Guida per l'utente

AWS CodeStar

AWS CodeStar: Guida per l'utente

Table of Contents

Il 31 luglio 2024, Amazon Web Services (AWS) interromperà il supporto per la creazione e la visualizzazione AWS CodeStar di progetti. Dopo il 31 luglio 2024, non potrai più accedere alla AWS CodeStar console o creare nuovi progetti. Tuttavia, le AWS risorse create da AWS CodeStar, inclusi gli archivi di origine, le pipeline e le build, non saranno influenzate da questa modifica e continueranno a funzionare. AWS CodeStar Le connessioni e AWS CodeStar le notifiche non saranno influenzate da questa interruzione.

Se desideri monitorare il lavoro, sviluppare codice e creare, testare e distribuire le tue applicazioni, Amazon CodeCatalyst offre un processo introduttivo semplificato e funzionalità aggiuntive per gestire i tuoi progetti software. Scopri di più sulle funzionalità e sui prezzi di Amazon CodeCatalyst.

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.

Che cos'è AWS CodeStar?

AWS CodeStar è un servizio basato su cloud per la creazione, la gestione e l'utilizzo di progetti di sviluppo software su. AWSÈ possibile sviluppare, creare e distribuire rapidamente applicazioni AWS con un progetto. AWS CodeStar Un AWS CodeStar progetto crea e integra AWS servizi per la toolchain di sviluppo del progetto. A seconda del modello di AWS CodeStar progetto scelto, tale toolchain potrebbe includere il controllo del codice sorgente, la compilazione, l'implementazione, server virtuali o risorse serverless e altro ancora. AWS CodeStar gestisce anche le autorizzazioni richieste per gli utenti del progetto (chiamati membri del team). Aggiungendo utenti come membri del team a un AWS CodeStar progetto, i proprietari del progetto possono concedere in modo rapido e semplice a ciascun membro del team l'accesso appropriato al progetto e alle relative risorse.

Argomenti

Cosa posso fare con? AWS CodeStar

Puoi utilizzarlo AWS CodeStar per aiutarti a configurare lo sviluppo delle tue applicazioni nel cloud e a gestirlo da un'unica dashboard centralizzata. Nello specifico, puoi eseguire le operazioni seguenti:

- Avvia nuovi progetti software AWS in pochi minuti utilizzando modelli per applicazioni Web, servizi Web e altro ancora: AWS CodeStar include modelli di progetto per vari tipi di progetto e linguaggi di programmazione. Poiché AWS CodeStar si occupa della configurazione, tutte le risorse del progetto sono configurate per funzionare insieme.
- Gestire l'accesso al progetto per il tuo team: AWS CodeStar offre una console centralizzata per assegnare ai membri del team di progetto i ruoli necessari per accedere a strumenti e risorse. Queste autorizzazioni vengono applicate automaticamente a tutti i AWS servizi utilizzati nel progetto, quindi non è necessario creare o gestire politiche IAM complesse.
- Visualizza, gestisci e collabora ai tuoi progetti in un unico posto: AWS CodeStar include una dashboard del progetto che fornisce una visione generale del progetto, della sua toolchain e degli eventi importanti. Puoi monitorare le attività più recenti del progetto, ad esempio commit recenti del codice, e tenere traccia dello stato delle modifiche al codice, dei risultati della compilazione e le distribuzioni, tutto da un'unica pagina Web. Puoi monitorare le attività del progetto tramite un unico pannello di controllo e approfondire i problemi da analizzare.

- Iterare in modo rapido con tutti gli strumenti di cui hai bisogno: AWS CodeStar include una toolchain di sviluppo integrata per il progetto. I membri del team possono effettuare il push del codice e le modifiche vengono distribuite automaticamente. L'integrazione con il monitoraggio dei problemi permette ai membri del team di tenere traccia delle operazioni successive da effettuare. Potrai collaborare con il team in modo più rapido ed efficiente in tutte le fasi della distribuzione del codice.

Come posso iniziare? AWS CodeStar

Per iniziare con AWS CodeStar:

1. Preparati all'uso AWS CodeStar seguendo la procedura riportata di seguitoConfigurazione AWS CodeStar.
2. Sperimenta AWS CodeStar seguendo i passaggi del Guida introduttiva con AWS CodeStar tutorial.
3. Condividi il tuo progetto con altri sviluppatori seguendo le fasi descritte in Aggiungere membri del team a un AWS CodeStar progetto .
4. Integra il tuo ambiente IDE preferito seguendo le fasi descritte in Usa un IDE con AWS CodeStar.

Configurazione AWS CodeStar

Prima di iniziare a utilizzare AWS CodeStar, è necessario completare i seguenti passaggi.

Argomenti

Passaggio 1: Creare un account

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.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la 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 Console di gestione AWScome 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 .

Fase 2: Creare il ruolo AWS CodeStar di servizio

Crea un ruolo di servizio che viene utilizzato per concedere AWS CodeStar l'autorizzazione ad amministrare AWS le risorse e le autorizzazioni IAM per tuo conto. Il ruolo del servizio deve essere creato solo una volta.

> **Important**
>
> Per creare un ruolo del servizio, è necessario accedere come utente amministrativo (o account radice). Per ulteriori informazioni, consulta Creazione del primo utente e gruppo IAM.

1. Apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.
2. Scegliere Start project (Avvia progetto).

   Se la voce Start project (Avvia progetto) non è visualizzata e si viene invece indirizzati alla pagina dell'elenco progetti, il ruolo del servizio è stato creato.
3. In Create service role (Crea ruolo del servizio) scegliere Yes, create role (Sì, crea ruolo).
4. Uscire dalla procedura guidata. Sarà possibile tornare in questo punto in seguito.

Fase 3: Configurare le autorizzazioni IAM per l'utente

Oltre all'utente amministrativo, puoi utilizzarlo AWS CodeStar come utente IAM, utente federato, utente root o ruolo assunto. Per informazioni su cosa è AWS CodeStar possibile fare per gli utenti IAM rispetto agli utenti federati, consulta. Ruoli AWS CodeStar IAM

Se non hai configurato alcun utente IAM, consulta Utente IAM.

Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .
- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente IAM.

Fase 4: creare una coppia di EC2 chiavi Amazon per AWS CodeStar i progetti

Molti AWS CodeStar progetti utilizzano AWS CodeDeploy o AWS Elastic Beanstalk distribuiscono codice su EC2 istanze Amazon. Per accedere alle EC2 istanze Amazon associate al tuo progetto, crea una coppia di EC2 chiavi Amazon per il tuo utente IAM. Il tuo utente IAM deve disporre delle autorizzazioni per creare e gestire EC2 le chiavi Amazon (ad esempio, l'autorizzazione per eseguire `ec2:ImportKeyPair` azioni `ec2:CreateKeyPair` e). Per ulteriori informazioni, consulta Amazon EC2 Key Pairs.

Passaggio 5: apri la AWS CodeStar console

Accedi a Console di gestione AWS, quindi apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.

Fasi successive

Congratulazioni, la configurazione è stata completata. Per iniziare a lavorare con AWS CodeStar, vediGuida introduttiva con AWS CodeStar.

Guida introduttiva con AWS CodeStar

In questo tutorial, si usa AWS CodeStar per creare un'applicazione web. Questo progetto include il codice di esempio in un repository di origine, una toolchain per la distribuzione continua e un pannello di controllo del progetto, dove è possibile visualizzare e monitorare il progetto.

Seguendo la procedura, è possibile:

- Crea un progetto in AWS CodeStar.
- Esplorare il progetto.
- Eseguire il commit di una modifica al software.
- Osservare la distribuzione automatica della modifica al codice.
- Permettere ad altri utenti di lavorare al progetto.
- Eliminare le risorse di progetto quando non sono più necessarie.

> **Note**
>
> Se non è già stato fatto, completare prima la procedura indicata in Configurazione AWS CodeStar, inclusi i passi descritti in Fase 2: Creare il ruolo AWS CodeStar di servizio. Devi aver effettuato l'accesso con un account che sia un utente amministrativo in IAM. Per creare un progetto, devi accedere Console di gestione AWS utilizzando un utente IAM che dispone della **`AWSCodeStarFullAccess`**policy.

Argomenti

- Fasi successive
- Tutorial: creare e gestire un progetto serverless in AWS CodeStar
- Tutorial: crea un progetto AWS CodeStar con AWS CLI
- Tutorial: crea un progetto Alexa Skill in AWS CodeStar
- Tutorial: creare un progetto con un repository GitHub di sorgenti

Fase 1: Creare un AWS CodeStar progetto

In questo passaggio, si crea un progetto di sviluppo software JavaScript (Node.js) per un'applicazione Web. Si utilizza un modello di AWS CodeStar progetto per creare il progetto.

> **Note**
>
> Il modello di AWS CodeStar progetto utilizzato in questo tutorial utilizza le seguenti opzioni:
>
> - Application category (Categoria applicazione): applicazione web
> - Programming language (Linguaggio di programmazione): Node.js
> - AWS Servizio: Amazon EC2
>
> Scegliendo opzioni differenti, il percorso potrebbe non corrispondere a quello descritto in questa esercitazione.

Per creare un progetto in AWS CodeStar

1. Accedere a Console di gestione AWS, quindi aprire la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.

   Assicurati di aver effettuato l'accesso alla AWS regione in cui desideri creare il progetto e le relative risorse. Ad esempio, per creare un progetto negli Stati Uniti orientali (Ohio), assicurati di aver selezionato quella AWS regione. Per informazioni sulle AWS regioni in cui AWS CodeStar è disponibile, consulta Regioni ed endpoint nella Guida AWS generale.
2. Nella AWS CodeStarpagina, scegli Crea progetto.
3. Nella pagina Scegli un modello di progetto, scegli il tipo di progetto dall'elenco dei modelli di AWS CodeStar progetto. Puoi utilizzare la barra dei filtri per ridurre la scelta. Ad esempio, per un progetto di applicazione Web scritto in Node.js da distribuire su EC2 istanze Amazon, seleziona

le caselle di EC2 controllo Applicazione Web, Node.js e Amazon. Quindi scegli tra i modelli disponibili per quel set di opzioni.

Per ulteriori informazioni, consulta AWS CodeStar Modelli di progetto.

4. Scegli Next (Successivo).
5. Nel campo di immissione del testo del nome del progetto, inserisci un nome per il progetto, ad esempio. `My First Project` In Project ID, l'ID del progetto deriva dal nome di questo progetto, ma è limitato a 15 caratteri.

   Ad esempio, l'ID di default per un progetto denominato `My First Project` è `my-first-projec`. Questo ID di progetto è la base per i nomi di tutte le risorse associate al progetto. AWS CodeStar utilizza questo ID di progetto come parte dell'URL per il repository di codice e per i nomi dei ruoli e delle politiche di accesso di sicurezza correlati in IAM. Dopo la creazione del progetto. l'ID del progetto non può essere modificato. Per modificare l'ID del progetto prima di creare il progetto, in ID progetto, inserisci l'ID che desideri utilizzare.

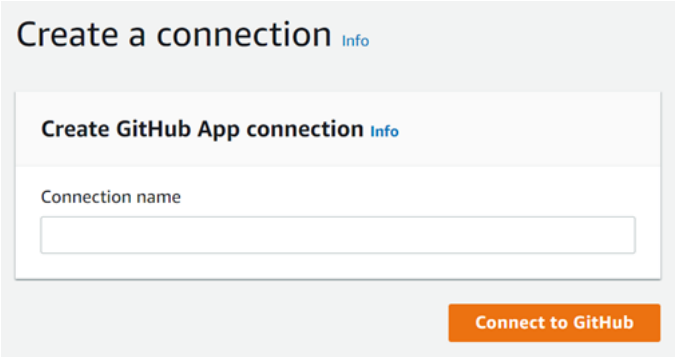
   Per informazioni sui limiti imposti ai nomi e ai progetti dei progetti IDs, consultaLimiti in AWS CodeStar.

   > **Note**
   >
   > Il progetto IDs deve essere unico per il tuo AWS account in una AWS regione.

6. Scegli il fornitore del repository, AWS CodeCommitoppure GitHub.
7. Se hai scelto AWS CodeCommit, per Nome del repository, accetta il nome del AWS CodeCommit repository predefinito o inseriscine uno diverso. Quindi vai avanti al passaggio 9.
8. Se hai scelto GitHub, devi scegliere o creare una risorsa di connessione. Se hai una connessione esistente, selezionala nel campo di ricerca. Altrimenti, crea subito una nuova connessione. Scegli Connect a GitHub.

   Viene visualizzata la pagina Crea una connessione.

   > **Note**
   >
   > Per creare una connessione, è necessario disporre di un GitHub account. Se stai creando una connessione per un'organizzazione, devi essere il proprietario dell'organizzazione.



a. In Crea connessione all' GitHub app, nel campo di testo di immissione del nome della connessione, inserisci un nome per la connessione. Scegli Connect a GitHub.

   La GitHub pagina Connect to visualizza e mostra il campo GitHub App.

b. In GitHub App, scegli l'installazione di un'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.

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

> **Note**
>
> 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.

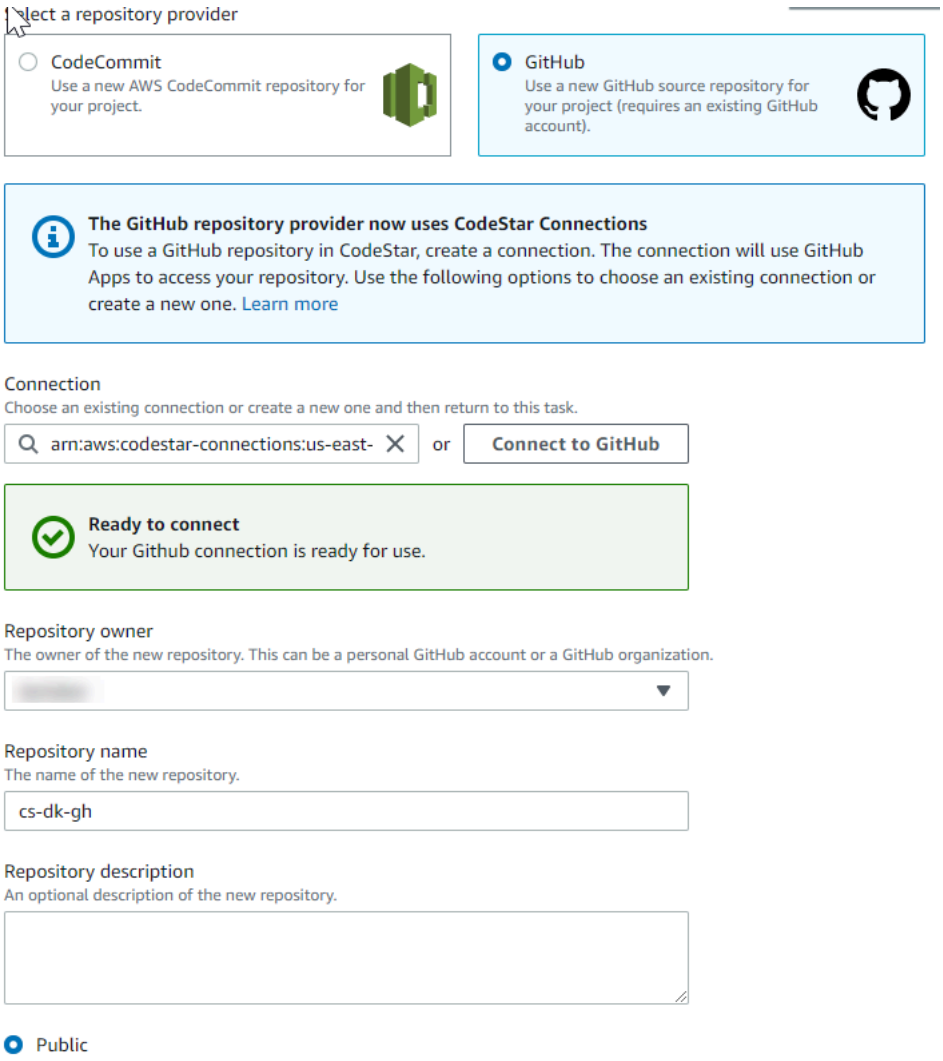
d. Se viene visualizzata la pagina Conferma la password per continuare, inserisci GitHub la password, quindi scegli Accedi.

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

f. Nella GitHub pagina Connect to, l'ID di installazione per la nuova installazione viene visualizzato nel campo di immissione di testo GitHub App.

Dopo aver creato la connessione, nella pagina di CodeStar creazione del progetto viene visualizzato il messaggio Ready to connect.

> **Note**
>
> Puoi visualizzare la tua connessione in Impostazioni nella console Developer Tools. Per ulteriori informazioni, consulta Guida introduttiva alle connessioni.



g. Per il proprietario del repository, scegli l' GitHub organizzazione o il tuo account personale. GitHub

h. Per Nome del repository, accetta il nome del GitHub repository predefinito o inseriscine uno diverso.

i. Scegli Pubblico o Privato.

> **Note**
>
> Per utilizzarlo AWS Cloud9 come ambiente di sviluppo, devi scegliere Pubblico.

j. (Facoltativo) Per la descrizione del repository, inserite una descrizione per il GitHub repository.

> **Note**
>
> Se scegli un modello di progetto Alexa Skill, devi collegare un account sviluppatore Amazon. Per ulteriori informazioni su come lavorare con i progetti Alexa Skill, consulta. Tutorial: crea un progetto Alexa Skill in AWS CodeStar

9. Se il tuo progetto è distribuito su EC2 istanze Amazon e desideri apportare modifiche, configura le EC2 istanze Amazon in Amazon Configuration. EC2 Ad esempio, è possibile scegliere tra i tipi di istanze disponibili per il progetto.

> **Note**
>
> I diversi tipi di EC2 istanze Amazon offrono diversi livelli di potenza di calcolo e possono avere costi associati diversi. Per ulteriori informazioni, consulta i tipi di EC2 istanze Amazon e EC2 i prezzi di Amazon.
> Se disponi di più di un cloud privato virtuale (VPC) o più sottoreti create in Amazon Virtual Private Cloud, puoi anche scegliere il VPC e la sottorete da utilizzare. Tuttavia, se scegli un tipo di EC2 istanza Amazon che non è supportato su istanze dedicate, non puoi scegliere un VPC la cui tenancy dell'istanza è impostata su Dedicato.
> Per ulteriori informazioni, consulta What Is Amazon VPC? e nozioni di base sulle istanze dedicate.

In Coppia di chiavi, scegli la coppia di EC2 chiavi Amazon in cui hai creatoFase 4: creare una coppia di EC2 chiavi Amazon per AWS CodeStar i progetti. Seleziona Riconosco di avere accesso al file della chiave privata.

10. Scegli Next (Successivo).
11. Esaminare le risorse e i dettagli di configurazione.
12. Scegli Next (Avanti) oppure Create project (Crea progetto). (L'opzione visualizzata dipende dal modello di progetto).

    Potrebbero essere necessari alcuni minuti per creare il progetto, incluso il repository.
13. Dopo che il progetto ha un repository, puoi utilizzare la pagina Repository per configurarne l'accesso. Utilizza i link nei passaggi successivi per configurare un IDE, impostare il monitoraggio dei problemi o aggiungere membri del team al progetto.

Passaggio 2: aggiungi le informazioni di visualizzazione per il tuo profilo AWS CodeStar utente

Al momento della creazione di un progetto, l'autore è aggiunto al team di progetto come proprietario. Se è la prima volta che lo usi AWS CodeStar, ti viene chiesto di fornire:

- Il nome da mostrare agli altri utenti.
- L'indirizzo e-mail da mostrare agli altri utenti.

Queste informazioni vengono utilizzate nel tuo profilo AWS CodeStar utente. I profili utente non sono specifici del progetto, ma sono limitati a una AWS regione. È necessario creare un profilo utente in ogni AWS regione in cui si appartiene ai progetti. Ogni profilo può contenere informazioni differenti, se si preferisce.

Inserire un nome utente e l'indirizzo e-mail, quindi scegliere Next (Avanti).

> **Note**
>
> Questo nome utente e indirizzo e-mail vengono utilizzati nel tuo profilo AWS CodeStar utente. Se il progetto utilizza risorse esterne AWS (ad esempio, un GitHub repository o problemi in Atlassian JIRA), tali fornitori di risorse potrebbero avere i propri profili utente, con nomi utente e indirizzi e-mail diversi. Per ulteriori informazioni, consultare la documentazione messa a disposizione dal fornitore delle risorse.

Fase 3: visualizzazione del progetto

Nella pagina AWS CodeStar del progetto, tu e il tuo team potete visualizzare lo stato delle risorse del progetto, compresi gli ultimi impegni assegnati al progetto, lo stato della pipeline di distribuzione continua e le prestazioni delle istanze. Per visualizzare ulteriori informazioni su ognuna di queste risorse, scegli la pagina corrispondente dalla barra di navigazione.

Nel nuovo progetto, la barra di navigazione contiene le seguenti pagine:

- La pagina Panoramica contiene informazioni sull'attività del progetto, sulle risorse del progetto e sui `README` contenuti del progetto.
- La pagina IDE consente di collegare il progetto a un ambiente di sviluppo integrato (IDE) per modificare, testare e inviare modifiche al codice sorgente. Contiene istruzioni per la configurazione IDEs di entrambi i AWS CodeCommit repository GitHub e informazioni sugli ambienti. AWS Cloud9
- La pagina Repository mostra i dettagli del repository, tra cui il nome, il provider, la data dell'ultima modifica e il clone. URLs Puoi anche visualizzare le informazioni sul commit più recente e visualizzare e creare richieste pull.
- La pagina Pipeline mostra le informazioni CI/CD sulla pipeline. È possibile visualizzare i dettagli della pipeline come il nome, l'azione più recente e lo stato. Puoi vedere la cronologia della pipeline e rilasciare una modifica. Puoi anche visualizzare lo stato dei singoli passaggi della tua pipeline.
- La pagina Monitoraggio mostra Amazon EC2 o le AWS Lambda metriche a seconda della configurazione del progetto. Ad esempio, mostra l'utilizzo della CPU di tutte EC2 le istanze Amazon distribuite da AWS Elastic Beanstalk o le CodeDeploy risorse nella tua pipeline. Nei progetti che lo utilizzano AWS Lambda, visualizza le metriche di invocazione e di errore per la funzione Lambda. Queste informazioni sono visualizzate con cadenza oraria. Se hai utilizzato il modello di AWS CodeStar progetto consigliato per questo tutorial, dovresti notare un notevole picco di attività non appena l'applicazione viene distribuita per la prima volta in quelle istanze. È possibile aggiornare il monitoraggio per visualizzare le modifiche dello stato dell'istanza. Questo potrebbe aiutare a individuare i problemi o la necessità di risorse aggiuntive.
- La pagina Problemi serve per integrare il AWS CodeStar progetto con un progetto Atlassian JIRA. La configurazione di questo riquadro permette all'utente a al suo team di progetto di monitorare il problemi JIRA dal pannello di controllo del progetto.

Il riquadro di navigazione sul lato sinistro della console consente di navigare tra le pagine Progetto, Team e Impostazioni.

Fase 4: Applica una modifica

Per prima cosa, dai un'occhiata all'applicazione di esempio inclusa nel tuo progetto. Scopri l'aspetto dell'applicazione scegliendo Visualizza applicazione da qualsiasi punto della navigazione del progetto. L'applicazione web di esempio verrà visualizzata in una nuova finestra o scheda del browser. Questo è l'esempio di progetto che è AWS CodeStar stato creato e distribuito.

Se vuoi dare un'occhiata al codice, nella barra di navigazione scegli Repository. Scegli il link sotto Nome del deposito e il repository del tuo progetto si aprirà in una nuova scheda o finestra. Leggere il contenuto del file README del repository (`README.md`) e sfogliare il contenuto dei file.

In questa fase, si apporta una modifica al codice e quindi si applica la modifica al repository. Ci sono diversi modi per farlo:

- Se il codice del progetto è archiviato in un GitHub repository CodeCommit or, puoi utilizzarlo AWS Cloud9 per lavorare con il codice direttamente dal tuo browser web, senza installare alcun strumento. Per ulteriori informazioni, consulta Crea un AWS Cloud9 ambiente per un progetto.
- Se il codice del progetto è archiviato in un CodeCommit repository e hai installato Visual Studio o Eclipse, puoi usare AWS Toolkit for Visual Studio o AWS Toolkit for Eclipse per connetterti più facilmente al codice. Per ulteriori informazioni, consulta Usa un IDE con AWS CodeStar. Se non si dispone di Visual Studio o Eclipse, installare un client Git e seguire le istruzioni che saranno illustrate più avanti in questa fase.
- Se il codice del progetto è archiviato in un GitHub repository, puoi utilizzare gli strumenti del tuo IDE per la connessione a. GitHub
  - Per Visual Studio, puoi usare strumenti come l' GitHub estensione per Visual Studio. Per ulteriori informazioni, consulta la pagina Panoramica sul sito Web GitHub Extension for Visual Studio e Getting Started with GitHub for Visual Studio sul GitHub sito Web.
  - Per Eclipse, puoi usare uno strumento come EGit Eclipse. Per ulteriori informazioni, consulta la EGitdocumentazione sul sito Web. EGit
  - Per altre informazioni IDEs, consultate la documentazione del vostro IDE.
- In caso di utilizzo di altri tipi di repository del codice, consulta la documentazione specifica del provider del repository.

Le seguenti istruzioni mostrano come apportare una piccola modifica all'esempio.

Per impostare il computer per eseguire il commit delle modifiche (utente IAM)

> **Note**
>
> In questa procedura, ipotizziamo che il codice del progetto venga memorizzato in un repository CodeCommit. In caso di utilizzo di altri tipi di repository del codice, consulta la documentazione del provider del repository e quindi passa direttamente alla procedura successiva, Per clonare il repository del progetto e apportare una modifica.
> Se il codice è memorizzato CodeCommit e lo stai già utilizzando CodeCommit o hai usato la AWS CodeStar console per creare un ambiente di AWS Cloud9 sviluppo per il progetto, non hai bisogno di ulteriori configurazioni. Passa direttamente alla procedura successiva, Per clonare il repository del progetto e apportare una modifica.

1. Installare Git sul computer locale.
2. Accedi Console di gestione AWS e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.

   Accedi come utente IAM che utilizzerà le credenziali Git per le connessioni al repository AWS CodeStar del tuo progetto. CodeCommit
3. Nella console IAM, nel pannello di navigazione, scegli Utenti e dall'elenco degli utenti, scegli il tuo utente IAM.
4. Nella pagina dei dettagli utente, scegli la scheda Credenziali di sicurezza e, in Credenziali Git HTTPS per CodeCommit, scegli Genera.

   > **Note**
   >
   > Non puoi scegliere le tue credenziali di accesso per le credenziali Git. Per ulteriori informazioni, consulta Utilizzare credenziali Git e HTTPS con CodeCommit.
5. Copia le credenziali di accesso che IAM ha generato per te. È possibile scegliere Show (Mostra) e quindi copiare e incollare queste informazioni in un file sicuro sul computer locale, oppure è possibile scegliere Download credentials (Scarica credenziali) per scaricare queste informazioni sotto forma di file .CSV. Queste informazioni sono necessarie per connettersi a CodeCommit.

   Dopo aver salvato le credenziali, scegliere Close (Chiudi).

> **Important**
>
> Questa è la tua unica possibilità per salvare le credenziali di accesso. Se non le salvi, puoi copiare il nome utente dalla console IAM, ma non puoi cercare la password. Sarà quindi necessario reimpostare la password e salvarla.

Per impostare il computer per eseguire il commit delle modifiche (utente federato)

È possibile utilizzare la console per caricare i file sul repository, oppure è possibile usare Git per connettersi dal proprio computer locale. Se si sta usando l'accesso federato, seguire questi passaggi per usare Git per connettersi e clonare il repository dal proprio computer locale.

> **Note**
>
> In questa procedura, ipotizziamo che il codice del progetto venga memorizzato in un repository CodeCommit. In caso di utilizzo di altri tipi di repository del codice, consulta la documentazione del provider del repository e quindi passa direttamente alla procedura successiva, Per clonare il repository del progetto e apportare una modifica.

1. Installare Git sul computer locale.
2. Installa il AWS CLI.
3. Configurare le credenziali di sicurezza temporanee per un utente federato. Per informazioni, consulta Accesso temporaneo ai CodeCommit repository. Le credenziali temporanee consistono di:

   - AWS chiave di accesso
   - AWS chiave segreta
   - Token di sessione

   Per ulteriori informazioni sulle credenziali temporanee, vedere Autorizzazioni per. GetFederationToken
4. Connect al repository utilizzando l'helper delle AWS CLI credenziali. Per informazioni, consulta Procedura di configurazione per le connessioni HTTPS ai CodeCommit repository su Linux, macOS o Unix con l'helper delle credenziali AWS CLI o Procedura di configurazione per le

connessioni HTTPS ai CodeCommit repository su Windows con l'helper delle credenziali CLI AWS

5. L'esempio seguente mostra come connettersi a un repository e inviarvi un commit. CodeCommit

Esempio: per copiare il repository del progetto ed effettuare una modifica

> **Note**
>
> Questa procedura mostra come clonare il repository del codice del progetto sul computer, modificare il file `index.html` del progetto e quindi applicare la modifica sul repository remoto. In questa procedura, supponiamo che il codice del tuo progetto sia archiviato in un CodeCommit repository e che tu stia utilizzando un client Git dalla riga di comando. Per gli altri tipi di repository di codice o di strumenti, consulta la documentazione del relativo provider per capire come clonare il repository, modificare il file e quindi applicare la modifica al codice.

1. Se hai utilizzato la AWS CodeStar console per creare un ambiente di AWS Cloud9 sviluppo per il progetto, apri l'ambiente di sviluppo e vai al passaggio 3 di questa procedura. Per aprire l'ambiente di sviluppo, consulta Aprire un AWS Cloud9 ambiente per un progetto.

   Con il progetto aperto nella AWS CodeStar console, nella barra di navigazione, scegli Repository. In Clone URL, scegli il protocollo per il tipo di connessione che hai impostato CodeCommit, quindi copia il link. Ad esempio, se hai seguito i passaggi della procedura precedente per configurare le credenziali Git per CodeCommit, scegli HTTPS.
2. Sul computer locale, aprire un terminale o una finestra a riga di comando e spostarsi in una cartella temporanea. Eseguire il comando git clone per clonare il repository sul computer. Incollare il collegamento copiato. Ad esempio, per CodeCommit utilizzare HTTPS:

   ```
   git clone https://git-codecommit.us-east-2.amazonaws.com/v1/repos/my-first-projec
   ```

   La prima volta che ti connetti, ti vengono richieste le credenziali di accesso per il repository. Per CodeCommit, inserisci le credenziali di accesso Git che hai scaricato nella procedura precedente.
3. Spostarsi nella directory clonata sul computer e sfogliare i contenuti.
4. Aprire il file `index.html` (nella cartella pubblica) e apportare una modifica al file. Ad esempio, aggiungere un paragrafo dopo il tag <H2>, ad esempio:

```
<P>Hello, world!</P>
```

Salvare il file.

5. Tramite il terminale o il prompt dei comandi aggiungere il file modificato e quindi applicare la modifica:

```
git add index.html
git commit -m "Making my first change to the web app"
git push
```

6. Nella pagina Repository, visualizza le modifiche in corso. La cronologia dei commit eseguiti sul repository dovrebbe risultare aggiornata con l'ultimo commit, incluso il messaggio di commit. Nella pagina Pipeline, puoi vedere la pipeline che raccoglie le modifiche nel repository e inizia a crearle e distribuirle. Dopo aver distribuito l'applicazione Web, puoi scegliere Visualizza applicazione per visualizzare le modifiche.

> **Note**
>
> Se per qualsiasi fase della pipeline viene visualizzata l'etichetta Failed (Non riuscito), consulta quanto segue per facilitare la risoluzione dei problemi:
>
> - Per la fase Source, consulta Risoluzione dei problemi AWS CodeCommit nella Guida per l'AWS CodeCommit utente.
> - Per la fase di compilazione, consulta Risoluzione dei problemi AWS CodeBuild nella Guida AWS CodeBuild per l'utente.
> - Per la fase di implementazione, consulta Risoluzione dei problemi AWS CloudFormation nella Guida per l'AWS CloudFormation utente.
> - Per altri problemi, consulta Risoluzione dei problemi AWS CodeStar.

