Guida per l'utente

Console Strumenti di sviluppo

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

Console Strumenti di sviluppo: Guida per l'utente

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Che cos'è la console Strumenti di sviluppo? 1
È il primo utilizzo? 3
Caratteristiche della console Strumenti di sviluppo 3
Cosa sono le notifiche? 4
Cosa posso fare con le notifiche? 4
Come funzionano le notifiche? 4
Come posso iniziare a usare le notifiche? 4
Concetti di notifica 5
Configurazione 13
Nozioni di base sulle notifiche 20
Utilizzo delle regole di notifica 27
Utilizzo delle destinazioni delle regole di notifica 40
Configurare l'integrazione tra notifiche e AWS Chatbot 50
Registrazione delle chiamate API di AWS CodeStar notifica con AWS CloudTrail 55
Risoluzione dei problemi 59
Quote 62
Che cosa sono le connessioni? 62
Cosa posso fare con le connessioni? 63
Per quali fornitori di terze parti posso creare connessioni? 63
Cosa si Servizi AWS integra con le connessioni? 64
Come funzionano le connessioni? 64
Risorse globali in AWS CodeConnections 71
Come posso iniziare a usare le connessioni? 71
Concetti di connessione 72
AWS CodeConnections provider e versioni supportati 73
Integrazioni di prodotti e servizi con AWS CodeConnections 74
Configurazione di una connessione 77
Nozioni di base sulle connessioni 80
Utilizzo delle connessioni 86
Utilizzo degli host 148
Utilizzo delle configurazioni di sincronizzazione per i repository collegati 159
Registrazione delle connessioni, chiamate API con CloudTrail 169
Endpoint VPC (AWS PrivateLink) 209
Risoluzione dei problemi relativi alle connessioni 213

Quote 228
Indirizzi IP da aggiungere all'elenco degli indirizzi consentiti 229
Sicurezza 231
Comprendere contenuti e sicurezza delle notifiche 232
Protezione dei dati 233
Gestione dell'identità e degli accessi 234
Destinatari 235
Autenticazione con identità 236
Gestione dell'accesso con policy 239
Come funzionano le caratteristiche nella console degli strumenti di sviluppo con IAM 240
AWS CodeConnections riferimento alle autorizzazioni 246
Esempi di policy basate su identità 261
Utilizzo dei tag per controllare l'accesso alle risorse AWS CodeConnections 273
Utilizzo della console 275
Consentire agli utenti di visualizzare le loro autorizzazioni 276
Risoluzione dei problemi 277
Utilizzo di ruoli collegati ai servizi per le notifiche AWS CodeStar 280
Utilizzo di ruoli collegati ai servizi per AWS CodeConnections 284
AWS politiche gestite 287
Convalida della conformità 290
Resilienza 290
Sicurezza dell'infrastruttura 291
Traffico tra le risorse di AWS CodeConnections tra regioni 291
Rinomina delle connessioni - Riepilogo delle modifiche 293
Prefisso di servizio rinominato 293
Azioni rinominate in IAM 294
Nuova risorsa ARN 294
Politiche relative ai ruoli di servizio interessati 4
Nuova CloudFormation risorsa 4
Cronologia dei documenti 295
AWS Glossario 304
..... cccv

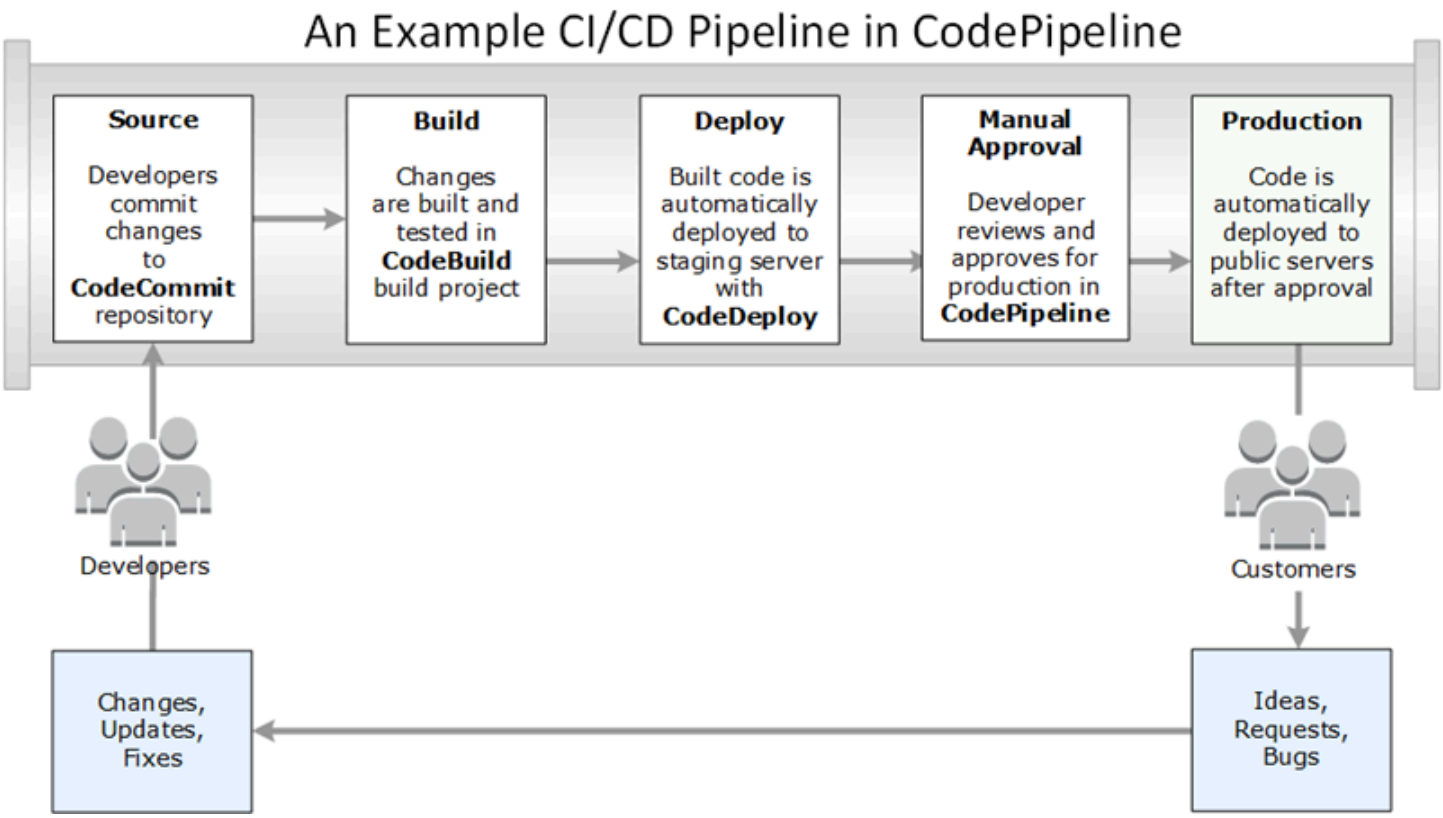
Che cos'è la console Strumenti di sviluppo?

La console Strumenti di sviluppo include una serie di servizi e caratteristiche che puoi utilizzare singolarmente o collettivamente per semplificare lo sviluppo del software, singolarmente o come un team. Gli strumenti di sviluppo possono aiutarti a archiviare, compilare, testare e implementare in modo sicuro il tuo software. Utilizzati singolarmente o collettivamente, questi strumenti forniscono supporto DevOps, integrazione continua e distribuzione continua (CI/CD).

Nella console Strumenti di sviluppo sono disponibili i seguenti servizi:

- AWS CodeCommit è un servizio di controllo del codice sorgente completamente gestito che ospita repository Git privati. È possibile utilizzare i repository per archiviare e gestire in modo privato le risorse, ad esempio documenti, codici sorgente e file binari, nel Cloud AWS. Nei repository è archiviata la cronologia del progetto, dal primo commit fino alle ultime modifiche. Puoi lavorare in modo collaborativo sul codice nei repository commentando il codice e creando richieste pull per garantire la qualità del codice.
- AWS CodeBuild è un servizio di compilazione completamente gestito che permette di compilare il tuo codice sorgente, eseguire unit test e produrre artefatti pronti per essere implementati. Fornisce ambienti di compilazione predefiniti per i linguaggi di programmazione più diffusi e strumenti di compilazione come Apache Maven, Gradle e molti altri. Puoi anche personalizzare gli ambienti di compilazione CodeBuild per utilizzare i tuoi strumenti di compilazione.
- AWS CodeDeployè un servizio di distribuzione completamente gestito che automatizza le distribuzioni di software su servizi di elaborazione come Amazon e sui EC2 server AWS Lambda locali. Semplifica le operazioni di rilascio di nuove caratteristiche, evita i tempi di inattività durante l'implementazione delle applicazioni e gestisce le complesse attività di aggiornamento delle applicazioni.
- AWS CodePipeline è un servizio di integrazione continua e distribuzione continua che può essere utilizzato per modellare, visualizzare e automatizzare le fasi necessarie al rilascio del software. Puoi modellare e configurare rapidamente i diversi stadi del processo di rilascio di un software. Puoi creare, eseguire il test e distribuire il codice ogni volta che viene modificato, in base a modelli del processo di rilascio definiti.

Ecco un esempio di come puoi utilizzare i servizi nella console Strumenti di sviluppo per sviluppare il software.



In questo esempio, gli sviluppatori creano un repository in CodeCommit e lo utilizzano per sviluppare e collaborare al loro codice. Creano un progetto di compilazione CodeBuild per compilare e testare il proprio codice e lo utilizzano CodeDeploy per distribuire il codice in ambienti di test e produzione. Desiderano iterare rapidamente, quindi creano una pipeline CodePipeline per rilevare le modifiche nel repository. CodeCommit Tali modifiche vengono compilate, i test vengono eseguiti e il codice compilato e testato correttamente viene implementato al server di test. Il team aggiunge le fasi di test alla pipeline per eseguire più test sul server di gestione temporanea, ad esempio test di integrazione o carico. Una volta completati con successo questi test, un membro del team esamina i risultati e, se soddisfatto, approva manualmente le modifiche per la produzione. CodePipeline distribuisce il codice testato e approvato nelle istanze di produzione.

Questo è solo un semplice esempio di come è possibile utilizzare uno o più dei servizi disponibili nella console Strumenti di sviluppo per sviluppare il software. Ciascuno dei servizi può essere personalizzato per soddisfare le proprie esigenze. Offrono molte integrazioni con altri prodotti e servizi, sia all'interno che con altri strumenti AWS di terze parti. Per ulteriori informazioni, consulta i seguenti argomenti:

- CodeCommit: integrazioni di prodotti e servizi
- CodeBuild: Utilizzare CodeBuild con Jenkins

- CodeDeploy: integrazioni di prodotti e servizi
- CodePipeline: integrazioni di prodotti e servizi

È il primo utilizzo?

Se è la prima volta che utilizzi uno o più dei servizi disponibili nella console Strumenti di sviluppo, ti consigliamo di iniziare leggendo i seguenti argomenti:

- Nozioni di base su CodeCommit
- Guida introduttiva a CodeBuild, Concepts
- Guida introduttiva CodeDeploy, Componenti primari
- Guida introduttiva a CodePipeline, Concepts

Caratteristiche della console Strumenti di sviluppo

Nella console Strumenti di sviluppo sono disponibili le seguenti caratteristiche:

- La console Developer Tools include una funzionalità di gestione delle notifiche che puoi utilizzare per iscriverti agli eventi in AWS CodeBuild AWS CodeCommit, AWS CodeDeploy, e AWS CodePipeline. Questa funzionalità dispone di una propria API, AWS CodeStar Notifications. Puoi utilizzare la caratteristica di notifica per inviare rapidamente notifiche agli utenti sugli eventi dei repository, dei progetti di compilazione, delle applicazioni di implementazione e delle pipeline più importanti per il loro lavoro. Un gestore di notifiche consente agli utenti di riconoscere gli eventi che si verificano su repository, compilazioni, implementazioni o pipeline, in modo che possano intraprendere rapidamente le azioni necessarie, come approvare le modifiche o correggere gli errori. Per ulteriori informazioni, consulta Cosa sono le notifiche?
- La console Strumenti per sviluppatori include una funzionalità di connessione che si può utilizzare per associare le risorse AWS a provider di codice sorgente di terze parti. Questa funzionalità ha una propria API, AWS CodeConnections. È possibile utilizzare la funzionalità di connessione per configurare una connessione autorizzata con un provider di terze parti e utilizzare la risorsa di connessione con altri AWS servizi. Per ulteriori informazioni, consulta Che cosa sono le connessioni?

Cosa sono le notifiche?

La funzionalità di notifica nella console Developer Tools è un gestore di notifiche per la sottoscrizione agli eventi in AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy e. AWS CodePipeline Dispone di una propria API, AWS CodeStar Notifications. Puoi utilizzare la caratteristica di notifica per inviare rapidamente notifiche agli utenti sugli eventi dei repository, dei progetti di compilazione, delle applicazioni di implementazione e delle pipeline più importanti per il loro lavoro. Un gestore di notifiche consente agli utenti di riconoscere gli eventi che si verificano su repository, compilazioni, implementazioni o pipeline, in modo che possano intraprendere rapidamente le azioni necessarie, come approvare le modifiche o correggere gli errori.

Cosa posso fare con le notifiche?

Puoi utilizzare la caratteristica di notifica per creare e gestire regole di notifica per inviare agli utenti notifiche relative a modifiche importanti apportate alle loro risorse, incluse:

- Costruisci successi e fallimenti nei progetti di CodeBuild costruzione.
- Successi e fallimenti dell'implementazione nelle applicazioni. CodeDeploy
- Creazione e aggiornamenti nelle richieste pull, inclusi i commenti sul codice, nei repository CodeCommit.
- Vengono eseguiti gli stati di approvazione e la pipeline manuali. CodePipeline

Puoi configurare le notifiche in modo che vengano inviate agli indirizzi e-mail degli utenti che hanno effettuato l'iscrizione a un argomento Amazon SNS. Puoi anche integrare questa funzionalità con AWS Chatbot e fare in modo che le notifiche vengano distribuite a canali Slack, al canale Microsoft Teams o alle chat room Amazon Chime.

Come funzionano le notifiche?

Quando configuri una regola di notifica per una risorsa supportata, come un repository, un progetto di build, un'applicazione o una pipeline, la funzionalità di notifica crea una EventBridge regola Amazon che monitora gli eventi specificati. Quando si verifica un evento di tale tipo, la regola di notifica invia notifiche agli argomenti Amazon SNS specificati come destinazioni per tale regola. Gli iscritti a tali destinazioni ricevono notifiche su questi eventi.

Come posso iniziare a usare le notifiche?

Per iniziare, ecco alcuni argomenti utili da esaminare:

- Ulteriori informazioni sui concetti per le notifiche.
- Configurare le risorse necessarie per iniziare a utilizzare le notifiche.
- Nozioni di base sulle prime regole di notifica e la ricezione delle prime notifiche.

Concetti di notifica

La configurazione e l'utilizzo delle notifiche risultano più semplici se si comprendono i concetti e i termini. Di seguito sono riportati alcuni concetti che occorre conoscere quando si utilizzano le notifiche.

Argomenti

- Notifiche
- Regole di notifica
- Eventi
- Tipi di dettaglio
- Destinazioni
- Notifiche e AWS CodeStar notifiche
- Eventi per regole di notifica su repository
- Eventi per regole di notifica su progetti di compilazione
- Eventi per le regole di notifica sulle applicazioni di implementazione
- Eventi per regole di notifica su pipeline

Notifiche

Una notifica è un messaggio che contiene informazioni sugli eventi che si verificano nelle risorse utilizzate da te e dagli sviluppatori. Puoi configurare le notifiche in modo che gli utenti di una risorsa, ad esempio un progetto di compilazione, un repository, un'applicazione di distribuzione o una pipeline, ricevano e-mail sui tipi di eventi specificati in base alla regola di notifica creata.

Le notifiche per AWS CodeCommit possono contenere informazioni sull'identità dell'utente, come un nome visualizzato o un indirizzo e-mail, tramite l'uso di tag di sessione. CodeCommit supporta l'uso di tag di sessione, che sono attributi di coppia chiave-valore che vengono trasmessi quando si assume un ruolo IAM, si utilizzano credenziali temporanee o si federa un utente in (). AWS Security Token Service AWS STS Puoi anche associare i tag a un utente IAM. CodeCommit include i valori per

`displayName` e `emailAddress` nel contenuto della notifica, se tali tag sono presenti. Per ulteriori informazioni, consulta Utilizzo dei tag per fornire informazioni di identità aggiuntive in CodeCommit.

> **Important**
>
> Le notifiche includono informazioni specifiche del progetto, ad esempio lo stato delle compilazioni e delle distribuzioni, le righe di codice con commenti e le approvazioni della pipeline. Il contenuto delle notifiche potrebbe cambiare man mano che vengono aggiunte nuove caratteristiche. Come best practice per la sicurezza, è necessario esaminare regolarmente i destinatari delle regole di notifica e gli iscritti agli argomenti Amazon SNS. Per ulteriori informazioni, consulta Comprendere contenuti e sicurezza delle notifiche.

Regole di notifica

Una regola di notifica è una AWS risorsa creata per specificare quando e dove vengono inviate le notifiche. Definisce:

- Le condizioni in base alle quali viene creata una notifica. Queste condizioni sono basate su eventi scelti dall'utente, che sono specifici per il tipo di risorsa. I tipi di risorse supportati includono progetti di compilazione in AWS CodeBuild, applicazioni di distribuzione in AWS CodeDeploy, pipeline in AWS CodePipeline e repository in. AWS CodeCommit
- Le destinazioni a cui viene inviata la notifica. Puoi specificare fino a 10 destinazioni per una regola di notifica.

Le regole di notifica sono rivolte a singoli progetti di compilazione, applicazioni di distribuzione, pipeline e repository. Le regole di notifica hanno sia nomi descrittivi definiti dall'utente che Amazon Resource Names (ARNs). Le regole di notifica devono essere create nella stessa AWS regione in cui esiste la risorsa. Ad esempio, se il progetto di compilazione si trova nella regione Stati Uniti orientali (Ohio), anche la regola di notifica deve essere creata nella regione Stati Uniti orientali (Ohio).

Puoi definire fino a 10 regole di notifica per una risorsa.

Eventi

Un evento è una modifica dello stato di una risorsa che desideri monitorare. Ogni risorsa dispone di un elenco di tipi di eventi tra cui puoi scegliere. Quando configuri una regola di notifica su una risorsa, specifichi gli eventi che causano l'invio delle notifiche. Ad esempio, se si impostano le notifiche per un

repository in CodeCommit e si seleziona Creato sia per la richiesta Pull che per i rami e i tag, viene inviata una notifica ogni volta che un utente in quel repository crea una richiesta pull, un ramo o un tag Git.

Tipi di dettaglio

Quando crei una regola di notifica, puoi scegliere il livello di dettaglio o il tipo di dettaglio incluso nelle notifiche (Full (Completo) o Basic (Di base)). L'impostazione Full (Completo) (valore predefinito) include tutte le informazioni disponibili per l'evento nella notifica, incluse le informazioni avanzate fornite dai servizi per eventi specifici. L'impostazione Basic (Di base) include solo un sottoinsieme delle informazioni disponibili.

Nella tabella seguente sono elencate le informazioni avanzate disponibili per i tipi di eventi specifici e vengono descritte le differenze tra i tipi di dettaglio.

Servizio	Evento	Full (Completo) include	Basic (Di base) non include
CodeCommit	Commenti sui commit Commenti sulle richieste pull	Tutti i dettagli dell'evento e il contenuto del commento, comprese eventuali risposte o thread di commento. Include anche il numero di riga e la riga di codice su cui è stato fatto il commento.	Il contenuto del commento, il numero di riga, la riga di codice o qualsiasi thread di commento.
CodeCommit	Richiesta pull creata	Tutti i dettagli dell'evento e il numero di file aggiunti, modificati o eliminati nella richiesta pull in relazione al ramo di destinazione.	Nessun elenco di file o dettagli sul fatto che il ramo di origine della richiesta pull abbia aggiunto, modificato o eliminato i file.

Servizio	Evento	Full (Completo) include	Basic (Di base) non include
CodePipeline	Approvazione manuale necessaria	Tutti i dettagli dell'evento e i dati personalizzati (se configurati). La notifica include anche un collegamento all'approvazione richiesta nella pipeline.	Nessun collegamento o dato personalizzato.
CodePipeline	Esecuzione dell'operazione non riuscita Esecuzione della pipeline non riuscita Esecuzione della fase non riuscita	Tutti i dettagli dell'evento e il contenuto del messaggio di errore per l'errore.	Nessun contenuto di messaggio di errore.

Destinazioni

Una destinazione è una posizione per la ricezione delle notifiche dalle regole di notifica. I tipi di target consentiti sono argomenti Amazon SNS e client Chatbot configurati per i AWS canali Slack o Microsoft Teams. Qualsiasi utente che ha effettuato l'iscrizione alla destinazione riceve le notifiche sugli eventi specificati nella regola di notifica.

Se desideri estendere la portata delle notifiche, puoi configurare manualmente l'integrazione tra notifiche e AWS Chatbot in modo che le notifiche vengano inviate alle chat room di Amazon Chime. Puoi quindi scegliere l'argomento Amazon SNS configurato per quel client Chatbot AWS come destinazione per la regola di notifica. Per ulteriori informazioni, consulta Per integrare le notifiche con AWS Chatbot e Amazon Chime.

Se scegli di utilizzare un client AWS Chatbot come obiettivo, devi prima creare quel client in AWS Chatbot. Quando scegli un client AWS Chatbot come obiettivo per una regola di notifica, viene

configurato un argomento Amazon SNS per quel client AWS Chatbot con tutte le politiche necessarie per l'invio delle notifiche al canale Slack o Microsoft Teams. Non è necessario configurare alcun argomento Amazon SNS esistente per il client Chatbot AWS .

Puoi scegliere di creare un argomento Amazon SNS come destinazione come parte della creazione di una regola di notifica (scelta consigliata). Puoi anche scegliere un argomento Amazon SNS esistente nella stessa AWS regione della regola di notifica, ma devi configurarlo con la politica richiesta. L'argomento Amazon SNS che usi per un target deve essere nel tuo AWS account. Inoltre, deve trovarsi nella stessa AWS regione della regola di notifica e della AWS risorsa per cui è stata creata la regola.

Ad esempio, se crei una regola di notifica per un repository nella regione Stati Uniti orientali (Ohio), l'argomento Amazon SNS deve esistere anche in tale regione. Se crei un argomento Amazon SNS durante la creazione di una regola di notifica, l'argomento viene configurato con la policy necessaria per consentire la pubblicazione degli eventi nell'argomento. Questo è il metodo migliore per lavorare con le destinazioni e le regole di notifica. Se scegli di utilizzare un argomento già esistente o di crearne uno manualmente, è necessario configurarlo con le autorizzazioni richieste prima che gli utenti ricevano le notifiche. Per ulteriori informazioni, consulta Configura gli argomenti di Amazon SNS per le notifiche.

> **Note**
>
> Se desideri utilizzare un argomento Amazon SNS esistente invece di crearne uno nuovo, in Targets (Destinazioni), scegli il relativo ARN. Assicurati che l'argomento disponga delle policy di accesso appropriate e che l'elenco degli iscritti contenga solo gli utenti autorizzati a visualizzare le informazioni sulla risorsa. Se l'argomento Amazon SNS è un argomento utilizzato per CodeCommit le notifiche prima del 5 novembre 2019, conterrà una politica che consente la pubblicazione su CodeCommit di esso con autorizzazioni diverse da quelle richieste per le notifiche. AWS CodeStar L'utilizzo di questi argomenti è sconsigliato. Se desideri utilizzarne uno creato per quell'esperienza, devi aggiungere la politica richiesta per AWS CodeStar le notifiche oltre a quella già esistente. Per ulteriori informazioni, consulta Configura gli argomenti di Amazon SNS per le notifiche e Comprendere contenuti e sicurezza delle notifiche.

Notifiche e AWS CodeStar notifiche

Sebbene siano una funzionalità della console Developer Tools, le notifiche hanno una propria API, AWS CodeStar Notifications. Hanno anche un proprio tipo di risorsa AWS (regole di notifica), autorizzazioni ed eventi. Gli eventi per le regole di notifica vengono registrati in AWS CloudTrail. Le operazioni API possono essere consentite o negate tramite le policy IAM.

Eventi per regole di notifica su repository

Categoria	Eventi	Evento IDs

Commenti	Sui commit
	
	Su richieste pull
		`codecommit-repository-comments-on-commits`
		
		`codecommit-repository-comments-on-pull-requests`

Approvazioni	Stato modificato
	
	Sostituzione delle regole
		`codecommit-repository-approvals-status-changed`
		
		`codecommit-repository-approvals-rule-override`

Richiesta pull	Creato
	
	Origine aggiornata
	
	Stato modificato
	
	Unito
		`codecommit-repository-pull-request-created`
		
		`codecommit-repository-pull-request-source-updated`
		
		`codecommit-repository-pull-request-status-changed`
		
		`codecommit-repository-pull-request-merged`

Categoria	Eventi	Evento IDs
Rami e tag	Creato Eliminato Aggiornato	codecommit-repository-branches-and-tags-created codecommit-repository-branches-and-tags-deleted codecommit-repository-branches-and-tags-updated

Eventi per regole di notifica su progetti di compilazione

Categoria	Eventi	Evento IDs
Stato di compilazione	Non riuscito Riuscito In corso Arrestato	codebuild-project-build-state-failed codebuild-project-build-state-succeeded codebuild-project-build-state-in-progress codebuild-project-build-state-stopped
Fase di compilazione	Errore Riuscito	codebuild-project-build-phase-failure codebuild-project-build-phase-success

Eventi per le regole di notifica sulle applicazioni di implementazione

Categoria	Eventi	Evento IDs

Implementazione	Non riuscito
	Riuscito
	Avviato
		`codedeploy-application-deployment-failed`
		`codedeploy-application-deployment-succeeded`
		`codedeploy-application-deployment-started`

Eventi per regole di notifica su pipeline

Categoria	Eventi	Evento IDs

Esecuzione dell'operazione	Riuscito
	Non riuscito
	Annullato
	Avviato
		`codepipeline-pipeline-action-execution-succeeded`
		`codepipeline-pipeline-action-execution-failed`
		`codepipeline-pipeline-action-execution-canceled`
		`codepipeline-pipeline-action-execution-started`

Esecuzione della fase	Avviato
	Riuscito
	Ripristinato
	Annullato
	Non riuscito
		`codepipeline-pipeline-stage-execution-started`
		`codepipeline-pipeline-stage-execution-succeeded`
		`codepipeline-pipeline-stage-execution-resumed`

Categoria	Eventi	Evento IDs
		`codepipeline-pipeline-stage-execution-canceled` `codepipeline-pipeline-stage-execution-failed`

Esecuzione pipeline	Non riuscito
	Annullato
	Avviato
	Ripristinato
	Riuscito
	Sostituito
		`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`

Approvazione manuale	Non riuscito
	Necessario
	Riuscito
		`codepipeline-pipeline-manual-approval-failed`
		`codepipeline-pipeline-manual-approval-needed`
		`codepipeline-pipeline-manual-approval-succeeded`

Configurazione

Se disponi di una policy gestita per AWS CodeBuild AWS CodeCommit AWS CodeDeploy, o AWS CodePipeline applicata al tuo utente o ruolo IAM, disponi delle autorizzazioni necessarie per lavorare con le notifiche entro i limiti dei ruoli e delle autorizzazioni forniti dalla policy. Ad esempio, gli utenti

che hanno applicata la policy gestita `AWSCodeBuildAdminAccess`, `AWSCodeCommitFullAccess`, `AWSCodeDeployFullAccess` o `AWSCodePipeline_FullAccess`, hanno l'accesso amministrativo completo alle notifiche.

Per ulteriori informazioni, incluse policy di esempio, consulta Policy basate sull'identità.

Se hai applicato una di queste policy al tuo utente o ruolo IAM e hai inserito un progetto di compilazione CodeBuild, un repository CodeCommit, un'applicazione di distribuzione o una pipeline in entrata CodeDeploy CodePipeline, sei pronto per creare la tua prima regola di notifica. Continua su Nozioni di base sulle notifiche. In caso contrario, vedi gli argomenti seguenti:

- CodeBuild: Guida introduttiva con CodeBuild
- CodeCommit: Guida introduttiva con CodeCommit
- CodeDeploy: Tutorial
- CodePipeline: Guida introduttiva con CodePipeline

Per gestire autonomamente le autorizzazioni amministrative per le notifiche per utenti, gruppi o ruoli IAM, segui le procedure descritte in questo argomento per impostare le autorizzazioni e le risorse necessarie per utilizzare il servizio.

Per utilizzare gli argomenti Amazon SNS creati in precedenza per le notifiche anziché creare argomenti specifici per le notifiche, è necessario configurare un argomento Amazon SNS da utilizzare come destinazione per una regola di notifica applicando una policy che consenta la pubblicazione degli eventi nell'argomento.

> **Note**
>
> Per eseguire le seguenti procedure, devi avere effettuato l'accesso con un account che dispone di autorizzazioni amministrative. Per ulteriori informazioni, consulta Creazione del primo utente amministratore e gruppo IAM.

Argomenti

- Creare e applicare una policy per l'accesso amministrativo alle notifiche
- Configura gli argomenti di Amazon SNS per le notifiche
- Iscrivere gli utenti agli argomenti Amazon SNS che sono destinazioni

Creare e applicare una policy per l'accesso amministrativo alle notifiche

Puoi amministrare le notifiche accedendo con un utente IAM o utilizzando un ruolo che dispone delle autorizzazioni per accedere al servizio e ai servizi (AWS CodeBuild, AWS CodeCommit AWS CodeDeploy, o AWS CodePipeline) per i quali desideri creare notifiche. Puoi inoltre creare policy personalizzate e applicarle a utenti o gruppi.

Nella procedura seguente viene illustrato come configurare un gruppo IAM con autorizzazioni per l'amministrazione delle notifiche e l'aggiunta di utenti IAM. Se non desideri configurare un gruppo, puoi applicare questa policy direttamente a utenti IAM o a un ruolo IAM che può essere assunto dagli utenti. Puoi anche utilizzare le policy gestite per CodeBuild,, or CodeCommit CodeDeploy CodePipeline, che includono l'accesso adeguato alle funzionalità di notifica in base alle policy, a seconda dell'ambito della policy.

Per la policy sottostante immetti un nome (ad esempio, `AWSCodeStarNotificationsFullAccess`) e una descrizione facoltativa. La descrizione consente di ricordare l'ambito della policy (ad esempio, **`This policy provides full access to AWS CodeStar Notifications.`**)

Come utilizzare l'editor di policy JSON per creare una policy

1. Accedi AWS Management Console e apri la console IAM all'indirizzo. https://console.aws.amazon.com/iam/
2. Nel riquadro di navigazione a sinistra, seleziona Policies (Policy).

   Se è la prima volta che selezioni Policy, verrà visualizzata la pagina Benvenuto nelle policy gestite. Seleziona Inizia.
3. Nella parte superiore della pagina, scegli Crea policy.
4. Nella sezione Editor di policy, scegli l'opzione JSON.
5. Inserisci il documento di policy JSON seguente:

```
{
   "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. Scegli Next (Successivo).

> **Note**
>
> È possibile alternare le opzioni dell'editor Visivo e JSON in qualsiasi momento. Se tuttavia si apportano modifiche o si seleziona Successivo nell'editor Visivo, IAM potrebbe ristrutturare la policy in modo da ottimizzarla per l'editor visivo. Per ulteriori informazioni, consulta Modifica della struttura delle policy nella Guida per l'utente di IAM.

7. Nella pagina Rivedi e crea, inserisci un valore in Nome policy e Descrizione (facoltativo) per la policy in fase di creazione. Rivedi Autorizzazioni definite in questa policy per visualizzare le autorizzazioni concesse dalla policy.
8. Seleziona Crea policy per salvare la nuova policy.

Configura gli argomenti di Amazon SNS per le notifiche

Il modo più semplice per impostare le notifiche consiste nel creare un argomento Amazon SNS al momento della creazione di una regola di notifica. Puoi utilizzare un argomento Amazon SNS esistente se soddisfa i seguenti requisiti:

- È stata creata nella Regione AWS stessa risorsa (progetto di compilazione, applicazione di distribuzione, repository o pipeline) per la quale desideri creare regole di notifica.

- Non è stato utilizzato per l'invio di notifiche CodeCommit prima del 5 novembre 2019. In tal caso, conterrà istruzioni delle policy che hanno abilitato tale funzionalità. È possibile scegliere di utilizzare questo argomento, ma sarà necessario aggiungere la policy aggiuntiva come specificato nella procedura. Non rimuovere l'istruzione di policy esistente se uno o più repository sono ancora configurati per le notifiche prima del 5 novembre 2019.
- Ha una politica che consente a AWS CodeStar Notifications di pubblicare notifiche sull'argomento.

Per configurare un argomento di Amazon SNS da utilizzare come destinazione per AWS CodeStar le regole di notifica delle notifiche

1. Accedi AWS Management Console e apri la console Amazon SNS nella versione v3/home. https://console.aws.amazon.com/sns/
2. Nella barra di spostamento scegli Topics (Argomenti), seleziona l'argomento che vuoi configurare e quindi scegli Edit (Modifica).
3. Espandi Access policy (Policy di accesso), quindi scegli Advanced (Avanzate).
4. Nell'editor JSON, aggiungi la seguente istruzione alla policy. Includi l'ARN Regione AWS, l' Account AWS ID e il nome dell'argomento.

```
 {
      "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"
    }
```

L'istruzione della policy dovrebbe essere simile alla seguente:

```
{
  "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"
      ],
      "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. Scegli Save changes (Salva modifiche).
6. Se desideri utilizzare un argomento Amazon SNS AWS KMS crittografato per inviare notifiche, devi anche abilitare la compatibilità tra l'origine dell'evento AWS CodeStar (Notifiche) e l'argomento crittografato aggiungendo la seguente dichiarazione alla politica di. AWS KMS key Sostituisci Regione AWS (in questo esempio, us-east-2) con Regione AWS il punto in cui è stata creata la chiave.

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

Per ulteriori informazioni, consulta Crittografia inattiva e Utilizzo delle condizioni delle policy con AWS KMS nella AWS Key Management Service Guida per gli sviluppatori.

Iscrivere gli utenti agli argomenti Amazon SNS che sono destinazioni

Prima che gli utenti possano ricevere le notifiche, devono essere iscritti all'argomento Amazon SNS che è la destinazione della regola di notifica. Se gli utenti sono iscritti tramite indirizzo e-mail, devono confermare l'iscrizione prima di ricevere le notifiche. Per inviare notifiche agli utenti nei canali Slack, Microsoft Teams o chat room di Slack o Amazon Chime, consulta Configurare l'integrazione tra notifiche e AWS Chatbot.

Per iscrivere gli utenti a un argomento Amazon SNS utilizzato per le notifiche

1. Accedi AWS Management Console e apri la console Amazon SNS nella versione v3/home. https://console.aws.amazon.com/sns/
2. Nella barra di navigazione, selezionare Topics (Argomenti), quindi scegliere l'argomento al quale si desidera iscrivere gli utenti.

3. In Subscriptions (Abbonamenti), scegliere Create subscription (Crea abbonamento).
4. Per Protocol (Protocollo), scegli Email. In Endpoint, digitare l'indirizzo e-mail, quindi scegliere Create subscription (Crea sottoscrizione).

Nozioni di base sulle notifiche

Il modo più semplice per iniziare a utilizzare le notifiche è configurare una regola di notifica su un progetto di compilazione, un'applicazione di distribuzione, una pipeline o un repository.

> **Note**
>
> La prima volta che crei una regola di notifica, viene creato un ruolo collegato ai servizi nel tuo account. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per le notifiche AWS CodeStar .

Argomenti

- Prerequisiti
- Creazione di una regola di notifica per un repository
- Creazione di una regola di notifica per un progetto di compilazione
- Creazione di una regola di notifica per un'applicazione di implementazione
- Creazione di una regola di notifica per una pipeline

Prerequisiti

Completa le fasi descritte in Configurazione. È inoltre necessaria la risorsa per cui crei la regola di notifica.

- Crea un progetto di compilazione CodeBuild o usane uno esistente.
- Crea un'applicazione o utilizza un'applicazione di implementazione esistente.
- Crea una pipeline CodePipeline o usane una esistente.
- Crea un AWS CodeCommit repository o usane uno esistente.

Creazione di una regola di notifica per un repository

Puoi creare regole di notifica per inviare notifiche relative agli eventi sul repository che sono per te importanti. La procedura seguente illustra come configurare una regola di notifica su un singolo evento del repository. Questi passaggi sono scritti partendo dal presupposto che nel tuo account sia configurato un repository. AWS

> **Important**
>
> Se configuri le notifiche CodeCommit prima del 5 novembre 2019, gli argomenti di Amazon SNS utilizzati per tali notifiche conterranno una policy che ne CodeCommit consente la pubblicazione con autorizzazioni diverse da quelle richieste per le notifiche. AWS CodeStar L'utilizzo di questi argomenti è sconsigliato. Se desideri utilizzarne una creata per quell'esperienza, devi aggiungere la politica richiesta per AWS CodeStar le notifiche oltre a quella già esistente. Per ulteriori informazioni, consulta Configura gli argomenti di Amazon SNS per le notifiche e Comprendere contenuti e sicurezza delle notifiche.

1. Apri la CodeCommit console all'indirizzo https://console.aws.amazon.com/codecommit/.
2. Scegli un repository dall'elenco e aprilo.
3. Scegli Notify (Notifica), quindi seleziona Create notification rule (Crea regola di notifica). Puoi anche scegliere Settings (Impostazioni), Notifications (Notifiche), quindi Create notification rule (Crea regola di notifica).
4. In Notification name (Nome notifica), immettere un nome per la regola.
5. In Tipo di dettaglio, scegli Basic se desideri che nella notifica siano EventBridge incluse solo le informazioni fornite ad Amazon. Scegli Completo se desideri includere le informazioni fornite ad Amazon EventBridge e le informazioni che potrebbero essere fornite dal servizio di risorse o dal gestore delle notifiche.

   Per ulteriori informazioni, consulta Comprendere contenuti e sicurezza delle notifiche.
6. In Events that trigger notifications (Eventi che attivano le notifiche), in Branches and tags (Rami e tag), seleziona Created (Creato).
7. In Targets (Destinazioni), scegli Create SNS topic (Crea argomento SNS).

> **Note**
>
> Quando crei l'argomento come parte della creazione della regola di notifica, viene applicata CodeCommit automaticamente la politica che consente di pubblicare eventi sull'argomento. L'utilizzo di un argomento creato per le regole di notifica consente di iscrivere solo gli utenti che vuoi ricevano le notifiche relative a questo repository.

Dopo il prefisso codestar-notifications- immetti un nome per l'argomento e quindi scegli Submit (Invia).

> **Note**
>
> Se desideri utilizzare un argomento Amazon SNS esistente invece di crearne uno nuovo, in Targets (Destinazioni), scegli il relativo ARN. Assicurati che l'argomento disponga delle policy di accesso appropriate e che l'elenco degli iscritti contenga solo gli utenti autorizzati a visualizzare le informazioni sulla risorsa. Se l'argomento Amazon SNS è un argomento utilizzato per CodeCommit le notifiche prima del 5 novembre 2019, conterrà una politica che consente la pubblicazione su CodeCommit di esso con autorizzazioni diverse da quelle richieste per le notifiche. AWS CodeStar L'utilizzo di questi argomenti è sconsigliato. Se desideri utilizzarne uno creato per quell'esperienza, devi aggiungere la politica richiesta per AWS CodeStar le notifiche oltre a quella già esistente. Per ulteriori informazioni, consulta Configura gli argomenti di Amazon SNS per le notifiche e Comprendere contenuti e sicurezza delle notifiche.

8. Scegliere Submit (Invia), quindi esaminare la regola di notifica.
9. Iscrivi il tuo indirizzo email all'argomento Amazon SNS appena creato. Per ulteriori informazioni, consulta Per iscrivere gli utenti a un argomento Amazon SNS utilizzato per le notifiche.
10. Passa al repository e crea un ramo di test dal ramo predefinito.
11. Dopo aver creato il ramo, la regola di notifica invia una notifica a tutti gli iscritti all'argomento con le informazioni sull'evento.

Creazione di una regola di notifica per un progetto di compilazione

Puoi creare regole di notifica per inviare notifiche relative a eventi sul progetto di compilazione che sono per te importanti. La procedura seguente illustra come configurare una regola di notifica per un

singolo evento del progetto di compilazione. Questi passaggi sono scritti partendo dal presupposto che nel tuo AWS account sia configurato un progetto di compilazione.

1. Apri la CodeBuild console all'indirizzo https://console.aws.amazon.com/codebuild/.
2. Scegli un progetto di compilazione dall'elenco e aprilo.
3. Scegli Notify (Notifica), quindi seleziona Create notification rule (Crea regola di notifica). Puoi anche scegliere Settings (Impostazioni) e quindi Create notification rule (Crea regola di notifica).
4. In Notification name (Nome notifica), immettere un nome per la regola.
5. In Tipo di dettaglio, scegli Basic se desideri che nella notifica siano EventBridge incluse solo le informazioni fornite ad Amazon. Scegli Completo se desideri includere le informazioni fornite ad Amazon EventBridge e le informazioni che potrebbero essere fornite dal servizio di risorse o dal gestore delle notifiche.

   Per ulteriori informazioni, consulta Comprendere contenuti e sicurezza delle notifiche.
6. In Events that trigger notifications (Eventi che attivano le notifiche), in Build phase (Fase di compilazione), seleziona Success (Riuscito).
7. In Targets (Destinazioni), scegli Create SNS topic (Crea argomento SNS).

> **Note**
>
> Quando crei l'argomento come parte della creazione della regola di notifica, viene applicata CodeBuild automaticamente la politica che consente di pubblicare eventi sull'argomento. L'utilizzo di un argomento creato per le regole di notifica consente di iscrivere solo gli utenti che vuoi ricevano le notifiche relative a questo progetto di compilazione.

Dopo il prefisso codestar-notifications- immetti un nome per l'argomento e quindi scegli Submit (Invia).

> **Note**
>
> Se desideri utilizzare un argomento Amazon SNS esistente invece di crearne uno nuovo, in Targets (Destinazioni), scegli il relativo ARN. Assicurati che l'argomento disponga delle policy di accesso appropriate e che l'elenco degli iscritti contenga solo gli utenti autorizzati a visualizzare le informazioni sulla risorsa. Se l'argomento Amazon SNS è un

argomento utilizzato per CodeCommit le notifiche prima del 5 novembre 2019, conterrà una politica che consente la pubblicazione su CodeCommit di esso con autorizzazioni diverse da quelle richieste per le notifiche. AWS CodeStar L'utilizzo di questi argomenti è sconsigliato. Se desideri utilizzarne uno creato per quell'esperienza, devi aggiungere la politica richiesta per AWS CodeStar le notifiche oltre a quella già esistente. Per ulteriori informazioni, consulta Configura gli argomenti di Amazon SNS per le notifiche e Comprendere contenuti e sicurezza delle notifiche.

8. Scegliere Submit (Invia), quindi esaminare la regola di notifica.
9. Iscrivi il tuo indirizzo email all'argomento Amazon SNS appena creato. Per ulteriori informazioni, consulta Per iscrivere gli utenti a un argomento Amazon SNS utilizzato per le notifiche.
10. Passa al progetto di compilazione e avvia una compilazione.
11. Al termine della fase di compilazione, la regola di notifica invia una notifica a tutti gli iscritti all'argomento con le informazioni sull'evento.

Creazione di una regola di notifica per un'applicazione di implementazione

Puoi creare regole di notifica per inviare notifiche relative agli eventi sull'applicazione di distribuzione che sono per te importanti. La procedura seguente illustra come configurare una regola di notifica per un singolo evento del progetto di compilazione. Questa procedura presuppone che sia stata già configurata un'applicazione di distribuzione nel tuo account AWS .

1. Apri la CodeDeploy console all'indirizzo https://console.aws.amazon.com/codedeploy/.
2. Scegli un'applicazione dall'elenco e aprila.
3. Scegli Notify (Notifica), quindi seleziona Create notification rule (Crea regola di notifica). Puoi anche scegliere Settings (Impostazioni) e quindi Create notification rule (Crea regola di notifica).
4. In Notification name (Nome notifica), immettere un nome per la regola.
5. In Tipo di dettaglio, scegli Basic se desideri che nella notifica siano EventBridge incluse solo le informazioni fornite ad Amazon. Scegli Completo se desideri includere le informazioni fornite ad Amazon EventBridge e le informazioni che potrebbero essere fornite dal servizio di risorse o dal gestore delle notifiche.

   Per ulteriori informazioni, consulta Comprendere contenuti e sicurezza delle notifiche.

6. In Events that trigger notifications (Eventi che attivano le notifiche), in Deployment (Distribuzione), seleziona Succeeded (Riuscito).

7. In Targets (Destinazioni), scegli Create SNS topic (Crea argomento SNS).

   > **Note**
   >
   > Quando crei l'argomento come parte della creazione della regola di notifica, viene applicata CodeDeploy automaticamente la politica che consente di pubblicare eventi sull'argomento. L'utilizzo di un argomento creato per le regole di notifica consente di iscrivere solo gli utenti che vuoi ricevano le notifiche relative a questa applicazione di distribuzione.

   Dopo il prefisso codestar-notifications- immetti un nome per l'argomento e quindi scegli Submit (Invia).

   > **Note**
   >
   > Se desideri utilizzare un argomento Amazon SNS esistente invece di crearne uno nuovo, in Targets (Destinazioni), scegli il relativo ARN. Assicurati che l'argomento disponga delle policy di accesso appropriate e che l'elenco degli iscritti contenga solo gli utenti autorizzati a visualizzare le informazioni sulla risorsa. Se l'argomento Amazon SNS è un argomento utilizzato per CodeCommit le notifiche prima del 5 novembre 2019, conterrà una politica che consente la pubblicazione su CodeCommit di esso con autorizzazioni diverse da quelle richieste per le notifiche. AWS CodeStar L'utilizzo di questi argomenti è sconsigliato. Se desideri utilizzarne uno creato per quell'esperienza, devi aggiungere la politica richiesta per AWS CodeStar le notifiche oltre a quella già esistente. Per ulteriori informazioni, consulta Configura gli argomenti di Amazon SNS per le notifiche e Comprendere contenuti e sicurezza delle notifiche.

8. Scegliere Submit (Invia), quindi esaminare la regola di notifica.
9. Iscrivi il tuo indirizzo email all'argomento Amazon SNS appena creato. Per ulteriori informazioni, consulta Per iscrivere gli utenti a un argomento Amazon SNS utilizzato per le notifiche.
10. Passa all'applicazione di distribuzione e avvia una distribuzione.
11. Una volta completata la distribuzione, la regola di notifica invia una notifica a tutti gli iscritti all'argomento con le informazioni sull'evento.

Creazione di una regola di notifica per una pipeline

Puoi creare regole di notifica per inviare notifiche relative agli eventi sulla pipeline che sono per te importanti. La procedura seguente illustra come configurare una regola di notifica su un singolo evento della pipeline. Questi passaggi sono scritti partendo dal presupposto che nel tuo AWS account sia configurata una pipeline.

1. Apri la CodePipeline console all'indirizzo. https://console.aws.amazon.com/codepipeline/
2. Scegli una pipeline dall'elenco e aprila.
3. Scegli Notify (Notifica), quindi seleziona Create notification rule (Crea regola di notifica). Puoi anche scegliere Settings (Impostazioni) e quindi Create notification rule (Crea regola di notifica).
4. In Notification name (Nome notifica), immettere un nome per la regola.
5. In Tipo di dettaglio, scegli Basic se desideri che nella notifica siano EventBridge incluse solo le informazioni fornite ad Amazon. Scegli Completo se desideri includere le informazioni fornite ad Amazon EventBridge e le informazioni che potrebbero essere fornite dal servizio di risorse o dal gestore delle notifiche.

   Per ulteriori informazioni, consulta Comprendere contenuti e sicurezza delle notifiche.
6. In Events that trigger notifications (Eventi che attivano le notifiche), in Action execution (Esecuzione dell'azione), seleziona Started (Avviato).
7. In Targets (Destinazioni), scegli Create SNS topic (Crea argomento SNS).

   > **Note**
   >
   > Quando crei l'argomento come parte della creazione della regola di notifica, viene applicata CodePipeline automaticamente la politica che consente di pubblicare eventi sull'argomento. L'utilizzo di un argomento creato per le regole di notifica consente di iscrivere solo gli utenti che vuoi ricevano le notifiche relative a questa pipeline.

   Dopo il prefisso codestar-notifications- immetti un nome per l'argomento e quindi scegli Submit (Invia).

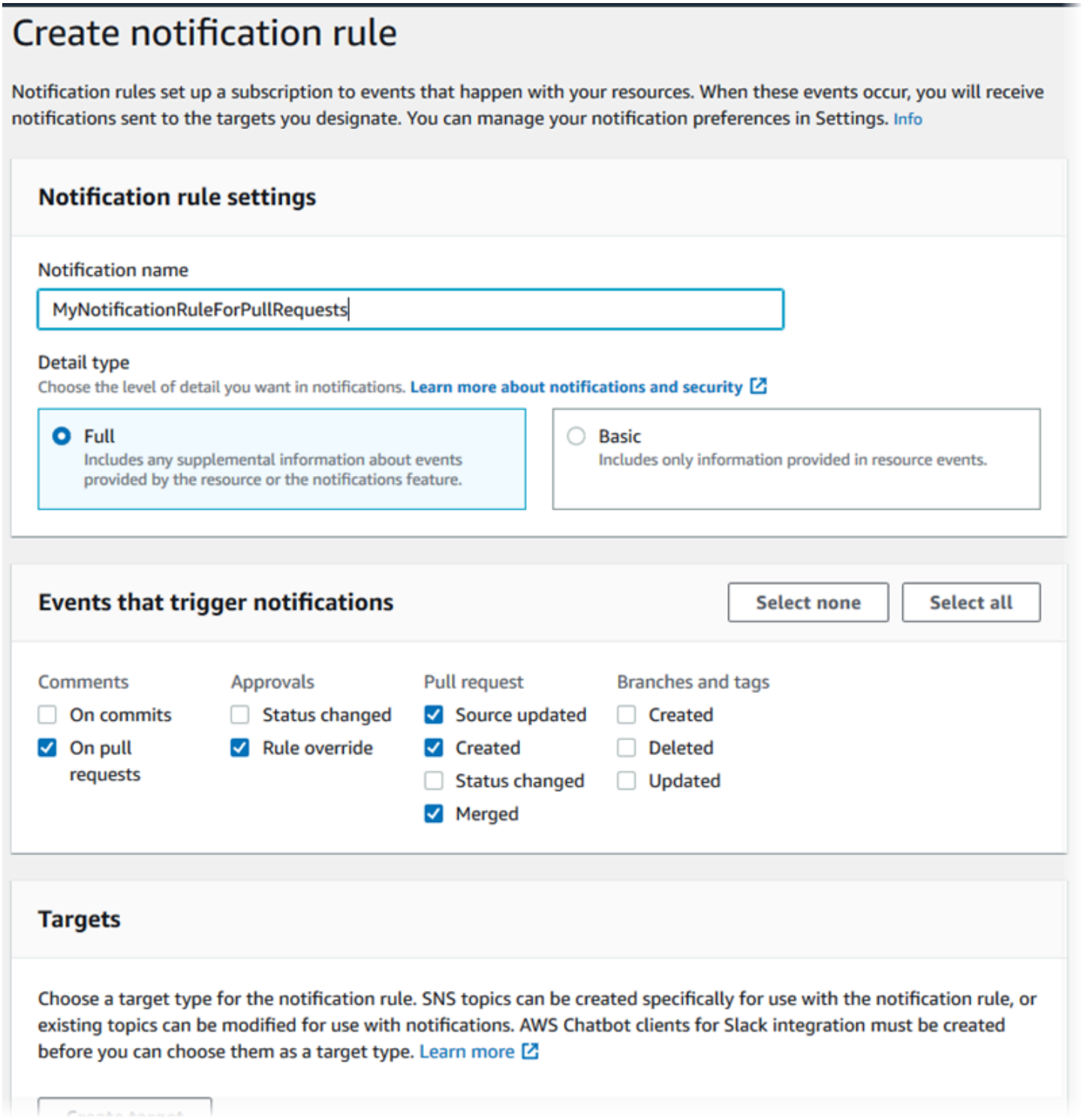
   > **Note**
   >
   > Se desideri utilizzare un argomento Amazon SNS esistente invece di crearne uno nuovo, in Targets (Destinazioni), scegli il relativo ARN. Assicurati che l'argomento disponga

delle policy di accesso appropriate e che l'elenco degli iscritti contenga solo gli utenti autorizzati a visualizzare le informazioni sulla risorsa. Se l'argomento Amazon SNS è un argomento utilizzato per CodeCommit le notifiche prima del 5 novembre 2019, conterrà una politica che consente la pubblicazione su CodeCommit di esso con autorizzazioni diverse da quelle richieste per le notifiche. AWS CodeStar L'utilizzo di questi argomenti è sconsigliato. Se desideri utilizzarne uno creato per quell'esperienza, devi aggiungere la politica richiesta per AWS CodeStar le notifiche oltre a quella già esistente. Per ulteriori informazioni, consulta Configura gli argomenti di Amazon SNS per le notifiche e Comprendere contenuti e sicurezza delle notifiche.

8. Scegliere Submit (Invia), quindi esaminare la regola di notifica.
9. Iscrivi il tuo indirizzo email all'argomento Amazon SNS appena creato. Per ulteriori informazioni, consulta Per iscrivere gli utenti a un argomento Amazon SNS utilizzato per le notifiche.
10. Passa alla pipeline, quindi scegli Release change (Rilascia modifica).
11. Una volta avviata l'azione, la regola di notifica invia una notifica a tutti gli iscritti all'argomento con le informazioni sull'evento.

Utilizzo delle regole di notifica

Una regola di notifica consente di configurare gli eventi per cui desideri che gli utenti ricevano le notifiche e di specificare le destinazioni che ricevono tali notifiche. Puoi inviare notifiche direttamente agli utenti tramite Amazon SNS o tramite client Chatbot configurati per i AWS canali Slack o Microsoft Teams. Se desideri estendere la portata delle notifiche, puoi configurare manualmente l'integrazione tra notifiche e AWS Chatbot in modo che le notifiche vengano inviate alle chat room di Amazon Chime. Per ulteriori informazioni, consulta Destinazioni e Per integrare le notifiche con AWS Chatbot e Amazon Chime.



È possibile utilizzare la console Developer Tools o AWS CLI per creare e gestire le regole di notifica.

Argomenti

- Creazione di una regola di notifica

- Visualizzazione delle regole di notifica
- Modifica di una regola di notifica
- Abilitazione o disabilitazione delle notifiche per una regola di notifica
- Eliminazione di una regola di notifica

Creazione di una regola di notifica

Puoi utilizzare la console Developer Tools o AWS CLI creare regole di notifica. Puoi creare un argomento Amazon SNS da utilizzare come destinazione per una regola di notifica durante la creazione della regola. Se desideri utilizzare un client AWS Chatbot come target, devi creare quel client prima di poter creare la regola. Per ulteriori informazioni, consulta Configura un client AWS Chatbot per un canale Slack.

Per creare una regola di notifica (console)

1. Apri la console AWS Developer Tools in https://console.aws.amazon.com/codesuite/impostazioni/notifiche.
2. Utilizza la barra di spostamento per accedere alla risorsa.
   - Per CodeBuild, scegli Costruisci, scegli Crea progetti e scegli un progetto di compilazione.
   - Per CodeCommit, scegli Source, scegli Repository e scegli un repository.
   - Per CodeDeploy, scegli Applicazioni e scegli un'applicazione.
   - Per CodePipeline, scegliete Pipeline, scegliete Pipeline e scegliete una pipeline.
3. Nella pagina delle risorse, scegliere Notify (Notifica), quindi selezionare Create notification rule (Crea regola di notifica). È anche possibile andare alla pagina Settings (Impostazioni) per la risorsa, passare a Notifications (Notifiche) o Notification rules (Regole notifiche) e scegliere Create notification rule (Crea regola di notifica).
4. In Notification name (Nome notifica), immettere un nome per la regola.
5. In Tipo di dettaglio, scegli Basic se desideri che nella notifica siano EventBridge incluse solo le informazioni fornite ad Amazon. Scegli Completo se desideri includere le informazioni fornite ad Amazon EventBridge e le informazioni che potrebbero essere fornite dal servizio di risorse o dal gestore delle notifiche.

