta si se le solicita.
4. En la página de instalación de la aplicación, en GitHub App name (Nombre de la aplicación GitHub), ingrese un nombre para la aplicación que desea instalar para el alojamiento. Elija Create GitHub App (Crear aplicación GitHub).
5. Una vez que el alojamiento se registró correctamente, aparece la página de detalles del alojamiento y muestra que el estado del alojamiento es Disponible.



6. Puede continuar con la creación de la conexión una vez que el alojamiento esté disponible. En el banner de realización correcta, elija Create connection (Crear conexión). Complete los pasos en Creación de una conexión.

Enumeración de alojamientos

Puede utilizar la consola de herramientas para desarrolladores o el comando list-connections en la AWS Command Line Interface (AWS CLI) para ver una lista de las conexiones de la cuenta.

Enumeración de alojamientos (consola)

Para enumerar alojamientos

1. Abra la consola de herramientas para desarrolladores en https://console.aws.amazon.com/codesuite/settings/connections.
2. Elija la pestaña Hosts (Alojamientos). Consulte el nombre, el estado y el ARN de los alojamientos.

Enumeración de alojamientos (CLI)

Puede utilizar la AWS CLI para enumerar los alojamientos para las conexiones de proveedores de terceros instalados.

Para ello, utilice el comando list-hosts.

Para enumerar alojamientos

- Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows) y utilice la AWS CLI para ejecutar el comando list-hosts.

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

  Este comando devuelve la siguiente salida.

  ```
  {
      "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"
          }
      ]
  }
  ```

Edición de un alojamiento

Puede editar la configuración de un alojamiento en estado `Pending`. Puede editar el nombre del alojamiento, la dirección URL o la configuración de la VPC.

No puede utilizar la misma URL para más de un alojamiento.

> **Note**
>
> Para obtener información acerca de las consideraciones de la configuración de un alojamiento en una VPC, consulte (Opcional) Requisitos previos: configuración de red o Amazon VPC para la conexión.

Para editar un alojamiento

1. Abra la consola de herramientas para desarrolladores en https://console.aws.amazon.com/codesuite/settings/connections.
2. Elija Settings > Connections (Configuración > Conexiones).
3. Elija la pestaña Hosts (Alojamientos).

   Se muestran los alojamientos asociados a su cuenta de AWS y creados en la región de AWS seleccionada.
4. Para editar el nombre del alojamiento, ingrese un valor nuevo en Name (Nombre).
5. Para editar el punto de enlace del alojamiento, ingrese un valor nuevo en URL.
6. Para editar la configuración de la VPC del alojamiento, ingrese valores nuevos en VPC ID (ID de la VPC).
7. Elija Edit host (Editar alojamiento).
8. Se muestra la configuración actualizada. Elija Set up Pending host (Configurar alojamiento pendiente).

Eliminación de un alojamiento

Puede utilizar la consola de herramientas para desarrolladores o el comando delete-host en la AWS Command Line Interface (AWS CLI) para eliminar un alojamiento.

Temas

Eliminación de un alojamiento (consola)

Para eliminar un alojamiento

1. Abra la consola de herramientas para desarrolladores en https://console.aws.amazon.com/codesuite/settings/connections.
2. Elija la pestaña Hosts (Alojamientos). En Name (Nombre), elija el nombre del alojamiento que desea eliminar.
3. Elija Eliminar.
4. Escriba **`delete`** en el campo para confirmar y elija Eliminar.

> **Important**
>
> Esta acción no se puede deshacer.

Eliminación de un alojamiento (CLI)

Puede utilizar la AWS Command Line Interface (AWS CLI) para eliminar un alojamiento.

Para ello, utilice el comando delete-host.

> **Important**
>
> Para poder eliminar un alojamiento, debe eliminar todas las conexiones asociadas al alojamiento.
> Después de ejecutar el comando, se elimina el alojamiento. No se muestra ningún cuadro de diálogo de confirmación.

Para eliminar un alojamiento

- Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice la AWS CLI para ejecutar el comando delete-host y especifique el nombre de recurso de Amazon (ARN) del alojamiento que desea eliminar.

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

Este comando no devuelve nada.

Visualización de los detalles del alojamiento

Puede utilizar la consola de herramientas para desarrolladores o el comando get-host en la AWS Command Line Interface (AWS CLI) para ver los detalles de un alojamiento.

Para ver los detalles del alojamiento (consola)

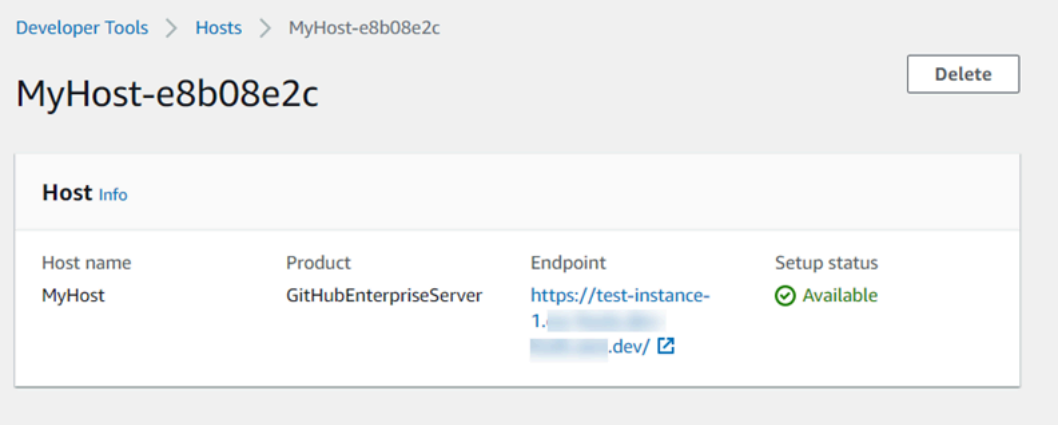
1. Inicie sesión en la AWS Management Console y abra la consola de herramientas para desarrolladores en https://console.aws.amazon.com/codesuite/settings/connections.
2. Elija Settings > Connections (Configuración > Conexiones) y, luego, elija la pestaña Hosts (Alojamientos).
3. Elija el botón situado junto al alojamiento que desea ver y, luego, elija View details (Ver detalles).
4. Aparecerá la siguiente información del alojamiento:

   - Se mostrará el nombre del alojamiento.
   - Se mostrará el tipo de proveedor de la conexión.
   - Se mostrará el punto de enlace de la infraestructura donde está instalado el proveedor.
   - Se mostrará el estado de configuración del alojamiento. Un alojamiento listo para una conexión está en estado Disponible. Si el alojamiento se creó y la configuración no se completó, es posible que el alojamiento tenga un estado diferente.

     Los siguientes estados están disponibles:

     - PENDING (PENDIENTE): el alojamiento completó la creación y está listo para iniciar la configuración mediante el registro de la aplicación del proveedor en el alojamiento.
     - AVAILABLE (DISPONIBLE): el alojamiento completó la creación y la configuración, y está disponible para utilizarse con conexiones.
     - ERROR: se produjo un error durante la creación o el registro del alojamiento.
     - VPC_CONFIG_VPC_INITIALIZING: se está creando la configuración de la VPC para el alojamiento.

- VPC_CONFIG_VPC_FAILED_INITIALIZATION: la configuración de la VPC para el alojamiento encontró un error y falló.
- VPC_CONFIG_VPC_AVAILABLE: la configuración de la VPC para el alojamiento completó la configuración y está disponible.
- VPC_CONFIG_VPC_DELETING: se está eliminando la configuración de la VPC para el alojamiento.



5. Para eliminar el alojamiento, elija Delete (Eliminar).
6. Si el alojamiento está en estado Pendiente, elija Set up host (Configurar alojamiento) para completar la configuración. Para obtener más información, consulte Configuración de un alojamiento pendiente.

Para ver los detalles del alojamiento (CLI)

- Abra un terminal (Linux, macOS o Unix) o el símbolo del sistema (Windows) y utilice la AWS CLI para ejecutar el comando get-host, mediante la especificación del nombre de recurso de Amazon (ARN) del alojamiento del que desea ver los detalles.

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

Este comando devuelve la siguiente salida.

```
{
    "Name": "MyHost",
    "Status": "AVAILABLE",
    "ProviderType": "GitHubEnterpriseServer",
```

```
    "ProviderEndpoint": "https://test-instance-1.dev/"
}
```

Trabajar con configuraciones de sincronización para repositorios enlazados

En AWS CodeStar Connections, utilizas una conexión para asociar AWS recursos a un repositorio de terceros GitHub, como Bitbucket Cloud, GitHub Enterprise Server y. GitLab Con el tipo de `CFN_STACK_SYNC` sincronización, puedes crear una configuración de sincronización que AWS permita sincronizar el contenido de un repositorio de Git para actualizar un AWS recurso específico. AWS CloudFormation se integra con las conexiones para que puedas usar Git sync para gestionar tus archivos de plantillas y parámetros en un repositorio vinculado con el que te sincronices.

Tras crear una conexión, puede utilizar la CLI de conexiones o la AWS CloudFormation consola para crear la configuración de enlace y sincronización del repositorio.

- Enlace de repositorio: un enlace de repositorio crea una asociación entre la conexión y un repositorio Git externo. El enlace de repositorio permite que la sincronización de Git monitoree y sincronice los cambios en los archivos de un repositorio Git específico.
- Configuración de sincronización: usa la configuración de sincronización para sincronizar el contenido de un repositorio de Git para actualizar un AWS recurso específico.

Para obtener más información, consulta la referencia de la API de AWS CodeStar conexiones.

Para ver un tutorial que te explica cómo crear una configuración de sincronización para una AWS CloudFormation pila mediante la AWS CloudFormation consola, consulta Cómo trabajar con AWS CloudFormation Git sync en la Guía del CloudFormation usuario.

Temas

- Trabajo con enlaces de repositorios
- Trabajo con configuraciones de sincronización

Trabajo con enlaces de repositorios

Un enlace de repositorio crea una asociación entre la conexión y un repositorio Git externo. El enlace al repositorio permite que Git sync supervise y sincronice los cambios en los archivos de un repositorio de Git específico con una AWS CloudFormation pila.

Para obtener más información sobre los enlaces a los repositorios, consulta la referencia de la API AWS CodeStar Connections.

Temas

- Crear un enlace de repositorio
- Actualizar un enlace de repositorio
- Mostrar los enlaces de repositorio
- Eliminación de un enlace a un repositorio
- Consultar los detalles de enlace de repositorio

Crear un enlace de repositorio

Puedes usar el create-repository-link comando de AWS Command Line Interface (AWS CLI) para crear un enlace entre tu conexión y el repositorio externo con el que deseas realizar la sincronización.

Para poder crear un enlace a un repositorio, debes haber creado ya tu repositorio externo con un proveedor externo, por ejemplo GitHub.

Para crear un enlace de repositorio

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice el AWS CLI para ejecutar el create-repository-link comando. Especifique el ARN de la conexión asociada, el ID de propietario y el nombre del repositorio.

```
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 devuelve la siguiente salida.

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

Actualizar un enlace de repositorio

Puede usar el update-repository-link comando de AWS Command Line Interface (AWS CLI) para actualizar un enlace de repositorio específico.

Puede actualizar la siguiente información para el enlace del repositorio:

- `--connection-arn`
- `--owner-id`
- `--repository-name`

Es posible que actualice el enlace de un repositorio cuando desee cambiar la conexión asociada al repositorio. Para usar una conexión diferente, debe especificar el ARN de la conexión. Para ver los pasos para consultar el ARN de la conexión, consulte Ver detalles de conexión.

Para actualizar un enlace de repositorio

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice el AWS CLI para ejecutar el update-repository-link comando, especificando el valor que se va a actualizar para el enlace al repositorio. Por ejemplo, el siguiente comando actualiza la conexión asociada al ID del enlace del repositorio. Especifica el nuevo ARN de la conexión con el parámetro `--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 devuelve la siguiente salida.

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

Mostrar los enlaces de repositorio

Puedes usar el list-repository-links comando de AWS Command Line Interface (AWS CLI) para enumerar los enlaces al repositorio de tu cuenta.

Para mostrar los enlaces de repositorio

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Use el AWS CLI para ejecutar el list-repository-links comando.

```
aws codestar-connections list-repository-links
```

2. Este comando devuelve la siguiente salida.

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

Eliminación de un enlace a un repositorio

Puede usar el delete-repository-link comando de AWS Command Line Interface (AWS CLI) para eliminar un enlace a un repositorio.

Antes de poder eliminar un enlace de repositorio, debe eliminar todas las configuraciones de sincronización asociadas al enlace de repositorio.

> **Important**
>
> Después de ejecutar el comando, se elimina el enlace de repositorio. No se muestra ningún cuadro de diálogo de confirmación. Puede crear un enlace de repositorio nuevo, pero el nombre de recurso de Amazon (ARN) no se reutiliza.

Para eliminar un enlace de repositorio

- Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice el AWS CLI para ejecutar el delete-repository-link comando, especificando el ID del enlace al repositorio que se va a eliminar.

  ```
  aws codestar-connections delete-repository-link --repository-link-id
   6053346f-8a33-4edb-9397-10394b695173
  ```

  Este comando no devuelve nada.

Consultar los detalles de enlace de repositorio

Puede usar el get-repository-link comando incluido en AWS Command Line Interface (AWS CLI) para ver los detalles sobre el enlace de un repositorio.

Para consultar los detalles de enlace de repositorio

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Use el AWS CLI para ejecutar el get-repository-link comando, especificando el ID del enlace al repositorio.

   ```
   aws codestar-connections get-repository-link --repository-link-id
    6053346f-8a33-4edb-9397-10394b695173
   ```

2. Este comando devuelve la siguiente salida.

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

Trabajo con configuraciones de sincronización

Una configuración de sincronización crea una asociación entre un repositorio específico y una conexión. Use la configuración de sincronización para sincronizar el contenido de un repositorio Git y actualizar un recurso de AWS específico.

Para obtener más información sobre las conexiones, consulta la referencia de la API de AWS CodeStar conexiones.

Temas

- Crear una configuración de sincronización
- Actualizar una configuración de sincronización
- Mostrar configuraciones de sincronización
- Eliminar una configuración de sincronización
- Consultar los detalles de la configuración de sincronización

Crear una configuración de sincronización

Puedes usar el create-repository-link comando de AWS Command Line Interface (AWS CLI) para crear un enlace entre tu conexión y el repositorio externo con el que deseas sincronizarla.

Antes de poder crear una configuración de sincronización, debe haber creado ya un enlace de repositorio entre la conexión y el repositorio de terceros.

Para crear una configuración de sincronización

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Usa el AWS CLI para ejecutar el create-repository-link comando. Especifique el ARN de la conexión asociada, el ID de propietario y el nombre del repositorio. El siguiente comando crea una configuración de sincronización con un tipo de sincronización para un recurso en AWS CloudFormation. También especifica la ramificación del repositorio y el archivo de configuración del repositorio. En este ejemplo, el recurso es una pilla que se llama **`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 devuelve la siguiente salida.