Fase 5: Aggiungere altri membri del team

Ogni AWS CodeStar progetto è già configurato con tre AWS CodeStar ruoli. Ogni ruolo fornisce il proprio livello di accesso al progetto e le proprie risorse:

- Proprietario: può aggiungere o rimuovere i membri del team di progetto, modificare il pannello di controllo ed eliminare il progetto.
- Collaboratore: può modificare la dashboard del progetto e contribuire al codice se il codice è memorizzato in CodeCommit, ma non può aggiungere o rimuovere membri del team o eliminare il progetto. Questo è il ruolo che dovresti scegliere per la maggior parte dei membri del team in un AWS CodeStar progetto.
- Visualizzatore: può visualizzare la dashboard del progetto, il codice del progetto (se il codice è memorizzato in CodeCommit) e lo stato del progetto, ma non può spostare, aggiungere o rimuovere riquadri dalla dashboard del progetto.

> **Important**
>
> Se il progetto utilizza risorse esterne AWS (ad esempio, un GitHub repository o problemi in Atlassian JIRA), l'accesso a tali risorse è controllato dal fornitore di risorse, non. AWS CodeStar Per ulteriori informazioni, consultare la documentazione messa a disposizione dal fornitore delle risorse.
> Chiunque abbia accesso a un AWS CodeStar progetto potrebbe essere in grado di utilizzare la AWS CodeStar console per accedere a risorse esterne AWS ma correlate al progetto. AWS CodeStar non consente ai membri del team di progetto di partecipare a nessun ambiente di AWS Cloud9 sviluppo correlato a un progetto. Per consentire a un membro del team di partecipare a un ambiente condiviso, consulta Condividi un AWS Cloud9 ambiente con un membro del team di progetto.

Per ulteriori informazioni sui team e sui ruoli dei progetti, consulta Lavorare con AWS CodeStar i team.

Per aggiungere un membro del team a un AWS CodeStar progetto (console)

1. Apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.
2. Scegli Progetti dal pannello di navigazione e scegli il tuo progetto.

3. Nel riquadro di navigazione laterale del progetto, scegli Team.
4. Nella pagina Team members (Membri del team), scegli Add team member (Aggiungi membro del team).
5. In Choose user (Seleziona utente), procedere in uno dei modi seguenti:

   - Se esiste già un utente IAM per la persona che desideri aggiungere, scegli l'utente IAM dall'elenco.

     > **Note**
     >
     > Gli utenti che sono già stati aggiunti a un altro AWS CodeStar progetto vengono visualizzati nell'elenco AWS CodeStar Utenti esistenti.

     Nel ruolo del progetto, scegli il AWS CodeStar ruolo (Proprietario, Collaboratore o Visualizzatore) per questo utente. Si tratta di un ruolo a livello di progetto AWS CodeStar che può essere modificato solo da un proprietario del progetto. Se applicato a un utente IAM, il ruolo fornisce tutte le autorizzazioni necessarie per accedere alle risorse AWS CodeStar del progetto. Applica le politiche necessarie per creare e gestire le credenziali Git per il codice archiviato CodeCommit in IAM o per caricare le chiavi Amazon EC2 SSH per l'utente in IAM.

     > **Important**
     >
     > Non puoi fornire o modificare il nome visualizzato o le informazioni e-mail per un utente IAM a meno che tu non abbia effettuato l'accesso alla console come tale utente. Per ulteriori informazioni, consulta Gestisci le informazioni di visualizzazione per il tuo profilo AWS CodeStar utente .

     Scegli Aggiungi membro del team.

   - Se non esiste un utente IAM per la persona che desideri aggiungere al progetto, scegli Crea nuovo utente IAM. Verrai reindirizzato alla console IAM dove potrai creare un nuovo utente IAM. Per ulteriori informazioni, consulta Creazione di utenti IAM nella guida per l'utente IAM. Dopo aver creato il tuo utente IAM, torna alla AWS CodeStar console, aggiorna l'elenco degli utenti e scegli l'utente IAM che hai creato dall'elenco a discesa. Inserisci il nome AWS CodeStar visualizzato, l'indirizzo email e il ruolo di progetto che desideri applicare a questo nuovo utente, quindi scegli Aggiungi membro del team.

> **Note**
>
> Per facilità di gestione, ad almeno un utente deve essere assegnato il ruolo di proprietario del progetto.

6. Invia al nuovo membro del team le seguenti informazioni:

   - Informazioni di connessione per il tuo AWS CodeStar progetto.
   - Se il codice sorgente è memorizzato in CodeCommit, istruzioni per configurare l'accesso con credenziali Git al CodeCommit repository dai loro computer locali.
   - Informazioni su come l'utente può gestire il nome visualizzato, l'indirizzo e-mail e la chiave Amazon EC2 SSH pubblica, come descritto inLavorare con il tuo profilo AWS CodeStar utente .
   - Password monouso e informazioni di connessione, se l'utente è nuovo AWS e hai creato un utente IAM per quella persona. La password scade la prima volta in cui l'utente effettua l'accesso. L'utente deve scegliere una nuova password.

Passaggio 6: Pulizia

Complimenti! L'esercitazione è terminata. Se non vuoi continuare a utilizzare questo progetto e le sue risorse, devi eliminarlo per evitare possibili addebiti continui AWS sul tuo account.

Per eliminare un progetto in AWS CodeStar

1. Apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.
2. Scegli Progetti nel riquadro di navigazione.
3. Seleziona il progetto che desideri eliminare e scegli Elimina.

   In alternativa, apri il progetto e scegli Impostazioni dal riquadro di navigazione sul lato sinistro della console. Nella pagina dei dettagli del progetto, seleziona Delete project (Elimina progetto).
4. Nella pagina di conferma dell'eliminazione, inserisci delete. Mantieni selezionata l'opzione Elimina risorse se desideri eliminare le risorse del progetto. Scegli Elimina.

   L'eliminazione di un progetto può richiedere alcuni minuti. Dopo l'eliminazione, il progetto non viene più visualizzato nell'elenco dei progetti nella AWS CodeStar console.

> **Important**
>
> Se il progetto utilizza risorse esterne AWS (ad esempio, un GitHub repository o problemi in Atlassian JIRA), tali risorse non vengono eliminate, anche se si seleziona la casella di controllo.
> Il progetto non può essere eliminato se alcune policy AWS CodeStar gestite sono state associate manualmente a ruoli che non sono utenti IAM. Se hai collegato le policy gestite del tuo progetto a un ruolo dell'utente federato, è necessario scollegare la policy prima di eliminare il progetto. Per ulteriori informazioni, consulta ???.

Fase 7: Preparate il progetto per un ambiente di produzione

Dopo aver creato il progetto, è possibile creare, testare e distribuire il codice. Per mantenere il progetto in un ambiente di produzione, prendere in esame le seguenti considerazioni:

- Applicare regolarmente le patch di sicurezza e rivedere le best practice di sicurezza per le dipendenze utilizzate dall'applicazione. Per ulteriori informazioni, consulta Best practice relative alla sicurezza per risorse AWS CodeStar.
- Monitorare regolarmente le impostazioni di ambiente suggerite per il linguaggio di programmazione del progetto.

Fasi successive

Ecco alcune altre risorse per aiutarti a saperne di più su AWS CodeStar:

- Tutorial: creare e gestire un progetto serverless in AWS CodeStarUtilizza un progetto che crea e distribuisce un servizio Web utilizzando la logica in AWS Lambda e può essere richiamato da un'API in Amazon API Gateway.
- AWS CodeStar Modelli di progetto descrive altri tipi di progetti che è possibile creare.
- Lavorare con AWS CodeStar i team fornisce informazioni sull'abilitazione di altri utenti come collaboratori sui progetti.

Tutorial: creare e gestire un progetto serverless in AWS CodeStar

In questo tutorial, viene utilizzato AWS CodeStar per creare un progetto che utilizza il AWS Serverless Application Model (AWS SAM) per creare e gestire AWS risorse per un servizio Web ospitato in. AWS Lambda

AWS CodeStar utilizza AWS SAM, su cui si basa AWS CloudFormation, per fornire un modo semplificato di creare e gestire AWS risorse supportate, tra cui Amazon API Gateway APIs, AWS Lambda funzioni e tabelle Amazon DynamoDB. (Questo progetto non utilizza alcuna tabella Amazon DynamoDB.)

Per ulteriori informazioni, consulta AWS Serverless Application Model (AWS SAM) su. GitHub

Prerequisito: Completa le fasi descritte in Configurazione AWS CodeStar.

> **Note**
>
> Al tuo AWS account potrebbero essere addebitati i costi relativi a questo tutorial, inclusi i costi per i AWS servizi utilizzati da AWS CodeStar. Per ulteriori informazioni, consulta AWS CodeStar Prezzi.

Argomenti

Panoramica

Nel corso di questo tutorial, apprenderai come:

1. AWS CodeStar Utilizzalo per creare un progetto che utilizza AWS SAM per creare e distribuire un servizio Web basato su Python. Questo servizio Web è ospitato AWS Lambda e accessibile tramite Amazon API Gateway.
2. Esplorare le risorse principali del progetto, che includono:
   - Il AWS CodeCommit repository in cui è archiviato il codice sorgente del progetto. Questo codice sorgente include la logica del servizio Web e definisce le risorse correlate ad AWS .
   - La AWS CodePipeline pipeline che automatizza la creazione del codice sorgente. Questa pipeline utilizza AWS SAM per creare e distribuire una funzione AWS Lambda, creare un'API correlata in Amazon API Gateway e connettere l'API alla funzione.
   - La funzione su cui viene distribuita. AWS Lambda
   - L'API creata in Amazon API Gateway.
3. Testa il servizio Web per confermare che abbia AWS CodeStar creato e distribuito il servizio Web come previsto.
4. Configurare la tua workstation locale affinché funzioni con il codice sorgente del progetto.
5. Modificare il codice sorgente del progetto utilizzando la workstation locale. Quando aggiungi una funzione al progetto ed esegui il push delle modifiche al codice sorgente, AWS CodeStar ricrea e ridistribuisce il servizio Web.
6. Prova nuovamente il servizio Web per confermare che sia AWS CodeStar stato ricostruito e ridistribuito come previsto.
7. Scrivere un test di unità utilizzando la workstation locale per sostituire alcuni test manuali con un test automatizzato. Quando si esegue il push dello unit test, AWS CodeStar ricostruisce e ridistribuisce il servizio Web ed esegue lo unit test.
8. Visualizzare i risultati dei test di unità.
9. Eliminare il progetto. Questo passaggio ti aiuta a evitare addebiti sul tuo AWS account per i costi relativi a questo tutorial.

Fase 1: creazione del progetto

In questo passaggio, si utilizza la AWS CodeStar console per creare un progetto.

1. Accedi Console di gestione AWS e apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.

   > **Note**
   >
   > Devi accedere Console di gestione AWS utilizzando le credenziali associate all'utente IAM che hai creato o in Configurazione AWS CodeStar cui ti sei identificato. Questo utente deve disporre della policy gestita **`AWSCodeStarFullAccess`** associata.

2. Scegli la AWS regione in cui desideri creare il progetto e le relative risorse.

   Per informazioni sulle AWS regioni in cui AWS CodeStar è disponibile, consulta Regioni ed endpoint nella Guida AWS generale.

3. Seleziona Crea progetto.
4. Nella pagina Choose a project template (Scegli un modello di progetto):

   - Per Tipo di applicazione, selezionare Servizio Web.
   - Per il linguaggio di programmazione, seleziona Python.
   - Per AWS assistenza, seleziona AWS Lambda.

5. Scegliere la casella che contiene le selezioni. Scegli Next (Successivo).
6. Per Project name (Nome progetto), immettere un nome per il progetto (ad esempio, **`My SAM Project`**). Se usi un nome diverso dall'esempio, assicurati di usarlo durante tutto il tutorial.

   Per Project ID, AWS CodeStar sceglie un identificatore correlato per questo progetto (ad esempio, my-sam-project). Se visualizzi un ID progetto diverso, assicurati di usarlo durante tutto il tutorial.

   Lasciare l'opzione AWS CodeCommit selezionata e non modificare il valore Repository name (Nome repository).

7. Scegli Next (Successivo).
8. Controlla le impostazioni, quindi scegli Crea progetto.

   Se è la prima volta che lo utilizzi AWS CodeStar in questa AWS regione, per Nome visualizzato ed Email, inserisci il nome visualizzato e l'indirizzo email che desideri utilizzare AWS CodeStar per il tuo utente IAM. Scegli Next (Successivo).

9. Wait while AWS CodeStar crea il progetto. Questo processo potrebbe richiedere diversi minuti. Non continuate finché non vedrete il banner Project provisioned durante l'aggiornamento.

Fase 2: esplorare le risorse del progetto

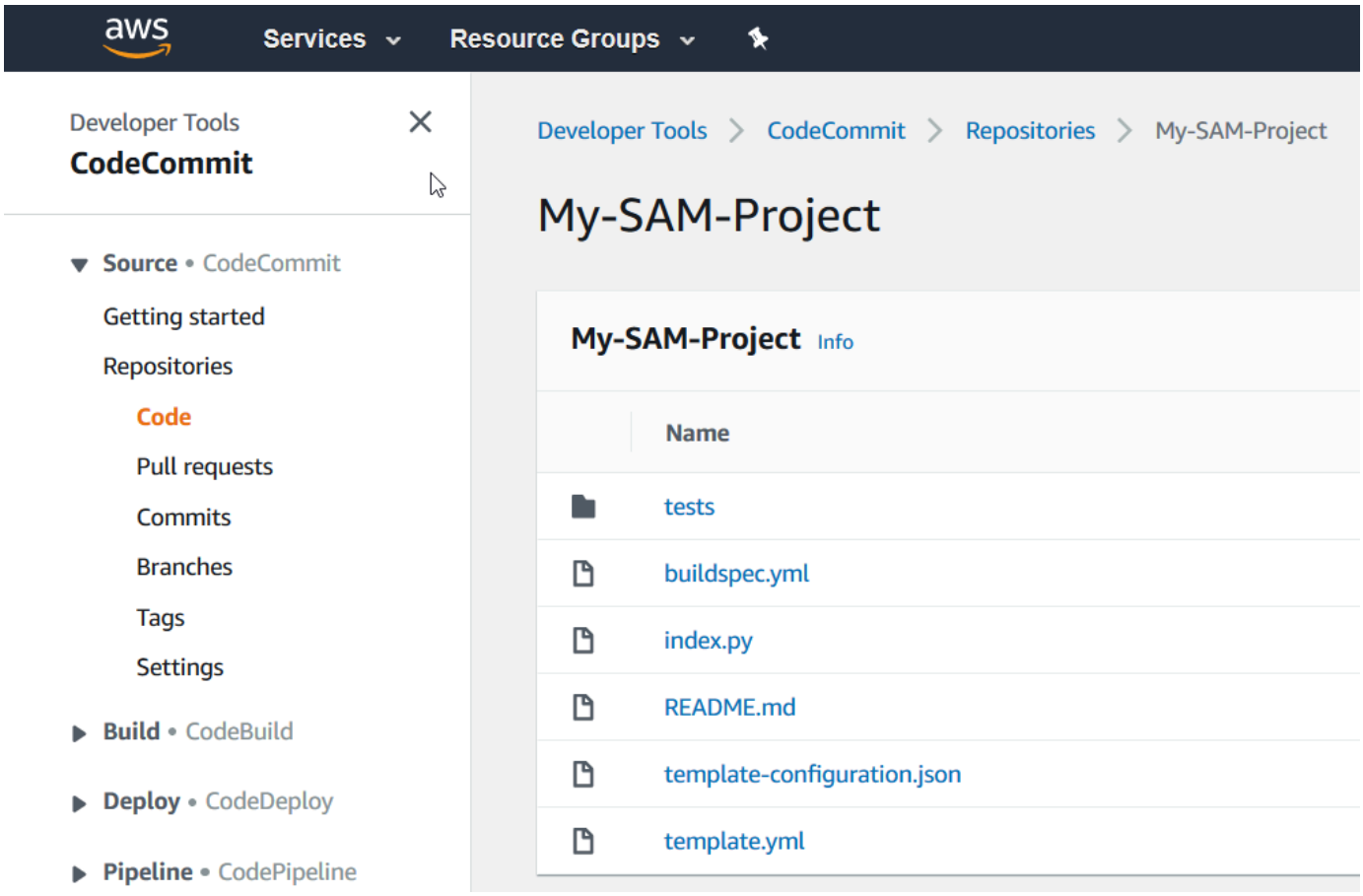
In questo passaggio, esplorerai quattro AWS risorse del progetto per capire come funziona il progetto:

- L' AWS CodeCommit archivio in cui è archiviato il codice sorgente del progetto. AWS CodeStar dà il nome al repository my-sam-project, my-sam-projectdov'è il nome del progetto.
- La AWS CodePipeline pipeline che utilizza CodeBuild un AWS SAM per automatizzare la creazione e l'implementazione della funzione Lambda e dell'API del servizio Web in API Gateway. AWS CodeStar dà alla pipeline il nome my-sam-project--Pipeline, dove my-sam-projectè l'ID del progetto.
- La funzione Lambda che contiene la logica del servizio Web. AWS CodeStar dà alla funzione il nome awscodestar-my-sam-project-lambda- HelloWorld - ***`RANDOM_ID`***, dove:
  - my-sam-projectè l'ID del progetto.
  - HelloWorldè l'ID della funzione specificato nel `template.yaml` file nel AWS CodeCommit repository. Puoi esplorare questo file più tardi.
  - *`RANDOM_ID`*è un ID casuale che AWS SAM assegna alla funzione per garantire l'unicità.
- L'API in API Gateway che semplifica la chiamata alla funzione Lambda. AWS CodeStar dà all'API il nome awscodestar-my-sam-project--lambda, dove my-sam-projectè l'ID del progetto.

Per esplorare il repository del codice sorgente in CodeCommit

1. Con il progetto aperto nella AWS CodeStar console, nella barra di navigazione, scegli Repository.
2. Scegli il link al tuo CodeCommit repository (**`My-SAM-Project`**) in Dettagli del deposito.
3. Nella CodeCommit console, nella pagina Codice, vengono visualizzati i file di codice sorgente del progetto:
   - `buildspec.yml`, che CodePipeline indica CodeBuild da utilizzare durante la fase di compilazione, per impacchettare il servizio Web utilizzando AWS SAM.
   - `index.py`, che contiene la logica per la funzione Lambda. Questa funzione semplicemente restituisce la stringa `Hello World` e un timestamp in formato ISO.
   - `README.md`, che contiene informazioni generali sul repository.
   - `template-configuration.json`, che contiene l'ARN del progetto con segnaposto utilizzati per taggare le risorse con l'ID del progetto

- `template.yml`, che AWS SAM utilizza per impacchettare il servizio Web e creare l'API in API Gateway.



Per visualizzare il contenuto di un file, sceglierlo nell'elenco.

Per ulteriori informazioni sull'uso della CodeCommit console, consulta la Guida AWS CodeCommit per l'utente.

Per esplorare la pipeline in CodePipeline

1. Per visualizzare le informazioni sulla pipeline, con il progetto aperto nella AWS CodeStar console, nella barra di navigazione, scegli Pipeline e vedrai che la pipeline contiene:

   - Una fase Source (Sorgente) per ottenere il codice sorgente da CodeCommit.
   - Una fase Build (Crea) per creare il codice sorgente con CodeBuild.

- Una fase di distribuzione per la distribuzione del codice sorgente e delle risorse integrati con SAM. AWS AWS

2. Per visualizzare ulteriori informazioni sulla pipeline, in Dettagli sulla pipeline, scegli la pipeline per aprirla nella console. CodePipeline

Per informazioni sull'uso della CodePipeline console, consulta la Guida per l'utente.AWS CodePipeline

Per esplorare le attività del progetto e le risorse di AWS servizio nella pagina Panoramica

1. Apri il progetto nella AWS CodeStar console e dalla barra di navigazione, scegli Panoramica.
2. Consulta gli elenchi delle attività del progetto e delle risorse del progetto.

Per esplorare la funzione in Lambda

1. Con il progetto aperto nella AWS CodeStar console, nella barra di navigazione laterale, scegli Panoramica.
2. In Risorse del progetto, nella colonna ARN, scegli il link per la funzione Lambda.

   Il codice della funzione viene visualizzato nella console Lambda.

Per informazioni sull'uso della console Lambda, consulta la Guida per gli AWS Lambda sviluppatori.

Per esplorare l'API in API Gateway

1. Con il progetto aperto nella AWS CodeStar console, nella barra di navigazione laterale, scegli Panoramica.
2. In Risorse del progetto, nella colonna ARN, scegli il link per l'API Amazon API Gateway.

   Le risorse per l'API vengono visualizzate nella console API Gateway.

Per informazioni sull'utilizzo della console API Gateway, consulta la API Gateway Developer Guide.

Fase 3: testare il servizio Web

In questo passaggio, si testa il servizio Web AWS CodeStar appena creato e distribuito.

1. Con il progetto ancora aperto rispetto al passaggio precedente, nella barra di navigazione, scegli Pipeline.
2. Assicurati che sia visualizzato Succeeded per le fasi Source, Build e Deploy prima di continuare. Questo processo potrebbe richiedere diversi minuti.

   > **Note**
   >
   > Se Failed (Non riuscita) viene visualizzata per una qualsiasi delle fasi, consulta quanto segue per facilitare la risoluzione dei problemi:
   >
   > - Per la fase Source, consulta Risoluzione dei problemi AWS CodeCommit nella Guida per l'AWS CodeCommit utente.
   > - Per la fase di compilazione, consulta Risoluzione dei problemi AWS CodeBuild nella Guida AWS CodeBuild per l'utente.
   > - Per la fase di implementazione, consulta Risoluzione dei problemi AWS CloudFormation nella Guida per l'AWS CloudFormation utente.
   > - Per altri problemi, consulta Risoluzione dei problemi AWS CodeStar.

3. Scegli Visualizza applicazione.

Nella nuova scheda che viene visualizzata in un browser Web, il servizio Web mostra i seguenti output di risposta:

```
{"output": "Hello World", "timestamp": "2017-08-30T15:53:42.682839"}
```

Fase 4: configurare la workstation locale per modificare il codice del progetto

In questa fase, è possibile configurare la workstation locale per modificare il codice sorgente nel progetto AWS CodeStar . La workstation locale può essere un computer fisico o virtuale che esegue macOS, Windows o Linux.

1. Con il tuo progetto ancora aperto dal passaggio precedente:

- Nella barra di navigazione, scegli IDE, quindi espandi Accedi al codice del progetto.
- Scegli Visualizza istruzioni sotto l'interfaccia della riga di comando.

  Se hai installato Visual Studio o Eclipse, scegli invece Visualizza istruzioni sotto Visual Studio o Eclipse, segui le istruzioni e poi passa a. Fase 5: aggiungere logica al servizio Web

2. Segui le istruzioni per completare le attività seguenti:

   a. Configurare Git sulla workstation locale.

   b. Usa la console IAM per generare credenziali Git per il tuo utente IAM.

   c. Clona il CodeCommit repository del progetto sulla tua workstation locale.

3. Nella barra di navigazione a sinistra, scegli Progetto per tornare alla panoramica del progetto.

Fase 5: aggiungere logica al servizio Web

In questa fase è necessario utilizzare la workstation locale per aggiungere logica al servizio Web. In particolare, aggiungi una funzione Lambda e poi la connetti all'API in API Gateway.

1. Nella workstation locale, andare alla directory che contiene il repository del codice sorgente clonato.
2. Nella directory, creare un file denominato `hello.py`. Aggiungere il codice seguente, quindi salvare il file:

```
import json

def handler(event, context):
  data = {
    'output': 'Hello ' + event["pathParameters"]["name"]
  }
  return {
    'statusCode': 200,
    'body': json.dumps(data),
    'headers': {'Content-Type': 'application/json'}
  }
```

   Il codice precedente genera la stringa `Hello` e la stringa che l'intermediario invia alla funzione.

3. Nella stessa directory, aprire il file `template.yml`. Aggiungere il codice seguente alla fine del file e quindi salvare il file:

```
  Hello:
    Type: AWS::Serverless::Function
    Properties:
      FunctionName: !Sub 'awscodestar-${ProjectId}-lambda-Hello'
      Handler: hello.handler
      Runtime: python3.7
      Role:
        Fn::GetAtt:
        - LambdaExecutionRole
        - Arn
      Events:
        GetEvent:
          Type: Api
          Properties:
            Path: /hello/{name}
            Method: get
```

AWS SAM utilizza questo codice per creare una funzione in Lambda, aggiungere un nuovo metodo e percorso all'API in API Gateway e quindi connettere questo metodo e percorso alla nuova funzione.

> **Note**
>
> L'identazione del codice precedente è importante. Se non si aggiunge il codice esattamente come mostrato, il progetto potrebbe non essere creato correttamente.

4. Eseguire git add . per aggiungere le modifiche del file all'area di gestione temporanea del repository clonato. Non dimenticare il punto (.), che aggiunge tutti i file modificati.

> **Note**
>
> Se stai utilizzando Visual Studio o Eclipse anziché la riga di comando, le istruzioni per l'utilizzo di Git potrebbero essere differenti. Consultare la documentazione di Visual Studio o Eclipse.

5. Eseguire git commit -m "Added hello.py and updated template.yaml." per eseguire il file di gestione temporanea nel repository clonato
6. Invocare il comando git push per eseguire il push del commit sul repository remoto.

> **Note**
>
> È possibile che ti vengano richieste le credenziali di accesso generate in precedenza. Per evitare che questi dati ti vengano richiesti ogni volta che in futuro interagisci con il repository remoto, prendi in considerazione l'installazione e la configurazione di un Git Credential Manager. Ad esempio, su macOS o Linux, è possibile eseguire git config credential.helper 'cache --timeout 900' nel terminale per non ricevere la richiesta prima di ogni 15 minuti. In alternativa, è possibile eseguire git config credential.helper 'store --file ~/.git-credentials' in modo da non ricevere più la richiesta. Git memorizza le credenziali in testo non crittografato in un file normale nella directory principale. Per ulteriori informazioni, consulta Git Tools - Credential Storage sul sito Web Git.

Dopo aver AWS CodeStar rilevato il push, indica di utilizzare CodeBuild e AWS SAM CodePipeline per ricostruire e ridistribuire il servizio Web. È possibile controllare l'avanzamento della distribuzione nella pagina Pipeline.

AWS SAM assegna alla nuova funzione il nome awscodestar-my-sam-project-Lambda-Hello -, dove: *RANDOM_ID*

- my-sam-projectè l'ID del progetto.
- Hello (Salve) è la funzione ID, come specificato nel file `template.yaml`.
- *RANDOM_ID*è un ID casuale che AWS SAM assegna alla funzione per motivi di unicità.

Fase 6: testare il servizio Web avanzato

In questo passaggio, si testa il servizio Web avanzato AWS CodeStar creato e distribuito, in base alla logica aggiunta nel passaggio precedente.

1. Con il progetto ancora aperto nella AWS CodeStar console, nella barra di navigazione scegli Pipeline.
2. Prima di continuare, assicurati che la pipeline sia stata nuovamente eseguita e che nelle fasi Source, Build e Deploy sia visualizzato Succeeded. Questo processo potrebbe richiedere diversi minuti.

> **Note**
>
> Se Failed (Non riuscita) viene visualizzata per una qualsiasi delle fasi, consulta quanto segue per facilitare la risoluzione dei problemi:
>
> - Per la fase Source, consulta Risoluzione dei problemi AWS CodeCommit nella Guida per l'AWS CodeCommit utente.
> - Per la fase di compilazione, consulta Risoluzione dei problemi AWS CodeBuild nella Guida AWS CodeBuild per l'utente.
> - Per la fase di implementazione, consulta Risoluzione dei problemi AWS CloudFormation nella Guida per l'AWS CloudFormation utente.
> - Per altri problemi, consulta Risoluzione dei problemi AWS CodeStar.

3. Scegli Visualizza applicazione.

   Nella nuova scheda che viene visualizzata in un browser Web, il servizio Web mostra i seguenti output di risposta:

   ```
   {"output": "Hello World", "timestamp": "2017-08-30T15:53:42.682839"}
   ```

4. Nella casella dell'indirizzo della scheda, aggiungi il percorso **`/hello/`** e il tuo nome alla fine dell'URL (ad esempio, https://***`API_ID`***.execute-api). ***`REGION_ID`***.amazonaws. com/Prod/hello/***`YOUR_FIRST_NAME`***), quindi premere Invio.

Se il nome è Mary, il servizio Web mostra i seguenti output di risposta:

```
{"output": "Hello Mary"}
```

Fase 7: aggiungere un test di unità per il Web Service

In questo passaggio, si utilizza la workstation locale per aggiungere un test da AWS CodeStar eseguire sul servizio Web. Questo test sostituisce i test manuali eseguiti precedentemente.

1. Nella workstation locale, andare alla directory che contiene il repository del codice sorgente clonato.
2. Nella directory, creare un file denominato `hello_test.py`. Aggiungere il codice seguente, quindi salvare il file.

```
from hello import handler

def test_hello_handler():

  event = {
    'pathParameters': {
      'name': 'testname'
    }
  }

  context = {}

  expected = {
    'body': '{"output": "Hello testname"}',
    'headers': {
      'Content-Type': 'application/json'
    },
    'statusCode': 200
  }

  assert handler(event, context) == expected
```

Questo test verifica se l'output della funzione Lambda è nel formato previsto. In questo caso, il test va a buon fine. In caso contrario, il test ha esito negativo.

3. Nella stessa directory, aprire il file `buildspec.yml`. Sostituire i contenuti del file con il codice seguente e quindi salvare il file.

```
version: 0.2

phases:
   install:
      runtime-versions:
         python: 3.7

      commands:
         - pip install pytest
```

```
         # Upgrade AWS CLI to the latest version
         - pip install --upgrade awscli


   pre_build:
      commands:
         - pytest

   build:
      commands:
         # Use AWS SAM to package the application by using AWS CloudFormation
         - aws cloudformation package --template template.yml --s3-bucket
 $S3_BUCKET --output-template template-export.yml

         # Do not remove this statement. This command is required for AWS CodeStar
 projects.
         # Update the AWS Partition, AWS Region, account ID and project ID in the
 project ARN on template-configuration.json file so AWS CloudFormation can tag
 project resources.
         - sed -i.bak 's/\$PARTITION\$/'${PARTITION}'/g;s/\$AWS_REGION
\$/'${AWS_REGION}'/g;s/\$ACCOUNT_ID\$/'${ACCOUNT_ID}'/g;s/\$PROJECT_ID\
$/'${PROJECT_ID}'/g' template-configuration.json

artifacts:
   type: zip
   files:
      - template-export.yml
      - template-configuration.json
```

Questa specifica di build indica di CodeBuild installare pytest, il framework di test Python, nel suo ambiente di compilazione. CodeBuild usa pytest per eseguire lo unit test. Il resto delle specifiche di compilazione è uguale alle precedenti.

4. Usare Git per inviare tali modifiche al repository remoto.

```
git add .

git commit -m "Added hello_test.py and updated buildspec.yml."

git push
```

Fase 8: visualizzare risultati del test di unità

In questa fase, è possibile vedere se il test di unità è riuscito o meno.

1. Con il progetto ancora aperto nella AWS CodeStar console, nella barra di navigazione, scegli Pipeline.
2. Assicurati che la pipeline sia stata nuovamente eseguita prima di continuare. Questo processo potrebbe richiedere diversi minuti.

   Se il test di unità è andato a buon fine, Succeeded (Riuscito) viene visualizzato per la fase Build (Crea).
3. Per visualizzare i dettagli dei risultati del test unitario, nella fase di creazione, scegli il CodeBuildlink.
4. Nella CodeBuild console, nella my-sam-project pagina Build Project:, in Cronologia build, scegli il link nella colonna Build run della tabella.
5. Nella *BUILD_ID* pagina my-sam-project:, in Build logs, scegli il link Visualizza l'intero registro.
6. Nella console Amazon CloudWatch Logs, cerca nell'output del log un risultato del test simile al seguente. Nel seguente risultato del test, il test è andato a buon fine:

   ```
   ...
   ============================= test session starts ==============================
   platform linux2 -- Python 2.7.12, pytest-3.2.1, py-1.4.34, pluggy-0.4.0
   rootdir: /codebuild/output/src123456789/src, inifile:
   collected 1 item

   hello_test.py .

   ========================== 1 passed in 0.01 seconds ===========================
   ...
   ```

   Se il test non è riuscito, devono essere presenti dettagli nell'output di log che consentono di risolvere il problema.

Fase 9: elimina

In questa fase, è necessario eliminare il progetto per evitare addebiti in corso per questo progetto.

Se desideri continuare a utilizzare questo progetto, puoi saltare questo passaggio, ma il tuo AWS account potrebbe continuare a ricevere addebiti.