   Per ulteriori informazioni, consulta Comprendere contenuti e sicurezza delle notifiche.
6. In Events that trigger notifications (Eventi che attivano le notifiche), selezionare gli eventi per i quali si desidera inviare notifiche. Per i tipi di evento per una risorsa, vedere quanto segue:

- CodeBuild: Eventi per regole di notifica su progetti di compilazione
- CodeCommit: Eventi per regole di notifica su repository
- CodeDeploy: Eventi per le regole di notifica sulle applicazioni di implementazione
- CodePipeline: Eventi per regole di notifica su pipeline

7. In Targets (Destinazioni), procedere in uno dei seguenti modi:

- Se è già stata configurata una risorsa da utilizzare con le notifiche, in Scegli il tipo di destinazione, scegliere AWS Chatbot (Slack), AWS Chatbot (Microsoft Teams) o Argomento SNS. In Scegli destinazione, scegli il nome del client (per un client Slack o Microsoft Teams configurato in AWS Chatbot) o l'Amazon Resource Name (ARN) dell'argomento Amazon SNS (per gli argomenti Amazon SNS già configurati con la politica richiesta per le notifiche).
- Se non è stata configurata una risorsa da utilizzare con le notifiche, scegliere Create target (Crea destinazione), e quindi scegliere SNS topic (Argomento SNS). Fornire un nome per l'argomento dopo codestar-notifications-, quindi scegliere Create (Crea).

> **Note**
>
> - Se si crea l'argomento Amazon SNS come parte della creazione della regola di notifica, viene applicata la policy che consente alla funzionalità di notifica di pubblicare eventi nell'argomento. L'utilizzo di un argomento creato per le regole di notifica consente di iscrivere solo gli utenti che si desidera ricevano le notifiche relative a questa risorsa.
> - Non è possibile creare un client AWS Chatbot come parte della creazione di una regola di notifica. Se scegli AWS Chatbot (Slack) o Chatbot AWS (Microsoft Teams), vedrai un pulsante che ti indirizza alla configurazione di un client in Chatbot. AWS Scegliendo questa opzione si apre la AWS console Chatbot. Per ulteriori informazioni, consulta Configura un client AWS Chatbot per un canale Slack.
> - Se desideri utilizzare un argomento Amazon SNS esistente come obiettivo, devi aggiungere la politica richiesta per AWS CodeStar le notifiche oltre a qualsiasi altra politica che potrebbe esistere per quell'argomento. Per ulteriori informazioni, consulta Configura gli argomenti di Amazon SNS per le notifiche e Comprendere contenuti e sicurezza delle notifiche.

8. Scegliere Submit (Invia), quindi esaminare la regola di notifica.

> **Note**
>
> Gli utenti devono iscriversi e confermare le iscrizioni all'argomento Amazon SNS specificato come destinazione della regola prima di ricevere le notifiche. Per ulteriori informazioni, consulta Per iscrivere gli utenti a un argomento Amazon SNS utilizzato per le notifiche.

Per creare una regola di notifica (AWS CLI)

1. Da un terminale o dal prompt dei comandi, eseguire il comando create-notification rule per generare lo skeleton JSON:

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

   È possibile assegnare al file un nome qualsiasi. In questo esempio, il file è denominato *rule.json*.

2. Aprire il file JSON in un editor di testo normale e modificarlo per includere la risorsa, i tipi di evento e la destinazione Amazon SNS desiderata per la regola.

   L'esempio seguente mostra una regola di notifica denominata **MyNotificationRule** per un repository denominato *MyDemoRepo* in un AWS account con l'ID. *123456789012* Le notifiche con il tipo di dettaglio completo vengono inviate a un argomento di Amazon SNS denominato *MyNotificationTopic* quando vengono creati rami e tag.

```
{
    "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"
}
```

Salvare il file.

3. Utilizzando il file appena modificato, dal terminale o dalla riga di comando, eseguire nuovamente il comando create-notification-rule per creare la regola di notifica:

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

4. In caso di esito positivo, il comando restituisce l'ARN della regola di notifica, simile al seguente.

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

Per elencare i tipi di eventi per le regole di notifica (AWS CLI)

1. Da un terminale o dal prompt dei comandi, eseguire il comando list-event-types. È possibile utilizzare l'opzione `--filters` per limitare la risposta a un tipo di risorsa specifico o ad un altro attributo. Ad esempio, quanto segue restituisce un elenco di tipi di eventi per CodeDeploy le applicazioni.

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

2. Questo comando genera un output simile al seguente.

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

Per aggiungere un tag a una regola di notifica (AWS CLI)

1. Da un terminale o dal prompt dei comandi, eseguire il comando tag-resource. Ad esempio, utilizzate il comando seguente per aggiungere una coppia chiave-valore di tag contenente il nome *Team* e il valore. *Li_Juan*

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

2. Questo comando genera un output simile al seguente.

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

Visualizzazione delle regole di notifica

Puoi utilizzare la console Developer Tools o AWS CLI visualizzare tutte le regole di notifica per tutte le risorse in una AWS regione. Puoi anche visualizzare i dettagli di ciascuna regola di notifica. A differenza del processo di creazione di una regola di notifica, non è necessario passare alla pagina della risorsa.

Per visualizzare le regole di notifica (console)

1. Apri la console AWS Developer Tools in https://console.aws.amazon.com/codesuite/impostazioni/notifiche.
2. Nella barra di navigazione, espandere Settings (Impostazioni), quindi scegliere Notification rules (Regole di notifica).
3. In Regole di notifica, esamina l'elenco delle regole configurate per le tue risorse nella pagina Account AWS in Regione AWS cui hai attualmente effettuato l'accesso. Utilizzare il selettore per cambiare la Regione AWS.
4. Per visualizzare i dettagli di una regola di notifica, selezionarla dall'elenco, quindi scegliere View details (Visualizza dettagli). È anche possibile semplicemente scegliere il nome nell'elenco.

Per visualizzare un elenco di regole di notifica (AWS CLI)

1. In un terminale o nel prompt dei comandi, esegui il list-notification-rules comando per visualizzare tutte le regole di notifica per la AWS regione specificata.

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

2. In caso di successo, questo comando restituisce l'ID e l'ARN per ogni regola di notifica nella AWS regione, in modo simile al seguente.

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

Per visualizzare i dettagli di una regola di notifica (AWS CLI)

1. Da un terminale o dal prompt dei comandi, eseguire il comando describe-notification-rule, specificando l'ARN della regola di notifica.

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

2. Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{
    "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"
}
```

Per visualizzare un elenco di tag per una regola di notifica (AWS CLI)

1. Da un terminale o dal prompt dei comandi, eseguire il comando list-tags-for-resource per visualizzare tutti i tag per un ARN della regola di notifica specificata.

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

2. Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente.

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

Modifica di una regola di notifica

Puoi modificare una regola di notifica per cambiarne il nome, gli eventi per i quali invia le notifiche, il tipo di dettaglio o la destinazione o le destinazioni a cui invia le notifiche. Puoi utilizzare la console Developer Tools o AWS CLI modificare una regola di notifica.

Per modificare una regola di notifica (console)

1. Apri la console AWS Developer Tools in https://console.aws.amazon.com/codesuite/impostazioni/notifiche.
2. Nella barra di navigazione, espandere Settings (Impostazioni), quindi scegliere Notification rules (Regole di notifica).
3. In Regole di notifica, esamina le regole configurate per le risorse del tuo AWS account nel luogo in Regione AWS cui hai attualmente effettuato l'accesso. Utilizzare il selettore per cambiare la Regione AWS.
4. Scegliere la regola dall'elenco e quindi scegliere Edit (Modifica). Apportare le modifiche, quindi fare clic su Submit (Invia).

Per modificare una regola di notifica (AWS CLI)

1. In un terminale o nel prompt dei comandi, esegui il describe-notification-rulecomando per visualizzare la struttura della regola di notifica.

2. Eseguire il comando update-notification rule per generare lo skeleton JSON e salvarlo in un file.

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

È possibile assegnare al file un nome qualsiasi. In questo esempio, il file è*update.json*.

3. Aprire il file JSON in un editor di testo normale e apportare modifiche alla regola.

L'esempio seguente mostra una regola di notifica denominata **MyNotificationRule** per un repository denominato *MyDemoRepo* in un AWS account con l'ID*123456789012*. Le notifiche vengono inviate a un argomento di Amazon SNS denominato *MyNotificationTopic* quando vengono creati rami e tag. Il nome della regola viene modificato in. *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"
}
```

Salvare il file.

4. Utilizzando il file appena modificato, dal terminale o dalla riga di comando, eseguire nuovamente il comando update-notification-rule per aggiornare la regola di notifica.

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

5. In caso di esito positivo, il comando restituisce l'Amazon Resource Name (ARN) della regola di notifica, simile al seguente.

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

Per rimuovere un tag da una regola di destinazione (AWS CLI)

1. Da un terminale o dal prompt dei comandi, eseguire il comando untag-resource. Ad esempio, il comando seguente rimuove un tag con il nome di*Team*.

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

2. In caso di successo, questo comando non restituisce alcun risultato.

Consulta anche

- Aggiungere o rimuovere una destinazione per una regola di notifica
- Abilitazione o disabilitazione delle notifiche per una regola di notifica
- Eventi

Abilitazione o disabilitazione delle notifiche per una regola di notifica

Quando crei una regola di notifica, le notifiche sono abilitate per impostazione predefinita. Non è necessario eliminare la regola per impedire l'invio delle notifiche. Puoi semplicemente modificarne lo stato di notifica.

Per modificare lo stato di notifica per una regola di notifica (console)

1. Apri la console AWS Developer Tools in https://console.aws.amazon.com/codesuite/impostazioni/notifiche.
2. Nella barra di navigazione, espandere Settings (Impostazioni), quindi scegliere Notification rules (Regole di notifica).
3. In Regole di notifica, esamina le regole configurate per le risorse del tuo AWS account nel luogo in Regione AWS cui hai attualmente effettuato l'accesso. Utilizzare il selettore per cambiare la Regione AWS.

4. Individuare la regola di notifica che si desidera abilitare o disabilitare e selezionarla per visualizzarne i dettagli.
5. In Notification status (Stato di notifica), selezionare il cursore per modificare lo stato della regola:
   - Sending notifications (Invio di notifiche): questa è l'impostazione predefinita.
   - Notifications paused (Notifiche in pausa): nessuna notifica viene inviata alle destinazioni specificate.

Per modificare lo stato di notifica per una regola di notifica (AWS CLI)

1. Seguire i passaggi in Per modificare una regola di notifica (AWS CLI) per ottenere il JSON per la regola di notifica.
2. Modificare il campo `Status` su `ENABLED` (predefinito) o `DISABLED` (nessuna notifica), quindi eseguire il comando update-notification-rule per modificare lo stato.

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

Eliminazione di una regola di notifica

Possono essere configurate solo 10 regole di notifica per risorsa, pertanto è consigliabile eliminare le regole non più necessarie. Puoi utilizzare la console Developer Tools o AWS CLI eliminare una regola di notifica.

> **Note**
>
> Non è possibile annullare l'eliminazione di una regola di notifica, ma è possibile ricrearla. L'eliminazione di una regola di notifica non elimina la destinazione.

Per eliminare una regola di notifica (console)

1. Apri la console AWS Developer Tools in https://console.aws.amazon.com/codesuite/impostazioni/notifiche.
2. Nella barra di navigazione, espandere Settings (Impostazioni), quindi scegliere Notification rules (Regole di notifica).

3. In Regole di notifica, esamina le regole configurate per le risorse del tuo AWS account nel luogo in Regione AWS cui hai attualmente effettuato l'accesso. Utilizzare il selettore per cambiare la Regione AWS.
4. Scegliere la regola di notifica e quindi scegliere Delete (Elimina).
5. Digitare **`delete`** e scegliere Delete (Elimina).

Per eliminare una regola di notifica (AWS CLI)

1. Da un terminale o dal prompt dei comandi, eseguire il comando delete-notification-rule, specificando l'ARN della regola di notifica.

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

2. In caso di esito positivo, il comando restituisce l'ARN della regola di notifica eliminata, simile al seguente.

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

Utilizzo delle destinazioni delle regole di notifica

Una destinazione delle regole di notifica è una destinazione che definisce dove inviare le notifiche quando si verificano le condizioni dell'evento di una regola di notifica. Puoi scegliere tra argomenti di Amazon SNS e client Chatbot AWS configurati per i canali Slack o Microsoft Teams. Puoi creare un argomento Amazon SNS come destinazione come parte della creazione di una regola di notifica (scelta consigliata). Puoi anche scegliere un argomento Amazon SNS esistente nella stessa AWS regione della regola di notifica, ma devi configurarlo con la politica richiesta. Se scegli di utilizzare un client AWS Chatbot come obiettivo, devi prima creare quel client in AWS Chatbot.

Se desideri estendere la portata delle notifiche, puoi configurare manualmente l'integrazione tra notifiche e AWS Chatbot in modo che le notifiche vengano inviate alle chat room di Amazon Chime. Puoi quindi scegliere l'argomento Amazon SNS configurato per quel client Chatbot AWS come destinazione per la regola di notifica. Per ulteriori informazioni, consulta Per integrare le notifiche con AWS Chatbot e Amazon Chime.

Puoi utilizzare la console Developer Tools o gestire gli AWS CLI obiettivi di notifica. Puoi utilizzare la console o AWS CLI per creare e configurare argomenti Amazon SNS e client Chatbot come AWS destinazioni. Puoi anche configurare l'integrazione tra gli argomenti di Amazon SNS che configuri come destinazioni e Chatbot AWS . Questo ti permette di inviare notifiche alle chat room Amazon Chime. Per ulteriori informazioni, consulta Configurare l'integrazione tra notifiche e AWS Chatbot.

Argomenti

- Creazione o configurazione di una destinazione delle regole di notifica
- Visualizzazione delle destinazioni delle regole di notifica
- Aggiungere o rimuovere una destinazione per una regola di notifica
- Eliminazione di una destinazione delle regole di notifica

Creazione o configurazione di una destinazione delle regole di notifica

Gli obiettivi delle regole di notifica sono gli argomenti di Amazon SNS o i client Chatbot AWS configurati per i canali Slack o Microsoft Teams.

È necessario creare un client AWS Chatbot prima di poter selezionare un client come destinazione. Quando scegli un client AWS Chatbot come obiettivo per una regola di notifica, viene configurato un argomento Amazon SNS per quel client AWS Chatbot con tutte le politiche necessarie per l'invio delle notifiche al canale Slack o Microsoft Teams. Non è necessario configurare argomenti Amazon SNS esistenti per il client AWS Chatbot.

È possibile creare destinazioni delle regole di notifica di Amazon SNS nella console Strumenti di sviluppo al momento della creazione di una regola di notifica. La policy che consente l'invio di notifiche all'argomento viene applicata automaticamente. Questo è il modo più semplice per creare una destinazione per una regola di notifica. Per ulteriori informazioni, consulta Creazione di una regola di notifica.

Se utilizzi un argomento Amazon SNS esistente, è necessario configurarlo con una policy di accesso che consenta alla risorsa di inviare notifiche all'argomento. Per vedere un esempio, consulta Configura gli argomenti di Amazon SNS per le notifiche.

> **Note**
>
> Se desideri utilizzare un argomento Amazon SNS esistente invece di crearne uno nuovo, in Targets (Destinazioni), scegli il relativo ARN. Assicurati che l'argomento disponga delle policy di accesso appropriate e che l'elenco degli iscritti contenga solo gli utenti autorizzati

a visualizzare le informazioni sulla risorsa. Se l'argomento Amazon SNS è un argomento utilizzato per CodeCommit le notifiche prima del 5 novembre 2019, conterrà una politica che consente la pubblicazione su CodeCommit di esso con autorizzazioni diverse da quelle richieste per le notifiche. AWS CodeStar L'utilizzo di questi argomenti è sconsigliato. Se desideri utilizzarne uno creato per quell'esperienza, devi aggiungere la politica richiesta per AWS CodeStar le notifiche oltre a quella già esistente. Per ulteriori informazioni, consulta Configura gli argomenti di Amazon SNS per le notifiche e Comprendere contenuti e sicurezza delle notifiche.

Se desideri estendere la portata delle notifiche, puoi configurare manualmente l'integrazione tra notifiche e AWS Chatbot in modo che le notifiche vengano inviate alle chat room di Amazon Chime. Per ulteriori informazioni, consulta Destinazioni e Per integrare le notifiche con AWS Chatbot e Amazon Chime.

Per configurare un argomento Amazon SNS esistente per l'utilizzo come una destinazione della regola di notifica (console)

1. Accedi AWS Management Console e apri la console Amazon SNS nella versione v3/home. https://console.aws.amazon.com/sns/
2. Nella barra di navigazione scegli Topics (Argomenti). Scegli l'argomento, quindi seleziona Edit (Modifica).
3. Espandi Access policy (Policy di accesso), quindi scegli Advanced (Avanzate).
4. Nell'editor JSON, aggiungi la seguente istruzione alla policy. Includi l'ARN Regione AWS, l' Account AWS ID e il nome dell'argomento.

```
{
     "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"
   }
```

L'istruzione della policy dovrebbe essere simile alla seguente:

```
{
  "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"
      ],
      "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. Scegli Save changes (Salva modifiche).
6. In Subscriptions (Sottoscrizioni), esamina l'elenco degli iscritti agli argomenti. Aggiungere, modificare o eliminare iscritti come appropriato per questa destinazione delle regole di notifica. Assicurati che l'elenco degli iscritti contenga solo gli utenti che sono autorizzati a visualizzare le informazioni sulla risorsa. Per ulteriori informazioni, consulta Comprendere contenuti e sicurezza delle notifiche.

Per creare un client AWS Chatbot con Slack da utilizzare come destinazione

1. Seguire le istruzioni riportate in Setting up AWS Chatbot with Slack (Configurazione di AWS Chatbot con Slack) nella Guida per l'amministratore di AWS Chatbot. Quando esegui questa operazione, prendi in considerazione le seguenti opzioni per un'integrazione ottimale con le notifiche:
   - Quando crei un ruolo IAM, è consigliabile scegliere un nome del ruolo che consenta di identificare facilmente le finalità di questo ruolo (ad esempio **`AWSCodeStarNotifications-Chatbot-Slack-Role`**). Questo può aiutarti a identificare le finalità del ruolo in futuro.
   - Negli argomenti SNS, non è necessario scegliere un argomento o una regione. AWS Quando scegli il client AWS Chatbot come destinazione, viene creato e configurato un argomento Amazon SNS con tutte le autorizzazioni richieste per il client AWS Chatbot come parte del processo di creazione delle regole di notifica.
2. Completa il processo di creazione del client. Questo client è quindi disponibile e potrai selezionarlo come destinazione durante la creazione di regole di notifica. Per ulteriori informazioni, consulta Creazione di una regola di notifica.

> **Note**
>
> Non rimuovere l'argomento Amazon SNS dal client Chatbot AWS dopo che è stato configurato per te. In questo modo si impedirà l'invio di notifiche a Slack.

Per creare un client AWS Chatbot con Microsoft Teams da utilizzare come destinazione

1. Seguire le istruzioni riportate in Setting up AWS Chatbot with Microsoft Teams (Configurazione di AWS Chatbot con Microsoft Teams) nella Guida per l'amministratore di AWS Chatbot. Quando

esegui questa operazione, prendi in considerazione le seguenti opzioni per un'integrazione ottimale con le notifiche:

- Quando crei un ruolo IAM, è consigliabile scegliere un nome del ruolo che consenta di identificare facilmente le finalità di questo ruolo (ad esempio **`AWSCodeStarNotifications-Chatbot-Microsoft-Teams-Role`**). Questo può aiutarti a identificare le finalità del ruolo in futuro.
- Negli argomenti SNS, non è necessario scegliere un argomento o una AWS regione. Quando scegli il client AWS Chatbot come destinazione, viene creato e configurato un argomento Amazon SNS con tutte le autorizzazioni richieste per il client AWS Chatbot come parte del processo di creazione delle regole di notifica.

2. Completa il processo di creazione del client. Questo client è quindi disponibile e potrai selezionarlo come destinazione durante la creazione di regole di notifica. Per ulteriori informazioni, consulta Creazione di una regola di notifica.

> **Note**
>
> Non rimuovere l'argomento Amazon SNS dal client Chatbot AWS dopo che è stato configurato per te. In questo modo si impedirà l'invio di notifiche a Microsoft Teams.

Visualizzazione delle destinazioni delle regole di notifica

Puoi utilizzare la console Developer Tools, non la console Amazon SNS per visualizzare tutti gli obiettivi delle regole di notifica per tutte le risorse in una AWS regione. Puoi anche visualizzare i dettagli di una destinazione delle regole di notifica.

Per visualizzare le destinazioni delle regole di notifica (console)

1. Apri la console AWS Developer Tools in https://console.aws.amazon.com/codesuite/impostazioni/notifiche.
2. Nella barra di navigazione, espandere Settings (Impostazioni), quindi scegliere Notification rules (Regole di notifica).
3. In Obiettivi delle regole di notifica, esamina l'elenco degli obiettivi utilizzati dalle regole di notifica nella pagina Account AWS in Regione AWS cui hai attualmente effettuato l'accesso. Utilizzare il selettore per cambiare la Regione AWS. Se lo stato della destinazione è Unreachable

(Irraggiungibile), potrebbe essere necessario svolgere delle verifiche. Per ulteriori informazioni, consulta Risoluzione dei problemi .

Per visualizzare un elenco di destinazioni delle regole di notifica (AWS CLI)

1. Da un terminale o dal prompt dei comandi, eseguire il comando list-targets per visualizzare un elenco di tutte le destinazioni delle regole di notifica per la regione AWS specificata:

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

2. In caso di successo, questo comando restituisce l'ID e l'ARN per ogni regola di notifica nella AWS regione, in modo simile al seguente:

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

Aggiungere o rimuovere una destinazione per una regola di notifica

Puoi modificare una regola di notifica per cambiare la destinazione o le destinazioni a cui invia le notifiche. È possibile utilizzare la console Developer Tools oppure AWS CLI modificare gli obiettivi di una regola di notifica.

Per modificare le destinazioni per una regola di notifica (console)

1. Apri la console AWS Developer Tools in https://console.aws.amazon.com/codesuite/impostazioni/notifiche.
2. Nella barra di navigazione, espandere Settings (Impostazioni), quindi scegliere Notification rules (Regole di notifica).
3. In Regole di notifica, consulta l'elenco delle regole configurate per le risorse del tuo AWS account nella pagina in Regione AWS cui hai attualmente effettuato l'accesso. Utilizzare il selettore per cambiare la Regione AWS.
4. Scegliere la regola, quindi selezionare Edit (Modifica).
5. In Targets (Destinazioni), procedere in uno dei seguenti modi:
   - Per aggiungere un altro target, scegli Aggiungi target, quindi scegli l'argomento Amazon SNS o il client AWS Chatbot (Slack) o AWS Chatbot (Microsoft Teams) che desideri aggiungere dall'elenco. È inoltre possibile scegliere Create SNS topic (Crea argomento SNS) per creare un argomento e aggiungerlo come destinazione. Una regola di notifica può avere fino a 10 destinazioni.
   - Per rimuovere una destinazione, scegliere Remove target (Rimuovi target) accanto alla destinazione da rimuovere.
6. Scegli Invia.

Per aggiungere una destinazione a una regola di notifica (AWS CLI)

1. Al terminale o al prompt dei comandi, eseguire il comando subscribe per aggiungere una destinazione. Ad esempio, il comando seguente aggiunge un argomento Amazon SNS come destinazione per una regola di notifica.

```
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. In caso di esito positivo, il comando restituisce l'ARN della regola di notifica aggiornata, simile al seguente.

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

Per rimuovere una destinazione da una regola di notifica (AWS CLI)

1. Al terminale o al prompt dei comandi, eseguire il comando unsubscribe per rimuovere una destinazione. Ad esempio, il comando seguente rimuove un argomento Amazon SNS come destinazione per una regola di notifica.

```
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. In caso di esito positivo, il comando restituisce l'ARN della regola di notifica aggiornata e informazioni relative alla destinazione rimossa, simili alle seguenti.

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

Consulta anche

- Modifica di una regola di notifica
- Abilitazione o disabilitazione delle notifiche per una regola di notifica

Eliminazione di una destinazione delle regole di notifica

È possibile eliminare una destinazione se non è più necessaria. Per una risorsa possono essere configurate solo 10 destinazioni delle regole di notifica, pertanto l'eliminazione di destinazioni

non necessarie permette di creare spazio per altre destinazioni che potrebbe essere necessario aggiungere a tale regola di notifica.

> **Note**
>
> L'eliminazione di una destinazione delle regole di notifica rimuove la destinazione da tutte le regole di notifica configurate per l'utilizzo come destinazione, ma non elimina la destinazione stessa.

Per eliminare una destinazione delle regole di notifica (console)

1. Apri la console AWS Developer Tools in https://console.aws.amazon.com/codesuite/impostazioni/notifiche.
2. Nella barra di navigazione, espandere Settings (Impostazioni), quindi scegliere Notification rules (Regole di notifica).
3. In Obiettivi delle regole di notifica, esamina l'elenco degli obiettivi configurati per le risorse del tuo AWS account nella pagina in Regione AWS cui hai attualmente effettuato l'accesso. Utilizzare il selettore per cambiare la Regione AWS.
4. Scegliere la destinazione della regola di notifica e quindi selezionare Delete (Elimina).
5. Digitare **`delete`** e scegliere Delete (Elimina).

Per eliminare una destinazione delle regole di notifica (AWS CLI)

1. Da un terminale o dal prompt dei comandi, eseguire il comando delete-target, specificando l'ARN della destinazione. Ad esempio, il comando seguente elimina una destinazione che utilizza un argomento Amazon SNS.

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

2. In caso di esito positivo, il comando non restituisce alcun risultato. In caso di esito negativo, il comando restituisce un errore. L'errore più comune è che l'argomento è la destinazione di una o più regole di notifica.

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

Puoi utilizzare il parametro `--force-unsubscribe-all` per rimuovere la destinazione da tutte le regole di notifica configurate per utilizzarla come una destinazione, quindi eliminare la destinazione.

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

Configurare l'integrazione tra notifiche e AWS Chatbot

AWS Chatbot è un AWS servizio che consente ai team di DevOps sviluppo software di utilizzare le chat room di Amazon Chime, i canali Slack e i canali Microsoft Team per monitorare e rispondere agli eventi operativi in. Cloud AWS Puoi configurare l'integrazione tra gli obiettivi delle regole di notifica e il AWS Chatbot in modo che le notifiche sugli eventi vengano visualizzate nella stanza Amazon Chime, nel canale Slack o nel canale Microsoft Teams che preferisci. Per ulteriori informazioni, consultare la documentazione di AWS Chatbot.

Prima di configurare l'integrazione con AWS Chatbot, devi configurare una regola di notifica e un obiettivo della regola. Per ulteriori informazioni, consulta Configurazione e Creazione di una regola di notifica. È inoltre necessario configurare un canale Slack, Microsoft Teams o una chat room Amazon Chime in AWS Chatbot. Per ulteriori informazioni, consulta la documentazione per questi servizi.

Argomenti

- Configura un client AWS Chatbot per un canale Slack
- Configurare un client AWS Chatbot per un canale Microsoft Teams
- Configurazione manuale dei client per Slack o Amazon Chime

Configura un client AWS Chatbot per un canale Slack

Puoi creare regole di notifica che utilizzano un client AWS Chatbot come destinazione. Se crei un client per un canale Slack, puoi utilizzarlo direttamente come destinazione nel flusso di lavoro per creare una regola di notifica. Questo è il modo più semplice per impostare le notifiche che appaiono nei canali Slack.

Per creare un client AWS Chatbot con Slack da utilizzare come destinazione

1. Seguire le istruzioni riportate in Setting up AWS Chatbot with Slack (Configurazione di AWS Chatbot con Slack) nella Guida per l'amministratore di AWS Chatbot. Quando esegui questa operazione, prendi in considerazione le seguenti opzioni per un'integrazione ottimale con le notifiche:

   - Quando crei un ruolo IAM, è consigliabile scegliere un nome del ruolo che consenta di identificare facilmente le finalità di questo ruolo (ad esempio **`AWSCodeStarNotifications-Chatbot-Slack-Role`**). Questo può aiutarti a identificare le finalità del ruolo in futuro.
   - Negli argomenti SNS, non è necessario scegliere un argomento o una regione. AWS Quando scegli il client AWS Chatbot come destinazione, viene creato e configurato un argomento Amazon SNS con tutte le autorizzazioni richieste per il client AWS Chatbot come parte del processo di creazione delle regole di notifica.
2. Completa il processo di creazione del client. Questo client è quindi disponibile e potrai selezionarlo come destinazione durante la creazione di regole di notifica. Per ulteriori informazioni, consulta Creazione di una regola di notifica.

   > **Note**
   >
   > Non rimuovere l'argomento Amazon SNS dal client Chatbot AWS dopo che è stato configurato per te. In questo modo si impedirà l'invio di notifiche a Slack.

Configurare un client AWS Chatbot per un canale Microsoft Teams

Puoi creare regole di notifica che utilizzano un client AWS Chatbot come destinazione. Se crei un client per un canale Microsoft Teams, puoi utilizzarlo direttamente come destinazione nel flusso di lavoro per creare una regola di notifica. Questo è il modo più semplice per impostare le notifiche che appaiono nei canali Microsoft Teams.

Per creare un client AWS Chatbot con Microsoft Teams da utilizzare come destinazione

1. Seguire le istruzioni riportate in Setting up AWS Chatbot with Microsoft Teams (Configurazione di AWS Chatbot con Microsoft Teams) nella Guida per l'amministratore di AWS Chatbot. Quando esegui questa operazione, prendi in considerazione le seguenti opzioni per un'integrazione ottimale con le notifiche:

- Quando crei un ruolo IAM, è consigliabile scegliere un nome del ruolo che consenta di identificare facilmente le finalità di questo ruolo (ad esempio **`AWSCodeStarNotifications-Chatbot-Microsoft-Teams-Role`**). Questo può aiutarti a identificare le finalità del ruolo in futuro.
- Negli argomenti SNS, non è necessario scegliere un argomento o una AWS regione. Quando scegli il client AWS Chatbot come destinazione, viene creato e configurato un argomento Amazon SNS con tutte le autorizzazioni richieste per il client AWS Chatbot come parte del processo di creazione delle regole di notifica.

2. Completa il processo di creazione del client. Questo client è quindi disponibile e potrai selezionarlo come destinazione durante la creazione di regole di notifica. Per ulteriori informazioni, consulta Creazione di una regola di notifica.

> **Note**
>
> Non rimuovere l'argomento Amazon SNS dal client Chatbot AWS dopo che è stato configurato per te. In questo modo si impedirà l'invio di notifiche a Microsoft Teams.

Configurazione manuale dei client per Slack o Amazon Chime

Puoi scegliere di creare l'integrazione tra notifiche e Slack o Amazon Chime direttamente. Questo è l'unico metodo disponibile per configurare le notifiche alle chat room Amazon Chime. Quando configuri questa integrazione manualmente, crei un client AWS Chatbot che utilizza un argomento Amazon SNS che hai precedentemente configurato come destinazione per una regola di notifica.

Per integrare manualmente le notifiche con AWS Chatbot e Slack

1. Apri la console AWS Developer Tools in impostazioni/notifichehttps://console.aws.amazon.com/codesuite/.
2. Scegliere Settings (Impostazioni), quindi selezionare Notification rules (Regole di notifica).
3. In Notification rule targets (Destinazioni regola di notifica), individuare e copiare la destinazione.

> **Note**
>
> È possibile configurare più regole di notifica per utilizzare lo stesso argomento Amazon SNS come sua destinazione. Questo consente di consolidare la messaggistica, ma

può avere conseguenze indesiderate se l'elenco di iscrizioni è specifico di una regola di notifica o risorsa.

4. Apri la console AWS Chatbot all'indirizzo. https://console.aws.amazon.com/chatbot/
5. Scegliere Configure new client (Configura nuovo client), quindi scegliere Slack.
6. Scegli Configura.
7. Accedere all'area di lavoro Slack.
8. Se viene chiesto di confermare le scelte, scegliere Allow (Consenti).
9. Scegliere Configure new channel (Configura nuovo canale).
10. In Configuration details (Dettagli configurazione), in Configuration name (Nome configurazione), immettere un nome per il client. Questo è il nome che verrà visualizzato nell'elenco delle destinazioni disponibili per il tipo di destinazione AWS Chatbot (Slack) quando si creano regole di notifica.
11. In Configura canale Slack, in Tipo di canale, scegliere Pubblico o Privato, a seconda del tipo di canale da integrare.
    - In Public channel (Canale pubblico), scegliere il nome del canale Slack dall'elenco.
    - In Private channel ID (ID canale privato), immettere il codice o l'URL del canale.
12. In IAM permissions (Autorizzazioni IAM), in Role (Ruolo), scegliere Create an IAM role using a template (Crea un ruolo IAM utilizzando un modello). In Policy templates (Modelli di policy), scegliere Notification permissions (Autorizzazioni di notifica). In Role name (Nome ruolo), immettere un nome per questo ruolo, ad esempio **`AWSCodeStarNotifications-Chatbot-Slack-Role`**. In Policy templates (Modelli di policy), scegliere Notification permissions (Autorizzazioni di notifica).
13. Negli argomenti SNS, in Regione SNS, scegli il Regione AWS luogo in cui hai creato l'obiettivo della regola di notifica. In SNS topics (Argomenti SNS), scegliere il nome dell'argomento Amazon SNS configurato come la destinazione delle regole di notifica.

    Note

    Questo passaggio non è necessario se si creerà una regola di notifica utilizzando questo client come destinazione.

14. Scegli Configura.

> **Note**
>
> Se è stata configurata l'integrazione con un canale privato, è necessario invitare AWS Chatbot al canale prima di visualizzare le notifiche in quel canale. Per ulteriori informazioni, consultare la documentazione di AWS Chatbot.

15. (Facoltativo) Per testare l'integrazione, apportare una modifica nella risorsa che corrisponde a un tipo di evento per una regola di notifica configurata per utilizzare l'argomento Amazon SNS come sua destinazione. Ad esempio, se si dispone di una regola di notifica configurata per inviare notifiche quando vengono effettuati commenti su una richiesta pull, aggiungere un commento a una richiesta pull e guardare il canale Slack nel browser per vedere quando la notifica viene visualizzata.

Per integrare le notifiche con AWS Chatbot e Amazon Chime

1. Apri la console AWS Developer Tools in impostazioni/notifichehttps://console.aws.amazon.com/codesuite/.
2. Scegliere Settings (Impostazioni), quindi selezionare Notification rules (Regole di notifica).
3. In Notification rule targets (Destinazioni regola di notifica), individuare e copiare la destinazione.

> **Note**
>
> È possibile configurare più regole di notifica per utilizzare lo stesso argomento Amazon SNS come sua destinazione. Questo consente di consolidare la messaggistica, ma può anche avere conseguenze indesiderate se l'elenco di iscrizioni è specifico di una regola di notifica o risorsa.

4. In Amazon Chime aprire la chat room da configurare per l'integrazione.
5. Selezionare l'icona a forma di ingranaggio nell'angolo in alto a destra e scegliere Manage webhooks (Gestisci webhook).
6. Nella finestra di dialogo Manage webhooks (Gestisci webhook), scegliere New (Nuovo), immettere un nome per il webhook e scegliere Create (Crea).
7. Verificare che il webhook sia visualizzato, quindi scegliere Copy webhook URL (Copia URL webhook).
8. Apri la console AWS Chatbot all'indirizzo. https://console.aws.amazon.com/chatbot/

9. Scegliere Configure new client (Configura nuovo client), quindi scegliere Amazon Chime.
10. In Configuration details (Dettagli configurazione), in Configuration name (Nome configurazione), immettere un nome per il client.
11. In Webhook URL (URL webhook), incollare l'URL. In Webhook description (Descrizione webhook), fornire una descrizione facoltativa.
12. In IAM permissions (Autorizzazioni IAM), in Role (Ruolo), scegliere Create an IAM role using a template (Crea un ruolo IAM utilizzando un modello). In Policy templates (Modelli di policy), scegliere Notification permissions (Autorizzazioni di notifica). In Role name (Nome ruolo), immettere un nome per questo ruolo, ad esempio **`AWSCodeStarNotifications-Chatbot-Chime-Role`**.
13. Negli argomenti SNS, in Regione SNS, scegli il Regione AWS luogo in cui hai creato l'obiettivo della regola di notifica. In SNS topics (Argomenti SNS), scegliere il nome dell'argomento Amazon SNS configurato come la destinazione delle regole di notifica.
14. Scegli Configura.
15. (Facoltativo) Per testare l'integrazione, apportare una modifica nella risorsa che corrisponde a un tipo di evento per una regola di notifica configurata per utilizzare l'argomento Amazon SNS come sua destinazione. Ad esempio, se si dispone di una regola di notifica configurata per inviare notifiche quando vengono effettuati commenti su una richiesta pull, aggiungere un commento a una richiesta pull e quindi guardare la chat room Amazon Chime per vedere quando la notifica viene visualizzata.

Registrazione delle chiamate API di AWS CodeStar notifica con AWS CloudTrail

AWS CodeStar Notifications è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio. CloudTrail acquisisce tutte le chiamate API per le notifiche come eventi. Le chiamate acquisite includono chiamate dalla console Developer Tools e chiamate di codice alle operazioni dell'API AWS CodeStar Notifications. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per le notifiche. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata a AWS CodeStar Notifications, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli.

Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.

AWS CodeStar Informazioni sulle notifiche in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività nelle AWS CodeStar Notifiche, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella Cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi del tuo Account AWS, compresi gli eventi per AWS CodeStar le notifiche, crea una traccia. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte AWS CodeStar le azioni di notifica vengono registrate CloudTrail e documentate in. *AWS CodeStar Notifications API Reference* Ad esempio, le chiamate alle operazioni `CreateNotificationRule`, `Subscribe` e `ListEventTypes` generano voci nei file di log CloudTrail.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle voci dei file di log di

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che dimostra la creazione di una regola di notifica, che include `CreateNotificationRule` sia `Subscribe` le azioni che.

> **Note**
>
> Alcuni degli eventi nelle voci del file di log delle notifiche potrebbero provenire dal ruolo collegato ai servizi 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"
}
```

Risoluzione dei problemi

Le informazioni seguenti possono essere utili per risolvere problemi comuni relativi alle notifiche.

Argomenti

- Quando cerco di creare una regola di notifica su una risorsa viene visualizzato un errore di autorizzazione
- Non riesco a visualizzare le regole di notifica
- Non riesco a creare regole di notifica
- Ricevo notifiche per una risorsa a cui non posso accedere
- Non ricevo alcuna notifica di Amazon SNS
- Ricevo notifiche duplicate sugli eventi
- Voglio capire perché uno stato di destinazione di notifica viene indicato come irraggiungibile
- Voglio aumentare le mie quote per le notifiche e le risorse

Quando cerco di creare una regola di notifica su una risorsa viene visualizzato un errore di autorizzazione

Assicurati di disporre di autorizzazioni sufficienti. Per ulteriori informazioni, consulta Esempi di policy basate su identità.

Non riesco a visualizzare le regole di notifica

Problema: Quando ti trovi nella console Strumenti di sviluppo e selezioni Notifications (Notifiche) in Settings (Impostazioni), viene visualizzato un errore di autorizzazione.

Possibili soluzioni: Potresti non disporre delle autorizzazioni necessarie per visualizzare le notifiche. Sebbene la maggior parte delle politiche gestite per i servizi AWS Developer Tools CodePipeline, come CodeCommit e, includano le autorizzazioni per le notifiche, i servizi che attualmente non supportano le notifiche non includono le autorizzazioni per visualizzarle. In alternativa, potrebbe essere applicata una policy personalizzata al ruolo o all'utente IAM che non consente di visualizzare le notifiche. Per ulteriori informazioni, consulta Esempi di policy basate su identità.

Non riesco a creare regole di notifica

Potresti non disporre delle autorizzazioni necessarie per creare una regola di notifica. Per ulteriori informazioni, consulta Esempi di policy basate su identità.

Ricevo notifiche per una risorsa a cui non posso accedere

Quando crei una regola di notifica e aggiungi una destinazione, la caratteristica di notifica non convalida se il destinatario ha accesso alla risorsa. È possibile ricevere notifiche relative a una risorsa a cui non puoi accedere. Se non riesci a rimuoverti autonomamente, chiedi di essere rimosso dall'elenco di iscrizioni per la destinazione.

Non ricevo alcuna notifica di Amazon SNS

Per risolvere i problemi relativi all'argomento Amazon SNS, verifica quanto segue:

- Assicurati che l'argomento Amazon SNS sia stato creato nella stessa AWS regione della regola di notifica.
- Assicurati di aver effettuato l'iscrizione del tuo alias e-mail all'argomento corretto e di averla confermata. Per ulteriori informazioni, consulta Iscrizione di un endpoint a un argomento Amazon SNS.
- Verifica che la politica dell'argomento sia stata modificata per consentire a AWS CodeStar Notifications di inviare notifiche a quell'argomento. La policy dell'argomento deve includere un'istruzione simile alla seguente:

```
{
    "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"
        }
    }
```

```
}
```

Per ulteriori informazioni, consulta Configura gli argomenti di Amazon SNS per le notifiche.

Ricevo notifiche duplicate sugli eventi

Ecco i motivi più comuni che comportano la ricezione di più notifiche:

- Sono state configurate più regole di notifica che includono lo stesso tipo di evento per una risorsa e sei iscritto agli argomenti Amazon SNS che sono le destinazioni di queste regole. Per risolvere questo problema, annulla l'iscrizione a uno degli argomenti o modifica le regole di notifica per rimuovere duplicati.
- Uno o più obiettivi delle regole di notifica sono integrati con AWS Chatbot e ricevi notifiche nella tua casella di posta elettronica e in un canale Slack, nel canale Microsoft Teams o nella chat room di Amazon Chime. Per risolvere questo problema, valuta se annullare l'iscrizione dell'indirizzo e-mail all'argomento Amazon SNS che è la destinazione per la regola e utilizzare il canale Slack, il canale Microsoft Teams o la chat room Amazon Chime per visualizzare le notifiche.

Voglio capire perché uno stato di destinazione di notifica viene indicato come irraggiungibile

Le destinazioni hanno due possibili stati: Attivo e Non raggiungibile. Non raggiungibile indica che le notifiche sono state inviate a una destinazione e la consegna non è riuscita. Le notifiche continuano a essere inviate a tale destinazione e, in caso di esito positivo, lo stato viene reimpostato su Attivo.

La destinazione di una regola di notifica potrebbe non essere disponibile per uno dei seguenti motivi:

- La risorsa (argomento Amazon SNS o client Chatbot) è AWS stata eliminata. Scegli un'altra destinazione per la regola di notifica.
- L'argomento Amazon SNS è crittografato e manca la policy richiesta per gli argomenti crittografati oppure la AWS KMS chiave è stata eliminata. Per ulteriori informazioni, consulta Configura gli argomenti di Amazon SNS per le notifiche.
- Nell'argomento Amazon SNS non è presente la policy richiesta per le notifiche. Le notifiche non possono essere inviate a un argomento Amazon SNS a meno che non disponga della relativa policy. Per ulteriori informazioni, consulta Configura gli argomenti di Amazon SNS per le notifiche.
- Il servizio di supporto per il target (Amazon SNS o AWS Chatbot) potrebbe avere dei problemi.

Voglio aumentare le mie quote per le notifiche e le risorse

Al momento non puoi modificare i limiti. Per informazioni, consulta Quote per le notifiche.

Quote per le notifiche

Nella seguente tabella sono elencate le quote (definite anche limiti) per le notifiche nella console Strumenti di sviluppo. Per informazioni sui limiti modificabili, consultare Service Quotas di AWS.

Risorsa	Limite predefinito
Numero massimo di regole di notifica in un AWS account	1000
Numero massimo di destinazioni per una regola di notifica	10
Numero massimo di regole di notifica per una risorsa	10

Che cosa sono le connessioni?

È possibile utilizzare la funzionalità di connessione nella console Developer Tools per connettere AWS risorse, ad esempio, AWS CodePipeline a repository di codice esterni. Questa funzionalità dispone di una propria API, l'AWS CodeConnectionsAPI di riferimento. Ogni connessione è una risorsa che puoi fornire ai AWS servizi per connettersi a un repository di terze parti, come Bitbucket. Ad esempio, puoi aggiungere la connessione in CodePipeline modo che attivi la pipeline quando viene apportata una modifica al codice del tuo repository di codice di terze parti. Ogni connessione è denominata e associata a un Amazon Resource Name (ARN) univoco utilizzato per fare riferimento alla connessione.

> **Important**
>
> Il nome del servizio AWS CodeStar Connections è stato rinominato. Le risorse create con il precedente namespace codestar-connections continueranno a essere supportate.

Cosa posso fare con le connessioni?

È possibile utilizzare le connessioni per integrare le risorse di fornitori di terze parti con le risorse AWS negli strumenti per sviluppatori, tra cui:

- Connettiti a un provider di terze parti, come Bitbucket, e utilizza la connessione di terze parti come integrazione sorgente con AWS le tue risorse, ad esempio. CodePipeline
- Gestisci in modo uniforme l'accesso alla tua connessione tra le tue risorse nella CodeBuild creazione di progetti, CodeDeploy applicazioni e pipeline CodePipeline per il tuo provider di terze parti.
- Usa un ARN di connessione nei tuoi modelli di stack per CodeBuild creare progetti, CodeDeploy applicazioni e pipeline CodePipeline, senza la necessità di fare riferimento a segreti o parametri memorizzati.

Per quali fornitori di terze parti posso creare connessioni?

Connections può associare AWS le tue risorse ai seguenti repository di terze parti:

- Bitbucket Cloud
- GitHub.com
- GitHub Cloud aziendale
- GitHub Server aziendale
- GitLab.com

> **Important**
>
> Il supporto per le connessioni GitLab include la versione 15.x e successive.

- GitLab installazione autogestita (per Enterprise Edition o Community Edition)

Per una panoramica del flusso di lavoro delle connessioni, consulta Flusso di lavoro per creare o aggiornare le connessioni.

I passaggi per creare connessioni per un tipo di provider cloud, ad esempio GitHub, sono diversi dai passaggi per un tipo di provider installato, come GitHub Enterprise Server. Per le fasi di alto livello per creare una connessione in base al tipo di provider, consulta Utilizzo delle connessioni.

> **Note**
>
> Per utilizzare le connessioni in Europa (Milano) Regione AWS, devi:
>
> 1. Installare un'app specifica per la regione
> 2. Abilitare la regione
>
> Questa app specifica per la regione supporta i collegamenti nella regione Europa (Milano). È pubblicata sul sito del provider di terze parti ed è separata dall'app esistente che supporta le connessioni per altre regioni. Installando questa app, autorizzi i provider di terze parti a condividere i tuoi dati con il servizio solo per questa regione e puoi revocare le autorizzazioni in qualsiasi momento disinstallando l'app.
> Il servizio non elaborerà o memorizzerà i dati a meno che tu non abiliti la Regione. Abilitando questa regione, concedi al nostro servizio le autorizzazioni per elaborare e archiviare i dati. Anche se la regione non è abilitata, i provider di terze parti possono comunque condividere i tuoi dati con il nostro servizio se l'app specifica per la regione rimane installata, quindi assicurati di disinstallarla dopo aver disabilitato la regione. Per ulteriori informazioni, consulta Enabling a Region (Abilitare una regione).

Cosa si Servizi AWS integra con le connessioni?

È possibile utilizzare le connessioni per integrare il repository di terze parti con i seguenti servizi Servizi AWS. Per visualizzare le integrazioni dei servizi per le connessioni, consulta Integrazioni di prodotti e servizi con AWS CodeConnections.

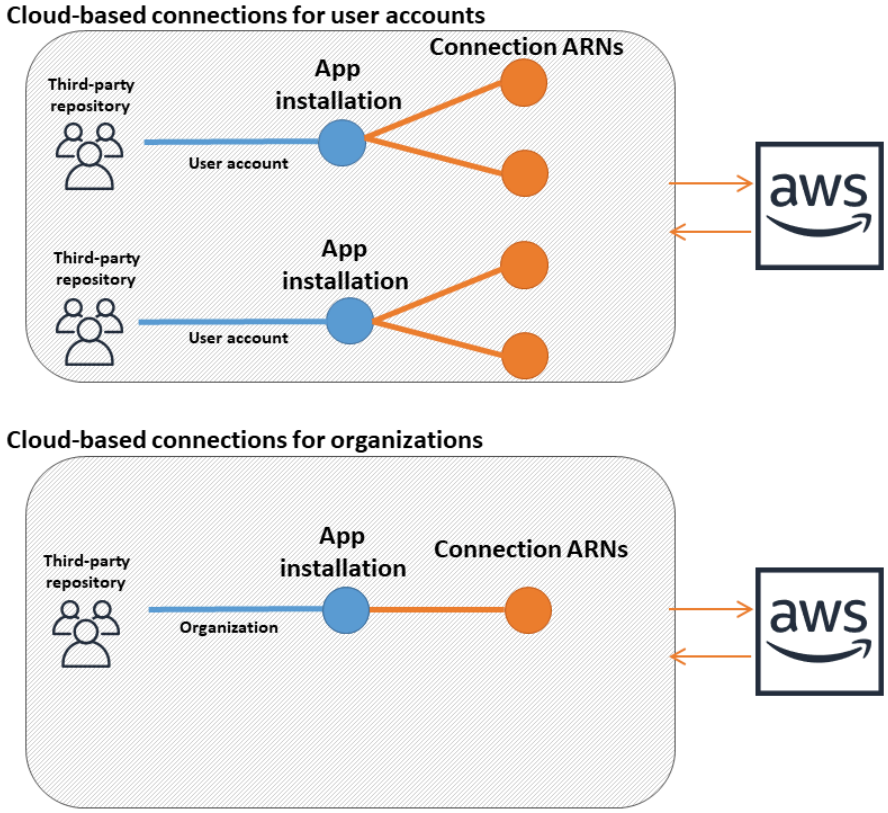
Come funzionano le connessioni?

Prima di poter creare una connessione, è necessario prima installare o fornire l'accesso all'app di autenticazione AWS nell'account di terze parti. Una volta installata, una connessione può essere aggiornata per utilizzare l'installazione. Quando si crea una connessione, è possibile fornire l'accesso alla risorsa AWS nel proprio account di terze parti. Ciò consente la connessione per accedere ai contenuti, come gli archivi di origine, nell'account di terze parti, per conto delle tue AWS risorse. È quindi possibile condividere tale connessione con altri Servizi AWS per fornire OAuth connessioni sicure tra le risorse.

Le connessioni basate sul cloud sono configurate come segue, con differenze evidenti tra gli account utente o le organizzazioni.

- Account utente: ogni account utente di terze parti basato sul cloud ha un'installazione dell'app Connector. È possibile associare più connessioni all'installazione dell'app.
- Organizzazioni: ogni organizzazione di terze parti basata sul cloud ha un'installazione di app Connector. Per le connessioni all'interno delle organizzazioni, la mappatura delle connessioni a ciascun account dell'organizzazione è 1:1. Non è possibile associare più connessioni all'installazione dell'app. Per ulteriori dettagli su come le organizzazioni utilizzano le connessioni, consulta Come funzionano le connessioni con le organizzazioni AWS CodeConnections .

Il diagramma seguente mostra come funzionano le connessioni basate sul cloud con gli account utente o le organizzazioni.



Le connessioni sono di proprietà di chi Account AWS le crea. Le connessioni sono identificate da un ARN contenente un ID della connessione. L'ID della connessione è un UUID che non può essere modificato o rimappato. L'eliminazione e il ripristino di una connessione comporta un nuovo ID della connessione e quindi un nuovo ARN della connessione. Ciò significa che le connessioni non ARNs vengono mai riutilizzate.

Una connessione appena creata si trova in uno stato `Pending`. È necessario un processo di handshake (OAuth flow) di terze parti per completare la configurazione della connessione e per farla

passare da uno stato `Pending` a uno `Available` stato. Una volta completata questa operazione, una connessione è `Available` e può essere utilizzata con AWS servizi come CodePipeline.

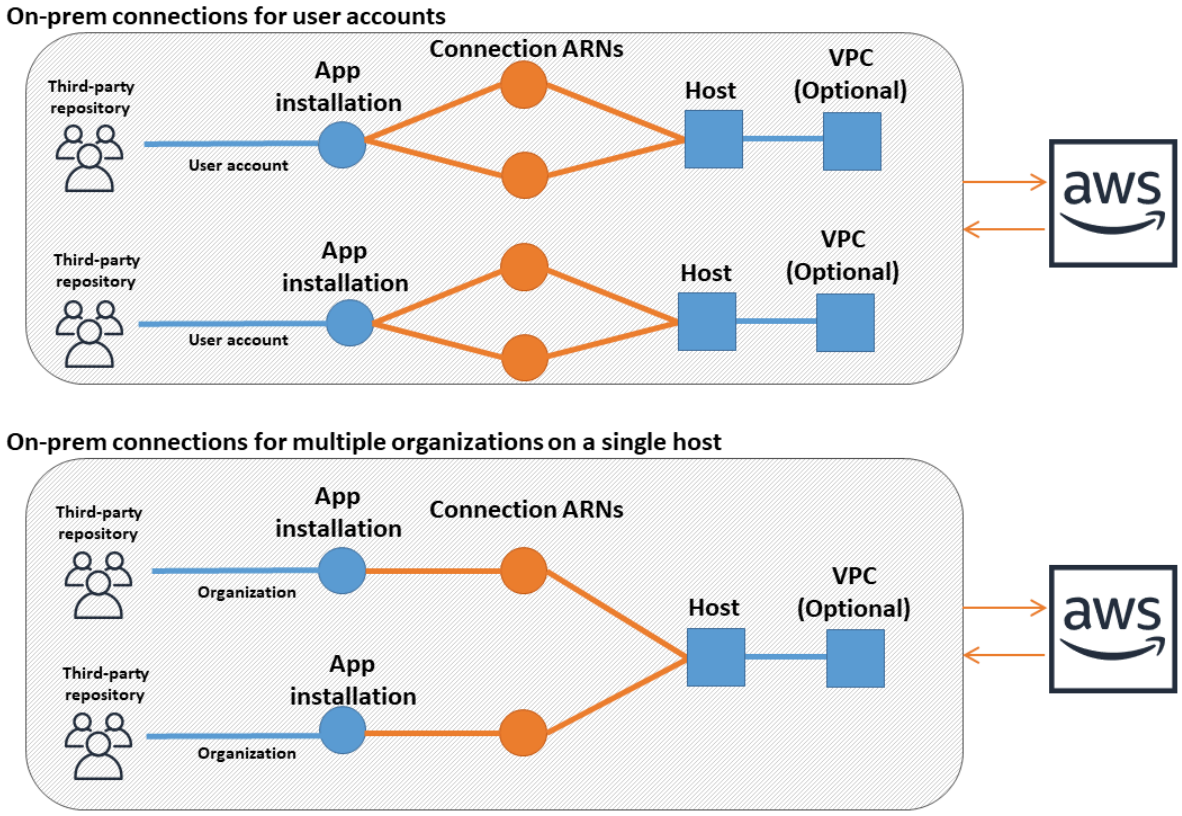
Se si desidera creare una connessione a un tipo di provider installato (on-prem), ad esempio GitHub Enterprise Server o GitLab autogestito, si utilizza una risorsa host con la connessione.

Le connessioni on-premise sono configurate come segue, con le differenze rilevate tra gli account utente o le organizzazioni.