```
{
    "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"
    }
```

Actualizar una configuración de sincronización

Puede usar el comando update-sync-configuration en AWS Command Line Interface (AWS CLI) para actualizar una configuración de sincronización específica.

Puede actualizar la siguiente información para la configuración de sincronización:

- `--branch`
- `--config-file`
- `--repository-link-id`
- `--resource-name`

- `--role-arn`

Para actualizar una configuración de sincronización

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice el AWS CLI para ejecutar el update-sync-configuration comando, especificando el valor que desea actualizar, junto con el nombre del recurso y el tipo de sincronización. Por ejemplo, el siguiente comando actualiza el nombre de la ramificación asociada a la configuración de sincronización con el parámetro `--branch`.

```
aws codestar-connections update-sync-configuration --sync-type CFN_STACK_SYNC --
resource-name mystack --branch feature-branch
```

2. Este comando devuelve la siguiente salida.

```
{
    "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"
    }
```

Mostrar configuraciones de sincronización

Puede usar el comando list-sync-configurations en AWS Command Line Interface (AWS CLI) para mostrar los enlaces de repositorio de la cuenta.

Para mostrar los enlaces de repositorio

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Usa el comando AWS CLI para ejecutar el list-sync-configurations comando, especificando el tipo de sincronización y el ID del enlace al repositorio.

```
aws codestar-connections list-sync-configurations --repository-link-id
 6053346f-8a33-4edb-9397-10394b695173  --sync-type CFN_STACK_SYNC
```

2. Este comando devuelve la siguiente salida.

```
{
    "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"
        }
    ]
}
```

Eliminar una configuración de sincronización

Puede usar el comando delete-sync-configuration en AWS Command Line Interface (AWS CLI) para eliminar una configuración de sincronización.

> **Important**
>
> Después de ejecutar el comando, se elimina la configuración de sincronización. No se muestra ningún cuadro de diálogo de confirmación. Puede crear una nueva configuración de sincronización, pero el nombre de recurso de Amazon (ARN) no se reutiliza.

Para eliminar una configuración de sincronización

- Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Utilice el AWS CLI para ejecutar el delete-sync-configuration comando, especificando el tipo de sincronización y el nombre del recurso para la configuración de sincronización que desee eliminar.

```
aws codestar-connections delete-sync-configuration --sync-type CFN_STACK_SYNC --
resource-name mystack
```

Este comando no devuelve nada.

Consultar los detalles de la configuración de sincronización

Puedes usar el get-sync-configuration comando incluido en AWS Command Line Interface (AWS CLI) para ver los detalles de una configuración de sincronización.

Para consultar los detalles de una configuración de sincronización

1. Abra un terminal (Linux, macOS o Unix) o un símbolo del sistema (Windows). Use el AWS CLI para ejecutar el get-sync-configuration comando, especificando el ID del enlace al repositorio.

```
aws codestar-connections get-sync-configuration --sync-type CFN_STACK_SYNC --
resource-name mystack
```

2. Este comando devuelve la siguiente salida.

```
{
    "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 llamadas a la API de AWS CodeConnections con AWS CloudTrail

AWS CodeConnections se integra con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS. CloudTrail captura todas las

llamadas a la API para las notificaciones en forma de eventos. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de herramientas para desarrolladores y las llamadas de código a las operaciones de la API de AWS CodeConnections.

Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon Simple Storage Service (Amazon S3), incluidos los eventos para notificaciones. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Event history (Historial de eventos). Mediante la información que CloudTrail recopila, se puede determinar la solicitud que se envió a AWS CodeConnections, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y otros detalles adicionales.

Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Información de AWS CodeConnections en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad en AWS CodeConnections, esa actividad se registra en un evento de CloudTrail junto con otros eventos de servicio de AWS en Event history (Historial de eventos). Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail en la Guía del usuario de AWS CloudTrail.

Para mantener un registro continuo de eventos en la cuenta de AWS, incluidos los eventos de AWS CodeConnections, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail.

Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS CloudTrail:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recepción de archivos de registro de CloudTrail de varias regiones
- Recepción de archivos de registro de CloudTrail de varias cuentas

Todas las acciones de AWS CodeConnections las registra CloudTrail y se documentan en la Referencia de la API de AWS CodeConnections. Por ejemplo, las llamadas a las acciones `CreateConnection`, `DeleteConnection` y `GetConnection` generan entradas en los archivos de registros de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz u otras credenciales de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el elemento userIdentity de CloudTrail.

Descripción de las entradas de los archivos de registro de

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros a un bucket de Amazon S3 que usted especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la acción `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"
}
```

AWS CodeStar Connections y puntos de conexión de VPC de la interfaz (AWS PrivateLink)

Puede establecer una conexión privada entre la VPC y AWS CodeStar Connections mediante la creación de un punto de conexión de VPC de interfaz. Los puntos de conexión de interfaz cuentan con tecnología de AWS PrivateLink que le permite acceder de forma privada a las API de AWS CodeStar Connections sin una puerta de enlace de Internet, un dispositivo NAT, una conexión de VPN o una conexión de AWS Direct Connect. Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con las API de AWS CodeStar Connections, ya que el tráfico entre su VPC y AWS CodeStar Connections no sale de la red de Amazon.

Cada punto de enlace de la interfaz está representado por una o más interfaces de red elásticas en las subredes.

Para obtener más información, consulte Puntos de enlace de la VPC de tipo interfaz (AWS PrivateLink) en la Guía del usuario de Amazon VPC.

Consideraciones para los puntos de conexión de VPC de AWS CodeStar Connections

Antes de configurar un punto de conexión de VPC de interfaz para AWS CodeStar Connections, asegúrese de consultar Puntos de conexión de interfaz en la Guía del usuario de Amazon VPC.

AWS CodeStar Connections admite la realización de llamadas a todas las acciones de la API desde su VPC.

Los puntos de conexión de VPC son compatibles con todas las regiones de AWS CodeStar Connections.

Conceptos de puntos de enlace de la VPC

A continuación se enumeran los conceptos clave de los puntos de enlace VPC:

Punto de conexión VPC

Se trata del punto de entrada de la VPC que permite conectarse de forma privada a un servicio. Los siguientes son los diferentes tipos de puntos de conexión de la VPC. Cree el tipo de punto de enlace de la VPC necesario en función del servicio compatible.

- Puntos de conexión de VPC para acciones de AWS CodeStar Connections
- Puntos de conexión de VPC para webhooks de AWS CodeStar Connections

AWS PrivateLink

Una tecnología que proporciona conectividad privada entre las VPC y los servicios.

Puntos de conexión de VPC para acciones de AWS CodeStar Connections

Puede administrar los puntos de conexión de VPC para el servicio de AWS CodeStar Connections.

Creación de puntos de conexión de VPC de interfaz para acciones de AWS CodeStar Connections

Puede crear un punto de conexión de VPC para el servicio de AWS CodeStar Connections mediante la consola de Amazon VPC o la AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Para comenzar a utilizar conexiones con su VPC, cree un punto de conexión de VPC de interfaz para AWS CodeStar Connections. Cuando cree un punto de conexión de VPC para AWS CodeStar Connections, elija AWS Services (Servicios de AWS) y en Service Name (Nombre del servicio), elija:

- com.amazonaws.***región***.codestar-connections.api: esta opción crea un punto de conexión de VPC para las operaciones de la API de AWS CodeStar Connections. Por ejemplo, elija esta opción si los usuarios utilizan la AWS CLI, la API de AWS CodeStar Connections o los AWS SDK

para interactuar con AWS CodeStar Connections para operaciones como `CreateConnection`, `ListConnections` y `CreateHost`.

En la opción Enable DNS name (Habilitar nombre de DNS), si selecciona DNS privado para el punto de conexión, puede realizar solicitudes de API a AWS CodeStar Connections mediante el nombre de DNS predeterminado para la región, como por ejemplo `codestar-connections.us-east-1.amazonaws.com`.

> **Important**
>
> El DNS privado está habilitado de forma predeterminada para los puntos de conexión creados por los servicios de AWS y los servicios de socios de AWS Marketplace.

Para obtener más información, consulte Acceso a un servicio a través de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Creación de una política de punto de conexión de VPC para acciones de AWS CodeStar Connections

Puede adjuntar una política de punto de conexión al punto de conexión de VPC que controla el acceso a AWS CodeStar Connections. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte Control del acceso a los servicios con puntos de enlace de la VPC en la guía del usuario de Amazon VPC.

> **Note**
>
> El punto de enlace com.amazonaws.*region*.codestar-connections.webhooks no es compatible con políticas.

Ejemplo: política de punto de conexión de VPC para acciones de AWS CodeStar Connections

A continuación, se muestra un ejemplo de una política de punto de conexión para AWS CodeStar Connections. Cuando se adjunta a un punto de conexión, esta política concede acceso a las acciones de AWS CodeStar Connections enumeradas para todas las entidades principales en todos los recursos.

```
{
  "Statement": [
    {
      "Sid": "GetConnectionOnly",
      "Principal": "*",
      "Action": [
        "codestar-connections:GetConnection"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Puntos de conexión de VPC para webhooks de AWS CodeStar Connections

AWS CodeStar Connections crea puntos de conexión de webhook cuando usted crea o elimina un host con configuración de VPC. El nombre del punto de enlace es com.amazonaws.***region***.codestar-connections.webhooks.

Con el punto de conexión de VPC para webhooks de GitHub, los hosts pueden enviar datos de eventos a través de webhooks a los servicios de AWS integrados mediante la red de Amazon.

> **Important**
>
> Cuando configura el host para GitHub Enterprise Server, AWS CodeStar Connections crea un punto de conexión de VPC para datos de eventos de webhooks. Si creó el alojamiento antes del 24 de noviembre de 2020 y desea utilizar los puntos de enlace de webhook de la VPC PrivateLink, primero debe eliminar su alojamiento y luego crear un alojamiento nuevo.

AWS CodeStar Connections administra el ciclo de vida de estos puntos de conexión. Para eliminar el punto de enlace, debe eliminar el recurso de alojamiento correspondiente.

Cómo se utilizan los puntos de conexión de webhooks para los hosts de AWS CodeStar Connections

El punto de conexión de webhook es donde se envían los webhooks de repositorios de terceros para el procesamiento de AWS CodeStar Connections. Un webhook describe la acción de un cliente. Cuando ejecuta `git push`, el punto de enlace de webhook recibe un webhook del proveedor que detalla la inserción. Por ejemplo, AWS CodeStar Connections puede notificar a CodePipeline para que inicie la canalización.

Para proveedores de nube, como Bitbucket, o para hosts de GitHub Enterprise Server que no utilizan una VPC, el punto de conexión de VPC de webhook no se aplica porque los proveedores envían webhooks a AWS CodeStar Connections donde no se utiliza la red de Amazon.

Solución de problemas de conexiones

La siguiente información puede ayudarlo a solucionar problemas comunes con las conexiones a recursos de AWS CodeBuild, AWS CodeDeploy y AWS CodePipeline.

Temas

- Me gustaría aumentar los límites de conexiones

No puedo crear conexiones

Es posible que no tenga permisos para crear una conexión. Para obtener más información, consulte Permisos y ejemplos de AWS CodeConnections.

Aparece un error de permisos cuando intento crear o completar una conexión.

Es posible que se devuelva el siguiente mensaje de error cuando intenta crear o ver una conexión en la consola de CodePipeline.

User: *username* is not authorized to perform: *permission* on resource: *connection-ARN* (Usuario: username no tiene autorización para realizar: permission en el recurso: connection-ARN)

Si aparece este mensaje, asegúrese de tener los permisos necesarios.

Los permisos para crear y ver conexiones en la AWS Command Line Interface (AWS CLI) o la AWS Management Console son solo una parte de los permisos que necesita para crear y completar conexiones en la consola. Los permisos necesarios para simplemente ver, editar o crear una conexión y, luego, completar la conexión pendiente deben aplicarse a los usuarios que solo necesitan realizar determinadas tareas. Para obtener más información, consulte Permisos y ejemplos de AWS CodeConnections.

Cuando intento utilizar una conexión aparece un error de permisos

Es posible que se devuelvan uno o ambos de los siguientes mensajes de error si intenta utilizar una conexión en la consola de CodePipeline, incluso si tiene los permisos para enumerar, obtener y crear permisos.

You have failed to authenticate your account (No se ha podido autenticar la cuenta).

User: *username* is not authorized to perform: codestar-connections:UseConnection on resource: *connection-ARN* (Usuario: username no está autorizado para realizar: codestar-connections:UseConnection en el recurso: connection-ARN)

Si esto sucede, asegúrese de tener los permisos necesarios.

Asegúrese de tener los permisos para utilizar una conexión, incluida la lista de los repositorios disponibles en la ubicación del proveedor. Para obtener más información, consulte Permisos y ejemplos de AWS CodeConnections.

Connection is not in available state or is no longer pending (La conexión no está disponible o ya no está pendiente)

Si la consola muestra un mensaje que indica que una conexión no está en estado disponible, elija Complete connection (Completar conexión).

Si elige completar la conexión y aparece un mensaje que indica que la conexión no está en estado pendiente, puede cancelar la solicitud, ya que la conexión ya está disponible.

Añadir permisos de GitClone para conexiones

Cuando se utiliza una conexión de AWS CodeStar en una acción de código fuente y una acción de CodeBuild, hay dos maneras en que el artefacto de entrada se puede pasar a la compilación:

- La forma predeterminada: la acción de origen produce un archivo zip que contiene el código que CodeBuild descarga.
- Clonación de Git: el código fuente se puede descargar directamente en el entorno de compilación.

  El modo de clonación de Git le permite interactuar con el código fuente como un repositorio de Git de trabajo. Para utilizar este modo, debe conceder permisos al entorno de CodeBuild para utilizar la conexión.

Para agregar permisos a la política de la función de servicio de CodeBuild, cree una política administrada por el cliente y adjúntela a la función de servicio de CodeBuild. Los siguientes pasos crean una política en la que se especifica el permiso `UseConnection` en el campo `action` y el nombre de recurso de Amazon (ARN) de conexión se especifica en el campo `Resource`.

Para usar la consola para añadir los permisos UseConnection

1. Para encontrar el ARN de conexión de su canalización, abra la canalización y elija el icono (i) de la acción de origen. Se abre el panel “Configuration” (Configuración) y junto a ConnectionArn aparece el ARN de conexión. Se agrega el ARN de conexión a la política de la función de servicio de CodeBuild.
2. Para encontrar la función de servicio de CodeBuild, abra el proyecto de compilación utilizado en la canalización y diríjase a la pestaña Build details (Detalles de compilación).
3. En la sección “Environment” (Entorno), elija el enlace Service role (Función de servicio). Esto abre la consola de AWS Identity and Access Management (IAM), donde puede agregar una política nueva que conceda acceso a la conexión.

4. En la consola de IAM, elija Attach policies (Asociar políticas), y, a continuación, elija Create policy (Crear política).

   Utilice la siguiente plantilla de política de ejemplo. Agregue el ARN de su conexión al campo `Resource`, como se muestra en este ejemplo.

   ```
   {
       "Version": "2012-10-17",
       "Statement": [
           {
               "Effect": "Allow",
               "Action": "codestar-connections:UseConnection",
               "Resource": "insert connection ARN here"
           }
       ]
   }
   ```

   En la pestaña JSON pegue la política.