1. Con il progetto ancora aperto nella AWS CodeStar console, nella barra di navigazione scegli Impostazioni.
2. In Dettagli del progetto, scegli Elimina progetto.
3. Invio**`delete`**, mantieni selezionata la casella Elimina risorse, quindi scegli Elimina.

> **Important**
>
> Se si deseleziona questa casella, il record del progetto viene eliminato da AWS CodeStar, ma molte AWS risorse del progetto vengono conservate. Il tuo AWS account potrebbe continuare a ricevere addebiti.

Se esiste ancora un bucket Amazon S3 AWS CodeStar creato per questo progetto, segui questi passaggi per eliminarlo. :

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Nell'elenco dei bucket, scegli l'icona accanto a aws-codestar- - - ***`REGION_ID`*** --pipe, dove: *`ACCOUNT_ID`* my-sam-project
   - *`REGION_ID`*è l'ID della AWS regione per il progetto che hai appena eliminato.
   - *`ACCOUNT_ID`*è l'ID AWS del tuo account.
   - my-sam-projectè l'ID del progetto che hai appena eliminato.
3. Scegli Empty Bucket (Svuota il bucket). Digitare il nome del bucket e quindi scegliere Confirm (Conferma).
4. Scegli Delete Bucket (Elimina bucket). Digitare il nome del bucket e quindi scegliere Confirm (Conferma).

Fasi successive

Ora che hai completato questo tutorial, ti consigliamo di esaminare le risorse seguenti:

- Il Guida introduttiva con AWS CodeStar tutorial utilizza un progetto che crea e distribuisce un'applicazione Web basata su Node.js in esecuzione su un'istanza Amazon. EC2

- AWS CodeStar Modelli di progetto descrive altri tipi di progetti che è possibile creare.
- Lavorare con AWS CodeStar i team illustra come gli altri possono aiutarti a lavorare sui progetti.

Tutorial: crea un progetto AWS CodeStar con AWS CLI

Questo tutorial mostra come utilizzare il per AWS CLI creare un AWS CodeStar progetto con un codice sorgente di esempio e un modello di toolchain di esempio. AWS CodeStar fornisce l' AWS infrastruttura e le risorse IAM specificate in un modello di CloudFormation toolchain. Il progetto gestisce le risorse della toolchain per creare e distribuire il codice sorgente.

AWS CodeStar utilizza CloudFormation per creare e distribuire il codice di esempio. Questo codice di esempio crea un servizio Web ospitato in Amazon API Gateway AWS Lambda e accessibile tramite Amazon API Gateway.

Prerequisiti:

- Completa le fasi descritte in Configurazione AWS CodeStar.
- Devi aver creato un bucket di storage Amazon S3. In questa esercitazione è possibile caricare il codice sorgente di esempio e il modello della toolchain in questa posizione.

> **Note**
>
> Potrebbero essere addebitati AWS sul tuo account i costi relativi a questo tutorial, inclusi AWS i servizi utilizzati da. AWS CodeStar Per ulteriori informazioni, consulta AWS CodeStar Prezzi.

Argomenti

Fase 1: Scaricare e rivedere il codice sorgente di esempio

Per questa esercitazione, è disponibile un file ZIP per il download. Questo contiene un esempio di codice sorgente di un'applicazione di esempio Node.js sulla piattaforma di elaborazione Lambda. Quando il codice sorgente viene copiato sul repository, la cartella e i file appaiono come segue:

```
tests/
app.js
buildspec.yml
index.js
package.json
README.md
template.yml
```

Nel codice sorgente del progetto di esempio, sono presenti i seguenti elementi del progetto:

- `tests/`: impostazioni dell'unit test configurato per questo progetto CodeBuild. Questa cartella è inclusa nel codice di esempio, ma non è necessaria per creare un progetto.
- `app.js`: codice sorgente dell'applicazione del progetto.
- `buildspec.yml`: istruzioni per la compilazione da utilizzare durante la fase di compilazione delle risorse CodeBuild. Questo file è obbligatorio per un modello di toolchain con una risorsa CodeBuild .
- `package.json`: informazioni sulle dipendenze per il codice sorgente dell'applicazione.
- `README.md`: file README del progetto incluso in tutti i progetti AWS CodeStar . Questo file è incluso nel codice di esempio, ma non è necessario per creare un progetto.
- `template.yml`: Il file modello di infrastruttura o il file modello SAM incluso in tutti i AWS CodeStar progetti. Questo è diverso dal file template.yml della toolchain caricato più avanti in questa esercitazione. Questo file è incluso nel codice di esempio, ma non è necessario per creare un progetto.

Fase 2: Scaricare il modello di esempio della toolchain

Il modello di toolchain di esempio fornito per questo tutorial crea un repository (CodeCommit), una pipeline (CodePipeline) e un build container (CodeBuild) e li utilizza CloudFormation per distribuire il codice sorgente su una piattaforma Lambda. Oltre a queste risorse, ci sono anche ruoli IAM che puoi utilizzare per definire le autorizzazioni del tuo ambiente di runtime, un bucket Amazon S3 che viene utilizzato per archiviare gli elementi della distribuzione e CloudWatch una regola Events CodePipeline

che viene utilizzata per attivare le distribuzioni di pipeline quando invii codice al tuo repository. Per allinearsi alle best practice AWS IAM, limitare le policy dei ruoli toolchain definiti in questo esempio.

Scarica e decomprimi il modello di esempio in formato YAML. AWS CloudFormation

Quando esegui il comando create-project successivamente nel tutorial, questo modello crea le seguenti risorse della toolchain personalizzate in CloudFormation. Per ulteriori informazioni sulle risorse create in questa esercitazione, consulta i seguenti argomenti nella Guida per l'utente AWS CloudFormation :

- La AWS::CodeCommit::Repository CloudFormation risorsa crea un repository. CodeCommit
- La AWS::CodeBuild::Project CloudFormation risorsa crea un progetto di CodeBuild compilazione.
- La AWS::CodeDeploy::Application CloudFormation risorsa crea un' CodeDeployapplicazione.
- La AWS::CodePipeline::Pipeline CloudFormation risorsa crea una CodePipeline pipeline.
- La AWS::S3::Bucket CloudFormation risorsa crea il bucket di artefatti della pipeline.
- La AWS::S3::BucketPolicy CloudFormation risorsa crea la policy relativa al bucket di artefatti della pipeline.
- La AWS::IAM::Role CloudFormation risorsa crea il ruolo di lavoratore CodeBuild IAM che fornisce AWS CodeStar le autorizzazioni per gestire il progetto di compilazione. CodeBuild
- La AWS::IAM::Role CloudFormation risorsa crea il ruolo di lavoratore CodePipeline IAM che fornisce AWS CodeStar le autorizzazioni per creare la pipeline.
- La AWS::IAM::Role CloudFormation risorsa crea il ruolo di lavoratore CloudFormation IAM che fornisce AWS CodeStar le autorizzazioni per creare lo stack di risorse.
- La AWS::IAM::Role CloudFormation risorsa crea il ruolo di lavoratore CloudFormation IAM che fornisce AWS CodeStar le autorizzazioni per creare lo stack di risorse.
- La AWS::IAM::Role CloudFormation risorsa crea il ruolo di lavoratore CloudFormation IAM che fornisce AWS CodeStar le autorizzazioni per creare lo stack di risorse.
- La AWS::Events::Rule CloudFormation risorsa crea la regola CloudWatch Events che monitora il tuo repository alla ricerca di eventi push.
- La AWS::IAM::Role CloudFormation risorsa crea il ruolo CloudWatch Events IAM.

Fase 3: Testa il tuo modello di toolchain in CloudFormation

Prima di caricare il modello di toolchain, è possibile testare il modello di toolchain su CloudFormation e risolvere gli eventuali errori.

1. Salva il modello aggiornato sul tuo computer locale e apri la CloudFormation console. Scegli Crea stack. Le nuove risorse dovrebbero essere visibili nell'elenco.
2. Visualizza lo stack per evidenziare la presenza di eventuali errori di creazione dello stack.
3. Dopo aver completato il test, eliminare lo stack.

> **Note**
>
> Assicurati di eliminare lo stack e tutte le risorse create in CloudFormation. In caso contrario, al momento della creazione di un progetto, è possibile che si verifichino errori a causa dei nomi delle risorse già in uso.

Fase 4: Caricare il codice sorgente e il modello di toolchain

Per creare un AWS CodeStar progetto, devi prima impacchettare il codice sorgente in un file.zip e inserirlo in Amazon S3. AWS CodeStar inizializza il tuo repository con questi contenuti. È possibile specificare questa posizione nel file di input quando si esegue il comando per creare il progetto nella AWS CLI.

È inoltre necessario caricare il `toolchain.yml` file e inserirlo in Amazon S3. Specificate questa posizione nel file di input quando eseguite il comando per creare il progetto in AWS CLI

Per caricare il codice sorgente e il modello di toolchain

1. L'esempio seguente mostra la struttura del file sorgente e del modello di toolchain pronti per essere compressi e caricati. Il codice di esempio include il file `template.yml`. Ricordare che questo file è diverso dal file `toolchain.yml`.

```
ls
src toolchain.yml

ls src/
README.md    app.js        buildspec.yml    index.js    package.json
 template.yml    tests
```

2. Creare il file .zip contenente i file del codice sorgente.

```
cd src; zip -r "../src.zip" *; cd ../
```

3. Utilizzate il cp comando e includete i file come parametri.

   I seguenti comandi caricano il file.zip e `toolchain.yml` lo caricano su Amazon S3.

   ```
   aws s3 cp src.zip s3://MyBucket/src.zip
   aws s3 cp toolchain.yml s3://MyBucket/toolchain.yml
   ```

Per configurare il bucket Amazon S3 per condividere il codice sorgente

- Poiché stai archiviando il codice sorgente e la toolchain in Amazon S3, puoi utilizzare le policy e gli ACLs oggetti dei bucket Amazon S3 per garantire che altri utenti AWS o account IAM possano creare progetti a partire dai tuoi esempi. AWS CodeStar assicura che ogni utente che crea un progetto personalizzato abbia accesso alla toolchain e alla fonte che desidera utilizzare.

  Per consentire a chiunque di utilizzare l'esempio, eseguire i comandi seguenti:

  ```
  aws s3api put-object-acl --bucket MyBucket --key toolchain.yml --acl public-read
  aws s3api put-object-acl --bucket MyBucket --key src.zip --acl public-read
  ```

Fase 5: Creare un progetto in AWS CodeStar

Per creare il progetto, utilizzare questa procedura.

> **Important**
>
> Assicurati di configurare la AWS regione preferita in AWS CLI. Il progetto viene creato nella AWS regione configurata in AWS CLI.

1. Eseguire il comando create-project e includere il parametro `--generate-cli-skeleton`:

   ```
   aws codestar create-project --generate-cli-skeleton
   ```

   Nell'output vengono visualizzati dati in formato JSON. Copia i dati in un file (ad esempio,*`input.json`*) in una posizione del computer locale o dell'istanza in cui AWS CLI è installato. Modificare i dati copiati come segue, quindi salvare i risultati. Questo file di input è configurato per un progetto denominato `MyProject` con nome di bucket `myBucket`.

- Assicurarsi di indicare il parametro `roleArn`. Nel caso di modelli personalizzati, come il modello di esempio in questo tutorial, è necessario specificare un ruolo. Questo ruolo deve disporre delle autorizzazioni per la creazione di tutte le risorse specificate in Fase 2: Scaricare il modello di esempio della toolchain.
- Assicurarsi di indicare il parametro `ProjectId` alla voce `stackParameters`. Il modello di esempio fornito per questa esercitazione richiede obbligatoriamente tale parametro.

```
{
    "name": "MyProject",
    "id": "myproject",
    "description": "Sample project created with the CLI",
    "sourceCode": [
        {
            "source": {
                "s3": {
                    "bucketName": "MyBucket",
                    "bucketKey": "src.zip"
                }
            },
            "destination": {
                "codeCommit": {
                    "name": "myproject"

                }
            }
        }
    ],
    "toolchain": {
        "source": {
            "s3": {
                "bucketName": "MyBucket",
                "bucketKey": "toolchain.yml"
            }
        },
        "roleArn": "role_ARN",
        "stackParameters": {
            "ProjectId": "myproject"
        }
    }
}
```

2. Passare alla directory contenente il file appena salvato ed eseguire nuovamente il comando create-project. Includere il parametro `--cli-input-json`.

```
aws codestar create-project --cli-input-json file://input.json
```

3. Se eseguito correttamente, nell'output compaiono dei dati simili ai seguenti:

```
{
    "id": "project-ID",
    "arn": "arn"
}
```

   - L'output contiene informazioni sul nuovo progetto.:
     - Il valore `id` rappresenta l'ID del progetto.
     - Il valore `arn` rappresenta l'ARN del progetto.

4. Per controllare lo stato della creazione del progetto, utilizzare il comando describe-project. Includere il parametro `--id`.

```
aws codestar describe-project --id <project_ID>
```

   Nell'output compaiono informazioni simili alle seguenti:

```
{
    "name": "MyProject",
    "id": "myproject",
    "arn": "arn:aws:codestar:us-east-1:account_ID:project/myproject",
    "description": "",
    "createdTimeStamp": 1539700079.472,
    "stackId": "arn:aws:cloudformation:us-east-1:account_ID:stack/awscodestar-
myproject/stack-ID",
    "status": {
        "state": "CreateInProgress"
    }
}
```

   - L'output contiene informazioni sul nuovo progetto.:
     - Il valore `id` rappresenta l'ID univoco del progetto.

- Il valore `state` rappresenta lo stato della creazione del progetto, ad esempio `CreateInProgress` o `CreateComplete`.

Durante la creazione del progetto, è possibile aggiungere membri del team o configurare l'accesso al repository del progetto dalla riga di comando o dall'IDE preferito.

Tutorial: crea un progetto Alexa Skill in AWS CodeStar

AWS CodeStar è un servizio di sviluppo basato sul cloud AWS che fornisce gli strumenti necessari per sviluppare, creare e distribuire rapidamente applicazioni. AWS Con AWS CodeStar, puoi configurare l'intera toolchain di distribuzione continua in pochi minuti, consentendoti di iniziare a rilasciare codice più velocemente. I modelli di progetto Alexa Skill disponibili ti AWS CodeStar consentono di creare una semplice skill Hello World Alexa dal tuo AWS account con pochi clic. Inoltre, i modelli creano una pipeline di distribuzione di base che consente di iniziare con un flusso di lavoro di integrazione continua (CI) per lo sviluppo di competenze.

I principali vantaggi della creazione di competenze con Alexa AWS CodeStar sono la possibilità di iniziare a sviluppare le competenze in AWS e collegare il proprio account sviluppatore Amazon al progetto per distribuire le competenze direttamente dalla fase di sviluppo. AWS Puoi anche ottenere una pipeline (CI) di distribuzione pronta per l'uso con un repository con tutto il codice sorgente per il progetto. Puoi configurare questo repository con il tuo IDE preferito per creare competenze con gli strumenti che ti sono più familiari.

Prerequisiti

- Crea un account sviluppatore Amazon accedendo a https://developer.amazon.com. La registrazione è gratuita. Questo account possiede le competenze Alexa.
- Se non disponi di un AWS account, utilizza la seguente procedura per crearne uno.

  Per iscriverti a AWS

  1. Apri https://aws.amazon.com/, quindi scegli Crea un AWS account.

     > **Note**
     >
     > Se in precedenza hai effettuato l'accesso Console di gestione AWS utilizzando Utente root dell'account AWS le credenziali, scegli Accedi a un altro account. Se in precedenza hai effettuato l'accesso alla console utilizzando credenziali IAM, scegli

Accedi utilizzando credenziali. Utente root dell'account AWS Quindi scegli Crea un nuovo account. AWS

2. Segui le istruzioni online.

> **Important**
>
> Dopo aver creato il progetto di competenze Alexa, apporta tutte le modifiche solo nel repository del progetto. È consigliabile non modificare questa competenza direttamente utilizzando altri strumenti di Alexa Skills Kit, ad esempio l'interfaccia a riga di comando o la console di sviluppatori ASK. Questi strumenti non sono integrati con il repository di progetto. Il loro utilizzo comporta un disallineamento tra la competenza e il codice nel repository.

Fase 1: crea il progetto e collega il tuo account sviluppatore di Amazon

In questo tutorial, crei una competenza utilizzando Node.js in esecuzione su AWS Lambda. La maggior parte dei passaggi sono analoghi per altri linguaggi, anche se il nome della competenza è diverso. Consulta il file README.md nel repository del progetto per i dettagli sul modello di progetto specifico scelto.

1. Accedi a Console di gestione AWS, quindi apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.
2. Scegli la AWS regione in cui desideri creare il progetto e le relative risorse. Lo skill runtime di Alexa è disponibile nelle seguenti AWS regioni:
   - Asia Pacifico (Tokyo)
   - UE (Irlanda)
   - Stati Uniti orientali (Virginia settentrionale)
   - US West (Oregon)
3. Seleziona Crea progetto.
4. Nella pagina Choose a project template (Scegli un modello di progetto):
   a. Per il tipo di applicazione, scegli Alexa Skill.
   b. Per Linguaggio di programmazione, scegli Node.js.
5. Scegliere la casella che contiene le selezioni.

6. Per Project name (Nome progetto), immettere un nome per il progetto (ad esempio, **`My Alexa Skill`**). Se usi un nome diverso, assicurati di usarlo durante questo tutorial. AWS CodeStar sceglie un identificatore correlato per questo progetto per l'ID del progetto (ad esempio, my-alexa-skill). Se visualizzi un ID progetto diverso, assicurati di usarlo durante tutto il tutorial.
7. Scegli AWS CodeCommit per il repository in questo tutorial e non modificare il valore del nome del repository.
8. Scegli Connect Amazon developer account (Collega account sviluppatore Amazon) per collegare il tuo account sviluppatore di Amazon per l'hosting della competenza. Se non disponi di un account sviluppatore Amazon, crea un account e completa prima la registrazione da Amazon Developers.
9. Accedi con le credenziali sviluppatore di Amazon. Scegli Consenti, quindi scegli Conferma per completare la connessione.
10. Se hai più fornitori IDs associati al tuo account sviluppatore Amazon, scegli quello che desideri utilizzare per questo progetto. Assicurati di utilizzare un account con il ruolo Amministratore o Sviluppatore assegnato.
11. Scegli Next (Successivo).
12. (Facoltativo) Se è la prima volta che lo utilizzi AWS CodeStar in questa AWS regione, inserisci il nome visualizzato e l'indirizzo email che desideri utilizzare AWS CodeStar per il tuo utente IAM. Scegli Next (Successivo).
13. Wait while AWS CodeStar crea il progetto. Questo processo potrebbe richiedere diversi minuti. Non continuare finché non vedi il banner Project provisioned.

Fase 2: testa la competenza nel simulatore Alexa

Nella prima fase, hai AWS CodeStar creato una skill per te e l'hai implementata nella fase di sviluppo delle abilità di Alexa. Successivamente, devi testare la competenza nel simulatore Alexa.

1. Nel tuo progetto nella AWS CodeStar console, scegli Visualizza applicazione. Si apre una nuova scheda nel simulatore Alexa.
2. Accedi con le credenziali sviluppatore di Amazon per l'account che hai collegato al progetto nella Fase 1.
3. Sotto Test, scegli Development (Sviluppo) per abilitare il testing.
4. Specificare `ask hello node hello`. Il nome di invocazione predefinito per la competenza è `hello node`.
5. La competenza deve rispondere `Hello World!`.

Quando la competenza è abilitata nel simulatore Alexa, puoi richiamarla anche su un dispositivo abilitato per Alexa registrato al tuo account sviluppatore di Amazon. Per testare la competenza su un dispositivo, pronuncia Alexa, ask hello node to say hello.

Per ulteriori informazioni sul simulatore Alexa, consulta Test della competenza nella console sviluppatore.

Fase 3: esplora le risorse del progetto

Come parte della creazione del progetto, hai AWS CodeStar anche creato AWS risorse per tuo conto. Queste risorse includono un archivio di progetto che utilizza CodeCommit, una pipeline di distribuzione CodePipeline e una AWS Lambda funzione. È possibile accedere a queste risorse dalla barra di navigazione. Ad esempio, scegliendo Repository vengono visualizzati i dettagli relativi al CodeCommit repository. È possibile visualizzare lo stato di distribuzione della pipeline nella pagina Pipeline. È possibile visualizzare un elenco completo delle AWS risorse create come parte del progetto scegliendo Panoramica nella barra di navigazione. Questo elenco include i collegamenti per ciascuna risorsa.

Fase 4: effettua una modifica nella risposta della competenza

In questa fase, apporti una piccola modifica alla risposta della competenza per comprendere il ciclo di iterazione.

1. Nella barra di navigazione, scegli Repository. Scegli il link sotto Nome del deposito e il repository del tuo progetto si aprirà in una nuova scheda o finestra. Questo repository contiene la specifica di build (buildspec.yml), lo stack applicativo CloudFormation (template.yml), il file Readme e il codice sorgente della competenza nel formato pacchetto competenza (struttura del progetto).
2. Passa al file lambda > custom > index.js (in caso di Node.js). Questo file contiene il codice di gestione delle richieste, che utilizza il kit SDK ASK.
3. Scegli Modifica.
4. Sostituisci la stringa `Hello World!` alla riga 24 con la stringa `Hello. How are you?`.
5. Scorri fino alla fine del file. Inserisci il nome dell'autore, l'indirizzo e-mail e un messaggio di commit opzionale.
6. Scegli Commit changes (Conferma modifiche) per confermare le modifiche nel repository.
7. Torna al progetto AWS CodeStar e controlla la pagina Pipeline. Ora dovresti vedere la distribuzione della pipeline.

8. Quando la pipeline termina la distribuzione, testa di nuovo la competenza nel simulatore Alexa. La competenza ora deve rispondere con `Hello. How are you?`.

Fase 5: configura la workstation locale per la connessione al repository di progetto

In precedenza hai apportato una piccola modifica al codice sorgente direttamente dalla CodeCommit console. In questa fase configuri il repository di progetto con la workstation locale in modo da poter modificare e gestire il codice dalla riga di comando o dal tuo IDE preferito. La procedura seguente spiega come configurare gli strumenti a riga di comando.

1. Se necessario AWS CodeStar, accedi alla dashboard del progetto in.
2. Nella barra di navigazione, scegli IDE.
3. In Accedi al codice del tuo progetto, Visualizza le istruzioni nell'interfaccia a riga di comando.
4. Segui le istruzioni per completare le attività seguenti:
   a. Installa Git sulla workstation locale scaricandolo da un sito web come Git Downloads.
   b. Installa la AWS CLI. Per informazioni, consulta Installazione dell'interfaccia AWS a riga di comando.
   c. Configura la AWS CLI con la chiave di accesso utente IAM e la chiave segreta. Per informazioni, consulta Configurazione della AWS CLI.
   d. Clona il CodeCommit repository del progetto sulla tua workstation locale. Per ulteriori informazioni, consulta Connect to a CodeCommit Repository.

Fasi successive

Questo tutorial ti ha illustrato come iniziare a utilizzare una competenza di base. Per continuare il tuo percorso di sviluppo delle competenze, consulta le seguenti risorse.

- Scopri i fondamenti di una skill guardando How Alexa Skills Work e altri video sul canale Alexa Developers. YouTube
- Comprendere i vari componenti della competenza consultando la documentazione per il formato del pacchetto di competenza, gli schemi manifest delle competenze e gli schemi di modello di interazione.
- Trasforma la tua idea in una competenza consultando la documentazione di Alexa Skills Kit e ASK. SDKs

Tutorial: creare un progetto con un repository GitHub di sorgenti

Con AWS CodeStar, puoi configurare il tuo repository per creare, rivedere e unire le richieste pull con il tuo team di progetto.

In questo tutorial, creerai un progetto con un esempio di codice sorgente di un'applicazione web in un GitHub repository, una pipeline che distribuisce le modifiche e EC2 istanze in cui l'applicazione è ospitata nel cloud. Dopo la creazione del progetto, questo tutorial mostra come creare e unire una GitHub pull request che apporta una modifica alla home page dell'applicazione web.

Argomenti

Passaggio 1: crea il progetto e crea il tuo repository GitHub

In questo passaggio, utilizza la console per creare il progetto e creare una connessione al nuovo GitHub repository. Per accedere al tuo GitHub repository, crei una risorsa di connessione da AWS CodeStar utilizzare per gestire l'autorizzazione con. GitHub Quando il progetto viene creato, le relative risorse aggiuntive vengono fornite automaticamente.

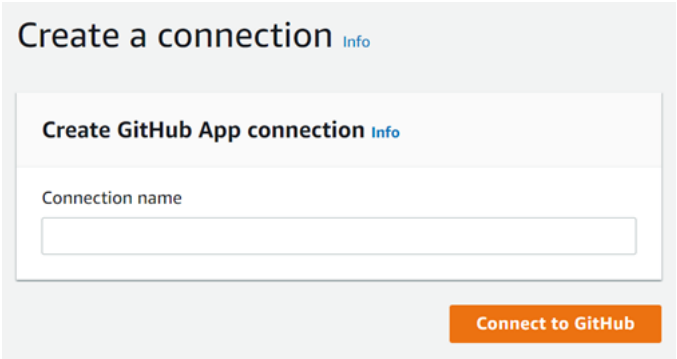
1. Accedere a Console di gestione AWS, quindi aprire la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.
2. Scegli la AWS regione in cui desideri creare il progetto e le relative risorse.
3. Nella AWS CodeStarpagina, scegli Crea progetto.
4. Nella pagina Scegli un modello di progetto, seleziona le caselle di EC2 controllo Applicazione Web, Node.js e Amazon. Quindi scegli tra i modelli disponibili per quel set di opzioni.

   Per ulteriori informazioni, consulta AWS CodeStar Modelli di progetto.
5. Scegli Next (Successivo).
6. Per Project name (Nome progetto), immettere un nome per il progetto (ad esempio, **`MyTeamProject`**). Se scegli un nome differente, assicurati di utilizzarlo in tutto il tutorial.
7. In Project repository, scegli GitHub.

8. Se hai scelto GitHub, dovrai scegliere o creare una risorsa di connessione. Se hai una connessione esistente, selezionala nel campo di ricerca. Altrimenti, creerai una nuova connessione qui. Scegli Connect a GitHub.

   Viene visualizzata la pagina Crea una connessione.

   > **Note**
   >
   > Per creare una connessione, è necessario disporre di un GitHub account. Se stai creando una connessione per un'organizzazione, devi essere il proprietario dell'organizzazione.



   a. In Crea connessione GitHub all'app, in Nome connessione, inserisci un nome per la connessione. Scegli Connect a GitHub.

      La GitHub pagina Connect to visualizza e mostra il campo GitHub App.

   b. In GitHub App, scegli l'installazione di un'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.

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

> **Note**
>
> 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.

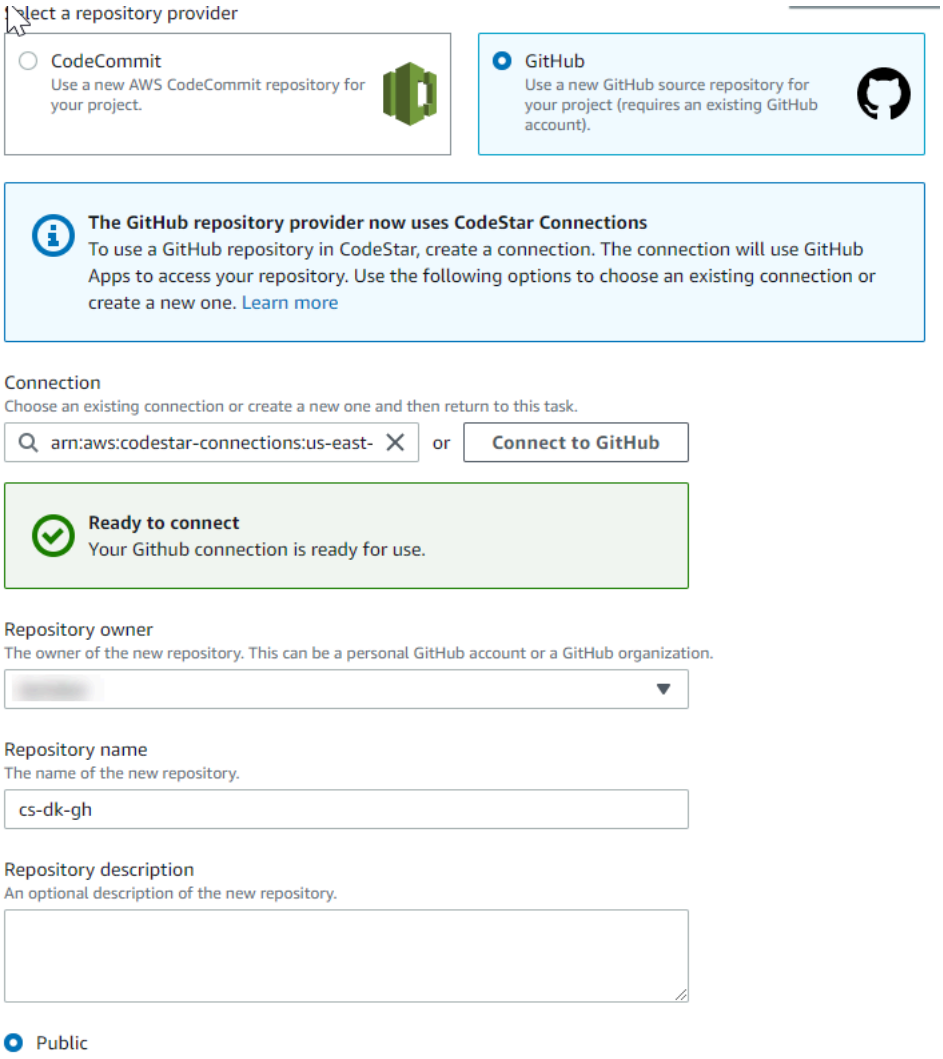
d. Se viene visualizzata la pagina Conferma la password per continuare, inserisci GitHub la password, quindi scegli Accedi.

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

f. Nella GitHub pagina Connect to, l'ID di installazione per la nuova installazione viene visualizzato in GitHubApp.

Dopo aver creato correttamente la connessione, nella pagina di CodeStar creazione del progetto viene visualizzato il messaggio Ready to connect.

> **Note**
>
> Puoi visualizzare la tua connessione in Impostazioni nella console Developer Tools. Per ulteriori informazioni, consulta Guida introduttiva alle connessioni.



g. Per il proprietario del repository, scegli l' GitHuborganizzazione o il tuo account personale. GitHub

h. Per Nome del repository, accetta il nome del GitHub repository predefinito o inseriscine uno diverso.

i. Scegli Pubblico o Privato.

> **Note**
>
> Se desideri utilizzarlo AWS Cloud9 come ambiente di sviluppo, devi scegliere un repository pubblico.

j. (Facoltativo) Per la descrizione del repository, inserisci una descrizione per il GitHub repository.

9. Configura le tue EC2 istanze Amazon in Amazon EC2 Configuration se il tuo progetto viene distribuito su EC2 istanze Amazon e desideri apportare modifiche. Ad esempio, è possibile scegliere tra i tipi di istanze disponibili per il progetto.

   In Coppia di chiavi, scegli la coppia di EC2 chiavi Amazon in cui hai creatoFase 4: creare una coppia di EC2 chiavi Amazon per AWS CodeStar i progetti. Seleziona Riconosco di avere accesso al file della chiave privata.
10. Scegli Next (Successivo).
11. Esaminare le risorse e i dettagli di configurazione.
12. Scegli Next (Avanti) oppure Create project (Crea progetto). (L'opzione visualizzata dipende dal modello di progetto).

    Attendi qualche minuto per la creazione del progetto.
13. Dopo aver creato il progetto, scegli Visualizza applicazione per visualizzare l'applicazione web.

Passaggio 2: Visualizza il codice sorgente

In questo passaggio vengono visualizzati il codice sorgente e gli strumenti che è possibile utilizzare per il repository dei sorgenti.

1. Nella barra di navigazione del progetto, scegli Repository.

   Per visualizzare un elenco di commit in GitHub, scegli Visualizza i commit. Verrà aperta la cronologia dei commit in. GitHub

   Per visualizzare i problemi, scegli la scheda Problemi relativa al tuo progetto. Per creare un nuovo problema in GitHub, scegli Crea GitHub problema. Verrà aperto il modulo di emissione del repository in GitHub.
2. Nella scheda Archivio, scegli il link sotto Nome archivio e il repository del tuo progetto si aprirà in una nuova scheda o finestra. Questo repository contiene il codice sorgente del tuo progetto.