- Account utente: ogni account utente di terze parti locale dispone di un'app Connector installata. È possibile associare più connessioni per un provider locale a un host.
- Organizzazioni: ogni organizzazione di terze parti locale ha un'installazione di app Connector. Per le connessioni locali nelle organizzazioni, come GitHub Organizations for GitHub Enterprise Server, crei un nuovo host per ogni connessione dell'organizzazione e assicurati di inserire le stesse informazioni nei campi di rete (VPC, Subnet IDs e Security Group IDs) per l'host. Per ulteriori dettagli su come le organizzazioni utilizzano le connessioni, vedere. Come funzionano le connessioni con le organizzazioni AWS CodeConnections
- Tutte: per ogni connessione on-premise, ogni VPC può essere associato a un solo host alla volta.

In tutti i casi, dovrai fornire l'URL del tuo server on-premise. Inoltre, se il server si trova all'interno di un VPC privato (ovvero non accessibile via Internet), dovrai fornire informazioni VPC insieme a informazioni opzionali sul certificato TLS. Queste configurazioni consentono di CodeConnections comunicare con l'istanza e sono condivise da tutte le connessioni create per questo host. Ad esempio, per una singola istanza di GitHub Enterprise Server, è necessario creare una singola app rappresentata da un host. Quindi, per la configurazione dell'account utente, è possibile creare più connessioni per quell'host, che corrispondono all'installazione dell'app, come illustrato nel diagramma seguente. Altrimenti, per un'organizzazione, crei un'unica installazione e connessione dell'app per quell'host.

Il diagramma seguente mostra come funzionano le connessioni locali con gli account utente o le organizzazioni.



Un host appena creato si trova in uno stato `Pending`. È necessario un processo di registrazione di terze parti per completare la configurazione dell'host e spostarsi da `Pending` a uno stato `Available`. Al termine di questo, un host è `Available` e può essere utilizzato per le connessioni ai tipi di provider installati.

Per una panoramica del flusso di lavoro delle connessioni, consulta Flusso di lavoro per creare o aggiornare le connessioni. Per una panoramica del flusso di lavoro di creazione di un host per i provider installati, consulta Flusso di lavoro per la creazione o l'aggiornamento di un host. Per le fasi di alto livello per creare una connessione in base al tipo di provider, consulta Utilizzo delle connessioni.

Come funzionano le connessioni con le organizzazioni AWS CodeConnections

Per le organizzazioni con un provider, come GitHub Organizations, non è possibile installare un' GitHub app in più GitHub Organizzazioni. Una connessione ha una mappatura 1:1 con un'organizzazione tramite l'uso dell'app Github Connector. L'app Connector deve essere separata per ogni organizzazione in GitHub GitHub Enterprise Server e deve avere una connessione associata.

Ad esempio, per lavorare con più organizzazioni sullo stesso GitHub server, è necessario creare connessioni separate per ogni organizzazione e installare GitHub app separate per queste organizzazioni. L'account di destinazione sul lato Github, tuttavia, può essere lo stesso.

Flusso di lavoro per creare o aggiornare le connessioni

Quando crei una connessione, crei o utilizzi anche un'installazione esistente dell'app Connector per l'handshake di autenticazione con il provider terzo.

Le connessioni possono avere i seguenti stati:

- `Pending` - Una connessione `pending` è una connessione che deve essere completata (spostata in `available`) prima di poter essere usata.
- `Available` - È possibile utilizzare o passare una connessione `available` ad altre risorse e utenti nell'account.
- `Error` - Una connessione che ha uno stato `error` viene ripetuta automaticamente. Non si può utilizzare fino a quando non è `available`.

Flusso di lavoro: creazione o aggiornamento di una connessione con CLI, l'SDK o AWS CloudFormation

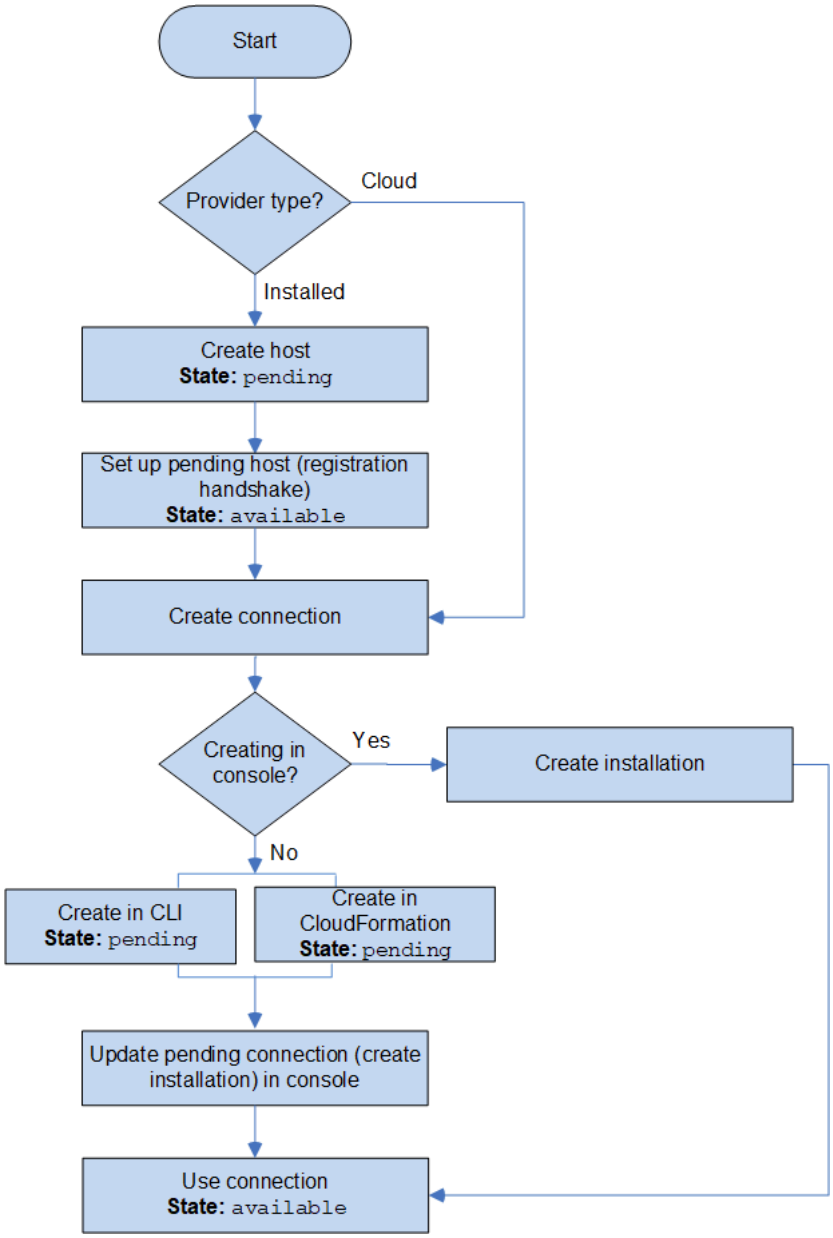
Utilizzi l'CreateConnectionAPI per creare una connessione utilizzando AWS Command Line Interface (AWS CLI), SDK o. AWS CloudFormation Dopo che è stata creata, la connessione si trova in uno stato `pending`. È possibile completare il processo utilizzando l'opzione della console Set up pending connection (Configurare una connessione in attesa). La console richiede di creare un'installazione o di utilizzare un'installazione esistente per la connessione. È quindi possibile utilizzare la console per completare l'handshake e spostare la connessione in uno stato `available`, scegliendo Complete connection (Completa connessione) sulla console.

Flusso di lavoro: creazione o aggiornamento di una connessione con la console

Se state creando una connessione a un tipo di provider installato, come GitHub Enterprise Server, dovete prima creare un host. Se ci si connette a un tipo di provider cloud, ad esempio Bitbucket, si ignora la creazione dell'host e si continua a creare una connessione.

Per creare o aggiornare una connessione utilizzando la console, si utilizza la pagina di CodePipeline modifica delle azioni sulla console per scegliere il provider di terze parti. La console richiede di creare un'installazione o di utilizzare un'installazione esistente per la connessione, e quindi utilizzare la

console per creare la connessione. La console completa l'handshake e sposta la connessione da `pending` a uno stato `available` automaticamente.



Flusso di lavoro per la creazione o l'aggiornamento di un host

Quando si crea una connessione per un provider installato (on-prem), si utilizza una risorsa host.

> **Note**
>
> Per le organizzazioni in GitHub Enterprise Server o GitLab gestite autonomamente, non viene assegnato un host disponibile. Crei un nuovo host per ogni connessione nell'organizzazione

e devi assicurarti di inserire le stesse informazioni nei campi di rete (ID VPC, sottorete IDs e gruppo di sicurezza IDs) per l'host. Per ulteriori informazioni, consulta Configurazione della connessione e dell'host per i provider installati che supportano le organizzazioni.

Gli host possono avere i seguenti stati:

- `Pending`: un host `pending` è un host che è stato creato e che deve essere configurato (passato nello stato `available`) prima di poter essere utilizzato.
- `Available`: puoi utilizzare o passare un host `available` alla connessione.

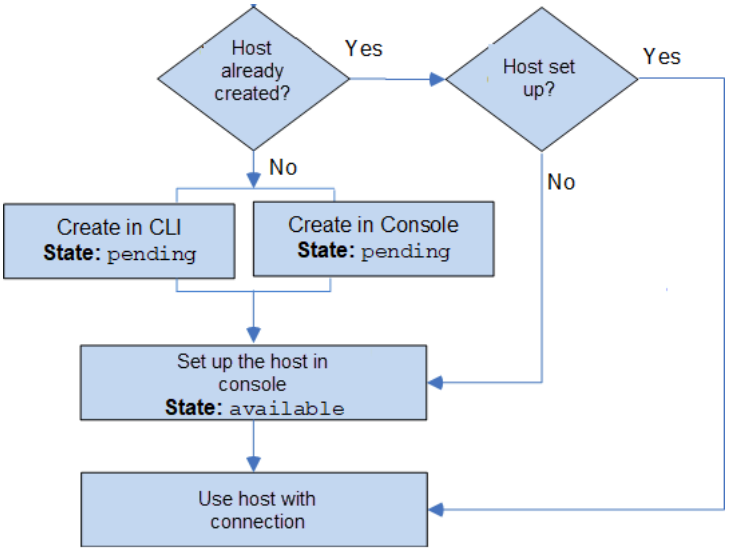
Flusso di lavoro: creazione o aggiornamento di un host con la CLI, l'SDK o AWS CloudFormation

L'CreateHostAPI viene utilizzata per creare un host utilizzando AWS Command Line Interface (AWS CLI), SDK o. AWS CloudFormation Dopo che è stato creato, l'host si trova in uno stato `pending`. Puoi completare il processo utilizzando l'opzione Configura della console.

Flusso di lavoro: creazione o aggiornamento di un host con la console

Se state creando una connessione a un tipo di provider installato, ad esempio GitHub Enterprise Server o GitLab self-managed, create un host o utilizzate un host esistente. Se ci si connette a un tipo di provider cloud, ad esempio Bitbucket, si ignora la creazione dell'host e si continua a creare una connessione.

Usa la console per configurare l'host e modificarne lo stato da `pending` a `available`.



Risorse globali in AWS CodeConnections

Le connessioni sono risorse globali, il che significa che la risorsa viene replicata in tutte le regioni Regioni AWS.

Sebbene il formato ARN della connessione rifletta il nome della regione in cui è stato creato, la risorsa non è vincolata ad alcuna regione. La regione in cui è stata creata la risorsa di connessione è la regione in cui vengono controllati gli aggiornamenti dei dati delle risorse di connessione. Esempi di operazioni API che controllano gli aggiornamenti dei dati delle risorse di connessione includono la creazione di una connessione, l'aggiornamento di un'installazione, l'eliminazione di una connessione o l'assegnazione di tag a una connessione.

Le risorse host per le connessioni non sono risorse disponibili a livello globale. Le risorse host vengono utilizzate solo nella regione in cui sono state create.

- È sufficiente creare una connessione sola volta e sarà possibile utilizzarla in qualsiasi regione Regione AWS.
- Se la regione in cui è stata creata la connessione presenta problemi, APIs ciò influirà sui dati delle risorse di controllo della connessione, ma è comunque possibile utilizzare correttamente la connessione in tutte le altre regioni.
- Quando si elencano risorse di connessione nella console o nella CLI, nell'elenco vengono visualizzate tutte le risorse di connessione associate all'account in tutte le regioni.
- Quando si elencano risorse host nella console o nella CLI, nell'elenco vengono visualizzate tutte le risorse host associate all'account soltanto nelle regioni selezionate.
- Quando una connessione con una risorsa host associata viene elencata o visualizzata con la CLI, l'output restituisce l'ARN dell'host indipendentemente dalla regione CLI configurata.

Come posso iniziare a usare le connessioni?

Per iniziare, ecco alcuni argomenti utili da esaminare:

- Ulteriori informazioni sui concetti per le connessioni.
- Configura le risorse necessarie per iniziare a utilizzare le connessioni.
- Inizia con le tue prime connessioni e connettile a una risorsa.

Concetti di connessione

La configurazione e l'utilizzo delle di funzionalità di connessione risultano più semplici se si comprendono i concetti e i termini. Di seguito sono riportati alcuni concetti che occorre conoscere quando si utilizzano le connessioni nella console Strumenti di sviluppo:

installazione

Un'istanza dell' AWS app su un account di terze parti. L'installazione dell'app AWS CodeStar Connector consente di accedere AWS alle risorse all'interno dell'account di terze parti. Un'installazione può essere modificata solo sul sito web del provider di terze parti.

connessione

AWS Risorsa utilizzata per connettere archivi di sorgenti di terze parti ad altri AWS servizi.

repository di terze parti

Un repository fornito da un servizio o da una società che non fa parte di AWS. Ad esempio, un repository Bitbucket è un repository di terze parti.

provider type (tipo di provider)

Servizio o società che fornisce il repository di origine di terze parti a cui si desidera connettersi. Colleghi le tue AWS risorse a tipi di provider esterni. Tipo di provider in cui il repository di origine è installato nella rete e l'infrastruttura è un tipo di provider installato. Ad esempio, GitHub Enterprise Server è un tipo di provider installato.

host

Una risorsa che rappresenta l'infrastruttura in cui è installato un provider di terze parti. Le connessioni utilizzano l'host per rappresentare il server in cui è installato il provider di terze parti, ad esempio GitHub Enterprise Server. Si crea un host per tutte le connessioni a quel tipo di provider.

> **Note**
>
> Quando si utilizza la console per creare una connessione a GitHub Enterprise Server, la console crea automaticamente una risorsa host come parte del processo.

AWS CodeConnections provider e versioni supportati

Questo capitolo fornisce informazioni sui provider e sulle versioni che AWS CodeConnections supporta.

Argomenti

- Tipo di provider supportato per Bitbucket
- Tipo di provider supportato per Enterprise Cloud GitHub GitHub
- Tipo e versioni di provider supportati per GitHub Enterprise Server
- Tipo di provider supportato per .com GitLab
- Tipo di provider supportato per la gestione automatica GitLab

Tipo di provider supportato per Bitbucket

Puoi utilizzare l'app di connessione con Atlassian Bitbucket Cloud.

I tipi di provider Bitbucket installati, ad esempio Bitbucket Server, non sono supportati.

Tipo di provider supportato per Enterprise Cloud GitHub GitHub

Puoi utilizzare l'app di connessione con GitHub GitHub Enterprise Cloud.

Tipo e versioni di provider supportati per GitHub Enterprise Server

È possibile utilizzare l'app per le connessioni con le versioni supportate di GitHub Enterprise Server. Per un elenco delle versioni supportate, consulta https://enterprise.github.com/releases/.

> **Important**
>
> AWS CodeConnections non supporta le versioni obsolete di GitHub Enterprise Server. Ad esempio, non AWS CodeConnections supporta la versione 2.22.0 di GitHub Enterprise Server a causa di un problema noto nella versione. Per connetterti, esegui l'aggiornamento alla versione 2.22.1 o all'ultima versione disponibile.

Tipo di provider supportato per .com GitLab

È possibile utilizzare le connessioni con GitLab .com. Per ulteriori informazioni, consulta Crea una connessione a GitLab.

> **Important**
>
> Il supporto per le connessioni GitLab include la versione 15.x e successive.

Tipo di provider supportato per la gestione automatica GitLab

È possibile utilizzare connessioni con installazione GitLab autogestita (per Enterprise Edition o Community Edition). Per ulteriori informazioni, consulta Crea una connessione a gestione automatica GitLab.

Integrazioni di prodotti e servizi con AWS CodeConnections

AWS CodeConnections è integrato con una serie di AWS servizi e prodotti e servizi dei partner. Utilizzare le informazioni nelle sezioni seguenti per configurare le connessioni per l'integrazione con i prodotti e i servizi utilizzati.

Le seguenti risorse correlate possono rivelarsi utili durante l'utilizzo di questo servizio.

Argomenti

- CodeGuru Revisore Amazon
- Amazon Q Developer
- Amazon SageMaker
- AWS App Runner
- AWS CloudFormation
- AWS CodeBuild
- AWS CodePipeline
- Service Catalog
- AWS Proton

CodeGuru Revisore Amazon

CodeGuru Reviewer è un servizio per il monitoraggio del codice del repository. È possibile utilizzare le connessioni per associare il repository di terze parti con il codice che si desidera esaminare. Per un tutorial in cui impari a configurare CodeGuru Reviewer per monitorare il codice sorgente in un GitHub

repository in modo che possa creare consigli per migliorarlo, consulta Tutorial: monitora il codice sorgente in un GitHub repository nella Amazon CodeGuru Reviewer User Guide.

Amazon Q Developer

Amazon Q Developer è un assistente conversazionale generativo basato sull'intelligenza artificiale che può aiutarti a comprendere, creare, estendere e utilizzare le applicazioni. AWS Per ulteriori informazioni, consulta Cos'è Amazon Q Developer? nella Guida per l'utente di Amazon Q Developer.

Amazon SageMaker

Amazon SageMaker è un servizio per la creazione, la formazione e la distribuzione di modelli linguistici di apprendimento automatico. Per un tutorial in cui configurare una connessione al tuo GitHub repository, consulta SageMaker MLOps Project Walkthrough Using Git Repos di terze parti nella Amazon Developer Guide. SageMaker

AWS App Runner

AWS App Runner è un servizio che fornisce un modo rapido, semplice e conveniente per implementare dal codice sorgente o da un'immagine di container direttamente a un'applicazione Web scalabile e sicura nel Cloud AWS. È possibile distribuire il codice dell'applicazione dal proprio repository con una pipeline di integrazione e distribuzione automatiche di App Runner. Puoi utilizzare le connessioni per distribuire il codice sorgente a un servizio App Runner da un repository privato. GitHub Per ulteriori informazioni, consulta la pagina relativa ai fornitori del repository di codice sorgente nella Guida per gli sviluppatori di AWS App Runner .

AWS CloudFormation

AWS CloudFormationè un servizio che consente di modellare e configurare le AWS risorse in modo da dedicare meno tempo alla gestione di tali risorse e più tempo alle applicazioni in esecuzione. AWS Crei un modello che descrive tutte le AWS risorse che desideri (come istanze Amazon o EC2 istanze database Amazon RDS) e CloudFormation si occupa del provisioning e della configurazione di tali risorse per te.

Utilizzi le connessioni con Git sync in CloudFormation per creare una configurazione di sincronizzazione che monitora il tuo repository Git. Per un tutorial che illustra l'utilizzo di Git sync per le distribuzioni in stack, consulta Lavorare con CloudFormation Git sync nella Guida per l'AWS CloudFormation utente.

Per ulteriori informazioni CloudFormation, consulta Registrazione dell'account per la pubblicazione di CloudFormation estensioni nella Guida per l'utente dell'interfaccia a riga di CloudFormation comando.

AWS CodeBuild

AWS CodeBuildè un servizio per creare e testare il codice. CodeBuild elimina la necessità di fornire, gestire e scalare i propri server di build e fornisce ambienti di compilazione preconfezionati per i linguaggi di programmazione e gli strumenti di compilazione più diffusi. Per ulteriori informazioni sull'utilizzo CodeBuild con connessioni a GitLab, consulta le GitLabconnessioni nella Guida per l'AWS CodeBuild utente.

AWS CodePipeline

CodePipeline è un servizio di distribuzione continua che può essere utilizzato per modellare, visualizzare e automatizzare le fasi necessarie al rilascio di software. È possibile utilizzare le connessioni per configurare un repository di terze parti per le azioni CodePipeline di origine.

Ulteriori informazioni:

- Consulta la CodePipeline pagina di riferimento per la configurazione dell'`SourceConnections`azione. Per visualizzare i parametri di configurazione e un esempio di frammento JSON/YAML, consulta la Guida per l'utente. CodeStarSourceConnectionAWS CodePipeline
- Per visualizzare un tutorial sulle Nozioni di base che crea una pipeline con un repository di origini di terze parti, consulta Nozioni di base sulle connessioni.

Service Catalog

Service Catalog consente alle organizzazioni di creare e gestire cataloghi di prodotti approvati per l'uso su AWS.

Quando autorizzi una connessione tra il tuo Account AWS e un provider di repository esterno, ad esempio GitHub Enterprise o Bitbucket, la connessione consente di sincronizzare i prodotti Service Catalog con file modello gestiti tramite repository di terze parti. GitHub

Per ulteriori informazioni, consulta Sincronizzazione dei prodotti Service Catalog con i file modello di GitHub GitHub Enterprise o Bitbucket nella Service Catalog User Guide.

AWS Proton

AWS Proton è un servizio basato sul cloud per l'implementazione su un'infrastruttura cloud. È possibile utilizzare le connessioni per creare un collegamento ai repository di terze parti per le risorse nei propri modelli per AWS Proton. Per ulteriori informazioni, consulta Crea un link al tuo repository nella Guida per l'utente di AWS Proton .

Configurazione di una connessione

Completa le attività in questa sezione per configurare la funzionalità di connessione nella console Strumenti di sviluppo.

Argomenti

- Iscriviti per AWS
- Creare e applicare una policy con autorizzazioni per creare connessioni

Iscriviti per AWS

Iscriviti per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Parte della procedura di registrazione prevede la ricezione di una telefonata o di un messaggio di testo e l'immissione di un codice di verifica sulla tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center .

Creare e applicare una policy con autorizzazioni per creare connessioni

Come utilizzare l'editor di policy JSON per creare una policy

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione a sinistra, seleziona Policies (Policy).

   Se è la prima volta che selezioni Policy, verrà visualizzata la pagina Benvenuto nelle policy gestite. Seleziona Inizia.
3. Nella parte superiore della pagina, scegli Crea policy.
4. Nella sezione Editor di policy, scegli l'opzione JSON.
5. Inserisci il documento di policy JSON seguente:

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "codeconnections:CreateConnection",
               "codeconnections:DeleteConnection",
               "codeconnections:GetConnection",
               "codeconnections:ListConnections",
               "codeconnections:GetInstallationUrl",
               "codeconnections:GetIndividualAccessToken",
               "codeconnections:ListInstallationTargets",
               "codeconnections:StartOAuthHandshake",
```

```
                "codeconnections:UpdateConnectionInstallation",
                "codeconnections:UseConnection"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. Scegli Next (Successivo).

> **Note**
>
> È possibile alternare le opzioni dell'editor Visivo e JSON in qualsiasi momento. Se tuttavia si apportano modifiche o si seleziona Successivo nell'editor Visivo, IAM potrebbe ristrutturare la policy in modo da ottimizzarla per l'editor visivo. Per ulteriori informazioni, consulta Modifica della struttura delle policy nella Guida per l'utente di IAM.

7. Nella pagina Rivedi e crea, inserisci un valore in Nome policy e Descrizione (facoltativo) per la policy in fase di creazione. Rivedi Autorizzazioni definite in questa policy per visualizzare le autorizzazioni concesse dalla policy.
8. Seleziona Crea policy per salvare la nuova policy.

Nozioni di base sulle connessioni

Il modo più semplice per iniziare a utilizzare le connessioni consiste nel configurare una connessione che associ l'archivio di sorgenti di terze parti alle risorse disponibili. AWS Se desideri connettere la tua pipeline a una AWS fonte, ad esempio CodeCommit, ti connetteresti ad essa come azione sorgente. Tuttavia, se disponi di un repository esterno, devi creare una connessione per associare il repository alla pipeline. In questo tutorial è possibile impostare una connessione con il repository Bitbucket e la pipeline.

In questa sezione vengono utilizzate connessioni con:

- AWS CodePipeline: in questi passaggi, si crea una pipeline con il repository Bitbucket come origine della pipeline.
- Amazon CodeGuru Reviewer: Successivamente, associ il tuo repository Bitbucket agli strumenti di feedback e analisi in Reviewer. CodeGuru

Argomenti

- Prerequisiti
- Fase 1: modifica del file sorgente
- Fase 2: creazione della pipeline
- Passaggio 3: Associa il tuo repository a Reviewer CodeGuru

Prerequisiti

Prima di iniziare, completa i passaggi descritti in Configurazione. Ti serve anche un archivio di sorgenti di terze parti che desideri connettere ai tuoi AWS servizi e che consenta alla connessione di gestire l'autenticazione al posto tuo. Ad esempio, potresti voler connettere un repository Bitbucket ai tuoi AWS servizi che si integrano con gli archivi di origine.

- Crea un repository Bitbucket con il proprio account Bitbucket.
- Prepara le credenziali Bitbucket. Quando utilizzi il AWS Management Console per configurare una connessione, ti viene chiesto di accedere con le tue credenziali Bitbucket.

Fase 1: modifica del file sorgente

Quando crei il repository Bitbucket, è incluso un file predefinito `README.md` che modificherai.

1. Accedi al tuo repository Bitbucket e scegli Source (Origine).
2. Seleziona il file `README.md` e scegli Edit (Modifica) nella parte superiore della pagina. Elimina il testo esistente e aggiungi il seguente testo.

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

3. Scegli Commit (Applica).

   Assicurati che il file `README.md` si trovi al livello root del repository.

Fase 2: creazione della pipeline

In questa sezione, andrai a creare una pipeline con le operazioni seguenti:

- Una fase di origine con una connessione al repository Bitbucket e all'operazione.
- Una fase di costruzione con un' AWS CodeBuild azione di costruzione.

Per creare una pipeline con la procedura guidata

1. Accedi alla CodePipeline console all'indirizzo https://console.aws.amazon.com/codepipeline/.
2. Nella pagina Welcome (Benvenuto), pagina Getting started (Nozioni di base) o pagina Pipelines (Pipeline), scegli Create pipeline (Crea pipeline).
3. In Step 1: Choose pipeline settings (Fase 1: scelta delle impostazioni della pipeline), in Pipeline name (Nome pipeline), immettere **`MyBitbucketPipeline`**.
4. In Service Role (Ruolo del servizio), scegliere New service role (Nuovo ruolo del servizio).

   > **Note**
   >
   > Se invece scegli di utilizzare il ruolo di CodePipeline servizio esistente, assicurati di aver aggiunto l'autorizzazione `codeconnections:UseConnection` IAM alla tua policy sui ruoli di servizio. Per istruzioni sul ruolo CodePipeline di servizio, consulta Aggiungere autorizzazioni al ruolo CodePipeline di servizio.

5. In Impostazioni avanzate non modificare le impostazioni predefinite. In Artifact store (Archivio artefatti), seleziona Default location (Posizione predefinita) per utilizzare l'archivio artefatti predefinito, ad esempio il bucket Amazon S3 dedicato agli artefatti designato come predefinito, per la pipeline nella regione selezionata.

   > **Note**
   >
   > Non si tratta del bucket di origine per il codice sorgente, ma dell'archivio artefatti per la pipeline. È richiesto un archivio artefatti separato, ad esempio un bucket S3, per ogni pipeline.

   Seleziona Next (Successivo).
6. Nella Fase 2: Aggiungi una fase di origine, aggiungi una fase di origine:

   a. In Source provider (Provider origine) seleziona Bitbucket.

   b. In Connection (Connessione), scegli Connect to Bitbucket (Connessione a Bitbucket).

   c. Nella pagina Connect to Bitbucket (Connetti a Bitbucket), in Connection name (Nome connessione), immetti il nome della connessione che desideri creare. Il nome permette di identificare la connessione in un secondo momento.

In Bitbucket apps (App Bitbucket), scegli Install a new app (Installa una nuova app).

d. Nella pagina di installazione dell'app, un messaggio indica che l' AWS CodeStar app sta tentando di connettersi al tuo account Bitbucket. Selezionare Grant access (Concedi accesso). Dopo aver autorizzato la connessione, i tuoi repository su Bitbucket vengono rilevati e puoi scegliere di associarne uno alla tua risorsa. AWS

e. Viene visualizzato l'ID di connessione per la nuova installazione. Selezionare Complete connection (Completa connessione). Verrai reindirizzato alla console. CodePipeline

f. In Repository name (Nome repository), scegli il nome del repository Bitbucket.

g. In Branch name (Nome del ramo), scegli il ramo per il repository.

h. Assicurati che l'opzione Avvia la pipeline alla modifica del codice sorgente sia selezionata.

i. In Formato degli artefatti di output, scegli una delle seguenti opzioni: CodePipeline predefinito.

- Scegliete CodePipeline predefinito per utilizzare il formato zip predefinito per gli artefatti nella pipeline.
- Scegli Clone completo per includere i metadati Git relativi al repository degli artefatti nella pipeline. Questo è supportato solo per le azioni. CodeBuild

Scegli Next (Successivo).

7. In Add build stage (Aggiungi fase di compilazione), aggiungi una fase di compilazione:

a. In Build provider (Provider compilazione), scegli AWS CodeBuild. Consenti a Region (Regione) di preimpostarsi sulla regione della pipeline.

b. Seleziona Crea progetto.

c. In Project name (Nome progetto) immettere un nome per questo progetto di compilazione.

d. In Environment image (Immagine ambiente), scegli Managed image (Immagine gestita). In Operating system (Sistema operativo), seleziona Ubuntu.

e. In Runtime, seleziona Standard. Per Image, scegliere:5.0aws/codebuild/standard.

f. Per Service Role (Ruolo del servizio), scegli New service role (Nuovo ruolo del servizio).

g. In Buildspec, per Build specifications (Specifiche di compilazione), scegli Insert build commands (Inserisci comandi di compilazione). Scegli Switch to editor (Passa all'editor) e incolla quanto segue in Build commands (Comandi di compilazione):