5. Elija Review policy (Revisar política). Escriba un nombre para la política (por ejemplo, **`connection-permissions`**) y elija Create policy (Crear política).

6. Vuelva a la página Attach Permissions (Adjuntar permisos) de la función de servicio, actualice la lista de políticas y seleccione la política que acaba de crear. Seleccione Attach policies (Asociar políticas).

El alojamiento no está en estado disponible.

Si la consola muestra un mensaje que indica que un alojamiento no está en estado `Available`, elija Set up host (Configurar alojamiento).

El primer paso para la creación de un alojamiento da como resultado el alojamiento creado ahora en un estado `Pending`. Para que el estado del alojamiento cambie a `Available`, debe elegir configurar el alojamiento en la consola. Para obtener más información, consulte Configuración de un alojamiento pendiente.

> **Note**
>
> No se puede utilizar la AWS CLI para configurar un host `Pending`.

Solución de problemas de un alojamiento con errores de conexión

Las conexiones y los alojamientos pueden presentar un estado de error si se elimina o se modifica la aplicación GitHub subyacente. Los alojamientos y las conexiones en estado de error no se pueden recuperar y el alojamiento debe volver a crearse.

- Las acciones como cambiar la clave pem de la aplicación o cambiar el nombre de la aplicación (después de la creación inicial) provocarán que el alojamiento y todas las conexiones asociadas entren en estado de error.

Si la consola o la CLI devuelve un alojamiento o una conexión relacionada a un alojamiento con un estado de `Error`, es posible que deba realizar el siguiente paso:

- Elimine y vuelva a crear el recurso de alojamiento y, luego, reinstale la aplicación de registro del alojamiento. Para obtener más información, consulte Creación de un alojamiento.

No puedo crear una conexión para mi alojamiento

Para crear una conexión o un alojamiento, se necesitan las siguientes condiciones.

- El alojamiento debe estar en estado DISPONIBLE. Para obtener más información, consulte
- Las conexiones se deben crear en la misma región que el alojamiento.

Solución de problemas de la configuración de una VPC para el alojamiento

Cuando se crea un recurso de alojamiento, se debe proporcionar la conexión de red o la información de la VPC para la infraestructura en la que está instalada la instancia de GitHub Enterprise Server. Para solucionar problemas de configuración de la VPC o de la subred del alojamiento, utilice como referencia la información de la VPC de ejemplo que se muestra aquí.

> **Note**
>
> Utilice esta sección para solucionar problemas relacionados con la configuración del alojamiento de GitHub Enterprise Server dentro de una Amazon VPC. Para solucionar problemas relacionados con la conexión que está configurada para utilizar el punto de enlace

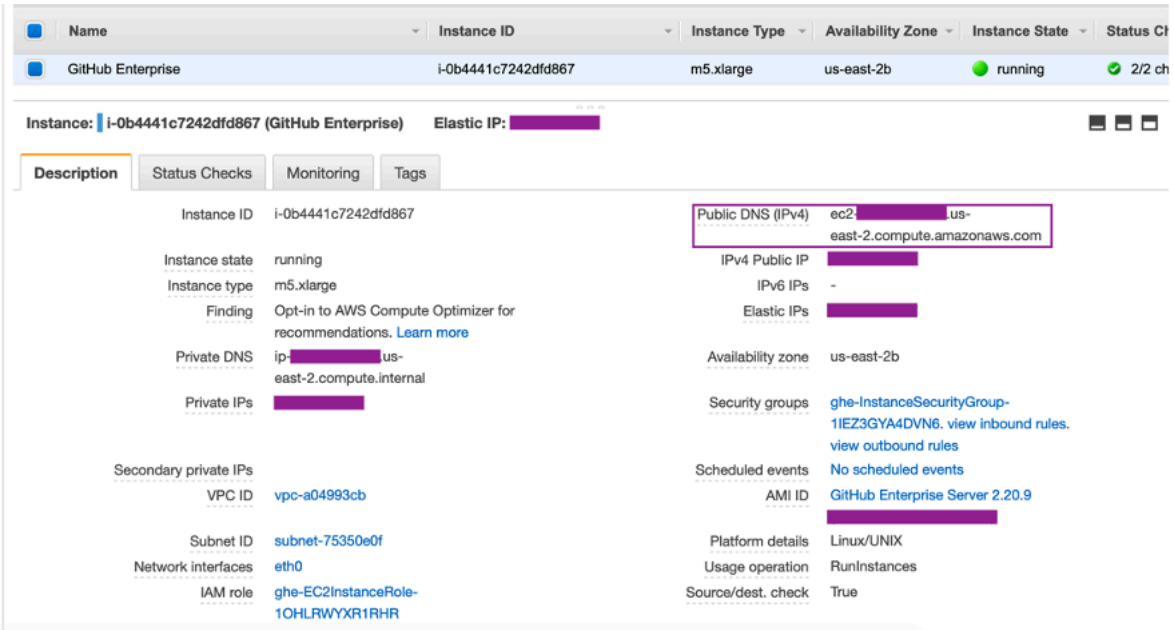
de webhook para VPC (PrivateLink), consulte Solución de problemas de los puntos de enlace de la VPC (PrivateLink) de webhook para conexiones de GitHub Enterprise Server.

Para este ejemplo, se utilizará el siguiente proceso para configurar la VPC y el servidor donde se instalará la instancia de GitHub Enterprise Server:

1. Cree una VPC. Para obtener más información, consulte https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#Create-VPC.
2. Cree una subred en su VPC. Para obtener más información, consulte https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#AddaSubnet.
3. Lance una instancia en su VPC. Para obtener más información, consulte https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#VPC_Launch_Instance.

> **Note**
>
> Cada VPC solo puede asociarse a un host (una instancia de GitHub Enterprise Server) a la vez.

La siguiente imagen muestra una instancia EC2 lanzada mediante la AMI de GitHub Enterprise.



Cuando utiliza una VPC para una conexión de GitHub Enterprise Server, debe proporcionar lo siguiente para su infraestructura al momento de configurar el alojamiento:

- ID de la VPC: la VPC del servidor donde está instalada la instancia de GitHub Enterprise Server o una VPC con acceso a la instancia instalada de GitHub Enterprise Server a través de VPN o Direct Connect.
- el ID o los ID de la subred: la subred del servidor donde está instalada la instancia de GitHub Enterprise Server o una subred con acceso a la instancia instalada de GitHub Enterprise Server a través de VPN o Direct Connect.
- grupo o grupos de seguridad: se trata del grupo de seguridad del servidor donde está instalada la instancia de GitHub Enterprise Server o de un grupo de seguridad con acceso a la instancia instalada de GitHub Enterprise Server a través de VPN o Direct Connect.
- punto de enlace: tenga listo el punto de enlace del servidor y continúe con el siguiente paso.

Para obtener más información acerca de cómo trabajar con las VPC y las subredes, consulte Tamaño de la subred y la VPC para una dirección IPv4 en la Guía del usuario de Amazon VPC.

Temas

No logro obtener un alojamiento en estado pendiente

Si su alojamiento entra en el estado VPC_CONFIG_FAILED_INITIALIZATION, es probable que esto se deba a un problema con la VPC, las subredes o los grupos de seguridad que ha seleccionado para el alojamiento.

- La VPC, las subredes y los grupos de seguridad deben pertenecer a la cuenta que crea el alojamiento.
- Las subredes y los grupos de seguridad deben pertenecer a la VPC seleccionada.
- Cada subred proporcionada debe estar en diferentes zonas de disponibilidad.
- El usuario que crea el alojamiento debe tener los siguientes permisos de IAM:

```
ec2:CreateNetworkInterface
ec2:CreateTags
ec2:DescribeDhcpOptionsec2:DescribeNetworkInterfaces
ec2:DescribeSubnets
ec2:DeleteNetworkInterface
ec2:DescribeVpcs
ec2:CreateVpcEndpoint
ec2:DeleteVpcEndpoints
ec2:DescribeVpcEndpoints
```

No logro obtener un alojamiento en estado disponible

Si no puede completar la configuración de la aplicación AWS CodeStar Connections para su host, es posible que se deba a un problema con las configuraciones de la VPC o con la instancia de GitHub Enterprise Server.

- Si no utiliza una entidad de certificación pública, deberá proporcionar un certificado TLS a su alojamiento, el cual es utilizado por la instancia de GitHub Enterprise. El valor del certificado TLS debe ser la clave pública del certificado.
- Debe ser administrador de la instancia de GitHub Enterprise Server para crear aplicaciones GitHub.

Mi conexión o mi alojamiento estaba funcionando y ahora ha dejado de funcionar

Si una conexión o un alojamiento funcionaba antes y ahora no funciona, podría deberse a un cambio de configuración en la VPC o a una modificación de la aplicación GitHub. Compruebe lo siguiente:

- El grupo de seguridad adjunto al recurso de host que creó para la conexión cambió o ya no tiene acceso a GitHub Enterprise Server. AWS CodeStar Connections requiere un grupo de seguridad que tenga conectividad con la instancia de GitHub Enterprise Server.
- La dirección IP del servidor DNS ha cambiado recientemente. Esto se puede verificar si se comprueban las opciones de DHCP adjuntas a la VPC especificada en el recurso de alojamiento que creó para la conexión. Tenga en cuenta que si recientemente se ha trasladado de AmazonProvidedDNS a un servidor DNS personalizado o ha comenzado a utilizar un servidor DNS personalizado nuevo, el alojamiento de la conexión podría dejar de funcionar. Para solucionar esto, debe eliminar el alojamiento existente y volver a crearlo, lo que almacenará la configuración de DNS más reciente en nuestra base de datos.

- La configuración de las ACL de red cambió y ya no permite conexiones HTTP a la subred donde se encuentra la infraestructura de GitHub Enterprise Server.
- Las configuraciones de la aplicación AWS CodeStar Connections en GitHub Enterprise Server han cambiado. Las modificaciones en cualquiera de las configuraciones, como direcciones URL o secretos de aplicaciones, pueden interrumpir la conectividad entre la instancia de GitHub Enterprise Server instalada y AWS CodeStar Connections.

No puedo eliminar mis interfaces de red

Si no puede detectar las interfaces de red, verifique lo siguiente:

- Las interfaces de red creadas por AWS CodeStar Connections solo se pueden eliminar si se elimina el host. El usuario no puede eliminarlas de forma manual.
- Debe tener los siguientes permisos:

```
ec2:DescribeNetworkInterfaces
ec2:DeleteNetworkInterface
```

Solución de problemas de los puntos de enlace de la VPC (PrivateLink) de webhook para conexiones de GitHub Enterprise Server

Cuando crea un alojamiento con configuración de VPC, se crea el punto de enlace de la VPC de webhook.

> **Note**
>
> Utilice esta sección para solucionar problemas relacionados con la conexión configurada para utilizar el punto de enlace de webhook para VPC (PrivateLink). Para solucionar problemas relacionados con la configuración del alojamiento de GitHub Enterprise Server dentro de una Amazon VPC, consulte Solución de problemas de la configuración de una VPC para el alojamiento.

Cuando crea una conexión a un tipo de proveedor instalado y ha especificado que el servidor está configurado en una VPC, AWS CodeStar Connections crea el host y se crea el punto de conexión de VPC (PrivateLink) para webhooks. Esto permite que el host envíe datos de eventos a través

de webhooks a los servicios de AWS integrados mediante la red de Amazon. Para obtener más información, consulte AWS CodeStar Connections y puntos de conexión de VPC de la interfaz (AWS PrivateLink).

Temas

- No puedo eliminar los puntos de enlace de la VPC de webhook

No puedo eliminar los puntos de enlace de la VPC de webhook

AWS CodeStar Connections administra el ciclo de vida de los puntos de conexión de VPC de webhook para el host. Si desea eliminar el punto de enlace, debe eliminar el recurso de alojamiento correspondiente.

- Los puntos de conexión de VPC (PrivateLink) de webhook creados por AWS CodeStar Connections solo se pueden eliminar si se elimina el host. No se pueden eliminar de forma manual.
- Debe tener los siguientes permisos:

```
ec2:DescribeNetworkInterfaces
ec2:DeleteNetworkInterface
```

Solución de problemas de un alojamiento creado antes del 24 de noviembre de 2020

A partir del 24 de noviembre de 2020, cuando AWS CodeStar Connections configure su host, se configurará una compatibilidad adicional con los puntos de conexión de VPC (PrivateLink). Para los alojamientos creados antes de esta actualización, utilice esta sección de solución de problemas.

Para obtener más información, consulte AWS CodeStar Connections y puntos de conexión de VPC de la interfaz (AWS PrivateLink).

Temas

- Tengo un alojamiento que se creó antes del 24 de noviembre de 2020 y quiero utilizar los puntos de enlace de la VPC (PrivateLink) para webhooks
- No puedo obtener un alojamiento en estado disponible (error de la VPC)

Tengo un alojamiento que se creó antes del 24 de noviembre de 2020 y quiero utilizar los puntos de enlace de la VPC (PrivateLink) para webhooks

Cuando configura su alojamiento de GitHub Enterprise Server, se crea el punto de enlace de webhook. Las conexiones ahora utilizan puntos de enlace de webhook de la VPC PrivateLink. Si creó el alojamiento antes del 24 de noviembre de 2020 y desea utilizar los puntos de enlace de webhook de la VPC PrivateLink, primero debe eliminar su alojamiento y luego crear un alojamiento nuevo.

No puedo obtener un alojamiento en estado disponible (error de la VPC)

Si su host se creó antes del 24 de noviembre de 2020 y no puede completar la configuración de la aplicación AWS CodeStar Connections para el host, es posible que se deba a un problema con las configuraciones de la VPC o con la instancia de GitHub Enterprise Server.

La VPC necesitará una gateway NAT (o acceso a Internet saliente) para que la instancia de GitHub Enterprise Server pueda enviar tráfico de red de salida para webhooks de GitHub.

No se puede crear la conexión para un repositorio de GitHub

Problema:

dado que una conexión a un repositorio de GitHub utiliza AWS Connector for GitHub, necesita permisos del propietario de la organización o permisos del administrador del repositorio para crear la conexión.

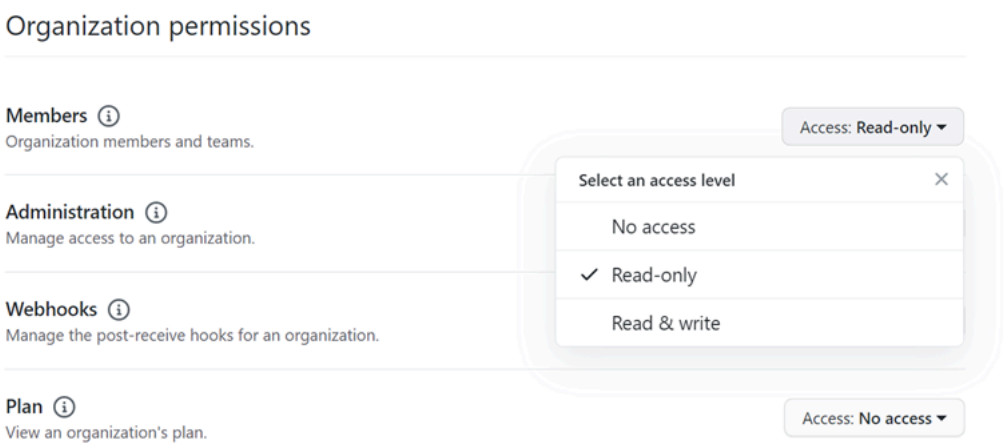
Soluciones posibles: para obtener información acerca de los niveles de permisos de un repositorio de GitHub, consulte https://docs.github.com/en/free-pro-team@latest/github/setting-up-and-managing-organizations-and-teams/permission-levels-for-an-organization.