Fase 3: Creare una GitHub Pull Request

In questo passaggio, apporti una piccola modifica al tuo codice sorgente e crei una pull request.

1. Nel GitHub, crea un nuovo ramo di funzionalità nel tuo repository. Scegli il campo a discesa del ramo principale e inserisci un nuovo ramo nel campo denominato. `feature-branch` Scegli Crea nuovo ramo. Il ramo viene creato e verificato automaticamente.
2. Nel GitHub, apporta una modifica al `feature-branch` ramo. Apri la cartella pubblica e apri il `index.html` file.
3. Nella AWS CodeStar console, in Richieste Pull, per creare una richiesta pull GitHub, scegli Crea richiesta pull. Questo apre il modulo di pull request del repository. GitHub In GitHub, scegli l'icona a forma di matita per modificare il file.

   Dopo`Congratulations!`, aggiungi la stringa `Well done, <name>!` e sostituiscila `<name>` con il tuo nome. Scegliere Commit changes (Applica modifiche). La modifica viene assegnata al tuo feature branch.
4. Nella AWS CodeStar console, scegli il tuo progetto. Scegli la scheda Repository. In Richieste pull, scegli Crea richiesta pull.

   Il modulo si apre in GitHub. Lascia il ramo principale nel ramo base. Per Compare to, scegli il tuo ramo di funzionalità. Visualizza la differenza.
5. In GitHub, scegli Crea pull request. Viene creata una richiesta pull denominata Update index.html.
6. Nella AWS CodeStar console, visualizza la nuova pull request. Scegli Unisci modifiche per confermare le modifiche al repository e unisci la pull request con il ramo principale del repository.
7. Torna al progetto AWS CodeStar e controlla la pagina Pipeline. Ora dovresti vedere la distribuzione della pipeline.
8. Dopo aver creato il progetto, scegli Visualizza applicazione per visualizzare l'applicazione web.

AWS CodeStar Modelli di progetto

AWS CodeStar i modelli di progetto consentono di iniziare con un'applicazione di esempio e di distribuirla utilizzando AWS risorse create per supportare il progetto di sviluppo. Quando scegli un modello di AWS CodeStar progetto, vengono forniti automaticamente il tipo di applicazione, il linguaggio di programmazione e la piattaforma di calcolo. Dopo avere creato progetti con applicazioni Web, servizi Web, competenze Alexa e pagine Web statiche, potrai sostituire l'applicazione di esempio con un'applicazione personalizzata.

Dopo aver AWS CodeStar creato il progetto, puoi modificare le AWS risorse che supportano la distribuzione dell'applicazione. AWS CodeStar collabora con AWS CloudFormation per consentirti di utilizzare il codice per creare servizi di supporto e server/piattaforme serverless nel cloud. AWS CloudFormation consente di modellare l'intera infrastruttura in un file di testo.

Argomenti

AWS CodeStar File e risorse di progetto

Un AWS CodeStar progetto è una combinazione di codice sorgente e risorse create per distribuire il codice. Le risorse che supportano la compilazione, il rilascio e la distribuzione del codice sono denominate risorse della toolchain. Al momento della creazione del progetto, un CloudFormation modello fornisce le risorse della toolchain in una pipeline integration/continuous deployment (CI/CD (continua).

Puoi utilizzarlo AWS CodeStar per creare progetti in due modi, a seconda del tuo livello di esperienza nella creazione di AWS risorse:

- Quando si utilizza la console per creare un progetto, AWS CodeStar crea le risorse della toolchain, incluso il repository, e popola il repository con esempi di codice applicativo e file di progetto. La console può essere utilizzata per impostare rapidamente progetti di esempio in base a una serie di opzioni di progetto preconfigurate.
- Quando si utilizza la CLI per creare un progetto, si fornisce il CloudFormation modello che crea le risorse della toolchain e il codice sorgente dell'applicazione. Usa la CLI per consentire di AWS

CodeStar creare il tuo progetto dal tuo modello e poi popola il tuo repository con il tuo codice di esempio.

Un AWS CodeStar progetto fornisce un unico punto di gestione. Per impostare un progetto di esempio, puoi utilizzare la procedura guidata Create project (Crea progetto) nella console e quindi utilizzare il progetto creato come piattaforma di collaborazione per la gestione di autorizzazioni e risorse del team. Per ulteriori informazioni, consulta Che cos'è AWS CodeStar?. Se utilizzi la console per creare un progetto, il codice sorgente viene fornito come codice di esempio e le risorse CI/CD della toolchain vengono create automaticamente.

Quando crei un progetto nella console, effettua il AWS CodeStar provisioning delle seguenti risorse:

- Un archivio di codice in GitHub o CodeCommit.
- Nel repository del progetto, un file `README.md` con informazioni dettagliate su file e directory.
- Nel repository del progetto, un file `template.yml` con la definizione per lo stack di runtime dell'applicazione. Questo file viene utilizzato per aggiungere o modificare risorse di progetto che non sono risorse della toolchain, ad esempio le AWS risorse utilizzate per le notifiche, il supporto del database, il monitoraggio e la traccia.
- AWS servizi e risorse creati in connessione con la tua pipeline, come il bucket di artefatti Amazon S3, CloudWatch Amazon Events e i ruoli di servizio correlati.
- Un'applicazione di esempio funzionante con codice sorgente completo e un endpoint HTTP pubblico.
- Una risorsa di AWS calcolo, basata sul tipo di modello di progetto: AWS CodeStar
  - Una funzione Lambda.
  - Un' EC2 istanza Amazon.
  - Un AWS Elastic Beanstalk ambiente.
- A partire dal 6 dicembre 2018 PDT:
  - Un limite di autorizzazioni, ovvero una policy IAM specializzata per controllare l'accesso alle risorse di progetto. Ai ruoli nel progetto di esempio è associato per default il limite di autorizzazione. Per ulteriori informazioni, consulta la pagina sul limite di autorizzazioni IAM per ruoli dipendente.
  - Un ruolo CloudFormation IAM per la creazione di risorse di progetto CloudFormation che include le autorizzazioni per tutte le risorse CloudFormation supportate, inclusi i ruoli IAM.
  - Un ruolo IAM toolchain.

    - Ruoli di esecuzione per Lambda definiti nello stack di applicazioni, che è possibile modificare.
- Prima del 6 dicembre 2018 PDT:
    - Un ruolo CloudFormation IAM per la creazione di risorse di progetto con supporto per un set limitato di CloudFormation risorse.
    - Un ruolo IAM per la creazione di una CodePipeline risorsa.
    - Un ruolo IAM per la creazione di una CodeBuild risorsa.
    - Un ruolo IAM per la creazione di una CodeDeploy risorsa, se applicabile al tipo di progetto.
    - Un ruolo IAM per la creazione dell'app EC2 web Amazon, se applicabile al tipo di progetto.
    - Un ruolo IAM per la creazione di una risorsa CloudWatch Events.
    - Un ruolo di esecuzione per Lambda che viene modificato dinamicamente per includere un set parziale di risorse.

Il progetto include pagine di dettaglio che mostrano lo stato e contengono collegamenti alla gestione del team, collegamenti alle istruzioni di configurazione del nostro repository e una cronologia dei commit delle modifiche al codice sorgente nel repository. IDEs Si possono anche selezionare strumenti per la connessione a strumenti esterni per il monitoraggio di problemi, ad esempio Jira.

Per iniziare: scegli un modello di progetto

Quando scegli un AWS CodeStar progetto nella console, scegli tra una serie di opzioni preconfigurate con codice di esempio e risorse per iniziare rapidamente. Queste opzioni sono chiamate modelli di progetto. Ogni modello di AWS CodeStar progetto è composto da un linguaggio di programmazione, un tipo di applicazione e una piattaforma di calcolo. La combinazione selezionata determina il modello di progetto.

Scegli una piattaforma di calcolo per il modello

Ogni modello permette di configurare uno dei seguenti tipi di piattaforma di calcolo:

- Quando scegli un AWS Elastic Beanstalk progetto, lo distribuisci in un AWS Elastic Beanstalk ambiente su istanze Amazon Elastic Compute Cloud nel cloud.
- Quando scegli un EC2 progetto Amazon, AWS CodeStar crea EC2 istanze Linux per ospitare la tua applicazione nel cloud. I membri del team di progetto possono accedere alle istanze e il team utilizza la coppia di chiavi che fornisci a SSH nelle tue istanze Amazon EC2 . AWS CodeStar

dispone anche di un SSH gestito che utilizza le autorizzazioni dei membri del team per gestire le connessioni di key pair.

- Se lo desideri AWS Lambda, AWS CodeStar crea un ambiente serverless accessibile tramite Amazon API Gateway, senza istanze o server da gestire.

Scegli un tipo di applicazione modello

Ogni modello ti permette di configurare uno dei seguenti tipi di applicazione:

- Servizio Web

  Un servizio Web viene utilizzato per attività eseguite in background, come le chiamate. APIs Dopo aver AWS CodeStar creato il progetto di servizio web di esempio, puoi scegliere l'URL dell'endpoint per visualizzare l'output di Hello World, ma l'uso principale di questo tipo di applicazione non è come interfaccia utente (UI). I modelli di AWS CodeStar progetto in questa categoria supportano lo sviluppo in Ruby, Java, ASP.NET, PHP, Node.js e altro ancora.

- Applicazione Web

  Un'applicazione Web offre un'interfaccia utente. Dopo aver AWS CodeStar creato il progetto di applicazione web di esempio, puoi scegliere l'URL dell'endpoint per vedere un'applicazione web interattiva. I modelli di AWS CodeStar progetto in questa categoria supportano lo sviluppo in Ruby, Java, ASP.NET, PHP, Node.js e altri.

- Pagina Web statica

  Puoi scegliere questo modello per creare un progetto per un sito Web HTML. I modelli di AWS CodeStar progetto in questa categoria supportano lo sviluppo in. HTML5

- Competenza di Alexa

  Scegli questo modello se desideri un progetto per una competenza Alexa con una funzione AWS Lambda . Quando crei il progetto di abilità, AWS CodeStar restituisce un Amazon Resource Name (ARN) che puoi utilizzare come endpoint di servizio. Per ulteriori informazioni, consulta Host a Custom Skill as an AWS Lambda Function.

> **Note**
>
> Le funzioni Lambda per le competenze Alexa sono supportate solo nelle regioni Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), UE (Irlanda) e Asia Pacifico (Tokyo).

- Regola di configurazione

  Scegli questo modello se desideri un progetto per una AWS Config regola che ti consenta di automatizzare le regole tra le AWS risorse del tuo account. La funzione restituisce un ARN che puoi utilizzare come endpoint del servizio per la regola.

Scegli un linguaggio di programmazione per il modello

Scegliendo un modello di progetto, puoi selezionare un linguaggio di programmazione, come Ruby, Java, ASP.NET, PHP, Node.js e altri ancora.

Come apportare modifiche al progetto AWS CodeStar

Per aggiornare un progetto puoi modificare:

- Il codice di esempio e le risorse del linguaggio di programmazione per l'applicazione.
- Le risorse che costituiscono l'infrastruttura in cui è archiviata e distribuita l'applicazione (sistemi operativi, applicazioni e servizi di supporto, parametri di distribuzione e piattaforma di calcolo nel cloud). Le risorse dell'applicazione possono essere modificate nel file `template.yml`, ovvero il file AWS CloudFormation che modella l'ambiente di runtime dell'applicazione.

> **Note**
>
> Se stai lavorando a un AWS CodeStar progetto Alexa Skills, non puoi apportare modifiche alla skill al di fuori dell'archivio di AWS CodeStar origine (CodeCommit o GitHub). Se modifichi la competenza nel portale per sviluppatori Alexa, la modifica potrebbe non essere visibile nel repository di origine e le due versioni non saranno sincronizzate.

Modificare il codice sorgente dell'applicazione e le modifiche push

Per modificare il codice sorgente di esempio, gli script e altri file di origine dell'applicazione, puoi modificare i file nel repository di origine nei modi seguenti:

- Utilizzo della modalità Modifica in CodeCommit o. GitHub
- Apertura del progetto in un IDE, ad esempio AWS Cloud9.
- Clonando il repository a livello locale e quindi eseguendo il commit e il push delle modifiche. Per informazioni, consultare Fase 4: Applica una modifica.

Modifica dell risorse dell'applicazione con il file template.yml

Invece di modificare manualmente una risorsa dell'infrastruttura, utilizzala AWS CloudFormation per modellare e distribuire le risorse di runtime dell'applicazione.

Per modificare o aggiungere una risorsa dell'applicazione nello stack di runtime, ad esempio una funzione Lambda, puoi modificare il file `template.yml` nel repository del progetto. Puoi aggiungere qualsiasi risorsa disponibile sotto forma di risorsa AWS CloudFormation .

Per modificare il codice o le impostazioni di una AWS Lambda funzione, vedere. Aggiungere una risorsa a un progetto

Modifica il `template.yml` file nel repository del progetto per aggiungere il tipo di AWS CloudFormation risorse che sono le risorse dell'applicazione. Quando aggiungi una risorsa applicativa alla `Resources` sezione del `template.yml` file AWS CloudFormation e AWS CodeStar crei la risorsa automaticamente. Per un elenco delle AWS CloudFormation risorse e delle relative proprietà richieste, consulta AWS Resource Types Reference. Per ulteriori informazioni, consulta questo esempio in Fase 1: Modifica il ruolo del CloudFormation lavoratore in IAM.

AWS CodeStar consente di implementare le migliori pratiche configurando e modellando l'ambiente di runtime dell'applicazione.

Come gestire le autorizzazioni per modificare le risorse dell'applicazione

Quando si utilizza AWS CloudFormation per aggiungere risorse applicative in fase di esecuzione, ad esempio una funzione Lambda, il ruolo di AWS CloudFormation lavoratore può utilizzare le autorizzazioni di cui già dispone. Per alcune risorse applicative di runtime, è necessario impostare

manualmente le autorizzazioni del ruolo lavoratore di AWS CloudFormation prima di modificare il file `template.yml`.

Per un esempio di modifica delle autorizzazioni del ruolo di AWS CloudFormation lavoratore, consulta. Fase 5: Aggiungere autorizzazioni a livello di risorsa con un policy inline

AWS CodeStar Le migliori pratiche

AWS CodeStar è integrato con una serie di prodotti e servizi. Le sezioni seguenti descrivono le migliori pratiche per AWS CodeStar i prodotti e i servizi correlati.

Argomenti

Best practice relative alla sicurezza per risorse AWS CodeStar

Dovresti applicare regolarmente patch e rivedere le best practice di sicurezza per le dipendenze utilizzate dall'applicazione. Utilizza queste best practice di sicurezza per aggiornare il tuo codice di esempio e mantenere il progetto in un ambiente di produzione:

- Controlla gli annunci e gli aggiornamenti di sicurezza in corso per il tuo framework.
- Prima di distribuire il tuo progetto, segui le best practice sviluppate per il tuo framework.
- Ricontrolla periodicamente le dipendenze per il framework e aggiornale se necessario.
- Ogni AWS CodeStar modello contiene istruzioni di configurazione per il linguaggio di programmazione in uso. Vedi il file `README.md` nella repository di origine del tuo progetto.
- Come best practice per isolare le risorse del progetto, gestisci l'accesso alle risorse con privilegi minimi utilizzando una strategia multi-account AWS , come introdotta in. Sicurezza in AWS CodeStar

Best practice per le versioni di impostazione per le dipendenze

Il codice sorgente di esempio del AWS CodeStar progetto utilizza le dipendenze elencate nel file del repository di origine. `package.json` Come best practice, impostare sempre le dipendenze in modo che puntino a una versione specifica. Questa prassi è nota come puntare la versione. Non è consigliabile impostare la versione a `latest` perché può introdurre modifiche che potrebbero interrompere l'applicazione senza preavviso.

Monitoraggio e registrazione di best practice per risorse AWS CodeStar

Puoi utilizzare le funzionalità di registrazione AWS per determinare le azioni intraprese dagli utenti nel tuo account e le risorse utilizzate. I file di log visualizzano:

- La data e l'ora delle operazioni.
- L'indirizzo IP di origine di un'operazione.
- Quali operazioni non sono riuscite a causa di autorizzazioni inadeguate.

AWS CloudTrail può essere utilizzato per registrare le chiamate AWS API e gli eventi correlati effettuati da o per conto di un AWS account. Per ulteriori informazioni, consulta Registrazione delle chiamate AWS CodeStar API con AWS CloudTrail.

Lavorare con progetti in AWS CodeStar

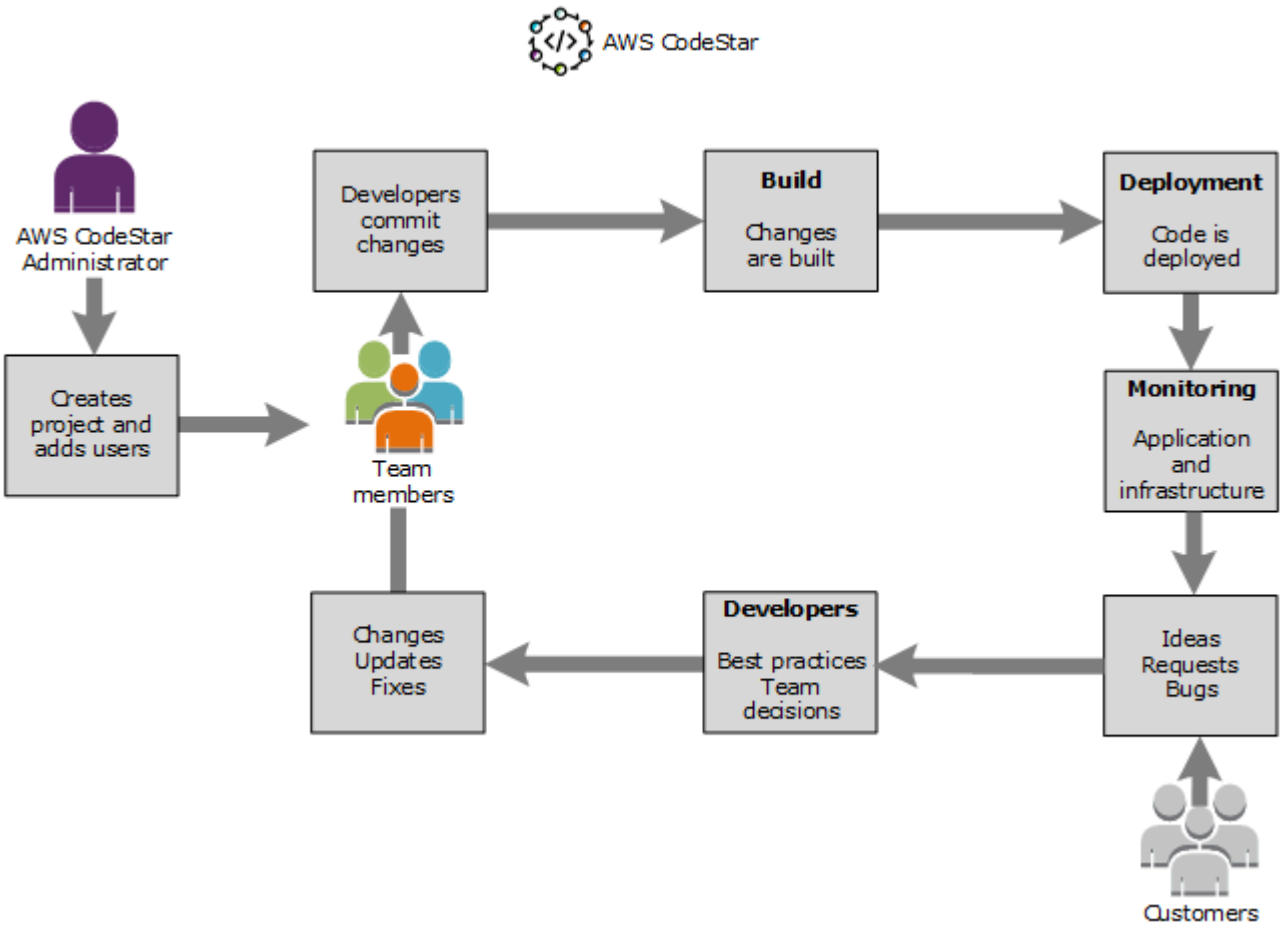
Quando utilizzi un modello di AWS CodeStar progetto, puoi creare rapidamente un progetto già configurato con le risorse necessarie, tra cui:

- Repository del codice sorgente
- Ambiente della build
- Distribuzione e risorse di hosting
- Linguaggio di programmazione

Il modello include anche un codice sorgente di esempio in modo da poter iniziare subito a lavorare sul progetto.

Dopo aver creato un progetto, puoi aggiungere o rimuovere le risorse, personalizzare il pannello di controllo del progetto e monitorare l'avanzamento.

Il diagramma seguente mostra un flusso di lavoro di base in un AWS CodeStar progetto.



Il flusso di lavoro di base nel diagramma mostra uno sviluppatore con la `AWSCodeStarFullAccess` politica applicata che crea un progetto e vi aggiunge membri del team. Svilupptore e team scrivono, creano, testano e distribuiscono il codice. Il pannello di controllo del progetto offre una serie di strumenti che possono essere utilizzati in tempo reale per visualizzare l'attività delle applicazioni e monitorare le build, il flusso di codice nella pipeline di distribuzione e altro ancora. Il team utilizza il riquadro del team wiki per condividere informazioni, best practice e collegamenti. Il team integra il software di gestione dei problemi per tenere traccia dei progressi e delle attività. Quando i clienti inviano richieste e feedback, il team aggiunge queste informazioni al progetto e le integra nella pianificazione e nello sviluppo del progetto. Man mano che il progetto si sviluppa, il team aggiunge altri membri del team per supportare il codice di base.

Crea un progetto in AWS CodeStar

Si utilizza la AWS CodeStar console per creare un progetto. Se utilizzi un modello di progetto, le risorse necessarie saranno già configurate. Il modello include anche il codice di esempio che puoi utilizzare per avviare la codifica.

Per creare un progetto, accedi a Console di gestione AWS con un utente IAM che dispone della `AWSCodeStarFullAccess` policy o di autorizzazioni equivalenti. Per ulteriori informazioni, consulta Configurazione AWS CodeStar.

> **Note**
>
> È necessario completare i passaggi indicati Configurazione AWS CodeStar prima di poter completare le procedure in questo argomento.

Argomenti

- Creazione di un progetto in AWS CodeStar (console)
- Crea un progetto in AWS CodeStar (AWS CLI)

Creazione di un progetto in AWS CodeStar (console)

Utilizzate la AWS CodeStar console per creare un progetto.

Per creare un progetto in AWS CodeStar

1. Accedere a Console di gestione AWS, quindi aprire la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.

   Assicurati di aver effettuato l'accesso alla AWS regione in cui desideri creare il progetto e le relative risorse. Ad esempio, per creare un progetto negli Stati Uniti orientali (Ohio), assicurati di aver selezionato quella AWS regione. Per informazioni sulle AWS regioni in cui AWS CodeStar è disponibile, consulta Regioni ed endpoint nella Guida AWS generale.
2. Nella AWS CodeStarpagina, scegli Crea progetto.
3. Nella pagina Scegli un modello di progetto, scegli il tipo di progetto dall'elenco dei modelli di AWS CodeStar progetto. Puoi utilizzare la barra dei filtri per ridurre la scelta. Ad esempio, per un progetto di applicazione Web scritto in Node.js da distribuire su EC2 istanze Amazon, seleziona le caselle di EC2 controllo Applicazione Web, Node.js e Amazon. Quindi scegli tra i modelli disponibili per quel set di opzioni.

   Per ulteriori informazioni, consulta AWS CodeStar Modelli di progetto.
4. Scegli Next (Successivo).

5. Nel campo di immissione del testo del nome del progetto, inserisci un nome per il progetto, ad esempio. *My First Project* In Project ID, l'ID del progetto deriva dal nome di questo progetto, ma è limitato a 15 caratteri.

   Ad esempio, l'ID di default per un progetto denominato *My First Project* è *my-first-projec*. Questo ID di progetto è la base per i nomi di tutte le risorse associate al progetto. AWS CodeStar utilizza questo ID di progetto come parte dell'URL per il repository di codice e per i nomi dei ruoli e delle politiche di accesso di sicurezza correlati in IAM. Dopo la creazione del progetto. l'ID del progetto non può essere modificato. Per modificare l'ID del progetto prima di creare il progetto, in ID progetto, inserisci l'ID che desideri utilizzare.

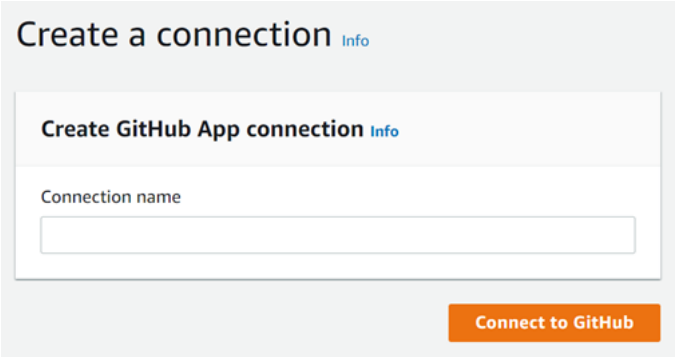
   Per informazioni sui limiti imposti ai nomi e ai progetti dei progetti IDs, consultaLimiti in AWS CodeStar.

   > **Note**
   >
   > Il progetto IDs deve essere unico per il tuo AWS account in una AWS regione.

6. Scegli il fornitore del repository, AWS CodeCommitoppure GitHub.
7. Se hai scelto AWS CodeCommit, per Nome del repository, accetta il nome del AWS CodeCommit repository predefinito o inseriscine uno diverso. Quindi vai avanti al passaggio 9.
8. Se hai scelto GitHub, devi scegliere o creare una risorsa di connessione. Se hai una connessione esistente, selezionala nel campo di ricerca. Altrimenti, crea subito una nuova connessione. Scegli Connect a GitHub.

   Viene visualizzata la pagina Crea una connessione.

   > **Note**
   >
   > Per creare una connessione, è necessario disporre di un GitHub account. Se stai creando una connessione per un'organizzazione, devi essere il proprietario dell'organizzazione.



a. In Crea connessione all' GitHub app, nel campo di testo di immissione del nome della connessione, inserisci un nome per la connessione. Scegli Connect a GitHub.

   La GitHub pagina Connect to visualizza e mostra il campo GitHub App.

b. In GitHub App, scegli l'installazione di un'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.

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

> **Note**
>
> 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.

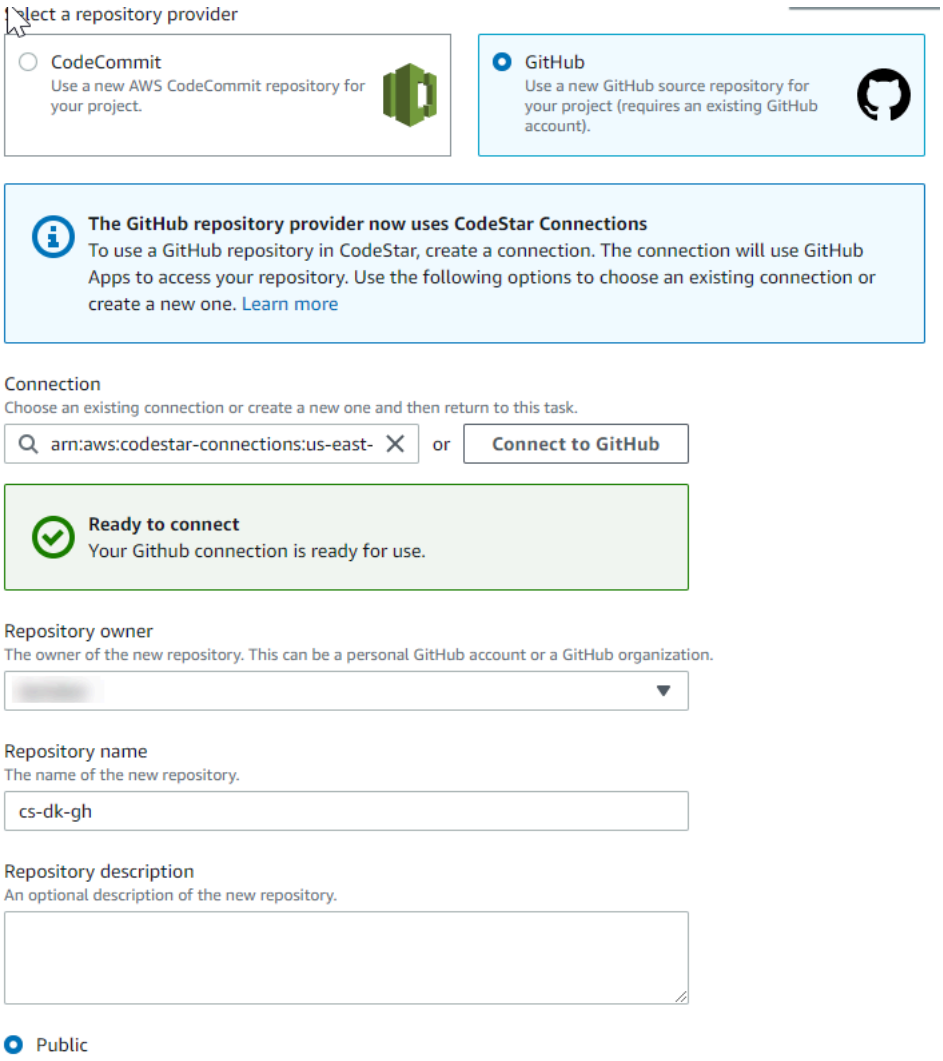
d. Se viene visualizzata la pagina Conferma la password per continuare, inserisci GitHub la password, quindi scegli Accedi.

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

f. Nella GitHub pagina Connect to, l'ID di installazione per la nuova installazione viene visualizzato nel campo di immissione di testo GitHub App.

Dopo aver creato la connessione, nella pagina di CodeStar creazione del progetto viene visualizzato il messaggio Ready to connect.

> **Note**
>
> Puoi visualizzare la tua connessione in Impostazioni nella console Developer Tools. Per ulteriori informazioni, consulta Guida introduttiva alle connessioni.



g. Per il proprietario del repository, scegli l' GitHub organizzazione o il tuo account personale. GitHub

h. Per Nome del repository, accetta il nome del GitHub repository predefinito o inseriscine uno diverso.

i. Scegli Pubblico o Privato.

> **Note**
>
> Per utilizzarlo AWS Cloud9 come ambiente di sviluppo, devi scegliere Pubblico.

j. (Facoltativo) Per la descrizione del repository, inserite una descrizione per il GitHub repository.

> **Note**
>
> Se scegli un modello di progetto Alexa Skill, devi collegare un account sviluppatore Amazon. Per ulteriori informazioni su come lavorare con i progetti Alexa Skill, consulta. Tutorial: crea un progetto Alexa Skill in AWS CodeStar

9. Se il tuo progetto è distribuito su EC2 istanze Amazon e desideri apportare modifiche, configura le EC2 istanze Amazon in Amazon Configuration. EC2 Ad esempio, è possibile scegliere tra i tipi di istanze disponibili per il progetto.

> **Note**
>
> I diversi tipi di EC2 istanze Amazon offrono diversi livelli di potenza di calcolo e possono avere costi associati diversi. Per ulteriori informazioni, consulta i tipi di EC2 istanze Amazon e EC2 i prezzi di Amazon.
> Se disponi di più di un cloud privato virtuale (VPC) o più sottoreti create in Amazon Virtual Private Cloud, puoi anche scegliere il VPC e la sottorete da utilizzare. Tuttavia, se scegli un tipo di EC2 istanza Amazon che non è supportato su istanze dedicate, non puoi scegliere un VPC la cui tenancy dell'istanza è impostata su Dedicato.
> Per ulteriori informazioni, consulta Che cos'è Amazon VPC? e nozioni di base sulle istanze dedicate.

In Coppia di chiavi, scegli la coppia di EC2 chiavi Amazon in cui hai creatoFase 4: creare una coppia di EC2 chiavi Amazon per AWS CodeStar i progetti. Seleziona Riconosco di avere accesso al file della chiave privata.

10. Scegli Next (Successivo).
11. Esaminare le risorse e i dettagli di configurazione.
12. Scegli Next (Avanti) oppure Create project (Crea progetto). (L'opzione visualizzata dipende dal modello di progetto).

    Potrebbero essere necessari alcuni minuti per creare il progetto, incluso il repository.
13. Dopo che il progetto ha un repository, puoi utilizzare la pagina Repository per configurarne l'accesso. Utilizza i link nei passaggi successivi per configurare un IDE, impostare il monitoraggio dei problemi o aggiungere membri del team al progetto.