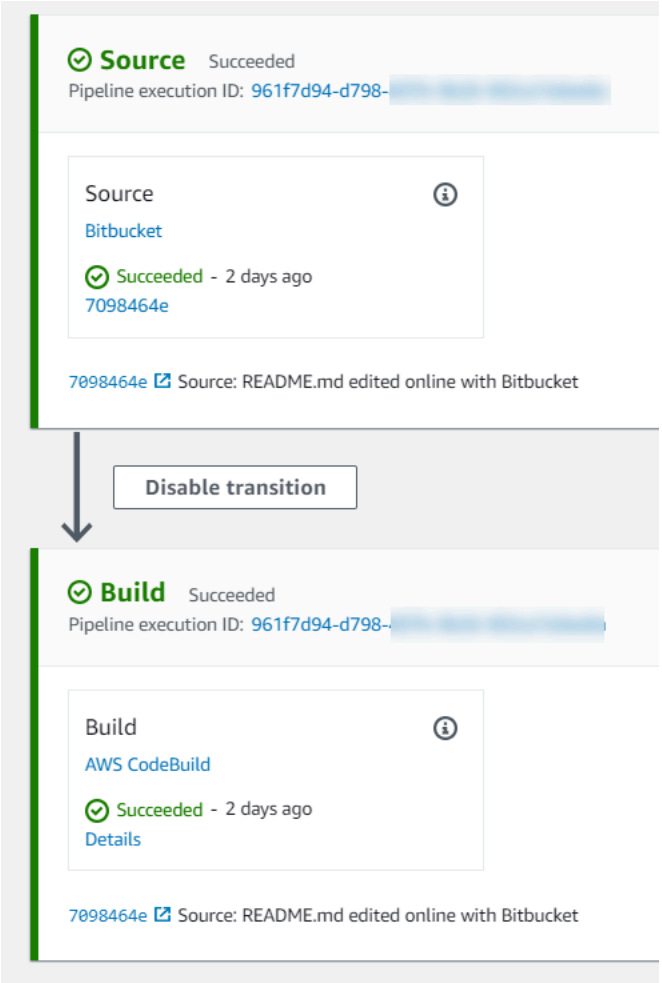
```
version: 0.2

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. Scegli Continua a. CodePipeline Questo ritorna alla CodePipeline console e crea un CodeBuild progetto che utilizza i comandi di compilazione per la configurazione. Il progetto di compilazione utilizza un ruolo di servizio per gestire le autorizzazioni AWS del servizio. Questa operazione potrebbe richiedere un paio di minuti.

i. Seleziona Next (Successivo).

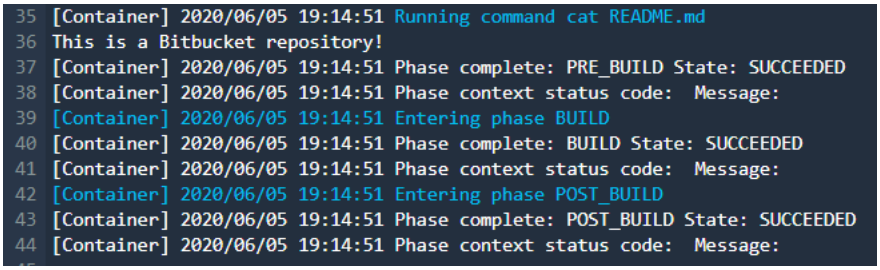
8. Nella pagina Step 4: Add deploy stage (Fase 4: aggiunta della fase di distribuzione), scegli Skip deploy stage (Ignora fase di distribuzione), quindi accetta il messaggio di avviso scegliendo Skip (Ignora). Seleziona Next (Successivo).
9. Nella Step 5: Review (Fase 5: revisione), scegliere Create pipeline (Crea pipeline).
10. Quando la pipeline viene creata correttamente, viene avviata un'esecuzione della pipeline.



11. Nella fase di compilazione riuscita, scegliere Details (Dettagli).

    In Dettagli di esecuzione, visualizza l'output della CodeBuild build. I comandi generano il contenuto del file `README.md` come segue:

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



Passaggio 3: Associa il tuo repository a Reviewer CodeGuru

Dopo aver creato una connessione, puoi utilizzarla per tutte le AWS risorse dello stesso account. Ad esempio, puoi utilizzare la stessa connessione Bitbucket per un'azione di CodePipeline origine in una pipeline e l'analisi del commit del repository in Reviewer. CodeGuru

1. Accedi alla console Reviewer. CodeGuru
2. In CodeGuru Revisore, scegli Associa repository.

   Viene visualizzata la procedura guidata di una pagina.
3. In Select source provider (Seleziona provider di origine), selezionare Bitbucket.
4. In Connect to Bitbucket (con AWS CodeConnections), scegli la connessione che hai creato per la tua pipeline.
5. In Repository location (Posizione del repository), scegliere il nome del repository Bitbucket e scegliere Associate (Associa).

   È possibile continuare a impostare le revisioni del codice. Per ulteriori informazioni, consulta Connessione a Bitbucket per associare un repository a Reviewer CodeGuru nella Amazon CodeGuru Reviewer User Guide.

Utilizzo delle connessioni

Le connessioni sono configurazioni utilizzate per connettere le risorse AWS a repository di codice esterni. Ogni connessione è una risorsa che può essere fornita a servizi come la connessione AWS CodePipeline a un repository di terze parti come Bitbucket. Ad esempio, puoi aggiungere la connessione in CodePipeline modo che attivi la pipeline quando viene apportata una modifica al codice del tuo repository di codice di terze parti. È inoltre possibile connettere le AWS risorse a un tipo di provider installato come GitHub Enterprise Server.

> **Note**
>
> Per le organizzazioni in GitHub o GitHub Enterprise Server, non è possibile installare un' GitHub app in più GitHub Organizzazioni. La mappatura tra app e GitHub organizzazione è una mappatura 1:1. Un'organizzazione può avere solo un'app alla volta; tuttavia, è possibile avere più connessioni che puntano alla stessa app. Per ulteriori dettagli, consulta Come funzionano le connessioni con le organizzazioni AWS CodeConnections .

Se desideri creare una connessione a un tipo di provider installato, ad esempio GitHub Enterprise Server, la console crea un host per te. Un host è una risorsa creata per rappresentare il server in cui è installato il provider. Per ulteriori informazioni, consulta Utilizzo degli host.

Quando si crea una connessione, si utilizza una procedura guidata nella console per installare l'app di connessione con il provider di terze parti e associarla a una nuova connessione. Se hai già installato l'app , puoi utilizzarla.

> **Note**
>
> Per utilizzare le connessioni in Europa (Milano) Regione AWS, devi:
>
> 1. Installare un'app specifica per la regione
> 2. Abilitare la regione
>
> Questa app specifica per la regione supporta i collegamenti nella regione Europa (Milano). È pubblicata sul sito del provider di terze parti ed è separata dall'app esistente che supporta le connessioni per altre regioni. Installando questa app, autorizzi i provider di terze parti a condividere i tuoi dati con il servizio solo per questa regione e puoi revocare le autorizzazioni in qualsiasi momento disinstallando l'app.
> Il servizio non elaborerà o memorizzerà i dati a meno che tu non abiliti la Regione. Abilitando questa regione, concedi al nostro servizio le autorizzazioni per elaborare e archiviare i dati. Anche se la regione non è abilitata, i provider di terze parti possono comunque condividere i tuoi dati con il nostro servizio se l'app specifica per la regione rimane installata, quindi assicurati di disinstallarla dopo aver disabilitato la regione. Per ulteriori informazioni, consulta Enabling a Region (Abilitare una regione).

Per ulteriori informazioni sulle connessioni, consulta il riferimento alle AWS CodeConnections API. Per ulteriori informazioni sull'azione di CodePipeline origine per Bitbucket, consulta CodestarConnectionSourcela Guida per l'AWS CodePipeline utente.

Per creare o allegare una policy al tuo utente o ruolo AWS Identity and Access Management (IAM) con le autorizzazioni necessarie per utilizzare le connessioni, consulta. AWS CodeConnections riferimento alle autorizzazioni A seconda di quando è stato creato il ruolo di CodePipeline servizio, potrebbe essere necessario aggiornarne le autorizzazioni all'assistenza. AWS CodeConnections Per istruzioni, consulta Aggiorna il ruolo di servizio nella AWS CodePipeline Guida per l'utente.

Argomenti

- Creazione di una connessione
- Crea una connessione a Bitbucket
- Crea una connessione a GitHub
- Creare una connessione a GitHub Enterprise Server
- Crea una connessione a GitLab
- Crea una connessione a gestione automatica GitLab
- Aggiornare una connessione in attesa
- Elenco delle connessioni
- Elimina connessione
- Tagging di risorse di connessione
- Visualizza i dettagli di connessione
- Condividi le connessioni con Account AWS

Creazione di una connessione

È possibile creare connessioni ai seguenti tipi di provider di terze parti:

- Per creare una connessione a Bitbucket, consulta Crea una connessione a Bitbucket.
- Per creare una connessione a GitHub o GitHub Enterprise Cloud, vediCrea una connessione a GitHub.
- Per creare una connessione a GitHub Enterprise Server, inclusa la creazione della risorsa host, vediCreare una connessione a GitHub Enterprise Server.

- Per creare una connessione a GitLab, vedereCrea una connessione a GitLab.

> **Note**
>
> A partire dal 1° luglio 2024, la console crea connessioni con `codeconnections` la risorsa ARN. Le risorse con entrambi i prefissi di servizio continueranno a essere visualizzate nella console.

Crea una connessione a Bitbucket

Puoi usare AWS Management Console o il AWS Command Line Interface (AWS CLI) per creare una connessione a un repository ospitato su bitbucket.org.

Prima di iniziare:

- Bisogna aver già creato un account con Bitbucket.
- Bisogna aver già creato un repository di codice su bitbucket.org.

> **Note**
>
> È possibile creare connessioni a un repository Bitbucket Cloud. I tipi di provider Bitbucket installati, ad esempio Bitbucket Server, non sono supportati. Consultare AWS CodeConnections provider e versioni supportati.

> **Note**
>
> Le connessioni forniscono l'accesso solo ai repository di proprietà dell'account utilizzato per creare la connessione.
> Se l'applicazione viene installata in un workspace Bitbucket, sono richieste le autorizzazioni Administer workspace (Amministrazione workspace). In caso contrario, l'opzione per installare l'app non verrà visualizzata.

Argomenti

- Creare una connessione a Bitbucket (console)

- Creare una connessione a Bitbucket (CLI)

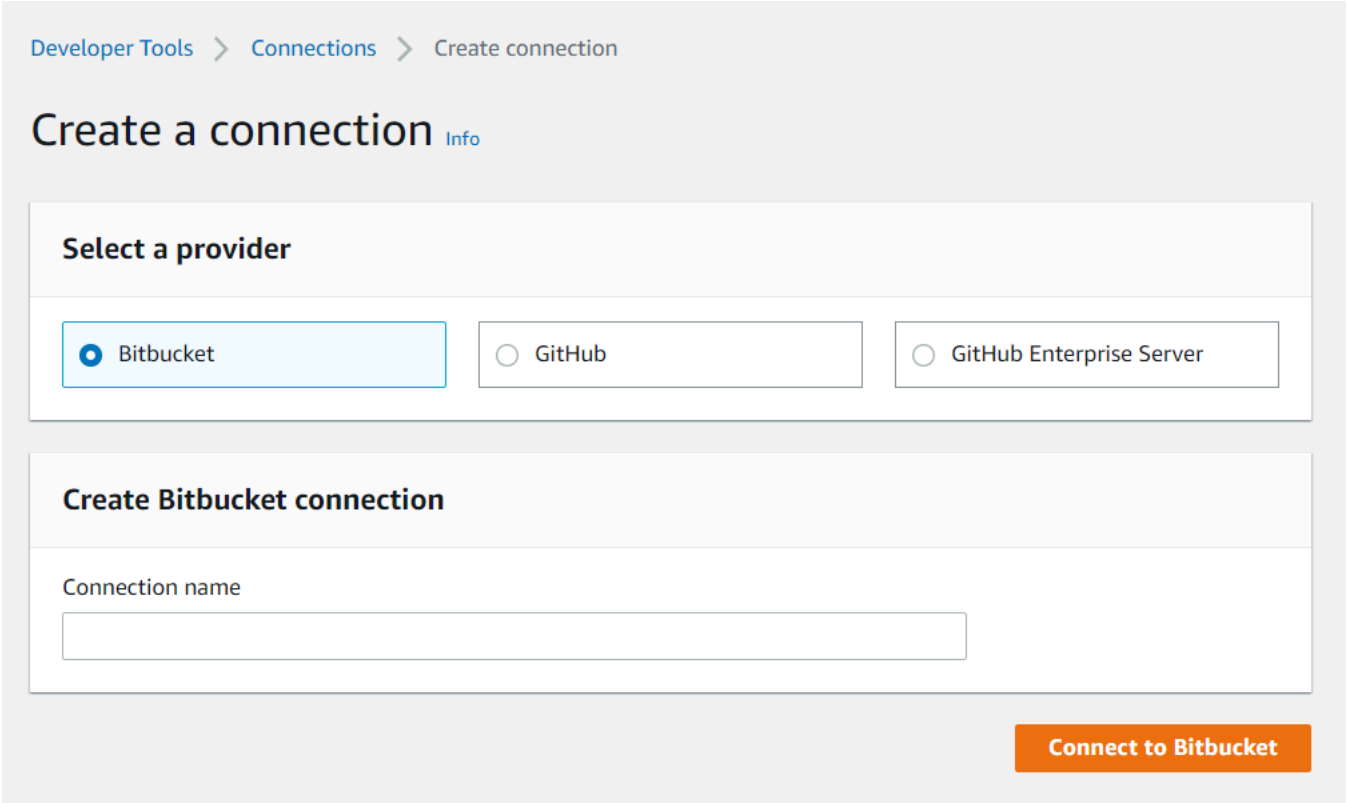
Creare una connessione a Bitbucket (console)

Puoi usare la console per creare una connessione a Bitbucket.

> **Note**
>
> A partire dal 1° luglio 2024, la console crea connessioni con `codeconnections` la risorsa ARN. Le risorse con entrambi i prefissi di servizio continueranno a essere visualizzate nella console.

Fase 1: creazione della connessione

1. Accedi a AWS Management Console, e apri la console AWS Developer Tools all'indirizzo. https://console.aws.amazon.com/codesuite/settings/connections
2. Seleziona Settings > Connections (Impostazioni > Connessioni), quindi Create connection (Crea connessione).
3. Per creare una connessione a un repository Bitbucket, in Select a provider (Seleziona un provider), scegli Bitbucket. In Connection name (Nome connessione), immetti il nome della connessione che desideri creare. Scegli Connect to Bitbucket (Connessione a Bitbucket) e procedi alla fase 2.

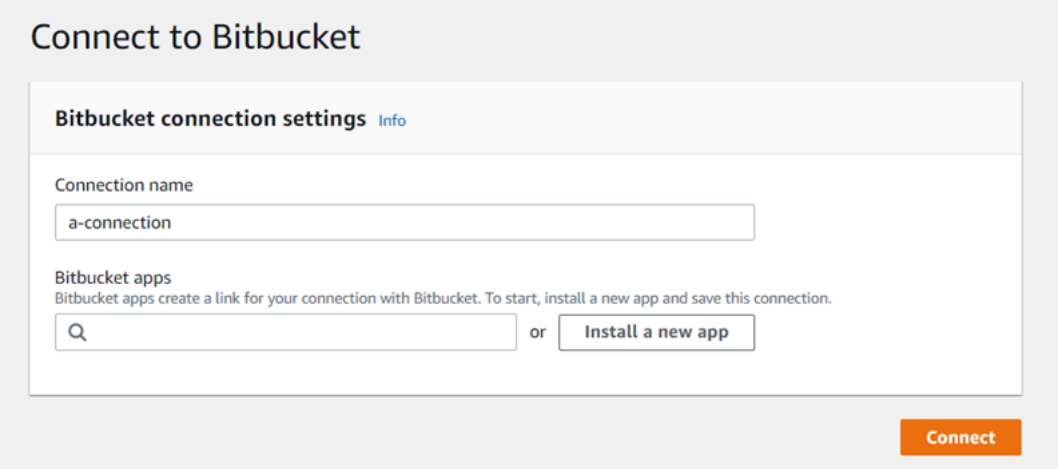


Fase 2: Connessione a Bitbucket

1. Sulla pagina di impostazioni Connect to Bitbucket (Connessione a Bitbucket), viene visualizzato il nome della connessione.

   In Bitbucket apps (App Bitbucket), selezionare l'installazione di un'app o Install a new app (Installa una nuova app) per crearne una.

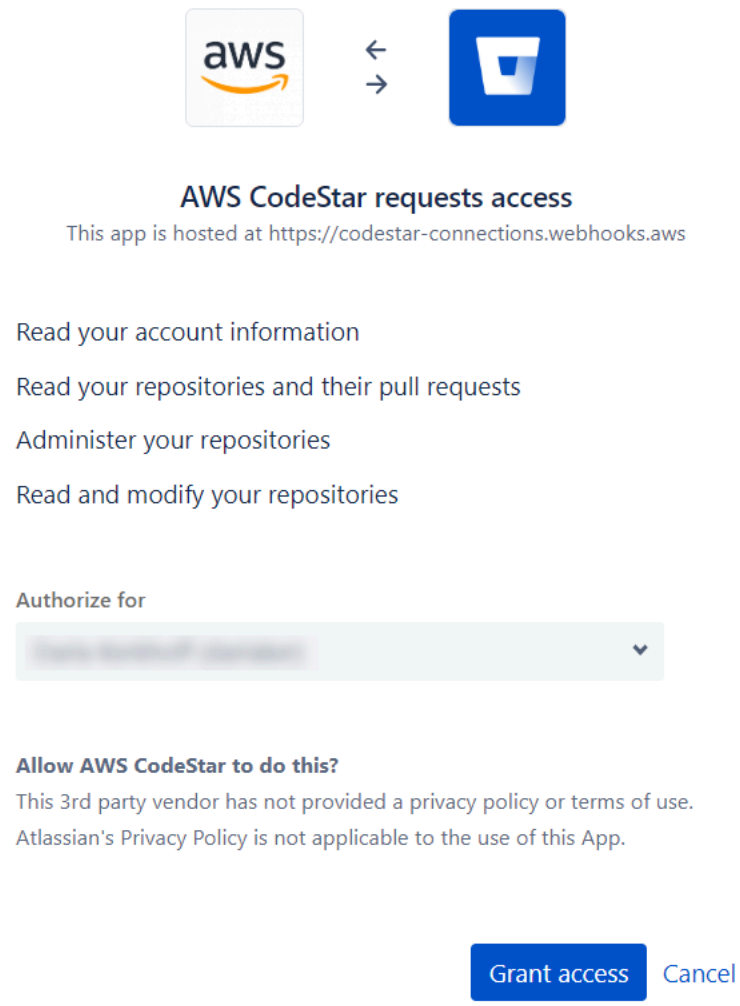
   > **Note**
   >
   > Installare l'app una sola volta per ogni workspace o account Bitbucket. Se l'app Bitbucket è già stata installata, selezionala e passa all'ultima fase di questa sezione.



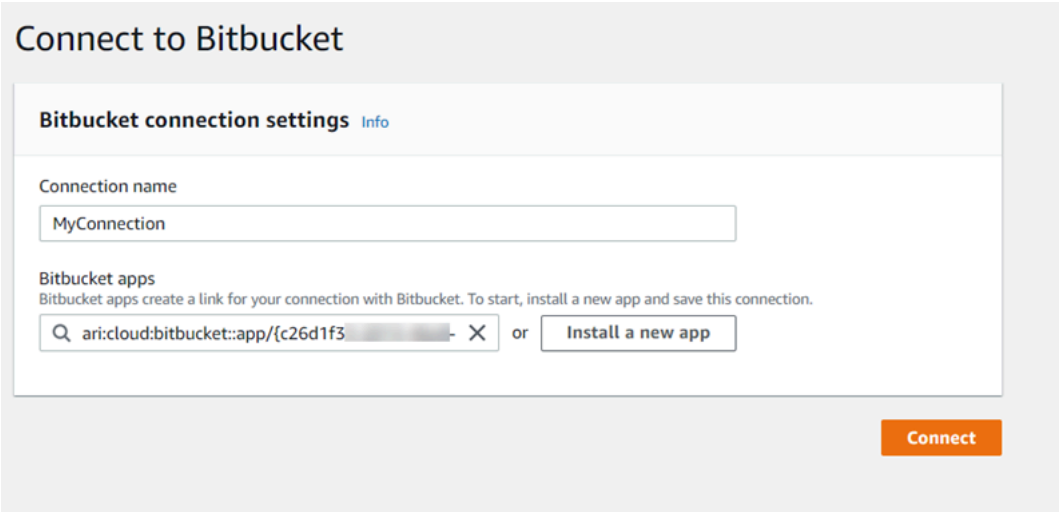
2. Se viene visualizzata la pagina di accesso per Bitbucket, accedi con le tue credenziali e scegli di continuare.
3. Nella pagina di installazione dell'app, un messaggio indica che l' AWS CodeStar app sta tentando di connettersi al tuo account Bitbucket.

   Se si sta usando un workspace Bitbucket, modificare l'opzione Authorize for (Autorizza) per il workspace. Verranno visualizzati solo i workspace ai quali è possibile accedere come amministratore.

   Selezionare Grant access (Concedi accesso).



4. In the connection ID for your new installation is displayed. (App Bitbucket), viene visualizzato l'ID di connessione per la nuova installazione. Scegli Connetti. La connessione creata viene visualizzata nell'elenco delle connessioni.



Creare una connessione a Bitbucket (CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per creare una connessione.

Per farlo, utilizzare il comando create-connection.

> **Important**
>
> Per impostazione predefinita, una connessione creata tramite AWS CLI o AWS CloudFormation è in `PENDING` stato. Dopo aver creato una connessione con la CLI o AWS CloudFormation, utilizza la console per modificare la connessione e definirne lo stato. `AVAILABLE`

Per creare una connessione a Bitbucket

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Usa il AWS CLI per eseguire il create-connection comando, specificando l'`--provider-typee --connection-name` per la tua connessione. In questo esempio, il nome del provider di terze parti è `Bitbucket` e il nome della connessione specificato è `MyConnection`.

   ```
   aws codeconnections create-connection --provider-type Bitbucket --connection-name
    MyConnection
   ```

   In caso di esito positivo, questo comando restituisce informazioni dell'ARN della connessione simili alle seguenti.

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

2. Utilizzare la console per completare la connessione. Per ulteriori informazioni, consulta Aggiornare una connessione in attesa.

Crea una connessione a GitHub

È possibile utilizzare AWS Management Console o il AWS Command Line Interface (AWS CLI) per creare una connessione a GitHub.

Prima di iniziare:

- Devi aver già creato un account con GitHub.
- È necessario aver già creato il repository di codice di terze parti.

> **Note**
>
> Per creare la connessione, devi essere il proprietario GitHub dell'organizzazione. Per i repository che non appartengono a un'organizzazione, è necessario esserne il proprietario.

Argomenti

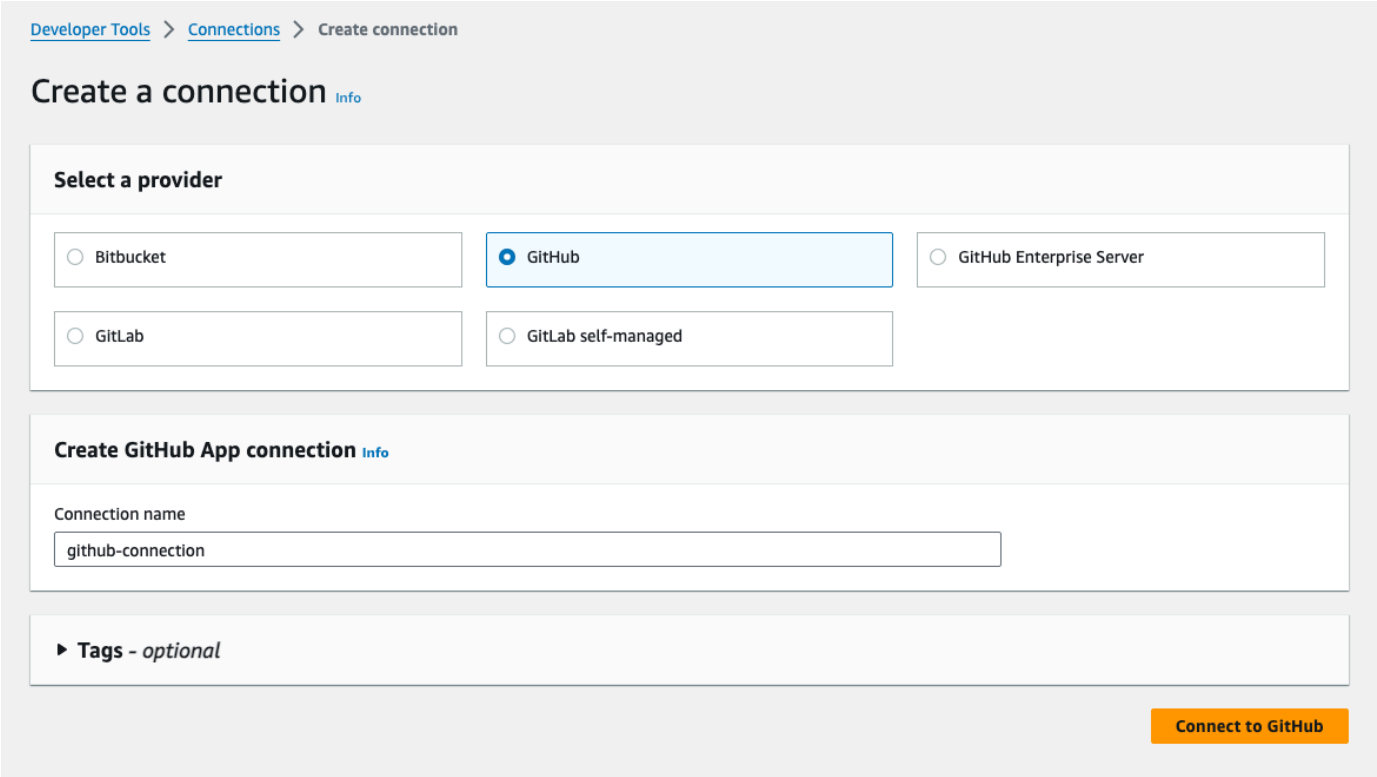
- Crea una connessione a GitHub (console)
- Creare una connessione a GitHub (CLI)

Crea una connessione a GitHub (console)

È possibile utilizzare la console per creare una connessione a GitHub.

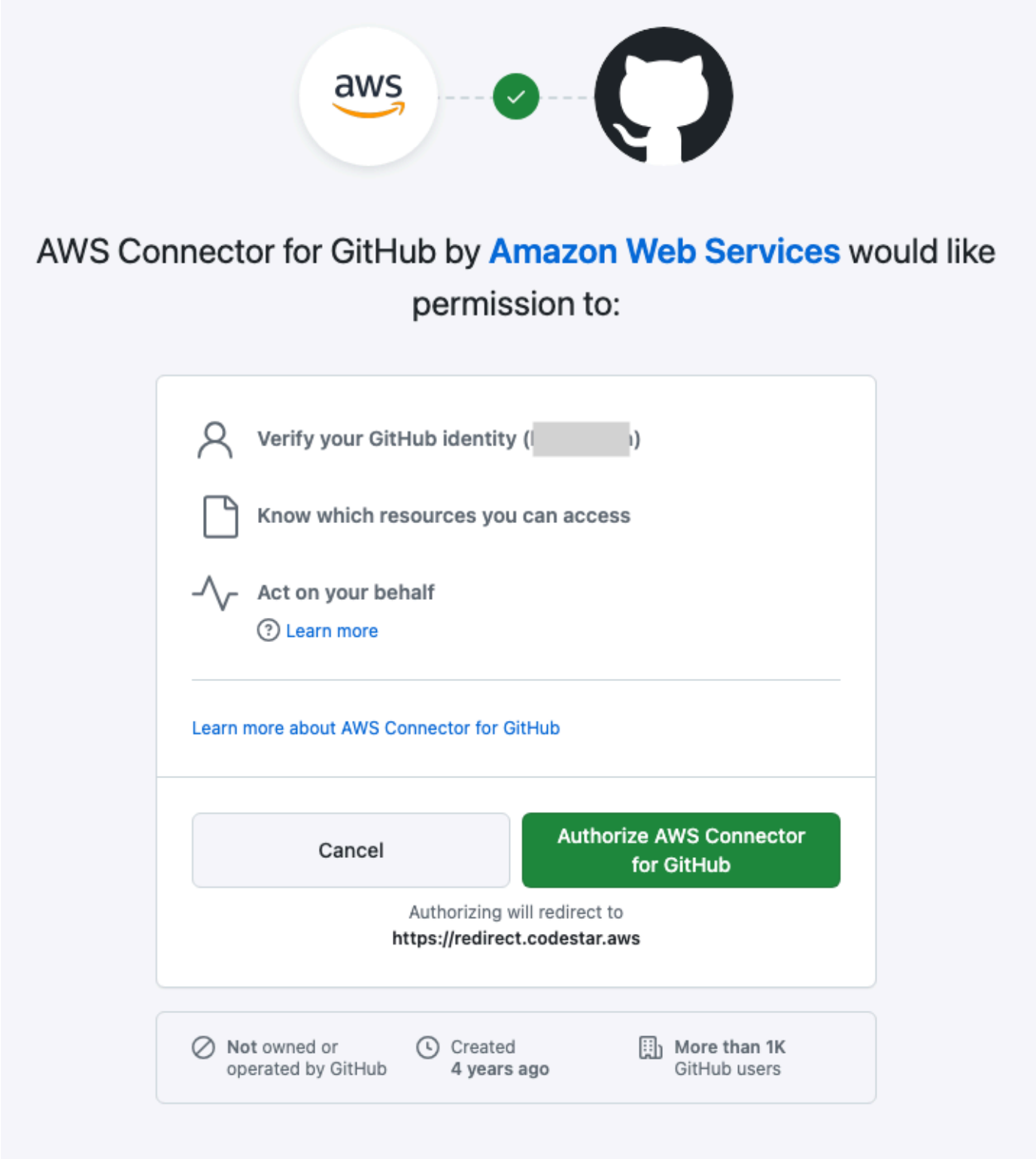
> **Note**
>
> A partire dal 1° luglio 2024, la console crea connessioni con `codeconnections` la risorsa ARN. Le risorse con entrambi i prefissi di servizio continueranno a essere visualizzate nella console.

1. Accedi a AWS Management Console, e apri la console Developer Tools all'indirizzo. https://console.aws.amazon.com/codesuite/settings/connections
2. Seleziona Settings > Connections (Impostazioni > Connessioni), quindi Create connection (Crea connessione).
3. Per creare una connessione a un repository GitHub o GitHub Enterprise Cloud, in Seleziona un provider, scegli GitHub. In Connection name (Nome connessione), immetti il nome della connessione che desideri creare. Scegli Connect GitHub to e procedi al passaggio 2.

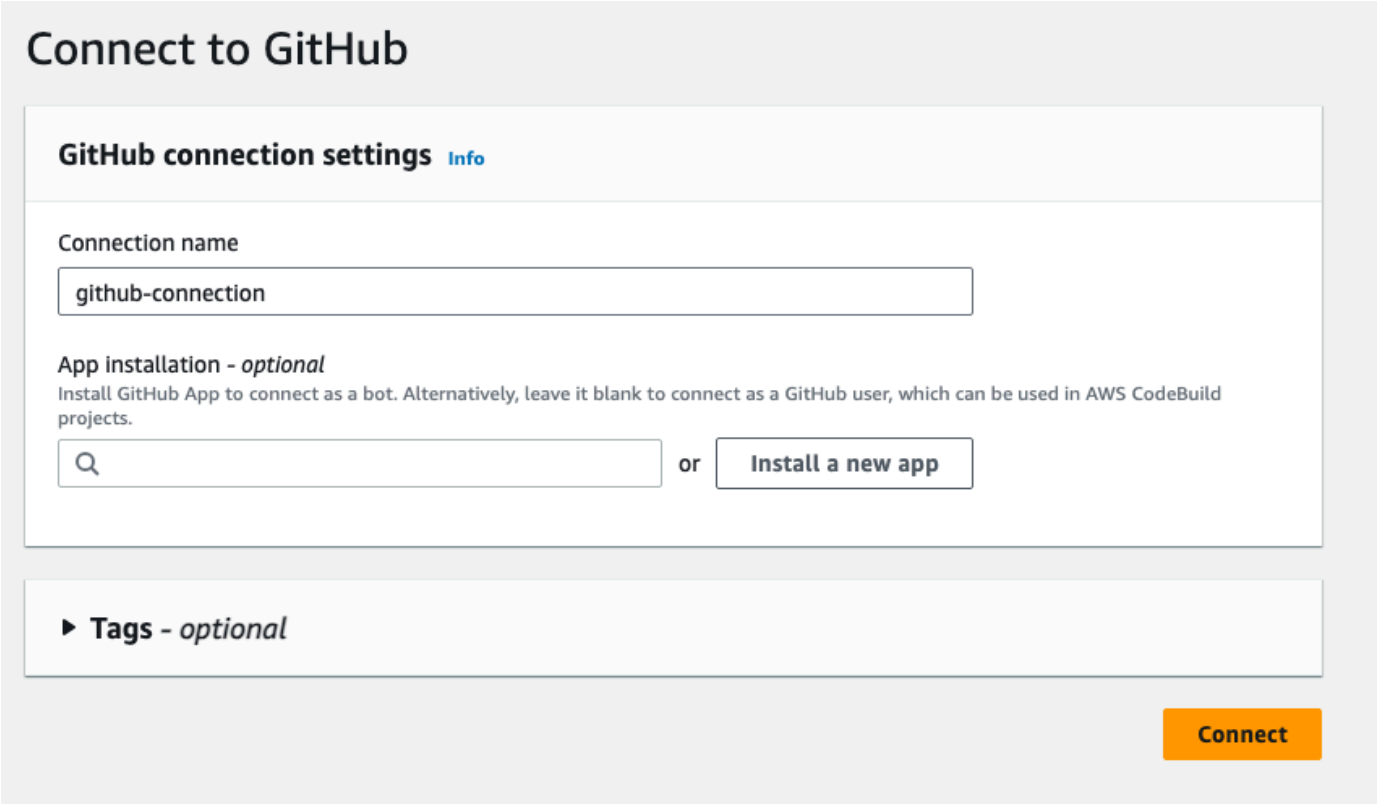


Per creare una connessione a GitHub

1. Nelle impostazioni di GitHub connessione, il nome della connessione viene visualizzato in Nome connessione. Scegliere Connect to GitHub (Connetti ad Amazon Aurora). Viene visualizzata la pagina di richiesta di accesso.



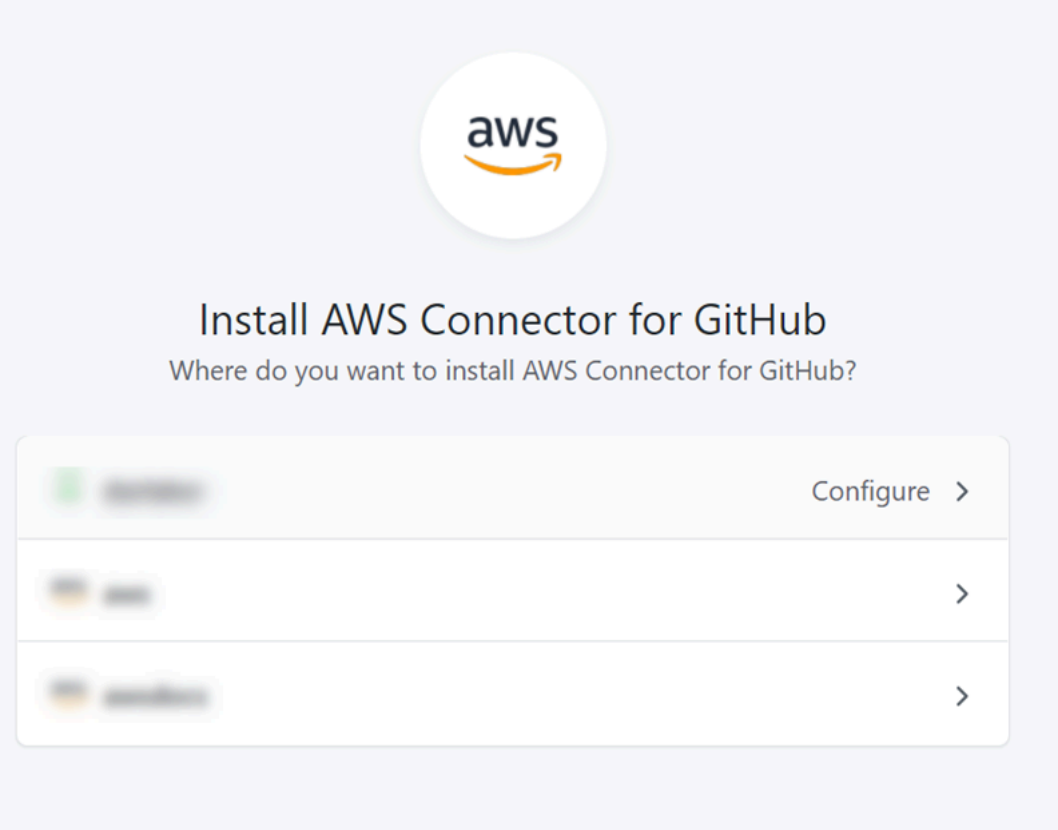
2. Scegli Authorize AWS Connector per. GitHub La pagina di connessione visualizza e mostra il campo GitHub App.



3. In GitHub App, scegli l'installazione dell'app o scegli Installa una nuova app per crearne una.

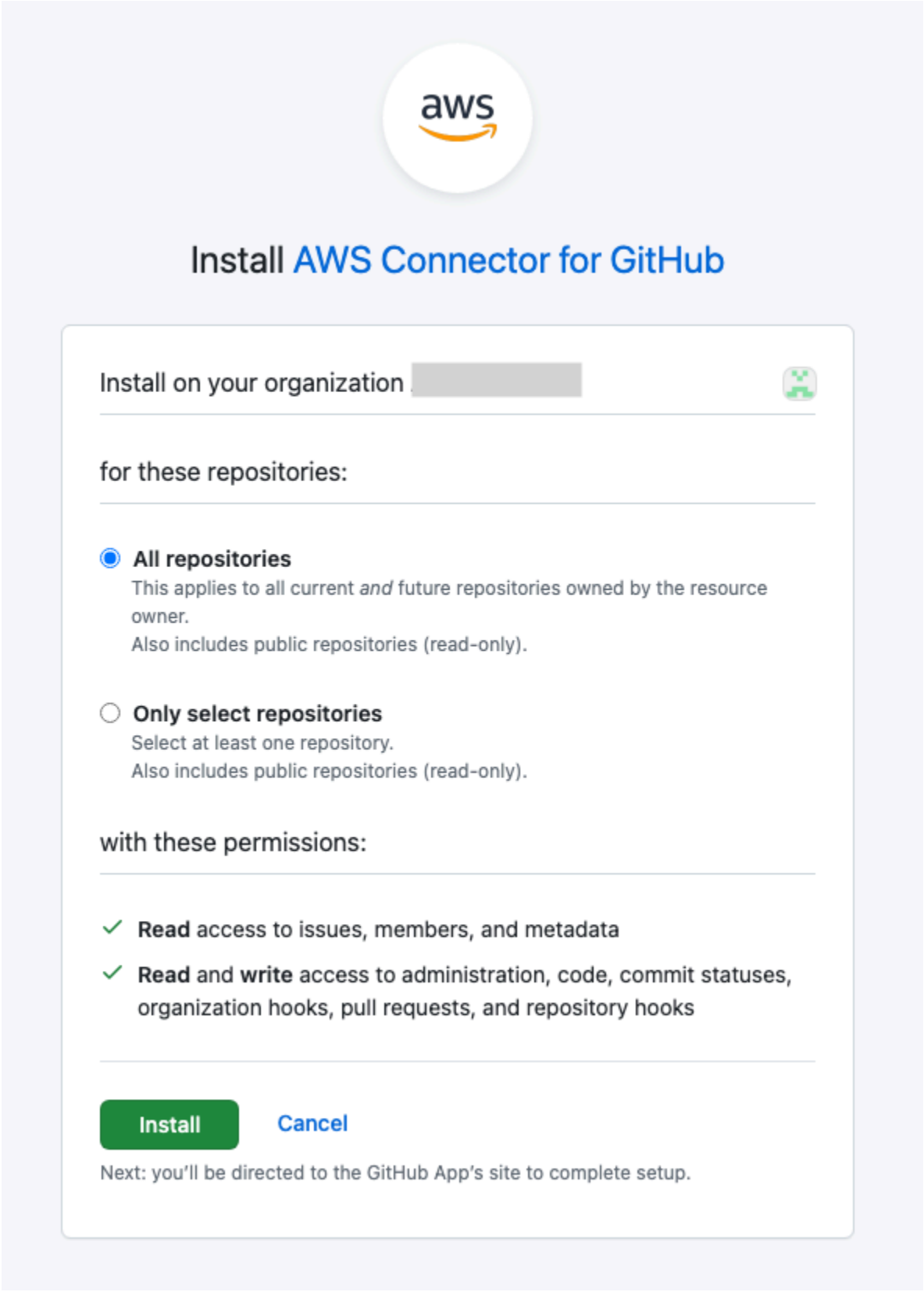
> **Note**
>
> È sufficiente installare una sola app per tutte le connessioni a un provider specifico. Se hai già installato il AWS Connector for GitHub app, sceglilo e salta questo passaggio.

4. Nella GitHub pagina Installa AWS Connector per, scegli l'account in cui desideri installare l'app.



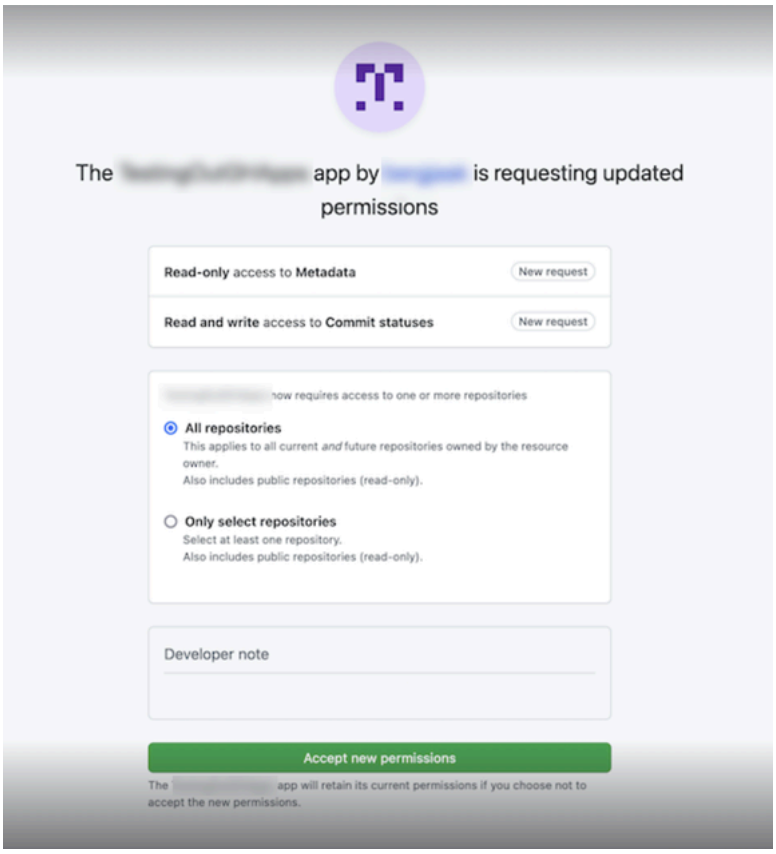
> **Note**
>
> L'app si installa una sola volta per ogni GitHub account. Se hai già installato l'app, puoi scegliere Configure (Configura) per passare a una pagina di modifica per l'installazione dell'app oppure è possibile utilizzare il pulsante Indietro per tornare alla console.

5. Nella GitHub pagina Install AWS Connector per, lascia le impostazioni predefinite e scegli Installa.


aws
Install AWS Connector for GitHub
Install on your organization
for these repositories:
All repositories
This applies to all current and future repositories owned by the resource owner.
Also includes public repositories (read-only).
Only select repositories
Select at least one repository.
Also includes public repositories (read-only).
with these permissions:
Read access to issues, members, and metadata
Read and write access to administration, code, commit statuses, organization hooks, pull requests, and repository hooks
Install
Cancel
Next: you'll be directed to the GitHub App's site to complete setup.

Dopo questo passaggio, potrebbe essere visualizzata una pagina delle autorizzazioni aggiornata. GitHub

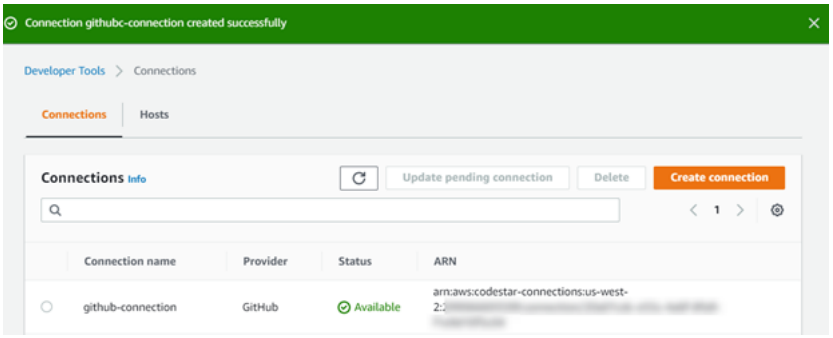
6. Se viene visualizzata una pagina che indica che sono disponibili autorizzazioni aggiornate per il AWS Connector for GitHub app, scegli Accetta nuove autorizzazioni.



7. Si torna alla GitHub pagina Connect to. L'ID di connessione per la nuova installazione viene visualizzato in GitHubApp. Scegli Connetti.

Visualizzare la connessione creata

- La connessione creata viene visualizzata nell'elenco delle connessioni.



Creare una connessione a GitHub (CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per creare una connessione a GitHub.

Per farlo, utilizzare il comando create-connection.

> **Important**
>
> Per impostazione predefinita, una connessione creata tramite AWS CLI o AWS CloudFormation è in `PENDING` stato. Dopo aver creato una connessione con la CLI o AWS CloudFormation, utilizza la console per modificare la connessione e definirne lo stato. `AVAILABLE`

Per creare una connessione a GitHub

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzate il AWS CLI per eseguire il create-connection comando, specificando `--provider-type` e `--connection-name` per la connessione. In questo esempio, il nome del provider di terze parti è `GitHub` e il nome della connessione specificato è `MyConnection`.

   ```
   aws codeconnections create-connection --provider-type GitHub --connection-name
    MyConnection
   ```

   In caso di esito positivo, questo comando restituisce informazioni dell'ARN della connessione simili alle seguenti.

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

2. Utilizzare la console per completare la connessione. Per ulteriori informazioni, consulta Aggiornare una connessione in attesa.

Creare una connessione a GitHub Enterprise Server

Le connessioni vengono utilizzate per associare le AWS risorse a un repository di terze parti. È possibile utilizzare AWS Management Console o il AWS Command Line Interface (AWS CLI) per creare una connessione a GitHub Enterprise Server.

Le connessioni forniscono l'accesso solo agli archivi di proprietà dell'account GitHub Enterprise Server utilizzato durante la creazione della connessione per autorizzare l'installazione dell' GitHubapp.

Prima di iniziare:

- È necessario disporre già di un'istanza di GitHub Enterprise Server e di un repository al suo interno.
- È necessario essere un amministratore dell'istanza di GitHub Enterprise Server per creare GitHub app e creare una risorsa host, come illustrato in questa sezione.

> **Important**
>
> Quando si configura l'host per GitHub Enterprise Server, viene creato automaticamente un endpoint VPC per i dati degli eventi webhook. Se hai creato l'host prima del 24 novembre 2020 e desideri utilizzare gli endpoint PrivateLink webhook VPC, devi prima eliminare l'host e quindi creare un nuovo host.

> **Note**
>
> Per le organizzazioni in GitHub Enterprise Server o GitLab gestite in modo autonomo, non è necessario fornire un host disponibile. Crei un nuovo host per ogni connessione nell'organizzazione e devi assicurarti di inserire le stesse informazioni nei campi di rete (ID VPC, sottorete IDs e gruppo di sicurezza IDs) per l'host. Per ulteriori informazioni, consulta Configurazione della connessione e dell'host per i provider installati che supportano le organizzazioni.

Argomenti

- Creare una connessione a GitHub Enterprise Server (console)

- Creare una connessione a GitHub Enterprise Server (CLI)

Creare una connessione a GitHub Enterprise Server (console)

Per creare una connessione GitHub Enterprise Server, è necessario fornire informazioni su dove è installato l' GitHub Enterprise Server e autorizzare la creazione della connessione con le credenziali GitHub Enterprise.

> **Note**
>
> A partire dal 1° luglio 2024, la console crea connessioni con `codeconnections` la risorsa ARN. Le risorse con entrambi i prefissi di servizio continueranno a essere visualizzate nella console.

Argomenti

- Crea la tua connessione GitHub Enterprise Server (console)

Crea la tua connessione GitHub Enterprise Server (console)

Per creare una connessione a GitHub Enterprise Server, tenete a portata di mano l'URL del server e le credenziali GitHub Enterprise.

Per creare un host

1. Accedere a e aprire AWS Management Console la console AWS Developer Tools all'indirizzohttps://console.aws.amazon.com/codesuite/settings/connections.
2. Sulla scheda Host (Host), sceglie Create host (Crea host).
3. In Host name (Nome host), immetti il nome da utilizzare per l'host.
4. In Seleziona un provider, scegli una delle seguenti opzioni:
   - GitHub Server aziendale
   - GitLab autogestito
5. In URL, immetti l'endpoint per l'infrastruttura in cui è installato il provider.
6. Se il tuo server è configurato all'interno di un VPC Amazon e vuoi connetterti al tuo VPC, scegli Use a VPC (Utilizza un VPC). In caso contrario, scegliere No VPC (Nessun VPC).

7. Se hai lanciato la tua istanza in un VPC Amazon e vuoi connetterti con il tuo VPC, scegli Use a VPC (Utilizzo di un VPC) e completa quanto segue.

   a. In VPC ID (ID VPC), seleziona l'ID VPC. Assicurati di scegliere il VPC per l'infrastruttura in cui è installata l'istanza o un VPC con accesso all'istanza tramite VPN o Direct Connect.

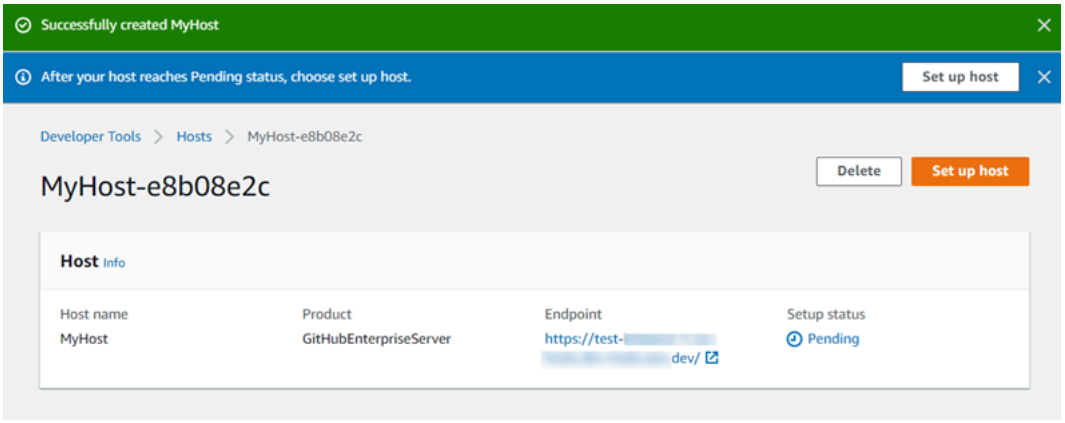
   b. Se disponi di un VPC privato configurato, e l'istanza è stata configurata per eseguire la convalida TLS utilizzando un'autorità di certificazione non pubblica, inserisci l'ID del certificato in Certificato TLS. Il valore del Certificato TLS è la chiave pubblica del certificato.

8. Scegli Create host (Crea host).

9. Dopo la visualizzazione della pagina dei dettagli dell'host, lo stato dell'host quando l'host viene creato.

> **Note**
>
> Se la configurazione dell'host include una configurazione VPC, attendi alcuni minuti per il provisioning dei componenti della rete host.

Attendi che il tuo host raggiunga uno stato Pending (In attesa) e completa l'installazione. Per ulteriori informazioni, consulta Impostare un host in attesa.



Fase 2: Creare la connessione a GitHub Enterprise Server (console)

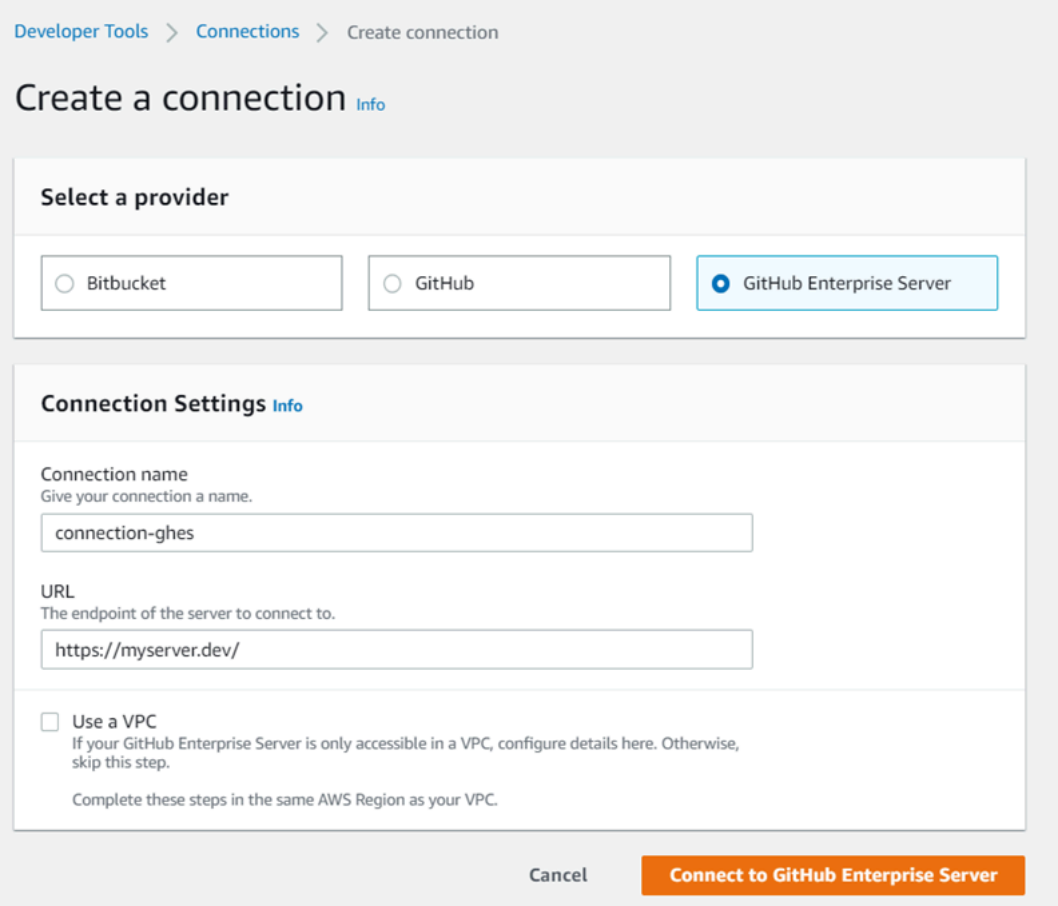
1. Accedi AWS Management Console e apri la console Developer Tools all'indirizzohttps://console.aws.amazon.com/codesuite/settings/connections.

2. Seleziona Settings > Connections (Impostazioni > Connessioni), quindi Create connection (Crea connessione).

3. Per creare una connessione a un repository GitHub Enterprise Server installato, scegli GitHub Enterprise Server.

Connect a GitHub Enterprise Server

1. In Connection Name (Nome connessione), immetti un nome per la connessione.



2. In URL, immetti l'endpoint per il server.

> **Note**
>
> Se l'URL fornito è già stato utilizzato per configurare un GitHub Enterprise Server per una connessione, verrà richiesto di scegliere l'ARN della risorsa host creato in precedenza per quell'endpoint.

3. (Facoltativo) Se hai lanciato il server in un Amazon VPC e vuoi connetterti con il VPC, scegli Utilizza un VPC e completa quanto segue.

> **Note**
>
> Per le organizzazioni in GitHub Enterprise Server o GitLab gestite in modo autonomo, non viene assegnato un host disponibile. Crei un nuovo host per ogni connessione nell'organizzazione e devi assicurarti di inserire le stesse informazioni nei campi di rete (ID VPC, sottorete IDs e gruppo di sicurezza IDs) per l'host. Per ulteriori informazioni, consulta Configurazione della connessione e dell'host per i provider installati che supportano le organizzazioni.

a. In VPC ID (ID VPC), seleziona l'ID VPC. Assicurati di scegliere il VPC per l'infrastruttura in cui è installata l'istanza di GitHub Enterprise Server o un VPC con accesso all'istanza GitHub Enterprise Server tramite VPN o Direct Connect.

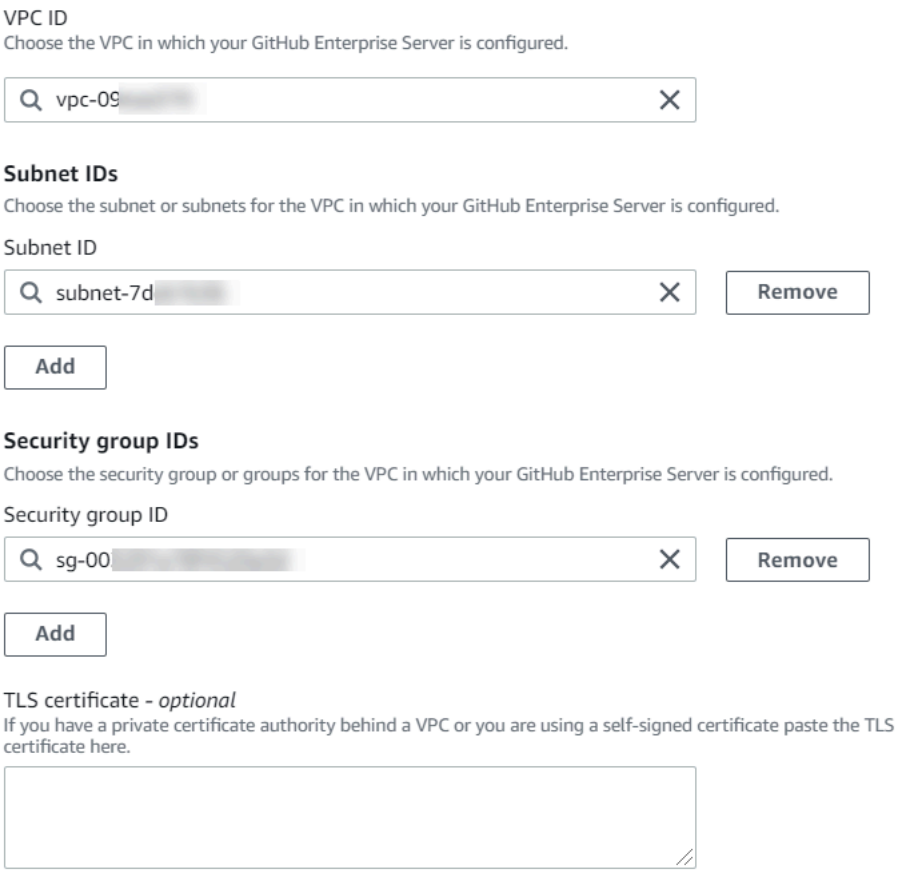
b. In Subnet ID (ID sottorete), scegliere Add (Aggiungi). Nel campo, selezionare l'ID della sottorete che si desidera utilizzare per l'host. È possibile scegliere fino a 10 sottoreti.

   Assicurati di scegliere la sottorete per l'infrastruttura in cui è installata l'istanza di GitHub Enterprise Server o una sottorete con accesso all'istanza GitHub Enterprise Server installata tramite VPN o Direct Connect.

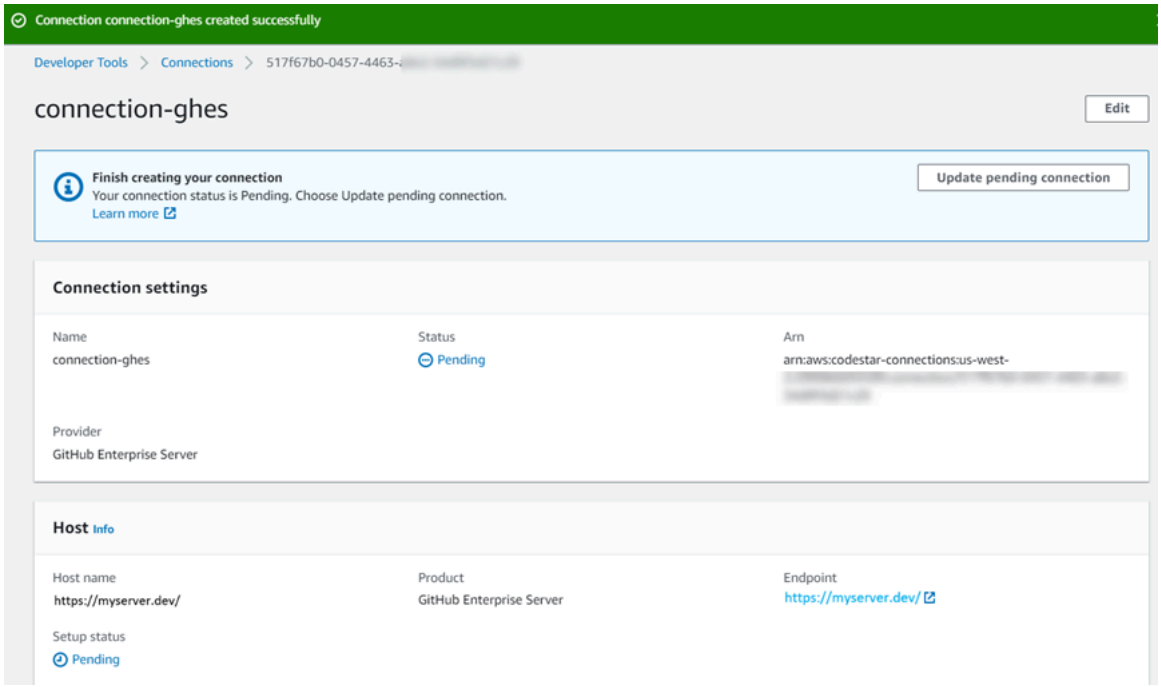
c. Nel gruppo di sicurezza IDs, scegli Aggiungi. Nel campo, selezionare il gruppo di sicurezza che si desidera utilizzare per l'host. È possibile creare fino a 10 gruppi di sicurezza.

   Assicurati di scegliere il gruppo di sicurezza per l'infrastruttura in cui è installata l'istanza di GitHub Enterprise Server o un gruppo di sicurezza con accesso all'istanza GitHub Enterprise Server installata tramite VPN o Direct Connect.

d. Se hai configurato un VPC privato e hai configurato l'istanza di GitHub Enterprise Server per eseguire la convalida TLS utilizzando un'autorità di certificazione non pubblica, nel certificato TLS inserisci l'ID del certificato. Il valore del Certificato TLS deve essere la chiave pubblica del certificato.

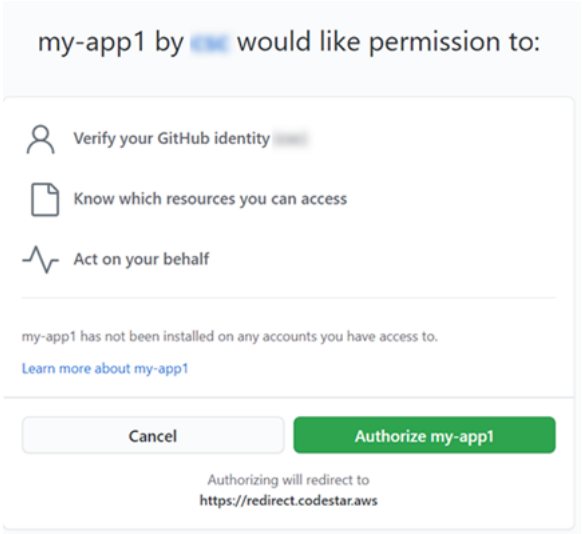


4. Scegli Connect to GitHub Enterprise Server. La connessione creata viene mostrata con uno stato Pending (In attesa). Viene creata una risorsa host per la connessione con le informazioni sul server fornite. Per il nome dell'host, viene utilizzato l'URL.
5. Scegli Update pending connection (Aggiornare la connessione in attesa).



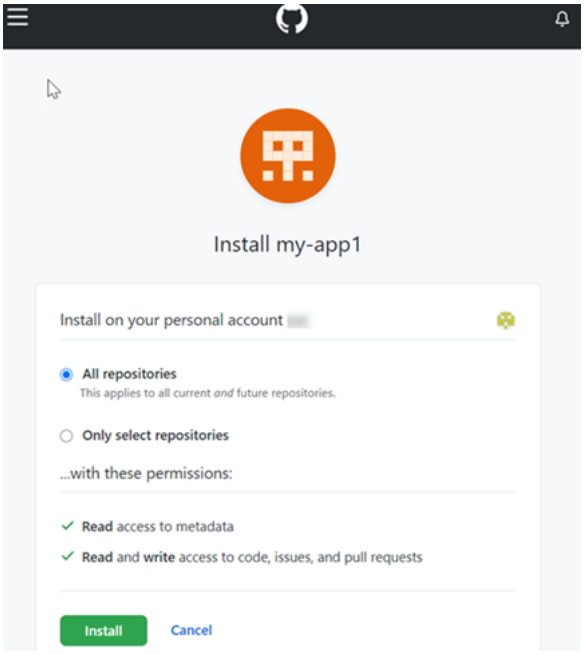
6. Se richiesto, nella pagina di accesso GitHub Enterprise, accedi con le tue GitHub credenziali Enterprise.
7. Nella pagina Crea GitHub app, scegli un nome per la tua app.

8. <app-name>Nella pagina di GitHub autorizzazione, scegli Autorizza.



9. Nella pagina di installazione dell'app, un messaggio indica che l'app Connector è pronta per essere installata. Se disponi di più organizzazioni, potrebbe essere richiesto di scegliere l'organizzazione in cui si desidera installare l'app.

   Scegli le impostazioni del repository in cui desideri installare l'app. Scegli Installa.



10. La pagina di connessione mostra la connessione creata in uno stato Available (Disponibile).

Creare una connessione a GitHub Enterprise Server (CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per creare una connessione.

Per farlo, utilizza i comandi create-host e create-connection.

> **Important**
>
> Per impostazione predefinita, una connessione creata tramite AWS CLI o AWS CloudFormation è in `PENDING` stato. Dopo aver creato una connessione con la CLI o AWS CloudFormation, utilizza la console per modificare la connessione e definirne lo stato. `AVAILABLE`

Fase 1: Creare un host per GitHub Enterprise Server (CLI)

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzare il AWS CLI per eseguire il create-host comando, specificando e `--provider-endpoint` per la `--name` connessione. `--provider-type` In questo esempio, il nome del provider di terze parti è `GitHubEnterpriseServer` e l'endpoint è `my-instance.dev`.

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

   In caso di esito positivo, questo comando restituisce informazioni dell'Amazon Resource Name (ARN) dell'host simili alle seguenti.

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

   Dopo questo passaggio, l'host è nello stato `PENDING`.

2. Utilizza la console per completare la configurazione dell'host e sposta l'host nello stato `Available`. Per ulteriori informazioni, consulta Impostare un host in attesa.

Fase 2: Configurazione di un host in attesa nella console

1. Accedi AWS Management Console e apri la console Developer Tools all'indirizzohttps://console.aws.amazon.com/codesuite/settings/connections.
2. Utilizza la console per completare la configurazione dell'host e sposta l'host nello stato `Available`. Consultare Impostare un host in attesa.

Fase 3: Creare una connessione per GitHub Enterprise Server (CLI)

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzare il AWS CLI per eseguire il create-connection comando, specificando l'`--host-arn` `--connection-name` per la connessione.

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

   In caso di esito positivo, questo comando restituisce informazioni dell'ARN della connessione simili alle seguenti.

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

2. Utilizzare la console per configurare la connessione in attesa. Per ulteriori informazioni, consulta Aggiornare una connessione in attesa.

Passaggio 4: Per completare una connessione per GitHub Enterprise Server nella console

1. Accedi AWS Management Console e apri la console Developer Tools all'indirizzohttps://console.aws.amazon.com/codesuite/settings/connections.
2. Usa la console per configurare la connessione in sospeso e passarla in uno stato `Available`. Per ulteriori informazioni, consulta Aggiornare una connessione in attesa.

Crea una connessione a GitLab

Puoi usare AWS Management Console o il AWS Command Line Interface (AWS CLI) per creare una connessione a un repository ospitato su gitlab.com.

> **Note**
>
> Autorizzando l'installazione di questa connessione in GitLab, concedi al nostro servizio le autorizzazioni per elaborare i tuoi dati e puoi revocare le autorizzazioni in qualsiasi momento disinstallando l'applicazione.

Prima di iniziare:

- Devi aver già creato un account con. GitLab

> **Note**
>
> Le connessioni forniscono l'accesso solo all'account utilizzato per creare e autorizzare la connessione.

> **Note**
>
> È possibile creare connessioni in cui si ricopre il ruolo di Proprietario e quindi la connessione può essere utilizzata con il repository con risorse come CodePipeline. GitLab Per i repository nei gruppi, non è necessario essere il proprietario del gruppo.

Argomenti

- Crea una connessione a GitLab (console)
- Creare una connessione a GitLab (CLI)

Crea una connessione a GitLab (console)

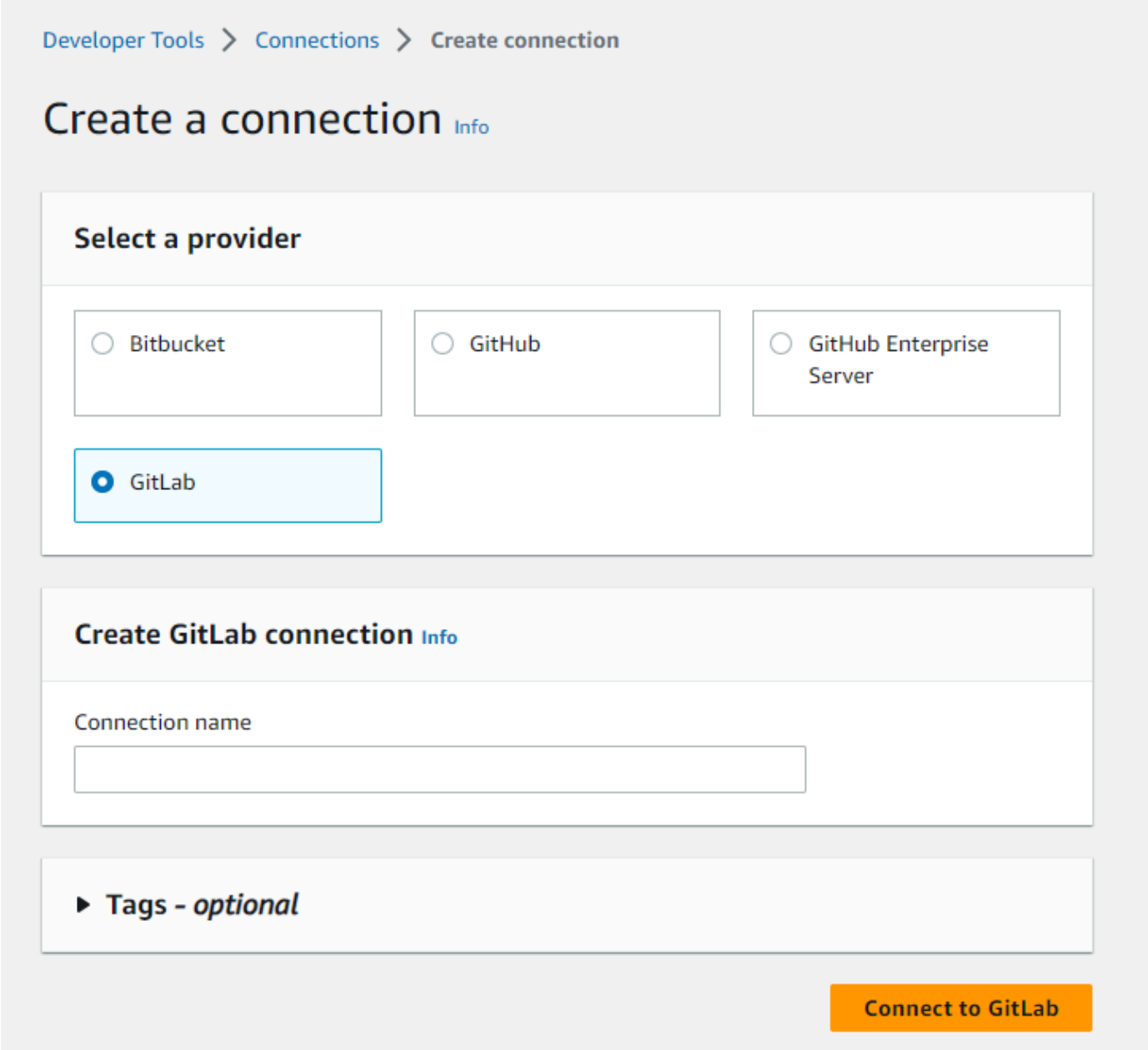
È possibile utilizzare la console per creare una connessione.

> **Note**
>
> A partire dal 1° luglio 2024, la console crea connessioni con `codeconnections` la risorsa ARN. Le risorse con entrambi i prefissi di servizio continueranno a essere visualizzate nella console.

Fase 1: creazione della connessione

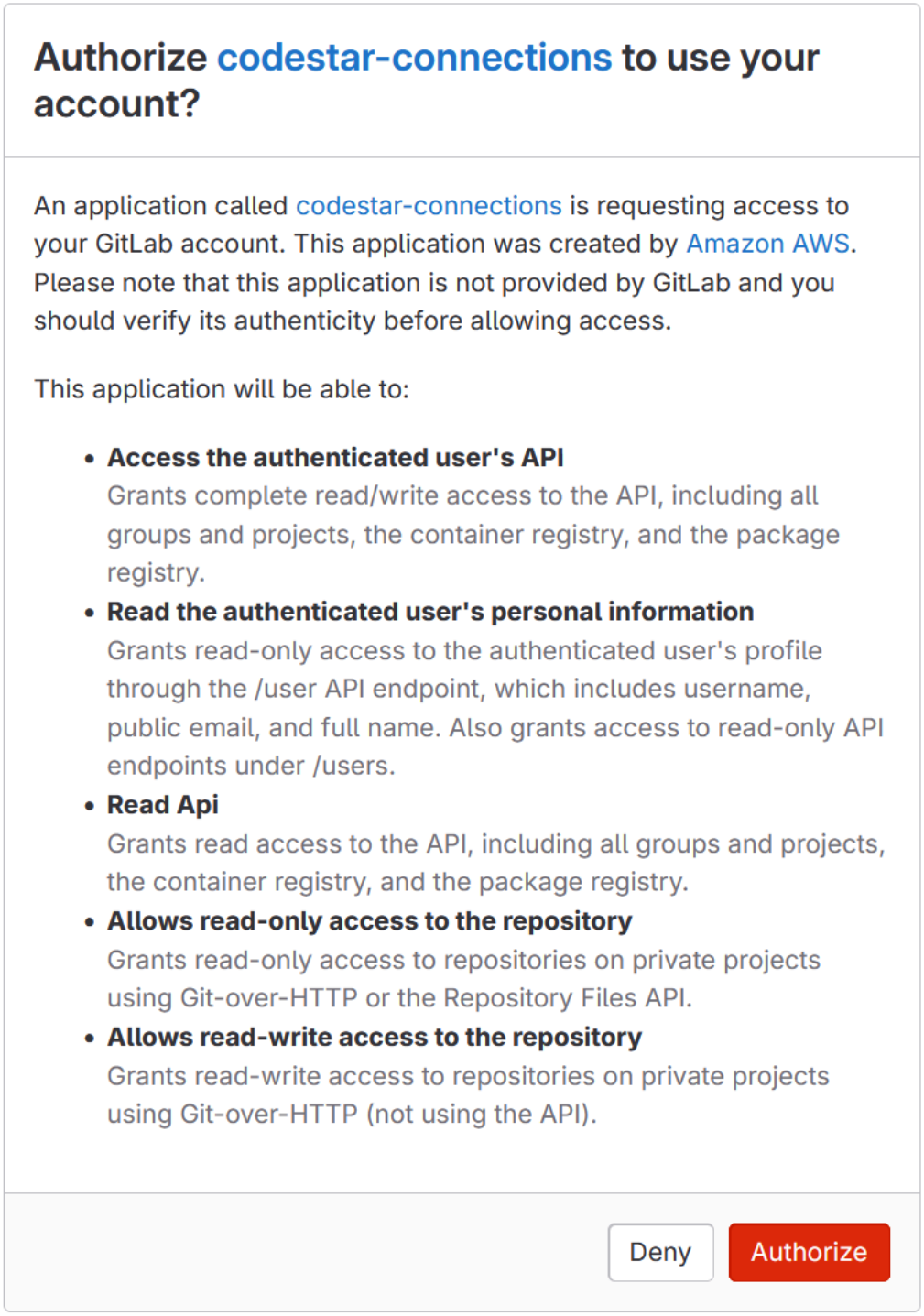
1. Accedi a AWS Management Console, quindi apri la console AWS Developer Tools all'indirizzo. https://console.aws.amazon.com/codesuite/settings/connections
2. Scegli Impostazioni, quindi seleziona Connessioni. Scegli Crea connessione.

3. Per creare una connessione a un GitLab repository, in Seleziona un provider, scegli GitLab. In Connection name (Nome connessione), immetti il nome della connessione che desideri creare. Scegli Connect a GitLab.



4. Quando viene GitLab visualizzata la pagina di accesso, accedi con le tue credenziali, quindi scegli Accedi.
5. Viene visualizzata una pagina di autorizzazione con un messaggio che richiede l'autorizzazione per la connessione per accedere al tuo account. GitLab

   Seleziona Authorize (Autorizza).



6. Il browser torna alla pagina della console delle connessioni. In Crea GitLab connessione, la nuova connessione viene mostrata in Nome connessione.
7. Scegli Connect a GitLab.

Dopo che la connessione è stata creata correttamente, viene visualizzato un banner di operazione riuscita. I dettagli della connessione vengono visualizzato nella pagina Impostazioni di connessione.

Creare una connessione a GitLab (CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per creare una connessione.

Per farlo, utilizzare il comando create-connection.

> **Important**
>
> Per impostazione predefinita, una connessione creata tramite AWS CLI o AWS CloudFormation è in `PENDING` stato. Dopo aver creato una connessione con la CLI o AWS CloudFormation, utilizza la console per modificare la connessione e definirne lo stato. `AVAILABLE`

Per creare una connessione a GitLab

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzate il AWS CLI per eseguire il create-connection comando, specificando `--provider-type` e `--connection-name` per la connessione. In questo esempio, il nome del provider di terze parti è `GitLab` e il nome della connessione specificato è `MyConnection`.

   ```
   aws codeconnections create-connection --provider-type GitLab --connection-name
    MyConnection
   ```

   In caso di esito positivo, questo comando restituisce informazioni dell'ARN della connessione simili alle seguenti.

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

2. Utilizzare la console per completare la connessione. Per ulteriori informazioni, consulta Aggiornare una connessione in attesa.

Crea una connessione a gestione automatica GitLab

È possibile creare connessioni per GitLab Enterprise Edition o GitLab Community Edition con un'installazione gestita automaticamente.

È possibile utilizzare AWS Management Console o il AWS Command Line Interface (AWS CLI) per creare una connessione e un host per la gestione GitLab automatica.

> **Note**
>
> Autorizzando questa applicazione di connessione in modalità GitLab autogestita, concedi al nostro servizio le autorizzazioni per elaborare i tuoi dati e puoi revocare le autorizzazioni in qualsiasi momento disinstallando l'applicazione.

Prima di creare una connessione a GitLab gestione automatica, è necessario creare un host da utilizzare per la connessione, come descritto in questi passaggi. Per una panoramica del flusso di lavoro di creazione di un host per i provider installati, consulta Flusso di lavoro per la creazione o l'aggiornamento di un host.

Facoltativamente, puoi configurare l'host con un VPC. Per ulteriori informazioni sulla configurazione di rete e del VPC per la risorsa host consulta i prerequisiti VPC in (Facoltativo) Prerequisiti: configurazione di rete o Amazon VPC per la connessione e Risoluzione dei problemi di configurazione VPC per l'host.

Prima di iniziare:

- È necessario aver già creato un account con GitLab GitLab Enterprise Edition o GitLab Community Edition con installazione autogestita. Per ulteriori informazioni, consulta https://docs.gitlab.com/ee/subscriptions/self_managed/.

  > **Note**
  >
  > Le connessioni forniscono l'accesso solo all'account utilizzato per creare e autorizzare la connessione.

> **Note**
>
> È possibile creare connessioni a un repository in cui si ricopre il ruolo di Proprietario e quindi la connessione può essere utilizzata con risorse come. GitLab CodePipeline Per i repository nei gruppi, non è necessario essere il proprietario del gruppo.

- È necessario aver già creato un token di accesso GitLab personale (PAT) solo con la seguente autorizzazione limitata:,. `api` `admin_mode` Per ulteriori informazioni, consulta _access_tokens.html. https://docs.gitlab.com/ee/ user/profile/personal È necessario essere un amministratore per creare e utilizzare il PAT.

> **Note**
>
> Il PAT viene utilizzato per autorizzare l'host e non viene altrimenti archiviato o utilizzato dalle connessioni. Per configurare un host, puoi creare un PAT temporaneo e quindi, dopo aver configurato l'host, puoi eliminare il PAT.

> **Note**
>
> Per le organizzazioni in GitHub Enterprise Server o GitLab gestite in modo autonomo, non è necessario fornire un host disponibile. Crei un nuovo host per ogni connessione nell'organizzazione e devi assicurarti di inserire le stesse informazioni nei campi di rete (ID VPC, sottorete IDs e gruppo di sicurezza IDs) per l'host. Per ulteriori informazioni, consulta Configurazione della connessione e dell'host per i provider installati che supportano le organizzazioni.

Argomenti

- Crea una connessione a GitLab gestione automatica (console)
- Crea una connessione a GitLab gestione automatica (CLI)

Crea una connessione a GitLab gestione automatica (console)

Utilizza questi passaggi per creare un host e una connessione per la GitLab gestione automatica nella console. Per le considerazioni relative alla configurazione di un host in un VPC, consulta (Facoltativo) Prerequisiti: configurazione di rete o Amazon VPC per la connessione.

> **Note**
>
> A partire dal 1° luglio 2024, la console crea connessioni con `codeconnections` la risorsa ARN. Le risorse con entrambi i prefissi di servizio continueranno a essere visualizzate nella console.

> **Note**
>
> È possibile creare un host per una singola installazione GitLab autogestita, quindi gestire una o più connessioni GitLab autogestite a tale host.

Fase 1: Creazione dell'host

1. Accedi a AWS Management Console, quindi apri la console AWS Developer Tools all'indirizzo. https://console.aws.amazon.com/codesuite/settings/connections
2. Sulla scheda Host (Host), sceglie Create host (Crea host).
3. In Host name (Nome host), immetti il nome da utilizzare per l'host.
4. In Seleziona un provider, scegli GitLabGestione automatica.
5. In URL, immetti l'endpoint per l'infrastruttura in cui è installato il provider.
6. Se il tuo server è configurato all'interno di un VPC Amazon e vuoi connetterti al tuo VPC, scegli Use a VPC (Utilizza un VPC). In caso contrario, scegliere No VPC (Nessun VPC).
7. (Facoltativo) Se hai lanciato l'host in un Amazon VPC e vuoi connetterti con il VPC, scegli Utilizza un VPC e completa quanto segue.

   > **Note**
   >
   > Per le organizzazioni in GitHub Enterprise Server o GitLab gestite in modo autonomo, non viene assegnato un host disponibile. Crei un nuovo host per ogni connessione nell'organizzazione e devi assicurarti di inserire le stesse informazioni nei campi di rete

(ID VPC, sottorete IDs e gruppo di sicurezza IDs) per l'host. Per ulteriori informazioni, consulta Configurazione della connessione e dell'host per i provider installati che supportano le organizzazioni.

a. In VPC ID (ID VPC), seleziona l'ID VPC. Assicurati di scegliere il VPC per l'infrastruttura in cui è installato l'host o un VPC con accesso all'istanza tramite VPN o Direct Connect.

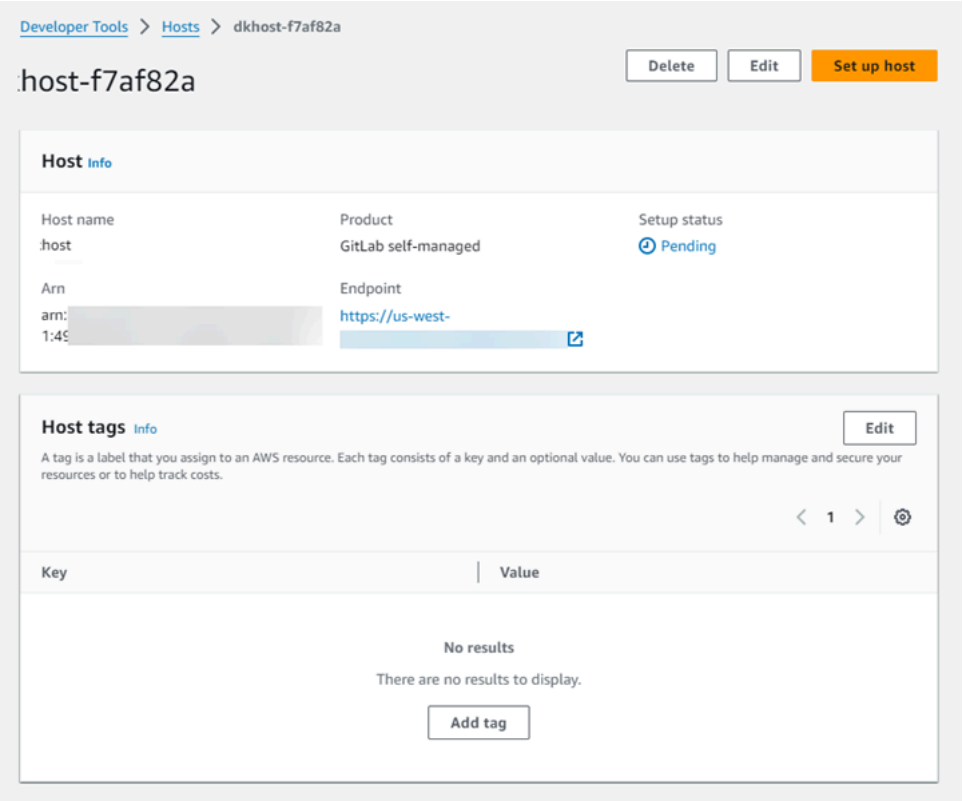
b. Se disponi di un VPC privato configurato, e l'host è stato configurato per eseguire la convalida TLS utilizzando un'autorità di certificazione non pubblica, inserisci l'ID del certificato in Certificato TLS. Il valore del Certificato TLS è la chiave pubblica del certificato.

8. Scegli Create host (Crea host).

9. Dopo la visualizzazione della pagina dei dettagli dell'host, lo stato dell'host quando l'host viene creato.

> **Note**
>
> Se la configurazione dell'host include una configurazione VPC, attendi alcuni minuti per il provisioning dei componenti della rete host.

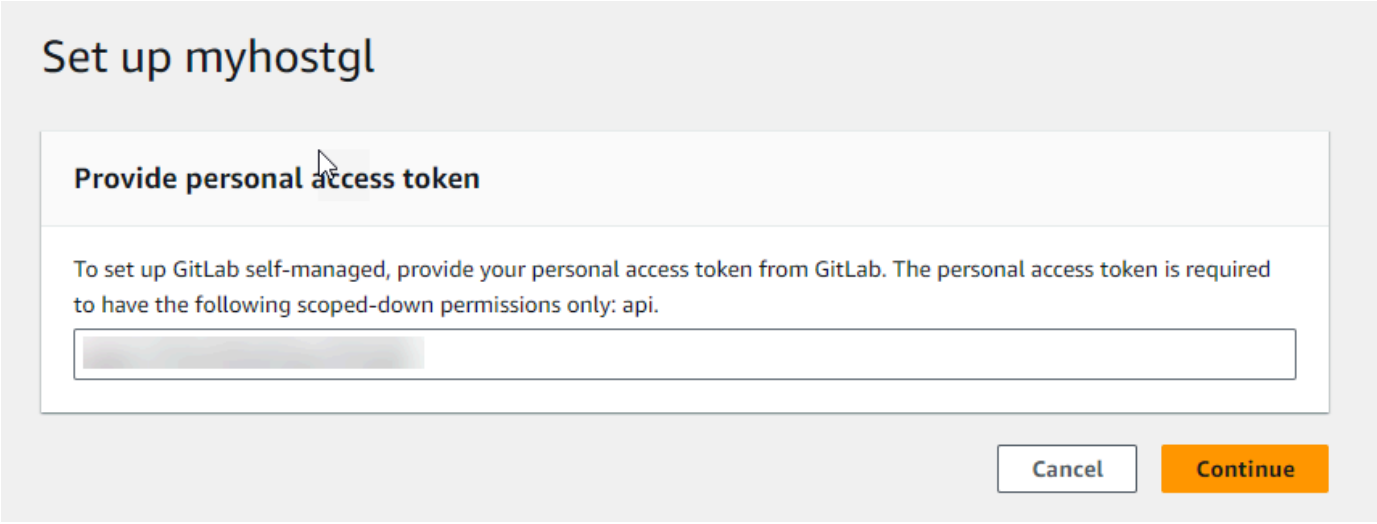
Attendi che il tuo host raggiunga uno stato Pending (In attesa) e completa l'installazione. Per ulteriori informazioni, consulta Impostare un host in attesa.



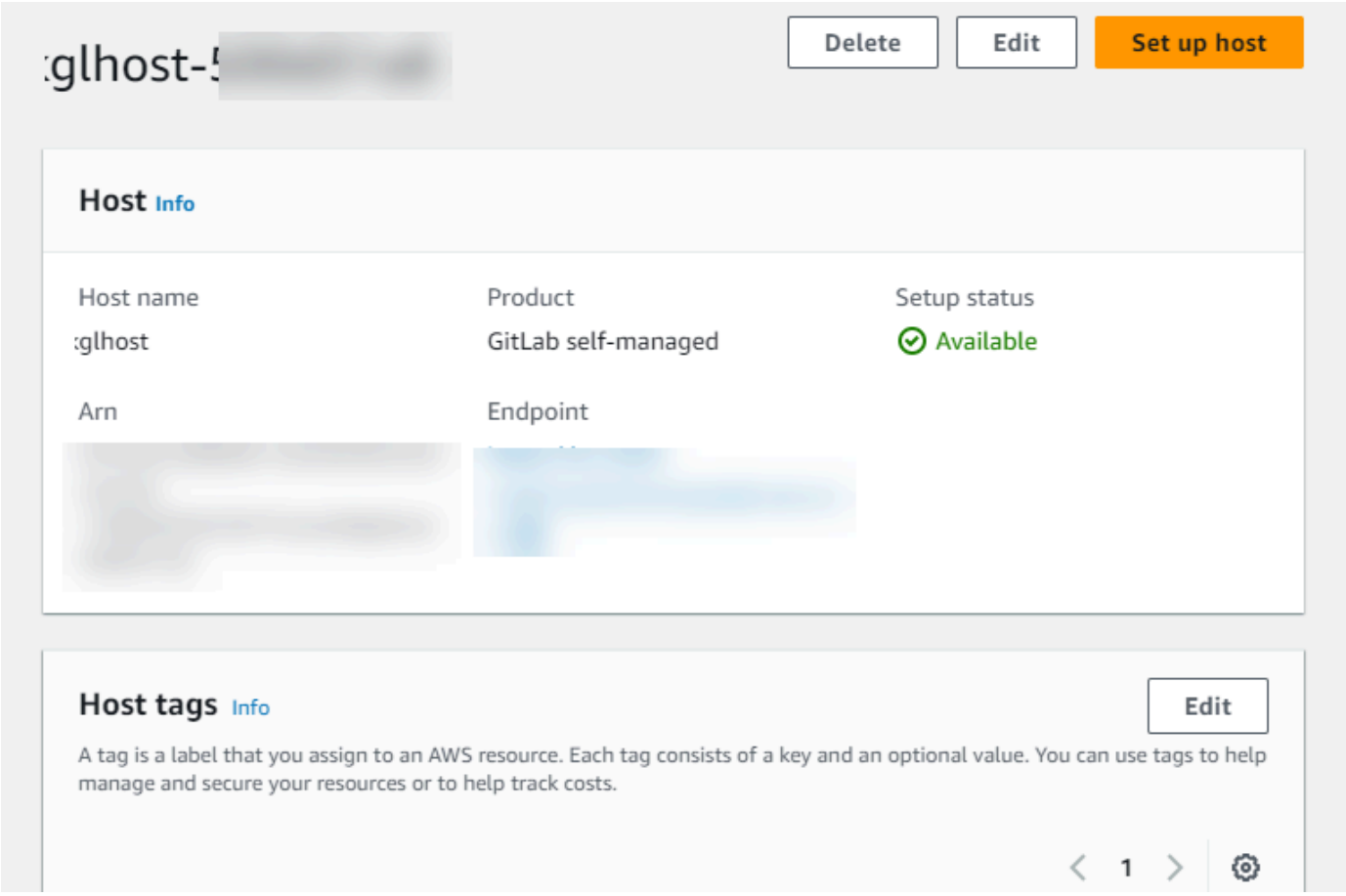
Fase 2: Configurazione dell'host in attesa

1. Scegli Configura host.
2. Viene visualizzata una pagina di configurazione. ***`host_name`*** In Fornisci un token di accesso personale, fornisci GitLab al tuo PAT solo le seguenti autorizzazioni ridotte: e. `api` `admin_mode`

> **Note**
>
> Solo un amministratore può creare e utilizzare il PAT.

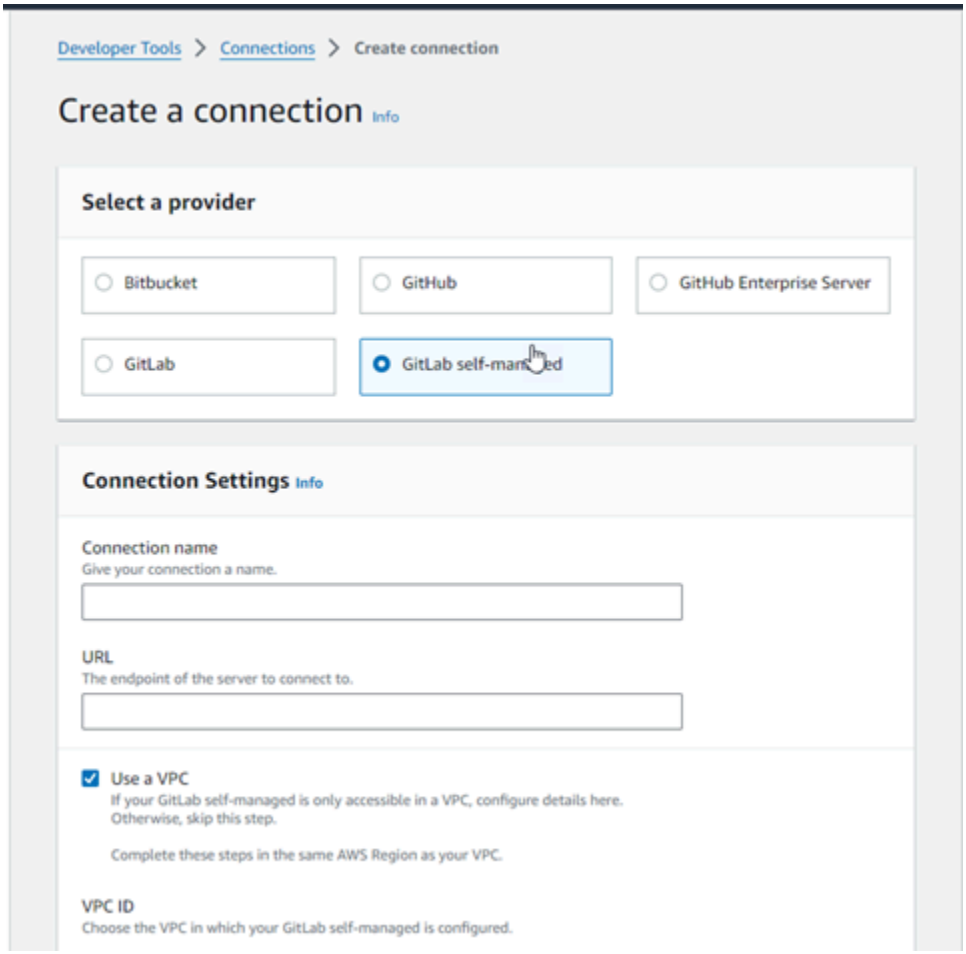


3. Dopo che l'host è stato registrato correttamente, viene visualizzata la pagina dei dettagli dell'host che mostra che lo stato dell'host è Available (Disponibile).



Fase 3: Creazione della connessione

1. Accedi a AWS Management Console, quindi apri la console AWS Developer Tools all'indirizzohttps://console.aws.amazon.com/codesuite/settings/connections.
2. Scegli Impostazioni, quindi seleziona Connessioni. Scegli Crea connessione.
3. Per creare una connessione a un GitLab repository, in Seleziona un provider, scegli Gestione GitLab automatica. In Connection name (Nome connessione), immetti il nome della connessione che desideri creare.



4. In URL, immetti l'endpoint per il server.
5. Se hai lanciato il tuo server in un VPC Amazon e vuoi connetterti con il tuo VPC, scegli Use a VPC (Utilizzo di un VPC) e completa quanto segue.

   a. In VPC ID (ID VPC), seleziona l'ID VPC. Assicurati di scegliere il VPC per l'infrastruttura in cui è installato l'host o un VPC con accesso all'host tramite VPN o Direct Connect.

   b. In Subnet ID (ID sottorete), scegliere Add (Aggiungi). Nel campo, selezionare l'ID della sottorete che si desidera utilizzare per l'host. È possibile scegliere fino a 10 sottoreti.

Assicurati di scegliere la sottorete per l'infrastruttura in cui è installato l'host o una sottorete con accesso all'host installato tramite VPN o Direct Connect.

c. Nel gruppo di sicurezza IDs, scegli Aggiungi. Nel campo, selezionare il gruppo di sicurezza che si desidera utilizzare per l'host. È possibile creare fino a 10 gruppi di sicurezza.

   Assicurati di scegliere il gruppo di sicurezza per l'infrastruttura in cui è installato l'host o un gruppo di sicurezza con accesso all'host installato tramite VPN o Direct Connect.

d. Se disponi di un VPC privato configurato, e l'host è stato configurato per eseguire la convalida TLS utilizzando un'autorità di certificazione non pubblica, inserisci l'ID del certificato in Certificato TLS. Il valore del Certificato TLS deve essere la chiave pubblica del certificato.

6. Scegli Connect to GitLab self-managed. La connessione creata viene mostrata con uno stato Pending (In attesa). Viene creata una risorsa host per la connessione con le informazioni sul server fornite. Per il nome dell'host, viene utilizzato l'URL.
7. Scegli Update pending connection (Aggiornare la connessione in attesa).
8. Quando viene GitLab visualizzata la pagina di accesso, accedi con le tue credenziali, quindi scegli Accedi.
9. Viene visualizzata una pagina di autorizzazione con un messaggio che richiede l'autorizzazione per la connessione per accedere al tuo account. GitLab

   Seleziona Authorize (Autorizza).
10. Il browser torna alla pagina della console delle connessioni. In Crea GitLab connessione, la nuova connessione viene mostrata in Nome connessione.
11. Scegli Connect to GitLab self-managed.

    Dopo che la connessione è stata creata correttamente, viene visualizzato un banner di operazione riuscita. I dettagli della connessione vengono visualizzato nella pagina Impostazioni di connessione.

Crea una connessione a GitLab gestione automatica (CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per creare un host e una connessione per GitLab la gestione automatica.

Per farlo, utilizza i comandi create-host e create-connection.

> **Important**
>
> Per impostazione predefinita, una connessione creata tramite AWS CLI o AWS CloudFormation è in `PENDING` stato. Dopo aver creato una connessione con la CLI o AWS CloudFormation, utilizza la console per modificare la connessione e definirne lo stato. `AVAILABLE`

Fase 1: Creare un host per la GitLab gestione automatica (CLI)

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzate il AWS CLI per eseguire il create-host comando, specificando e `--provider-endpoint` per la `--name` connessione. `--provider-type` In questo esempio, il nome del provider di terze parti è `GitLabSelfManaged` e l'endpoint è `my-instance.dev`.

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

   In caso di esito positivo, questo comando restituisce informazioni dell'Amazon Resource Name (ARN) dell'host simili alle seguenti.

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

   Dopo questo passaggio, l'host è nello stato `PENDING`.

2. Usa la console per completare la configurazione dell'host e sposta l'host nello stato `Available` nella seguente fase.

Fase 2: Configurazione di un host in attesa nella console

1. Accedi AWS Management Console e apri la console Developer Tools all'indirizzohttps://console.aws.amazon.com/codesuite/settings/connections.
2. Utilizza la console per completare la configurazione dell'host e sposta l'host nello stato `Available`. Consultare Impostare un host in attesa.

Fase 3: Creare una connessione per la GitLab gestione automatica (CLI)

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Usa il AWS CLI per eseguire il create-connection comando, specificando l'`--host-arn` e `--connection-name` per la tua connessione.

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

   In caso di esito positivo, questo comando restituisce informazioni dell'ARN della connessione simili alle seguenti.

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

2. Usa la console per configurare la connessione in attesa nella seguente fase.

Passaggio 4: Per completare una connessione per la GitLab gestione automatica nella console

1. Accedi AWS Management Console e apri la console Developer Tools all'indirizzohttps://console.aws.amazon.com/codesuite/settings/connections.
2. Usa la console per configurare la connessione in sospeso e passarla in uno stato `Available`. Per ulteriori informazioni, consulta Aggiornare una connessione in attesa.

Aggiornare una connessione in attesa

Una connessione creata tramite AWS Command Line Interface (AWS CLI) o AWS CloudFormation è in `PENDING` stato per impostazione predefinita. Dopo aver creato una connessione con AWS CLI o AWS CloudFormation, utilizza la console per aggiornare la connessione e definirne lo stato`AVAILABLE`.

> **Note**
>
> È necessario utilizzare la console per aggiornare una connessione in attesa. Non è possibile aggiornare una connessione in attesa utilizzando la AWS CLI.

La prima volta che usi la console per aggiungere una nuova connessione a un provider di terze parti, devi completare l' OAuth handshake con il provider terzo utilizzando l'installazione associata alla connessione.

È possibile utilizzare la console Strumenti di sviluppo per completare una connessione in sospeso.

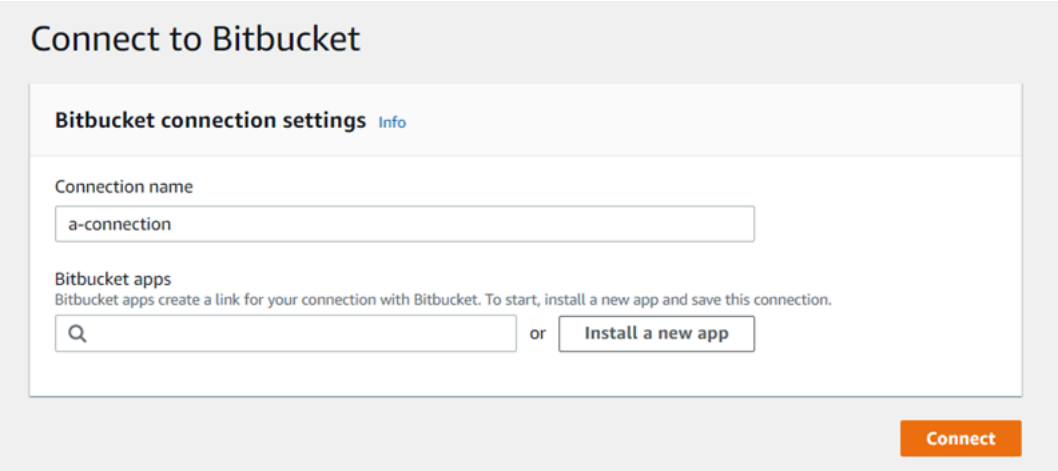
Per completare una connessione

1. Apri la console AWS Developer Tools all'indirizzohttps://console.aws.amazon.com/codesuite/settings/connections.
2. Scegli Settings > Connections (Impostazioni > Connessioni).

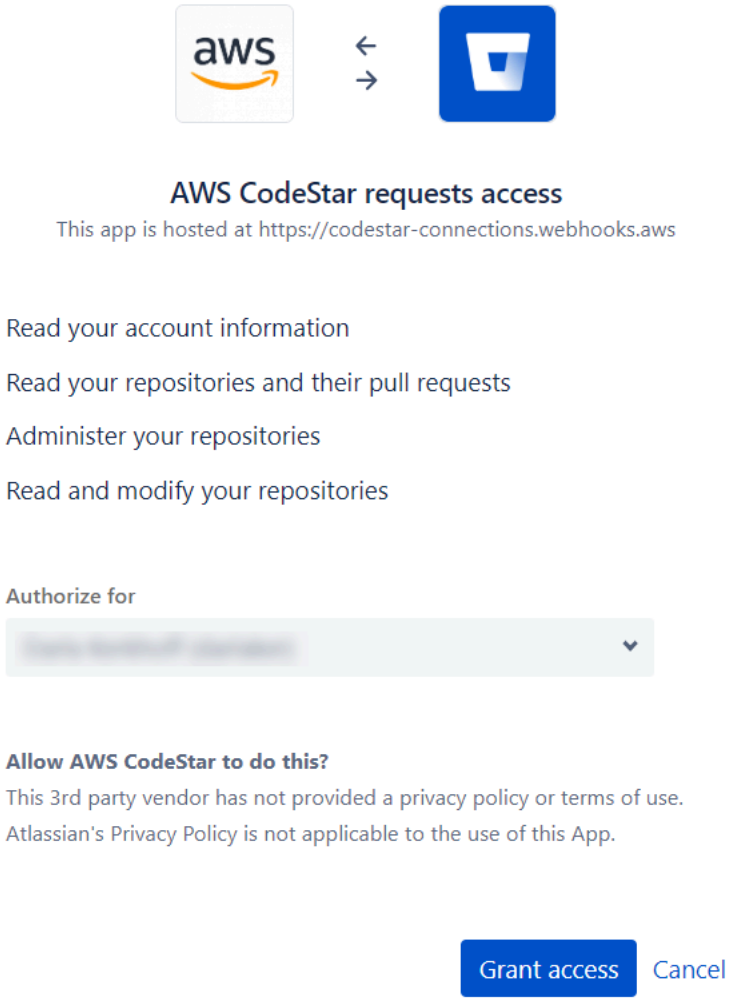
   Vengono visualizzati i nomi di tutte le connessioni associate all' AWS account.
3. In Name (Nome), scegliere il nome della connessione in sospeso che si desidera aggiornare.

   Update a pending connection (Aggiorna una connessione in attesa) è attivata quando si sceglie una connessione con stato Pending (In attesa).
4. Scegliere Update a pending connection (Aggiornare la connessione in attesa).
5. Nella pagina Connect to Bitbucket (Connetti a Bitbucket) in Connection name (Nome connessione), verificare il nome della connessione.

   In Bitbucket apps (App Bitbucket), selezionare l'installazione di un'app o Install a new app (Installa una nuova app) per crearne una.



6. Nella pagina di installazione dell'app, un messaggio indica che l' AWS CodeStar app sta tentando di connettersi al tuo account Bitbucket. Selezionare Grant access (Concedi accesso).



7. Viene visualizzato l'ID di connessione per la nuova installazione. Selezionare Complete connection (Completa connessione).

Elenco delle connessioni

È possibile utilizzare la console di Strumenti per sviluppatori o il comando list-connections nell' AWS Command Line Interface (AWS CLI) per visualizzare un elenco di connessioni nel proprio account.

Elenco delle connessioni (console)

Per elencare le connessioni

1. Apri la console Strumenti di sviluppo all'indirizzo https://console.aws.amazon.com/codesuite/settings/connections.
2. Scegli Settings > Connections (Impostazioni > Connessioni).

3. Visualizzare il nome, lo stato e l'ARN per le connessioni.

Elenco delle connessioni (CLI)

È possibile utilizzare il AWS CLI per elencare le connessioni a repository di codice di terze parti. Per una connessione associata a una risorsa host, ad esempio le connessioni a GitHub Enterprise Server, l'output restituisce inoltre l'ARN dell'host.

Per farlo, utilizzare il comando list-connections.

Per elencare le connessioni

- Aprire un terminale (Linux, macOS o Unix) o un prompt dei comandi (Windows) e AWS CLI utilizzarlo per eseguire il comando. list-connections

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

Questo comando restituisce il seguente output.

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

Elimina connessione

È possibile utilizzare la console Strumenti di sviluppo o il comando delete-connection in AWS Command Line Interface (AWS CLI) per eliminare una connessione.

Argomenti

- Eliminazione di una connessione (console)
- Eliminazione di una connessione (CLI)

Eliminazione di una connessione (console)

Per eliminare una connessione

1. Apri la console Strumenti di sviluppo all'indirizzo https://console.aws.amazon.com/codesuite/settings/connections.
2. Scegli Settings > Connections (Impostazioni > Connessioni).
3. In Connection name (Nome connessione), scegliere il nome della connessione che si desidera eliminare.
4. Scegliere Delete (Elimina).
5. Digitare **`delete`** nel campo per confermare e quindi scegliere Delete (Elimina).

> **Important**
>
> Questa operazione non può essere annullata.

Eliminazione di una connessione (CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per eliminare una connessione.

Per farlo, utilizzare il comando delete-connection.

> **Important**
>
> Dopo aver eseguito il comando, la connessione viene eliminata. Non viene visualizzata alcuna finestra di dialogo di conferma. È possibile creare una nuova connessione, ma l'Amazon Resource Name (ARN) non viene mai riutilizzato.

Per eliminare una connessione

- Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzare il AWS CLI per eseguire il delete-connection comando, specificando l'ARN della connessione che si desidera eliminare.

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

  Questo comando non restituisce alcun risultato.

Tagging di risorse di connessione

Un tag è un'etichetta di attributo personalizzata che l'utente o AWS assegna a una AWS risorsa. Ogni AWS tag è composto da due parti:

- Una chiave del tag (ad esempio, `CostCenter`, `Environment` o `Project`). Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.
- Un campo facoltativo noto come valore del tag (ad esempio, `111122223333`, `Production` o un nome di team). Non specificare il valore del tag equivale a utilizzare una stringa vuota. Analogamente alle chiavi dei tag, i valori dei tag prevedono una distinzione tra lettere maiuscole e minuscole.

Tutti questi sono noti come coppie chiave-valore.

È possibile utilizzare la console o l'interfaccia a riga di comando per aggiungere tag alle risorse.

Puoi taggare i seguenti tipi di risorse in AWS CodeConnections:

- Connessioni
- Host

Questi passaggi presuppongono che tu abbia già installato una versione recente di AWS CLI o aggiornata alla versione corrente. Per ulteriori informazioni, consulta Installazione dell' AWS CLI nella Guida per l'utente dell'AWS Command Line Interface .

Oltre a identificare, organizzare e tracciare la risorsa con i tag, puoi utilizzare i tag nelle policy AWS Identity and Access Management (IAM) per controllare chi può visualizzare e interagire con la tua

risorsa. Per esempi di policy di accesso basate su tag, consulta Utilizzo dei tag per controllare l'accesso alle risorse AWS CodeConnections .

Argomenti

- Assegnazione di tag alle risorse (console)
- Risorse tag (CLI)

Assegnazione di tag alle risorse (console)

È possibile utilizzare la console per aggiungere, aggiornare o rimuovere i tag in una risorsa di connessione.

Argomenti

- Aggiunta dei tag a una risorsa di connessione (console)
- Visualizzazione dei tag per una risorsa di connessione (console)
- Modifica dei tag per una risorsa di connessione (console)
- Rimozione dei tag da una risorsa di connessione (console)

Aggiunta dei tag a una risorsa di connessione (console)

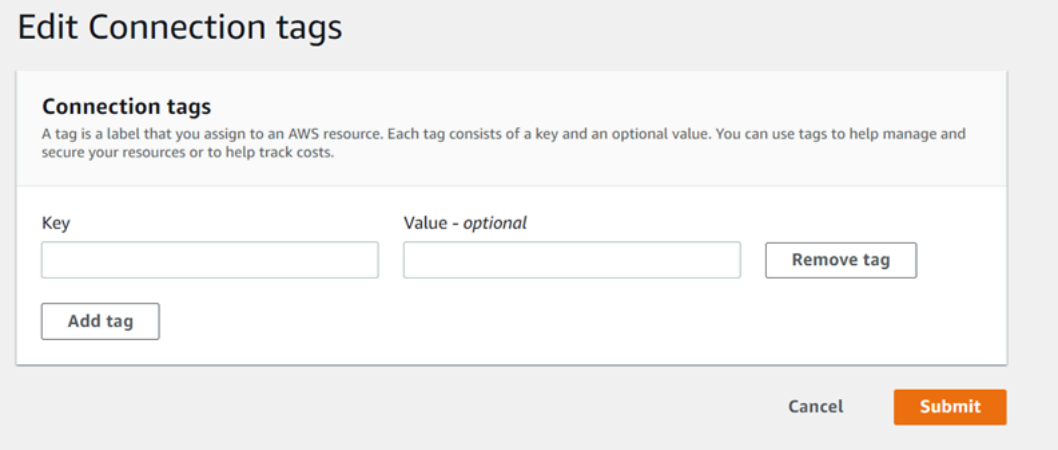
È possibile utilizzare la console per aggiungere i tag a una connessione o un host esistente.

> **Note**
>
> Quando create una connessione per un provider installato come GitHub Enterprise Server e viene creata anche una risorsa host per voi, i tag durante la creazione vengono aggiunti solo alla connessione. Ciò consente di taggare un host separatamente se si desidera riutilizzarlo per una nuova connessione. Se desideri aggiungere tag all'host, segui la procedura descritta di seguito.

Per aggiungere tag per una connessione

1. Accedere alla console. Nel riquadro di navigazione scegliere Impostazioni.
2. In Settings (Impostazioni), scegliere Connections (Connessioni). Scegliere la scheda Connessioni.

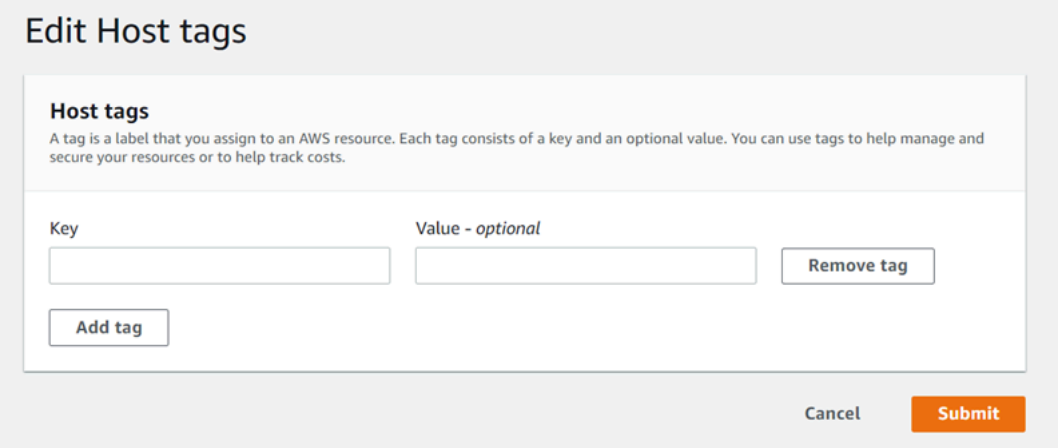
3. Scegliere la connessione da modificare. Viene visualizzata la pagina Impostazioni connessione.
4. In Connection tags (Tag di connessione), scegliere Edit (Modifica). Viene visualizzata la pagina Edit Connection tags (Modifica dei tag di connessione).
5. Nei campi Key (Chiave) e Value (Valore), immettere una coppia di chiavi per ogni set di tag che si desidera aggiungere. Il campo Value (Valore) è facoltativo. Ad esempio, in Key (Chiave), immettere **`Project`**. In Valore, immetti **`ProjectA`**.



6. (Facoltativo) Scegliere Add tag (Aggiungi tag) per aggiungere ulteriori righe e inserire più tag.
7. Scegli Invia. I tag sono elencati nelle impostazioni della connessione.

Per aggiungere tag per un host

1. Accedere alla console. Nel riquadro di navigazione scegliere Impostazioni.
2. In Settings (Impostazioni), scegliere Connections (Connessioni). Seleziona la scheda Hosts (Host).
3. Scegli l'host che desideri modificare. Viene visualizzata la pagina Host settings (Impostazioni host).
4. In Host tags (Tag host), scegliere Edit (Modifica). Viene visualizzata la pagina Host tags (Tag host).
5. Nei campi Key (Chiave) e Value (Valore), immettere una coppia di chiavi per ogni set di tag che si desidera aggiungere. Il campo Value (Valore) è facoltativo. Ad esempio, in Key (Chiave), immettere **`Project`**. In Valore, immetti **`ProjectA`**.



6. (Facoltativo) Scegli Add tag (Aggiungi tag) per aggiungere ulteriori righe e inserisci più tag per un host.
7. Scegli Invia. I tag sono elencati nelle impostazioni dell'host.

Visualizzazione dei tag per una risorsa di connessione (console)

È possibile utilizzare la console per visualizzare i tag delle risorse esistenti.

Per visualizzare i tag per una connessione

1. Accedere alla console. Nel riquadro di navigazione scegliere Impostazioni.
2. In Settings (Impostazioni), scegliere Connections (Connessioni). Scegliere la scheda Connessioni.
3. Scegliere la connessione da visualizzare. Viene visualizzata la pagina Impostazioni connessione.
4. In Connection tags (Tag connessioni), visualizzare i tag per la connessione nelle colonne Key (Chiave) e Value (Valore).

Per visualizzare i tag per un host

1. Accedere alla console. Nel riquadro di navigazione scegliere Impostazioni.
2. In Settings (Impostazioni), scegliere Connections (Connessioni). Seleziona la scheda Hosts (Host).
3. Scegliere l'host che si desidera visualizzare.
4. In Host tags (Tag host), visualizzare i tag per l'host nelle colonne Key (Chiave) e Value (Valore).

Modifica dei tag per una risorsa di connessione (console)

È possibile utilizzare la console per modificare i tag che sono stati aggiunti alle risorse di connessione.

Per modificare i tag per una connessione

1. Accedere alla console. Nel riquadro di navigazione scegliere Impostazioni.
2. In Settings (Impostazioni), scegliere Connections (Connessioni). Scegliere la scheda Connessioni.
3. Scegliere la connessione da modificare. Viene visualizzata la pagina Impostazioni connessione.
4. In Connection tags (Tag di connessione), scegliere Edit (Modifica). Viene visualizzata la pagina Connection tags (Tag di connessione).
5. Nei campi Key (Chiave) e Value (Valore), aggiornare i valori di ogni campo in base alle esigenze. Ad esempio, per la chiave **`Project`**, in Value (Valore), modificare **`ProjectA`** in **`ProjectB`**.
6. Scegli Invia.

Per modificare i tag per un host

1. Accedere alla console. Nel riquadro di navigazione scegliere Impostazioni.
2. In Settings (Impostazioni), scegliere Connections (Connessioni). Seleziona la scheda Hosts (Host).
3. Scegli l'host che desideri modificare. Viene visualizzata la pagina Host settings (Impostazioni host).
4. In Host tags (Tag host), scegliere Edit (Modifica). Viene visualizzata la pagina Host tags (Tag host).
5. Nei campi Key (Chiave) e Value (Valore), aggiornare i valori di ogni campo in base alle esigenze. Ad esempio, per la chiave **`Project`**, in Value (Valore), modificare **`ProjectA`** in **`ProjectB`**.
6. Scegli Invia.

Rimozione dei tag da una risorsa di connessione (console)

Puoi utilizzare la console per rimuovere i tag dalle risorse di connessione. Quando rimuovi i tag dalla risorsa associata, questi vengono eliminati.

Per rimuovere i tag per una connessione

1. Accedere alla console. Nel riquadro di navigazione scegliere Impostazioni.
2. In Settings (Impostazioni), scegliere Connections (Connessioni). Scegliere la scheda Connessioni.
3. Scegliere la connessione da modificare. Viene visualizzata la pagina Impostazioni connessione.
4. In Connection tags (Tag di connessione), scegliere Edit (Modifica). Viene visualizzata la pagina Connection tags (Tag di connessione).
5. Accanto alla chiave e al valori di ciascun tag che desideri eliminare, scegli Remove tag (Rimuovi tag).
6. Scegli Invia.

Per rimuovere i tag per un host

1. Accedere alla console. Nel riquadro di navigazione scegliere Impostazioni.
2. In Settings (Impostazioni), scegliere Connections (Connessioni). Seleziona la scheda Hosts (Host).
3. Scegli l'host che desideri modificare. Viene visualizzata la pagina Host settings (Impostazioni host).
4. In Host tags (Tag host), scegliere Edit (Modifica). Viene visualizzata la pagina Host tags (Tag host).
5. Accanto alla chiave e al valori di ciascun tag che desideri eliminare, scegli Remove tag (Rimuovi tag).
6. Scegli Invia.

Risorse tag (CLI)

È possibile utilizzare la CLI per visualizzare, aggiungere, aggiornare o rimuovere i tag in una risorsa di connessione.

Argomenti

- Aggiunta dei tag a una risorsa di connessione (CLI)
- Visualizzazione dei tag per una risorsa di connessione (CLI)
- Modifica dei tag per una risorsa di connessione (CLI)
- Rimozione dei tag da una risorsa di connessione (CLI)

Aggiunta dei tag a una risorsa di connessione (CLI)

È possibile utilizzare il AWS CLI per etichettare le risorse nelle connessioni.

Al terminale o alla riga di comando, eseguire il comando tag-resource, specificando l'Amazon Resource Name (ARN) della risorsa in cui aggiungere i tag e la chiave e il valore del tag che si desidera aggiungere. È possibile aggiungere più di un tag.

Per aggiungere tag per una connessione

1. Ottenere l'ARN per la risorsa. Utilizzare il comando list-connections mostrato in Elenco delle connessioni per ottenere la connessione ARN.
2. In un terminale o nella riga di comando, eseguire il comando tag-resource.

   Ad esempio, utilizzate il comando seguente per etichettare una connessione con due tag, una chiave di tag denominata *Project* con il valore del tag di *ProjectA* e una chiave di tag denominata *ReadOnly* con il valore del tag di*true*.

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

   In caso di successo, questo comando non restituisce alcun risultato.

Per aggiungere tag per un host

1. Ottenere l'ARN per la risorsa. Utilizzare il comando list-hosts mostrato in Elenca gli host per ottenere l'ARN dell'host.
2. In un terminale o nella riga di comando, eseguire il comando tag-resource.

   Ad esempio, utilizzate il comando seguente per etichettare un host con due tag, una chiave di tag denominata *Project* con il valore del tag di *ProjectA* e una chiave di tag denominata *IscontainerBased* con il valore del tag di*true*.

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

   In caso di successo, questo comando non restituisce alcun risultato.

Visualizzazione dei tag per una risorsa di connessione (CLI)

È possibile utilizzare il AWS CLI per visualizzare i AWS tag per una risorsa di connessioni. Se non sono stati aggiunti tag, l'elenco restituito è vuoto. Utilizzare il comando list-tags-for-resource per visualizzare i tag che sono stati aggiunti a una connessione o a un host.

Per visualizzare i tag per una connessione

1. Ottenere l'ARN per la risorsa. Utilizzare il comando list-connections mostrato in Elenco delle connessioni per ottenere la connessione ARN.
2. In un terminale o nella riga di comando, eseguire il comando list-tags-for-resource. Ad esempio, utilizzare il comando seguente per visualizzare un elenco di chiavi di tag e valori di tag per una connessione.

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

   Questo comando restituisce i tag associati alla risorsa. In questo esempio vengono illustrate due coppie chiave-valore restituite per una connessione.

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

Per visualizzare i tag per un host

1. Ottenere l'ARN per la risorsa. Utilizzare il comando list-hosts mostrato in Elenca gli host per ottenere l'ARN dell'host.

2. In un terminale o nella riga di comando, eseguire il comando list-tags-for-resource. Ad esempio, utilizzare il comando seguente per visualizzare un elenco di chiavi di tag e valori di tag per un host.

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

Questo comando restituisce i tag associati alla risorsa. Questo esempio mostra due coppie chiave-valore restituite per un host.

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

Modifica dei tag per una risorsa di connessione (CLI)

È possibile utilizzare il AWS CLI per modificare un tag per una risorsa. È possibile modificare il valore di una chiave esistente o aggiungere un'altra chiave.

Al terminale o nella riga di comando, eseguire il comando tag-resource specificando l'ARN (Amazon Resource Name) della risorsa in cui si desidera aggiornare un tag e specificare la chiave e il valore di tag da aggiornare.

Quando si modificano i tag, tutte le chiavi di tag non specificate verranno mantenute, mentre qualsiasi elemento con la stessa chiave ma un nuovo valore verrà aggiornato. Le nuove chiavi aggiunte con il comando modifica vengono aggiunte come una nuova coppia chiave-valore.

Per modificare i tag per una connessione

1. Ottenere l'ARN per la risorsa. Utilizzare il comando list-connections mostrato in Elenco delle connessioni per ottenere la connessione ARN.

2. In un terminale o nella riga di comando, eseguire il comando tag-resource.

   In questo esempio, il valore della chiave `Project` viene modificato in `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
   ```