Edición de los permisos de la aplicación de conexión de GitHub Enterprise Server

Si instaló la aplicación de GitHub Enterprise Server el 23 de diciembre de 2020 o antes, es posible que deba conceder el acceso de solo lectura de la aplicación a los miembros de la organización. Si es el propietario de la aplicación GitHub, siga estos pasos para editar los permisos de la aplicación que se instaló cuando se creó el alojamiento.

> **Note**
>
> Debe completar estos pasos en la instancia de GitHub Enterprise Server y debe ser el propietario de la aplicación GitHub.

1. En GitHub Enterprise Server, en la opción desplegable de su fotografía de perfil, elija Settings (Configuración).
2. Elija Developer settings (Configuración del desarrollador) y, luego, elija GitHub Apps (Aplicaciones GitHub).
3. En la lista de aplicaciones, elija el nombre de la aplicación para la conexión y, luego, elija Permissions and events (Permisos y eventos) en la pantalla de configuración.
4. En Organization permissions (Permisos de la organización), para Members (Miembros), elija Read-only (Solo lectura) en el menú desplegable Access (Acceso).



5. En Add a note to users (Agregar una nota para los usuarios), agregue una descripción del motivo de la actualización. Elija Save changes (Guardar cambios).

Error de conexiones al conectarse a GitHub: «Ha ocurrido un problema, asegúrese de que las cookies estén habilitadas en el navegador» o «El propietario de una organización debe instalar la aplicación de GitHub»

Problema:

Para crear la conexión para un repositorio de GitHub, debe ser el propietario de la organización de GitHub. Para los repositorios que no pertenecen a una organización, debe ser el propietario del repositorio. Cuando alguien que no sea el propietario de la organización crea una conexión, se crea una solicitud para el propietario de la organización y se muestra uno de los siguientes errores:

Se ha producido un problema, asegúrese de que las cookies estén habilitadas en el navegador

O BIEN

El propietario de una organización debe instalar la aplicación de GitHub

Posibles correcciones: Para los repositorios de una organización de GitHub, el propietario de la organización debe crear la conexión con el repositorio de GitHub. Para los repositorios que no pertenecen a una organización, debe ser el propietario del repositorio.

Me gustaría aumentar los límites de conexiones

Puede solicitar un aumento de límite para determinados límites de AWS CodeStar Connections. Para obtener más información, consulte Cuotas para conexiones.

Cuotas para conexiones

En las siguientes tablas se enumeran las cuotas (también denominadas límites) de las conexiones en la consola de herramientas para desarrolladores.

Las cuotas de esta tabla se aplican por Región de AWS y pueden aumentar. Para solicitar un aumento, utilice la consola del Centro de asistencia. Para obtener información de Región de AWS y cuotas que se pueden cambiar, consulte Service Quotas de AWS.

> **Note**
>
> Debe habilitar la Región de AWS Europa (Milán) antes de poder usarlo. Para obtener más información, consulte Habilitar una región.

Recursos	Límite predeterminado
Número máximo de conexiones por Cuenta de AWS	250

Las cuotas de esta tabla son fijas y no pueden modificarse.

Recursos	Límite predeterminado
Número máximo de caracteres en nombres de conexión	32 caracteres

Recursos	Límite predeterminado
Número máximo de hosts por Cuenta de AWS	50
Número máximo de enlaces de repositorios	100
Número máximo de configuraciones de sincronización de pilas de AWS CloudFormation	100
Número máximo de configuraciones de sincronización por enlace de repositorio	100
Número máximo de configuraciones de sincronización por ramificación	50

Direcciones IP para añadir a la lista de permitidas

Si implementa el filtrado IP o permite determinadas direcciones IP en las instancias de Amazon EC2, añada las siguientes direcciones IP a su lista de direcciones permitidas. De este modo, se habilitan las conexiones con proveedores, como GitHub Bitbucket.

En la siguiente tabla, se enumeran las direcciones IP de las conexiones en la consola de herramientas para desarrolladores por Región de AWS.

> **Note**
>
> En el caso de la región Europa (Milán), debe habilitar esta región antes de poder utilizarla. Para obtener más información, consulte Habilitar una región.

Región	Direcciones IP
Oeste de EE. UU. (Oregón) (us-west-2)	35.160.210.199, 54.71.206.108, 54.71.36.205
Este de EE. UU. (Norte de Virginia) (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

Región	Direcciones IP
Este de EE. UU. (Ohio) (us-east-2)	18,217.188190, 18.218158,91, 18.220,4,80
Asia-Pacífico (Singapur) (ap-southeast-1)	18138,171,151, 18139,22,70, 3.1.157,176
Asia-Pacífico (Sídney) (ap-southeast-2)	13,236,59,253, 52.64,166.86, 54.206,1112
Asia-Pacífico (Tokio) (ap-northeast-1)	52,196132231, 54,95133227, 18,181,13,91
Europa (Fráncfort) (eu-central-1)	18,196,145164, 3,1121,252,59, 52,59104,195
Asia-Pacífico (Seúl) (ap-northeast-2)	13.125.8.239, 13.209.223.177, 3.37.200,23
Asia Pacífico (Bombay) (ap-south-1)	13.234.199152, 13.235,29220, 35.154,230,124
América del Sur (São Paulo) (sa-east-1)	18229,77,26, 54,233.226,52, 54,233.207,69
Canadá (centro) (ca-central-1)	15,222,219,210, 35,182,166,138, 99,79,111 .198
Europa (Londres) (eu-west-2)	3.9.97.205, 35.177.150185, 35.177.200225
EE. UU. Oeste (Norte de California) (us-west-1)	5252,16,175, 52,863,87
Europa (París) (eu-west-3)	35,181127,138, 35,181,45,22, 35,181,20 200
Europa (Estocolmo) (eu-north-1)	13.48,66148, 13.488.79, 13.53.78182
UE (Milán) (eu-south-1)	18.102.28.105, 18.102.35.130, 18.102.8.116

Seguridad para las características de la consola de herramientas para desarrolladores

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de cumplimiento que se aplican a AWS CodeStar las notificaciones y AWS CodeStar conexiones, consulte AWS los servicios incluidos en el ámbito de aplicación por programa de cumplimiento.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al utilizar AWS CodeStar Notificaciones y AWS CodeStar conexiones. En los temas siguientes, se muestra cómo configurar AWS CodeStar las notificaciones y AWS CodeStar las conexiones para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de AWS CodeStar notificaciones y AWS CodeStar conexiones.

Para obtener más información acerca de la seguridad de los servicios de la consola de herramientas para desarrolladores, consulte lo siguiente:

- CodeBuild Seguridad
- CodeCommit Seguridad
- CodeDeploy Seguridad
- CodePipeline Seguridad

Descripción del contenido y la seguridad de las notificaciones

Las notificaciones proporcionan información acerca de los recursos a los usuarios que están suscritos a los destinos de las reglas de notificación que configure. Esta información puede incluir detalles sobre los recursos de las herramientas para desarrolladores, como, por ejemplo, el contenido de los repositorios, los estados de compilación, los estados de implementación y las ejecuciones de canalizaciones.

Por ejemplo, puedes configurar una regla de notificación para un repositorio CodeCommit que incluya comentarios en las confirmaciones o solicitudes de cambios. En caso afirmativo, las notificaciones enviadas en respuesta a dicha regla podrían incluir la línea o líneas de código a las que se hace referencia en dicho comentario. Del mismo modo, puedes configurar una regla de notificación para un proyecto de compilación CodeBuild que incluya los éxitos o los fracasos en los estados y fases de compilación. Las notificaciones enviadas en respuesta a dicha regla incluirán dicha información.

Puedes configurar una regla de notificación para una canalización CodePipeline que incluya información sobre las aprobaciones manuales, y las notificaciones que se envíen en respuesta a esa regla pueden incluir el nombre de la persona que proporciona la aprobación. Puede configurar una regla de notificación para una aplicación que indique CodeDeploy que la implementación se ha realizado correctamente, y las notificaciones enviadas en respuesta a esa regla pueden contener información sobre el objetivo de la implementación.

Las notificaciones pueden contener información específica del proyecto, como, por ejemplo, estados de compilación, líneas de código que tienen comentarios, estado de implementación y aprobaciones de canalizaciones. Por lo tanto, para ayudar a garantizar la seguridad de su proyecto, asegúrese de revisar periódicamente tanto los destinos de las reglas de notificación como la lista de suscriptores de los temas de Amazon SNS especificados como destinos. Además, el contenido de las notificaciones enviadas en respuesta a eventos podría cambiar a medida que se añadan características adicionales a los servicios subyacentes. Este cambio puede producirse sin previo aviso a las reglas de notificación ya existentes. Considere la posibilidad de revisar el contenido de los mensajes de notificación periódicamente para ayudar a garantizar que entiende lo que se envía y a quién se envía.

Para obtener más información acerca de los tipos de eventos disponibles para las reglas de notificación, consulte Conceptos de notificación.

Puede elegir limitar los detalles incluidos en las notificaciones solo a lo que se incluye en un evento. A esto se lo denomina tipo de detalle Básico. Estos eventos contienen exactamente la misma información que se envía a Amazon EventBridge y Amazon CloudWatch Events.

Los servicios de consola de Developer Tools CodeCommit, por ejemplo, pueden optar por añadir información sobre algunos o todos sus tipos de eventos en los mensajes de notificación más allá de lo que está disponible en un evento. Esta información complementaria podría agregarse en cualquier momento para mejorar los tipos de eventos actuales o complementar los tipos de eventos futuros. Puede elegir incluir cualquier información adicional sobre el evento, si está disponible, en la notificación seleccionando el tipo de detalle Full (completo). Para obtener más información, consulte Tipos de detalles.

Protección de los datos en AWS CodeStar Notifications y AWS CodeStar Connections

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos de AWS CodeStar Notifications y AWS CodeStar Connections. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la AWS Cloud. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. También es responsable de la configuración de seguridad y de las tareas de administración para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la cuenta de AWS y configurar cuentas de usuario individuales con AWS Single Sign-On o AWS Identity and Access Management (IAM). De esta manera, cada usuario recibe solamente los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilizar la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Se requiere el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de AWS.

- Utilizar servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no ingresar información confidencial o sensible, como por ejemplo direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaje con AWS CodeStar Notifications y AWS CodeStar Connections u otros Servicios de AWS mediante la consola, la API, la AWS CLI o los AWS SDK. Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Gestión de identidad y acceso para AWS CodeStar notificaciones y AWS CodeStar conexiones

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de AWS CodeStar notificaciones y AWS CodeStar conexiones. La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

- Permitir a los usuarios consultar sus propios permisos
- Solución de problemas de identidad y acceso a AWS CodeStar notificaciones y AWS CodeStar conexiones
- Uso de roles vinculados a servicios para AWS CodeStar Notifications
- Uso de roles vinculados a servicios de AWS CodeConnections
- Políticas administradas de AWS para AWS CodeConnections

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en AWS CodeStar Notificaciones y AWS CodeStar Conexiones.

Usuario del servicio: si utiliza el servicio de AWS CodeStar notificaciones y AWS CodeStar conexiones para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más funciones de AWS CodeStar notificaciones y AWS CodeStar conexiones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una función de AWS CodeStar Notificaciones y AWS CodeStar conexiones, consulteSolución de problemas de identidad y acceso a AWS CodeStar notificaciones y AWS CodeStar conexiones.

Administrador de servicios: si está a cargo de los recursos de AWS CodeStar notificaciones y AWS CodeStar conexiones en su empresa, probablemente tenga acceso total a AWS CodeStar las notificaciones y AWS CodeStar conexiones. Su trabajo consiste en determinar a qué funciones y recursos de AWS CodeStar Notificaciones y AWS CodeStar Conexiones deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con AWS CodeStar notificaciones y AWS CodeStar conexiones, consulteCómo funcionan las características de la consola de herramientas para desarrolladores con IAM.

Administrador de IAM: si es administrador de IAM, puede que le interese obtener más información sobre cómo redactar políticas para gestionar el acceso a las AWS CodeStar notificaciones y las conexiones. AWS CodeStar Para ver ejemplos de políticas de AWS CodeStar notificaciones y AWS CodeStar conexiones basadas en la identidad que puede utilizar en IAM, consulte. Ejemplos de políticas basadas en identidades

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Usuario raíz de la cuenta de AWS

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos de Servicios de AWS la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué

pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS Single Sign-On.

- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Cómo funcionan las características de la consola de herramientas para desarrolladores con IAM

Antes de utilizar IAM para administrar el acceso a características de la consola de herramientas para desarrolladores, debe saber qué características de IAM están disponibles para utilizarse con la consola. Para obtener una visión general de cómo funcionan las notificaciones y otros AWS servicios con IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Temas

- Políticas basadas en identidad de la consola de herramientas para desarrolladores
- AWS CodeStar Políticas de notificaciones y AWS CodeStar conexiones basadas en recursos
- Autorización basada en etiquetas
- Roles de IAM

Políticas basadas en identidad de la consola de herramientas para desarrolladores

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. AWS CodeStar Las notificaciones y AWS CodeStar las conexiones admiten acciones, recursos y claves de condición específicos. Para obtener más información acerca de los elementos que utiliza

en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Acciones

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones de política para las notificaciones de la consola de herramientas para desarrolladores utilizan los siguientes prefijos antes de la acción: `codestar-notifications and codestar-connections`. Por ejemplo, para conceder a alguien permiso para ver todas las reglas de notificación de su cuenta, incluya la acción `codestar-notifications:ListNotificationRules` en su política. Las declaraciones de política deben incluir un `NotAction` elemento `Action` o. AWS CodeStar Notifications and AWS CodeStar Connections define su propio conjunto de acciones que describen las tareas que puede realizar con este servicio.

Para especificar varias acciones de AWS CodeStar notificación en una sola instrucción, sepárelas con comas de la siguiente manera.

```
"Action": [
      "codestar-notifications:action1",
      "codestar-notifications:action2"
```

Para especificar varias AWS CodeConnections acciones en una sola sentencia, sepárelas con comas de la siguiente manera.

```
"Action": [
      "codestar-connections:action1",
      "codestar-connections:action2"
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `List`, incluya la siguiente acción.