Durante la creazione del progetto, è possibile aggiungere membri del team o configurare l'accesso al repository del progetto dalla riga di comando o dall'IDE preferito.

Crea un progetto in AWS CodeStar (AWS CLI)

Un AWS CodeStar progetto è una combinazione di codice sorgente e risorse create per distribuire il codice. Le risorse che supportano la compilazione, il rilascio e la distribuzione del codice sono denominate risorse della toolchain. Al momento della creazione del progetto, un CloudFormation modello fornisce le risorse della toolchain in una pipeline integration/continuous deployment (CI/CD (continua).

Quando utilizzi la console per creare un progetto, il modello di toolchain viene creato per te. Quando si utilizza il AWS CLI per creare un progetto, si crea il modello di toolchain che crea le risorse della toolchain.

Per una toolchain completa sono richieste le seguenti risorse consigliate:

1. Un GitHub repository CodeCommit or che contiene il codice sorgente.
2. Una CodePipeline pipeline configurata per ascoltare le modifiche al tuo repository.
   a. Quando lo utilizzi CodeBuild per eseguire test unitari o di integrazione, ti consigliamo di aggiungere una fase di compilazione alla pipeline per creare artefatti di compilazione.
   b. Ti consigliamo di aggiungere alla tua pipeline una fase di distribuzione che utilizzi CodeDeploy o distribuisca gli artefatti CloudFormation di build e il codice sorgente nell'infrastruttura di runtime.

> **Note**
>
> Poiché CodePipeline richiede almeno due fasi in una pipeline e la prima fase deve essere la fase di origine, aggiungi una fase di compilazione o distribuzione come seconda fase.

AWS CodeStar Le toolchain sono definite come modelli. CloudFormation

Per un tutorial dettagliato di questa attività e della configurazione delle risorse di esempio, consultare Tutorial: crea un progetto AWS CodeStar con AWS CLI.

Prerequisiti:

Quando crei un progetto, devi fornire i seguenti parametri in un file di input. Se quanto segue non viene fornito, AWS CodeStar crea un progetto vuoto.

- Codice sorgente. Se questo parametro è incluso nella tua richiesta, devi includere anche un modello di toolchain.
  - Il codice sorgente deve includere il codice dell'applicazione richiesto per l'esecuzione del progetto.
  - Il codice sorgente deve includere tutti i file di configurazione richiesti, ad esempio buildspec.yml per un CodeBuild progetto o appspec.yml per una distribuzione. CodeDeploy
  - È possibile includere elementi opzionali nel codice sorgente, ad esempio un README o un template.yml per risorse non appartenenti alla toolchain. AWS
- modello di toolchain. Il modello di toolchain fornisce le AWS risorse e i ruoli IAM da gestire per il progetto.
- Posizione di origine. Se per il tuo progetto specifichi un codice sorgente e un modello di toolchain, devi fornire una posizione. Carica i tuoi file sorgente e il tuo modello di toolchain nel bucket Amazon S3. AWS CodeStar recupera i file e li usa per creare il progetto.

> **Important**
>
> Assicurati di configurare la AWS regione preferita in. AWS CLI Il progetto viene creato nella AWS regione configurata in AWS CLI.

1. Eseguire il comando create-project e includere il parametro `--generate-cli-skeleton`:

```
aws codestar create-project --generate-cli-skeleton
```

Nell'output vengono visualizzati dati in formato JSON. Copia i dati in un file (ad esempio,*input.json*) in una posizione del computer locale o dell'istanza in cui AWS CLI è installato. Modificare i dati copiati come segue, quindi salvare i risultati.

```
{
    "name": "project-name",
    "id": "project-id",
    "description": "description",
    "sourceCode": [
        {
            "source": {
                "s3": {
                    "bucketName": "s3-bucket-name",
                    "bucketKey": "s3-bucket-object-key"
                }
            },
            "destination": {
                "codeCommit": {
                    "name": "codecommit-repository-name"
                },
                "gitHub": {
                    "name": "github-repository-name",
                    "description": "github-repository-description",
                    "type": "github-repository-type",
                    "owner": "github-repository-owner",
                    "privateRepository": true,
                    "issuesEnabled": true,
                    "token": "github-personal-access-token"
                }
            }
        }
    ],
    "toolchain": {
        "source": {
            "s3": {
                "bucketName": "s3-bucket-name",
                "bucketKey": "s3-bucket-object-key"
            }
```

```
        },
        "roleArn": "service-role-arn",
        "stackParameters": {
            "KeyName": "key-name"
        }
    },
    "tags": {
        "KeyName": "key-name"
    }
}
```

Sostituisci quanto segue:

- *project-name*: richiesto. Il nome descrittivo per questo AWS CodeStar progetto.
- *project-id*: richiesto. L'ID del AWS CodeStar progetto.

> **Note**
>
> Al momento della creazione di un progetto, è necessario disporre di un ID del progetto univoco. Se si invia un file di input con un ID del progetto esistente, si riceverà un errore.

- *description*: facoltativo. La descrizione di questo AWS CodeStar progetto.
- *sourceCode*: facoltativo. Le informazioni di configurazione del codice sorgente fornito per il progetto. Al momento, è supportato un singolo oggetto `sourceCode`. Ogni `sourceCode` oggetto contiene informazioni sulla posizione da cui viene recuperato il codice sorgente AWS CodeStar e sulla destinazione in cui viene compilato il codice sorgente.
  - *source*: richiesto. Definisce il percorso in cui è stato caricato il codice sorgente. L'unica fonte supportata è Amazon S3. AWS CodeStar recupera il codice sorgente e lo include nel repository dopo la creazione del progetto.
    - *S3*: facoltativo. La posizione Amazon S3 del tuo codice sorgente.
      - *bucket-name*: Il bucket che contiene il codice sorgente.
      - *bucket-key*: Il prefisso del bucket e la chiave dell'oggetto che puntano al file.zip che contiene il codice sorgente (ad esempio,). `src.zip`
  - *destination*: facoltativo. Le posizioni di destinazione in cui il codice sorgente deve essere compilato quando viene creato il progetto. Le destinazioni supportate per il codice sorgente sono e. CodeCommit GitHub

È possibile fornire solo una di queste due opzioni:

- *codeCommit*: L'unico attributo obbligatorio è il nome del CodeCommit repository che dovrebbe contenere il codice sorgente. Questo repository deve trovarsi nel modello di toolchain.

  > **Note**
  >
  > Infatti CodeCommit, è necessario fornire il nome del repository definito nello stack della toolchain. AWS CodeStar inizializza questo repository con il codice sorgente fornito in Amazon S3.

- *gitHub*: Questo oggetto rappresenta le informazioni necessarie per creare il GitHub repository e inserirlo con il codice sorgente. Se si sceglie un GitHub repository, sono necessari i seguenti valori.

  > **Note**
  >
  > Infatti GitHub, non è possibile specificare un GitHub repository esistente. AWS CodeStar ne crea uno per te e popola questo repository con il codice sorgente che hai caricato su Amazon S3. AWS CodeStar utilizza le seguenti informazioni per creare il tuo repository in. GitHub

  - *name*: richiesto. Il nome del tuo GitHub repository.
  - *description*: richiesto. La descrizione del tuo GitHub repository.
  - *type*: richiesto. Il tipo di GitHub repository. I valori validi sono User o Organization.
  - *owner*: richiesto. Il nome GitHub utente del proprietario del repository. Se il repository deve essere di proprietà di un' GitHub organizzazione, fornisci il nome dell'organizzazione.
  - *privateRepository*: richiesto. Per definire se il repository è privato o pubblico. I valori validi sono true o false.
  - *issuesEnabled*: richiesto. Se desideri abilitare i problemi in GitHub questo repository. I valori validi sono true o false.
  - *token*: facoltativo. Si tratta di un token di accesso personale AWS CodeStar utilizzato per accedere al tuo GitHub account. Il token deve contenere i seguenti ambiti: repo,

user e admin:repo_hook. Per recuperare un token di accesso personale da GitHub, consulta Creazione di un token di accesso personale per la riga di comando sul GitHub sito Web.

> **Note**
>
> Se utilizzi la CLI per creare un progetto con un repository di GitHub origine, AWS CodeStar utilizza il tuo token per accedere al repository tramite app. OAuth Se utilizzi la console per creare un progetto con un repository di origine, AWS CodeStar utilizza una GitHub risorsa di connessione, che accede al repository con le app. GitHub

- *`toolchain`*: Informazioni sulla toolchain CI/CD da configurare al momento della creazione del progetto. Ciò include il percorso sul quale è stato caricato il modello di toolchain. Il modello crea lo stack CloudFormation che contiene le risorse della toolchain. Ciò include anche eventuali sostituzioni dei parametri a cui CloudFormation fare riferimento e il ruolo da utilizzare per creare lo stack. AWS CodeStar recupera il modello e lo utilizza CloudFormation per eseguire il modello.
  - *`source`*: richiesto. La posizione del modello della toolchain. Amazon S3 è l'unica posizione di origine supportata.
    - *`S3`*: facoltativo. La posizione Amazon S3 in cui hai caricato il modello di toolchain.
      - *`bucket-name`*: nome del bucket Amazon S3.
      - *`bucket-key`*: il prefisso del bucket e la chiave dell'oggetto che puntano al file .yml o .json che contiene il modello della toolchain (ad esempio,). `files/toolchain.yml`
  - *`stackParameters`*: facoltativo. Contiene coppie chiave-valore da passare a CloudFormation. Si tratta dei parametri, se disponibili, ai quali il modello di toolchain fa riferimento.
  - *`role`*: facoltativo. Il ruolo utilizzato per creare le risorse della toolchain nell'account dell'utente. Il ruolo è richiesto come di seguito specificato:
    - Se il ruolo non viene fornito, AWS CodeStar utilizza il ruolo di servizio predefinito creato per il tuo account se la toolchain è un modello di avvio rapido. AWS CodeStar Se il ruolo del servizio non esiste nell'account dell'utente, è possibile crearne uno. Per informazioni, consultare Fase 2: Creare il ruolo AWS CodeStar di servizio.

- Se stai caricando e utilizzando il tuo modello personalizzato di toolchain è necessario specificare il ruolo. È possibile creare un ruolo in base al ruolo del servizio e alla dichiarazione di policy di AWS CodeStar . Per un esempio di questa dichiarazione di policy, consulta AWSCodeStarServiceRole Politica.

- *tags*: facoltativo. I tag allegati al tuo AWS CodeStar progetto.

> **Note**
>
> Questi tag non sono collegati alle risorse contenute nel progetto.

2. Passare alla directory contenente il file appena salvato ed eseguire nuovamente il comando create-project. Includere il parametro `--cli-input-json`.

```
aws codestar create-project --cli-input-json file://input.json
```

3. Se eseguito correttamente, nell'output compaiono dei dati simili ai seguenti:

```
{
    "id": "project-ID",
    "arn": "arn"
}
```

- L'output contiene informazioni sul nuovo progetto.:
  - Il valore `id` rappresenta l'ID del progetto.
  - Il valore `arn` rappresenta l'ARN del progetto.

4. Per controllare lo stato della creazione del progetto, utilizzare il comando describe-project. Includere il parametro `--id`.

```
aws codestar describe-project --id <project_ID>
```

Nell'output compaiono informazioni simili alle seguenti:

```
{
    "name": "MyProject",
    "id": "myproject",
    "arn": "arn:aws:codestar:us-east-1:account_ID:project/myproject",
    "description": "",
    "createdTimeStamp": 1539700079.472,
```

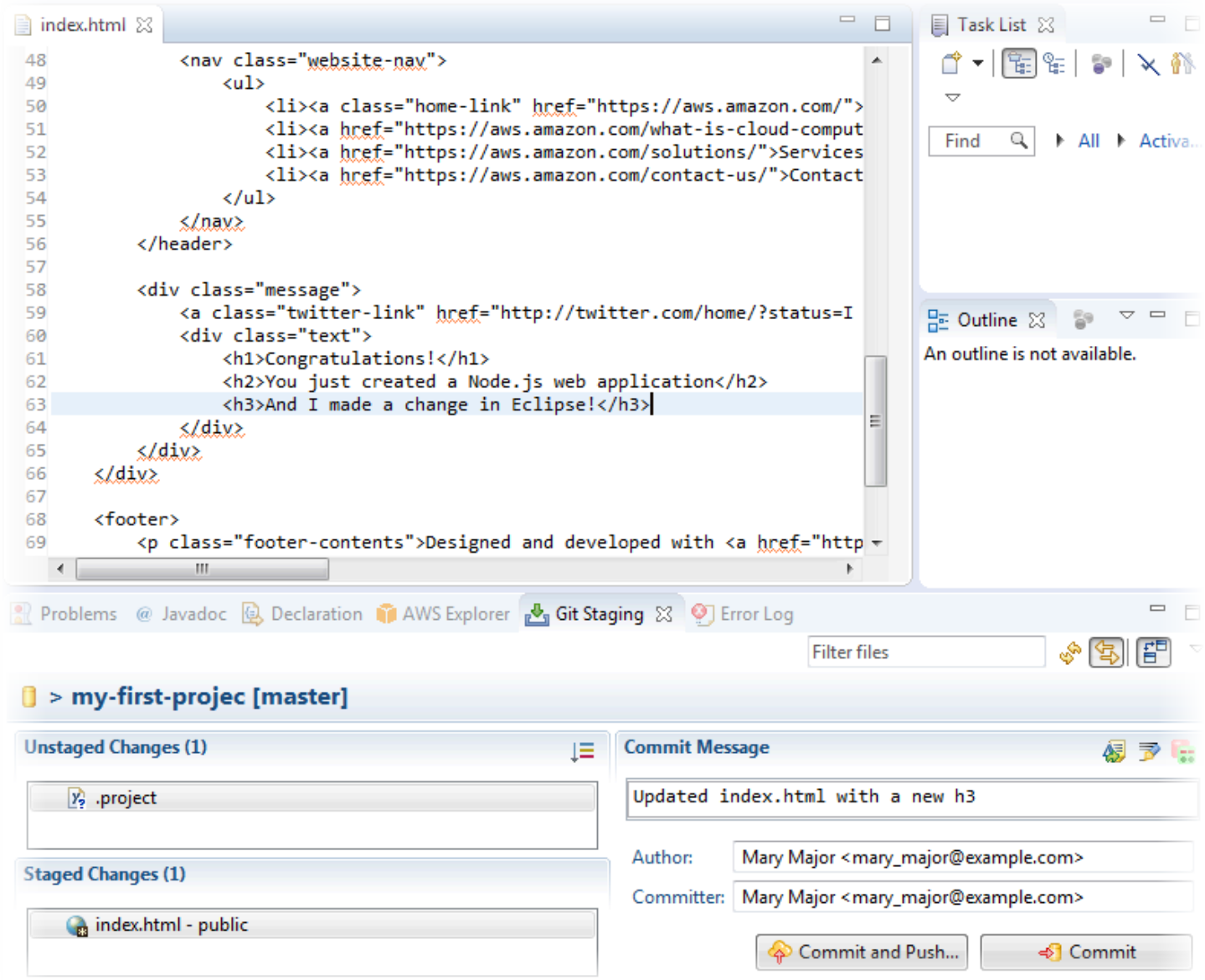
```
    "stackId": "arn:aws:cloudformation:us-east-1:account_ID:stack/awscodestar-
myproject/stack-ID",
    "status": {
        "state": "CreateInProgress"
    }
}
```

- L'output contiene informazioni sul nuovo progetto.:
  - Il valore `state` rappresenta lo stato della creazione del progetto, ad esempio `CreateInProgress` o `CreateComplete`.

Durante la creazione del progetto, è possibile aggiungere membri del team o configurare l'accesso al repository del progetto dalla riga di comando o dall'IDE preferito.

Usa un IDE con AWS CodeStar

Quando integri un IDE con AWS CodeStar, puoi continuare a scrivere e sviluppare codice nel tuo ambiente preferito. Le modifiche apportate vengono incluse nel AWS CodeStar progetto ogni volta che esegui il commit e il push del codice.



Argomenti

- Usare AWS Cloud9 con AWS CodeStar
- Usa Eclipse con AWS CodeStar
- Usa Visual Studio con AWS CodeStar

Usare AWS Cloud9 con AWS CodeStar

È possibile AWS Cloud9 utilizzarlo per apportare modifiche al codice e sviluppare software in un AWS CodeStar progetto. AWS Cloud9 è un IDE online, a cui puoi accedere tramite il tuo browser web. L'IDE offre una ricca esperienza di modifica del codice con supporto per diversi linguaggi di

programmazione e debugger runtime, nonché un terminale integrato. In background, un' EC2 istanza Amazon ospita un ambiente di AWS Cloud9 sviluppo. Questo ambiente fornisce l' AWS Cloud9 IDE e l'accesso ai file di codice del AWS CodeStar progetto. Per ulteriori informazioni, consulta la Guida per l'utente AWS Cloud9.

È possibile utilizzare la AWS CodeStar console o la AWS Cloud9 console per creare ambienti di AWS Cloud9 sviluppo per progetti in cui è memorizzato il codice CodeCommit. Per AWS CodeStar i progetti che memorizzano il codice in GitHub, puoi usare solo la AWS Cloud9 console. In questo argomento viene spiegato l'utilizzo di entrambe le console.

Per utilizzarlo AWS Cloud9, è necessario:

- Un utente IAM che è stato aggiunto come membro del team a un AWS CodeStar progetto.
- Se il AWS CodeStar progetto memorizza il codice sorgente in CodeCommit, AWS credenziali per l'utente IAM.

Argomenti

Crea un AWS Cloud9 ambiente per un progetto

Segui questi passaggi per creare un ambiente di AWS Cloud9 sviluppo per un AWS CodeStar progetto.

1. Segui i passaggi indicati Creazione di un progetto se desideri creare un nuovo progetto.
2. Apri il progetto nella AWS CodeStar console. Nella barra di navigazione, scegli IDE. Scegli Crea ambiente, quindi utilizza i seguenti passaggi.

> **Important**
>
> Se il progetto si trova in una AWS regione in cui AWS Cloud9 non è supportato, non vedrai AWS Cloud9 le opzioni nella scheda IDE sulla barra di navigazione. Tuttavia, puoi utilizzare la AWS Cloud9 console per creare un ambiente di sviluppo, aprire il nuovo ambiente e collegarlo al AWS CodeCommit repository del progetto. Ignora i passaggi seguenti e consulta gli argomenti Creazione di un ambiente, Apertura di un ambiente e l'Esempio di AWS CodeCommit nella Guida per l'utente di AWS Cloud9 . Per l'elenco delle AWS regioni supportate, AWS Cloud9consulta Riferimenti generali di Amazon Web Services.

In Crea AWS Cloud9 ambiente, personalizza le impostazioni predefinite del progetto.

1. Per modificare il tipo predefinito di EC2 istanza Amazon per ospitare l'ambiente, per Tipo di istanza, scegli il tipo di istanza.
2. AWS Cloud9 utilizza Amazon Virtual Private Cloud (Amazon VPC) nel tuo AWS account per comunicare con l'istanza. A seconda di come Amazon VPC è configurato nel tuo AWS account, esegui una delle seguenti operazioni.

L'account dispone di un VPC con almeno una sottorete?	Il VPC che desideri AWS Cloud9 utilizzare è il VPC predefinito nell'account?	Il VPC dispone di una singola sottorete?	Esegui questa operazione
No	—	—	Se non esiste alcun VPC, creane uno. Espandere Network settings (Impostazioni di rete). In Network (VPC) (Rete (VPC)), scegliere Create VPC (Crea VPC) e seguire le istruzioni nella pagina. Per ulteriori informazioni, consulta Create an Amazon

L'account dispone di un VPC con almeno una sottorete?	Il VPC che desideri AWS Cloud9 utilizzare è il VPC predefinito nell'account?	Il VPC dispone di una singola sottorete?	Esegui questa operazione
			VPC for AWS Cloud9 nella Guida per l'AWS Cloud9 utente. Se un VPC esiste ma è privo di sottorete, creane una. Espandere Network settings (Impostazioni di rete). In Network (VPC) (Rete (VPC)), scegliere Create subnet (Crea sottorete), quindi seguire le istruzioni. Per ulteriori informazioni, consulta Creazione di una sottorete per AWS Cloud9 nella Guida per l'utente di AWS Cloud9 .
Sì	Sì	Sì	Passa al passaggio 4 di questa procedura. (AWS Cloud9 utilizza il VPC predefinito con la sua singola sottorete.)
Sì	Sì	No	In Subnet (Sottorete), selezionare la sottorete che si desidera AWS Cloud9 utilizzi nel VPC predefinito.
Sì	No	Sì o No	Per Rete (VPC), scegli il VPC che desideri utilizzare. AWS Cloud9 Per Subnet, scegli la sottorete che desideri AWS Cloud9 utilizzare in quel VPC.

Per ulteriori informazioni, consulta Amazon VPC Settings for AWS Cloud9 Development Environments nella Guida per l'AWS Cloud9 utente.

3. Inserisci un nome di ambiente e, facoltativamente, aggiungi una descrizione dell'ambiente.

> **Note**
>
> I nomi degli ambienti devono essere univoci per ciascun utente.

4. Per modificare il periodo di tempo predefinito dopo il quale AWS Cloud9 spegne l'ambiente quando non è stato utilizzato, espandi Impostazioni per il risparmio dei costi, quindi modifica l'impostazione.
5. Seleziona Create environment (Crea ambiente).

Per aprire l'ambiente, consulta Aprire un AWS Cloud9 ambiente per un progetto.

È possibile utilizzare questi passaggi per creare più di un ambiente per un progetto. Ad esempio, è possibile utilizzare un ambiente per lavorare su una porzione del codice e un altro ambiente per lavorare sulla stessa porzione con impostazioni diverse.

Aprire un AWS Cloud9 ambiente per un progetto

Segui questi passaggi per aprire un ambiente di AWS Cloud9 sviluppo creato per un AWS CodeStar progetto.

1. Con il progetto aperto nella AWS CodeStar console, nella barra di navigazione, scegli IDE.

> **Important**
>
> Se il codice sorgente del progetto è memorizzato in GitHub, non vedrai IDE nella barra di navigazione. Tuttavia, puoi utilizzare la AWS Cloud9 console per aprire un ambiente esistente. Ignora il resto della procedura e consulta l'argomento Apertura di un ambiente nella Guida per l'utente di AWS Cloud9 e Usa GitHub con AWS Cloud9.

2. Per i tuoi AWS Cloud9 ambienti o AWS Cloud9 Ambienti condivisi, scegli Open IDE per l'ambiente che desideri aprire.

Puoi usare l' AWS Cloud9 IDE per iniziare subito a lavorare con il codice nel AWS CodeCommit repository del progetto. Per ulteriori informazioni, consulta La finestra Ambiente, Editor, schede e riquadri e Il terminal nella Guida per l'utente di AWS Cloud9 e Comandi Git di base nella Guida per l'utente di AWS CodeCommit .

Condividi un AWS Cloud9 ambiente con un membro del team di progetto

Dopo aver creato un ambiente di AWS Cloud9 sviluppo per un AWS CodeStar progetto, puoi invitare altri utenti del tuo AWS account, inclusi i membri del team di progetto, ad accedere allo stesso ambiente. Questo è particolarmente utile per la programmazione di coppia, in cui due programmatori si alternano nella codifica e nei consigli sullo stesso codice tramite la condivisione di uno schermo o lavorando nella stessa postazione. I membri dell'ambiente possono utilizzare l' AWS Cloud9 IDE condiviso per vedere le modifiche al codice di ogni membro evidenziate nell'editor di codice e per chattare con gli altri membri durante la codifica.

L'aggiunta di un membro del team a un progetto non consente automaticamente a quel membro di partecipare a qualsiasi ambiente di AWS Cloud9 sviluppo correlato al progetto. Per invitare un membro del team di progetto ad accedere a un ambiente per un progetto, è necessario determinare il ruolo corretto di accesso dei membri dell'ambiente, applicare politiche AWS gestite all'utente e invitare l'utente nel proprio ambiente. Per ulteriori informazioni, consulta Informazioni sui ruoli di accesso dei membri dell'ambiente e Invita un utente IAM al tuo ambiente nella Guida per l'AWS Cloud9 utente.

Quando inviti un membro del team di progetto ad accedere a un ambiente per un progetto, la console AWS CodeStar mostra l'ambiente al membro del team. L'ambiente viene visualizzato nell'elenco Ambienti condivisi nella scheda IDE nella AWS CodeStar console del progetto. Per visualizzare questo elenco, chiedi al membro del team di aprire il progetto nella console, quindi scegli IDE nella barra di navigazione.

> **Important**
>
> Se il codice sorgente del progetto è memorizzato in GitHub, non vedrai IDE nella barra di navigazione. Tuttavia, puoi utilizzare la AWS Cloud9 console per invitare altri utenti del tuo AWS account, inclusi i membri del team di progetto, ad accedere a un ambiente. A tale scopo, consulta Usa GitHub con AWS Cloud9 questa guida e consulta About Environment Member Access Roles e Invita un utente IAM al tuo ambiente nella Guida per l'AWS Cloud9 utente.

Puoi invitare ad accedere a un ambiente anche un utente non membro del team di progetto. Ad esempio, si può volere che un utente lavori al codice di un progetto ma che non possa accedervi in altri modi. Per invitare questo tipo di utente, consulta About Environment Member Access Roles e Invita un utente IAM to Your Environment nella Guida per l'AWS Cloud9 utente. Quando inviti un

utente non membro del team di progetto ad accedere a un ambiente per un progetto, l'utente può utilizzare la console AWS Cloud9 per accedere all'ambiente. Per ulteriori informazioni, consulta Aprire un ambiente nella Guida per l'utente di AWS Cloud9 .

Eliminare un AWS Cloud9 ambiente da un progetto

Quando si elimina un progetto e tutte le relative AWS risorse da AWS CodeStar, vengono eliminati anche tutti gli ambienti di AWS Cloud9 sviluppo correlati creati con la AWS CodeStar console e non possono essere ripristinati. È possibile eliminare un ambiente di sviluppo da un progetto senza eliminare il progetto.

1. Con il progetto aperto nella AWS CodeStar console, nella barra di navigazione, scegli IDE.

   > **Important**
   >
   > Se il codice sorgente del progetto è memorizzato in GitHub, non vedrai IDE nella barra di navigazione. Tuttavia, puoi utilizzare la AWS Cloud9 console per eliminare un ambiente di sviluppo. Ignora il resto della procedura e consulta Eliminazione di un ambiente nella Guida per l'utente di AWS Cloud9 .

2. Scegli l'ambiente che desideri eliminare negli ambienti Cloud9 e scegli Elimina
3. Inserisci **`delete`** per confermare l'eliminazione per l'ambiente di sviluppo, quindi scegli Elimina.

   > **Warning**
   >
   > Non è possibile recuperare un ambiente di sviluppo dopo che è stato eliminato. Tutte le modifiche del codice non eseguite nell'ambiente vengono perse.

Usa GitHub con AWS Cloud9

Per AWS CodeStar i progetti in cui è memorizzato il codice sorgente GitHub, la AWS CodeStar console non supporta l'utilizzo diretto degli ambienti di AWS Cloud9 sviluppo. Tuttavia, puoi utilizzare la AWS Cloud9 console per lavorare con il codice sorgente nei GitHub repository.

1. Usa la AWS Cloud9 console per creare un ambiente di AWS Cloud9 sviluppo. Per informazioni, consulta Creating an Environment (Creazione di un ambiente) nella Guida per l'utente di AWS Cloud9 .

2. Usa la AWS Cloud9 console per aprire l'ambiente di sviluppo. Per informazioni, consulta Apertura di un ambiente nella Guida per l'utente di AWS Cloud9 .
3. Nell'IDE, utilizzate una sessione terminale per connettervi al GitHub repository (un processo noto come clonazione). Se la sessione del terminale non è in esecuzione, nella barra dei menu dell'IDE scegliere Window, New Terminal (Finestra, Nuovo terminale). Per i comandi da utilizzare per clonare il GitHub repository, consultate Cloning a Repository sul sito Web di aiuto. GitHub

   Per accedere alla pagina principale del GitHub repository, con il progetto aperto nella AWS CodeStar console, nella barra di navigazione laterale, scegli Codice.
4. Utilizza la finestra Environment (Ambiente) e le schede dell'editor nell'IDE per visualizzare, modificare e salvare il codice. Per ulteriori informazioni, consulta La finestra Ambiente ed Editor, schede e riquadri nella Guida per l'utente di AWS Cloud9 .
5. Utilizza Git nella sessione del terminale dell'IDE per inviare modifiche del codice al repository, nonché modifiche periodiche del pull del codice da parte di altri utenti dal repository. Per ulteriori informazioni, consulta Pushing to a Remote Repository e Fetching a Remote Repository sul sito Web di Help. GitHub Per i comandi Git, vedi Git Cheatsheet sul sito Web di GitHub Help.

   > **Note**
   >
   > Per evitare che Git ti richieda le credenziali di GitHub accesso ogni volta che invii o estrai codice dal repository, puoi usare un credenziali helper. Per ulteriori informazioni, consulta Memorizzazione nella cache della GitHub password in Git sul sito Web di GitHub assistenza.

Risorse aggiuntive

Per ulteriori informazioni sull'utilizzo AWS Cloud9, consulta quanto segue nella Guida per l'AWS Cloud9 utente:

- Tutorial
- Lavorare con gli ambienti
- Lavorare con l'IDE
- Esempi

Usa Eclipse con AWS CodeStar

È possibile utilizzare Eclipse per apportare modifiche al codice e sviluppare software in un AWS CodeStar progetto. È possibile modificare il codice AWS CodeStar del progetto con Eclipse, quindi eseguire il commit e inviare le modifiche al repository dei sorgenti del progetto. AWS CodeStar

> **Note**
>
> Le informazioni contenute in questo argomento si applicano solo ai AWS CodeStar progetti che memorizzano il codice sorgente in. CodeCommit Se il AWS CodeStar progetto memorizza il codice sorgente in GitHub, puoi usare uno strumento come EGit Eclipse. Per ulteriori informazioni, consulta la EGit documentazione sul EGit sito Web.

Se il AWS CodeStar progetto memorizza il codice sorgente in CodeCommit, è necessario installare una versione di AWS Toolkit for Eclipse che supporti AWS CodeStar. È inoltre necessario essere un membro del team di AWS CodeStar progetto con il ruolo di proprietario o collaboratore.

Per utilizzare Eclipse, hai inoltre bisogno di:

- Un utente IAM che è stato aggiunto a un AWS CodeStar progetto come membro del team.
- Se il AWS CodeStar progetto memorizza il codice sorgente in CodeCommit, credenziali Git (credenziali di accesso) per l'utente IAM.
- Autorizzazioni sufficienti per installare Eclipse and the sul AWS Toolkit for Eclipse computer locale.

Argomenti

Fase 1: Installazione AWS Toolkit for Eclipse

Il Toolkit for Eclipse è un pacchetto software che puoi aggiungere a Eclipse. installato e gestito nello stesso modo degli altri pacchetti software in Eclipse. Il AWS CodeStar toolkit è incluso come parte del Toolkit for Eclipse.

Per installare il Toolkit for Eclipse AWS CodeStar con il modulo

1. Installare Eclipse sul computer locale. Le versioni supportate di Eclipse includono Luna, Marte e Neon.
2. Scarica e installa il Toolkit for Eclipse. Per ulteriori informazioni, consulta la Guida alle operazioni di base di AWS Toolkit for Eclipse.
3. In Eclipse, scegliere Help (Aiuto), quindi Install New Software (Installa nuovo software).
4. In Available Software (Software disponibili), scegliere Add (Aggiungi).
5. In Add Repository (Aggiungi repository), scegliere Archive (Archivia), individuare il percorso in cui è stato salvato il file .zip e aprire il file. Lasciare vuoto il campo Name (Nome) e scegliere OK.
6. In Software disponibile, scegli Seleziona tutto per selezionare Strumenti di gestione di AWS base e Strumenti per sviluppatori, quindi scegli Avanti.
7. In Install Details (Dettagli installazione), scegliere Next (Avanti).
8. In Review Licenses (Esamina licenze), rivedere i contratti di licenza. Scegliere I accept the terms of the license agreement (Accetto i termini del contratto di licenza), quindi scegliere Finish (Fine). Riavviare Eclipse.

Passaggio 2: importa il tuo AWS CodeStar progetto in Eclipse

Dopo aver installato Toolkit for Eclipse, AWS CodeStar puoi importare progetti e modificare, eseguire il commit e inviare codice dall'IDE.