   In caso di successo, questo comando non restituisce alcun risultato. Per verificare i tag associati alla connessione, esegui il comando list-tags-for-resource.

Per modificare i tag per un host

1. Ottenere l'ARN per la risorsa. Utilizzare il comando list-hosts mostrato in Elenca gli host per ottenere l'ARN dell'host.
2. In un terminale o nella riga di comando, eseguire il comando tag-resource.

   In questo esempio, il valore della chiave `Project` viene modificato in `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
   ```

   In caso di successo, questo comando non restituisce alcun risultato. Per verificare i tag associati all'host, esegui il comando list-tags-for-resource.

Rimozione dei tag da una risorsa di connessione (CLI)

Segui questi passaggi per utilizzare AWS CLI per rimuovere un tag da una risorsa. Quando rimuovi i tag dalla risorsa associata, questi vengono eliminati.

> **Note**
>
> Se si elimina una risorsa di connessione, tutte le associazioni di tag vengono rimosse dalla risorsa eliminata. Non è necessario rimuovere i tag prima di eliminare una risorsa di connessione.

Al terminale o nella riga di comando, eseguire il comando untag-resource specificando l'ARN della risorsa in cui si desidera rimuovere i tag e la chiave del tag che si desidera rimuovere. Ad esempio, per rimuovere più tag su una connessione con le chiavi dei tag *Project* e*ReadOnly*, usa il seguente 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
```

In caso di successo, questo comando non restituisce alcun risultato. Per verificare i tag associati alla risorsa, eseguire il comando list-tags-for-resource. L'output mostra che tutti i tag sono stati rimossi.

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

Visualizza i dettagli di connessione

È possibile utilizzare la console Strumenti di sviluppo o il comando get-connection in AWS Command Line Interface (AWS CLI) per vedere i dettagli per una connessione. Per utilizzare AWS CLI, è necessario aver già installato una versione recente AWS CLI o aggiornata alla versione corrente. Per ulteriori informazioni, consulta Installazione dell' AWS CLI nella Guida per l'utente dell'AWS Command Line Interface .

Per visualizzare una connessione (console)

1. Apri la console Strumenti di sviluppo all'indirizzo https://console.aws.amazon.com/codesuite/settings/connections.
2. Scegli Settings > Connections (Impostazioni > Connessioni).
3. Seleziona il pulsante accanto alla connessione che desideri visualizzare, quindi seleziona View details (Visualizza i dettagli).
4. Per la connessione vengono visualizzate le seguenti informazioni:

   - Il nome della connessione.
   - Il tipo di provider per la connessione.
   - Lo stato della connessione.
   - La connessione ARN.

- Se la connessione è stata creata per un provider installato, ad esempio GitHub Enterprise Server, le informazioni sull'host associate alla connessione.
- Se la connessione è stata creata per un provider installato, ad esempio GitHub Enterprise Server, le informazioni sull'endpoint associate all'host per la connessione.

5. Se la connessione è nello stato Pending (In attesa), per completare la connessione, scegli Update pending connection (Aggiorna connessione in attesa). Per ulteriori informazioni, consulta Update a pending connection (Aggiornare una connessione in attesa).

Per visualizzare una connessione (CLI)

- Dal terminale o dalla riga di comando, esegui il comando get-connection. Ad esempio, utilizza il comando seguente per visualizzare i dettagli per una connessione con il valore ARN `arn:aws:codestar-connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f`.

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

Se viene eseguito correttamente, il comando restituisce i dettagli delle connessioni.

Esempio di output per una connessione Bitbucket:

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

Esempio di output per una GitHub connessione:

```
{
    "Connection": {
        "ConnectionName": "MyGitHubConnection",
```

```
        "ConnectionArn": "arn:aws:codeconnections:us-west-2:account_id:connection/
ebcd4a13-EXAMPLE",
        "ProviderType": "GitHub",
        "OwnerAccountId": "account_id",
        "ConnectionStatus": "AVAILABLE"
    }
}
```

Esempio di output per una connessione GitHub Enterprise Server:

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

Condividi le connessioni con Account AWS

È possibile utilizzare la condivisione delle risorse con AWS RAM per condividere una connessione esistente con un altro utente Account AWS o con gli account della propria organizzazione. È possibile utilizzare la connessione condivisa AWS con le risorse gestite per connessioni di origine di terze parti, ad esempio in CodePipeline.

> **Important**
>
> La condivisione della connessione non è supportata per `codestar-connections` le risorse. Questa funzionalità è supportata solo per `codeconnections` le risorse.

Prima di iniziare:

- Devi aver già creato una connessione con il tuo Account AWS.

- È necessario che la condivisione delle risorse sia abilitata.

> **Note**
>
> Per condividere la connessione, devi essere il proprietario dell'organizzazione o il proprietario del repository se non fai parte di un'organizzazione. L'account con cui stai condividendo avrà bisogno anche delle autorizzazioni per accedere al repository.

Argomenti

- Condividi una connessione (console)
- Condivisione di una connessione (CLI)
- Visualizza connessioni condivise (console)
- Visualizza connessioni condivise (CLI)

Condividi una connessione (console)

È possibile utilizzare la console per creare risorse di connessione condivise.

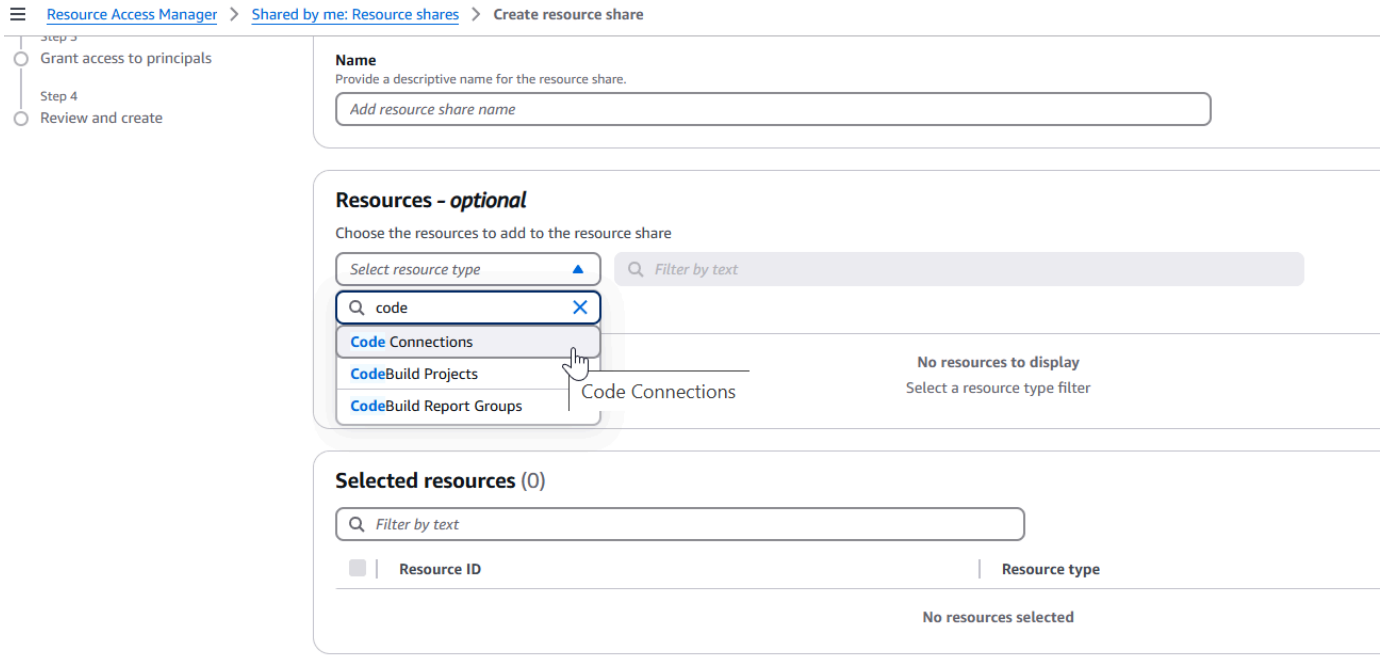
1. Accedi alla AWS Management Console.

   Scegli Crea condivisione di risorse nella pagina Condivise da me: Risorse condivise della AWS RAM console.

2. Poiché le condivisioni di AWS RAM risorse esistono in regioni AWS specifiche, scegli la regione AWS appropriata dall'elenco a discesa nell'angolo in alto a destra della console. Per creare condivisioni di risorse che contengano risorse globali, devi impostare la regione AWS su Stati Uniti orientali (Virginia settentrionale),

   Per ulteriori informazioni sulla condivisione di risorse globali, consulta Condivisione delle risorse regionali rispetto alle risorse globali.

3. Nella pagina di creazione, in Nome, inserisci un nome per la condivisione di risorse. In Risorse, scegli Code Connections.



4. Scegli la tua risorsa di connessione e assegna i principali con cui desideri condividerla.
5. Scegli Create (Crea).

Condivisione di una connessione (CLI)

Puoi usare AWS Command Line Interface (AWS CLI) per condividere una connessione esistente con altri account e visualizzare le connessioni che possiedi o che hai condiviso con te.

Per fare ciò, usa i `accept-resource-share-invitation` comandi create-resource-share and for AWS RAM.

Per condividere una connessione

1. Accedi con l'account che condividerà la connessione.
2. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Usa il AWS CLI per eseguire il create-resource-share comando, specificando la `--name` e `--principals` per la condivisione della connessione. `--resource-arns` In questo esempio, il nome è `my-shared-resource` e il nome della connessione specificato si trova `MyConnection` nella risorsa ARN. In`principals`, fornisci l'account o gli account di destinazione con cui stai condividendo.

```
aws ram create-resource-share --name my-shared-resource --resource-
arns connection_ARN --principals destination_account
```

In caso di esito positivo, questo comando restituisce informazioni dell'ARN della connessione simili alle seguenti.

```
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-west-2:111111111111:resource-
share/4476c27d-8feb-4b21-afe9-7de23EXAMPLE",
        "name": "MyNewResourceShare",
        "owningAccountId": "111111111111",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": 1634586271.302,
        "lastUpdatedTime": 1634586271.302
    }
}
```

3. Le richieste di condivisione possono essere accettate come descritto nella procedura successiva.

Per autenticare e accettare la connessione, condividi con l'account di destinazione

La procedura seguente è facoltativa per gli account di destinazione che appartengono alla stessa organizzazione e per i quali è abilitata la condivisione delle risorse in Organizations.

1. Accedi con l'account di destinazione che riceverà l'invito.
2. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Usa il AWS CLI per eseguire il get-resource-share-invitations comando.

```
aws ram get-resource-share-invitations
```

Acquisisci l'ARN di invito alla condivisione delle risorse per il passaggio successivo.

3. Esegui il accept-resource-share-invitation comando, specificando il. `--resource-share-invitation-arn`

```
aws ram accept-resource-share-invitation --resource-share-invitation-
arn invitation_ARN
```

In caso di successo, questo comando restituisce il seguente risultato.

```
{
```

```
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-west-2:111111111111:resource-
share-invitation/1e3477be-4a95-46b4-bbe0-c4001EXAMPLE",
        "resourceShareName": "MyResourceShare",
        "resourceShareArn": "arn:aws:ram:us-west-2:111111111111:resource-
share/27d09b4b-5e12-41d1-a4f2-19dedEXAMPLE",
        "senderAccountId": "111111111111",
        "receiverAccountId": "222222222222",
        "invitationTimestamp": "2021-09-22T15:07:35.620000-07:00",
        "status": "ACCEPTED"
    }
}
```

Visualizza connessioni condivise (console)

È possibile utilizzare la console per visualizzare le risorse di connessione condivise.

1. Accedi alla AWS Management Console.

   Apri la pagina Shared by me: Shared resources nella console RAM AWS.

2. Poiché le condivisioni di risorse RAM AWS esistono in regioni AWS specifiche, scegli la regione AWS appropriata dall'elenco a discesa nell'angolo in alto a destra della console. Per visualizzare le condivisioni di risorse che contengono risorse globali, devi impostare la regione AWS su Stati Uniti orientali (Virginia settentrionale),

   Per ulteriori informazioni sulla condivisione di risorse globali, consulta Condivisione delle risorse regionali rispetto alle risorse globali.