```
"Action": "codestar-notifications:List*"
```

AWS CodeStar Las acciones de la API de notificaciones incluyen:

- `CreateNotificationRule`
- `DeleteNotificationRule`
- `DeleteTarget`
- `DescribeNotificationRule`
- `ListEventTypes`
- `ListNotificationRules`
- `ListTagsForResource`
- `ListTargets`
- `Subscribe`
- `TagResource`
- `Unsubscribe`
- `UntagResource`
- `UpdateNotificationRule`

AWS CodeConnections Las acciones de la API incluyen las siguientes:

- `CreateConnection`
- `DeleteConnection`
- `GetConnection`
- `ListConnections`
- `ListTagsForResource`
- `TagResource`
- `UntagResource`

AWS CodeConnections Para completar el protocolo de autenticación, se requieren las siguientes acciones que solo requieren permisos:

- `GetIndividualAccessToken`
- `GetInstallationUrl`
- `ListInstallationTargets`
- `StartOAuthHandshake`
- `UpdateConnectionInstallation`

Para usar una conexión, se requiere la siguiente acción, que solo requiere permisos: AWS CodeConnections

- `UseConnection`

AWS CodeConnections Para transferir una conexión a un servicio se requiere la siguiente acción, que solo requiere permisos:

- `PassConnection`

Para ver una lista de AWS CodeStar las acciones de notificaciones y AWS CodeStar conexiones, consulte las acciones definidas por las AWS CodeStar notificaciones y las acciones definidas por las AWS CodeStar conexiones en la Guía del usuario de IAM.

Recursos

AWS CodeStar Las notificaciones y AWS CodeStar las conexiones no permiten especificar los ARN de los recursos en una política.

Claves de condición

AWS CodeStar Las notificaciones y AWS CodeStar las conexiones definen sus propios conjuntos de claves de condición y también admiten el uso de algunas claves de condición globales. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Todas las acciones de AWS CodeStar notificación admiten la clave de `codestar-notifications:NotificationsForResource` condición. Para obtener más información, consulte Ejemplos de políticas basadas en identidades.

AWS CodeConnections defina las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener más información, consulte AWS CodeConnections referencia de permisos.

Claves de condición	Descripción
`codestar-connections:BranchName`	Filtra el acceso por el nombre de ramificación del repositorio de terceros.
`codestar-connections:FullRepositoryId`	Filtra el acceso del repositorio que se incluye en la solicitud. Se aplica solo a las solicitudes `UseConnection` para acceder a un repositorio específico.
`codestar-connections:InstallationId`	Filtra el acceso por el ID de terceros (como el ID de instalación de la aplicación de Bitbucket) que se utiliza para actualizar una conexión. Permite restringir las instalaciones de aplicaciones de terceros que se pueden utilizar para realizar una conexión.
`codestar-connections:OwnerId`	Filtra el acceso por propietario o ID de cuenta del proveedor de terceros.
`codestar-connections:PassedToService`	Filtra el acceso por el servicio al que la entidad principal puede pasar una conexión.
`codestar-connections:ProviderAction`	Filtra el acceso por acción del proveedor en una solicitud `UseConnection` , como `ListRepositories` .
`codestar-connections:ProviderPermissionsRequired`	Filtra el acceso por el tipo de permisos del proveedor de terceros.

Claves de condición	Descripción
`codestar-connections:ProviderType`	Filtra el acceso por el tipo de proveedor externo incluido en la solicitud
`codestar-connections:ProviderTypeFilter`	Filtra el acceso por el tipo de proveedor externo utilizado para filtrar resultados
`codestar-connections:RepositoryName`	Filtra el acceso por el nombre del repositorio de terceros.

Ejemplos

Para ver ejemplos de políticas de AWS CodeStar notificaciones y AWS CodeStar conexiones basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades

AWS CodeStar Políticas de notificaciones y AWS CodeStar conexiones basadas en recursos

AWS CodeStar Las notificaciones y AWS CodeStar las conexiones no admiten políticas basadas en recursos.

Autorización basada en etiquetas

Puede adjuntar etiquetas a los recursos de AWS CodeStar Notificaciones y AWS CodeStar Conexiones o transferir etiquetas en una solicitud. Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `codestar-notifications and codestar-connections:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`. Para obtener más información sobre las estrategias de etiquetado, consulte Recursos de etiquetado. AWS Para obtener más información sobre el etiquetado de los recursos de AWS CodeStar notificaciones y AWS CodeStar conexiones, consulte. Etiquetado de recursos de conexiones

Para ver ejemplos de políticas basadas en identidad para limitar el acceso a un recurso en función de las etiquetas de ese recurso, consulte Uso de etiquetas para controlar el acceso a los recursos de AWS CodeStar Connections.

Roles de IAM

Un rol de IAM es una entidad de tu AWS cuenta que tiene permisos específicos.

Uso de credenciales temporales

Puede utilizar credenciales temporales para iniciar sesión con federación y asumir un rol de IAM o un rol de acceso entre cuentas. Para obtener credenciales de seguridad temporales, puede llamar a operaciones de AWS STS API como AssumeRoleo GetFederationToken.

AWS CodeStar Notifications and AWS CodeStar Connections admite el uso de credenciales temporales.

Roles vinculados al servicio

Las funciones vinculadas al servicio permiten a AWS los servicios acceder a los recursos de otros servicios para completar una acción en tu nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

AWS CodeStar Las notificaciones admiten los roles vinculados al servicio. Para obtener más información sobre la creación o la administración de funciones vinculadas al servicio de AWS CodeStar Notificaciones y AWS CodeStar Conexiones, consulte. Uso de roles vinculados a servicios para AWS CodeStar Notifications

AWS CodeStar Connections no admite funciones vinculadas al servicio.

AWS CodeConnections referencia de permisos

En las tablas siguientes se enumeran cada operación de la AWS CodeConnections API, las acciones correspondientes para las que puedes conceder permisos y el formato del ARN del recurso que se va a utilizar para conceder los permisos. Las AWS CodeConnections API se agrupan en tablas según el alcance de las acciones permitidas por esa API. Consulte esta tabla cuando escriba políticas de permisos que pueda adjuntar a una identidad de IAM (políticas basadas en identidad).

Al crear una política de permisos, debe especificar las acciones en el campo `Action`de la política. Debe especificar un valor del recurso en el campo `Resource` de la política como ARN, con o sin un carácter comodín (*).

Para expresar condiciones en las políticas de conexiones, utilice las claves de condición descritas aquí y enumeradas en Claves de condición. También puedes usar claves de condición que AWS

abarquen todo el conjunto. Para obtener una lista completa de las claves AWS de ancho, consulte las claves disponibles en la Guía del usuario de IAM.

Para especificar una acción, use el prefijo `codestar-connections:` seguido del nombre de la operación API (por ejemplo, `codestar-connections:ListConnections` o `codestar-connections:CreateConnection`).

Uso de comodines

Para especificar varias acciones o recursos, utilice el carácter de comodín (*) en el ARN. Por ejemplo, `codestar-connections:*` especifica todas AWS CodeConnections las acciones y `codestar-connections:Get*` especifica todas AWS CodeConnections las acciones que comienzan por la palabra. `Get` El siguiente ejemplo concede acceso a todos los recursos con nombres que comienzan con `MyConnection`.

```
arn:aws:codestar-connections:us-west-2:account-ID:connection/*
```

Puede utilizar comodines solo con los recursos de *`connection`* que se muestran en la siguiente tabla. No puede utilizar comodines con los recursos *`region`* o *`account-id`*. Para obtener más información acerca de los comodines, consulte identificadores de IAM en la Guía del usuario de IAM.

Temas

- Permisos para administrar conexiones
- Permisos para administrar alojamientos
- Permisos para completar conexiones
- Permisos para configurar alojamientos
- Pasar una conexión a un servicio
- Uso de una conexión
- Tipos de acceso admitidos para ProviderAction
- Permisos compatibles con el etiquetado de recursos de conexión
- Pasar una conexión a un enlace de repositorio
- Clave de condición compatible para los enlaces de repositorios

Permisos para administrar conexiones

Un rol o usuario designado para usar el SDK AWS CLI o el SDK para ver, crear o eliminar conexiones debe tener permisos limitados a lo siguiente.

> **Note**
>
> No puede completar ni usar una conexión en la consola solo con los permisos siguientes. Debe agregar los permisos en Permisos para completar conexiones.

```
codestar-connections:CreateConnection
codestar-connections:DeleteConnection
codestar-connections:GetConnection
codestar-connections:ListConnections
```

AWS CodeStar Las notificaciones y AWS CodeStar las conexiones requieren permisos para las acciones de administración de las conexiones

CreateConnection

Acciones: `codestar-connections:CreateConnection`

Se necesita para utilizar la CLI o la consola para crear una conexión.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

DeleteConnection

Acciones: `codestar-connections:DeleteConnection`

Se necesita para utilizar la CLI o la consola para eliminar una conexión.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetConnection

Acciones: `codestar-connections:GetConnection`

Se necesita para utilizar la CLI o la consola para ver los detalles de una conexión.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListConnections

Acciones: `codestar-connections:ListConnections`

Se necesita para utilizar la CLI o la consola para enumerar todas las conexiones de la cuenta.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Estas operaciones admiten las siguientes claves de condición:

Acción	Claves de condición
`codestar-connections:CreateConnection`	`codestar-connections:ProviderType`
`codestar-connections:DeleteConnection`	N/A
`codestar-connections:GetConnection`	N/A
`codestar-connections:ListConnections`	`codestar-connections:ProviderTypeFilter`

Permisos para administrar alojamientos

Un rol o usuario designado para usar el SDK AWS CLI o el SDK para ver, crear o eliminar hosts debe tener permisos limitados a lo siguiente.

> **Note**
>
> No puede completar ni utilizar una conexión en el alojamiento solo con los siguientes permisos. Debe agregar los permisos en Permisos para configurar alojamientos.

```
codestar-connections:CreateHost
codestar-connections:DeleteHost
codestar-connections:GetHost
codestar-connections:ListHosts
```

AWS CodeStar Las notificaciones y AWS CodeStar las conexiones requerían permisos para realizar acciones de administración de hosts

CreateHost

Acciones: `codestar-connections:CreateHost`

Se necesita para utilizar la CLI o la consola para crear un alojamiento.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

DeleteHost

Acciones: `codestar-connections:DeleteHost`

Se necesita para utilizar la CLI o la consola para eliminar un alojamiento.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

GetHost

Acciones: `codestar-connections:GetHost`

Se necesita para utilizar la CLI o la consola para ver los detalles de un alojamiento.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

ListHosts

Acciones: `codestar-connections:ListHosts`

Se necesita para utilizar la CLI o la consola para enumerar todos los alojamientos de la cuenta.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

Estas operaciones admiten las siguientes claves de condición:

Acción	Claves de condición
codestar-connections:CreateHost	codestar-connections:ProviderType
codestar-connections:DeleteHost	N/A
codestar-connections:GetHost	N/A
codestar-connections:ListHosts	codestar-connections:ProviderTypeFilter

Permisos para completar conexiones

Un rol o un usuario designado para administrar conexiones en la consola debe tener los permisos necesarios para completar una conexión en la consola y crear una instalación, lo que incluye autorizar el protocolo de enlace al proveedor y crear instalaciones para que se utilicen las conexiones. Utilice los siguientes permisos además de los anteriores.

La consola utiliza las siguientes operaciones de IAM al realizar el protocolo de conexión basado en navegador. `ListInstallationTargets`, `GetInstallationUrl`, `StartOAuthHandshake`, `UpdateConnectionInstallation` y `GetIndividualAccessToken` son permisos de política de IAM. No son acciones de API.

```
codestar-connections:GetIndividualAccessToken
codestar-connections:GetInstallationUrl
codestar-connections:ListInstallationTargets
codestar-connections:StartOAuthHandshake
codestar-connections:UpdateConnectionInstallation
```

En función de esto, se necesitan los siguientes permisos para utilizar, crear, actualizar o eliminar una conexión en la consola.

```
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
```

AWS CodeConnections permisos necesarios para realizar acciones destinadas a completar las conexiones

GetIndividualAccessToken

Acciones: `codestar-connections:GetIndividualAccessToken`

Se necesita para utilizar la consola para completar una conexión. Se trata únicamente de un permiso de política de IAM, no de una acción de API.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetInstallationUrl

Acciones: `codestar-connections:GetInstallationUrl`

Se necesita para utilizar la consola para completar una conexión. Se trata únicamente de un permiso de política de IAM, no de una acción de API.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListInstallationTargets

Acciones: `codestar-connections:ListInstallationTargets`

Se necesita para utilizar la consola para completar una conexión. Se trata únicamente de un permiso de política de IAM, no de una acción de API.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Empezar a AuthHandshake

Acciones: `codestar-connections:StartOAuthHandshake`

Se necesita para utilizar la consola para completar una conexión. Se trata únicamente de un permiso de política de IAM, no de una acción de API.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

UpdateConnectionInstallation

Acciones: `codestar-connections:UpdateConnectionInstallation`

Se necesita para utilizar la consola para completar una conexión. Se trata únicamente de un permiso de política de IAM, no de una acción de API.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Estas operaciones admiten las siguientes claves de condición.

Acción	Claves de condición
`codestar-connections:GetIndividualAccessToken`	`codestar-connections:ProviderType`
`codestar-connections:GetInstallationUrl`	`codestar-connections:ProviderType`
`codestar-connections:ListInstallationTargets`	N/A
`codestar-connections:StartOAuthHandshake`	`codestar-connections:ProviderType`
`codestar-connections:UpdateConnectionInstallation`	`codestar-connections:InstallationId`

Permisos para configurar alojamientos

Un rol o un usuario designado para administrar conexiones en la consola debe tener los permisos necesarios para configurar un alojamiento en la consola, lo que incluye la autorización del protocolo

de enlace al proveedor y la instalación de la aplicación del alojamiento. Utilice los siguientes permisos además de los permisos para alojamientos anteriores.

La consola utiliza las siguientes operaciones de IAM cuando realiza el registro de alojamiento basado en navegador. `RegisterAppCode` y `StartAppRegistrationHandshake` son permisos de política de IAM. No son acciones de API.

```
codestar-connections:RegisterAppCode
codestar-connections:StartAppRegistrationHandshake
```

En función de esto, se necesitan los siguientes permisos para utilizar, crear, actualizar o eliminar una conexión en la consola que requiere un alojamiento (como, por ejemplo, tipos de proveedor 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
```

AWS CodeConnections permisos necesarios para realizar las acciones necesarias para completar la configuración del host

RegisterAppCode

- Acciones: `codestar-connections:RegisterAppCode`

  Se necesita para utilizar la consola para completar la configuración del alojamiento. Se trata únicamente de un permiso de política de IAM, no de una acción de API.

  Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

StartAppRegistrationHandshake

- Acciones: `codestar-connections:StartAppRegistrationHandshake`

Se necesita para utilizar la consola para completar la configuración del alojamiento. Se trata únicamente de un permiso de política de IAM, no de una acción de API.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

Estas operaciones admiten las siguientes claves de condición.

Pasar una conexión a un servicio

Cuando se pasa una conexión a un servicio (por ejemplo, cuando se proporciona un ARN de conexión en una definición de canalización para crear o actualizar una canalización), el usuario debe tener el permiso `codestar-connections:PassConnection`.