> **Note**
>
> È possibile aggiungere più AWS CodeStar progetti a un singolo spazio di lavoro in Eclipse, ma è necessario aggiornare le credenziali del progetto quando si passa da un progetto all'altro.

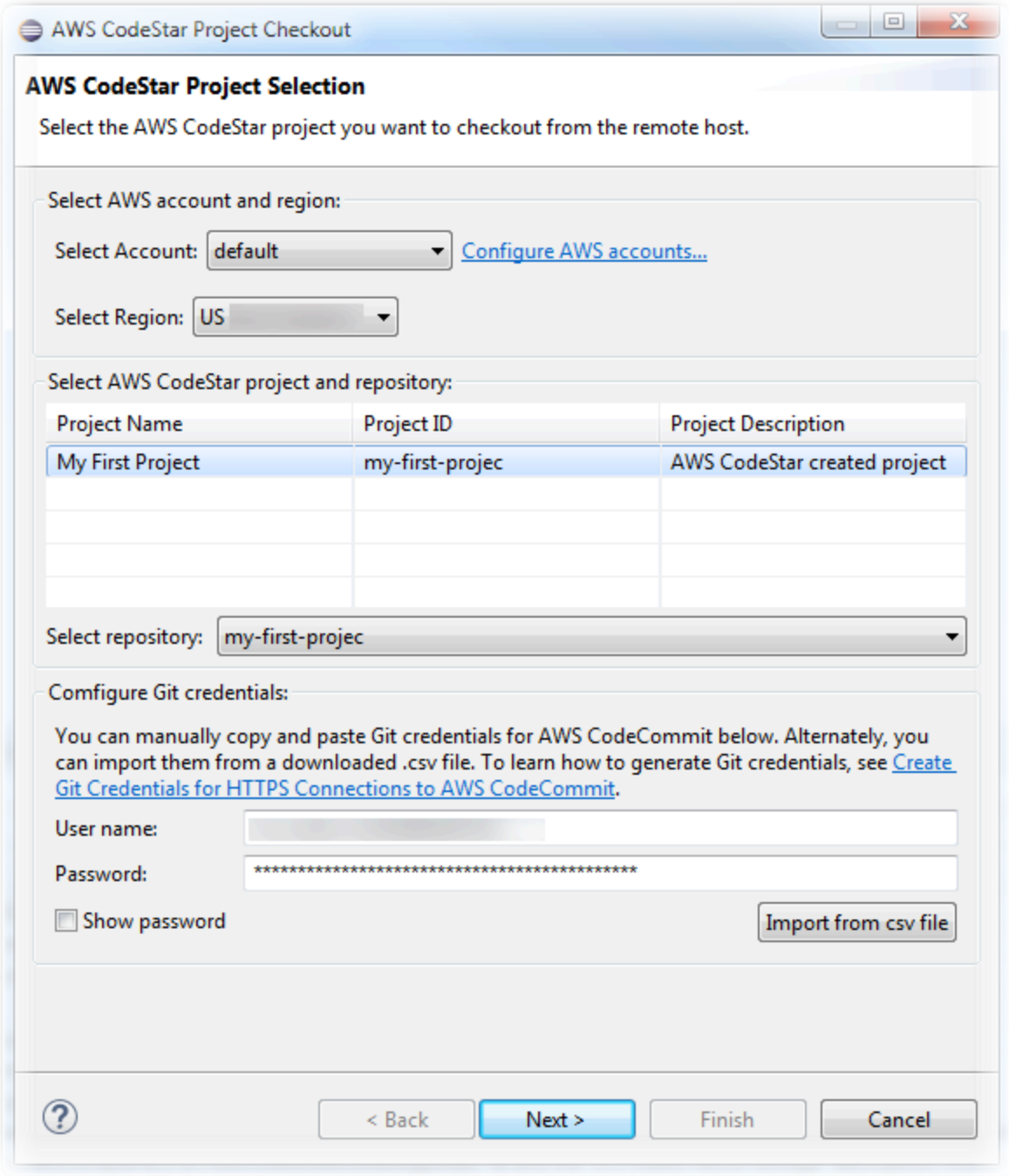
Per importare un progetto AWS CodeStar

1. Dal AWS menu, scegli Importa AWS CodeStar progetto. In alternativa, scegliere File, quindi Import (Importa). In Select, espandi AWS, quindi scegli AWS CodeStar Project.

   Scegli Next (Successivo).

2. In AWS CodeStar Project Selection, scegli il tuo AWS profilo e la AWS regione in cui è ospitato il AWS CodeStar progetto. Se non hai un AWS profilo configurato con una chiave di accesso e una chiave segreta sul tuo computer, scegli Configura AWS account e segui le istruzioni.

   In Seleziona AWS CodeStar progetto e archivio, scegli il tuo AWS CodeStar progetto. In Configura le credenziali Git, inserisci le credenziali di accesso che hai generato per accedere al repository del progetto. Se non si dispone di credenziali Git, consultare la pagina Nozioni di base. Scegli Next (Successivo).



3. Tutti i rami del repository del progetto sono selezionati per impostazione predefinita. Se non si desidera importare uno o più rami, deselezionare le caselle, quindi scegliere Next (Avanti).
4. In Local Destination (Destinazione locale), scegliere una destinazione in cui la procedura guidata di importazione crei il repository locale sul compute, quindi scegliere Finish (Fine).
5. In Project Explorer, espandi l'albero del progetto per sfogliare i file del AWS CodeStar progetto.

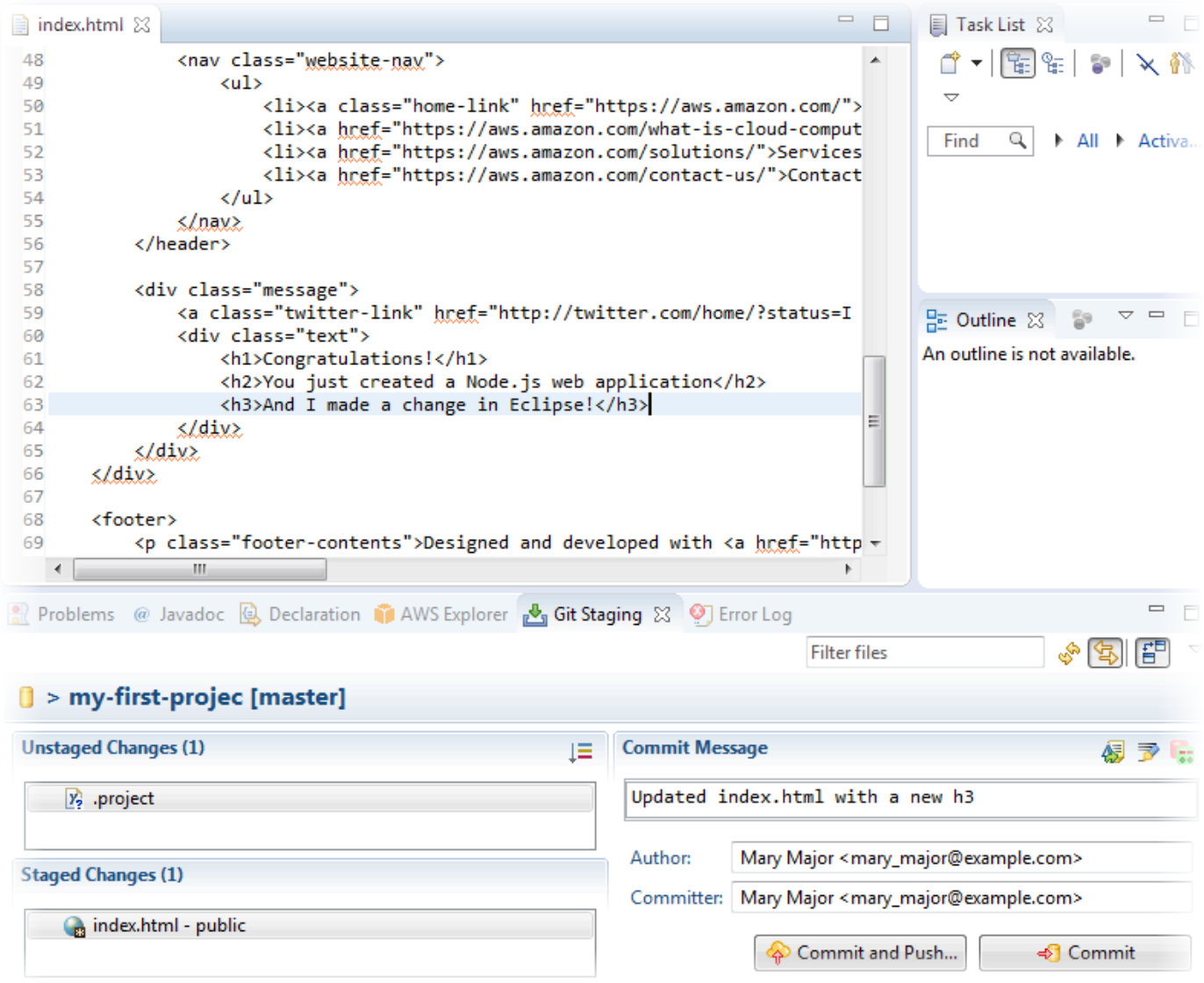
Passaggio 3: Modifica il codice AWS CodeStar del progetto in Eclipse

Dopo aver importato un AWS CodeStar progetto in un'area di lavoro di Eclipse, puoi modificare il codice del progetto, salvare le modifiche, eseguire il commit e inviarlo al repository di origine del progetto. Questo è lo stesso processo che segui per qualsiasi repository Git che utilizza il EGit plugin per Eclipse. Per ulteriori informazioni, consulta la Guida per l'EGit utente sul sito Web di Eclipse.

Per modificare il codice del progetto ed effettuare il primo commit nell'archivio dei sorgenti di un progetto AWS CodeStar

1. In Project Explorer, espandi l'albero del progetto per sfogliare i file del AWS CodeStar progetto.
2. Modificare uno o più file di codice e salvare le modifiche.
3. Quando si è pronti per eseguire il commit delle modifiche, aprire il menu contestuale per quel file, scegliere Team, quindi Commit.

   È possibile ignorare questa fase se nella vista del progetto è già aperta la finestra Git Staging (Gestione Git).
4. In Git Staging (Gestione dello staging in Git), gestisci le modifiche spostando i file modificati in Staged Changes (Modifiche gestite). Inserire un messaggio di commit in Commit Message (Messaggio commit) e scegliere Commit and Push (Commit e invio).



Per visualizzare la distribuzione delle modifiche del codice, tornare al pannello di controllo del progetto. Per ulteriori informazioni, consulta Fase 3: visualizzazione del progetto.

Usa Visual Studio con AWS CodeStar

Puoi usare Visual Studio per apportare modifiche al codice e sviluppare software in un AWS CodeStar progetto.

> **Note**
>
> Visual Studio per Mac non supporta il AWS Toolkit, quindi non può essere utilizzato con AWS CodeStar.

> Le informazioni contenute in questo argomento si applicano solo ai AWS CodeStar progetti che memorizzano il codice sorgente in CodeCommit. Se il AWS CodeStar progetto memorizza il codice sorgente in GitHub, puoi usare uno strumento come GitHub Extension for Visual Studio. Per ulteriori informazioni, consulta la pagina Panoramica sul sito Web di GitHub Extension for Visual Studio e Getting Started with GitHub for Visual Studio sul GitHub sito Web.

Per utilizzare Visual Studio per modificare il codice nell'archivio dei sorgenti di un AWS CodeStar progetto, devi installare una versione AWS Toolkit for Visual Studio che supporti AWS CodeStar. Inoltre, devi essere un membro del team del progetto AWS CodeStar con ruolo di proprietario o collaboratore.

Per utilizzare Visual Studio, hai anche bisogno di:

- Un utente IAM che è stato aggiunto a un AWS CodeStar progetto come membro del team.
- AWS credenziali per il tuo utente IAM (ad esempio, la chiave di accesso e la chiave segreta).
- Autorizzazioni sufficienti per installare Visual Studio e il AWS Toolkit for Visual Studio sul computer locale.

Toolkit for Visual Studio è un pacchetto software che puoi aggiungere a Visual Studio. Viene installato e gestito allo stesso modo degli altri pacchetti software in Visual Studio.

Per installare Toolkit for Visual Studio con AWS CodeStar il modulo e configurare l'accesso all'archivio del progetto

1. Installa Visual Studio sul tuo computer locale.
2. Scarica e installa Toolkit for Visual Studio e salva il file.zip in una cartella o directory locale. Nella AWS Toolkit for Visual Studio pagina Guida introduttiva, inserisci o importa AWS le tue credenziali, quindi scegli Salva e chiudi.
3. In Visual Studio, apri Team Explorer. In Hosted Service Providers (Fornitori di servizi ospitati), individuare CodeCommit e scegliere Connect (Connetti).
4. In Manage Connections (Gestisci connessioni), scegliere Clone (Clona). Scegliere il repository del progetto e la cartella nel computer locale in cui clonare il repository, quindi scegliere OK.
5. Se viene richiesto di creare le credenziali Git, scegli Yes (Sì). Il kit di strumenti tenterà di creare le credenziali a tuo nome. Salvare il file delle credenziali in un percorso sicuro. Questa è l'unica

opportunità che si ha per salvare tali credenziali. Se il kit di strumenti non è in grado di creare le credenziali al posto dell'utente, oppure se si sceglie No, sarà necessario creare e fornire le proprie credenziali Git. Per ulteriori informazioni, consulta Per impostare il computer per eseguire il commit delle modifiche (utente IAM) o segui le istruzioni online.

Una volta terminata la clonazione del progetto, sei pronto per iniziare a modificare il codice in Visual Studio e inserire e inserire le modifiche nell'archivio del progetto. CodeCommit

Modificare AWS le risorse in un AWS CodeStar progetto

Dopo aver creato un progetto in AWS CodeStar, puoi modificare il set di AWS risorse predefinito che AWS CodeStar viene aggiunto al progetto.

Modifiche delle risorse supportate

La tabella seguente elenca le modifiche supportate alle AWS risorse predefinite in un AWS CodeStar progetto.

Modifica	Note
Aggiungi una fase a AWS CodePipeline.	Per informazioni, consulta Aggiungi una fase a AWS CodePipeline.
Modifica le impostazioni dell'ambiente Elastic Beanstalk.	Per informazioni, consulta Modifica delle impostazioni AWS Elastic Beanstalk dell'ambiente.
Modifica il codice o le impostazioni di una AWS Lambda funzione, il suo ruolo IAM o la sua API in Amazon API Gateway.	Per informazioni, consulta Modificare una AWS Lambda funzione nel codice sorgente.
Aggiungi una risorsa a un AWS Lambda progetto ed espandi le autorizzazioni per creare e accedere alla nuova risorsa.	Per informazioni, consulta Aggiungere una risorsa a un progetto.
Aggiungi lo spostamento del traffico con CodeDeploy per una AWS Lambda funzione.	Per informazioni, consulta Trasferimento del traffico per un progetto AWS Lambda.

Modifica	Note
Aggiungi supporto AWS X-Ray	Per informazioni, consulta Abilitazione del tracciamento per un progetto.
Modifica il file buildspec.yml del tuo progetto per aggiungere una fase di compilazione di unit test da eseguire. AWS CodeBuild	Consulta Fase 7: aggiungere un test di unità per il Web Service nel tutorial sul progetto serverless
Aggiunta del proprio ruolo IAM al proprio progetto	Per informazioni, consulta Aggiunta di un ruolo IAM a un progetto.
Modifica la definizione di un ruolo IAM.	Per i ruoli definiti nello stack di applicazioni. Non è possibile modificare i ruoli definiti nella toolchain o negli CloudFormation stack.
Modifica del progetto Lambda per aggiungere un endpoint.	
Modifica il tuo EC2 progetto per aggiungere un endpoint.	
Modifica del progetto Elastic Beanstalk per aggiungere un endpoint.	
Modifica del progetto per aggiungere una fase Prod e un endpoint.	Per informazioni, consulta Aggiunta di una fase Prod e di un endpoint a un progetto.
Usa in modo sicuro i parametri SSM in un progetto. AWS CodeStar	Per informazioni, consulta the section called “Utilizzo sicuro dei parametri SSM in un progetto AWS CodeStar”.

Non sono supportate le seguenti modifiche.

- Passa a un obiettivo di distribuzione diverso (ad esempio, implementa to AWS Elastic Beanstalk invece di). AWS CodeDeploy
- Aggiunta di un nome di un endpoint web intellegibile.

- Cambia il nome del CodeCommit repository (per un AWS CodeStar progetto connesso a CodeCommit).
- Per un AWS CodeStar progetto connesso a GitHub, disconnetti il GitHub repository, quindi ricollega il repository a quel progetto o connetti qualsiasi altro repository a quel progetto. È possibile utilizzare la CodePipeline console (non la AWS CodeStar console) per disconnettersi e riconnettersi nella fase Source di una pipeline. GitHub Tuttavia, se ricollegate la fase di origine a un altro GitHub repository, nella AWS CodeStar dashboard del progetto, le informazioni nei riquadri Repository e Issues potrebbero essere errate o non aggiornate. La disconnessione del GitHub repository non rimuove le informazioni del repository dai riquadri della cronologia dei commit e dei GitHub problemi nella dashboard del progetto. AWS CodeStar Per rimuovere queste informazioni, utilizza il GitHub sito Web per disabilitare l'accesso al progetto GitHub . AWS CodeStar Per revocare l'accesso, sul GitHub sito Web, utilizza la sezione OAuth App autorizzate della pagina delle impostazioni del profilo del tuo GitHub account.
- Disconnetti il CodeCommit repository (per un AWS CodeStar progetto collegato a CodeCommit), quindi ricollega il repository a quel progetto o collega qualsiasi altro repository a quel progetto.

Aggiungi una fase a AWS CodePipeline

Puoi aggiungere una nuova fase a una pipeline AWS CodeStar creata in un progetto. Per ulteriori informazioni, consulta Modifica una pipeline AWS CodePipeline nella Guida per l'AWS CodePipeline utente.

> **Note**
>
> Se la nuova fase dipende da AWS risorse che AWS CodeStar non sono state create, la pipeline potrebbe interrompersi. Questo perché il ruolo IAM AWS CodeStar creato per AWS CodePipeline potrebbe non avere accesso a tali risorse per impostazione predefinita.
> Per tentare di AWS CodePipeline consentire l'accesso a AWS risorse che AWS CodeStar non sono state create, potresti voler modificare il ruolo IAM che AWS CodeStar ha creato. Questo non è supportato perché AWS CodeStar potrebbe rimuovere le modifiche al ruolo IAM quando esegue controlli di aggiornamento regolari sul progetto.

Modifica delle impostazioni AWS Elastic Beanstalk dell'ambiente

Puoi modificare le impostazioni di un AWS CodeStar ambiente Elastic Beanstalk creato in un progetto. Ad esempio, potresti voler modificare l'ambiente Elastic Beanstalk predefinito AWS

CodeStar nel tuo progetto da Single Instance a Load Balanced. Per fare ciò, modificare il file `template.yml` nel repository del progetto. Potrebbe inoltre essere necessario modificare le autorizzazioni per i ruoli di lavoro del progetto. Dopo aver effettuato la modifica del modello AWS CodeStar e aver fornito le risorse CloudFormation al posto tuo.

Per ulteriori informazioni sulla modifica di questo file `template.yml`, consulta Modifica dell risorse dell'applicazione con il file template.yml. Per ulteriori informazioni sugli ambienti Elastic Beanstalk AWS Elastic Beanstalk , consulta Environment Management Console nella Developer Guide.AWS Elastic Beanstalk

Modificare una AWS Lambda funzione nel codice sorgente

Puoi modificare il codice o le impostazioni di una funzione Lambda, o il relativo ruolo IAM o API Gateway API, che AWS CodeStar viene creata in un progetto. A tale scopo, ti consigliamo di utilizzare il AWS Serverless Application Model (AWS SAM) insieme al `template.yaml` file nel repository del CodeCommit progetto. Questo `template.yaml` file definisce il nome, il gestore, il runtime, il ruolo IAM e l'API della funzione in API Gateway. Per ulteriori informazioni, consulta Come creare applicazioni serverless utilizzando AWS SAM sul GitHub sito Web.

Abilitazione del tracciamento per un progetto

AWS X-Ray offre il tracciamento, che è possibile utilizzare per analizzare il comportamento delle prestazioni delle applicazioni distribuite (ad esempio, le latenze nei tempi di risposta). Dopo aver aggiunto le tracce al AWS CodeStar progetto, è possibile utilizzare la AWS X-Ray console per visualizzare le visualizzazioni delle applicazioni e i tempi di risposta.

> **Note**
>
> Puoi utilizzare questi passaggi per i seguenti progetti, creati con le seguenti modifiche di supporto progetto:
>
> - Qualsiasi progetto Lambda.
> - Per i progetti Amazon EC2 o Elastic Beanstalk creati dopo il 3 agosto AWS CodeStar 2018, è stato eseguito il `/template.yml` provisioning di un file nel repository del progetto.

Ogni AWS CodeStar modello include un CloudFormation file che modella le dipendenze di AWS runtime dell'applicazione, come le tabelle del database e le funzioni Lambda. Il file è archiviato nel repository di origine nel file `/template.yml`.

È possibile modificare questo file per aggiungere tracce aggiungendo la AWS X-Ray risorsa alla sezione. `Resources` Quindi modifichi le autorizzazioni IAM per il tuo progetto CloudFormation per consentire la creazione della risorsa. Per informazioni sugli elementi del modello e sulla formattazione, consulta AWS Resource Types Reference.

Questi sono i passaggi di alto livello da seguire per personalizzare il modello.

1. Fase 1: modificare il ruolo di dipendente in IAM per il tracciamento
2. Fase 2: Modificare il file template.yml per il tracciamento
3. Fase 3: eseguire il commit e l'applicazione della modifica al modello per il tracciamento
4. Fase 4: Monitorare l'aggiornamento dello stack di AWS CloudFormation per il tracciamento

Fase 1: modificare il ruolo di dipendente in IAM per il tracciamento

Per eseguire le fasi da 1 a 4, è necessario avere effettuato l'accesso come amministratore. Questa fase mostra un esempio di modifica delle autorizzazioni per un progetto Lambda.

> **Note**
>
> Puoi saltarla se il tuo progetto è dotato di una policy per il limite di autorizzazioni.
> Per i progetti creati dopo il 6 dicembre 2018 PDT, hai dotato il progetto AWS CodeStar di una politica sui limiti delle autorizzazioni.

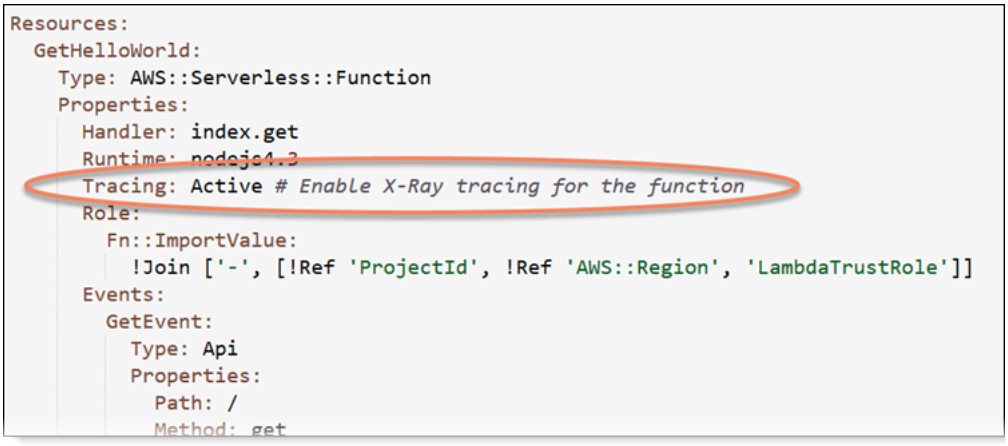
1. Accedi a Console di gestione AWS e apri la console all'indirizzo. AWS CodeStar https://console.aws.amazon.com/codestar/
2. Creare un progetto o scegliere un progetto esistente con un `template.yml file`, quindi aprire la pagina Project resources (Risorse del progetto).
3. In Project Resources, individua il ruolo IAM creato per il ruolo CodeStarWorker / Lambda nell'elenco delle risorse. Il nome del ruolo segue questo formato: `role/CodeStarWorker-`*`Project_name`*`-lambda-`*`Function_name`*. Scegliere l'ARN per il ruolo.
4. Il ruolo si apre nella console IAM. Scegli Collega policy. Cercare la policy `AWSXrayWriteOnlyAccess`, selezionare la casella di controllo accanto a essa e scegliere Attach policy (Collega policy).

Fase 2: Modificare il file template.yml per il tracciamento

1. Apri la AWS CodeStar console all'indirizzo. https://console.aws.amazon.com/codestar/
2. Scegliere il progetto serverless esistente e aprire la pagina Code (Codice). Nel livello principale del repository, individuare e modificare il file `template.yml`. Sotto `Resources`, incollare la risorsa nella sezione `Properties`.

```
      Tracing: Active
```

Questo esempio illustra un modello modificato:



Fase 3: eseguire il commit e l'applicazione della modifica al modello per il tracciamento

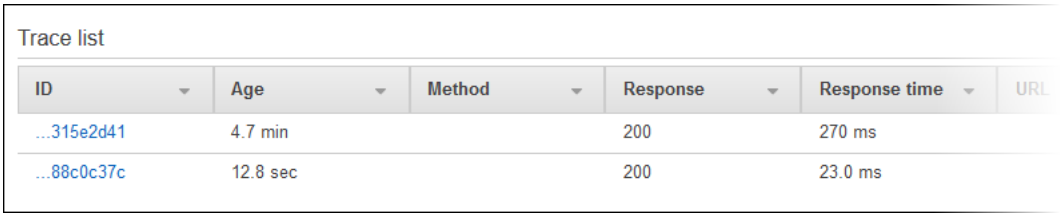
- Eseguire il commit e applicare le modifiche al file `template.yml`.

> **Note**
>
> Questo avvia la pipeline. Se esegui le modifiche prima di aggiornare le autorizzazioni IAM, la pipeline si avvia, l'aggiornamento dello AWS CloudFormation stack rileva errori e l'aggiornamento dello stack viene ripristinato. In questo caso, riavviare la pipeline dopo aver corretto le autorizzazioni.

Fase 4: Monitorare l'aggiornamento dello stack di AWS CloudFormation per il tracciamento

1. L'aggiornamento AWS CloudFormation dello stack inizia quando la pipeline del progetto inizia la fase di distribuzione. Per vedere lo stato dell'aggiornamento dello stack, nella AWS CodeStar dashboard, scegli la AWS CloudFormation fase della pipeline.

   Se l'aggiornamento dello stack AWS CloudFormation restituisce errori, consulta le linee guida per la risoluzione dei problemi in. AWS CloudFormation: la creazione di stack è stata sottoposta a rollback per autorizzazioni mancanti Se il ruolo worker non dispone delle autorizzazioni, modificare la policy associata al ruolo worker del progetto Lambda. Per informazioni, consulta Fase 1: modificare il ruolo di dipendente in IAM per il tracciamento.
2. Utilizzare il pannello di controllo per visualizzare il completamento della pipeline. Il tracciamento dell'applicazione è ora abilitato.
3. Verificare che il tracciamento sia attivato visualizzando i dettagli della funzione Lambda nella console.
4. Scegliere l'endpoint dell'applicazione del progetto. Questa interazione con l'applicazione viene tracciata. È possibile visualizzare le informazioni di tracciamento nella console AWS X-Ray .



Aggiungere una risorsa a un progetto

Ogni AWS CodeStar modello per tutti i progetti viene fornito con un CloudFormation file che modella le dipendenze di AWS runtime dell'applicazione, come le tabelle del database e le funzioni Lambda. Esso è memorizzato nel repository del codice sorgente del progetto nel file `/template.yml`.

> **Note**
>
> Puoi utilizzare questi passaggi per i seguenti progetti, creati con le seguenti modifiche di supporto progetto:
>
> - Qualsiasi progetto Lambda.

- Per i progetti Amazon EC2 o Elastic Beanstalk creati dopo il 3 agosto AWS CodeStar 2018, ha `/template.yml` fornito un file nell'archivio del progetto.

Puoi modificare questo file aggiungendo CloudFormation risorse alla sezione. `Resources` La modifica del `template.yml` file consente AWS CodeStar di CloudFormation aggiungere la nuova risorsa al progetto. Alcune risorse richiedono l'aggiunta di altre autorizzazioni alla politica per il ruolo di CloudFormation lavoratore del progetto. Per informazioni sugli elementi e sulla formattazione del modello, consulta AWS Resource Types Reference.

Dopo aver determinato quali risorse è necessario aggiungere al progetto, questi sono i passaggi di alto livello da seguire per personalizzare un modello. Per un elenco delle CloudFormation risorse e delle relative proprietà richieste, vedere AWS Resource Types Reference.

1. Fase 1: Modifica il ruolo del CloudFormation lavoratore in IAM (se necessario)
2. Fase 2: modificare il file template.yml
3. Fase 3: eseguire il commit e l'applicazione della modifica al modello
4. Fase 4: monitorare l'aggiornamento dello stack di AWS CloudFormation
5. Fase 5: Aggiungere autorizzazioni a livello di risorsa con un policy inline

Utilizza i passaggi di questa sezione per modificare il modello di AWS CodeStar progetto per aggiungere una risorsa e quindi espandere le autorizzazioni del ruolo di CloudFormation lavoratore del progetto in IAM. In questo esempio, la AWS::SQS::Queuerisorsa viene aggiunta al `template.yml` file. La modifica avvia una risposta automatica AWS CloudFormation che aggiunge una coda Amazon Simple Queue Service al progetto.

Fase 1: Modifica il ruolo del CloudFormation lavoratore in IAM

Per eseguire le fasi da 1 a 5, è necessario avere effettuato l'accesso come amministratore.

> **Note**
>
> Puoi saltarla se il tuo progetto è dotato di una policy per il limite di autorizzazioni.
> Per i progetti creati dopo il 6 dicembre 2018 PDT, AWS CodeStar hai dotato il progetto di una politica sui limiti delle autorizzazioni.

1. Accedi Console di gestione AWS e apri la console all'indirizzo. AWS CodeStar https://console.aws.amazon.com/codestar/
2. Creare un progetto o scegliere un progetto esistente con un `template.yml file`, quindi aprire la pagina Project resources (Risorse del progetto).
3. In Project Resources, individua il ruolo IAM creato per il AWS CloudFormation ruolo CodeStarWorker/nell'elenco delle risorse. Il nome del ruolo segue questo formato: `role/CodeStarWorker-`*`Project_name`*`-CloudFormation`.
4. Il ruolo si apre nella console IAM. Nella scheda Permissions (Autorizzazioni), alla voce Inline Policies (Policy inline), espandere la riga della policy del ruolo del servizio e scegliere Edit Policy (Modifica policy).
5. Scegliere la scheda JSON per modificare la policy.

> **Note**
>
> La policy associata al ruolo worker è `CodeStarWorkerCloudFormationRolePolicy`.

6. Nel campo JSON, aggiungere la seguente dichiarazione della policy all'interno dell'elemento `Statement`.

```
{
  "Action": [
    "sqs:CreateQueue",
    "sqs:DeleteQueue",
    "sqs:GetQueueAttributes",
    "sqs:SetQueueAttributes",
    "sqs:ListQueues",
    "sqs:GetQueueUrl"
  ],
  "Resource": [
    "*"
  ],
  "Effect": "Allow"
}
```

7. Scegliere Review policy (Esamina policy) per garantire che la policy non contenga errori e quindi scegliere Save changes (Salva modifiche).

Fase 2: modificare il file template.yml

1. Apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.
2. Scegliere il progetto serverless esistente e aprire la pagina Code (Codice). Nel livello principale del repository, annotare la posizione di `template.yml`.
3. Utilizzare un IDE, la console o la riga di comando nel repository locale per modificare il file `template.yml` sul repository. Incollare la risorsa nella sezione `Resources`. In questo esempio, quando il seguente testo viene copiato, viene aggiunta la sezione `Resources`.

```
Resources:
  TestQueue:
    Type: AWS::SQS::Queue
```

Questo esempio illustra un modello modificato:

Fase 3: eseguire il commit e l'applicazione della modifica al modello

- Eseguire il commit e applicare le modifiche al file `template.yml` salvato nella fase 2.