3. Per ogni risorsa condivisa, sono disponibili le seguenti informazioni:

   - ID risorsa: l'ID della risorsa. Scegliete l'ID di una risorsa per aprire una nuova scheda del browser e visualizzare la risorsa nella sua console di servizio nativa.
   - Tipo di risorsa: il tipo di risorsa.
   - Data ultima condivisione: la data in cui la risorsa è stata condivisa l'ultima volta.
   - Condivisioni di risorse: il numero di condivisioni di risorse che includono la risorsa. Per visualizzare l'elenco delle condivisioni di risorse, scegli il numero.
   - Responsabili: il numero di responsabili che possono accedere alla risorsa. Scegli il valore per visualizzare i principali.

Visualizza connessioni condivise (CLI)

Puoi utilizzarlo AWS CLI per visualizzare le connessioni che possiedi o che hai condiviso con te.

Per farlo, utilizzare il comando get-resource-shares.

Per visualizzare le connessioni condivise

- Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzare il AWS CLI per eseguire il get-resource-shares comando.

  ```
  aws ram get-resource-shares
  ```

  L'output restituisce un elenco di risorse condivise per il tuo account.

Utilizzo degli host

Per creare una connessione a un tipo di provider installato, ad esempio GitHub Enterprise Server, è innanzitutto necessario creare un host utilizzando il AWS Management Console. Un host è una risorsa creata per rappresentare l'infrastruttura in cui è installato il provider. Quindi si crea una connessione utilizzando tale host. Per ulteriori informazioni, consulta Utilizzo delle connessioni.

Ad esempio, si crea un host per la connessione in modo che l'app di terze parti per il provider possa essere registrata per rappresentare l'infrastruttura. Si crea un host per un tipo di provider, e tutte le connessioni a tale tipo di provider utilizzeranno tale host.

Quando si utilizza la console per creare una connessione a un tipo di provider installato, ad esempio GitHub Enterprise Server, la console crea la risorsa host per l'utente.

Argomenti

- Creare di un host
- Impostare un host in attesa
- Elenca gli host
- Modificare un host
- Eliminare un host
- Visualizzare i dettagli dell'host

Creare di un host

Puoi usare AWS Management Console o the AWS Command Line Interface (AWS CLI) per creare una connessione a un repository di codice di terze parti installato sulla tua infrastruttura. Ad esempio, potresti avere GitHub Enterprise Server in esecuzione come macchina virtuale su un' EC2istanza Amazon. Prima di creare una connessione a GitHub Enterprise Server, crei un host da utilizzare per la connessione.

Per una panoramica del flusso di lavoro di creazione di un host per i provider installati, consulta Flusso di lavoro per la creazione o l'aggiornamento di un host.

Prima di iniziare:

- (Facoltativo) Se desideri creare l'host con un VPC, devi aver già creato una rete o un cloud privato virtuale (VPC).
- Devi aver già creato l'istanza e, se prevedi di connetterti con il VPC, aver avviato l'host nel VPC.

> **Note**
>
> Ogni VPC può essere associato solo a un host alla volta.

Facoltativamente, puoi configurare l'host con un VPC. Per ulteriori informazioni sulla configurazione di rete e del VPC per la risorsa host consulta i prerequisiti VPC in (Facoltativo) Prerequisiti: configurazione di rete o Amazon VPC per la connessione e Risoluzione dei problemi di configurazione VPC per l'host.

Per utilizzare la console per creare un host e una connessione a GitHub Enterprise Server, vedereCrea la tua connessione GitHub Enterprise Server (console). La console crea il tuo host.

Per utilizzare la console per creare un host e una connessione a GitLab gestione automatica, vedereCrea una connessione a gestione automatica GitLab. La console crea il tuo host.

(Facoltativo) Prerequisiti: configurazione di rete o Amazon VPC per la connessione

Se l'infrastruttura è configurata con una connessione di rete, è possibile ignorare questa sezione.

Se l'host è accessibile solo in un VPC, prima di continuare, attieniti ai requisiti VPC.

Requisiti VPC

Puoi scegliere facoltativamente di creare l'host con un VPC. Di seguito sono riportati i requisiti VPC generali, a seconda del VPC configurato per l'installazione.

- È possibile configurare un VPC pubblico con sottoreti pubbliche e private. È possibile utilizzare il VPC predefinito per l' Account AWS se non sono presenti sottoreti o blocchi CIDR preferiti.
- Se hai configurato un VPC privato e hai configurato l'istanza di GitHub Enterprise Server per eseguire la convalida TLS utilizzando un'autorità di certificazione non pubblica, devi fornire il certificato TLS per la risorsa host.
- Quando connections crea il tuo host, l'endpoint VPC (PrivateLink) per i webhook viene creato automaticamente. Per ulteriori informazioni, consulta AWS CodeConnections e endpoint VPC di interfaccia ()AWS PrivateLink.
- Configurazione del gruppo di sicurezza:
  - I gruppi di sicurezza utilizzati durante la creazione dell'host necessitano di regole in entrata e in uscita che consentano all'interfaccia di rete di connettersi all'istanza di Enterprise Server GitHub
  - I gruppi di sicurezza collegati all'istanza di GitHub Enterprise Server (che non fanno parte della configurazione dell'host) richiedono l'accesso in entrata e in uscita dalle interfacce di rete create dalle connessioni.
- Le sottoreti VPC devono risiedere in diverse zone di disponibilità della regione. Le zone di disponibilità sono sedi isolate dai guasti che si verificano in altre zone di disponibilità. Ogni sottorete deve risiedere totalmente all'interno di una zona di disponibilità e non può estendersi in altre zone.

Per ulteriori informazioni sull'utilizzo delle sottoreti VPCs e delle sottoreti, consulta VPC and Subnet Sizing nella Amazon VPC User IPv4 Guide.

Informazioni VPC fornite per la configurazione dell'host

Quando si crea la risorsa host per le connessioni nella fase successiva, è necessario fornire quanto segue:

- ID VPC: l'ID del VPC per il server su cui è installata l'istanza di GitHub Enterprise Server o un VPC che ha accesso all'istanza di GitHub Enterprise Server installata tramite VPN o Direct Connect.
- ID di sottorete o IDs: l'ID della sottorete per il server su cui è installata l'istanza di GitHub Enterprise Server o una sottorete con accesso all'istanza di GitHub Enterprise Server installata tramite VPN o Direct Connect.

- Gruppo o gruppi di sicurezza: il gruppo di sicurezza per il server su cui è installata l'istanza di GitHub Enterprise Server o un gruppo di sicurezza con accesso all'istanza di GitHub Enterprise Server installata tramite VPN o Direct Connect.
- Endpoint: avere l'endpoint del server pronto e continuare con la fase successiva.

Per ulteriori informazioni, inclusa la risoluzione dei problemi di connessione VPC o host, consulta Risoluzione dei problemi di configurazione VPC per l'host.

Requisiti per l'autorizzazione

Come parte del processo di creazione dell'host, AWS CodeConnections crea risorse di rete per conto dell'utente per facilitare la connettività VPC. Ciò include un'interfaccia di rete AWS CodeConnections per interrogare i dati dall'host e un endpoint VPC o PrivateLinkper l'host per inviare i dati degli eventi tramite webhook alle connessioni. Per poter creare queste risorse di rete, è necessario assicurarsi che l'utente IAM che crea l'host disponga delle seguenti autorizzazioni:

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

Per ulteriori informazioni sulle autorizzazioni per la risoluzione dei problemi o la connessione host in un VPC, consulta Risoluzione dei problemi di configurazione VPC per l'host.

Per ulteriori informazioni sul webhook endpoint VPC, consulta AWS CodeConnections e endpoint VPC di interfaccia ()AWS PrivateLink.

Argomenti

- Creare un host per una connessione (console)
- Creazione di un host per una connessione (CLI)

Creare un host per una connessione (console)

Per le connessioni per le installazioni, ad esempio con GitHub Enterprise Server o con GitLab gestione automatica, si utilizza un host per rappresentare l'endpoint dell'infrastruttura in cui è installato il provider di terze parti.

> **Note**
>
> A partire dal 1° luglio 2024, la console crea connessioni con `codeconnections` la risorsa ARN. Le risorse con entrambi i prefissi di servizio continueranno a essere visualizzate nella console.

Per informazioni sulle considerazioni relative alla configurazione di un host in un VPC, consulta Crea una connessione a gestione automatica GitLab.

Per utilizzare la console per creare un host e una connessione a GitHub Enterprise Server, vedere. Crea la tua connessione GitHub Enterprise Server (console) La console crea il tuo host.

Per utilizzare la console per creare un host e una connessione a GitLab gestione automatica, vedereCrea una connessione a gestione automatica GitLab. La console crea il tuo host.

> **Note**
>
> È possibile creare un host solo una volta per GitHub Enterprise Server o account GitLab autogestito. Tutte le connessioni a uno specifico GitHub Enterprise Server o a un account GitLab autogestito utilizzeranno lo stesso host.

Creazione di un host per una connessione (CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per creare un host per le connessioni installate.

> **Note**
>
> È possibile creare un host solo una volta per account GitHub Enterprise Server. Tutte le connessioni a un account GitHub Enterprise Server specifico utilizzeranno lo stesso host.

È possibile utilizzare un host per rappresentare l'endpoint per l'infrastruttura in cui è installato il provider di terze parti. Per creare un host con la CLI, utilizza il comando create-host. Dopo aver completato la creazione dell'host, l'host si trova nello stato Pending (In attesa). Allora si può Configurare l'host per spostarlo nello stato Available (Disponibile). Quando l'host sarà disponibile, completa i passaggi per creare una connessione.

> **Important**
>
> Per impostazione predefinita, un host creato tramite il AWS CLI è attivo. `Pending` Dopo aver creato un host con la CLI, utilizza la console per configurare l'host e impostarne lo stato `Available`.

Per utilizzare la console per creare un host e una connessione a GitHub Enterprise Server, vedereCrea la tua connessione GitHub Enterprise Server (console). La console crea il tuo host.

Per utilizzare la console per creare un host e una connessione a GitLab gestione automatica, vedereCrea una connessione a gestione automatica GitLab. La console crea il tuo host.

Impostare un host in attesa

Un host creato tramite AWS Command Line Interface (AWS CLI) o SDK è in `Pending` stato per impostazione predefinita. Dopo aver creato una connessione con la console o l'SDK, utilizza la console per configurare l'host e impostarne lo stato. AWS CLI`Available`

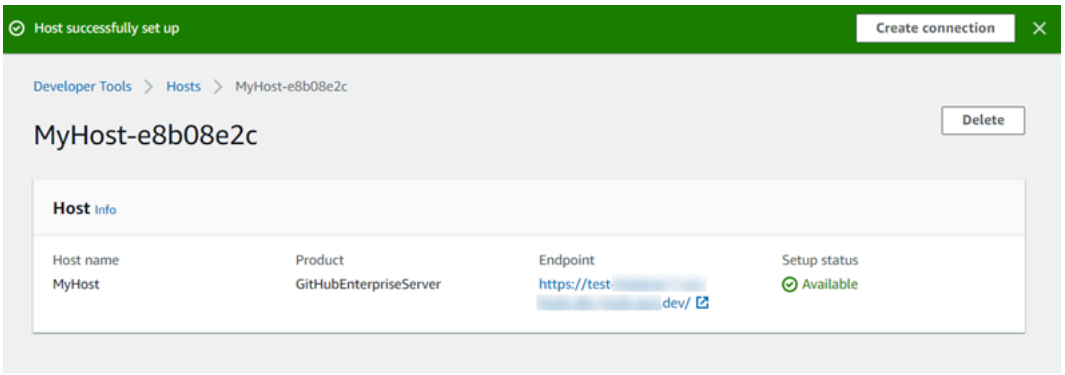
È necessario avere già creato un host. Per ulteriori informazioni, consulta la sezione Creazione di un host.

Per impostare un host in attesa

Una volta creato, l'host si trova nello stato Pending (In attesa). Per spostare l'host da Pending (In attesa) a Available (Disponibile), completa questi passaggi. Questo processo esegue una stretta di mano con il provider terzo per registrare l'app di AWS connessione sull'host.

1. Dopo che l'host ha raggiunto lo stato In sospeso nella console AWS Developer Tools, scegli Configura host.
2. Se stai creando un host per la GitLab gestione automatica, viene visualizzata una pagina di configurazione. In Fornisci un token di accesso personale, fornisci GitLab al tuo PAT solo la seguente autorizzazione riportata di seguito: api.

3. Nella pagina di accesso del provider installato da terze parti, ad esempio la pagina di accesso di GitHub Enterprise Server, accedi con le credenziali del tuo account, se richiesto.
4. Nella pagina di installazione dell'app, in Nome GitHub app, inserisci un nome per l'app che desideri installare per il tuo host. Scegli Crea GitHub app.
5. Dopo che l'host è stato registrato correttamente, viene visualizzata la pagina dei dettagli dell'host che mostra che lo stato dell'host è Available (Disponibile).



6. È possibile continuare con la creazione della connessione una volta che l'host è disponibile. Nel banner che indica l'esito positivo, scegli Create connection (Crea connessione). Completa i passaggi descritti in Creazione di una connessione.

Elenca gli host

È possibile utilizzare la console di Strumenti per sviluppatori o il comando list-connections nell' AWS Command Line Interface (AWS CLI) per visualizzare un elenco di connessioni nel proprio account.

Elenca gli host (console)

Per elencare gli host

1. Apri la console Strumenti di sviluppo all'indirizzo https://console.aws.amazon.com/codesuite/settings/connections.
2. Seleziona la scheda Hosts (Host). Visualizza il nome, lo stato e l'ARN per gli host.

Elenca gli host (CLI)

Puoi utilizzarlo AWS CLI per elencare gli host per le connessioni installate con provider di terze parti.

Per farlo, utilizzare il comando list-hosts.

Per elencare gli host

- Aprire un terminale (Linux, macOS o Unix) o un prompt dei comandi (Windows) e AWS CLI utilizzarlo per eseguire il comando. list-hosts

```
aws codeconnections list-hosts
```

Questo comando restituisce il seguente output.

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

Modificare un host

È possibile modificare le impostazioni dell'host per un host nello stato `Pending`. È possibile modificare il nome host, l'URL o la configurazione VPC.

Non è possibile utilizzare lo stesso URL per più di un host.

> **Note**
>
> Per informazioni sulle considerazioni relative alla configurazione di un host in un VPC, consulta (Facoltativo) Prerequisiti: configurazione di rete o Amazon VPC per la connessione.

Per modificare un host

1. Apri la console Strumenti di sviluppo all'indirizzo https://console.aws.amazon.com/codesuite/settings/connections.
2. Scegli Settings > Connections (Impostazioni > Connessioni).

3. Seleziona la scheda Hosts (Host).

   Vengono visualizzati gli host associati al tuo AWS account e creati nella AWS regione selezionata.
4. Per modificare il nome host, immetti un nuovo valore in Nome.
5. Per modificare il l'endpoint dell'host immetti un nuovo valore in URL.
6. Per modificare la configurazione VPC host, immetti nuovi valori in ID VPC.
7. Scegli Edit host (Modifica host).
8. Vengono visualizzate le impostazioni aggiornate. Scegli Set up Pending host (Imposta host in attesa).

Eliminare un host

È possibile utilizzare la console Strumenti di sviluppo o il comando delete-host in AWS Command Line Interface (AWS CLI) per eliminare un host.

Argomenti

- Eliminare un host (console)
- Eliminare un host (CLI)

Eliminare un host (console)

Per eliminare un host

1. Apri la console Strumenti di sviluppo all'indirizzo https://console.aws.amazon.com/codesuite/settings/connections.
2. Seleziona la scheda Hosts (Host). In Name (Nome), scegli il nome dell'host da eliminare.
3. Scegli Elimina.
4. Digitare **`delete`** nel campo per confermare e quindi scegliere Delete (Elimina).

> **Important**
>
> Questa operazione non può essere annullata.

Eliminare un host (CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per eliminare un host.

Per farlo, utilizzare il comando delete-host.

> **Important**
>
> Per eliminare un host, è necessario eliminare tutte le connessioni associate all'host.
> Dopo aver eseguito il comando, l'host viene eliminato. Non viene visualizzata alcuna finestra di dialogo di conferma.

Per eliminare un host

- Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Usa AWS CLI per eseguire il delete-host comando, specificando l'Amazon Resource Name (ARN) dell'host che desideri eliminare.

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

  Questo comando non restituisce alcun risultato.

Visualizzare i dettagli dell'host

È possibile utilizzare la console Strumenti di sviluppo o il comando get-host in AWS Command Line Interface (AWS CLI) per visualizzare i dettagli dell'host.

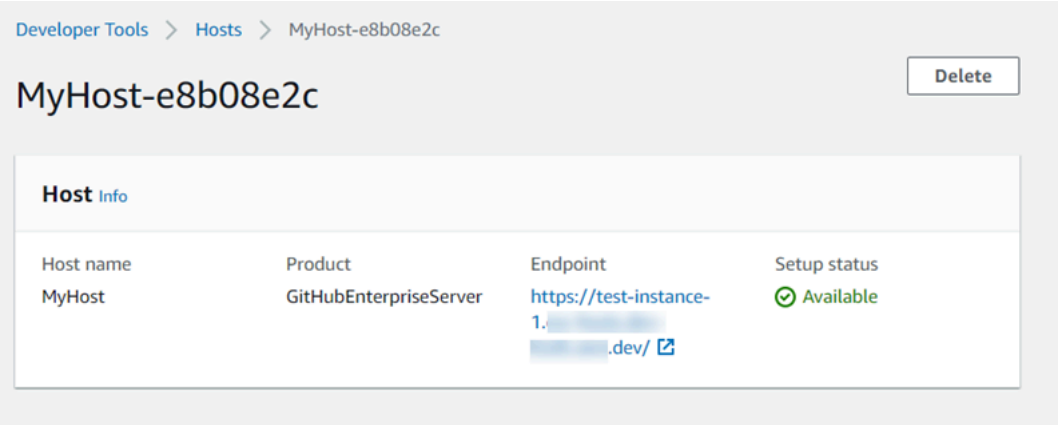
Per visualizzare i dettagli dell'host (console)

1. Accedi alla AWS Management Console e apri la console Strumenti di sviluppo all'indirizzo https://console.aws.amazon.com/codesuite/settings/connections.
2. Scegli Settings > Connections (Impostazioni > Connessioni), quindi seleziona la scheda Hosts (Host).
3. Seleziona il pulsante accanto all'host che desideri visualizzare, quindi seleziona View details (Visualizza i dettagli).
4. Vengono visualizzate le seguenti informazioni per l'host:

- Il nome host.
- Il tipo di provider per la connessione.
- L'endpoint dell'infrastruttura in cui è installato il provider.
- Lo stato di configurazione per l'host. Un host pronto per una connessione è nello stato Available (Disponibile). Se l'host è stato creato ma l'installazione non è stata completata, l'host potrebbe trovarsi in uno stato diverso.

  Sono disponibili i seguenti stati:

  - IN ATTESA - L'host ha completato la creazione ed è pronto per avviare la configurazione registrando l'app provider sull'host.
  - DISPONIBILE - L'host ha completato la creazione e la configurazione ed è disponibile per l'utilizzo con le connessioni.
  - ERRORE - Si è verificato un errore durante la creazione o la registrazione dell'host.
  - VPC_CONFIG_VPC_INIZIALIZZAZIONE - Viene creata la configurazione VPC per l'host.
  - VPC_CONFIG_VPC_INIZIALIZZAZIONE_FALLITA - La configurazione VPC per l'host ha rilevato e errore e non è riuscita.
  - VPC_CONFIG_VPC_DISPONIBILE - La configurazione VPC per l'host ha completato l'installazione ed è disponibile.
  - VPC_CONFIG_VPC_ELIMINAZIONE - Viene eliminata la configurazione VPC per l'host.



5. Per eliminare l'host, scegli Delete (Elimina).
6. Se l'host è nello stato Pending (In attesa), per completare la configurazione, scegli Set up host (Configura host). Per ulteriori informazioni, consulta Set up a pending host (Impostare un host in attesa).

Per visualizzare i dettagli dell'host (CLI)

- Apri un terminale (Linux, macOS o Unix) o un prompt dei comandi (Windows) e usalo AWS CLI per eseguire il get-host comando, specificando l'Amazon Resource Name (ARN) dell'host di cui desideri visualizzare i dettagli.

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

  Questo comando restituisce il seguente output.

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

Utilizzo delle configurazioni di sincronizzazione per i repository collegati

In AWS CodeConnections, utilizzi una connessione per associare AWS risorse a un repository di terze parti, ad esempio Bitbucket Cloud GitHub, GitHub Enterprise Server e. GitLab Utilizzando il tipo di `CFN_STACK_SYNC` sincronizzazione, è possibile creare una configurazione di sincronizzazione, che consente di AWS sincronizzare il contenuto da un repository Git per aggiornare una AWS risorsa specificata. AWS CloudFormation si integra con le connessioni in modo da poter utilizzare Git sync per gestire i file di modelli e parametri in un repository collegato con cui eseguire la sincronizzazione.

Dopo aver creato una connessione, puoi utilizzare la CLI delle connessioni o la AWS CloudFormation console per creare il collegamento al repository e sincronizzare la configurazione.

- Collegamento al repository: attraverso un collegamento al repository associ la tua connessione a un repository Git esterno. Il collegamento al repository consente alla sincronizzazione Git di monitorare e sincronizzare le modifiche ai file in un repository Git specificato.
- Configurazione di sincronizzazione: usa la configurazione di sincronizzazione per sincronizzare il contenuto da un repository Git per aggiornare una AWS risorsa specificata.

Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS CodeConnections .

Per un tutorial che illustra come creare una configurazione di sincronizzazione per uno AWS CloudFormation stack utilizzando la AWS CloudFormation console, consulta Lavorare con AWS CloudFormation Git sync nella Guida per l'CloudFormation utente.

Argomenti

- Utilizzo dei collegamenti al repository
- Utilizzo delle configurazioni di sincronizzazione

Utilizzo dei collegamenti al repository

Attraverso un collegamento al repository puoi associare la tua connessione a un repository Git esterno. Il collegamento al repository consente a Git sync di monitorare e sincronizzare le modifiche ai file in un repository Git specificato con uno AWS CloudFormation stack.

Per ulteriori informazioni sui collegamenti ai repository, consulta il riferimento alle API.AWS CodeConnections

Argomenti

- Creazione di un collegamento di repository
- Aggiornare il collegamento a un repository
- Elencare i collegamenti al repository
- Eliminare il collegamento a un repository
- Visualizzare i dettagli di un collegamento a un repository

Creazione di un collegamento di repository

È possibile utilizzare il create-repository-link comando in AWS Command Line Interface (AWS CLI) per creare un collegamento tra la connessione e il repository esterno con cui effettuare la sincronizzazione.

Prima di poter creare un link al repository, è necessario aver già creato il repository esterno con il provider di terze parti, ad esempio. GitHub

Per creare un collegamento di repository.

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzate il AWS CLI per eseguire il comando. create-repository-link Specifica l'ARN della connessione associata, l'ID del proprietario e il nome del repository.

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

2. Questo comando restituisce il seguente output.

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

Aggiornare il collegamento a un repository

È possibile utilizzare il update-repository-link comando in AWS Command Line Interface (AWS CLI) per aggiornare un collegamento al repository specificato.

È possibile aggiornare le informazioni seguenti per il collegamento al repository:

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

Aggiorna il collegamento a un repository quando desideri modificare la connessione associata al repository. Per utilizzare una connessione diversa, devi specificare l'ARN della connessione. Per i passaggi per visualizzare l'ARN della connessione, consulta Visualizza i dettagli di connessione.

Per aggiornare il collegamento a un repository

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzate il AWS CLI per eseguire il update-repository-link comando, specificando il valore da aggiornare per il link al repository. Ad esempio, il comando seguente aggiorna la connessione associata all'ID del collegamento al repository. Specifica il nuovo ARN di connessione con il parametro `--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. Questo comando restituisce il seguente output.

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

Elencare i collegamenti al repository

Puoi usare il list-repository-links comando in AWS Command Line Interface (AWS CLI) per elencare i link ai repository per il tuo account.

Per elencare i collegamenti al repository

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Usa il AWS CLI per eseguire il list-repository-links comando.

```
aws codeconnections list-repository-links
```

2. Questo comando restituisce il seguente output.

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

Eliminare il collegamento a un repository

È possibile utilizzare il delete-repository-link comando in AWS Command Line Interface (AWS CLI) per eliminare un collegamento al repository.

Per eliminare il collegamento a un repository, è necessario eliminare tutte le configurazioni di sincronizzazione associate a tale collegamento.

> **Important**
>
> Dopo aver eseguito il comando, il collegamento al repository viene eliminato. Non viene visualizzata alcuna finestra di dialogo di conferma. È possibile creare un nuovo collegamento a un repository, ma il nome della risorsa Amazon (ARN) non viene riutilizzato.

Per eliminare il collegamento a un repository

- Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzate il AWS CLI per eseguire il delete-repository-link comando, specificando l'ID del link al repository da eliminare.

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

Questo comando non restituisce alcun risultato.

Visualizzare i dettagli di un collegamento a un repository

È possibile utilizzare il get-repository-link comando in AWS Command Line Interface (AWS CLI) per visualizzare i dettagli su un collegamento al repository.

Per visualizzare i dettagli di un collegamento a un repository

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzate il AWS CLI per eseguire il get-repository-link comando, specificando l'ID del link al repository.

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

2. Questo comando restituisce il seguente output.

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

Utilizzo delle configurazioni di sincronizzazione

Attraverso una configurazione di sincronizzazione viene creata un'associazione tra un repository e una connessione specificati. Usa la configurazione di sincronizzazione per sincronizzare i contenuti di un repository Git e aggiornare una risorsa AWS specifica.

Per ulteriori informazioni sulle connessioni, consulta il riferimento alle AWS CodeConnections API.

Argomenti

- Creazione di una configurazione di sincronizzazione
- Aggiornare una configurazione di sincronizzazione
- Elencare le configurazioni di sincronizzazione
- Eliminare una configurazione di sincronizzazione
- Visualizzare i dettagli di configurazione

Creazione di una configurazione di sincronizzazione

Puoi usare il create-repository-link comando in AWS Command Line Interface (AWS CLI) per creare un collegamento tra la tua connessione e l'archivio esterno con cui sincronizzarti.

Prima di poter creare una configurazione di sincronizzazione, devi aver creato un collegamento al repository tra la connessione e il repository di terze parti.

Per creare una configurazione di sincronizzazione

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzate il AWS CLI per eseguire il create-repository-link comando. Specifica l'ARN della connessione associata, l'ID del proprietario e il nome del repository. Il comando seguente crea una configurazione di sincronizzazione con un tipo di sincronizzazione per una risorsa in AWS CloudFormation. Specifica inoltre il ramo del repository e il file di configurazione nel repository. In questo esempio, la risorsa è uno stack denominato **`mystack`**.

   ```
   aws codeconnections 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. Questo comando restituisce il seguente output.

   ```
   {
   ```

```
    "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"
    }
```

Aggiornare una configurazione di sincronizzazione

Usa il comando update-sync-configuration nella AWS Command Line Interface (AWS CLI) per aggiornare una configurazione di sincronizzazione specificata.

È possibile aggiornare le seguenti informazioni per la configurazione di sincronizzazione:

- `--branch`
- `--config-file`
- `--repository-link-id`
- `--resource-name`
- `--role-arn`

Per aggiornare una configurazione di sincronizzazione

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzate il AWS CLI per eseguire il update-sync-configuration comando, specificando il valore che desiderate aggiornare, insieme al nome della risorsa e al tipo di sincronizzazione. Ad esempio, il comando seguente aggiorna il nome del ramo associato alla configurazione di sincronizzazione con il parametro `--branch`.

   ```
   aws codeconnections update-sync-configuration --sync-type CFN_STACK_SYNC --
   resource-name mystack --branch feature-branch
   ```

2. Questo comando restituisce il seguente output.

   ```
   {
   ```

```
    "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"
    }
```

Elencare le configurazioni di sincronizzazione

Utilizza il comando list-sync-configurations nella AWS Command Line Interface (AWS CLI) per elencare i link ai repository per il tuo account.

Per elencare i collegamenti al repository

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzate il AWS CLI per eseguire il list-sync-configurations comando, specificando il tipo di sincronizzazione e l'ID del link al repository.

```
aws codeconnections list-sync-configurations --repository-link-id
 6053346f-8a33-4edb-9397-10394b695173  --sync-type CFN_STACK_SYNC
```

2. Questo comando restituisce il seguente output.

```
{
    "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"
        }
    ]
```

```
}
```

Eliminare una configurazione di sincronizzazione

Usa il comando delete-sync-configuration nella AWS Command Line Interface (AWS CLI) per eliminare una configurazione di sincronizzazione.

> **Important**
>
> Dopo aver eseguito il comando, la configurazione di sincronizzazione viene eliminata. Non viene visualizzata alcuna finestra di dialogo di conferma. È possibile creare una nuova connessione, ma il nome della risorsa Amazon (ARN) non viene riutilizzato.

Per eliminare una configurazione di sincronizzazione

- Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzate il AWS CLI per eseguire il delete-sync-configuration comando, specificando il tipo di sincronizzazione e il nome della risorsa per la configurazione di sincronizzazione che desiderate eliminare.

  ```
  aws codeconnections delete-sync-configuration --sync-type CFN_STACK_SYNC --
  resource-name mystack
  ```

  Questo comando non restituisce alcun risultato.

Visualizzare i dettagli di configurazione

È possibile utilizzare il get-sync-configuration comando in AWS Command Line Interface (AWS CLI) per visualizzare i dettagli di una configurazione di sincronizzazione.

Per visualizzare i dettagli di una connessione di configurazione

1. Apri un terminale (Linux, macOS o Unix) o prompt dei comandi (Windows). Utilizzate il AWS CLI per eseguire il get-sync-configuration comando, specificando l'ID del link al repository.

   ```
   aws codeconnections get-sync-configuration --sync-type CFN_STACK_SYNC --resource-
   name mystack
   ```

2. Questo comando restituisce il seguente output.

```
{
    "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"
    }
}
```

Registrazione delle chiamate AWS CodeConnections API con AWS CloudTrail

AWS CodeConnections è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio. CloudTrail acquisisce tutte le chiamate API per le notifiche come eventi. Le chiamate acquisite includono le chiamate dalla console Strumenti per sviluppatori e le chiamate di codice alle operazioni delle API AWS CodeConnections .

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon Simple Storage Service (Amazon S3), inclusi gli eventi per le notifiche. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviata AWS CodeConnections, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli.

Per ulteriori informazioni, consulta la AWS CloudTrail Guida per l'utente di .

AWS CodeConnections informazioni in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in AWS CodeConnections, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con cronologia degli CloudTrail eventi nella Guida AWS CloudTrail per l'utente.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per AWS CodeConnections, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail

Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente di AWS CloudTrail :

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni
- Ricezione di file di CloudTrail registro da più account

Tutte AWS CodeConnections le azioni vengono registrate CloudTrail e documentate nel riferimento AWS CodeConnections API. Ad esempio, le chiamate a `DeleteConnection` e `CreateConnection` le `GetConnection` azioni generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali IAM o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle voci dei file di log di

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

`CreateConnection` Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`CreateConnection`azione.


```
{
    "EventId": "b4374fde-c544-4d43-b511-7d899568e55a",
    "EventName": "CreateConnection",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-09T15:13:46-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:user/Mary_Major",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-09T23:03:08Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-09T23:13:46Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "CreateConnection",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.create-connection",
        "requestParameters": {
```

```
            "providerType": "GitHub",
            "connectionName": "my-connection"
        },
        "responseElements": {
            "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/df03df74-8e05-45cf-b420-b39e389dd264"
        },
        "requestID": "57640a88-97b7-481d-9665-cfd79a681379",
        "eventID": "b4374fde-c544-4d43-b511-7d899568e55a",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

CreateHost Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`CreateHost`azione.

```
{
    "EventId": "af4ce349-9f21-43fb-8003-267fbf9b1a93",
    "EventName": "CreateHost",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-11T12:43:06-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
```

```
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T20:43:06Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "CreateHost",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "52.94.133.137",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.create-host",
        "requestParameters": {
            "name": "Demo1",
            "providerType": "GitHubEnterpriseServer",
            "providerEndpoint": "IP"
        },
        "responseElements": {
            "hostArn": "arn:aws:codeconnections:us-east-1:123456789012:host/Demo1-
EXAMPLE"
        },
        "requestID": "974459b3-8a04-4cff-9c8f-0c88647831cc",
        "eventID": "af4ce349-9f21-43fb-8003-267fbf9b1a93",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

CreateSyncConfiguration Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`CreateSyncConfiguration`azione.


```
{
    "EventId": "be1397e1-eefb-49f0-b4ee-2708c45e94e7",
    "EventName": "CreateSyncConfiguration",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T17:38:30+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T17:34:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-24T17:38:30Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "CreateSyncConfiguration",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
```

```
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/offcommand/
codeconnections.create-sync-configuration",
        "requestParameters": {
            "branch": "master",
            "configFile": "filename",
            "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "resourceName": "mystack",
            "roleArn": "arn:aws:iam::123456789012:role/my-role",
            "syncType": "CFN_STACK_SYNC"
        },
        "responseElements": {
            "syncConfiguration": {
                "branch": "main",
                "configFile": "filename",
                "ownerId": "owner_ID",
                "providerType": "GitHub",
                "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                "repositoryName": "MyGitHubRepo",
                "resourceName": "mystack",
                "roleArn": "arn:aws:iam::123456789012:role/my-role",
                "syncType": "CFN_STACK_SYNC"
            }
        },
        "requestID": "bad2f662-3f2a-42c0-b638-6115384896f6",
        "eventID": "be1397e1-eefb-49f0-b4ee-2708c45e94e7",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

DeleteConnection Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`DeleteConnection`azione.

```
{
    "EventId": "672837cd-f977-4fe2-95c7-14280b2af76c",
```

```
    "EventName": "DeleteConnection",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-10T13:00:50-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::001919387613:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-10T20:41:16Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-10T21:00:50Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "DeleteConnection",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.delete-connection",
        "requestParameters": {
            "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/df03df74-8e05-45cf-b420-b39e389dd264"
        },
        "responseElements": null,
        "requestID": "4f26ceab-d665-41df-9e15-5ed0fbb4eca6",
        "eventID": "672837cd-f977-4fe2-95c7-14280b2af76c",
```

```
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

DeleteHost Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`DeleteHost`azione.

```
{
    "EventId": "6018ba5c-6f24-4a30-b201-16ec19a1687a",
    "EventName": "DeleteHost",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-11T12:56:47-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
```

```
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T20:56:47Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "DeleteHost",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.delete-host",
        "requestParameters": {
            "hostArn": "arn:aws:codeconnections:us-east-1:123456789012:host/Demo1-
EXAMPLE"
        },
        "responseElements": null,
        "requestID": "1b244528-143a-4028-b9a4-9479e342bce5",
        "eventID": "6018ba5c-6f24-4a30-b201-16ec19a1687a",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

DeleteSyncConfiguration Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`DeleteSyncConfiguration`azione.

```
{
    "EventId": "588660c7-3202-4998-a906-7bb72bcf4438",
    "EventName": "DeleteSyncConfiguration",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T17:41:59+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
```

```
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T17:34:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-24T17:41:59Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "DeleteSyncConfiguration",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "52.94.133.142",
        "userAgent": "aws-
cli/2.15.11Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/
offcommand/codeconnections.delete-sync-configuration",
        "requestParameters": {
            "syncType": "CFN_STACK_SYNC",
            "resourceName": "mystack"
        },
        "responseElements": null,
        "requestID": "221e0b1c-a50e-4cf0-ab7d-780154e29c94",
        "eventID": "588660c7-3202-4998-a906-7bb72bcf4438",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
```

```
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

GetConnection Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`GetConnection`azione.

```
{
    "EventId": "672837cd-f977-4fe2-95c7-14280b2af76c",
    "EventName": "DeleteConnection",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-10T13:00:50-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-10T20:41:16Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-10T21:00:50Z",
        "eventSource": "codeconnections.amazonaws.com",
```

```
        "eventName": "DeleteConnection",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.delete-connection",
        "requestParameters": {
            "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/df03df74-8e05-45cf-b420-b39e389dd264"
        },
        "responseElements": null,
        "requestID": "4f26ceab-d665-41df-9e15-5ed0fbb4eca6",
        "eventID": "672837cd-f977-4fe2-95c7-14280b2af76c",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "001919387613",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

GetHost Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`GetHost`azione.

```
{
    "EventId": "faa147e7-fe7c-4ab9-a11b-2568a2883c01",
    "EventName": "GetHost",
    "ReadOnly": "true",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-11T12:44:34-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
```

```
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T20:44:34Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "GetHost",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "52.94.133.137",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.get-host",
        "requestParameters": {
            "hostArn": "arn:aws:codeconnections:us-east-1:123456789012:host/Demo1-
EXAMPLE"
        },
        "responseElements": null,
        "requestID": "0ad61bb6-f88f-4f96-92fe-997f017ec2bb",
        "eventID": "faa147e7-fe7c-4ab9-a11b-2568a2883c01",
        "readOnly": true,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

GetRepositoryLink Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`GetRepositoryLink`azione.


```
{
    "EventId": "b46acb67-3612-41c7-8987-adb6c9ed4ad4",
    "EventName": "GetRepositoryLink",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T02:59:28+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T02:58:52Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-24T02:59:28Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "GetRepositoryLink",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
```

```
        "userAgent": "aws-cli/2.15.11
 Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off
 command/codeconnections.get-repository-link",
        "requestParameters": {
            "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173"
        },
        "responseElements": {
            "repositoryLinkInfo": {
                "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/7df263cc-f055-4843-adef-4ceaefcb2167",
                "ownerId": "123456789012",
                "providerType": "GitHub",
                "repositoryLinkArn": "arn:aws:codeconnections:us-
east-1:123456789012:repository-link/6053346f-8a33-4edb-9397-10394b695173",
                "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                "repositoryName": "MyGitHubRepo"
            }
        },
        "requestID": "d46704dd-dbe9-462f-96a6-022a8d319fd1",
        "eventID": "b46acb67-3612-41c7-8987-adb6c9ed4ad4",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-ea-1.codeconnections.aws.dev"
        }
    }
}
```

GetRepositorySyncStatus Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'GetRepositorySyncStatusazione.

```
{
    "EventId": "3e183b74-d8c4-4ad3-9de3-6b5721c522e9",
    "EventName": "GetRepositorySyncStatus",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-25T03:41:44+00:00",
    "EventSource": "codeconnections.amazonaws.com",
```

```
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-25T02:56:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-25T03:41:44Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "GetRepositorySyncStatus",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "52.94.133.138",
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.get-repository-sync-status",
        "errorCode": "ResourceNotFoundException",
        "errorMessage": "Could not find a sync status for repository
 link:6053346f-8a33-4edb-9397-10394b695173",
        "requestParameters": {
            "branch": "feature-branch",
            "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "syncType": "CFN_STACK_SYNC"
        },
        "responseElements": null,
        "requestID": "e0cee3ee-31e8-4ef5-b749-96cdcabbe36f",
        "eventID": "3e183b74-d8c4-4ad3-9de3-6b5721c522e9",
```

```
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

GetResourceSyncStatus Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'GetResourceSyncStatusazione.

```
{
    "EventId": "9c47054e-f6f6-4345-96d0-9a5af3954a8d",
    "EventName": "GetResourceSyncStatus",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-25T03:44:11+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
```

```
                    "creationDate": "2024-01-25T02:56:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-25T03:44:11Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "GetResourceSyncStatus",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.get-resource-sync-status",
        "requestParameters": {
            "resourceName": "mystack",
            "syncType": "CFN_STACK_SYNC"
        },
        "responseElements": null,
        "requestID": "e74b5503-d651-4920-9fd2-0f40fb5681e0",
        "eventID": "9c47054e-f6f6-4345-96d0-9a5af3954a8d",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

`GetSyncBlockerSummary` Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'GetSyncBlockerSummaryazione.

```
{
    "EventId": "c16699ba-a788-476d-8c6c-47511d76309e",
    "EventName": "GetSyncBlockerSummary",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-25T03:03:02+00:00",
    "EventSource": "codeconnections.amazonaws.com",
```

```
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-25T02:56:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-25T03:03:02Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "GetSyncBlockerSummary",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.get-sync-blocker-summary",
        "requestParameters": {
            "syncType": "CFN_STACK_SYNC",
            "resourceName": "mystack"
        },
        "responseElements": {
            "syncBlockerSummary": {
                "resourceName": "mystack",
                "latestBlockers": []
            }
        },
        "requestID": "04240091-eb25-4138-840d-776f8e5375b4",
```

```
        "eventID": "c16699ba-a788-476d-8c6c-47511d76309e",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

GetSyncConfiguration Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'GetSyncConfigurationazione.

```
{
    "EventId": "bab9aa16-4553-4206-a1ea-88219233dd25",
    "EventName": "GetSyncConfiguration",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T17:40:40+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
```

```
                    "creationDate": "2024-01-24T17:34:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-24T17:40:40Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "GetSyncConfiguration",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "52.94.133.142",
        "userAgent": "aws-
cli/2.15.11Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/
offcommand/codeconnections.get-sync-configuration",
        "requestParameters": {
            "syncType": "CFN_STACK_SYNC",
            "resourceName": "mystack"
        },
        "responseElements": {
            "syncConfiguration": {
                "branch": "main",
                "configFile": "filename",
                "ownerId": "123456789012",
                "providerType": "GitHub",
                "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                "repositoryName": "MyGitHubRepo",
                "resourceName": "mystack",
                "roleArn": "arn:aws:iam::123456789012:role/my-role",
                "syncType": "CFN_STACK_SYNC"
            }
        },
        "requestID": "0aa8e43a-6e34-4d8f-89fb-5c2d01964b35",
        "eventID": "bab9aa16-4553-4206-a1ea-88219233dd25",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

ListConnections Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'ListConnectionsazione.


```
{
    "EventId": "3f8d80fe-fbe1-4755-903c-4f58fc8262fa",
    "EventName": "ListConnections",
    "ReadOnly": "true",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-08T14:11:23-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-08T22:11:02Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-08T22:11:23Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "ListConnections",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/1.18.147 Python/2.7.18
 Linux/5.10.201-168.748.amzn2int.x86_64 botocore/1.18.6",
        "requestParameters": {
```

```
            "maxResults": 50
        },
        "responseElements": null,
        "requestID": "5d456d59-3e92-44be-b941-a429df59e90b",
        "eventID": "3f8d80fe-fbe1-4755-903c-4f58fc8262fa",
        "readOnly": true,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

ListHosts Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'ListHostsazione.

```
{
    "EventId": "f6e9e831-feaf-4ad1-ac47-51681109c401",
    "EventName": "ListHosts",
    "ReadOnly": "true",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-11T13:00:55-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
```

```
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T21:00:55Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "ListHosts",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.list-hosts",
        "requestParameters": {
            "maxResults": 50
        },
        "responseElements": null,
        "requestID": "ea87e2cf-6bf1-4cc7-9666-f3fad85d6d83",
        "eventID": "f6e9e831-feaf-4ad1-ac47-51681109c401",
        "readOnly": true,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```


ListRepositoryLinks Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'ListRepositoryLinksazione.


```
{
    "EventId": "4f714bbb-0716-4f6e-9868-9b379b30757f",
    "EventName": "ListRepositoryLinks",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T01:57:29+00:00",
```

```
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T01:43:49Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-24T01:57:29Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "ListRepositoryLinks",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-
cli/2.15.11Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/
offcommand/codeconnections.list-repository-links",
        "requestParameters": {
            "maxResults": 50
        },
        "responseElements": {
            "repositoryLinks": [
                {
                    "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/001f5be2-a661-46a4-b96b-4d277cac8b6e",
                    "ownerId": "123456789012",
                    "providerType": "GitHub",
```

```
                    "repositoryLinkArn": "arn:aws:codeconnections:us-
east-1:123456789012:repository-link/be8f2017-b016-4a77-87b4-608054f70e77",
                    "repositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
                    "repositoryName": "MyGitHubRepo"
                },
                {
                    "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/7df263cc-f055-4843-adef-4ceaefcb2167",
                    "ownerId": "owner",
                    "providerType": "GitHub",
                    "repositoryLinkArn": "arn:aws:codeconnections:us-
east-1:123456789012:repository-link/6053346f-8a33-4edb-9397-10394b695173",
                    "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                    "repositoryName": "MyGitHubRepo"
                }
            ]
        },
        "requestID": "7c8967a9-ec15-42e9-876b-0ef58681ec55",
        "eventID": "4f714bbb-0716-4f6e-9868-9b379b30757f",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```


ListRepositorySyncDefinitions Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'ListRepositorySyncDefinitionsazione.


```
{
    "EventId": "12e52dbb-b00d-49ad-875a-3efec36e5aa1",
    "EventName": "ListRepositorySyncDefinitions",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-25T16:56:19+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
```

```
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-25T16:43:03Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-25T16:56:19Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "ListRepositorySyncDefinitions",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.list-repository-sync-definitions",
        "requestParameters": {
            "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "syncType": "CFN_STACK_SYNC",
            "maxResults": 50
        },
        "responseElements": {
            "repositorySyncDefinitions": []
        },
        "requestID": "df31d11d-5dc7-459b-9a8f-396b4769cdd9",
        "eventID": "12e52dbb-b00d-49ad-875a-3efec36e5aa1",
        "readOnly": false,
        "eventType": "AwsApiCall",
```

```
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
```

ListSyncConfigurations Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'ListSyncConfigurationsazione.

```
{
    "EventId": "aa4ae557-ec31-4151-8d21-9e74dd01344c",
    "EventName": "ListSyncConfigurations",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T17:42:06+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T17:34:55Z",
                    "mfaAuthenticated": "false"
```

```
                }
            }
        },
        "eventTime": "2024-01-24T17:42:06Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "ListSyncConfigurations",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.804.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/offcommand/
codeconnections.list-sync-configurations",
        "requestParameters": {
            "maxResults": 50,
            "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "syncType": "CFN_STACK_SYNC"
        },
        "responseElements": {
            "syncConfigurations": [
                {
                    "branch": "feature-branch",
                    "configFile": "filename.yaml",
                    "ownerId": "owner",
                    "providerType": "GitHub",
                    "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                    "repositoryName": "MyGitHubRepo",
                    "resourceName": "dkstacksync",
                    "roleArn": "arn:aws:iam::123456789012:role/my-role",
                    "syncType": "CFN_STACK_SYNC"
                }
            ]
        },
        "requestID": "7dd220b5-fc0f-4023-aaa0-9555cfe759df",
        "eventID": "aa4ae557-ec31-4151-8d21-9e74dd01344c",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

`ListTagsForResource` Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'ListTagsForResourceazione.


```
{
    "EventId": "fc501054-d68a-4325-824c-0e34062ef040",
    "EventName": "ListTagsForResource",
    "ReadOnly": "true",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-25T17:16:56+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "dMary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-25T16:43:03Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-25T17:16:56Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "ListTagsForResource",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.list-tags-for-resource",
```

```
        "requestParameters": {
            "resourceArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/9703702f-bebe-41b7-8fc4-8e6d2430a330"
        },
        "responseElements": null,
        "requestID": "994584a3-4807-47f2-bb1b-a64f0af6c250",
        "eventID": "fc501054-d68a-4325-824c-0e34062ef040",
        "readOnly": true,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

`TagResource` Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'TagResourceazione.

```
{
    "EventId": "b7fbc943-2dd1-4c5b-a5ad-fc6d60a011f1",
    "EventName": "TagResource",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-11T12:22:11-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T20:22:11Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "TagResource",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.tag-resource",
        "requestParameters": {
            "resourceArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/8dcf69d1-3316-4392-ae09-71e038adb6ed",
            "tags": [
                {
                    "key": "Demo1",
                    "value": "hhvh1"
                }
            ]
        },
        "responseElements": null,
        "requestID": "ba382c33-7124-48c8-a23a-25816ce27604",
        "eventID": "b7fbc943-2dd1-4c5b-a5ad-fc6d60a011f1",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

`UnTagResource` Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'UntagResourceazione.


```
{
    "EventId": "8a85cdee-2586-4679-be18-eec34204bc7e",
    "EventName": "UntagResource",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-11T12:31:14-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T20:31:14Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "UntagResource",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.untag-resource",
        "requestParameters": {
```

```
            "resourceArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/8dcf69d1-3316-4392-ae09-71e038adb6ed",
            "tagKeys": [
                "Project",
                "ReadOnly"
            ]
        },
        "responseElements": null,
        "requestID": "05ef26a4-8c39-4f72-89bf-0c056c51b8d7",
        "eventID": "8a85cdee-2586-4679-be18-eec34204bc7e",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```

UpdateHost Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'UpdateHostazione.

```
"Events": [{
        "EventId": "4307cf7d-6d1c-40d9-a659-1bb41b31a2b6",
        "EventName": "UpdateHost",
        "ReadOnly": "false",
        "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "EventTime": "2024-01-11T12:54:32-08:00",
        "EventSource": "codeconnections.amazonaws.com",
        "Username": "Mary_Major",
        "Resources": [],
        "CloudTrailEvent": "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
```

```
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-11T20:09:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-11T20:54:32Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "UpdateHost",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
 command/codeconnections.update-host",
        "requestParameters": {
            "hostArn": "arn:aws:codeconnections:us-east-1:123456789012:host/
Demo1-34e70ecb",
            "providerEndpoint": "https://54.218.245.167"
        },
        "responseElements": null,
        "requestID": "b17f46ac-1acb-44ab-a9f5-c35c20233441",
        "eventID": "4307cf7d-6d1c-40d9-a659-1bb41b31a2b6",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
```


UpdateRepositoryLink Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'UpdateRepositoryLinkazione.


```
{
    "EventId": "be358c9a-5a8f-467e-8585-2860070be4fe",
```

```
    "EventName": "UpdateRepositoryLink",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T02:03:24+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T01:43:49Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-24T02:03:24Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "UpdateRepositoryLink",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-
cli/2.15.11Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/
offcommand/codeconnections.update-repository-link",
        "requestParameters": {
            "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/7df263cc-f055-4843-adef-4ceaefcb2167",
            "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173"
        },
        "responseElements": {
```

```
            "repositoryLinkInfo": {
                "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/7df263cc-f055-4843-adef-4ceaefcb2167",
                "ownerId": "owner",
                "providerType": "GitHub",
                "repositoryLinkArn": "arn:aws:codeconnections:us-
east-1:123456789012:repository-link/6053346f-8a33-4edb-9397-10394b695173",
                "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                "repositoryName": "MyGitHubRepo"
            }
        },
        "additionalEventData": {
            "providerAction": "UpdateRepositoryLink"
        },
        "requestID": "e01eee49-9393-4983-89e4-d1b3353a70d9",
        "eventID": "be358c9a-5a8f-467e-8585-2860070be4fe",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```


UpdateSyncBlocker Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'UpdateSyncBlockerazione.


```
{
    "EventId": "211d19db-9f71-4d93-bf90-10f9ddefed88",
    "EventName": "UpdateSyncBlocker",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-25T03:01:05+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
```

```
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-25T02:56:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-25T03:01:05Z",
        "eventSource": "codeconnections.amazonaws.com",
        "eventName": "UpdateSyncBlocker",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11 Python/3.11.6
 Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.update-sync-blocker",
        "requestParameters": {
            "id": "ID",
            "syncType": "CFN_STACK_SYNC",
            "resourceName": "mystack",
            "resolvedReason": "Reason"
        },
        "responseElements": null,
        "requestID": "eea03b39-b299-4099-ba55-608480f8d96d",
        "eventID": "211d19db-9f71-4d93-bf90-10f9ddefed88",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
```

```
        }
    }
}
```

UpdateSyncConfiguration Esempio

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'UpdateSyncConfigurationazione.

```
{
    "EventId": "d961c94f-1881-4fe8-83bf-d04cb9f22577",
    "EventName": "UpdateSyncConfiguration",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T17:40:55+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-01-24T17:34:55Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-01-24T17:40:55Z",
        "eventSource": "codeconnections.amazonaws.com",
```

```
        "eventName": "UpdateSyncConfiguration",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "IP",
        "userAgent": "aws-cli/2.15.11
 Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/offcommand/
codeconnections.update-sync-configuration",
        "requestParameters": {
            "branch": "feature-branch",
            "resourceName": "mystack",
            "syncType": "CFN_STACK_SYNC"
        },
        "responseElements": {
            "syncConfiguration": {
                "branch": "feature-branch",
                "configFile": "filename",
                "ownerId": "owner",
                "providerType": "GitHub",
                "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
                "repositoryName": "MyGitHubRepo",
                "resourceName": "mystack",
                "roleArn": "arn:aws:iam::123456789012:role/my-role",
                "syncType": "CFN_STACK_SYNC"
            }
        },
        "requestID": "2ca545ef-4395-4e1f-b14a-2750481161d6",
        "eventID": "d961c94f-1881-4fe8-83bf-d04cb9f22577",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "123456789012",
        "eventCategory": "Management",
        "tlsDetails": {
            "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
        }
    }
}
```


AWS CodeConnections e endpoint VPC di interfaccia ()AWS PrivateLink

Puoi stabilire una connessione privata tra il tuo VPC e creare un AWS CodeConnections endpoint VPC di interfaccia. Gli endpoint di interfaccia sono alimentati da AWS PrivateLink, una tecnologia che consente l'accesso privato AWS CodeConnections APIs senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione AWS Direct Connect. Le istanze del tuo VPC non

necessitano di indirizzi IP pubblici AWS CodeConnections APIs con cui comunicare, perché il traffico tra il tuo VPC AWS CodeConnections e il tuo VPC non esce dalla rete Amazon.

Ogni endpoint dell'interfaccia è rappresentato da una o più interfacce di rete elastiche nelle sottoreti.

Per ulteriori informazioni, consultare Endpoint VPC di interfaccia (AWS PrivateLink) nella Guida per l'utente di Amazon VPC.

Considerazioni sugli endpoint AWS CodeConnections VPC

Prima di configurare un endpoint VPC di interfaccia AWS CodeConnections, assicurati di consultare gli endpoint dell'interfaccia nella Amazon VPC User Guide.

AWS CodeConnections supporta l'esecuzione di chiamate a tutte le sue azioni API dal tuo VPC.

Gli endpoint VPC sono supportati in tutte le regioni. AWS CodeConnections

Concetti di endpoint VPC

Di seguito sono elencati i concetti fondamentali relativi agli endpoint VPC:

Endpoint VPC

Il punto di ingresso nel VPC che consente di connettersi privatamente a un servizio. Di seguito sono riportati i diversi tipi di endpoint VPC. Crea il tipo di endpoint VPC richiesto dal servizio supportato.

- Endpoint VPC per azioni AWS CodeConnections
- Endpoint VPC per webhook AWS CodeConnections

AWS PrivateLink

Una tecnologia che fornisce connettività privata tra e servizi. VPCs

Endpoint VPC per azioni AWS CodeConnections

Puoi gestire gli endpoint VPC per il servizio. AWS CodeConnections

Creazione di endpoint VPC di interfaccia per le azioni AWS CodeConnections

Puoi creare un endpoint VPC per il AWS CodeConnections servizio utilizzando la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta Creazione di un endpoint dell'interfaccia nella Guida per l'utente di Amazon VPC.

Per iniziare a utilizzare le connessioni con il tuo VPC, crea un endpoint VPC di interfaccia per. AWS CodeConnections Quando crei un endpoint VPC per AWS CodeConnections, scegli AWS Servizi e in Nome servizio scegli:

- com.amazonaws. ***region***.codestar-connections.api: questa opzione crea un endpoint VPC per le operazioni API. AWS CodeConnections Ad esempio, scegli questa opzione se gli utenti utilizzano la AWS CLI, l' AWS CodeConnections API o con cui interagire AWS SDKs AWS CodeConnections per operazioni come `CreateConnection`, `ListConnections`, e. `CreateHost`

Per l'opzione Abilita nome DNS, se si seleziona DNS privato per l'endpoint, è possibile effettuare richieste API AWS CodeConnections utilizzando il nome DNS predefinito per la regione, ad esempio. `codestar-connections.us-east-1.amazonaws.com`

> **Important**
>
> Il DNS privato è abilitato per impostazione predefinita per gli endpoint creati per i servizi e AWS i servizi AWS Marketplace Partner.

Per ulteriori informazioni, consulta Accesso a un servizio tramite un endpoint dell'interfaccia in Guida per l'utente di Amazon VPC.

Creazione di una policy degli endpoint VPC per le azioni AWS CodeConnections

È possibile allegare un criterio all'endpoint VPC che controlla l'accesso all' AWS CodeConnections. La policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire operazioni.

Per ulteriori informazioni, consulta Controllo degli accessi ai servizi con endpoint VPC in Guida per l'utente di Amazon VPC.

> **Note**
>
> Il file com.amazonaws. *region* L'endpoint .codestar-connections.webhooks non supporta le politiche.

Esempio: policy degli endpoint VPC per le azioni AWS CodeConnections

Di seguito è riportato un esempio di policy sugli endpoint per. AWS CodeConnections Se associata a un endpoint, questa politica consente l'accesso alle AWS CodeConnections azioni elencate per tutti i principali su tutte le risorse.