AWS CodeConnections permisos necesarios para transferir una conexión

PassConnection

Acciones: `codestar-connections:PassConnection`

Se necesita para pasar una conexión a un servicio.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Esta operación también admite la siguiente clave de condición:

- `codestar-connections:PassedToService`

Valores admitidos para claves de condición

Clave	Proveedores válidos de la acción
`codestar-connections:PassedToService`	• `codeguru-reviewer` • `codepipeline.amazonaws.com` • `proton.amazonaws.com`

Uso de una conexión

Cuando un servicio como este CodePipeline usa una conexión, el rol del servicio debe tener el `codestar-connections:UseConnection` permiso para una conexión determinada.

Para administrar las conexiones en la consola, la política de usuario debe tener el permiso `codestar-connections:UseConnection`.

AWS CodeConnections acción necesaria para utilizar una conexión

UseConnection

Acciones: `codestar-connections:UseConnection`

Se necesita para utilizar una conexión.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Esta operación también admite las siguientes claves de condición:

- `codestar-connections:BranchName`
- `codestar-connections:FullRepositoryId`
- `codestar-connections:OwnerId`
- `codestar-connections:ProviderAction`
- `codestar-connections:ProviderPermissionsRequired`
- `codestar-connections:RepositoryName`

Valores admitidos para claves de condición

Clave	Proveedores válidos de la acción
`codestar-connections:FullRepositoryId`	Nombre de usuario y nombre de repositorio de un repositorio, como `my-owner/my-repository` . Se admite solo cuando la conexión se utiliza para obtener acceso a un repositorio específico.

Clave	Proveedores válidos de la acción
`codestar-connections:ProviderPermissionsRequired`	read_only o read_write
`codestar-connections:ProviderAction`	`GetBranch` , `ListRepositories` , `ListOwners` , `ListBranches` , `StartUploadArchiveToS3` , `GitPush`, `GitPull`, `GetUploadArchiveToS3Status` , `CreatePullRequestDiffComment` , `GetPullRequest` , `ListBranchCommits` , `ListCommitFiles` , `ListPullRequestComments` , `ListPullRequestCommits` . Para obtener información, consulte la siguiente sección.

Las claves de condición necesarias para algunas funciones pueden cambiar con el tiempo. Es recomendable que utilice `codestar-connections:UseConnection` para controlar el acceso a una conexión, a menos que sus requisitos de control de acceso requieran permisos diferentes.

Tipos de acceso admitidos para **`ProviderAction`**

Cuando un AWS servicio utiliza una conexión, se realizan llamadas a la API a su proveedor de código fuente. Por ejemplo, un servicio puede mostrar los repositorios para una conexión de Bitbucket llamando a la API `https://api.bitbucket.org/2.0/repositories/`*`username`*.

La clave de condición `ProviderAction` le permite restringir las API de un proveedor a las que se puede llamar. Como la ruta de la API se puede generar de forma dinámica y varía de un proveedor a otro, el valor `ProviderAction` se mapea a un nombre de acción abstracto en lugar de a la URL de la API. Esto le permite escribir políticas que tengan el mismo efecto independientemente del tipo de proveedor de la conexión.

A continuación, se encuentran los tipos de acceso que se conceden para cada uno de los valores `ProviderAction` admitidos. A continuación, se presentan permisos de política de IAM. No son acciones de API.

AWS CodeConnections tipos de acceso compatibles para **`ProviderAction`**

GetBranch

Acciones: `codestar-connections:GetBranch`

Se necesita para acceder a la información sobre una ramificación, como, por ejemplo, la última confirmación de esa ramificación.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListRepositories

Acciones: `codestar-connections:ListRepositories`

Se necesita para acceder a una lista de repositorios públicos y privados, incluidos los detalles de esos repositorios, que pertenecen a un propietario.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListOwners

Acciones: `codestar-connections:ListOwners`

Se necesita para acceder a una lista de propietarios a los que la conexión tiene acceso.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListBranches

Acciones: `codestar-connections:ListBranches`

Se necesita para acceder a la lista de ramificaciones que existen en un repositorio determinado.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

StartUploadArchiveToS3

Acciones: `codestar-connections:StartUploadArchiveToS3`

Se necesita para leer el código fuente y cargarlo en Amazon S3.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GitPush

Acciones: `codestar-connections:GitPush`

Se necesita para escribir en un repositorio con Git.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GitPull

Acciones: `codestar-connections:GitPull`

Se necesita para leer desde un repositorio con Git.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetUploadArchiveToEstado S3

Acciones: `codestar-connections:GetUploadArchiveToS3Status`

Se necesita para acceder al estado de una carga, incluidos los mensajes de error, iniciada por `StartUploadArchiveToS3`.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

CreatePullRequestDiffComment

Acciones: `codestar-connections:CreatePullRequestDiffComment`

Se necesita para acceder a los comentarios de una solicitud de extracción.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetPullRequest

Acciones: `codestar-connections:GetPullRequest`

Se necesita para ver las solicitudes de extracción de un repositorio.

Recurso:`arn:aws:codestar-connections:region:account-id:connection/connection-id`

ListBranchCommits

Acciones: `codestar-connections:ListBranchCommits`

Se necesita para ver una lista de confirmaciones de una ramificación de repositorio.

Recurso:`arn:aws:codestar-connections:region:account-id:connection/connection-id`

ListCommitFiles

Acciones: `codestar-connections:ListCommitFiles`

Se necesita para ver una lista de archivos de una confirmación.

Recurso:`arn:aws:codestar-connections:region:account-id:connection/connection-id`

ListPullRequestComments

Acciones: `codestar-connections:ListPullRequestComments`

Se necesita para ver una lista de comentarios de una solicitud de extracción.

Recurso:`arn:aws:codestar-connections:region:account-id:connection/connection-id`

ListPullRequestCommits

Acciones: `codestar-connections:ListPullRequestCommits`

Se necesita para ver una lista de confirmaciones de una solicitud de extracción.

Recurso:`arn:aws:codestar-connections:region:account-id:connection/connection-id`

Permisos compatibles con el etiquetado de recursos de conexión

Las siguientes operaciones de IAM se utilizan al etiquetar los recursos de conexión.

```
codestar-connections:ListTagsForResource
codestar-connections:TagResource
codestar-connections:UntagResource
```

AWS CodeConnections acciones necesarias para etiquetar los recursos de conexión

ListTagsForResource

Acciones: `codestar-connections:ListTagsForResource`

Se necesita para ver una lista de etiquetas asociadas al recurso de conexión.

Recurso:`arn:aws:codestar-connections:`*region*`:`*account-id*`:connection/`*connection-id*, `arn:aws:codestar-connections:`*region*`:`*account-id*`:host/`*host-id*

TagResource

Acciones: `codestar-connections:TagResource`

Se necesita para etiquetar un recurso de conexión.

Recurso:`arn:aws:codestar-connections:`*region*`:`*account-id*`:connection/`*connection-id*, `arn:aws:codestar-connections:`*region*`:`*account-id*`:host/`*host-id*

UntagResource

Acciones: `codestar-connections:UntagResource`

Se necesita para eliminar etiquetas de un recurso de conexión.

Recurso:`arn:aws:codestar-connections:`*region*`:`*account-id*`:connection/`*connection-id*, `arn:aws:codestar-connections:`*region*`:`*account-id*`:host/`*host-id*

Pasar una conexión a un enlace de repositorio

Cuando se proporciona un enlace al repositorio en una configuración de sincronización, el usuario debe tener el permiso `codestar-connections:PassRepository` para el ARN o recurso del enlace al repositorio.

AWS CodeConnections permisos necesarios para transferir una conexión

PassRepository

Acciones: `codestar-connections:PassRepository`

Necesario para pasar un enlace de repositorio a una configuración de sincronización.

Recurso:`arn:aws:codestar-connections:`*`region`*`:`*`account-id`*`:repository-link/`*`repository-link-id`*

Esta operación también admite la siguiente clave de condición:

- `codestar-connections:PassedToService`

Valores admitidos para claves de condición

Clave	Proveedores válidos de la acción
`codestar-connections:PassedToService`	• `cloudformation.sync.codeconnections.amazonaws.com`

Clave de condición compatible para los enlaces de repositorios

La siguiente clave de condición admite las operaciones de los enlaces de repositorio y los recursos de configuración de sincronización:

- `codestar-connections:Branch`

  Filtra el acceso por el nombre de ramificación que se incluye en la solicitud.

Acciones compatibles con la clave de condición

Clave	Valores válidos
`codestar-connections:Branch`	Esta clave de condición admite las siguientes acciones: • CreateSyncConfiguration • UpdateSyncConfiguration

Clave	Valores válidos
	• GetRepositorySyncStatus

Ejemplos de políticas basadas en identidades

De forma predeterminada, los usuarios y roles de IAM que tienen una de las políticas gestionadas o AWS CodePipeline aplicada tienen permisos para AWS CodeCommit las conexiones, las notificaciones y las reglas de notificación que se ajustan a la intención de esas políticas. AWS CodeBuild AWS CodeDeploy Por ejemplo, los usuarios o roles de IAM a los que se les haya aplicado una de las políticas de acceso total (AWSCodeCommitFullAccessAWSCodeBuildAdminAccessAWSCodeDeployFullAccess,, o AWSCodePipeline_FullAccess) también tienen acceso total a las notificaciones y a las reglas de notificación creadas para los recursos de esos servicios.

Otros usuarios y roles de IAM no tienen permiso para crear o modificar los recursos de AWS CodeStar Notificaciones y AWS CodeStar Conexiones. Tampoco pueden realizar tareas mediante la AWS API AWS Management Console AWS CLI, o. Un administrador de IAM debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API en los recursos específicos que necesiten. El administrador debe asociar esas políticas a los usuarios o grupos de IAM que necesiten esos permisos.

Permisos y ejemplos de AWS CodeStar notificaciones

Las siguientes declaraciones y ejemplos de políticas pueden ayudarle a gestionar AWS CodeStar las notificaciones.

Permisos relacionados con las notificaciones en políticas administradas de acceso total

Las políticas administradas AWSCodeCommitFullAccessAWSCodeBuildAdminAccessAWSCodeDeployFullAccess, y las políticas AWSCodePipeline_FullAccessadministradas incluyen las siguientes declaraciones para permitir el acceso total a las notificaciones en la consola de herramientas para desarrolladores. Los usuarios con una de estas políticas administradas aplicadas también pueden crear y administrar temas de Amazon SNS para notificaciones, suscribirse y cancelar la suscripción a los temas, y enumerar temas para elegir como destinos para las reglas de notificación.

> **Note**
>
> En la política administrada, la clave de condición `codestar-notifications:NotificationsForResource` tendrá un valor específico para el tipo de recurso del servicio. Por ejemplo, en la política de acceso total de CodeCommit, el valor es `arn: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": "*"
    }
```

Permisos relacionados con las notificaciones en políticas administradas de solo lectura

Las políticas AWSCodeCommitReadOnlyAccess, AWSCodeBuildReadOnlyAccessAWSCodeDeployReadOnlyAccess, y AWSCodePipeline_ReadOnlyAccessgestionadas incluyen las siguientes instrucciones para permitir el acceso de solo lectura a las notificaciones. Por ejemplo, pueden ver notificaciones de recursos en la consola de herramientas para desarrolladores, pero no pueden crearlas, administrarlas ni suscribirse a ellas.

> **Note**
>
> En la política administrada, la clave de condición `codestar-notifications:NotificationsForResource` tendrá un valor específico para el tipo de recurso del servicio. Por ejemplo, en la política de acceso total de CodeCommit, el valor es. `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": "*"
    }
```

Permisos relacionados con las notificaciones en otras políticas administradas

Las políticas AWSCodeBuildDeveloperAccessadministradas AWSCodeCommitPowerUserAWSCodeBuildDeveloperAccess, y las administradas incluyen las siguientes declaraciones para permitir a los desarrolladores que tengan aplicada una de estas políticas administradas crear, editar y suscribirse a las notificaciones. No pueden eliminar reglas de notificación ni administrar etiquetas para recursos.

> **Note**
>
> En la política administrada, la clave de condición `codestar-notifications:NotificationsForResource` tendrá un valor específico para el tipo de recurso del servicio. Por ejemplo, en la política de acceso total de CodeCommit, el valor es`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": "*"
    }
```

Ejemplo: una política a nivel de administrador para gestionar las notificaciones AWS CodeStar

En este ejemplo, desea conceder a un usuario de IAM de su AWS cuenta acceso completo a AWS CodeStar las notificaciones para que pueda revisar los detalles de las reglas de notificación y enumerar las reglas de notificación, los objetivos y los tipos de eventos. También desea permitir al usuario añadir, actualizar y eliminar reglas de notificación. Se trata de una política de acceso total, equivalente a los permisos de notificación incluidos como parte de las políticas AWSCodeBuildAdminAccessAWSCodeCommitFullAccess, AWSCodeDeployFullAccess, y AWSCodePipeline_FullAccessgestionadas. Al igual que esas políticas gestionadas, solo debes adjuntar este tipo de declaración de política a los usuarios, grupos o funciones de IAM que requieran un acceso administrativo total a las notificaciones y a las reglas de notificación de tu AWS cuenta.

> **Note**
>
> Esta política incluye permisos para `CreateNotificationRule`. Cualquier usuario que aplique esta política a su usuario o rol de IAM podrá crear reglas de notificación para todos los tipos de recursos compatibles con las AWS CodeStar notificaciones de la AWS cuenta, incluso si ese usuario no tiene acceso a esos recursos por sí mismo. Por ejemplo, un usuario con esta política podría crear una regla de notificación para un CodeCommit repositorio sin tener permisos de acceso a CodeCommit sí mismo.

```
{
    "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": "*"
      }
   ]
}
```

Ejemplo: una política a nivel de colaborador para usar las notificaciones AWS CodeStar

En este ejemplo, quieres conceder acceso al day-to-day uso de AWS CodeStar las notificaciones, como la creación de notificaciones y la suscripción a ellas, pero no a acciones más destructivas, como eliminar las reglas o los objetivos de las notificaciones. Esto equivale al acceso que se proporciona en las políticas AWSCodeCommitPowerUseradministradas y AWSCodeBuildDeveloperAccessAWSCodeDeployDeveloperAccess,

> **Note**
>
> Esta política incluye permisos para `CreateNotificationRule`. Cualquier usuario que tenga esta política aplicada a su usuario o rol de IAM podrá crear reglas de notificación para todos y cada uno de los tipos de recursos compatibles con AWS CodeStar las notificaciones de la AWS cuenta, incluso si ese usuario no tiene acceso a esos recursos por sí mismo. Por ejemplo, un usuario con esta política podría crear una regla de notificación para un CodeCommit repositorio sin tener permisos de acceso a CodeCommit sí mismo.

```
{
    "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": "*"
        }
```

```
    ]
}
```

Ejemplo: una read-only-level política para usar AWS CodeStar las notificaciones

En este ejemplo, desea conceder a un usuario de IAM de su cuenta acceso de solo lectura a las reglas de notificación, los destinos y los tipos de eventos de su cuenta de AWS . En este ejemplo se muestra cómo crear una política que permita visualizar estos elementos. Esto equivale a los permisos incluidos como parte de las AWSCodeBuildReadOnlyAccesspolíticas AWSCodePipeline_ReadOnlyAccessadministradas y las políticas administradas. 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": "*"
        }
    ]
}
```

Permisos y ejemplos de AWS CodeConnections

Los siguientes ejemplos e instrucciones de política pueden ayudarlo a administrar AWS CodeConnections.