> **Note**
>
> Questo avvia la pipeline. Se esegui le modifiche prima di aggiornare le autorizzazioni IAM, la pipeline si avvia e l'aggiornamento dello AWS CloudFormation stack rileva degli

errori, che causano il rollback dell'aggiornamento dello stack. In questo caso, riavviare la pipeline dopo aver corretto le autorizzazioni.

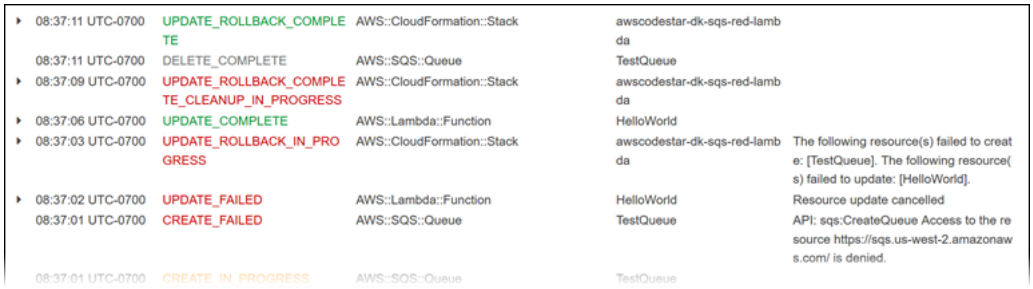
Fase 4: monitorare l'aggiornamento dello stack di AWS CloudFormation

1. Quando la pipeline del progetto avvia la fase di implementazione, inizia l'aggiornamento dello stack. AWS CloudFormation Puoi scegliere la AWS CloudFormation fase della pipeline sulla AWS CodeStar dashboard per vedere l'aggiornamento dello stack.

   Risoluzione dei problemi

   Se mancano le necessarie autorizzazioni sulle risorse, l'aggiornamento dello stack ha esito negativo. Visualizza lo stato dell'errore nella visualizzazione del AWS CodeStar pannello di controllo della pipeline del tuo progetto.

   Scegli il CloudFormationlink nella fase di distribuzione della pipeline per risolvere l'errore nella console. AWS CloudFormation All'interno dell'elenco Events (Eventi) della console, scegliere il progetto per visualizzare i dettagli della creazione dello stack. È presente un messaggio con i dettagli dell'errore. In questo esempio, risulta mancante l'autorizzazione `sqs:CreateQueue`.



   Aggiungi le autorizzazioni mancanti modificando la politica allegata al ruolo di lavoratore del tuo progetto. AWS CloudFormation Per informazioni, consulta Fase 1: Modifica il ruolo del CloudFormation lavoratore in IAM.

2. Dopo un'esecuzione corretta della pipeline, le risorse vengono create nello stack AWS CloudFormation . Nell'elenco Risorse di AWS CloudFormation, visualizza la risorsa creata per il tuo progetto. In questo esempio, la TestQueue coda è elencata nella sezione Risorse.

   L'URL della coda è disponibile in. AWS CloudFormation L'URL della coda segue il seguente formato:

```
https://{REGION_ENDPOINT}/queue.|api-domain|/{YOUR_ACCOUNT_NUMBER}/
{YOUR_QUEUE_NAME}
```

Per ulteriori informazioni, consulta Inviare un messaggio Amazon SQS, Ricevere un messaggio da una coda Amazon SQS ed Eliminare un messaggio da una coda Amazon SQS.

Fase 5: Aggiungere autorizzazioni a livello di risorsa con un policy inline

È possibile consentire l'accesso alla nuova risorsa ai membri del team aggiungendo al ruolo dell'utente le opportune policy inline. Non tutte le risorse necessitano dell'aggiunta di autorizzazioni. Per eseguire i seguenti passaggi, è necessario aver effettuato l'accesso alla console come utente root, utente amministratore dell'account oppure utente IAM o utente federato con la policy `AdministratorAccess` gestita o equivalente.

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

1. Accedi Console di gestione AWS 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:

```
{
 "Action": [
   "sqs:CreateQueue",
   "sqs:DeleteQueue",
   "sqs:GetQueueAttributes",
   "sqs:SetQueueAttributes",
   "sqs:ListQueues",
   "sqs:GetQueueUrl"
 ],
 "Resource": [
   "*"
 ],
```

```
  "Effect": "Allow"
}
```

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.

Aggiunta di un ruolo IAM a un progetto

A partire dal 6 dicembre 2018 PDT puoi definire i tuoi ruoli e le tue politiche nello stack dell'applicazione (template.yml). Per mitigare i rischi di escalation dei privilegi e azioni distruttive, ti viene richiesto di impostare il limite di autorizzazioni specifico per il progetto per ogni entità IAM creata. Se disponi di un progetto Lambda con più funzioni, è consigliabile creare un ruolo IAM per ogni funzione.

Per aggiungere un ruolo IAM al tuo progetto

1. Modificare il file `template.yml` per il progetto.
2. Nella sezione `Resources:` aggiungere le proprie risorse IAM servendosi del formato nel seguente esempio:

```
SampleRole:
Description: Sample Lambda role
Type: AWS::IAM::Role
Properties:
  AssumeRolePolicyDocument:
    Statement:
    - Effect: Allow
```

```
        Principal:
          Service: [lambda.amazonaws.com]
        Action: sts:AssumeRole
    ManagedPolicyArns:
      -  arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
    PermissionsBoundary: !Sub 'arn:${AWS::Partition}:iam::${AWS::AccountId}:policy/
CodeStar_${ProjectId}_PermissionsBoundary'
```

3. Rilasciare le modifiche tramite la pipeline e verificare il completamento dell'operazione.

Aggiunta di una fase Prod e di un endpoint a un progetto

Utilizza le procedure indicate in questa sezione per aggiungere una nuova fase di produzione(Prod) alla tua pipeline e una fase di approvazione manuale tra le fasi Deploy e Prod della tua pipeline. Questa operazione consente di creare uno stack di risorse aggiuntivo quando la pipeline del progetto è in esecuzione.

> **Note**
>
> Puoi utilizzare queste procedure se:
>
> - Per i progetti creati dopo il 3 agosto 2018, hai AWS CodeStar fornito al tuo progetto Amazon EC2, Elastic Beanstalk o Lambda `/template.yml` un file nel repository del progetto.
> - Per i progetti creati dopo il 6 dicembre 2018 PDT, hai dotato il progetto di una politica sui limiti delle AWS CodeStar autorizzazioni.

Tutti i AWS CodeStar progetti utilizzano un file CloudFormation modello che modella le dipendenze di AWS runtime dell'applicazione, come le istanze Linux e le funzioni Lambda. Il file `/template.yml` viene archiviato nel repository del codice sorgente.

Nel file `/template.yml`, utilizza il parametro `Stage` per aggiungere uno stack di risorse per una nuova fase nella pipeline del progetto.

```
  Stage:
    Type: String
    Description: The name for a project pipeline stage, such as Staging or Prod, for
which resources are provisioned and deployed.
```

```
    Default: ''
```

Il parametro `Stage` si applica a tutte le risorse denominate con l'ID di progetto a cui si fa riferimento nella risorsa. Ad esempio, il seguente nome del ruolo è una risorsa denominata nel modello:

```
RoleName: !Sub 'CodeStar-${ProjectId}-WebApp${Stage}'
```

Prerequisiti

Utilizza le opzioni del modello nella AWS CodeStar console per creare un progetto.

Assicurati che il tuo utente IAM disponga delle seguenti autorizzazioni:

- `iam:PassRole`sul CloudFormation ruolo del progetto.
- `iam:PassRole` sul ruolo della toolchain del progetto.
- `cloudformation:DescribeStacks`
- `cloudformation:ListChangeSets`

Solo per progetti Elastic Beanstalk o Amazon: EC2

- `codedeploy:CreateApplication`
- `codedeploy:CreateDeploymentGroup`
- `codedeploy:GetApplication`
- `codedeploy:GetDeploymentConfig`
- `codedeploy:GetDeploymentGroup`
- `elasticloadbalancing:DescribeTargetGroups`

Argomenti

Fase 1: creare un nuovo gruppo di distribuzione in CodeDeploy (solo Amazon EC2 Projects)

Scegli la tua CodeDeploy applicazione e quindi aggiungi un nuovo gruppo di distribuzione associato alla nuova istanza.

> **Note**
>
> Se il tuo progetto è un progetto Lambda o Elastic Beanstalk, puoi saltare questo passaggio.

1. Apri la console in /codedeploy. CodeDeploy https://console.aws.amazon.com
2. Scegli l' CodeDeploy applicazione che è stata generata per il tuo progetto al momento della creazione in. AWS CodeStar
3. In Deployment groups (Gruppo di distribuzione), scegliere Create deployment group (Crea gruppo di distribuzione).
4. In Deployment group name (Nome del gruppo di distribuzione), immettere ***<project-id>-prod-Env***.
5. In Service role, scegli il ruolo di lavoratore della toolchain per il tuo AWS CodeStar progetto.
6. In Deployment type (Tipo di distribuzione), scegliere In-place (In loco).
7. In Configurazione dell'ambiente, scegli la scheda Amazon EC2 Instances.
8. Nel gruppo di tag, in Key (Chiave), scegliere `aws:cloudformation:stack-name`. In Valore, scegli `awscodestar-<projectid>-infrastructure-prod` (lo stack da creare per l'GenerateChangeSetazione).
9. In Deployment settings (Impostazioni di distribuzione), scegliere `CodeDeployDefault.AllAtOnce`.
10. Deselezionare Choose a load balancer (Scegli un sistema di bilanciamento del carico).
11. Scegliere Create deployment group (Crea gruppo di distribuzione).

    È stato così creato il secondo gruppo di distribuzione.

Fase 2: aggiunta di una nuova fase della pipeline per la fase Prod

Aggiungi una fase con lo stesso set di operazioni di distribuzione della fase Deploy del progetto. Ad esempio, la nuova fase Prod per un EC2 progetto Amazon dovrebbe avere le stesse azioni della fase Deploy creata per il progetto.

Per copiare i parametri e i campi dalla fase Deploy

1. Dalla dashboard AWS CodeStar del progetto, scegli Pipeline Details per aprire la pipeline nella console. CodePipeline
2. Scegli Modifica.
3. Nella fase Deploy, scegliere Edit stage (Modifica fase).
4. Scegli l'icona di modifica sull'azione GenerateChangeSet. Prendere nota dei valori nei seguenti campi. Utilizzare questi valori durante la creazione di una nuova operazione.
   - Stack name (Nome stack)
   - Change set name (Modifica nome set)
   - Template (Modello)
   - Template configuration (Configurazione modello)
   - Input artifact (Artefatti di input)
5. Espandere la sezione Advanced (Avanzate) e, in Parameters (Parametri), copiare i parametri del proprio progetto. È possibile incollare questi parametri nella nuova operazione. È infatti possibile, ad esempio, copiare i parametri mostrati qui in formato JSON:
   - Progetti Lambda:

```
{
  "ProjectId":"MyProject"
}
```

   - EC2 Progetti Amazon:

```
{

  "ProjectId":"MyProject",
  "InstanceType":"t2.micro",
  "WebAppInstanceProfile":"awscodestar-MyProject-WebAppInstanceProfile-
EXAMPLEY5VSFS",
```

```
  "ImageId":"ami-EXAMPLE1",
  "KeyPairName":"my-keypair",
  "SubnetId":"subnet-EXAMPLE",
  "VpcId":"vpc-EXAMPLE1"
}
```

- Progetti Elastic Beanstalk:

```
{
  "ProjectId":"MyProject",
  "InstanceType":"t2.micro",
  "KeyPairName":"my-keypair",
  "SubnetId":"subnet-EXAMPLE",
  "VpcId":"vpc-EXAMPLE",
  "SolutionStackName":"64bit Amazon Linux 2018.03 v3.0.5 running Tomcat 8 Java
 8",
  "EBTrustRole":"CodeStarWorker-myproject-EBService",
  "EBInstanceProfile":"awscodestar-myproject-EBInstanceProfile-11111EXAMPLE"
}
```

6. Nel riquadro di modifica della fase, scegliere Cancel (Annulla).

Per creare un' GenerateChangeSet azione nella tua nuova fase Prod

> **Note**
>
> Dopo aver aggiunto la nuova operazione ma mentre si è ancora in modalità di modifica, se si riapre la nuova operazione per modificarla, alcuni campi potrebbero non essere visualizzati. È inoltre possibile visualizzare il seguente messaggio: Stack stack-name non esiste
> Questo errore non impedisce di salvare la pipeline. Tuttavia, per ripristinare i campi mancanti, è necessario eliminare la nuova operazione e aggiungerla di nuovo. Dopo aver salvato ed eseguito la pipeline, lo stack viene riconosciuto e l'errore non si ripresenta.

1. Se la pipeline non è già visualizzata, dalla dashboard AWS CodeStar del progetto, scegli Pipeline Details per aprire la pipeline nella console.
2. Scegli Modifica.
3. In fondo al diagramma, scegliere + Add stage (+ Aggiungi fase)

4. Immettere un nome della fase (ad esempio, **Prod**), quindi scegliere + Add action group (+ Aggiungi gruppo di operazioni).
5. In Action name (Nome operazione), immetti un nome (ad esempio, **GenerateChangeSet**).
6. In Action provider, scegli. AWS CloudFormation
7. In Action mode (Modalità operazione) selezionare Create or replace a change set (Crea o sostituisci un set di modifiche).
8. Nel nome dello stack, inserisci un nuovo nome per lo CloudFormation stack che deve essere creato con questa azione. Iniziare con un nome uguale a quello dello stack di distribuzione, quindi aggiungere **-prod**:

   - Progetti Lambda: `awscodestar-<project_name>-lambda-prod`
   - Progetti Amazon EC2 ed Elastic Beanstalk: `awscodestar-<project_name>-infrastructure-prod`

   > **Note**
   >
   > Il nome dello stack deve iniziare con **awscodestar-<project_name>-**, altrimenti la creazione dello stack non va a buon fine.

9. In Change set name (Modifica nome set), immettere lo stesso nome del set di modifiche utilizzato nella fase Deploy esistente (ad esempio, **pipeline-changeset**).
10. In Input artifacts (Artefatti di input), scegliere l'artefatto di compilazione.
11. In Template (Modello), immettere lo stesso nome del modello delle modifiche utilizzato nella fase Deploy esistente (ad esempio, **<project-ID>-BuildArtifact::template.yml**).
12. In Template configuration (Configurazione modello), immettere lo stesso nome del modello delle modifiche utilizzato nella fase di Deploy (ad esempio, **<project-ID>-BuildArtifact::template-configuration.json**).
13. In Capabilities (Funzionalità), scegliere CAPABILITY_NAMED_IAM.
14. In Role name (Nome ruolo), scegliere il nome del ruolo di dipendente CloudFormation del progetto.
15. Espandere la sezione Advanced (Avanzate) e, in Parameters (Parametri), incollare i parametri del proprio progetto. Includi il `Stage` parametro, mostrato qui in formato JSON, per un EC2 progetto Amazon:

```
{

  "ProjectId":"MyProject",
  "InstanceType":"t2.micro",
  "WebAppInstanceProfile":"awscodestar-MyProject-WebAppInstanceProfile-
EXAMPLEY5VSFS",
  "ImageId":"ami-EXAMPLE1",
  "KeyPairName":"my-keypair",
  "SubnetId":"subnet-EXAMPLE",
  "VpcId":"vpc-EXAMPLE1",
  "Stage":"Prod"
}
```

> **Note**
>
> Assicurarsi di incollare tutti i parametri per il progetto, non soltanto quelli nuovi o quelli che si desidera modificare.

16. Seleziona Salva.
17. Nel AWS CodePipeline riquadro, scegli Salva modifica alla pipeline, quindi scegli Salva modifica.

> **Note**
>
> Potrebbe essere visualizzato un messaggio che notifica l'eliminazione e l'aggiunta di risorse per il rilevamento delle modifiche. Conferma il messaggio e continua con il passaggio successivo di questo tutorial.

Visualizza la pipeline aggiornata.

Per creare un' ExecuteChangeSet azione nella tua nuova fase Prod

1. Se non state già visualizzando la pipeline, dalla dashboard AWS CodeStar del progetto, scegliete Pipeline Details per aprire la pipeline nella console.
2. Scegli Modifica.
3. Nella nuova fase Prod, dopo la nuova GenerateChangeSetazione, scegli + Aggiungi gruppo di azioni.

4. In Action name (Nome operazione), immetti un nome (ad esempio, **`ExecuteChangeSet`**).
5. In Action provider, scegli AWS CloudFormation.
6. In Action mode (Modalità operazione), selezionare Execute a change set (Esegui un set di modifiche).
7. Nel nome dello stack, inserisci il nuovo nome per lo CloudFormation stack che hai inserito nell' GenerateChangeSet azione (ad esempio,**`awscodestar-<project-ID>-infrastructure-prod`**).
8. In Change set name, immettete lo stesso nome del set di modifiche utilizzato nella fase di distribuzione (ad esempio,). **`pipeline-changeset`**
9. Seleziona Fatto.
10. Nel AWS CodePipeline riquadro, scegli Salva modifica alla pipeline, quindi scegli Salva modifica.

> **Note**
>
> Potrebbe essere visualizzato un messaggio che notifica l'eliminazione e l'aggiunta di risorse per il rilevamento delle modifiche. Conferma il messaggio e continua con il passaggio successivo di questo tutorial.

Visualizza la pipeline aggiornata.

Per creare un'azione CodeDeploy Deploy nella tua nuova fase Prod (solo EC2 progetti Amazon)

1. Dopo le nuove operazioni nella fase Prod, scegliere + Action (+ Operazione).
2. In Action name (Nome operazione), immetti un nome (ad esempio, **`Deploy`**).
3. In Action provider, scegli. AWS CodeDeploy
4. In Nome applicazione, scegli il nome dell' CodeDeployapplicazione per il tuo progetto.
5. In Deployment group (Gruppo di distribuzione), scegliere il nome del nuovo gruppo di distribuzione CodeDeploy creato nella fase 2.
6. In Input artifacts (Artefatti di input), scegliere lo stesso artefatto di compilazione utilizzato nella fase esistente.
7. Seleziona Fatto.
8. Nel AWS CodePipeline riquadro, scegli Salva modifica alla pipeline, quindi scegli Salva modifica. Visualizza la pipeline aggiornata.

Fase 3: aggiungere una fase di approvazione manuale

Come best practice, aggiungere una fase di approvazione manuale davanti alla nuova fase di produzione.

1. In alto a sinistra, scegliere Edit (Modifica).
2. Nel grafico della pipeline, tra le fasi di distribuzione Deploy e Prod, scegliere + Add stage (+ Aggiungi fase).
3. In Edit stage (Modifica fase), immettere un nome per la fase (ad esempio, **`Approval`**), quindi scegliere + Add action group (+ Aggiungi gruppo di operazioni).
4. In Action name (Nome operazione), immetti un nome (ad esempio, **`Approval`**).
5. In Approval type (Tipo di approvazione), scegliere Manual approval (Approvazione manuale).
6. (Facoltativo) In Configuration (Configurazione), in SNS Topic ARN (ARN argomento SNS), scegliere l'argomento SNS che è stato creato e sottoscritto.
7. Selezionare Add action (Aggiungi operazione).
8. Nel AWS CodePipeline riquadro, scegli Salva modifica alla pipeline, quindi scegli Salva modifica. Visualizza la pipeline aggiornata.
9. Per inviare le modifiche e avviare una compilazione tramite pipeline, scegliere Release change (Rilascia modifica) e quindi scegliere Release (Rilascia).

Passaggio 4: inserisci una modifica e monitora lo AWS CloudFormation stack Update

1. Mentre la pipeline è in esecuzione, puoi seguire i passaggi riportati qui per seguire la creazione dello stack e degli endpoint per la tua nuova fase.
2. Quando la pipeline avvia la fase di distribuzione, inizia l'aggiornamento dello stack. AWS CloudFormation Puoi scegliere la AWS CloudFormation fase della pipeline sulla AWS CodeStar dashboard per visualizzare la notifica di aggiornamento dello stack. Per visualizzare i dettagli della creazione dello stack,scegliere il progetto dall'elenco Events (Eventi) nella console.
3. Dopo il completamento con successo della pipeline, le risorse vengono create nello stack. AWS CloudFormation Nella AWS CloudFormation console, scegli lo stack di infrastruttura per il tuo progetto. I nomi dello stack seguono questo formato:

   - Progetti Lambda: `awscodestar-<project_name>-lambda-prod`
   - Progetti Amazon EC2 ed Elastic Beanstalk: `awscodestar-<project_name>-infrastructure-prod`

Nell'elenco Risorse della AWS CloudFormation console, visualizza la risorsa creata per il tuo progetto. In questo esempio, la nuova EC2 istanza Amazon viene visualizzata nella sezione Risorse.

4. Accedere all'endpoint per la fase di produzione:

   - Per un progetto Elastic Beanstalk, apri il nuovo stack AWS CloudFormation nella console ed espandi Resources. Scegli l'applicazione Elastic Beanstalk. Il collegamento si apre nella console Elastic Beanstalk. Scegliere Environments (Ambienti). Scegliere l'URL in URL per aprire l'endpoint in un browser.
   - Per un progetto Lambda, apri il nuovo stack nella AWS CloudFormation console ed espandi Risorse. Scegli la risorsa API Gateway. Il collegamento si apre nella console API Gateway. Scegliere Stages (Fasi). Scegliere l'URL in Invoke URL (Richiama URL) per aprire l'endpoint in un browser.
   - Per un EC2 progetto Amazon, scegli la nuova EC2 istanza Amazon nell'elenco delle risorse del progetto nella AWS CodeStar console. Il link si apre nella pagina Istanza della EC2 console Amazon. Scegli la scheda Descrizione, copia l'URL in Public DNS (IPv4) e apri l'URL in un browser.

5. Verificare che la modifica venga distribuita.

Utilizzo sicuro dei parametri SSM in un progetto AWS CodeStar

Molti clienti archiviano segreti, come le credenziali, nei parametri dell'archivio dei parametri di Systems Manager. Ora è possibile utilizzare in modo sicuro questi parametri in un AWS CodeStar progetto. Ad esempio, potreste voler utilizzare i parametri SSM nelle specifiche di build CodeBuild o durante la definizione delle risorse dell'applicazione nello stack della toolchain (template.yml).

Per utilizzare i parametri SSM in un CodeStar progetto AWS, devi etichettare manualmente i parametri con l'ARN del CodeStar progetto AWS. È inoltre necessario fornire le autorizzazioni appropriate al ruolo di operatore della CodeStar toolchain AWS per accedere ai parametri che hai taggato.

Prima di iniziare

- Create un nuovo parametro di Systems Manager o identificatene uno esistente che contenga le informazioni a cui desiderate accedere.

- Identifica il CodeStar progetto AWS che desideri utilizzare o crea un nuovo progetto.
- Prendi nota dell'ARN del CodeStar progetto. Ha un aspetto simile a questo: `arn:aws:codestar:`*`region-id`*`:`*`account-id`*`:project/`*`project-id`*.

Etichetta un parametro con l'ARN del CodeStar progetto AWS

Per le istruzioni dettagliate, consulta Tagging di parametri del System Manager.

1. In Key (Chiave), immettere `awscodestar:projectArn`.
2. In Valore, inserisci l'ARN del progetto da CodeStar:. `arn:aws:codestar:`*`region-id`*`:`*`account-id`*`:project/`*`project-id`*
3. Seleziona Salva.

Ora puoi fare riferimento al parametro SSM nel file template.yml. Se intendi utilizzarlo con un ruolo lavoratore della toolchain, devi concedere delle autorizzazioni aggiuntive.

Concedi le autorizzazioni per utilizzare i parametri con tag nella tua AWS CodeStar Project Toolchain

> **Note**
>
> Questi passaggi sono applicabili solo ai progetti creati dopo il 6 dicembre 2018 PDT.

1. Apri la dashboard CodeStar del progetto AWS per il progetto che desideri utilizzare.
2. Fare clic su Project (Progetto) per visualizzare l'elenco delle risorse create e individuare il ruolo dipendente della toolchain. Si tratta di una risorsa di IAM con un nome nel formato: `role/CodeStarWorker-`*`project-id`*`-ToolChain`.
3. Fare clic su ARN per aprirlo nella console IAM.
4. Individua ToolChainWorkerPolicy ed espandilo, se necessario.
5. Fare clic su Edit Policy (Modifica Policy).
6. Aggiungere la riga seguente alla sezione `Action:`:

   ```
   ssm:GetParameter*
   ```

7. Fare clic su Review policy (Esamina policy), quindi fare clic su Save changes (Salva le modifiche).

Per i progetti creati prima del 6 dicembre 2018 PDT, dovrai aggiungere le seguenti autorizzazioni ai ruoli dei lavoratori per ogni servizio.

```
        {
            "Action": [
                "ssm:GetParameter*"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ssm:ResourceTag/awscodestar:projectArn": "arn:aws:codestar:region-
id:account-id:project/project-id"
                }
            }
        }
```

Trasferimento del traffico per un progetto AWS Lambda

AWS CodeDeploy supporta le distribuzioni in versione funzionale per le funzioni nei progetti serverless AWS Lambda . AWS CodeStar Un' AWS Lambda implementazione sposta il traffico in entrata da una funzione Lambda esistente a una versione aggiornata della funzione Lambda. Puoi testare una funzione Lambda aggiornata distribuendo una versione separata e quindi ripristinando la distribuzione alla prima versione, se necessario.

Utilizza i passaggi di questa sezione per modificare il modello di AWS CodeStar progetto e aggiornare le CodeStarWorker autorizzazioni IAM dei ruoli. Questa attività avvia una risposta automatica AWS CloudFormation che crea AWS Lambda funzioni con alias e quindi ordina di spostare il traffico AWS CodeDeploy verso un ambiente aggiornato.

> **Note**
>
> Completa questi passaggi solo se hai creato il tuo CodeStar progetto AWS prima del 12 dicembre 2018.

AWS CodeDeploy dispone di tre opzioni di distribuzione che ti consentono di spostare il traffico verso le versioni della tua AWS Lambda funzione nell'applicazione:

- Canary: il traffico viene trasferito in due incrementi. Puoi scegliere tra opzioni Canary predefinite che specificano la percentuale del traffico trasferito alla versione della funzione Lambda aggiornata nel primo incremento e l'intervallo, in minuti, prima che il traffico rimanente venga trasferito nel secondo incremento.
- Lineare: il traffico viene trasferito in incrementi uguali con lo stesso intervallo di tempo, in minuti, tra ciascun incremento. Puoi scegliere tra opzioni lineari predefinite che specificano la percentuale del traffico trasferito in ogni incremento e l'intervallo di tempo, in minuti, tra ciascun incremento. Il traffico viene trasferito in incrementi uguali con lo stesso intervallo di tempo, in minuti, tra ciascun incremento. Puoi scegliere tra opzioni lineari predefinite che specificano la percentuale del traffico trasferito in ogni incremento e l'intervallo di tempo, in minuti, tra ciascun incremento.
- Rll-at-once: Tutto il traffico viene spostato contemporaneamente dalla funzione Lambda originale alla versione aggiornata della funzione Lambda.

Tipo di distribuzione di preferenza
Canary10Percent30Minutes
Canary10Percent5Minutes
Canary10Percent10Minutes
Canary10Percent15Minutes
Lineare 10 10 minuti PercentEvery
Lineare PercentEvery 10 1 minuto
Lineare 10 PercentEvery 2 minuti
Lineare 10 PercentEvery 3 minuti
AllAtOnce

Per ulteriori informazioni sulle AWS CodeDeploy distribuzioni su una piattaforma di AWS Lambda elaborazione, consulta Implementazioni su una AWS piattaforma di elaborazione Lambda.

Per ulteriori informazioni su AWS SAM, vedere AWS Serverless Application Model (SAM) su.AWS GitHub

Prerequisiti:

Quando crei un progetto serverless, devi selezionare un modello per la piattaforma di calcolo Lambda. Per eseguire le fasi da 4 a 6, è necessario avere effettuato l'accesso come amministratore della piattaforma.

Fase 1: Modificare il modello SAM per aggiungere i parametri di distribuzione della AWS Lambda versione

1. Apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.
2. Creare un progetto o scegliere un progetto esistente con un file `template.yml`, quindi aprire la pagina Code (Codice). Nel livello principale del repository, prendere nota della posizione del modello SAM denominato `template.yml` da modificare.
3. Aprire il file `template.yml` nell'IDE o nel repository locale. Copiare il testo seguente per aggiungere una sezione `Globals` al file. Nel testo di esempio di questo tutorial viene scelta l'opzione `Canary10Percent5Minutes`.

```
Globals:
  Function:
    AutoPublishAlias: live
    DeploymentPreference:
      Enabled: true
      Type: Canary10Percent5Minutes
```

Questo esempio illustra un modello modificato dopo l'aggiunta della sezione `Globals`:

```
AWSTemplateFormatVersion: 2010-09-09
Transform:
- AWS::Serverless-2016-10-31
- AWS::CodeStar

Parameters:
  ProjectId:
    Type: String
    Description: CodeStar projectId used to associate new resources to team members

Globals:
  Function:
    AutoPublishAlias: live
    DeploymentPreference:
      Enabled: true
      Type: Canary10Percent5Minutes

Resources:
  HelloWorld:
    Type: AWS::Serverless::Function
    Properties:
      Handler: index.handler
      Runtime: python3.6
      Role:
        Fn::ImportValue:
          !Join ['-', [!Ref 'ProjectId', !Ref 'AWS::Region', 'LambdaTrustRole']]
      Events:
```

Per ulteriori informazioni, consultare la guida di riferimento Globals Section dei modelli SAM.

Passaggio 2: Modifica il CloudFormation ruolo per aggiungere autorizzazioni

1. Accedi a Console di gestione AWS e apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.

   > **Note**
   >
   > Devi accedere Console di gestione AWS utilizzando le credenziali associate all'utente IAM che hai creato o in Configurazione AWS CodeStar cui ti sei identificato. Questo utente deve avere la policy AWS gestita denominata **`AWSCodeStarFullAccess`**allegata.

2. Scegliere il progetto serverless esistente e aprire la pagina Project resources (Risorse del progetto).
3. In Risorse, scegli il ruolo IAM creato per il AWS CloudFormation ruolo CodeStarWorker /. Il ruolo si apre nella console IAM.
4. Nella scheda Permissions (Autorizzazioni), in Inline Policies (Policy inline), nella riga della policy del ruolo del servizio, scegli Edit Policy (Modifica policy). Scegliere la scheda JSON per modificare la policy nel formato JSON.

> **Note**
>
> Il ruolo del servizio è denominato `CodeStarWorkerCloudFormationRolePolicy`.

5. Nel campo JSON, aggiungere le seguenti istruzioni della policy all'interno dell'elemento `Statement`. Sostituisci i *`id`* segnaposto *`region`* and con la tua regione e l'ID dell'account.

```
{
  "Action": [
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:GetBucketVersioning"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::codepipeline*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "lambda:*"
  ],
  "Resource": [
    "arn:aws:lambda:region:id:function:*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "apigateway:*"
  ],
  "Resource": [
    "arn:aws:apigateway:region::*"
  ],
```

```
    "Effect": "Allow"
  },
  {
    "Action": [
      "iam:GetRole",
      "iam:CreateRole",
      "iam:DeleteRole",
      "iam:PutRolePolicy"
    ],
    "Resource": [
      "arn:aws:iam::id:role/*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "iam:AttachRolePolicy",
      "iam:DeleteRolePolicy",
      "iam:DetachRolePolicy"
    ],
    "Resource": [
      "arn:aws:iam::id:role/*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "iam:PassRole"
    ],
    "Resource": [
      "*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "codedeploy:CreateApplication",
      "codedeploy:DeleteApplication",
      "codedeploy:RegisterApplicationRevision"
    ],
    "Resource": [
      "arn:aws:codedeploy:region:id:application:*"
    ],
    "Effect": "Allow"
```

```
},
{
  "Action": [
    "codedeploy:CreateDeploymentGroup",
    "codedeploy:CreateDeployment",
    "codedeploy:DeleteDeploymentGroup",
    "codedeploy:GetDeployment"
  ],
  "Resource": [
    "arn:aws:codedeploy:region:id:deploymentgroup:*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "codedeploy:GetDeploymentConfig"
  ],
  "Resource": [
    "arn:aws:codedeploy:region:id:deploymentconfig:*"
  ],
  "Effect": "Allow"
}
```

6. Scegliere Review policy (Esamina policy) per accertarsi che la policy non contenga errori. Se la policy è priva di errori, scegliere Save changes (Salva modifiche).