```
{
  "Statement": [
    {
      "Sid": "GetConnectionOnly",
      "Principal": "*",
      "Action": [
        "codestar-connections:GetConnection"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Endpoint VPC per webhook AWS CodeConnections

AWS CodeConnections crea endpoint webhook per te quando crei o elimini un host con configurazione VPC. Il nome dell'endpoint è com.amazonaws. ***region***.codestar-connections.webhooks.

Con l'endpoint VPC per GitHub webhook, gli host possono inviare dati sugli eventi tramite webhook ai tuoi servizi integrati sulla rete Amazon. AWS

> **Important**
>
> Quando configuri il tuo host per GitHub Enterprise Server, AWS CodeConnections crea per te un endpoint VPC per i dati degli eventi dei webhook. Se hai creato l'host prima del

24 novembre 2020 e desideri utilizzare gli endpoint PrivateLink webhook VPC, devi prima eliminare l'host e quindi creare un nuovo host.

AWS CodeConnections gestisce il ciclo di vita di questi endpoint. Per eliminare l'endpoint, è necessario eliminare la risorsa host corrispondente.

Come vengono utilizzati gli endpoint webhook per gli host AWS CodeConnections

L'endpoint webhook è il luogo in cui i webhook provenienti da repository di terze parti vengono inviati per l'elaborazione. AWS CodeConnections Un webhook descrive un'azione del cliente. Quando si esegue un `git push`, l'endpoint webhook riceve un webhook dal provider che descrive in dettaglio il push. Ad esempio, AWS CodeConnections puoi notificare CodePipeline l'avvio della pipeline.

Per i provider di servizi cloud, come Bitbucket, o gli host GitHub Enterprise Server che non utilizzano un VPC, l'endpoint VPC webhook non si applica perché i provider inviano webhook a luoghi in cui non viene utilizzata la rete Amazon. AWS CodeConnections

Risoluzione dei problemi relativi alle connessioni

Le seguenti informazioni possono aiutarti a risolvere i problemi più comuni relativi alle connessioni alle risorse in AWS CodeBuild AWS CodeDeploy, e. AWS CodePipeline

Argomenti

- Non riesco a creare connessioni
- Quando cerco di creare o completare una connessione viene visualizzato un errore di autorizzazione
- Viene visualizzato un errore di autorizzazione quando cerco di utilizzare una connessione
- La connessione non è disponibile o non è più in attesa
- Aggiungi le GitClone autorizzazioni per le connessioni
- L'host non è nello stato disponibile
- Risoluzione dei problemi di un host con errori di connessione
- Non riesco a creare una connessione per il mio host
- Risoluzione dei problemi di configurazione VPC per l'host
- Risoluzione dei problemi relativi agli endpoint VPC webhook PrivateLink () GitHub per le connessioni Enterprise Server

- Risoluzione dei problemi per un host creato prima del 24 novembre 2020
- Impossibile creare la connessione per un repository GitHub
- Modifica le autorizzazioni dell'app di connessione GitHub Enterprise Server
- Errore di connessione durante la connessione a GitHub: «Si è verificato un problema, assicurati che i cookie siano abilitati nel tuo browser» o «Il proprietario di un'organizzazione deve installare l' GitHub app»
- Potrebbe essere necessario aggiornare il prefisso del servizio Connections nelle risorse per le politiche IAM
- Errore di autorizzazione dovuto al prefisso del servizio nelle risorse create utilizzando la console
- Configurazione della connessione e dell'host per i provider installati che supportano le organizzazioni
- Desidero aumentare i miei limiti per le connessioni

Non riesco a creare connessioni

Potresti non disporre delle autorizzazioni per creare una connessione. Per ulteriori informazioni, consulta Autorizzazioni ed esempi per AWS CodeConnections.

Quando cerco di creare o completare una connessione viene visualizzato un errore di autorizzazione

Il seguente messaggio di errore potrebbe essere restituito quando si tenta di creare o visualizzare una connessione nella CodePipeline console.

Utente: non *`username`* è autorizzato a eseguire: *`permission`* sulla risorsa: *`connection-ARN`*

Se viene visualizzato questo messaggio, assicurati di disporre di autorizzazioni sufficienti.

Le autorizzazioni per creare e visualizzare le connessioni in AWS Command Line Interface (AWS CLI) o AWS Management Console sono solo una parte delle autorizzazioni necessarie per creare e completare le connessioni sulla console. Le autorizzazioni necessarie per visualizzare, modificare o creare una connessione e quindi completare la connessione in attesa devono essere ridotte per gli utenti che devono eseguire solo determinate attività. Per ulteriori informazioni, consulta Autorizzazioni ed esempi per AWS CodeConnections.

Viene visualizzato un errore di autorizzazione quando cerco di utilizzare una connessione

Uno o entrambi i seguenti messaggi di errore potrebbero essere restituiti se si tenta di utilizzare una connessione nella CodePipeline console, anche se si dispone delle autorizzazioni per elencare, ottenere e creare autorizzazioni.

L'autenticazione dell'account non è riuscita.

Utente: non *`username`* è autorizzato a eseguire: codestar-connections: on resource: UseConnection *`connection-ARN`*

Se si verifica ciò, assicurati di disporre di autorizzazioni sufficienti.

Assicurati di disporre delle autorizzazioni per utilizzare una connessione, incluso l'elenco dei repository disponibili nella posizione del provider. Per ulteriori informazioni, consulta Autorizzazioni ed esempi per AWS CodeConnections.

La connessione non è disponibile o non è più in attesa

Se nella console viene visualizzato un messaggio che indica che una connessione non è disponibile, scegli Complete connection (Completa connessione).

Se scegli di completare la connessione e viene visualizzato un messaggio che indica che la connessione non è in attesa, puoi annullare la richiesta perché la connessione è già disponibile.

Aggiungi le GitClone autorizzazioni per le connessioni

Quando si utilizza una AWS CodeStar connessione in un'azione di origine e in un' CodeBuild azione, ci sono due modi in cui l'artefatto di input può essere passato alla build:

- L'opzione predefinita: l'operazione di origine produce un file zip contenente il codice scaricato da CodeBuild.
- Git clone: il codice sorgente può essere scaricato direttamente nell'ambiente di compilazione.

  La modalità Git clone permette di interagire con il codice sorgente come repository Git funzionante. Per utilizzare questa modalità, è necessario concedere CodeBuild all'ambiente le autorizzazioni per utilizzare la connessione.

Per aggiungere autorizzazioni alla politica relativa al ruolo di CodeBuild servizio, è necessario creare una politica gestita dai clienti da allegare al proprio ruolo di CodeBuild servizio. La procedura

seguente crea una policy in cui l'autorizzazione `UseConnection` è specificata nel campo `action` e l'Amazon Resource Name (ARN) della connessione è specificato nel campo `Resource`.

Per utilizzare la console per aggiungere le UseConnection autorizzazioni

1. Per trovare l'ARN della connessione per la pipeline, scegliere la pipeline e fare clic sull'icona (i) nell'operazione di origine. Si apre il riquadro Configurazione e accanto viene visualizzato l'ARN della connessione. ConnectionArn L'ARN della connessione viene aggiunto alla politica del ruolo CodeBuild di servizio.
2. Per trovare il tuo ruolo di CodeBuild servizio, apri il progetto di build utilizzato nella tua pipeline e vai alla scheda Dettagli della build.
3. Nella sezione Ambiente, scegli il collegamento Service role (Ruolo del servizio). Si apre la console AWS Identity and Access Management (IAM), dove puoi aggiungere una nuova policy che concede l'accesso alla tua connessione.
4. Nella console IAM, scegliere Attach policies (Collega policy), quindi selezionare Create policy (Crea policy).

   Utilizzare il seguente esempio di modello di policy. Aggiungere l'ARN della connessione nel campo `Resource`, come mostrato in questo esempio.

   ```
   {
       "Version": "2012-10-17",
       "Statement": [
           {
               "Effect": "Allow",
               "Action": "codestar-connections:UseConnection",
               "Resource": "insert connection ARN here"
           }
       ]
   }
   ```

   Nella scheda JSON incollare la policy.
5. Scegli Verifica policy. Immettere un nome per la policy (ad esempio **`connection-permissions`**), quindi scegliere Create policy (Crea policy).
6. Tornare alla pagina Attach Permissions (Collega autorizzazioni) del ruolo di servizio, aggiornare l'elenco delle policy e selezionare la policy appena creata. Scegli Collega policy.

L'host non è nello stato disponibile

Se la console visualizza un messaggio che indica che un host non si trova in uno stato `Available`, scegliere Set up host (Configurazione dell'host).

Il primo passo per la creazione dell'host si traduce nell'host creato ora in uno stato `Pending`. Per spostare l'host in uno stato `Available`, è necessario scegliere di configurare l'host nella console. Per ulteriori informazioni, consulta Impostare un host in attesa.

> **Note**
>
> Non è possibile utilizzare la AWS CLI per configurare un `Pending` host.

Risoluzione dei problemi di un host con errori di connessione

Le connessioni e gli host possono passare allo stato di errore se l' GitHub app sottostante viene eliminata o modificata. Gli host e le connessioni nello stato di errore non possono essere recuperati e l'host deve essere ricreato.

- Azioni come la modifica della chiave pem dell'app, la modifica del nome dell'app (dopo la creazione iniziale) causeranno lo stato di errore dell'host e di tutte le connessioni associate.

Se la console o la CLI restituiscono un host o una connessione correlata a un host con uno stato `Error`, potrebbe essere necessario eseguire la seguente procedura:

- Elimina e ricrea la risorsa host, quindi reinstalla l'app di registrazione dell'host. Per ulteriori informazioni, consulta Creare di un host.

Non riesco a creare una connessione per il mio host

Per creare una connessione o un host, sono necessarie le seguenti condizioni.

- L'host deve essere nello stato AVAILABLE (DISPONIBILE). Per ulteriori informazioni, consulta
- Le connessioni devono essere create nella stessa regione dell'host.

Risoluzione dei problemi di configurazione VPC per l'host

Quando si crea una risorsa host, è necessario fornire informazioni sulla connessione di rete o sul VPC per l'infrastruttura in cui è installata l'istanza di GitHub Enterprise Server. Per la risoluzione dei problemi relativi alla configurazione del VPC o della sottorete per l'host, utilizzare come riferimento le informazioni VPC di esempio riportate di seguito.

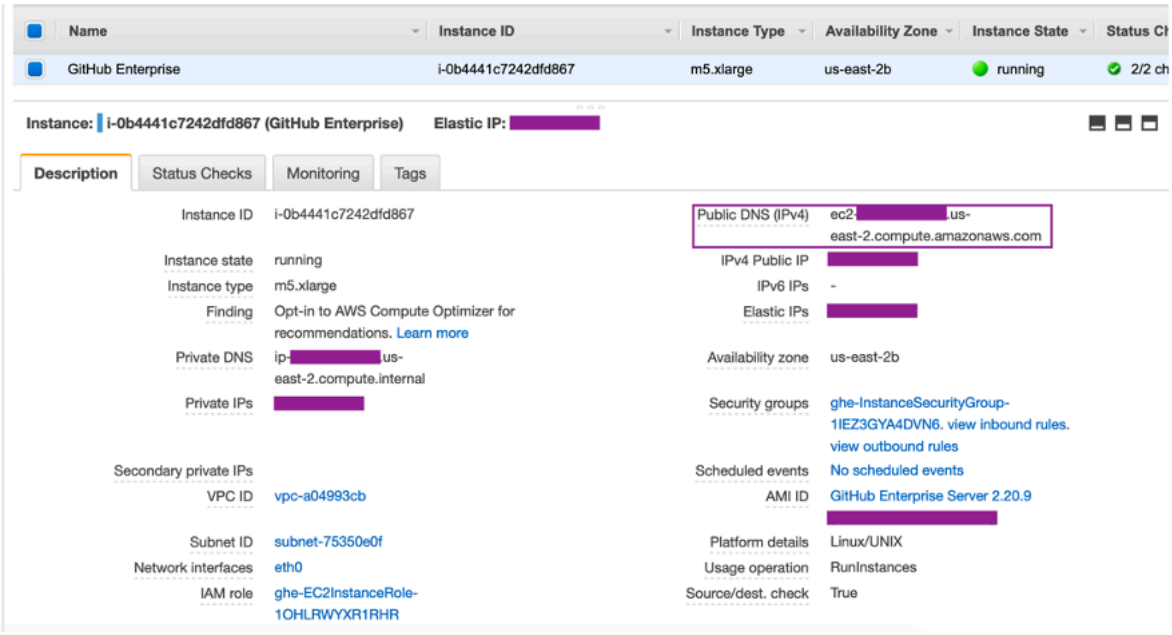
> **Note**
>
> Utilizza questa sezione per la risoluzione dei problemi relativi alla configurazione host di GitHub Enterprise Server all'interno di un Amazon VPC. Per la risoluzione dei problemi relativi alla connessione configurata per utilizzare l'endpoint webhook per VPC ()PrivateLink, vedere. Risoluzione dei problemi relativi agli endpoint VPC webhook PrivateLink () GitHub per le connessioni Enterprise Server

Per questo esempio, si utilizza il seguente processo per configurare il VPC e il server in cui verrà installata l'istanza di GitHub Enterprise Server:

1. Crea un VPC. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#Create-VPC.
2. Creazione di una sottorete nel VPC. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#AddaSubnet.
3. Per avviare un'istanza nel VPC. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#VPC_Launch_Instance.

> **Note**
>
> Ogni VPC può essere associato a un solo host (istanza GitHub Enterprise Server) alla volta.

L'immagine seguente mostra un' EC2 istanza avviata utilizzando l'AMI GitHub Enterprise.



Quando si utilizza un VPC per una connessione GitHub Enterprise Server, è necessario fornire quanto segue per l'infrastruttura quando si configura l'host:

- ID VPC: il VPC del server su cui è installata l'istanza di GitHub Enterprise Server o un VPC che ha accesso all'istanza GitHub Enterprise Server installata tramite VPN o Direct Connect.
- ID di sottorete o IDs: la sottorete del server su cui è installata l'istanza di GitHub Enterprise Server o una sottorete con accesso all'istanza di GitHub Enterprise Server installata tramite VPN o Direct Connect.
- Gruppo o gruppi di sicurezza: il gruppo di sicurezza per il server su cui è installata l'istanza di GitHub Enterprise Server o un gruppo di sicurezza con accesso all'istanza di GitHub Enterprise Server installata tramite VPN o Direct Connect.
- Endpoint: avere l'endpoint del server pronto e continuare con la fase successiva.

Per ulteriori informazioni sull'utilizzo delle sottoreti VPCs e delle sottoreti, consulta VPC and Subnet Sizing nella Amazon VPC User IPv4 Guide.

Argomenti

- Non riesco a ottenere un host con stato in attesa
- Non riesco a ottenere un host con stato disponibile
- La mia connessione/host funzionava e ora ha smesso di funzionare
- Non riesco a eliminare le interfacce di rete

Non riesco a ottenere un host con stato in attesa

Se l'host entra nello stato VPC_CONFIG_FAILED_INITIALIZZATION, ciò è probabilmente dovuto a un problema con il VPC, le sottoreti o i gruppi di protezione selezionati per l'host.

- Il VPC, le sottoreti e i gruppi di sicurezza devono appartenere all'account che crea l'host.
- Le sottoreti e i gruppi di sicurezza devono appartenere al VPC selezionato.
- Ogni sottorete fornita deve trovarsi in diverse zone di disponibilità.
- L'utente che crea l'host deve disporre delle seguenti autorizzazioni IAM:

```
ec2:CreateNetworkInterface
ec2:CreateTags
ec2:DescribeDhcpOptionsec2:DescribeNetworkInterfaces
ec2:DescribeSubnets
ec2:DeleteNetworkInterface
ec2:DescribeVpcs
ec2:CreateVpcEndpoint
ec2:DeleteVpcEndpoints
ec2:DescribeVpcEndpoints
```

Non riesco a ottenere un host con stato disponibile

Se non riesci a completare la configurazione dell' CodeConnections app per il tuo host, potrebbe essere a causa di un problema con le configurazioni VPC o l'istanza di GitHub Enterprise Server.

- Se non si utilizza un'autorità di certificazione pubblica, sarà necessario fornire all'host un certificato TLS utilizzato dall'istanza Enterprise. GitHub Il valore del Certificato TLS deve essere la chiave pubblica del certificato.
- È necessario essere un amministratore dell'istanza GitHub Enterprise Server per creare GitHub app.

La mia connessione/host funzionava e ora ha smesso di funzionare

Se una connessione/host funzionava prima e non funziona ora, potrebbe essere dovuto a una modifica della configurazione nel tuo VPC o all' GitHub app è stata modificata. Verifica quanto segue:

- Il gruppo di sicurezza collegato alla risorsa host creata per la connessione è ora cambiato o non ha più accesso a Enterprise Server. GitHub CodeConnections richiede un gruppo di sicurezza con connettività all'istanza di GitHub Enterprise Server.
- L'IP del server DNS è stato modificato di recente. È possibile verificarlo controllando le opzioni DHCP associate al VPC specificato nella risorsa host creata per la connessione. Tieni presente che se sei passato di recente da un server AmazonProvided DNS a un server DNS personalizzato o hai iniziato a utilizzare un nuovo server DNS personalizzato, l'host/la connessione smetterebbe di funzionare. Per risolvere questo problema, elimina il tuo host esistente e ricrealo. Così dovrebbero essere memorizzate le ultime impostazioni DNS nel nostro database.
- Le ACLs impostazioni di rete sono cambiate e non consentono più connessioni HTTP alla sottorete in cui si trova l'infrastruttura Enterprise Server. GitHub
- Tutte le configurazioni dell' CodeConnections app sull' GitHub Enterprise Server sono state modificate. Le modifiche a qualsiasi configurazione, ad esempio URLs o ai segreti dell'app, possono interrompere la connettività tra l'istanza di GitHub Enterprise Server installata e. CodeConnections

Non riesco a eliminare le interfacce di rete

Se non riesci a rilevare le interfacce di rete, verifica quanto segue:

- Le interfacce di rete create da CodeConnections possono essere eliminate solo eliminando l'host. Non possono essere eliminate manualmente dall'utente.
- Bisogna possedere le seguenti autorizzazioni:

```
ec2:DescribeNetworkInterfaces
ec2:DeleteNetworkInterface
```

Risoluzione dei problemi relativi agli endpoint VPC webhook PrivateLink () GitHub per le connessioni Enterprise Server

Quando si crea un host con configurazione VPC, viene creato automaticamente l'endpoint VPC webhook.

> **Note**
>
> Utilizza questa sezione per la risoluzione dei problemi relativi alla tua connessione configurata per utilizzare l'endpoint webhook per VPC (). PrivateLink Per la risoluzione dei problemi relativi alla configurazione GitHub dell'host Enterprise Server all'interno di un Amazon VPC, consulta. Risoluzione dei problemi di configurazione VPC per l'host

Quando crei una connessione a un tipo di provider installato e hai specificato che il tuo server è configurato all'interno di un VPC, AWS CodeConnections crea il tuo host e l'endpoint VPC (PrivateLink) per i webhook viene creato automaticamente. Ciò consente all'host di inviare dati sugli eventi tramite webhook ai tuoi AWS servizi integrati sulla rete Amazon. Per ulteriori informazioni, consulta AWS CodeConnections e endpoint VPC di interfaccia ()AWS PrivateLink.

Argomenti

- Non riesco a eliminare i miei endpoint VPC webhook

Non riesco a eliminare i miei endpoint VPC webhook

AWS CodeConnections gestisce il ciclo di vita degli endpoint VPC webhook per il tuo host. Se si desidera eliminare l'endpoint, è necessario eseguire questa operazione eliminando la risorsa host corrispondente.

- Gli endpoint VPC webhook PrivateLink () creati CodeConnections da possono essere eliminati solo eliminando l'host. Non possono essere eliminate manualmente.
- Bisogna possedere le seguenti autorizzazioni:

```
ec2:DescribeNetworkInterfaces
ec2:DeleteNetworkInterface
```

Risoluzione dei problemi per un host creato prima del 24 novembre 2020

A partire dal 24 novembre 2020, al momento AWS CodeConnections della configurazione dell'host, viene configurato un supporto aggiuntivo per gli endpoint VPC (PrivateLink). Per gli host creati prima di questo aggiornamento, utilizzare questa sezione di risoluzione dei problemi.

Per ulteriori informazioni, consulta AWS CodeConnections e endpoint VPC di interfaccia ()AWS PrivateLink.

Argomenti

- Ho un host creato prima del 24 novembre 2020 e voglio utilizzare gli endpoint VPC () PrivateLink per i webhook
- Non riesco a ottenere un host con stato disponibile (errore VPC)

Ho un host creato prima del 24 novembre 2020 e voglio utilizzare gli endpoint VPC () PrivateLink per i webhook

Quando configuri l'host per GitHub Enterprise Server, l'endpoint webhook viene creato automaticamente. Le connessioni ora utilizzano gli endpoint PrivateLink webhook VPC. Se hai creato l'host prima del 24 novembre 2020 e desideri utilizzare gli endpoint PrivateLink webhook VPC, devi prima eliminare l'host e quindi creare un nuovo host.

Non riesco a ottenere un host con stato disponibile (errore VPC)

Se il tuo host è stato creato prima del 24 novembre 2020 e non riesci a completare la configurazione dell' CodeConnections app per il tuo host, potrebbe essere a causa di un problema con le configurazioni VPC o l'istanza di GitHub Enterprise Server.

Il VPC avrà bisogno di un gateway NAT (o accesso a Internet in uscita) in modo che l'istanza di GitHub Enterprise Server possa inviare traffico di rete in uscita per i webhook. GitHub

Impossibile creare la connessione per un repository GitHub

Problema

Poiché una connessione a un GitHub repository utilizza il AWS Connector for GitHub, per creare la connessione sono necessarie le autorizzazioni del proprietario dell'organizzazione o delle autorizzazioni di amministratore per accedere al repository.

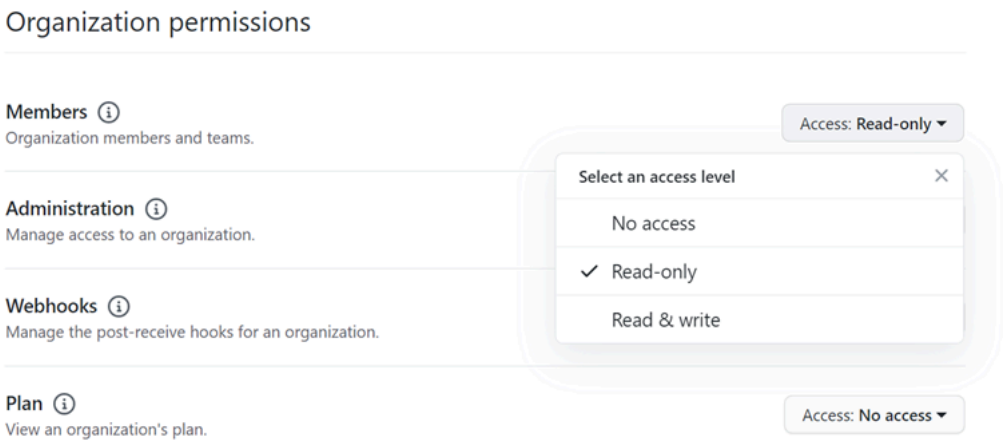
Possibili correzioni: per informazioni sui livelli di autorizzazione per un GitHub repository, vedi @ -. https://docs.github.com/en/ free-pro-team latest/github/setting-up-and-managing-organizations-and-teams/permission levels-for-an-organization

Modifica le autorizzazioni dell'app di connessione GitHub Enterprise Server

Se hai installato l'app per GitHub Enterprise Server entro il 23 dicembre 2020, potresti dover concedere all'app l'accesso in sola lettura ai membri dell'organizzazione. Se sei il proprietario dell' GitHub app, segui questi passaggi per modificare le autorizzazioni per l'app che è stata installata al momento della creazione dell'host.

> **Note**
>
> Devi completare questi passaggi sull'istanza di GitHub Enterprise Server e devi essere il proprietario dell' GitHub app.

1. In GitHub Enterprise Server, dall'opzione a discesa sulla foto del profilo, scegli Impostazioni.
2. Scegli Impostazioni sviluppatore, quindi scegli GitHub App.
3. Nell'elenco delle app, scegli il nome dell'app per la connessione, quindi scegli Permissions and events (Autorizzazioni ed eventi) nel display delle impostazioni.
4. In Autorizzazioni organizzazione, per Membri, scegli Sola lettura dall'elenco a discesa Accesso.



5. In Aggiungi una nota per gli utenti, aggiungi una descrizione del motivo dell'aggiornamento. Scegli Save changes (Salva modifiche).

Errore di connessione durante la connessione a GitHub: «Si è verificato un problema, assicurati che i cookie siano abilitati nel tuo browser» o «Il proprietario di un'organizzazione deve installare l' GitHub app»

Problema

Per creare la connessione per un GitHub repository, devi essere il proprietario dell' GitHub organizzazione. Per i repository che non appartengono a un'organizzazione, è necessario esserne il proprietario. Quando una connessione viene creata da qualcuno diverso dal proprietario dell'organizzazione, viene creata una richiesta per il proprietario dell'organizzazione e viene visualizzato uno dei seguenti errori:

A problem occurred, make sure cookies are enabled in your browser (Si è verificato un problema, assicurarsi che i cookie siano abilitati nel browser)

O

Il proprietario dell'organizzazione deve installare l'app GitHub

Possibili correzioni: per i repository di un' GitHuborganizzazione, il proprietario dell'organizzazione deve creare la connessione al GitHub repository. Per i repository che non appartengono a un'organizzazione, è necessario esserne il proprietario.

Potrebbe essere necessario aggiornare il prefisso del servizio Connections nelle risorse per le politiche IAM

Il 29 marzo 2024, il servizio è stato rinominato da AWS CodeStar Connections a. AWS CodeConnections A partire dal 1° luglio 2024, la console crea connessioni con `codeconnections` la risorsa ARN. Le risorse con entrambi i prefissi di servizio continueranno a essere visualizzate nella console. Il prefisso di servizio per le risorse create utilizzando la console è. `codeconnections` Le nuove risorse SDK/CLI vengono create con `codeconnections` la risorsa ARN. Le risorse create avranno automaticamente il nuovo prefisso di servizio.

Di seguito sono elencate le risorse create in AWS CodeConnections:

- Connessioni
- Host

Problema

Le risorse create con `codestar-connections` l'ARN non verranno automaticamente rinominate con il nuovo prefisso di servizio nell'ARN della risorsa. La creazione di una nuova risorsa creerà una risorsa con il prefisso del servizio di connessione. Tuttavia, le politiche IAM con il prefisso `codestar-connections` di servizio non funzioneranno per le risorse con il nuovo prefisso di servizio.

Possibili correzioni: per evitare problemi di accesso o di autorizzazioni per le risorse, completa le seguenti azioni:

- Aggiorna le politiche IAM per il nuovo prefisso del servizio. In caso contrario, le risorse rinominate o create non saranno in grado di utilizzare le policy IAM.
- Aggiorna le risorse per il nuovo prefisso di servizio creandole utilizzando la console o. CLI/CDK/CFN

Aggiorna le azioni, le risorse e le condizioni della politica in base alle esigenze. Nell'esempio seguente, il `Resource` campo è stato aggiornato per entrambi i prefissi di servizio.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "codeconnections:UseConnection"
        ],
        "Resource": [
            "arn:aws:codestar-connections:*:*:connection/*",
            "arn:aws:codeconnections:*:*:connection/*"
        ]
    }
}
```

Errore di autorizzazione dovuto al prefisso del servizio nelle risorse create utilizzando la console

Attualmente, le risorse di connessione create utilizzando la console avranno solo il prefisso di `codestar-connections` servizio. Per le risorse create utilizzando la console, le azioni relative alle policy statement devono includere `codestar-connections` come prefisso di servizio.

> **Note**
>
> A partire dal 1° luglio 2024, la console crea connessioni con `codeconnections` la risorsa ARN. Le risorse con entrambi i prefissi di servizio continueranno a essere visualizzate nella console.

Problema

Quando si crea una risorsa di connessione utilizzando la console, nella policy è necessario utilizzare il prefisso del `codestar-connections` servizio. Quando si utilizza una policy con il prefisso di `codeconnections` servizio nella policy, le risorse di connessione create utilizzando la console ricevono il seguente messaggio di errore:

```
User: user_ARN is not authorized to perform: codestar-connections:action on
 resource: resource_ARN because no identity-based policy allows the codestar-
connections:action action
```

Possibili correzioni: per le risorse create utilizzando la console, le azioni relative alle policy statement devono includere `codestar-connections` come prefisso del servizio, come illustrato nell'esempio di policy in. Esempio: una politica per la creazione AWS CodeConnections con la console

Configurazione della connessione e dell'host per i provider installati che supportano le organizzazioni

Per i provider installati che supportano organizzazioni, come GitHub Organizations, non viene assegnato un host disponibile. Crei un nuovo host per ogni connessione nella tua organizzazione e assicurati di inserire le stesse informazioni nei seguenti campi di rete:

- ID VPC
- ID di sottorete
- Gruppo di sicurezza IDs

Consulta i passaggi correlati per creare una connessione GHES o una connessione GitLab autogestita.

Desidero aumentare i miei limiti per le connessioni

Puoi richiedere un aumento del limite per determinati limiti in. CodeConnections Per ulteriori informazioni, consulta Quote per le connessioni.

Quote per le connessioni

Nelle seguenti tabelle sono elencate le quote (definite anche limiti) per le connessioni nella console Strumenti di sviluppo.

Le quote riportate in questa tabella si applicano per persona Regione AWS e possono essere aumentate. Per ulteriori informazioni sulle Regione AWS e sulle quote modificabili, consulta Quote di servizio AWS.

> **Note**
>
> È necessario abilitare l'Europa (Milano) Regione AWS prima di poterlo utilizzare. Per ulteriori informazioni, consulta Abilitare una regione.

Risorsa	Limite predefinito
Numero massimo di connessioni per Account AWS	250

Le quote in questa tabella sono fisse e non possono essere modificate.

Risorsa	Limite predefinito
Numero massimo di caratteri nei nomi delle connessioni	32 caratteri
Numero massimo di host per Account AWS	50
Numero massimo di collegamenti al repository	100
Numero massimo di configurazioni di sincronizzazione dello stack AWS CloudFormation	100

Risorsa	Limite predefinito
Numero massimo di configurazioni di sincronizzazione per collegamento al repository	100
Numero massimo di configurazioni di sincronizzazione per ramo	50

Indirizzi IP da aggiungere all'elenco degli indirizzi consentiti

Se implementi il filtro IP o consenti determinati indirizzi IP su EC2 istanze Amazon, aggiungi i seguenti indirizzi IP all'elenco degli indirizzi IP consentiti. In questo modo si abilitano le connessioni a provider come GitHub e Bitbucket.

Nella seguente tabella sono elencati gli indirizzi IP per le connessioni nella console Strumenti di sviluppo per Regione AWS.

> **Note**
>
> Per la regione Europa (Milano): è necessario abilitare questa regione prima di poterla utilizzare. Per ulteriori informazioni, consulta Enabling a Region (Abilitare una regione).

Regione	Indirizzi IP
Stati Uniti occidentali (Oregon) (us-west-2)	35.160.210.199, 54,71.206.108, 54,71.36205
Stati Uniti orientali (Virginia settentrionale) (us-east-1)	3,216,216,90, 3,216,243,220, 3,217,241,85
Europa (Irlanda) (eu-west-1)	34,242,64,82, 5218,37201, 54,7775,62
Stati Uniti orientali (Ohio) (us-east-2)	18,217,188,190, 18,218,158,91, 18,220,4,80
Asia Pacifico (Singapore) (ap-southeast-1)	18,138,171,151, 18,139,22,70, 31,157,1176
Asia Pacifico (Sydney) (ap-southeast-2)	13,236,59253, 5264,166,86, 54206,1112

Regione	Indirizzi IP
Asia Pacifico (Tokyo) (ap-northeast-1)	52,196,132231, 54,95133,227, 18,181,13,91
Europa (Francoforte) (eu-central-1)	18,196145,1164, 3,121,252,59, 52,59104,195
Asia Pacifico (Seoul) (ap-northeast-2)	13,125,8239, 13209,223,17, 3,37200,23
Asia Pacifico (Mumbai) (ap-south-1)	13,234,199,152, 13,235,29220, 35,154,230,124
Sud America (San Paolo) (sa-east-1)	18229,77,26, 54,233,226,52, 54,233207,69
Canada (Centrale) (ca-central-1)	15,222,219,210, 35,182,166,138, 99,79,111 ,198
Europa (Londra) (eu-west-2)	3,9,97205, 35,177,150,185, 35,177.200225
Stati Uniti occidentali (California settentrionale) (us-west-1)	52,5216,175, 52,863,87
Europe (Parigi) (eu-west-3)	35,181,127,138, 35,181,145,22, 35,181,20200
Europa (Stoccolma) (eu-north-1)	13,48,66148, 13,48,8,79, 13,5378,182
Europa (Milano) (eu-south-1)	18,102,28,105, 18,102,35130, 18,102,8116
AWS GovCloud (Stati Uniti orientali)	18,252,168,157, 18,252,207,77, 18,253185119

Sicurezza per le caratteristiche della console Strumenti di sviluppo

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità che si applicano alle AWS CodeStar notifiche e AWS CodeConnections, consulta la sezione AWS Servizi rientranti nell'ambito del programma di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi AWS CodeStar Notifications and AWS CodeConnections. I seguenti argomenti mostrano come configurare AWS CodeStar le notifiche e AWS CodeConnections raggiungere gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le AWS CodeStar notifiche e le AWS CodeConnections risorse.

Per ulteriori informazioni sulla sicurezza dei servizi nella console Strumenti di sviluppo, consulta quanto segue:

- CodeBuild Sicurezza
- CodeCommit Sicurezza
- CodeDeploy Sicurezza
- CodePipeline Sicurezza

Comprendere contenuti e sicurezza delle notifiche

Le notifiche forniscono informazioni sulle risorse agli utenti che hanno effettuato l'iscrizione alle destinazioni delle regole di notifica configurate. Questa informazione può includere dettagli sulle risorse degli strumenti di sviluppo, inclusi i contenuti del repository, gli stati delle compilazioni, gli stati delle implementazioni e le esecuzioni delle pipeline.

Ad esempio, puoi configurare una regola di notifica per un repository in CodeCommit modo da includere commenti su commit o pull request. In questo caso, le notifiche inviate in risposta a tale regola potrebbero contenere la riga o le righe di codice a cui si fa riferimento nel commento. Allo stesso modo, è possibile configurare una regola di notifica per un progetto di compilazione in modo CodeBuild da includere successi o errori per gli stati e le fasi di compilazione. Le notifiche inviate in risposta a tale regola conterranno tali informazioni.

È possibile configurare una regola di notifica per una pipeline in CodePipeline modo da includere informazioni sulle approvazioni manuali e le notifiche inviate in risposta a tale regola potrebbero contenere il nome della persona che fornisce l'approvazione. È possibile configurare una regola di notifica per un'applicazione in modo CodeDeploy da indicare il successo della distribuzione e le notifiche inviate in risposta a tale regola potrebbero contenere informazioni sull'obiettivo di distribuzione.

Le notifiche possono includere informazioni specifiche del progetto, ad esempio stati di compilazione, righe di codice con commenti, stati dell'implementazione e approvazioni della pipeline. Per garantire la sicurezza del progetto, assicurati di rivedere regolarmente sia le destinazioni delle regole di notifica sia l'elenco degli iscritti agli argomenti Amazon SNS specificati come destinazioni. Inoltre, il contenuto delle notifiche inviate in risposta a eventi potrebbe cambiare man mano che vengono aggiunte caratteristiche aggiuntive ai servizi sottostanti. Questa modifica può verificarsi senza preavviso per regole di notifica già esistenti. Valuta la possibilità di rivedere periodicamente i contenuti dei messaggi di notifica per essere certo di comprendere cosa viene inviato e il destinatario dell'invio.

Per ulteriori informazioni sui tipi di eventi disponibili per regole di notifica, consulta Concetti di notifica.

Puoi scegliere di limitare i dettagli nelle notifiche a solo ciò che è incluso in un evento. Questo viene definito il tipo di dettaglio Basic (Base). Questi eventi contengono esattamente le stesse informazioni inviate ad Amazon EventBridge e Amazon CloudWatch Events.

I servizi della console Developer Tools CodeCommit, ad esempio, potrebbero scegliere di aggiungere informazioni su alcuni o tutti i relativi tipi di eventi nei messaggi di notifica oltre a quelle disponibili in un evento. Queste informazioni supplementari possono essere aggiunte in qualsiasi momento

per migliorare i tipi di eventi attuali o integrare quelli futuri. Puoi scegliere di includere eventuali informazioni supplementari sull'evento, se disponibili, nella notifica scegliendo il tipo di dettaglio Full (Completo) . Per ulteriori informazioni, consulta Tipi di dettaglio.

Protezione dei dati nelle AWS CodeStar notifiche e AWS CodeConnections

Il modello di responsabilità AWS condivisa modello si applica alla protezione dei dati in AWS CodeStar Notifiche e AWS CodeConnections. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include

quando lavori con AWS CodeStar Notifications AWS CodeConnections e/o altro Servizi AWS utilizzando la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Gestione delle identità e degli accessi per AWS CodeStar notifiche e AWS CodeConnections

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare AWS CodeStar le notifiche e le risorse. AWS CodeConnections IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

> **Note**
>
> Sono disponibili azioni per le risorse create con il nuovo prefisso `codeconnections` di servizio. La creazione di una risorsa con il nuovo prefisso di servizio verrà utilizzata `codeconnections` nella risorsa ARN. Le azioni e le risorse per il prefisso del `codestar-connections` servizio restano disponibili. Quando si specifica una risorsa nella policy IAM, il prefisso del servizio deve corrispondere a quello della risorsa.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come funzionano le caratteristiche nella console degli strumenti di sviluppo con IAM
- AWS CodeConnections riferimento alle autorizzazioni
- Esempi di policy basate su identità
- Utilizzo dei tag per controllare l'accesso alle risorse AWS CodeConnections
- Utilizzo di notifiche e connessioni nella console
- Consentire agli utenti di visualizzare le loro autorizzazioni

- Risoluzione dei problemi relativi a AWS CodeStar notifiche, identità e accesso AWS CodeConnections
- Utilizzo di ruoli collegati ai servizi per le notifiche AWS CodeStar
- Utilizzo di ruoli collegati ai servizi per AWS CodeConnections
- AWS politiche gestite per AWS CodeConnections

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in AWS CodeStar Notifications e. AWS CodeConnections

Utente del servizio: se utilizzi le AWS CodeStar notifiche e il AWS CodeConnections servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS CodeStar notifiche e AWS CodeConnections funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS CodeStar Notifiche AWS CodeConnections, consultaRisoluzione dei problemi relativi a AWS CodeStar notifiche, identità e accesso AWS CodeConnections.

Amministratore del servizio: se sei responsabile delle AWS CodeStar notifiche e AWS CodeConnections delle risorse della tua azienda, probabilmente hai pieno accesso a AWS CodeStar Notifiche e AWS CodeConnections. È tuo compito determinare a quali AWS CodeStar notifiche e AWS CodeConnections funzionalità e risorse devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS CodeStar Notifications e AWS CodeConnections, consultaCome funzionano le caratteristiche nella console degli strumenti di sviluppo con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso alle AWS CodeStar notifiche e AWS CodeConnections. Per visualizzare esempi di AWS CodeStar notifiche e policy AWS CodeConnections basate sull'identità che puoi utilizzare in IAM, consulta. Esempi di policy basate su identità

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA)AWS in IAM nella Guida per l'utente IAM.

Utente root dell'account AWS

Quando ne crei un Account AWS, inizi con un'unica identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Create a role for a third-party identity provider (federation) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM

per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano

richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Come funzionano le caratteristiche nella console degli strumenti di sviluppo con IAM

Prima di utilizzare IAM per gestire l'accesso alle caratteristiche nella console degli strumenti di sviluppo, è necessario comprendere quali caratteristiche IAM sono disponibili per l'uso con essa. Per avere una visione di alto livello di come le notifiche e gli altri AWS servizi funzionano con IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Argomenti

- Policy basate sull'identità nella console Strumenti di sviluppo
- AWS CodeStar Notifiche e politiche basate sulle risorse AWS CodeConnections
- Autorizzazione basata su tag
- Ruoli IAM

Policy basate sull'identità nella console Strumenti di sviluppo

Con le policy basate su identità di IAM, è possibile specificare quali azioni e risorse sono consentite o rifiutate, nonché le condizioni in base alle quali le azioni sono consentite o rifiutate. AWS CodeStar Notifiche e AWS CodeConnections supporto per azioni, risorse e chiavi di condizione specifiche. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta Documentazione di riferimento degli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Azioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che

non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le operazioni delle policy per le notifiche nella console degli strumento di sviluppo utilizzano il seguente prefisso prima dell'operazione: `codestar-notifications and codeconnections`. Ad esempio, per concedere a qualcuno l'autorizzazione per visualizzare tutte le regole di notifica nel suo account, includi l'operazione `codestar-notifications:ListNotificationRules` nella rispettiva policy. Le dichiarazioni politiche devono includere un `NotAction` elemento `Action` or. AWS CodeStar AWS CodeConnections Notifica e definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

Per specificare più azioni di AWS CodeStar notifica in un'unica istruzione, separale con virgole come segue.

```
"Action": [
      "codestar-notifications:action1",
      "codestar-notifications:action2"
```

Per specificare più AWS CodeConnections azioni in un'unica istruzione, separale con virgole come segue.

```
"Action": [
      "codeconnections:action1",
      "codeconnections:action2"
```

Puoi specificare più operazioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le operazioni che iniziano con la parola `List`, includi la seguente operazione.

```
"Action": "codestar-notifications:List*"
```

AWS CodeStar Le azioni dell'API di notifica includono:

- `CreateNotificationRule`
- `DeleteNotificationRule`
- `DeleteTarget`

- `DescribeNotificationRule`
- `ListEventTypes`
- `ListNotificationRules`
- `ListTagsForResource`
- `ListTargets`
- `Subscribe`
- `TagResource`
- `Unsubscribe`
- `UntagResource`
- `UpdateNotificationRule`

AWS CodeConnections Le azioni API includono quanto segue:

- `CreateConnection`
- `DeleteConnection`
- `GetConnection`
- `ListConnections`
- `ListTagsForResource`
- `TagResource`
- `UntagResource`

Le seguenti azioni che richiedono solo le autorizzazioni sono necessarie AWS CodeConnections per completare l'handshake di autenticazione:

- `GetIndividualAccessToken`
- `GetInstallationUrl`
- `ListInstallationTargets`
- `StartOAuthHandshake`
- `UpdateConnectionInstallation`

Le seguenti azioni relative ai soli permessi sono necessarie per utilizzare una connessione: AWS CodeConnections

- `UseConnection`

La seguente azione basata solo sulle autorizzazioni è richiesta AWS CodeConnections per passare una connessione a un servizio:

- `PassConnection`

Per visualizzare un elenco di AWS CodeStar notifiche e AWS CodeConnections azioni, consulta Actions defined by AWS CodeStar Notifications and Actions Defined by AWS CodeConnections nella IAM User Guide.

Risorse

AWS CodeStar Le notifiche e AWS CodeConnections non supportano la specificazione della risorsa ARNs in una policy.

Chiavi di condizione

AWS CodeStar Le notifiche AWS CodeConnections definiscono i propri set di chiavi di condizione e supportano anche l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Tutte le azioni di AWS CodeStar notifica supportano la chiave di `codestar-notifications:NotificationsForResource` condizione. Per ulteriori informazioni, consulta Esempi di policy basate su identità.

AWS CodeConnections definiscono le seguenti chiavi di condizione che possono essere utilizzate nell'`Condition`elemento di una policy IAM. Puoi utilizzare queste chiavi per ottimizzare ulteriormente le condizioni in cui si applica l'istruzione di policy. Per ulteriori informazioni, consulta AWS CodeConnections riferimento alle autorizzazioni.

Chiavi di condizione	Descrizione
`codeconnections:BranchName`	Filtra l'accesso in base al nome del ramo del repository di terze parti
`codeconnections:FullRepositoryId`	Filtra l'accesso dal repository passato nella richiesta. Si applica solo alle richieste

Chiavi di condizione	Descrizione
	`UseConnection` per l'accesso a un repository specifico
`codeconnections:InstallationId`	Filtra l'accesso in base all'ID di terza parte (ad esempio l'ID di installazione dell'app Bitbucket) utilizzato per aggiornare una connessione. Consente di limitare le installazioni di app di terze parti che possono essere utilizzate per creare una connessione
`codeconnections:OwnerId`	Filtra l'accesso in base all'ID del proprietario o dell'account del provider di terze parti
`codeconnections:PassedToService`	Filtra l'accesso in base al servizio a cui l'entità può passare una connessione
`codeconnections:ProviderAction`	Filtra l'accesso in base all'operazione del provider in una richiesta `UseConnection` , ad esempio `ListRepositories` .
`codeconnections:ProviderPermissionsRequired`	Filtra l'accesso in base al tipo di autorizzazioni del provider di terze parti
`codeconnections:ProviderType`	Filtra l'accesso in base al tipo di provider di terze parti passato nella richiesta
`codeconnections:ProviderTypeFilter`	Filtra l'accesso in base al tipo di provider di terze parti utilizzato per filtrare i risultati
`codeconnections:RepositoryName`	Filtra l'accesso in base al nome del repository di terze parti

Esempi

Per visualizzare esempi di AWS CodeStar notifiche e politiche AWS CodeConnections basate sull'identità, consulta. Esempi di policy basate su identità

AWS CodeStar Notifiche e politiche basate sulle risorse AWS CodeConnections

AWS CodeStar Notifiche e politiche basate sulle AWS CodeConnections risorse non sono supportate.

Autorizzazione basata su tag

Puoi allegare tag a AWS CodeStar Notifiche e AWS CodeConnections risorse o inserire tag in una richiesta. Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `codestar-notifications and codeconnections:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. Per ulteriori informazioni sulle strategie di tagging, consulta Tagging resources AWS. Per ulteriori informazioni sull'etichettatura di AWS CodeStar notifiche e AWS CodeConnections risorse, consulta. Tagging di risorse di connessione

Per visualizzare policy basate sulle identità di esempio per limitare l'accesso a una risorsa basata su tag su tale risorsa, consulta Utilizzo dei tag per controllare l'accesso alle risorse AWS CodeConnections .

Ruoli IAM

Un ruolo IAM è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee

È possibile utilizzare credenziali temporanee per effettuare l'accesso utilizzando la federazione, assumere un ruolo IAM o assumere un ruolo tra account. Ottieni credenziali di sicurezza temporanee chiamando operazioni AWS STS API come AssumeRoleo. GetFederationToken

AWS CodeStar Notifiche e AWS CodeConnections supporti all'uso di credenziali temporanee.

Ruoli collegati ai servizi

I ruoli collegati ai AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione per conto dell'utente. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

AWS CodeStar Le notifiche supportano i ruoli collegati ai servizi. Per informazioni dettagliate sulla creazione o la gestione delle AWS CodeStar notifiche e dei ruoli AWS CodeConnections collegati ai servizi, consulta. Utilizzo di ruoli collegati ai servizi per le notifiche AWS CodeStar

CodeConnections non supporta ruoli collegati ai servizi.

AWS CodeConnections riferimento alle autorizzazioni

Le tabelle seguenti elencano ogni operazione AWS CodeConnections API, le azioni corrispondenti per le quali è possibile concedere le autorizzazioni e il formato della risorsa ARN da utilizzare per la concessione delle autorizzazioni. AWS CodeConnections APIs Sono raggruppate in tabelle in base all'ambito delle azioni consentite da tale API. Usale come riferimento durante la stesura delle policy di autorizzazione da collegare a un'identità IAM (policy basate su identità).

Quando si crea una policy di autorizzazione, è necessario specificare le operazioni nel campo `Action` della policy. Puoi specificare il valore della risorsa nel campo `Resource` della policy come ARN, con o senza un carattere jolly (*).

Per esprimere le condizioni nelle policy di connessione, utilizza le chiavi di condizione descritte qui ed elencate in Chiavi di condizione. Puoi anche usare i tasti di condizione AWS-wide. Per un elenco completo delle chiavi AWS-wide, consulta Available keys nella IAM User Guide.

Per specificare un'operazione, utilizza il prefisso `codeconnections` seguito dal nome dell'operazione API (ad esempio, `codeconnections:ListConnections` o `codeconnections:CreateConnection`).

Utilizzo di caratteri jolly

Per specificare più operazioni o risorse, usa un carattere jolly (*) nell'ARN. Ad esempio, `codeconnections:*` specifica tutte le AWS CodeConnections azioni e `codeconnections:Get*` specifica tutte le AWS CodeConnections azioni che iniziano con la parola. `Get` L'esempio seguente concede l'accesso completo a tutte le risorse con nomi che iniziano con `MyConnection`.

```
arn:aws:codeconnections:us-west-2:account-ID:connection/*
```

È possibile utilizzare i caratteri jolly solo con le *`connection`* risorse elencate nella tabella seguente. Non puoi usare i caratteri jolly con le nostre risorse*`region`*. *`account-id`* Per ulteriori informazioni sui caratteri jolly, consulta Identificatori IAM nella Guida per l'utente IAM.

Argomenti

- Autorizzazioni per la gestione delle connessioni
- Autorizzazioni per la gestione degli host

- Autorizzazioni per completare le connessioni
- Autorizzazioni per la configurazione degli host
- Trasferimento di una connessione a un servizio
- Utilizzo di una connessione
- Tipi di accesso supportati per ProviderAction
- Autorizzazioni supportate per l'assegnazione di tag alle risorse di connessione
- Passare una connessione a un collegamento di repository
- Chiave di condizione supportata per i collegamenti al repository

Autorizzazioni per la gestione delle connessioni

Un ruolo o un utente designato a utilizzare l'SDK AWS CLI o l'SDK per visualizzare, creare o eliminare connessioni deve avere le autorizzazioni limitate a quanto segue.

> **Note**
>
> Non è possibile completare o utilizzare una connessione nella console con solo le seguenti autorizzazioni. È necessario aggiungere le autorizzazioni in Autorizzazioni per completare le connessioni.

```
codeconnections:CreateConnection
codeconnections:DeleteConnection
codeconnections:GetConnection
codeconnections:ListConnections
```

AWS CodeStar Notifiche e autorizzazioni richieste per le azioni di gestione delle connessioni AWS CodeConnections

CreateConnection

Operazioni: `codeconnections:CreateConnection`

Necessario per utilizzare la CLI o la console per creare una connessione.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

DeleteConnection

Operazioni: `codeconnections:DeleteConnection`

Necessario per utilizzare la CLI o la console per eliminare una connessione.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetConnection

Operazioni: `codeconnections:GetConnection`

Necessario per utilizzare la CLI o la console per visualizzare i dettagli su una connessione.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListConnections

Operazioni: `codeconnections:ListConnections`

Necessario per utilizzare la CLI o la console per elencare tutte le connessioni nell'account.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Queste operazioni supportano le seguenti chiavi di condizione:

Azione	Chiavi di condizione
`codeconnections:CreateConnection`	`codeconnections:ProviderType`
`codeconnections:DeleteConnection`	N/D
`codeconnections:GetConnection`	N/D
`codeconnections:ListConnections`	`codeconnections:ProviderTypeFilter`

Autorizzazioni per la gestione degli host

Un ruolo o un utente designato a utilizzare l'SDK AWS CLI o l'SDK per visualizzare, creare o eliminare gli host deve disporre delle autorizzazioni limitate ai seguenti.

> **Note**
>
> Non è possibile completare o utilizzare una connessione nell'host con solo le seguenti autorizzazioni. È necessario aggiungere le autorizzazioni in Autorizzazioni per la configurazione degli host.

```
codeconnections:CreateHost
codeconnections:DeleteHost
codeconnections:GetHost
codeconnections:ListHosts
```

AWS CodeStar Notifiche e autorizzazioni richieste per le azioni di gestione degli host AWS CodeConnections

CreateHost

Operazioni: `codeconnections:CreateHost`

Necessario per utilizzare la CLI o la console per creare un host.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

DeleteHost

Operazioni: `codeconnections:DeleteHost`

Necessario per utilizzare la CLI o la console per eliminare un host.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

GetHost

Operazioni: `codeconnections:GetHost`

Necessario per utilizzare la CLI o la console per visualizzare i dettagli di un host.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

ListHosts

Operazioni: `codeconnections:ListHosts`

Necessario per utilizzare la CLI o la console per elencare tutti gli host nell'account.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

Queste operazioni supportano le seguenti chiavi di condizione:

Azione	Chiavi di condizione
`codeconnections:CreateHost`	`codeconnections:ProviderType` `codeconnections:VpcId`
`codeconnections:DeleteHost`	N/D
`codeconnections:GetHost`	N/D
`codeconnections:ListHosts`	`codeconnections:ProviderTypeFilter`

Per un esempio di politica che utilizza la chiave VpcIdcondition, vediEsempio: limita le autorizzazioni VPC dell'host utilizzando la chiave di contesto VpcId.

Autorizzazioni per completare le connessioni

Un ruolo o un utente designato per gestire le connessioni nella console deve disporre delle autorizzazioni necessarie per completare una connessione nella console e creare un'installazione, che include l'autorizzazione dell'handshake al provider e la creazione di installazioni da utilizzare per le connessioni. Utilizzare le seguenti autorizzazioni oltre alle autorizzazioni precedenti.

Le seguenti operazioni IAM vengono utilizzate dalla console durante l'esecuzione di un handshake basato su browser. `ListInstallationTargets`, `GetInstallationUrl`, `StartOAuthHandshake`, `UpdateConnectionInstallation`, e `GetIndividualAccessToken` sono autorizzazioni di policy IAM. Non sono operazioni API.

```
codeconnections:GetIndividualAccessToken
codeconnections:GetInstallationUrl
codeconnections:ListInstallationTargets
codeconnections:StartOAuthHandshake
codeconnections:UpdateConnectionInstallation
```

In base a ciò, sono necessarie le seguenti autorizzazioni per utilizzare, creare, aggiornare o eliminare una connessione nella console.