Para obtener más información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas de JSON de ejemplo, consulte Creación de políticas en la pestaña JSON en la Guía del usuario de IAM.

Ejemplo: una política para crear AWS CodeConnections con la CLI y ver con la consola

Un rol o usuario designado para usar el SDK AWS CLI o el SDK para ver, crear, etiquetar o eliminar conexiones debe tener permisos limitados a lo siguiente.

> **Note**
>
> No puede completar una conexión en la consola solo con los permisos siguientes. Debe agregar los permisos en la siguiente sección.

Para utilizar la consola para ver una lista de las conexiones disponibles, ver etiquetas y usar una conexión, utilice la política siguiente.

```
{
    "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": "*"
      }
   ]
}
```

Ejemplo: una política para crear AWS CodeConnections con la consola

Un rol o un usuario designado para administrar conexiones en la consola debe tener los permisos necesarios para completar una conexión en la consola y crear una instalación, lo que incluye autorizar el protocolo de enlace al proveedor y crear instalaciones para que se utilicen las

conexiones. `UseConnection` también se debe agregar para usar la conexión en la consola. Utilice la siguiente política para ver, utilizar, crear, etiquetar o eliminar una conexión en la consola.

```
{
    "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": [
                "*"
            ]
        }
    ]
}
```

Ejemplo: una política de administración a nivel de administrador AWS CodeConnections

En este ejemplo, desea conceder a un usuario de IAM de su AWS cuenta acceso completo para que CodeConnections pueda añadir, actualizar y eliminar conexiones. Se trata de una política de acceso total, equivalente a la política AWSCodePipeline_FullAccessgestionada. Al igual que esa política gestionada, solo debes adjuntar este tipo de declaración de política a los usuarios, grupos o funciones de IAM que requieran un acceso administrativo total a las conexiones de tu AWS cuenta.

```
{
    "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": "*"
     }
   ]
}
```

Ejemplo: una política de uso a nivel de colaborador AWS CodeConnections

En este ejemplo, desea conceder acceso al day-to-day uso de, por ejemplo CodeConnections, la creación y la visualización de los detalles de las conexiones, pero no a acciones más destructivas, como la eliminación de conexiones.

```
{
    "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": "*"
        }
    ]
}
```

Ejemplo: una read-only-level política de uso AWS CodeConnections

En este ejemplo, desea conceder a un usuario de IAM de su cuenta acceso de solo lectura a las conexiones de su cuenta. AWS En este ejemplo se muestra cómo crear una política que permita visualizar estos elementos.

```
{
    "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": "*"
        }
    ]
}
```

Ejemplo: una política restringida para usarla con un repositorio específico AWS CodeConnections

En el siguiente ejemplo, el cliente quiere que la función de CodeBuild servicio acceda al repositorio de Bitbucket especificado. La política sobre el rol CodeBuild de servicio:

```
{
    "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"}}
    }
}
```

Ejemplo: una política para usar una conexión con CodePipeline

En el ejemplo siguiente, un administrador quiere que los usuarios usen una conexión con CodePipeline. La política adjunta al usuario:

```
{
    "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"}}
    }
}
```

Ejemplo: usa un rol de CodeBuild servicio para las operaciones de lectura de Bitbucket con AWS CodeConnections

En el siguiente ejemplo, el cliente quiere que la función de CodeBuild servicio realice operaciones de lectura en Bitbucket, independientemente del repositorio. La política sobre el rol CodeBuild de servicio:

```
{
    "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"}}
    }
}
```

Ejemplo: limite la función CodeBuild de servicio para que no realice operaciones con AWS CodeConnections

En el siguiente ejemplo, el cliente quiere impedir que la función de CodeBuild servicio realice una operación similar`CreateRepository`. La política sobre la función CodeBuild de servicio:

```
{
    "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"}}
    }
}
```

Uso de etiquetas para controlar el acceso a los recursos de AWS CodeStar Connections

Las etiquetas se pueden asociar al recurso o pasarse dentro de la solicitud a los servicios que admiten etiquetado. En CodeConnections, los recursos pueden tener etiquetas y algunas acciones pueden incluirlas. Cuando crea una política de IAM, puede utilizar claves de condición de etiqueta para controlar lo siguiente:

- Qué usuarios pueden realizar acciones en un recurso de canalización, basándose en las etiquetas que ya tiene.
- Qué etiquetas se pueden pasar en la solicitud de una acción.
- Si se pueden utilizar claves de etiqueta específicas en una solicitud.

Los siguientes ejemplos muestran cómo especificar las condiciones de etiqueta en las políticas para los usuarios de CodeConnections .

Example 1: permitir acciones en función de las etiquetas en la solicitud

La siguiente política concede a los usuarios permiso para crear conexiones en CodeConnections.

Para ello, permite las acciones `CreateConnection` y `TagResource` si la solicitud especifica una etiqueta denominada `Project` con el valor `ProjectA`. (La clave de condición `aws:RequestTag` se utiliza para controlar qué etiquetas se pueden pasar en una solicitud de IAM). La condición `aws:TagKeys` garantiza la distinción entre mayúsculas y minúsculas de las claves de etiqueta.

```
{
  "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 acciones en función de las etiquetas de recursos

La siguiente política concede a los usuarios permiso para realizar acciones en los recursos de CodeConnections y obtener información sobre ellos.

Para ello, permite realizar determinadas acciones si la canalización tiene una etiqueta denominada `Project` con el valor `ProjectA`. (La clave de condición `aws:RequestTag` se utiliza para controlar

qué etiquetas se pueden pasar en una solicitud de IAM). La condición `aws:TagKeys` garantiza la distinción entre mayúsculas y minúsculas de las claves de etiqueta.

```
{
  "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 notificaciones y conexiones en la consola

La experiencia de notificaciones está integrada en las CodePipeline consolas CodeBuild CodeCommit, CodeDeploy, y, además, en la consola Developer Tools, situada en la propia barra de navegación de configuración. Para tener acceso a las notificaciones de las consolas, debe tener aplicada una de las políticas administradas para esos servicios o tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de AWS CodeStar notificaciones y AWS CodeStar conexiones de su AWS cuenta. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles de IAM) que tengan esa política. Para obtener más información sobre cómo conceder acceso a esas consolas e AWS CodeBuild AWS CodeCommit AWS CodeDeploy AWS CodePipeline, incluido el acceso a ellas, consulte los siguientes temas:

- CodeBuild: Utilizar políticas basadas en la identidad para CodeBuild

- CodeCommit: Utilizar políticas basadas en la identidad para CodeCommit
- AWS CodeDeploy: Gestión de identidad y acceso para AWS CodeDeploy
- CodePipeline: Control de acceso con políticas de IAM

AWS CodeStar Las notificaciones no tienen ninguna política AWS gestionada. Para proporcionar acceso a la funcionalidad de notificación, debe aplicar una de las políticas administradas para uno de los servicios enumerados anteriormente o debe crear políticas con el nivel de permiso que desea conceder a los usuarios o entidades y, luego, adjuntar esas políticas a los usuarios, los grupos o los roles que necesitan esos permisos. Para obtener más información y ejemplos, consulte lo siguiente:

- Ejemplo: una política a nivel de administrador para gestionar las notificaciones AWS CodeStar
- Ejemplo: una política a nivel de colaborador para usar las notificaciones AWS CodeStar
- Ejemplo: una read-only-level política para usar AWS CodeStar las notificaciones.

AWS CodeStar Connections no tiene políticas AWS administradas. Utilice los permisos y las combinaciones de permisos de acceso, como los permisos detallados en Permisos para completar conexiones.

Para más información, consulte los siguientes temas:

- Ejemplo: una política de administración a nivel de administrador AWS CodeConnections
- Ejemplo: una política de uso a nivel de colaborador AWS CodeConnections
- Ejemplo: una read-only-level política de uso AWS CodeConnections

No es necesario que concedas permisos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o 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": "*"
        }
    ]
}
```

Solución de problemas de identidad y acceso a AWS CodeStar notificaciones y AWS CodeStar conexiones

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con notificaciones e IAM.

Temas

- Soy administrador y quiero permitir que otros obtengan acceso a las notificaciones

- Creé un tema de Amazon SNS y lo agregué como destino de regla de notificación, pero no recibo emails sobre eventos
- Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos de AWS CodeStar notificaciones y AWS CodeStar conexiones

Soy administrador y quiero permitir que otros obtengan acceso a las notificaciones

Para permitir que otras personas accedan a AWS CodeStar las notificaciones y AWS CodeStar conexiones, debe crear una entidad de IAM (usuario o rol) para la persona o aplicación a la que necesita acceso. Esta persona utilizará las credenciales de la entidad para acceder a AWS. A continuación, debe adjuntar una política a la entidad que le conceda los permisos correctos en AWS CodeStar Notificaciones y AWS CodeStar conexiones.

Para comenzar de inmediato, consulte Creación del primer grupo y usuario delegado de IAM en la Guía del usuario de IAM.

Para obtener información específica sobre AWS CodeStar las notificaciones, consultePermisos y ejemplos de AWS CodeStar notificaciones.

Creé un tema de Amazon SNS y lo agregué como destino de regla de notificación, pero no recibo emails sobre eventos

Para recibir notificaciones sobre eventos, debe tener un tema de Amazon SNS válido suscrito como destino para la regla de notificación y su dirección de email debe estar suscrita al tema de Amazon SNS. Para solucionar problemas con el tema de Amazon SNS, verifique lo siguiente:

- Asegúrese de que el tema de Amazon SNS esté en la misma AWS región que la regla de notificación.
- Asegúrese de que su alias de correo electrónico está suscrito al tema correcto y de que ha confirmado la suscripción. Para obtener más información, consulte Suscripción de un punto de enlace a un tema de Amazon SNS.
- Compruebe que la política temática se haya modificado para permitir que AWS CodeStar Notifications envíe notificaciones a ese tema. La política de temas debe incluir una instrucción similar a la siguiente:

```
{
    "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 obtener más información, consulte Configuración.

Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos de AWS CodeStar notificaciones y AWS CodeStar conexiones

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si AWS CodeStar Notifications and AWS CodeStar Connections admite estas funciones, consulteCómo funcionan las características de la consola de herramientas para desarrolladores con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.

- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Uso de roles vinculados a servicios para AWS CodeStar Notifications

AWS CodeStar Notifications utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado de forma directa a AWS CodeStar Notifications. Los roles vinculados a servicios están predefinidos por AWS CodeStar Notifications e incluyen todos los permisos que el servicio necesita para llamar a otros servicios de AWS en su nombre. Este rol se crea la primera vez que crea una regla de notificación. No es preciso crear el rol.

Un rol vinculado a servicios simplifica la configuración de AWS CodeStar Notifications porque ya no tendrá que agregar de forma manual los permisos necesarios. AWS CodeStar Notifications define los permisos de los roles vinculados a servicios y, a menos que esté definido de otra manera, solo AWS CodeStar Notifications puede asumir los roles. Los permisos definidos incluyen las políticas de confianza y de permisos y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Para eliminar un rol vinculado a servicios, primero debe eliminar sus recursos relacionados. De esta forma, se protegen los recursos de AWS CodeStar Notifications, ya que se evita que se puedan eliminar de forma accidental permisos de acceso a los recursos.

Para obtener más información sobre otros servicios que admiten los roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM.

Permisos de roles vinculados a servicios para AWS CodeStar Notifications

AWS CodeStar Notifications utiliza el rol AWSServiceRoleForCodeStarNotifications vinculado a servicios para recuperar información sobre los eventos que se producen en la cadena de herramientas y enviar notificaciones a los destinos especificados.

El rol AWSServiceRoleForCodeStarNotifications vinculado a servicios confía en que los siguientes servicios asuman el rol:

- `codestar-notifications.amazonaws.com`

La política de permisos del rol permite que AWS CodeStar Notifications complete las siguientes acciones en los recursos especificados:

- Acción: `PutRule` en `CloudWatch Event rules that are named awscodestar-notifications-*`
- Acción: `DescribeRule` en `CloudWatch Event rules that are named awscodestar-notifications-*`
- Acción: `PutTargets` en `CloudWatch Event rules that are named awscodestar-notifications-*`
- Acción: `CreateTopic` para `create Amazon SNS topics for use with AWS CodeStar Notifications with the prefix CodeStarNotifications-`
- Acción: `GetCommentsForPullRequests` en `all comments on all pull requests in all CodeCommit repositories in the AWS account`
- Acción: `GetCommentsForComparedCommit` en `all comments on all commits in all CodeCommit repositories in the AWS account`
- Acción: `GetDifferences` en `all commits in all CodeCommit repositories in the AWS account`
- Acción: `GetCommentsForComparedCommit` en `all comments on all commits in all CodeCommit repositories in the AWS account`
- Acción: `GetDifferences` en `all commits in all CodeCommit repositories in the AWS account`
- Acción: `DescribeSlackChannelConfigurations` en `all AWS Chatbot clients in the AWS account`
- Acción: `UpdateSlackChannelConfiguration` en `all AWS Chatbot clients in the AWS account`
- Acción: `ListActionExecutions` en `all actions in all pipelines in the AWS account`
- Acción: `GetFile` en `all files in all CodeCommit repositories in the AWS account unless otherwise tagged`

Puede ver estas acciones en la instrucción de política para el rol AWSServiceRoleForCodeStarNotifications vinculado a servicios.

```
{
```

```
    "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"
        }
    ]
```

```
}
```

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a servicios para AWS CodeStar Notifications

No necesita crear manualmente un rol vinculado a servicios. Puede utilizar la consola de herramientas para desarrolladores o la API CreateNotificationRule de los SDK para crear una regla de notificación. También puede llamar de forma directa a la API. No importa el método utilizado, el rol vinculado a servicios se crea de forma automática.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Puede utilizar la consola de herramientas para desarrolladores o la API CreateNotificationRule de los SDK para crear una regla de notificación. También puede llamar de forma directa a la API. No importa el método utilizado, el rol vinculado a servicios se crea de forma automática.

Edición de un rol vinculado a servicios para AWS CodeStar Notifications

Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin embargo, puede utilizar IAM para editar la descripción del rol. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a servicios para AWS CodeStar Notifications

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine el rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Debe limpiar los recursos del rol vinculado a servicio antes de eliminarlo. En AWS CodeStar Notifications, esto significa eliminar todas las reglas de notificación que utilizan el rol de servicio en su cuenta de AWS.

> **Note**
>
> Si el servicio AWS CodeStar Notifications está utilizando el rol cuando intenta eliminar los recursos, la eliminación podría fallar. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar recursos de AWS CodeStar Notifications utilizados por AWSServiceRoleForCodeStarNotifications

1. Abra la consola de las herramientas para desarrolladores de AWS en https://console.aws.amazon.com/codesuite/settings/notifications.

   > **Note**
   >
   > Las reglas de notificación son específicas de la región de AWS en la que se crean. Si tiene reglas de notificación en más de una región de AWS, utilice el selector de región para cambiar la Región de AWS.

2. Elija todas las reglas de notificación que aparecen en la lista y, a continuación, elija Delete (Eliminar).
3. Repita estos pasos en todas las regiones de AWS en las que ha creado reglas de notificación.

Para utilizar IAM para eliminar el rol vinculado a servicios

Utilice la consola de IAM, la AWS CLI o la API de AWS Identity and Access Management para eliminar el rol AWSServiceRoleForCodeStarNotifications vinculado a servicios. Para obtener más información, consulte Eliminar un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles para roles vinculados a servicios de AWS CodeStar Notifications

AWS CodeStar Notifications admite el uso de roles vinculados a servicios en todas las regiones de AWS donde el servicio está disponible. Para obtener más información, consulte Regiones y puntos de conexión de AWS y AWS CodeStar Notifications.

Uso de roles vinculados a servicios de AWS CodeConnections

AWS CodeConnections utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a AWS CodeConnections. Los roles vinculados a servicios están predefinidos por AWS CodeConnections e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre. Este rol se crea la primera vez que crea una conexión. No es preciso crear el rol.

Con un rol vinculado a un servicio, resulta más sencillo configurar AWS CodeConnections, porque no es preciso agregar los permisos necesarios manualmente. AWS CodeConnections define los permisos de los roles vinculados con su propio servicio y, a menos que esté definido de otra manera, solo AWS CodeConnections puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Para eliminar un rol vinculado a servicios, primero debe eliminar sus recursos relacionados. De esta forma, se protegen los recursos de AWS CodeConnections, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener más información sobre otros servicios que admiten los roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM.

Permisos de roles vinculados a servicios de AWS CodeConnections

AWS CodeConnections usa el rol vinculado al servicio AWSServiceRoleForGitSync para usar la sincronización de Git con los repositorios conectados basados en Git.

El rol vinculado a servicios AWSServiceRoleForGitSync confía los siguientes servicios para asumir el rol:

- `repository.sync.codeconnections.amazonaws.com`

La política de permisos del rol denominada AWSGitSyncServiceRolePolicy permite a AWS CodeConnections completar las siguientes acciones en los recursos especificados:

- Acción: Concede permisos para permitir a los usuarios crear conexiones a los repositorios basados en Git externos y usar la sincronización de Git con esos repositorios.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio de AWS CodeConnections

No necesita crear manualmente un rol vinculado a servicios. El rol se crea al crear un recurso para el proyecto sincronizado con Git con la API CreateRepositoryLink.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta.

Modificación de un rol vinculado a un servicio de AWS CodeConnections

Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin embargo, puede utilizar IAM para editar la descripción del rol. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de AWS CodeConnections

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine el rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Debe limpiar los recursos del rol vinculado a servicio antes de eliminarlo. Esto significa eliminar todas las conexiones que utilizan el rol de servicio en la cuenta de AWS.

> **Note**
>
> Si el servicio AWS CodeConnections está utilizando el rol cuando intenta eliminar los recursos, la eliminación podría producir un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de AWS CodeConnections utilizados por AWSServiceRoleForGitSync

1. Abra la consola de herramientas para desarrolladores y, a continuación, elija Configuración.
2. Elija todas las conexiones que aparecen en la lista y, a continuación, elija Eliminar.
3. Repita estos pasos en todas las regiones de AWS en las que ha creado conexiones.

Para utilizar IAM para eliminar el rol vinculado a servicios

Utilice la consola de IAM, la AWS CLI o la API de AWS Identity and Access Management para eliminar el rol vinculado a servicios AWSServiceRoleForGitSync. Para obtener más información, consulte Eliminar un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de AWS CodeConnections

AWS CodeConnections admite el uso de roles vinculados a servicios en todas las regiones de AWS en las que el servicio esté disponible. Para obtener más información, consulte Regiones y puntos de conexión de AWS.

Políticas administradas de AWS para AWS CodeConnections

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

Tenga presente que es posible que las políticas administradas de AWS no concedan permisos de privilegio mínimo para los casos de uso concretos, ya que están disponibles para que las utilicen todos los clientes de AWS. Se recomienda definir políticas administradas por el cliente para los casos de uso a fin de reducir aún más los permisos.

No puede cambiar los permisos definidos en las políticas administradas de AWS. Si AWS actualiza los permisos definidos en un política administrada de AWS, la actualización afecta a todas las identidades de entidades principales (usuarios, grupos y roles) a las que está adjunta la política. Lo más probable es que AWS actualice una política administrada de AWS cuando se lance un nuevo Servicio de AWS o las operaciones de la API nuevas estén disponibles para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

Política administrada por AWS: AWSGitSyncServiceRolePolicy

No puede asociar AWSGitSyncServiceRolePolicy a las entidades de IAM. Esta política está adjunta a un rol vinculado a servicios que permite a AWS CodeConnections realizar acciones en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios de AWS CodeConnections.

Esta política permite a los clientes acceder a los repositorios basados en Git para usarlos con las conexiones. Los clientes accederán a estos recursos después de usar la API de CreateRepositoryLink.

Detalles sobre los permisos

Esta política incluye los siguientes permisos.

- `codestar-connections`: concede permisos para permitir a los usuarios crear conexiones a repositorios externos basados en 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}"
    }
   }
  }
 ]
}
```

Actualizaciones de AWS CodeConnections en las políticas administradas de AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas de AWS para AWS CodeConnections debido a que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de AWS CodeConnections.

Cambio	Descripción	Fecha
AWSGitSyncServiceRolePolicy: nueva política	AWS CodeConnections agregó la política. Concede permisos para permitir a los usuarios de AWS CodeConnections usar la sincronización de Git con los repositorios conectados basados en Git.	26 de noviembre de 2023
AWS CodeConnections comenzó el seguimiento de los cambios	AWS CodeConnections comenzó el seguimiento de los cambios de las políticas administradas de AWS.	26 de noviembre de 2023

Validación de conformidad para AWS CodeStar notificaciones y AWS CodeStar conexiones

AWS CodeStar Las notificaciones y AWS CodeStar las conexiones no están incluidas en el ámbito de ningún programa de AWS cumplimiento.

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de cumplimiento específicos, consulte AWS los servicios incluidos en el ámbito de aplicación por programa de cumplimiento. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulta Descarga de informes en AWS Artifact.

Su responsabilidad de cumplimiento al utilizar AWS CodeStar Notifications and AWS CodeStar Connections viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS
- AWS recursos de conformidad: esta colección de libros de trabajo y guías puede aplicarse a su sector y ubicación.
- AWS Config— Este AWS servicio evalúa en qué medida las configuraciones de sus recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar el cumplimiento de los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en AWS CodeStar Notifications y AWS CodeStar Connections

La infraestructura global de AWS se compone de regiones y zonas de disponibilidad de AWS. AWS Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las zonas de disponibilidad y las regiones de AWS, consulte Infraestructura global de AWS.

- Las reglas de notificación son específicas de la Región de AWS en la que se crean. Si tiene reglas de notificación en más de una Región de AWS, utilice el selector de región para revisar las reglas de notificación en cada Región de AWS.
- AWS CodeStar Notifications se basa en los temas de Amazon Simple Notification Service (Amazon SNS) como destinos de las reglas de notificación. La información sobre los temas de Amazon SNS y los destinos de las reglas de notificación podrían almacenarse en una región de AWS distinta de aquella en la que ha configurado la regla de notificación.

Seguridad de la infraestructura de AWS CodeStar Notifications y AWS CodeStar Connections

Como se trata de una característica de un servicio administrado, AWS CodeStar Notifications y AWS CodeStar Connections están protegidos por los procedimientos de seguridad de red globales de AWS que se describen en el documento técnico Amazon Web Services: Overview of security processes.

Se utilizan las llamadas a la API publicadas por AWS para obtener acceso a AWS CodeStar Notifications y AWS CodeStar Connections a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.0 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos admiten estos modos.

Las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Tráfico entre los recursos de AWS CodeConnections en las distintas regiones

Si utiliza la característica de conexiones que permite la conexión de sus recursos, usted acepta y nos concede permiso para que almacenemos y procesemos la información asociada a tales recursos de conexión en las Regiones de AWS fuera de las Regiones de AWS en las que esté utilizando el servicio subyacente, únicamente a efectos de proporcionar conexión a esos recursos en regiones distintas de aquella en la que se creó.

Para obtener más información, consulte Recursos globales en AWS CodeStar Connections.

> **Note**
>
> Si utiliza la característica Connections para habilitar la conexión de sus recursos en regiones en las que no es necesario habilitarla primero, almacenaremos y procesaremos la información tal como se detalla en los temas anteriores.

En el caso de las conexiones establecidas en regiones en las que hay que habilitarla primero, como la región Europa (Milán), solo almacenaremos y procesaremos la información de esa conexión en esa región.

Historial del documento

En la siguiente tabla, se describe la documentación de esta versión de la consola de herramientas para desarrolladores.

- Versión de la API de AWS CodeStar Notifications: 2019-10-15
- Versión de la API de AWS CodeStar Connections: 2019-12-01

Cambio	Descripción	Fecha
Compatibilidad con GitLab autoadministrado	Se ha agregado compatibilidad para configurar conexiones y hosts para que los recursos de AWS interactúen con GitLab autoadministrado. Para obtener más información, consulte Flujo de trabajo para crear o actualizar un host y Creación de una conexión a GitLab autoadministrado.	28 de diciembre de 2023
Nuevos enlaces a repositorios y configuraciones de sincronización para las conexiones	Se ha agregado información sobre la configuración de los enlaces a los repositorios y las configuraciones de sincronización. Use la configuración de sincronización para sincronizar el contenido de un repositorio Git y actualizar los recursos de la pila de AWS CloudFormation. Para obtener más información, consulte Cómo trabajar con enlaces de repositorios y	27 de noviembre de 2023

	Cómo trabajar con configuraciones de sincronización.	
Compatibilidad con roles vinculados a servicios de conexiones	Se ha agregado compatibilidad para configurar las conexiones para usar la sincronización de Git con los repositorios de Git. Para obtener más información, consulte Uso de roles vinculados a servicios para AWS CodeStar Connections y Políticas administradas.	26 de noviembre de 2023
Compatibilidad con grupos de GitLab	Se ha añadido compatibilidad para configurar conexiones para que los recursos de AWS interactúen con los grupos de GitLab. Para obtener más información, consulte Crear una conexión y Crear una conexión a GitLab.	15 de septiembre de 2023
Nuevo tipo de proveedor de GitLab	Ahora puede crear conexiones a GitLab. Para obtener más información, consulte Crear una conexión y Crear una conexión a GitLab.	10 de agosto de 2023

Nuevo tipo de destino para reglas de notificación	A partir de ahora, puede elegir clientes de AWS Chatbot configurados para los canales de Microsoft Teams como destino para las reglas de notificación. Para obtener más información, consulte Creación de una regla de notificación y Uso de los destinos de las reglas de notificación.	17 de mayo de 2023
Connections está disponible en la región Europa (Milán)	Se han añadido conexiones en la región de Europa (Milán). Para obtener más información, consulte Tráfico entre los recursos de AWS CodeStar Connections en las distintas regiones.	17 de mayo de 2023
Se ha agregado solución de problemas para errores de conexiones con permisos de repositorio	Al crear una conexión a un repositorio en una organización de GitHub, debe ser el propietario de la organización de GitHub. Para obtener más información, consulte Error de conexiones al conectarse a GitHub.	29 de agosto de 2022
Información agregada para etiquetar recursos de alojamiento	A partir de ahora, puede etiquetar alojamientos mediante la consola y la CLI. Para obtener más información, consulte Recursos de etiqueta en AWS CodeStar Connections.	19 de abril de 2021

Compatibilidad con puntos de conexión de VPC para las conexiones	A partir de ahora, puede utilizar los puntos de enlace de la VPC con las conexiones. Para obtener más información, consulte AWS CodeStar Connections y puntos de conexión de VPC de interfaz (AWS PrivateLink).	24 de noviembre de 2020
Nuevos tipos de proveedores de GitHub y GitHub Enterprise Cloud	A partir de ahora, puede crear conexiones a GitHub y GitHub Enterprise Cloud. Para obtener más información, consulte Creación de una conexión y Creación de una conexión a GitHub.	30 de septiembre de 2020
Recursos de alojamiento y tipo de proveedor de GitHub Enterprise Server agregados	Se ha agregado a esta guía información sobre el recurso de alojamiento para las conexiones. A partir de ahora, puede crear conexiones a GitHub Enterprise Server. Para obtener más información, consulte Creación de una conexión y Trabajo con alojamientos. Esta es la versión de disponibilidad general de la característica de conexiones en la Guía del usuario de la consola de herramientas para desarrolladores.	29 de junio de 2020

Información agregada sobre el uso y el etiquetado de las conexiones	Se ha agregado a esta guía información sobre la característica de las conexiones en la consola. Puede consultar conceptos, pasos necesarios para comenzar, una referencia de permisos que contiene ejemplos de políticas y, además, pasos para crear, visualizar y etiquetar conexiones. Para obtener más información, consulte Qué son las conexiones, Conceptos de conexiones, Introducción a las conexiones, Creación de una conexión, Recursos de etiqueta en AWS CodeStar Connections, Seguridad, Cuotas de las conexiones, Solución de problemas y Llamadas a la API de AWS CodeStar Connections con AWS CloudTrail. Para visualizar una lista de acciones adicionales del proveedor (acciones de solo permisos), consulte Acciones de ProviderType.	28 de junio de 2020

Nuevo tipo de destino para reglas de notificación	A partir de ahora, puede elegir clientes de AWS Chatbot configurados para los canales de Slack como destino para las reglas de notificación. Para obtener más información, consulte Creación de una regla de notificación y Uso de los destinos de las reglas de notificación.	2 de abril de 2020
Se han agregado notificaciones sobre eventos de AWS CodeCommit adicionales	Ahora puede configurar notificaciones para eventos relacionados con las aprobaciones de solicitudes de extracción. Para obtener más información, consulte Eventos para las reglas de notificación de repositorios y Trabajo con solicitudes de extracción en CodeCommit.	10 de febrero de 2020
Notificaciones disponibles en dos regiones de AWS adicionales	La consola de herramientas para desarrolladores ahora admite notificaciones en Medio Oriente (Baréin) y Asia-Pacífico (Hong Kong). Para obtener más información, consulte AWS CodeStar Notifications en la Referencia general de AWS.	5 de febrero de 2020

Compatibilidad agregada con los temas de Amazon SNS cifrados	Se ha agregado una guía para el uso de temas de Amazon SNS cifrados como destinos de notificación. Para obtener más información, consulte Configuración de temas de Amazon SNS para notificaciones .	4 de febrero de 2020
Las notificaciones pueden incluir información de etiqueta de sesión para CodeCommit	Las notificaciones para CodeCommit ahora pueden contener información de identidad del usuario, como un nombre de visualización o una dirección de email, mediante el uso de etiquetas de sesión. Para obtener más informaci ón, consulte Conceptos y Uso de etiquetas para proporcionar información de identidad en CodeCommit.	19 de diciembre de 2019
Versión inicial	Esta es la versión inicial de la Guía del usuario de la consola de herramientas para desarroll adores.	5 de noviembre de 2019

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.