```
codeconnections:CreateConnection
codeconnections:DeleteConnection
codeconnections:GetConnection
codeconnections:ListConnections
codeconnections:UseConnection
codeconnections:ListInstallationTargets
codeconnections:GetInstallationUrl
codeconnections:StartOAuthHandshake
codeconnections:UpdateConnectionInstallation
codeconnections:GetIndividualAccessToken
```

AWS CodeConnections autorizzazioni necessarie per le azioni volte a completare le connessioni

GetIndividualAccessToken

Operazioni: `codeconnections:GetIndividualAccessToken`

Necessario per utilizzare la console per completare una connessione. Si tratta solo di un'autorizzazione di policy IAM, non di un'operazione API.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetInstallationUrl

Operazioni: `codeconnections:GetInstallationUrl`

Necessario per utilizzare la console per completare una connessione. Si tratta solo di un'autorizzazione di policy IAM, non di un'operazione API.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListInstallationTargets

Operazioni: `codeconnections:ListInstallationTargets`

Necessario per utilizzare la console per completare una connessione. Si tratta solo di un'autorizzazione di policy IAM, non di un'operazione API.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Avvia OAuth Handshake

Operazioni: `codeconnections:StartOAuthHandshake`

Necessario per utilizzare la console per completare una connessione. Si tratta solo di un'autorizzazione di policy IAM, non di un'operazione API.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

UpdateConnectionInstallation

Operazioni: `codeconnections:UpdateConnectionInstallation`

Necessario per utilizzare la console per completare una connessione. Si tratta solo di un'autorizzazione di policy IAM, non di un'operazione API.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Queste operazioni supportano le seguenti chiavi di condizione.

Azione	Chiavi di condizione
`codeconnections:GetIndividualAccessToken`	`codeconnections:ProviderType`
`codeconnections:GetInstallationUrl`	`codeconnections:ProviderType`
`codeconnections:ListInstallationTargets`	N/D
`codeconnections:StartOAuthHandshake`	`codeconnections:ProviderType`
`codeconnections:UpdateConnectionInstallation`	`codeconnections:InstallationId`

Autorizzazioni per la configurazione degli host

Un ruolo o un utente designato per gestire le connessioni nella console deve disporre delle autorizzazioni necessarie per configurare un host nella console, incluse l'autorizzazione dell'handshake al provider e l'installazione dell'app host. Utilizzare le seguenti autorizzazioni oltre alle autorizzazioni per host precedenti.

Le seguenti operazioni IAM vengono utilizzate dalla console per eseguire una registrazione dell'host basata su browser. `RegisterAppCode` e `StartAppRegistrationHandshake` sono autorizzazioni delle policy IAM. Non sono operazioni API.

```
codeconnections:RegisterAppCode
codeconnections:StartAppRegistrationHandshake
```

In base a ciò, sono necessarie le seguenti autorizzazioni per utilizzare, creare, aggiornare o eliminare una connessione nella console che richiede un host (ad esempio i tipi di provider installati).

```
codeconnections:CreateConnection
codeconnections:DeleteConnection
codeconnections:GetConnection
codeconnections:ListConnections
codeconnections:UseConnection
codeconnections:ListInstallationTargets
codeconnections:GetInstallationUrl
codeconnections:StartOAuthHandshake
codeconnections:UpdateConnectionInstallation
codeconnections:GetIndividualAccessToken
codeconnections:RegisterAppCode
codeconnections:StartAppRegistrationHandshake
```

AWS CodeConnections autorizzazioni necessarie per le azioni volte a completare la configurazione dell'host

RegisterAppCode

Operazioni: `codeconnections:RegisterAppCode`

Necessario per utilizzare la console per completare la configurazione dell'host. Si tratta solo di un'autorizzazione di policy IAM, non di un'operazione API.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

StartAppRegistrationHandshake

Operazioni: `codeconnections:StartAppRegistrationHandshake`

Necessario per utilizzare la console per completare la configurazione dell'host. Si tratta solo di un'autorizzazione di policy IAM, non di un'operazione API.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

Queste operazioni supportano le seguenti chiavi di condizione.

Trasferimento di una connessione a un servizio

Quando una connessione viene trasferita a un servizio (ad esempio, quando un ARN di connessione viene fornito in una definizione di pipeline per creare o aggiornare una pipeline), l'utente deve disporre dell'autorizzazione `codeconnections:PassConnection`.

AWS CodeConnections autorizzazioni richieste per il passaggio di una connessione

PassConnection

Operazioni: `codeconnections:PassConnection`

Necessario per passare una connessione a un servizio.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Questa operazione supporta anche la seguente chiave di condizione:

- `codeconnections:PassedToService`

Valori supportati per le chiavi di condizione

Chiave	Provider di operazione validi
`codeconnections:PassedToService`	• `codeguru-reviewer` • `codepipeline.amazonaws.com` • `proton.amazonaws.com`

Utilizzo di una connessione

Quando un servizio simile CodePipeline utilizza una connessione, il ruolo del servizio deve disporre dell'`codeconnections:UseConnection`autorizzazione per una determinata connessione.

Per gestire le connessioni nella console, è necessario che la policy utente disponga dell'autorizzazione `codeconnections:UseConnection`.

AWS CodeConnections azione richiesta per l'utilizzo di una connessione

UseConnection

Operazioni: `codeconnections:UseConnection`

Necessario per utilizzare una connessione.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

Questa operazione supporta anche le seguenti chiavi di condizione:

- `codeconnections:BranchName`
- `codeconnections:FullRepositoryId`
- `codeconnections:OwnerId`
- `codeconnections:ProviderAction`
- `codeconnections:ProviderPermissionsRequired`
- `codeconnections:RepositoryName`

Valori supportati per le chiavi di condizione

Chiave	Provider di operazione validi
`codeconnections:FullRepositoryId`	Il nome utente e il nome di repository di un repository, ad esempio `my-owner/my-repository` . Supportato solo quando la connessione viene utilizzata per accedere a un repository specifico.
`codeconnections:ProviderPermissionsRequired`	read_only o read_write
`codeconnections:ProviderAction`	`GetBranch` , `ListRepositories` , `ListOwners` , `ListBranches` , `StartUploadArchiveToS3` , `GitPush`, `GitPull`, `GetUploadArchiveToS3Status` , `CreatePullRequestDiffComment` , `GetPullRequest` , `ListBranc`

Chiave	Provider di operazione validi
	hCommits , ListCommitFiles , ListPullRequestComments , ListPullRequestCommits . Per informazioni, consulta la sezione successiva.

Le chiavi di condizione necessarie per alcune funzionalità potrebbero cambiare nel tempo. Si consiglia di utilizzare `codeconnections:UseConnection` per controllare l'accesso a una connessione, a meno che i requisiti di controllo dell'accesso non richiedano autorizzazioni diverse.

Tipi di accesso supportati per **`ProviderAction`**

Quando una connessione viene utilizzata da un AWS servizio, vengono effettuate chiamate API al provider del codice sorgente. Ad esempio, un servizio potrebbe elencare i repository per una connessione Bitbucket chiamando l'API `https://api.bitbucket.org/2.0/repositories/`*`username`*.

La chiave di `ProviderAction` condizione consente di limitare APIs il numero di provider che è possibile chiamare. Poiché il percorso API potrebbe essere generato dinamicamente e il percorso varia da provider a provider, il valore `ProviderAction` viene mappato a un nome di operazione astratto anziché all'URL dell'API. Ciò permette di scrivere policy che hanno lo stesso effetto indipendentemente dal tipo di provider per la connessione.

Di seguito sono riportati i tipi di accesso concessi per ciascuno dei valori `ProviderAction` supportati. Le seguenti sono autorizzazioni di policy IAM. Non sono operazioni API.

AWS CodeConnections tipi di accesso supportati per **`ProviderAction`**

GetBranch

Operazioni: `codeconnections:GetBranch`

Necessario per accedere alle informazioni su un ramo, ad esempio il commit più recente per quel ramo.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListRepositories

Operazioni: `codeconnections:ListRepositories`

Necessario per accedere a un elenco di repository pubblici e privati che appartengono a un proprietario, inclusi i dettagli su tali repository.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListOwners

Operazioni: `codeconnections:ListOwners`

Necessario per accedere a un elenco di proprietari a cui la connessione ha accesso.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListBranches

Operazioni: `codeconnections:ListBranches`

Necessario per accedere all'elenco dei rami esistenti in un determinato repository.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

StartUploadArchiveToS3

Operazioni: `codeconnections:StartUploadArchiveToS3`

Necessario per leggere il codice sorgente e caricarlo su Amazon S3.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GitPush

Operazioni: `codeconnections:GitPush`

Necessario per scrivere in un repository utilizzando Git.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GitPull

Operazioni: `codeconnections:GitPull`

Necessario per leggere da un repository utilizzando Git.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetUploadArchiveToStato S3

Operazioni: `codeconnections:GetUploadArchiveToS3Status`

Necessario per accedere allo stato di un caricamento, inclusi eventuali messaggi di errore, avviato da `StartUploadArchiveToS3`.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

CreatePullRequestDiffComment

Operazioni: `codeconnections:CreatePullRequestDiffComment`

Necessario per accedere ai commenti su una richiesta pull.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

GetPullRequest

Operazioni: `codeconnections:GetPullRequest`

Necessario per visualizzare le richieste pull per un repository.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListBranchCommits

Operazioni: `codeconnections:ListBranchCommits`

Necessario per visualizzare un elenco di commit per un ramo del repository.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListCommitFiles

Operazioni: `codeconnections:ListCommitFiles`

Necessario per visualizzare un elenco di file per un commit.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*

ListPullRequestComments

Operazioni: `codeconnections:ListPullRequestComments`

Necessario per visualizzare un elenco di commenti per una richiesta pull.

Risorsa:`arn:aws:codeconnections:region:account-id:connection/connection-id`

ListPullRequestCommits

Operazioni: `codeconnections:ListPullRequestCommits`

Necessario per visualizzare un elenco di commit per una richiesta pull.

Risorsa:`arn:aws:codeconnections:region:account-id:connection/connection-id`

Autorizzazioni supportate per l'assegnazione di tag alle risorse di connessione

Le seguenti operazioni IAM vengono utilizzate per taggare le risorse di connessione.

```
codeconnections:ListTagsForResource
codeconnections:TagResource
codeconnections:UntagResource
```

AWS CodeConnections azioni necessarie per etichettare le risorse di connessione

ListTagsForResource

Operazioni: `codeconnections:ListTagsForResource`

Necessario per visualizzare un elenco di tag associati alla risorsa di connessione.

Risorsa:`arn:aws:codeconnections:region:account-id:connection/connection-id`, `arn:aws:codeconnections:region:account-id:host/host-id`

TagResource

Operazioni: `codeconnections:TagResource`

Necessario per aggiungere tag a una risorsa di connessione.

Risorsa:`arn:aws:codeconnections:region:account-id:connection/connection-id`, `arn:aws:codeconnections:region:account-id:host/host-id`

UntagResource

Operazioni: `codeconnections:UntagResource`

Necessario per rimuovere i tag da una risorsa di connessione.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:connection/`*`connection-id`*, `arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:host/`*`host-id`*

Passare una connessione a un collegamento di repository

Quando in una configurazione di sincronizzazione viene fornito un collegamento di repository, l'utente deve disporre dell'autorizzazione `codeconnections:PassRepository` per l'ARN o la risorsa di collegamento al repository.

AWS CodeConnections autorizzazioni necessarie per il passaggio di una connessione

PassRepository

Operazioni: `codeconnections:PassRepository`

Necessaria per passare un collegamento di repository a una configurazione di sincronizzazione.

Risorsa:`arn:aws:codeconnections:`*`region`*`:`*`account-id`*`:repository-link/`*`repository-link-id`*

Questa operazione supporta anche la seguente chiave di condizione:

- `codeconnections:PassedToService`

Valori supportati per le chiavi di condizione

Chiave	Provider di operazione validi
`codeconnections:PassedToService`	• `cloudformation.sync.codeconnections.amazonaws.com`

Chiave di condizione supportata per i collegamenti al repository

La seguente chiave di condizione supporta le operazioni per i collegamenti ai repository e le risorse di configurazione delle sincronizzazioni:

- `codeconnections:Branch`

  Filtra l'accesso in base al nome del ramo passato nella richiesta.

Azioni supportate per la chiave di condizione

Chiave	Valori validi
`codeconnections:Branch`	Per questa chiave di condizione sono supportate le seguenti operazioni: • CreateSyncConfiguration • UpdateSyncConfiguration • GetRepositorySyncStatus

Esempi di policy basate su identità

Per impostazione predefinita, gli utenti e i ruoli IAM che dispongono di una delle policy gestite o AWS CodePipeline applicate dispongono di autorizzazioni per AWS CodeCommit connessioni, notifiche e regole di notifica in linea con l'intento di tali policy. AWS CodeBuild AWS CodeDeploy Ad esempio, gli utenti o i ruoli IAM a cui è stata applicata una delle politiche di accesso completo (AWSCodeCommitFullAccessAWSCodeBuildAdminAccessAWSCodeDeployFullAccess,, or AWSCodePipeline_FullAccess) hanno anche accesso completo alle notifiche e alle regole di notifica create per le risorse di tali servizi.

Gli altri utenti e ruoli IAM non sono autorizzati a creare o modificare AWS CodeStar notifiche e AWS CodeConnections risorse. Inoltre, non possono eseguire attività utilizzando l' AWS API AWS Management Console AWS CLI, o. Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi collegare queste policy a utenti o IAM che richiedono tali autorizzazioni.

Autorizzazioni ed esempi per le notifiche AWS CodeStar

Le seguenti dichiarazioni ed esempi di policy possono aiutarti a gestire AWS CodeStar le notifiche.

Autorizzazioni correlate alle notifiche nelle policy gestite di accesso completo

Le politiche AWSCodeCommitFullAccessAWSCodeBuildAdminAccess, AWSCodeDeployFullAccess, e AWSCodePipeline_FullAccessgestite includono le seguenti istruzioni per consentire l'accesso completo alle notifiche nella console Developer Tools. Gli utenti a cui è stata applicata una di queste policy gestite possono anche creare e gestire argomenti Amazon SNS per le notifiche, iscrivere

e annullare l'iscrizione degli utenti agli argomenti ed elencare gli argomenti da scegliere come destinazioni per le regole di notifica.

> **Note**
>
> Nella policy gestita, la chiave di condizione `codestar-notifications:NotificationsForResource` ha un valore specifico per il tipo di risorsa del servizio. Ad esempio, nella politica di accesso completo per CodeCommit, il valore è`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": "*"
    }
```

Autorizzazioni correlate alle notifiche nelle policy gestite di sola lettura

Le politiche AWSCodeCommitReadOnlyAccessAWSCodeBuildReadOnlyAccess, AWSCodeDeployReadOnlyAccess, e AWSCodePipeline_ReadOnlyAccessgestite includono le seguenti istruzioni per consentire l'accesso in sola lettura alle notifiche. Ad esempio, possono visualizzare le notifiche per le risorse nella console Strumenti di sviluppo, ma non possono crearle, gestirle o iscriversi a esse.

> **Note**
>
> Nella policy gestita, la chiave di condizione `codestar-notifications:NotificationsForResource` ha un valore specifico per il tipo di risorsa del servizio. Ad esempio, nella politica di accesso completo per CodeCommit, il valore è. `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": "*"
    }
```

Autorizzazioni correlate alle notifiche in altre policy gestite

Le AWSCodeCommitPowerUserpolicy e AWSCodeBuildDeveloperAccessle policy AWSCodeBuildDeveloperAccessgestite includono le seguenti istruzioni per consentire agli sviluppatori a cui è stata applicata una di queste politiche gestite di creare, modificare e sottoscrivere le notifiche. Non possono eliminare le regole di notifica o gestire i tag per le risorse.

> **Note**
>
> Nella policy gestita, la chiave di condizione `codestar-notifications:NotificationsForResource` ha un valore specifico per il tipo di risorsa del servizio. Ad esempio, nella politica di accesso completo per CodeCommit, il valore è`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": "*"
    }
```

Esempio: una politica a livello di amministratore per la gestione delle notifiche AWS CodeStar

In questo esempio, vuoi concedere a un utente IAM del tuo AWS account l'accesso completo alle AWS CodeStar notifiche in modo che l'utente possa esaminare i dettagli delle regole di notifica ed elencare le regole di notifica, gli obiettivi e i tipi di eventi. Si vuole anche consentire all'utente di aggiungere, aggiornare ed eliminare regole di notifica. Si tratta di una policy di accesso completa, equivalente ai permessi di notifica inclusi nelle policy e nelle AWSCodeBuildAdminAccesspolicy AWSCodePipeline_FullAccessgestite. AWSCodeCommitFullAccessAWSCodeDeployFullAccess Analogamente a queste policy gestite, dovresti allegare questo tipo di dichiarazione politica solo a utenti, gruppi o ruoli IAM che richiedono l'accesso amministrativo completo alle notifiche e alle regole di notifica del tuo AWS account.

> **Note**
>
> Questa policy contiene `CreateNotificationRule`. Qualsiasi utente con questa policy applicata al proprio utente o ruolo IAM sarà in grado di creare regole di notifica per tutti i tipi di risorse supportati da AWS CodeStar Notifications nell' AWS account, anche se l'utente stesso non ha accesso a tali risorse. Ad esempio, un utente con questa politica potrebbe creare una regola di notifica per un CodeCommit repository senza disporre delle autorizzazioni per l'accesso CodeCommit stesso.

```
{
    "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": "*"
      }
   ]
}
```

Esempio: una politica a livello di collaboratore per l'utilizzo delle notifiche AWS CodeStar

In questo esempio, si desidera concedere l'accesso all' day-to-dayutilizzo delle AWS CodeStar notifiche, come la creazione e la sottoscrizione di notifiche, ma non ad azioni più distruttive, come l'eliminazione di regole o obiettivi di notifica. Questo è l'equivalente dell'accesso fornito nelle politiche e AWSCodeBuildDeveloperAccessgestite AWSCodeDeployDeveloperAccess. AWSCodeCommitPowerUser

> **Note**
>
> Questa policy contiene `CreateNotificationRule`. Qualsiasi utente con questa policy applicata al proprio utente o ruolo IAM sarà in grado di creare regole di notifica per tutti i tipi di risorse supportati da AWS CodeStar Notifications nell' AWS account, anche se l'utente stesso non ha accesso a tali risorse. Ad esempio, un utente con questa politica potrebbe creare una regola di notifica per un CodeCommit repository senza disporre delle autorizzazioni per l'accesso CodeCommit stesso.

```
{
    "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": "*"
        }
```

```
    ]
}
```

Esempio: una read-only-level politica per l'utilizzo delle notifiche AWS CodeStar

In questo esempio, desideri concedere a un utente IAM nel tuo account l'accesso in sola lettura alle regole di notifica, ai destinatari e ai tipi di eventi nell'account AWS . Questo esempio mostra come creare una policy che consente di visualizzare questi elementi. È l'equivalente delle autorizzazioni incluse nelle politiche e AWSCodePipeline_ReadOnlyAccessgestite. AWSCodeBuildReadOnlyAccessAWSCodeCommitReadOnly

```
{
    "Version": "2012-10-17",
    "Id": "CodeNotification__ReadOnly",
    "Statement": [
        {
            "Sid": "Reads_API_Access",
            "Effect": "Allow",
            "Action": [
                "CodeNotification:DescribeNotificationRule",
                "CodeNotification:ListNotificationRules",
                "CodeNotification:ListTargets",
                "CodeNotification:ListEventTypes"
            ],
            "Resource": "*"
        }
    ]
}
```

Autorizzazioni ed esempi per AWS CodeConnections

Le istruzioni e gli esempi di policy riportati di seguito consentono di gestire AWS CodeConnections.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy nella scheda JSON nella Guida per l'utente IAM.

Esempio: una politica per la creazione AWS CodeConnections con la CLI e la visualizzazione con la console

Un ruolo o un utente designato a utilizzare l'SDK AWS CLI o l'SDK per visualizzare, creare, etichettare o eliminare le connessioni deve avere le autorizzazioni limitate a quanto segue.

> **Note**
>
> Non è possibile completare una connessione nella console con solo le seguenti autorizzazioni. È necessario aggiungere le autorizzazioni nella sezione successiva.

Per utilizzare la console per visualizzare un elenco di connessioni disponibili, visualizzare i tag e utilizzare una connessione, utilizzare la policy seguente.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "ConnectionsFullAccess",
        "Effect": "Allow",
        "Action": [
            "codeconnections:CreateConnection",
            "codeconnections:DeleteConnection",
            "codeconnections:UseConnection",
            "codeconnections:GetConnection",
            "codeconnections:ListConnections",
            "codeconnections:TagResource",
            "codeconnections:ListTagsForResource",
            "codeconnections:UntagResource"
        ],
        "Resource": "*"
     }
   ]
}
```

Esempio: una politica per la creazione AWS CodeConnections con la console

Un ruolo o un utente designato per gestire le connessioni nella console deve disporre delle autorizzazioni necessarie per completare una connessione nella console e creare un'installazione, che include l'autorizzazione dell'handshake al provider e la creazione di installazioni da utilizzare per le connessioni. `UseConnection` dovrebbe anche essere aggiunto per utilizzare la connessione nella console. Utilizzare la policy seguente per visualizzare, utilizzare, creare taggare o eliminare una connessione nella console.

> **Note**
>
> A partire dal 1° luglio 2024, la console crea connessioni con `codeconnections` la risorsa ARN. Le risorse con entrambi i prefissi di servizio continueranno a essere visualizzate nella console.

> **Note**
>
> Per le risorse create utilizzando la console, le azioni relative alle policy statement devono includere `codestar-connections` come prefisso di servizio, come illustrato nell'esempio seguente.

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

Esempio: una politica a livello di amministratore per la gestione AWS CodeConnections

In questo esempio, vuoi concedere a un utente IAM del tuo AWS account l'accesso completo a in CodeConnections modo che l'utente possa aggiungere, aggiornare ed eliminare connessioni. Questa è una politica di accesso completo, equivalente alla politica AWSCodePipeline_FullAccessgestita. Analogamente a quella politica gestita, dovresti allegare questo tipo di dichiarazione politica solo a utenti, gruppi o ruoli IAM che richiedono l'accesso amministrativo completo alle connessioni tra il tuo AWS account.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "ConnectionsFullAccess",
        "Effect": "Allow",
        "Action": [
            "codeconnections:CreateConnection",
            "codeconnections:DeleteConnection",
            "codeconnections:UseConnection",
            "codeconnections:GetConnection",
            "codeconnections:ListConnections",
            "codeconnections:ListInstallationTargets",
            "codeconnections:GetInstallationUrl",
            "codeconnections:StartOAuthHandshake",
            "codeconnections:UpdateConnectionInstallation",
            "codeconnections:GetIndividualAccessToken",
            "codeconnections:TagResource",
            "codeconnections:ListTagsForResource",
            "codeconnections:UntagResource"
        ],
        "Resource": "*"
     }
   ]
}
```

Esempio: una politica a livello di collaboratore da utilizzare AWS CodeConnections

In questo esempio, si desidera concedere l'accesso all' day-to-dayutilizzo di CodeConnections, ad esempio la creazione e la visualizzazione dei dettagli delle connessioni, ma non ad azioni più distruttive, come l'eliminazione delle connessioni.

```
{
```

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

Esempio: una read-only-level politica per l'utilizzo AWS CodeConnections

In questo esempio, vuoi concedere a un utente IAM del tuo account l'accesso in sola lettura alle connessioni del tuo AWS account. Questo esempio mostra come creare una policy che consente di visualizzare questi elementi.

```
{
    "Version": "2012-10-17",
    "Id": "Connections__ReadOnly",
    "Statement": [
        {
            "Sid": "Reads_API_Access",
            "Effect": "Allow",
            "Action": [
            "codeconnections:GetConnection",
            "codeconnections:ListConnections",
            "codeconnections:ListInstallationTargets",
            "codeconnections:GetInstallationUrl",
            "codeconnections:ListTagsForResource"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Esempio: limita le autorizzazioni VPC dell'host utilizzando la chiave di contesto VpcId

Nell'esempio seguente, il cliente può utilizzare la chiave di VpcIdcontesto per limitare la creazione o la gestione degli host agli host con un VPC specificato.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "codeconnections:CreateHost",
                "codeconnections:UpdateHost"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "codeconnections:VpcId": "vpc-EXAMPLE"
                }
            }
        }
    ]
}
```

Utilizzo dei tag per controllare l'accesso alle risorse AWS CodeConnections

I tag possono essere collegati alla risorsa o trasferiti nella richiesta verso servizi che supportano il tagging. In AWS CodeConnections, le risorse possono avere tag e alcune azioni possono includere tag. Quando si crea una policy IAM, è possibile utilizzare le chiavi di condizione di tag per controllare:

- Quali utenti possono eseguire operazioni su una risorsa della pipeline, in base ai tag di cui la risorsa dispone già.
- Quali tag possono essere passati in una richiesta di operazione.
- Se delle chiavi di tag specifiche possono essere utilizzate in una richiesta.

Gli esempi seguenti mostrano come specificare le condizioni dei tag nelle politiche per AWS CodeConnections gli utenti.

Example 1: Consentire operazioni in base ai tag nella richiesta

La seguente politica concede agli utenti il permesso di creare connessioni in AWS CodeConnections.

A questo scopo, consente le operazioni `CreateConnectione` `TagResource` se la richiesta specifica un tag denominato `Project` con il valore `ProjectA`. La chiave di condizione `aws:RequestTag` viene utilizzata per controllare quali tag possono essere passati in una richiesta IAM. La condizione `aws:TagKeys` garantisce che la chiave tag rileva la distinzione tra maiuscole e minuscole.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codeconnections:CreateConnection",
        "codeconnections:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Project": "ProjectA"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["Project"]
        }
      }
    }
  ]
}
```

Example 2: Consentire operazioni in base ai tag delle risorse

La policy seguente concede agli utenti l'autorizzazione per eseguire operazioni e ottenere informazioni sulle risorse in AWS CodeConnections.

A questo scopo, consente operazioni specifiche se la pipeline dispone di un tag denominato `Project` con il valore `ProjectA`. La chiave di condizione `aws:RequestTag` viene utilizzata per

controllare quali tag possono essere passati in una richiesta IAM. La condizione `aws:TagKeys` garantisce che la chiave tag rileva la distinzione tra maiuscole e minuscole.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codeconnections:CreateConnection",
        "codeconnections:DeleteConnection",
        "codeconnections:ListConnections"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "ProjectA"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["Project"]
        }
      }
    }
  ]
}
```

Utilizzo di notifiche e connessioni nella console

L'esperienza di notifica è integrata nelle console CodeBuild CodeCommit, CodeDeploy, e, nonché nella CodePipeline console Developer Tools nella barra di navigazione delle Impostazioni stessa. Per accedere alle notifiche nelle console, è necessario applicare una delle policy gestite a tali servizi oppure disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle AWS CodeStar notifiche e sulle AWS CodeConnections risorse del tuo AWS account. Se crei una policy basata su identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti e ruoli IAM) associate a tale policy. Per ulteriori informazioni sulla concessione dell'accesso a AWS CodeBuild,, e AWS CodeCommit AWS CodeDeploy AWS CodePipeline, incluso l'accesso a tali console, consulta i seguenti argomenti:

- CodeBuild: Utilizzo di politiche basate sull'identità per CodeBuild

- CodeCommit: Utilizzo di politiche basate sull'identità per CodeCommit
- AWS CodeDeploy: Gestione delle identità e degli accessi per AWS CodeDeploy
- CodePipeline: controllo degli accessi con policy IAM

AWS CodeStar Le notifiche non hanno politiche AWS gestite. Per fornire l'accesso alla funzionalità di notifica, è necessario applicare una delle policy gestite per uno dei servizi elencati in precedenza oppure creare policy con il livello di autorizzazione che si desidera concedere agli utenti o alle entità e quindi allegare le policy agli utenti, ai gruppi o ai ruoli che richiedono le autorizzazioni. Per maggiori informazioni ed esempi, consulta:

- Esempio: una politica a livello di amministratore per la gestione delle notifiche AWS CodeStar
- Esempio: una politica a livello di collaboratore per l'utilizzo delle notifiche AWS CodeStar
- Esempio: una read-only-level politica per l'utilizzo delle notifiche AWS CodeStar .

AWS CodeConnections non dispone di politiche AWS gestite. È possibile utilizzare le autorizzazioni e le combinazioni di autorizzazioni per l'accesso, ad esempio le autorizzazioni descritte in Autorizzazioni per completare le connessioni.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Esempio: una politica a livello di amministratore per la gestione AWS CodeConnections
- Esempio: una politica a livello di collaboratore da utilizzare AWS CodeConnections
- Esempio: una read-only-level politica per l'utilizzo AWS CodeConnections

Non è necessario concedere le autorizzazioni della console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è possibile accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI 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": "*"
        }
    ]
}
```

Risoluzione dei problemi relativi a AWS CodeStar notifiche, identità e accesso AWS CodeConnections

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo delle notifiche e IAM.

Argomenti

- Sono un amministratore e desidero consentire ad altri utenti di accedere alle notifiche

- Ho creato un argomento Amazon SNS e l'ho aggiunto come una destinazione delle regole di notifica, ma non ricevo e-mail sugli eventi
- Voglio consentire a persone esterne al mio AWS account di accedere alle mie AWS CodeStar notifiche e AWS CodeConnections risorse

Sono un amministratore e desidero consentire ad altri utenti di accedere alle notifiche

Per consentire ad altri di accedere alle AWS CodeStar notifiche e AWS CodeConnections, è necessario concedere l'autorizzazione alle persone o alle applicazioni che devono accedere. Se si utilizza AWS IAM Identity Center per gestire persone e applicazioni, si assegnano set di autorizzazioni a utenti o gruppi per definirne il livello di accesso. I set di autorizzazioni creano e assegnano automaticamente le policy IAM ai ruoli IAM associati alla persona o all'applicazione. Per ulteriori informazioni, consulta Set di autorizzazioni nella Guida per l'AWS IAM Identity Center utente.

Se non utilizzi IAM Identity Center, devi creare entità IAM (utenti o ruoli) per le persone o le applicazioni che necessitano di accesso. È quindi necessario allegare una policy all'entità che conceda loro le autorizzazioni corrette in AWS CodeStar Notifiche e. AWS CodeConnections Dopo aver concesso le autorizzazioni, fornisci le credenziali all'utente o allo sviluppatore dell'applicazione. Utilizzeranno tali credenziali per accedere. AWSPer ulteriori informazioni sulla creazione di utenti, gruppi, policy e autorizzazioni IAM, consulta IAM Identities and Policies and permissions in IAM nella IAM User Guide.

Per informazioni specifiche AWS CodeStar sulle notifiche, consulta. Autorizzazioni ed esempi per le notifiche AWS CodeStar

Ho creato un argomento Amazon SNS e l'ho aggiunto come una destinazione delle regole di notifica, ma non ricevo e-mail sugli eventi

Per ricevere notifiche sugli eventi, devi aver effettuato l'iscrizione a un argomento Amazon SNS valido come una destinazione per la regola di notifica e devi aver effettuato l'iscrizione del tuo indirizzo e-mail all'argomento Amazon SNS. Per risolvere i problemi relativi all'argomento Amazon SNS, verifica quanto segue:

- Assicurati che l'argomento Amazon SNS si trovi nella stessa AWS regione della regola di notifica.
- Verifica di aver effettuato l'iscrizione del tuo alias e-mail all'argomento corretto e di averla confermata. Per ulteriori informazioni, consulta Iscrizione di un endpoint a un argomento Amazon SNS.

- Verifica che la politica dell'argomento sia stata modificata per consentire a AWS CodeStar Notifications di inviare notifiche a quell'argomento. La policy dell'argomento deve includere un'istruzione simile alla seguente:

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

  Per ulteriori informazioni, consulta Configurazione.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie AWS CodeStar notifiche e AWS CodeConnections risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS CodeStar Notifications and AWS CodeConnections supporta queste funzionalità, consulta. Come funzionano le caratteristiche nella console degli strumenti di sviluppo con IAM
- Per scoprire come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.

- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Utilizzo di ruoli collegati ai servizi per le notifiche AWS CodeStar

AWS CodeStar Le notifiche utilizzano ruoli AWS Identity and Access Management collegati ai servizi (IAM). Un ruolo collegato al servizio è un tipo unico di ruolo IAM collegato direttamente alle notifiche. AWS CodeStar I ruoli collegati ai servizi sono predefiniti da AWS CodeStar Notifications e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS Questo ruolo viene creato la prima volta che crei una regola di notifica. Non devi creare il ruolo.

Un ruolo collegato al servizio semplifica la configurazione AWS CodeStar delle notifiche perché non è necessario aggiungere le autorizzazioni manualmente. AWS CodeStar Le notifiche definiscono le autorizzazioni dei relativi ruoli collegati al servizio e, se non diversamente definito, solo AWS CodeStar Notifications può assumere i relativi ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per eliminare un ruolo collegato al servizio, è necessario innanzitutto eliminarne le risorse correlate. In questo modo proteggi AWS CodeStar le tue risorse di Notifiche perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi consulta Servizi AWS che funzionano con IAM.

Autorizzazioni di ruolo collegate al servizio per le notifiche AWS CodeStar

AWS CodeStar Notifications utilizza il ruolo AWSService RoleForCodeStarNotifications collegato al servizio per recuperare informazioni sugli eventi che si verificano nella toolchain e inviare notifiche agli obiettivi specificati.

Il ruolo AWSService RoleForCodeStarNotifications collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `codestar-notifications.amazonaws.com`

La politica di autorizzazione dei ruoli consente a AWS CodeStar Notifications di completare le seguenti azioni sulle risorse specificate:

- Operazione: `PutRule` su `CloudWatch Event rules that are named awscodestar-notifications-*`
- Operazione: `DescribeRule` su `CloudWatch Event rules that are named awscodestar-notifications-*`
- Operazione: `PutTargets` su `CloudWatch Event rules that are named awscodestar-notifications-*`
- Operazione: `CreateTopic` su `create Amazon SNS topics for use with AWS CodeStar Notifications with the prefix CodeStarNotifications-`
- Operazione: `GetCommentsForPullRequests` su `all comments on all pull requests in all CodeCommit repositories in the AWS account`
- Operazione: `GetCommentsForComparedCommit` su `all comments on all commits in all CodeCommit repositories in the AWS account`
- Operazione: `GetDifferences` su `all commits in all CodeCommit repositories in the AWS account`
- Operazione: `GetCommentsForComparedCommit` su `all comments on all commits in all CodeCommit repositories in the AWS account`
- Operazione: `GetDifferences` su `all commits in all CodeCommit repositories in the AWS account`
- Operazione: `DescribeSlackChannelConfigurations` su `all AWS Chatbot clients in the AWS account`
- Operazione: `UpdateSlackChannelConfiguration` su `all AWS Chatbot clients in the AWS account`
- Operazione: `ListActionExecutions` su `all actions in all pipelines in the AWS account`
- Operazione: `GetFile` su `all files in all CodeCommit repositories in the AWS account unless otherwise tagged`

È possibile visualizzare queste azioni nella dichiarazione politica per il ruolo collegato al AWSService RoleForCodeStarNotifications servizio.

```
{
```

```
    "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"
        }
    ]
```

```
}
```

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato al servizio per le notifiche AWS CodeStar

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Puoi utilizzare la console Developer Tools o l' CreateNotificationRule API di AWS CLI o SDKs per creare una regola di notifica. Puoi anche chiamare direttamente l'API. Indipendentemente dal metodo utilizzato, il ruolo collegato ai servizi viene creato automaticamente.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Puoi utilizzare la console Developer Tools o l' CreateNotificationRule API di AWS CLI o SDKs per creare una regola di notifica. Puoi anche chiamare direttamente l'API. Indipendentemente dal metodo utilizzato, il ruolo collegato ai servizi viene creato automaticamente.

Modifica di un ruolo collegato al servizio per le notifiche AWS CodeStar

Dopo aver creato un ruolo collegato ai servizi, non è possibile modificarne il nome perché varie entità possono farvi riferimento. Puoi tuttavia utilizzare IAM per modificare la descrizione del ruolo. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Notifications AWS CodeStar

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. È necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare. Per quanto riguarda AWS CodeStar le notifiche, ciò significa eliminare tutte le regole di notifica che utilizzano il ruolo di servizio nell'account. AWS

> **Note**
>
> Se il servizio AWS CodeStar Notifiche utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare AWS CodeStar le risorse di notifica utilizzate da AWSService RoleForCodeStarNotifications

1. Apri la console AWS Developer Tools in https://console.aws.amazon.com/codesuite/impostazioni/notifiche.

   > **Note**
   >
   > Le regole di notifica si applicano alla AWS regione in cui vengono create. Se hai regole di notifica in più di una AWS regione, usa il selettore della regione per modificare le Regione AWS.

2. Scegli tutte le regole di notifica visualizzate nell'elenco, quindi seleziona Delete (Elimina).
3. Ripeti questi passaggi in tutte le AWS regioni in cui hai creato le regole di notifica.

Per utilizzare IAM per eliminare il ruolo collegato ai servizi

Utilizza la console o l' AWS CLI AWS Identity and Access Management API IAM per eliminare il ruolo AWSService RoleForCodeStarNotifications collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati al servizio AWS CodeStar Notifications

AWS CodeStar Notifications supporta l'utilizzo di ruoli collegati al servizio in tutte le AWS regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta AWS Regioni ed endpoint e Notifiche.AWS CodeStar

Utilizzo di ruoli collegati ai servizi per AWS CodeConnections

AWS CodeConnections utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS CodeConnections I ruoli collegati ai servizi sono predefiniti AWS CodeConnections e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS Questo ruolo viene creato la prima volta che crei una connessione. Non devi creare il ruolo.

Un ruolo collegato al servizio semplifica la configurazione AWS CodeConnections perché non è necessario aggiungere le autorizzazioni manualmente. AWS CodeConnections definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli.

AWS CodeConnections Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per eliminare un ruolo collegato al servizio, è necessario innanzitutto eliminarne le risorse correlate. In questo modo proteggi AWS CodeConnections le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi consulta Servizi AWS che funzionano con IAM.

> **Note**
>
> Sono disponibili azioni per le risorse create con il nuovo prefisso `codeconnections` di servizio. La creazione di una risorsa con il nuovo prefisso di servizio verrà utilizzata `codeconnections` nella risorsa ARN. Le azioni e le risorse per il prefisso del `codestar-connections` servizio rimangono disponibili. Quando si specifica una risorsa nella policy IAM, il prefisso del servizio deve corrispondere a quello della risorsa.

Autorizzazioni di ruolo collegate al servizio per AWS CodeConnections

AWS CodeConnections utilizza il ruolo AWSService RoleForGitSync collegato al servizio per utilizzare Git sync con repository basati su Git collegati.

Il ruolo AWSService RoleForGitSync collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `repository.sync.codeconnections.amazonaws.com`

La politica di autorizzazione dei ruoli denominata AWSGit SyncServiceRolePolicy consente di AWS CodeConnections completare le seguenti azioni sulle risorse specificate:

- Azione: concede agli utenti le autorizzazioni per creare connessioni a repository esterni basati su Git e per utilizzare la sincronizzazione Git con tali repository.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per AWS CodeConnections

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Crei il ruolo quando crei una risorsa per il tuo progetto sincronizzato con Git con l'API. CreateRepositoryLink

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account.

Modifica di un ruolo collegato ai servizi per AWS CodeConnections

Dopo aver creato un ruolo collegato ai servizi, non è possibile modificarne il nome perché varie entità possono farvi riferimento. Puoi tuttavia utilizzare IAM per modificare la descrizione del ruolo. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AWS CodeConnections

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. È necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare. Ciò significa eliminare tutte le connessioni che utilizzano il ruolo di servizio nel tuo account. AWS

> **Note**
>
> Se il AWS CodeConnections servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare AWS CodeConnections le risorse utilizzate da AWSService RoleForGitSync

1. Apri la console degli strumenti di sviluppo e scegli Impostazioni.
2. Scegli tutte le connessioni che appaiono nell'elenco, quindi seleziona Elimina.
3. Ripeti questi passaggi in tutte le AWS regioni in cui hai creato le connessioni.

Per utilizzare IAM per eliminare il ruolo collegato ai servizi

Utilizza la console o l' AWS CLI AWS Identity and Access Management API IAM per eliminare il ruolo AWSService RoleForGitSync collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi AWS CodeConnections

AWS CodeConnections supporta l'utilizzo di ruoli collegati al servizio in tutte le AWS regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint di AWS.

AWS politiche gestite per AWS CodeConnections

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consulta Policy gestite da AWSnella Guida per l'utente di IAM.

> **Note**
>
> Sono disponibili azioni per le risorse create con il nuovo prefisso `codeconnections` del servizio. La creazione di una risorsa con il nuovo prefisso di servizio verrà utilizzata `codeconnections` nella risorsa ARN. Le azioni e le risorse per il prefisso del `codestar-connections` servizio rimangono disponibili. Quando si specifica una risorsa nella policy IAM, il prefisso del servizio deve corrispondere a quello della risorsa.

AWS politica gestita: AWSGit SyncServiceRolePolicy

Non puoi collegarti AWSGit SyncServiceRolePolicy alle tue entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente di AWS CodeConnections eseguire azioni per tuo conto. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AWS CodeConnections.

Questa policy consente ai clienti di accedere ai repository basati su Git da utilizzare con le connessioni. I clienti accederanno a queste risorse dopo aver utilizzato l' CreateRepositoryLink API.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `codeconnections`: concede agli utenti le autorizzazioni per creare connessioni a repository esterni basati su Git.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AccessGitRepos",
   "Effect": "Allow",
   "Action": [
    "codestar-connections:UseConnection",
    "codeconnections:UseConnection"
   ],
   "Resource": [
    "arn:aws:codestar-connections:*:*:connection/*",
    "arn:aws:codeconnections:*:*:connection/*"
   ],
   "Condition": {
    "StringEquals": {
```

```
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   }
  ]
}
```

AWS CodeConnections aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS CodeConnections da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei AWS CodeConnections documenti.

Modifica	Descrizione	Data
AWSGitSyncServiceRolePolicy— Politica aggiornata	Il nome del servizio AWS CodeStar Connections è cambiato in AWS CodeConnections. È stata aggiornata la policy per le risorse ARNs che contengono entrambi i prefissi di servizio.	26 aprile 2024
AWSGitSyncServiceRolePolicy: nuova policy	AWS CodeStar Connections ha aggiunto la policy. Concede le autorizzazioni per consentire agli utenti delle connessioni di utilizzare Git sync con repository basati su Git collegati.	26 novembre 2023
AWS CodeConnections ha iniziato a tenere traccia delle modifiche	AWS CodeConnections ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	26 novembre 2023

Convalida della conformità per AWS CodeStar le notifiche e AWS CodeConnections

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, consulta la sezione AWS Servizi rientranti nell'ambito del programma di conformità. Per informazioni generali, consultare Programmi per la conformità di AWS.

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact.

La tua responsabilità di conformità quando utilizzi AWS CodeStar Notifiche AWS CodeConnections è determinata dalla sensibilità dei tuoi dati, dagli obiettivi di conformità della tua azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e la conformità. AWS
- AWS risorse per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il settore e la località in cui operi.
- AWS Config— Questo AWS servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente e consente AWS di verificare la conformità agli standard e alle best practice del settore della sicurezza.

Resilienza nelle AWS CodeStar notifiche e AWS CodeConnections

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta infrastruttura globale.AWS

- Le regole di notifica sono specifiche del Regione AWS luogo in cui vengono create. Se hai regole di notifica in più di una Regione AWS, usa il selettore Regione per rivedere le regole di notifica in Regione AWS ognuna di esse.
- AWS CodeStar Notifications si basa sugli argomenti di Amazon Simple Notification Service (Amazon SNS) come obiettivi delle regole di notifica. Le informazioni sugli argomenti Amazon SNS e sulle destinazioni delle regole di notifica potrebbero essere archiviate in una regione AWS diversa da quella in cui è stata configurata la regola di notifica.

Sicurezza dell'infrastruttura nelle AWS CodeStar notifiche e AWS CodeConnections

Come funzionalità di un servizio gestito, AWS CodeStar Notifications e C AWS CodeConnections sono protette dalle procedure di sicurezza di rete AWS globali descritte nel white paper Amazon Web Services: panoramica dei processi di sicurezza.

Utilizzi chiamate API AWS pubblicate per accedere alle AWS CodeStar notifiche e AWS CodeConnections attraverso la rete. I client devono supportare Transport Layer Security (TLS) 1.0 o versioni successive. I client devono, inoltre, supportare le suite di crittografia con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni supportano queste modalità.

Le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta che è associata a un'entità IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Traffico tra le risorse di AWS CodeConnections tra regioni

Se utilizzate la funzionalità di connessione per consentire la connessione delle vostre risorse, accettate e ci autorizzate a memorizzare ed elaborare le informazioni associate a tali risorse di connessione al di Regioni AWS fuori del Regioni AWS luogo in cui state utilizzando il servizio sottostante, esclusivamente in connessione e al solo scopo di fornire la connessione a tali risorse in Regioni diverse da quella in cui la risorsa è stata creata.

Per ulteriori informazioni, consulta Risorse globali in AWS CodeConnections.

> **Note**
>
> Se utilizzi la funzionalità di connessione per abilitare la connessione alle tue risorse in regioni che non richiedono prima l'attivazione, archivieremo ed elaboreremo le informazioni come descritto negli argomenti precedenti.
> Per le connessioni stabilite in regioni che devono essere prima abilitate, come la regione Europa (Milano), archivieremo ed elaboreremo le informazioni relative a tale connessione solo in quella regione.

Rinomina delle connessioni - Riepilogo delle modifiche

La funzionalità di connessione nella console Developer Tools consente di connettere le AWS risorse a repository di sorgenti di terze parti. Il 29 marzo 2024, AWS CodeStar Connections è stato rinominato in. AWS CodeConnections Le sezioni seguenti descrivono le diverse parti della funzionalità che sono state modificate con la ridenominazione e le azioni da intraprendere per garantire che le risorse continuino a funzionare correttamente.

Questo elenco non è completo. Mentre anche altre parti del prodotto sono cambiate, questi aggiornamenti sono i più rilevanti.

> **Note**
>
> Sono disponibili azioni per le risorse create con il nuovo prefisso `codeconnections` di servizio. La creazione di una risorsa con il nuovo prefisso di servizio verrà utilizzata `codeconnections` nella risorsa ARN. Le azioni e le risorse per il prefisso del `codestar-connections` servizio rimangono disponibili. Quando si specifica una risorsa nella policy IAM, il prefisso del servizio deve corrispondere a quello della risorsa.

> **Note**
>
> A partire dal 1° luglio 2024, la console crea connessioni con `codeconnections` la risorsa ARN. Le risorse con entrambi i prefissi di servizio continueranno a essere visualizzate nella console.

Prefisso di servizio rinominato

Le connessioni APIs utilizzano un prefisso di servizio rinominato:. codeconnections

Per utilizzare il nuovo prefisso nei comandi CLI, scarica la versione 2 di. AWS CLI Di seguito è riportato un comando di esempio con il prefisso aggiornato.

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

Azioni rinominate in IAM

Le azioni in IAM utilizzano il nuovo prefisso, come illustrato negli esempi seguenti:

```
codeconnections:CreateConnection
codeconnections:DeleteConnection
codeconnections:GetConnection
codeconnections:ListConnections
```

Nuova risorsa ARN

Le risorse Connections create avranno un nuovo ARN:

```
arn:aws:codeconnections:us-west-2:account-ID:connection/*
```

Politiche relative ai ruoli di servizio interessati

Per i seguenti servizi, le policy relative ai ruoli di servizio utilizzeranno il nuovo prefisso nelle dichiarazioni relative alle policy. È inoltre possibile aggiornare le politiche esistenti relative ai ruoli di servizio per utilizzare le nuove autorizzazioni, ma le politiche create con il vecchio prefisso continueranno a essere supportate.

- La politica relativa ai CodePipeline ruoli di servizio gestiti dal cliente
- La politica del ruolo AWS CodeStar di servizio `AWSCodeStarServiceRole`

Nuova CloudFormation risorsa

Per utilizzare le AWS CloudFormation risorse per le connessioni, sarà disponibile una nuova risorsa. La risorsa esistente sarà comunque supportata.

- La nuova AWS CloudFormationrisorsa è denominata AWS::CodeConnections: :Connection. Vedi AWS::CodeConnections::Connectionnella Guida per l' CloudFormation utente.
- La risorsa esistente AWS::CodeStarConnections: :Connection sarà ancora supportata. Vedi AWS::CodeStarConnections::Connectionnella Guida per l' CloudFormation utente.

Cronologia dei documenti

La tabella seguente descrive la documentazione per questa versione della console Strumenti di sviluppo.

- AWS CodeStar Versione dell'API per le notifiche: 2019-10-15
- AWS CodeConnections Versione API: 2023-12-01

Modifica	Descrizione	Data
Nuova chiave di condizione per il VPC host IDs	È possibile gestire l'accesso all'host per GitHub Enterpris e Server e gli host GitLab autogestiti utilizzando la chiave di VpcId condizione. La chiave di condizione consente di applicare le politiche relative alla creazione o all'aggio rnamento degli host per utilizzare un ID VPC specifica to. Per ulteriori informazi oni, consulta il riferimento all'autorizzazione Connections.	13 marzo 2025
Aggiungi il supporto per la condivisione di connessioni tra account	Puoi visualizzare e gestire le connessioni come risorse in AWS Resource Access Manager e puoi condividere le connessioni tra Account AWS. Per ulteriori informazi oni, consulta Condividere connessioni con Account AWS.	6 marzo 2025
Aggiornamento per aggiunger e e correggere informazioni	Le panoramiche e le informazi oni sulla risoluzione dei	9 dicembre 2024

che descrivono il funzionamento delle connessioni con gli account utente o le organizzazioni	problemi sono state aggiornate per descrivere correttamente il funzionamento delle connessioni con gli account utente o le organizzazioni. Vedi Come funzionano le connessioni, Come funzionano le connessioni con le organizzazioni e Configurazione della connessione e dell'host per i provider installati che supportano le organizzazioni. AWS CodeConnections	
Aggiornamento della politica gestita per le connessioni service-linked-role	La politica gestita per il ruolo collegato al servizio di utilizzare Git sync con i repository Git è stata aggiornata per le risorse con entrambi i prefissi di servizio. Per ulteriori informazioni, vedere Utilizzo di ruoli collegati ai servizi per e politiche gestite. AWS CodeConnections	26 aprile 2024
AWS CodeStar Connessioni rinominate in AWS CodeConnections	Ti presentiamo AWS CodeConnections, che consente di creare e gestire connessioni tra AWS risorse, come le pipeline in CodePipeline, verso provider Git di terze parti.	29 marzo 2024

Connessioni a GitLab ora supportate in CodeBuild	Support aggiunto CodeBuild per la configurazione delle connessioni a GitLab. Per ulteriori informazioni, consulta Integrazioni di prodotti e servizi con. AWS CodeConnections	27 marzo 2024
Support per la GitLab gestione automatica	Support aggiunto per la configurazione di connessioni e host per AWS le risorse con cui interagire con la gestione GitLab automatica. Per ulteriori informazioni, consulta Workflow per creare o aggiornare un host e Creare una connessione a GitLab gestione automatica.	28 dicembre 2023
Nuovi collegamenti ai repository e configurazioni di sincronizzazione per le connessioni	Sono state aggiunte informazioni sulla configurazione dei collegamenti ai repository e sulle configurazioni di sincronizzazione. Usa la configurazione di sincronizzazione per sincronizzare i contenuti da un repository Git per aggiornare le risorse AWS CloudFormation dello stack. Per maggiori informazioni, consulta Utilizzo di collegamento ai repository e Utilizzo delle configurazioni di sincronizzazione.	27 novembre 2023

Support per le connessioni service-linked-role	Aggiunto supporto per la configurazione delle connessioni per la sincronizzazione Git con i repository Git. Per ulteriori informazioni, vedere Utilizzo di ruoli collegati ai servizi AWS CodeConnections e Politiche gestite.	26 novembre 2023
Support per GitLab gruppi	Support aggiunto per la configurazione delle connessioni affinché AWS le risorse interagiscano con GitLab i gruppi. Per ulteriori informazioni, vedere Creare una connessione e Creare una connessione a GitLab.	15 settembre 2023
Nuovo tipo GitLab di provider	Ora puoi creare connessioni a GitLab. Per ulteriori informazioni, vedere Creare una connessione e Creare una connessione a GitLab.	10 agosto 2023
Nuovo tipo di destinazione per le regole di notifica	Ora puoi scegliere i client AWS Chatbot configurati per i canali Microsoft Teams come target per le regole di notifica. Per ulteriori informazioni, consulta Creazione di una regola di notifica e Utilizzo delle destinazioni delle regole di notifica.	17 maggio 2023

Le connessioni sono disponibili nella regione Europa (Milano)	Sono state aggiunte informazioni sulle connessioni nella regione Europa (Milano). Per ulteriori informazioni, consulta Traffico tra AWS CodeConnections le risorse tra le regioni.	17 maggio 2023
È stata aggiunta la risoluzione dei problemi di connessione con le autorizzazioni del repository	Quando crei una connessione a un repository in un' GitHub organizzazione, devi essere il proprietario dell' GitHub organizzazione. Per ulteriori informazioni, consulta Errore di connessione durante la connessione a GitHub.	29 agosto 2022
Aggiunte le informazioni per l'assegnazione di tag alle risorse host	È ora possibile taggare gli host utilizzando la console e la CLI. Per ulteriori informazioni, consulta Etichettare le risorse in AWS CodeConnections.	19 aprile 2021
Supporto degli endpoint VPC per le connessioni	Ora puoi utilizzare gli endpoint VPC con le connessioni. Per ulteriori informazioni, consulta AWS CodeConnections e interfaccia gli endpoint VPC ().AWS PrivateLink	24 novembre 2020
Tipi di provider Cloud nuovi GitHub ed GitHub Enterprise	Ora puoi creare connessioni a GitHub GitHub Enterprise Cloud. Per ulteriori informazioni, consulta Creare una connessione e Creare una connessione a GitHub.	30 settembre 2020

Sono stati aggiunti il tipo di provider e le risorse host di GitHub Enterprise Server	A questa guida sono state aggiunte informazioni sulla risorsa host per le connessioni. È ora possibile creare connessioni a GitHub Enterprise Server. Per ulteriori informazioni consulta Creazione di una connessione e Utilizzo degli host. Questa è la versione di disponibilità generale della funzionalità di connessione nella Guida per l'utente della console degli strumenti di sviluppo.	29 giugno 2020

Aggiunte le informazioni per l'utilizzo delle connessioni e l'aggiunta di tag	A questa guida sono state aggiunte informazioni sulla funzionalità di connessione nella console. È possibile visualizzare concetti, passaggi per iniziare, un riferimento per le autorizzazioni, incluse policy di esempio e passaggi per creare, visualizzare e taggare le connessioni. Per ulteriori informazioni, consulta Cosa sono le connessioni, Concetti relativi alle connessioni, Guida introduttiva alle connessioni, Creazione di una connessione, Etichette alle risorse AWS CodeConnections, Sicurezza, Quote per le connessioni, Risoluzione dei problemi e Chiamate AWS CodeConnections API con AWS CloudTrail. Per visualizzare un elenco di azioni aggiuntive del provider (solo azioni relative alle autorizzazioni), consulta Azioni per. ProviderType	28 giugno 2020
Nuovo tipo di destinazione per le regole di notifica	Ora puoi scegliere i client AWS Chatbot configurati per i canali Slack come target per le regole di notifica. Per ulteriori informazioni, consulta Creazione di una regola di notifica e Utilizzo delle destinazioni delle regole di notifica.	2 aprile 2020

Aggiunte notifiche su eventi aggiuntivi AWS CodeCommit	È ora possibile configurare le notifiche per gli eventi relativi alle approvazioni delle richieste pull. Per ulteriori informazioni, consulta Events for notification rules on repository e Working with pull request in CodeCommit.	10 febbraio 2020
Notifiche disponibili in due aree aggiuntive AWS	La console Strumenti di sviluppo supporta ora le notifiche in Medio Oriente (Bahrein) e Asia Pacifico (Hong Kong). Per ulteriori informazioni, consulta AWS CodeStar Notifiche in Riferimenti generali di AWS.	5 febbraio 2020
Aggiunto il supporto per argomenti Amazon SNS crittografati	Aggiunte indicazioni per l'utilizzo di argomenti Amazon SNS crittografati come destinazioni di notifica. Per ulteriori informazioni, consulta l'argomento relativo alla Configurazione degli argomenti Amazon SNS per le notifiche .	4 febbraio 2020

Le notifiche possono includere informazioni sui tag di sessione per CodeCommit	Le notifiche di ora CodeCommit possono contenere informazioni sull'identità dell'utente, come un nome visualizzato o un indirizzo e-mail, tramite l'uso di tag di sessione. Per ulteriori informazioni, consulta Concetti e utilizzo dei tag per fornire informazioni sull'identità CodeCommit.	19 dicembre 2019
Versione iniziale	Questa è la versione iniziale della Guida per l'utente della console per gli strumenti di sviluppo.	5 novembre 2019

AWS Glossario

Per la AWS terminologia più recente, consultate il AWS glossario nella sezione Reference.Glossario AWS

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.