Passaggio 3: Conferma e invia la modifica al modello per avviare il AWS Lambda cambio di versione

1. Eseguire il commit e il push delle modifiche al file `template.yml` salvato nella fase 1.

> **Note**
>
> Questo avvia la pipeline. Se esegui le modifiche prima di aggiornare le autorizzazioni IAM, la pipeline si avvia e l'aggiornamento dello AWS CloudFormation stack rileva errori che ripristinano l'aggiornamento dello stack. In questo caso, riavviare la pipeline dopo che le autorizzazioni sono state corrette.

2. L'aggiornamento AWS CloudFormation dello stack inizia quando la pipeline del progetto avvia la fase di distribuzione. Per visualizzare la notifica di aggiornamento dello stack all'inizio della distribuzione, nella AWS CodeStar dashboard, seleziona la AWS CloudFormation fase della pipeline.

Durante l'aggiornamento dello stack, aggiorna AWS CloudFormation automaticamente le risorse del progetto come segue:

- AWS CloudFormation elabora il `template.yml` file creando funzioni Lambda, hook di eventi e risorse con alias.
- AWS CloudFormation chiama Lambda per creare la nuova versione della funzione.
- AWS CloudFormation crea un AppSpec file e chiama AWS CodeDeploy per spostare il traffico.

Per ulteriori informazioni sulla pubblicazione di funzioni Lambda con alias in SAM, consulta AWS il riferimento al modello Serverless Application Model (SAM). Per ulteriori informazioni sugli event hook e sulle risorse presenti nel AWS CodeDeploy AppSpec file, consultate la sezione AppSpec 'resources' (solo distribuzioni AWS Lambda) AppSpec e la sezione 'hooks' per una distribuzione Lambda. AWS

3. Dopo il corretto completamento della pipeline, le risorse vengono create nello stack AWS CloudFormation . Nella pagina Progetto, nell'elenco Risorse del progetto, visualizza l' AWS CodeDeploy applicazione, il gruppo di AWS CodeDeploy distribuzione e le risorse per i ruoli di AWS CodeDeploy servizio create per il progetto.
4. Per creare una nuova versione, modificare la funzione Lambda nel repository. La nuova distribuzione viene avviata e sposta il traffico in base al tipo di distribuzione indicato nel modello SAM. Per visualizzare lo stato del traffico che viene spostato alla nuova versione, nella pagina Progetto, nell'elenco Risorse del progetto, scegli il link alla AWS CodeDeploy distribuzione.
5. Per visualizzare i dettagli su ciascuna revisione, in Revisioni, scegli il link al AWS CodeDeploy gruppo di distribuzione.
6. Nella directory di lavoro locale, puoi apportare modifiche alla tua AWS Lambda funzione e salvare la modifica nell'archivio del tuo progetto. AWS CloudFormation aiuta AWS CodeDeploy a gestire la revisione successiva nello stesso modo. Per ulteriori informazioni sulla ridistribuzione, l'interruzione o il rollback di una distribuzione Lambda, consulta Distribuzioni su una piattaforma di elaborazione Lambda. AWS

Trasferisci il tuo CodeStar progetto AWS alla produzione

Dopo aver creato la tua applicazione utilizzando un CodeStar progetto AWS e visto cosa CodeStar offre AWS, potresti voler passare il tuo progetto all'uso di produzione. Un modo per farlo è replicare le AWS risorse dell'applicazione al di fuori di AWS CodeStar. Avrai comunque bisogno di un repository,

un progetto di build, una pipeline e una distribuzione, ma invece di farli CodeStar creare da AWS per te, li ricreerai utilizzando. CloudFormation

> **Note**
>
> Può essere utile creare o visualizzare un progetto simile utilizzando prima uno dei CodeStar Quick Start di AWS e utilizzarlo come modello per il proprio progetto per assicurarsi di includere le risorse e le policy necessarie.

Un CodeStar progetto AWS è una combinazione di codice sorgente e risorse create per distribuire il codice. Le risorse che supportano la compilazione, il rilascio e la distribuzione del codice sono denominate risorse della toolchain. Al momento della creazione del progetto, un CloudFormation modello fornisce le risorse della toolchain in una pipeline integration/continuous deployment (CI/CD (continua).

Quando utilizzi la console per creare un progetto, il modello di toolchain viene creato per te. Quando si utilizza il AWS CLI per creare un progetto, si crea il modello di toolchain che crea le risorse della toolchain.

Per una toolchain completa sono richieste le seguenti risorse consigliate:

1. Un CodeCommit o un GitHub repository che contiene il codice sorgente.
2. Una CodePipeline pipeline configurata per ascoltare le modifiche al tuo repository.
   a. Quando usi AWS CodeBuild per eseguire test di unità o di integrazione, ti consigliamo di aggiungere una fase di compilazione alla tua pipeline per creare artefatti di build.
   b. Ti consigliamo di aggiungere alla tua pipeline una fase di distribuzione che utilizzi CodeDeploy o distribuisca gli artefatti CloudFormation di build e il codice sorgente nell'infrastruttura di runtime.

      > **Note**
      >
      > Poiché CodePipeline richiede almeno due fasi in una pipeline e la prima fase deve essere la fase di origine, aggiungi una fase di compilazione o distribuzione come seconda fase.

Argomenti

- Crea un repository GitHub

Crea un repository GitHub

Crei un GitHub repository definendolo nel tuo modello di toolchain. Assicurarsi di aver già creato una posizione per un file ZIP contenente il codice sorgente, in modo che il codice possa essere caricato nel repository. Inoltre, devi aver già creato un token di accesso personale in GitHub modo che tu AWS possa connetterti GitHub a tuo nome. Oltre al token di accesso personale per GitHub, è necessario disporre anche dell'`s3.GetObject`autorizzazione per l'`Code`oggetto che si trasmette.

Per specificare un GitHub repository pubblico, aggiungi un codice come il seguente al tuo modello di toolchain in. CloudFormation

```
GitHubRepo:
Condition: CreateGitHubRepo
Description: GitHub repository for application source code
Properties:
  Code:
    S3:
      Bucket: MyCodeS3Bucket
      Key: MyCodeS3BucketKey
  EnableIssues: true
  IsPrivate: false
  RepositoryAccessToken: MyGitHubPersonalAccessToken
  RepositoryDescription: MyAppCodeRepository
  RepositoryName: MyAppSource
  RepositoryOwner: MyGitHubUserName
Type: AWS::CodeStar::GitHubRepository
```

Questo codice specifica le informazioni riportate di seguito:

- La posizione del codice che desideri includere, che deve essere un bucket Amazon S3.
- Se desideri abilitare i problemi nel repository. GitHub
- Se il GitHub repository è privato.
- Il token di accesso GitHub personale che hai creato.
- Descrizione, nome e proprietario del repository che stai creando.

Per i dettagli completi sulle informazioni da specificare, consulta AWS::CodeStar::GitHubRepository nella Guida per l'AWS CloudFormation utente.

Lavorare con i tag di progetto in AWS CodeStar

In AWS CodeStarè possibile associare dei tag ai progetti. I tag semplificano la gestione dei progetti. Ad esempio, potresti aggiungere un tag con una chiave `Release` e un valore `Beta` a tutti i progetti che la tua organizzazione sta utilizzando per il rilascio di una versione beta.

Aggiungere un tag a un progetto

1. Con il progetto aperto nella AWS CodeStar console, nel pannello di navigazione laterale, scegli Impostazioni.
2. In Tag, scegli Modifica.
3. In Chiave, inserisci il nome del tag. In Value (Valore) immettere il valore del tag.
4. Facoltativo: scegli Aggiungi tag per aggiungere altri tag.
5. Una volta che hai finito di aggiungere i tag, scegli Salva.

Rimuovere un tag da un progetto

1. Con il progetto aperto nella AWS CodeStar console, nel pannello di navigazione laterale, scegli Impostazioni.
2. In Tag, scegli Modifica.
3. In Tag, trova il tag che desideri rimuovere e scegli Rimuovi tag.
4. Seleziona Salva.

Ottenere un elenco di tag per un progetto

Usa il AWS CLI per eseguire il AWS CodeStar list-tags-for-project comando, specificando il nome del progetto:

```
aws codestar list-tags-for-project --id my-first-projec
```

Se il comando viene eseguito correttamente, l'output restituisce un elenco di tag simile al seguente:

```
{
  "tags": {
    "Release": "Beta"
  }
```

```
}
```

Eliminare un AWS CodeStar progetto

Se non ne hai più bisogno, puoi eliminare un progetto e le sue risorse così da non incorrere in ulteriori costi in AWS. Quando elimini un progetto, tutti i membri del team vengono rimossi dal progetto I loro ruoli di progetto vengono rimossi dagli utenti IAM, ma i loro profili utente non AWS CodeStar vengono modificati. Puoi usare la AWS CodeStar console o AWS CLI eliminare un progetto. L'eliminazione di un progetto richiede il ruolo AWS CodeStar di servizio`aws-codestar-service-role`, che non deve essere modificato e assunto da. AWS CodeStar

Important

L'eliminazione di un progetto in non può essere annullata AWS CodeStar . Per impostazione predefinita, tutte AWS le risorse per il progetto vengono eliminate dal tuo AWS account, tra cui:

- L' CodeCommit archivio del progetto insieme a tutto ciò che è memorizzato in quel repository.
- I ruoli AWS CodeStar del progetto e le politiche IAM associate configurati per il progetto e le sue risorse.
- Qualsiasi EC2 istanza Amazon creata per il progetto.
- L'applicazione di distribuzione e le risorse associate, come:
  - Un' CodeDeploy applicazione e i gruppi di distribuzione associati.
  - Una AWS Lambda funzione e un API Gateway associato APIs.
  - Un' AWS Elastic Beanstalk applicazione e un ambiente associato.
- La pipeline di distribuzione continua per il progetto in CodePipeline.
- Gli AWS CloudFormation stack associati al progetto.
- Qualsiasi ambiente di AWS Cloud9 sviluppo creato con la AWS CodeStar console. Tutte le modifiche del codice non eseguite negli ambienti vengono perse.

Per eliminare tutte le risorse del progetto insieme al progetto, seleziona la casella di controllo Elimina risorse. Se si deseleziona questa opzione, il progetto viene eliminato in AWS CodeStar IAM e i ruoli del progetto che hanno consentito l'accesso a tali risorse vengono eliminati in IAM, ma tutte le altre risorse vengono mantenute. Potresti continuare a incorrere

in addebiti per queste risorse in. AWS Se non desideri più una o più di queste risorse, devi eliminarle manualmente. Per ulteriori informazioni, consulta Eliminazione del progetto: un AWS CodeStar progetto è stato eliminato, ma le risorse esistono ancora.
Se decidi di mantenere le risorse quando elimini un progetto, come best practice, copia l'elenco delle risorse dalla pagina dei dettagli del progetto. In questo modo avrai un record di tutte le risorse che hai mantenuto, anche se il progetto non esiste più.

Argomenti

Elimina un progetto in AWS CodeStar (Console)

È possibile utilizzare la AWS CodeStar console per eliminare un progetto.

Per eliminare un progetto in AWS CodeStar

1. Apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.
2. Scegli Progetti nel riquadro di navigazione.
3. Seleziona il progetto che desideri eliminare e scegli Elimina.

   In alternativa, apri il progetto e scegli Impostazioni dal riquadro di navigazione sul lato sinistro della console. Nella pagina dei dettagli del progetto, seleziona Delete project (Elimina progetto).
4. Nella pagina di conferma dell'eliminazione, inserisci delete. Mantieni selezionata l'opzione Elimina risorse se desideri eliminare le risorse del progetto. Scegli Elimina.

   L'eliminazione di un progetto può richiedere alcuni minuti. Dopo l'eliminazione, il progetto non viene più visualizzato nell'elenco dei progetti nella AWS CodeStar console.

   Important

   Se il progetto utilizza risorse esterne AWS (ad esempio, un GitHub repository o problemi in Atlassian JIRA), tali risorse non vengono eliminate, anche se si seleziona la casella di controllo.
   Il progetto non può essere eliminato se alcune policy AWS CodeStar gestite sono state associate manualmente a ruoli che non sono utenti IAM. Se hai collegato le policy gestite

del tuo progetto a un ruolo dell'utente federato, è necessario scollegare la policy prima di eliminare il progetto. Per ulteriori informazioni, consulta ???.

Elimina un progetto in AWS CodeStar (AWS CLI)

È possibile utilizzare il AWS CLI per eliminare un progetto.

Per eliminare un progetto in AWS CodeStar

1. In un terminale (Linux, macOS o Unix) o dal prompt dei comandi (Windows), esegui il delete-project comando, incluso il nome del progetto. Ad esempio, per eliminare un progetto con l'ID: *my-2nd-project*

   ```
   aws codestar delete-project --id my-2nd-project
   ```

   Questo comando restituisce un output simile al seguente:

   ```
   {
       "projectArn":"arn:aws:codestar:us-east-2:111111111111:project/my-2nd-project"
   }
   ```

   I progetti non vengono eliminati immediatamente.
2. Eseguire il comando describe-project, incluso il nome del progetto. Ad esempio, per verificare lo stato di un progetto con l'ID*my-2nd-project*:

   ```
   aws codestar describe-project --id my-2nd-project
   ```

   se il progetto non viene ancora eliminato, questo comando restituisce un output simile al seguente:

   ```
   {
       "name": "my project",
       "id": "my-2nd-project",
       "arn": "arn:aws:codestar:us-west-2:123456789012:project/my-2nd-project",
       "description": "My second CodeStar project.",
       "createdTimeStamp": 1572547510.128,
   ```

```
    "status": {
        "state": "CreateComplete"
    }
}
```

Se il progetto viene eliminato, questo comando restituisce output simile al seguente:

```
   An error occurred (ProjectNotFoundException) when calling the DescribeProject
 operation: The project ID was not found: my-2nd-project. Make sure that the
 project ID is correct and then try again.
```

3. Eseguire il comando list-projects e verificare che il progetto eliminato non sia più disponibile nell'elenco di progetti associati al proprio account AWS .

```
aws codestar list-projects
```

Lavorare con AWS CodeStar i team

Dopo aver creato un progetto di sviluppo, puoi concedere l'accesso ad altri utenti per collaborare con loro. Nel AWS CodeStar, ogni progetto ha un team di progetto. Un utente può appartenere a più AWS CodeStar progetti e avere AWS CodeStar ruoli diversi (e quindi autorizzazioni diverse) in ciascuno di essi. Nella AWS CodeStar console, gli utenti vedono tutti i progetti associati al tuo AWS account, ma possono visualizzare e lavorare solo su quei progetti di cui fanno parte del team.

I membri del team possono scegliere un nome descrittivo. I membri del team possono anche aggiungere un indirizzo e-mail in modo che altre persone del team possano contattarli. I membri del team che non sono proprietari non possono modificare il proprio ruolo AWS CodeStar per il progetto.

Ogni progetto AWS CodeStar ha tre ruoli:

Ruoli e autorizzazioni in un progetto AWS CodeStar

Nome ruolo	Visualizzazione stato e pannello di controllo del progetto	Add/Remove/ AccessRisorse del progetto	Aggiunta/ rimozione di membri del team	Eliminazione del progetto
Owner	x	x	x	x
Collaboratore	x	x		
Visualizzatore	x			

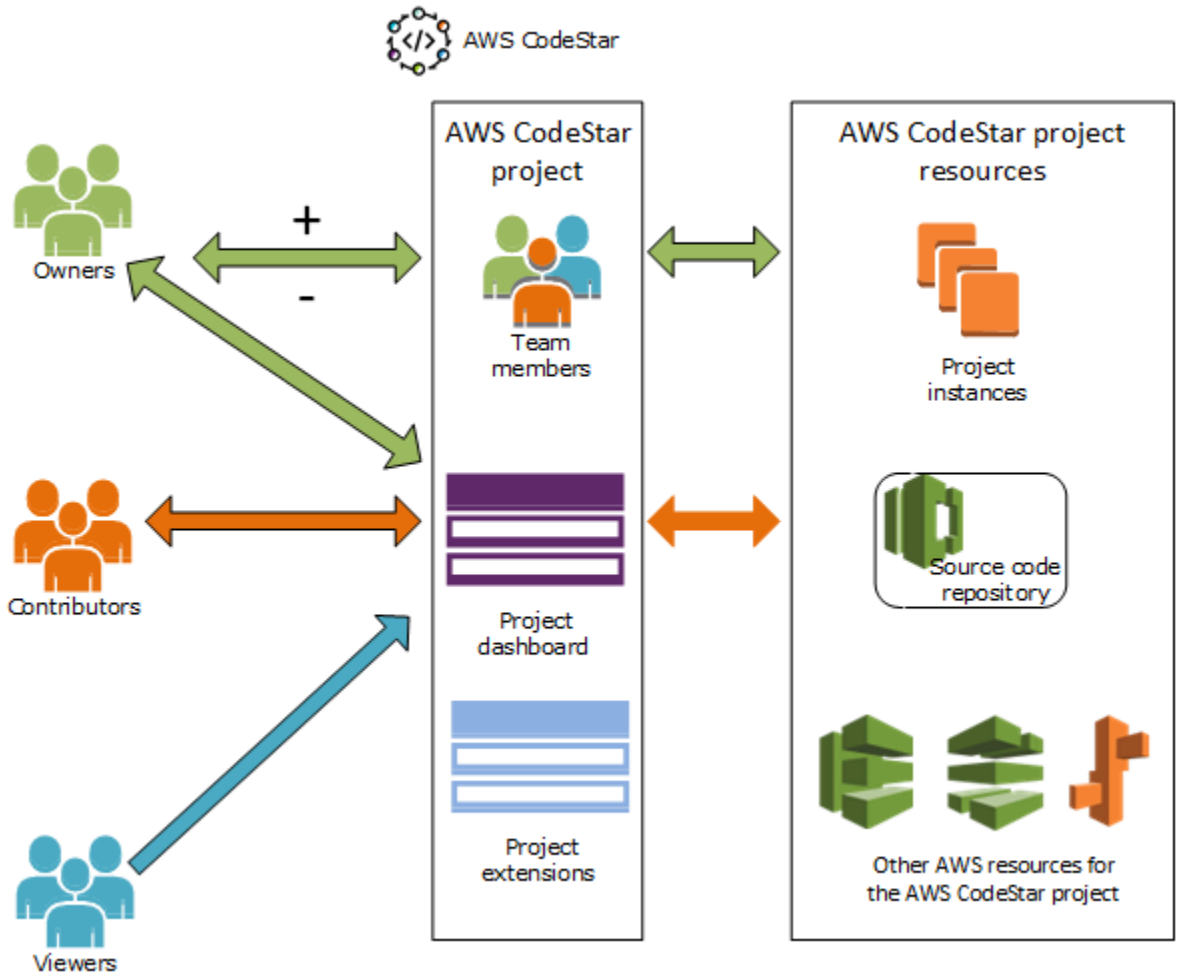
- Proprietario: può aggiungere e rimuovere altri membri del team, contribuire con codice a un repository di progetto se il codice è archiviato in CodeCommit, concedere o negare agli altri membri del team l'accesso remoto a qualsiasi EC2 istanza Amazon che esegue Linux associata al progetto, configurare la dashboard del progetto ed eliminare il progetto.
- Collaboratore: può aggiungere e rimuovere risorse del pannello di controllo come un riquadro JIRA, aggiungere codice all'archivio del progetto se il codice è memorizzato nel CodeCommit pannello di controllo e interagire completamente con la dashboard. Non può aggiungere né rimuovere i membri del team, né concedere o rifiutare l'accesso remoto alle risorse o eliminare il progetto. Questo è il ruolo che si dovrebbe scegliere per la maggior parte dei membri del team.

- Visualizzatore: può visualizzare la dashboard del progetto, il codice in cui è memorizzato e CodeCommit, nei riquadri della dashboard, lo stato del progetto e delle sue risorse.

> **Important**
>
> Se il progetto utilizza risorse esterne AWS (ad esempio, un GitHub repository o problemi in Atlassian JIRA), l'accesso a tali risorse è controllato dal fornitore di risorse, non. AWS CodeStar Per ulteriori informazioni, consultare la documentazione messa a disposizione dal fornitore delle risorse.
>
> Chiunque abbia accesso a un AWS CodeStar progetto può utilizzare la AWS CodeStar console per accedere a risorse esterne AWS ma correlate al progetto.
>
> AWS CodeStar non consente automaticamente ai membri del team di progetto di partecipare agli ambienti di AWS Cloud9 sviluppo correlati a un progetto. Per consentire a un membro del team di partecipare a un ambiente condiviso, consulta Condividi un AWS Cloud9 ambiente con un membro del team di progetto.

A ogni ruolo del progetto è associata una policy IAM. La policy è personalizzata in modo da riflettere le risorse di progetto. Per ulteriori informazioni su questo tipo di policy, consulta Esempi di policy CodeStar basate sull'identità di AWS.

Il diagramma seguente mostra la relazione tra ciascun ruolo e un progetto AWS CodeStar .



Argomenti

- Aggiungere membri del team a un AWS CodeStar progetto
- Gestisci le autorizzazioni per i AWS CodeStar membri del team
- Rimuovere membri del team da un AWS CodeStar progetto

Aggiungere membri del team a un AWS CodeStar progetto

Se hai il ruolo di proprietario in un AWS CodeStar progetto o hai la `AWSCodeStarFullAccess` policy applicata al tuo utente IAM, puoi aggiungere altri utenti IAM al team di progetto. Si tratta di un processo semplice che applica un AWS CodeStar ruolo (proprietario, collaboratore o spettatore) all'utente. Questi ruoli sono in base ai progetti e personalizzati. Ad esempio, un membro collaboratore del team in un progetto A potrebbe avere delle autorizzazioni per le risorse diverse da quelle di un membro collaboratore del team in un progetto B. Un membro del team può avere solo un ruolo in un

progetto. Dopo aver aggiunto un membro del team, quest'ultimo può interagire immediatamente con il tuo progetto al livello definito dal ruolo.

I vantaggi dei AWS CodeStar ruoli e dell'appartenenza al team includono:

- Non è necessario configurare manualmente le autorizzazioni in IAM per i membri del team.
- È possibile modificare facilmente il livello di un membro del team di accesso a un progetto.
- Gli utenti possono accedere ai progetti nella AWS CodeStar console solo se sono membri del team.
- L'accesso degli utenti a un progetto è definito in base al ruolo.

Per ulteriori informazioni su team e AWS CodeStar ruoli, vedere Lavorare con AWS CodeStar i team eLavorare con il tuo profilo AWS CodeStar utente .

Per aggiungere un membro del team a un progetto, devi avere il ruolo di AWS CodeStar proprietario del progetto o della `AWSCodeStarFullAccess` politica.

> **Important**
>
> L'aggiunta di un membro del team non influisce sull'accesso di tale membro a risorse esterne AWS (ad esempio, un GitHub repository o problemi in Atlassian JIRA). Queste autorizzazioni di accesso sono controllate dal fornitore di risorse, non. AWS CodeStar Per ulteriori informazioni, consultare la documentazione messa a disposizione dal fornitore delle risorse.
> Chiunque abbia accesso a un AWS CodeStar progetto può utilizzare la AWS CodeStar console per accedere a risorse esterne AWS ma correlate a quel progetto.
> L'aggiunta di un membro del team a un progetto non consente automaticamente a tale membro di partecipare a qualsiasi ambiente di AWS Cloud9 sviluppo correlato al progetto. Per consentire a un membro del team di partecipare a un ambiente condiviso, consulta Condividi un AWS Cloud9 ambiente con un membro del team di progetto.
> La concessione dell'accesso a un progetto a un utente federato implica collegare manualmente la policy gestita dal proprietario, dal collaboratore o dal visualizzatore di AWS CodeStar al ruolo assunto dall'utente federato. Per ulteriori informazioni, consulta Accesso utente federato a AWS CodeStar.

Argomenti

Aggiungi un membro del team (Console)

Puoi usare la AWS CodeStar console per aggiungere un membro del team al tuo progetto. Se esiste già un utente IAM per la persona che desideri aggiungere, puoi aggiungere l'utente IAM. Altrimenti, puoi creare un utente IAM per quella persona quando la aggiungi al tuo progetto.

Per aggiungere un membro del team a un AWS CodeStar progetto (console)

1. Apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.
2. Scegli Progetti dal pannello di navigazione e scegli il tuo progetto.
3. Nel riquadro di navigazione laterale del progetto, scegli Team.
4. Nella pagina Team members (Membri del team), scegli Add team member (Aggiungi membro del team).
5. In Choose user (Seleziona utente), procedere in uno dei modi seguenti:

   - Se esiste già un utente IAM per la persona che desideri aggiungere, scegli l'utente IAM dall'elenco.

     > **Note**
     >
     > Gli utenti che sono già stati aggiunti a un altro AWS CodeStar progetto vengono visualizzati nell'elenco AWS CodeStar Utenti esistenti.

     Nel ruolo del progetto, scegli il AWS CodeStar ruolo (Proprietario, Collaboratore o Visualizzatore) per questo utente. Si tratta di un ruolo a livello di progetto AWS CodeStar che può essere modificato solo da un proprietario del progetto. Se applicato a un utente IAM, il ruolo fornisce tutte le autorizzazioni necessarie per accedere alle risorse AWS CodeStar del progetto. Applica le politiche necessarie per creare e gestire le credenziali Git per il codice archiviato CodeCommit in IAM o per caricare le chiavi Amazon EC2 SSH per l'utente in IAM.

> **Important**
>
> Non puoi fornire o modificare il nome visualizzato o le informazioni e-mail per un utente IAM a meno che tu non abbia effettuato l'accesso alla console come tale utente. Per ulteriori informazioni, consulta Gestisci le informazioni di visualizzazione per il tuo profilo AWS CodeStar utente .

Scegli Aggiungi membro del team.

- Se non esiste un utente IAM per la persona che desideri aggiungere al progetto, scegli Crea nuovo utente IAM. Verrai reindirizzato alla console IAM dove potrai creare un nuovo utente IAM. Per ulteriori informazioni, consulta Creazione di utenti IAM nella guida per l'utente IAM. Dopo aver creato il tuo utente IAM, torna alla AWS CodeStar console, aggiorna l'elenco degli utenti e scegli l'utente IAM che hai creato dall'elenco a discesa. Inserisci il nome AWS CodeStar visualizzato, l'indirizzo email e il ruolo di progetto che desideri applicare a questo nuovo utente, quindi scegli Aggiungi membro del team.

> **Note**
>
> Per facilità di gestione, ad almeno un utente deve essere assegnato il ruolo di proprietario del progetto.

6. Invia al nuovo membro del team le seguenti informazioni:

   - Informazioni di connessione per il tuo AWS CodeStar progetto.
   - Se il codice sorgente è memorizzato in CodeCommit, istruzioni per configurare l'accesso con credenziali Git al CodeCommit repository dai loro computer locali.
   - Informazioni su come l'utente può gestire il nome visualizzato, l'indirizzo e-mail e la chiave Amazon EC2 SSH pubblica, come descritto inLavorare con il tuo profilo AWS CodeStar utente .
   - Password monouso e informazioni di connessione, se l'utente è nuovo AWS e hai creato un utente IAM per quella persona. La password scade la prima volta in cui l'utente effettua l'accesso. L'utente deve scegliere una nuova password.

Aggiungi e Visualizza i membri del team (AWS CLI)

Puoi usare il AWS CLI per aggiungere membri del team al tuo team di progetto. Puoi inoltre visualizzare le informazioni su tutti i membri del team nel progetto.

Per aggiungere un membro del team

1. Apri un finestra dei comandi o di terminale.
2. Esegui il comando associate-team-member con i parametri `--project-id`, `-user-arn` e `--project-role`. Puoi anche specificare se l'utente dispone di accesso remoto alle istanze del progetto includendo i parametri `--remote-access-allowed` oppure `--no-remote-access-allowed`. Per esempio:

   ```
   aws codestar associate-team-member --project-id my-first-projec --user-arn
    arn:aws:iam:111111111111:user/Jane_Doe --project-role Contributor --remote-access-
   allowed
   ```

   Questo comando non restituisce alcun output.

Per visualizzare tutti i membri del team (AWS CLI)

1. Apri un finestra dei comandi o di terminale.
2. Eseguire il comando list-team-members con il parametro `--project-id`. Per esempio:

   ```
   aws codestar list-team-members --project-id my-first-projec
   ```

   Questo comando restituisce un output simile al seguente:

   ```
   {
       "teamMembers":[

    {"projectRole":"Owner","remoteAccessAllowed":true,"userArn":"arn:aws:iam::111111111111:use
   Mary_Major"},

    {"projectRole":"Contributor","remoteAccessAllowed":true,"userArn":"arn:aws:iam::1111111111
   Jane_Doe"},

    {"projectRole":"Contributor","remoteAccessAllowed":true,"userArn":"arn:aws:iam::1111111111
   John_Doe"},
   ```

```
 {"projectRole":"Viewer","remoteAccessAllowed":false,"userArn":"arn:aws:iam::111111111111:u
John_Stiles"}
 ]
}
```

Gestisci le autorizzazioni per i AWS CodeStar membri del team

Puoi modificare le autorizzazioni per i membri del team cambiando il loro AWS CodeStar ruolo. A ciascun membro del team può essere assegnato un solo ruolo in un AWS CodeStar progetto, ma è possibile assegnare lo stesso ruolo a più utenti. Puoi usare la AWS CodeStar console o gestire AWS CLI le autorizzazioni.

> **Important**
>
> Per modificare il ruolo di un membro del team, devi avere il ruolo di AWS CodeStar proprietario per quel progetto o applicare la `AWSCodeStarFullAccess` politica.
> La modifica delle autorizzazioni di un membro del team non influisce sull'accesso di tale membro del team a risorse esterne AWS (ad esempio, un GitHub repository o problemi in Atlassian JIRA). Queste autorizzazioni di accesso vengono controllate dal provider della risorsa, non da AWS CodeStar. Per ulteriori informazioni, consultare la documentazione messa a disposizione dal fornitore delle risorse.
> Chiunque abbia accesso a un AWS CodeStar progetto può essere in grado di utilizzare la AWS CodeStar console per accedere a risorse esterne AWS ma correlate a quel progetto.
> La modifica del ruolo di un membro del team per un progetto non consente o impedisce automaticamente a quel membro di partecipare a qualsiasi ambiente di AWS Cloud9 sviluppo del progetto. Per consentire o impedire al membro del team di partecipare a un ambiente condiviso, consulta Condividi un AWS Cloud9 ambiente con un membro del team di progetto.

Puoi anche concedere agli utenti le autorizzazioni per accedere in remoto a qualsiasi istanza Amazon EC2 Linux associata al progetto. Dopo aver concesso questa autorizzazione, l'utente deve caricare una chiave pubblica SSH associata al proprio profilo AWS CodeStar utente in tutti i progetti del team. Per connettersi correttamente alle istanze Linux, l'utente deve disporre dell'SSH configurata e della chiave privata sul computer locale.

Argomenti

Gestione delle autorizzazioni per il team (console)

Puoi utilizzare la AWS CodeStar console per gestire i ruoli dei membri del team. Puoi anche stabilire se i membri del team hanno accesso remoto alle EC2 istanze Amazon associate al tuo progetto.

Per modificare il ruolo di un membro del team

1. Apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.
2. Scegli Progetti dal pannello di navigazione e scegli il tuo progetto.
3. Nel riquadro di navigazione laterale del progetto, scegli Team.
4. Nella pagina Membri del team, scegli il membro del team e scegli Modifica.
5. Nel ruolo del progetto, scegli il AWS CodeStar ruolo (proprietario, collaboratore o spettatore) che desideri concedere a questo utente.

   Per ulteriori informazioni sui AWS CodeStar ruoli e le relative autorizzazioni, consulta. Lavorare con AWS CodeStar i team

   Scegli Modifica membro del team.

Per concedere a un membro del team le autorizzazioni di accesso remoto alle istanze Amazon EC2

1. Apri la AWS CodeStar console all'indirizzo. https://console.aws.amazon.com/codestar/
2. Scegli Progetti dal pannello di navigazione e scegli il tuo progetto.
3. Nel riquadro di navigazione laterale del progetto, scegli Team.
4. Nella pagina Membri del team, scegli il membro del team e scegli Modifica.
5. Seleziona Consenti l'accesso SSH alle istanze del progetto, quindi scegli Modifica membro del team.
6. (Facoltativo) Informa i membri del team che devono caricare una chiave pubblica SSH per i loro AWS CodeStar utenti, se non l'hanno già fatto. Per ulteriori informazioni, consulta Aggiungi una chiave pubblica al tuo profilo AWS CodeStar utente .

Gestione delle autorizzazioni per il team (AWS CLI)

Puoi utilizzare il AWS CLI per gestire il ruolo del progetto assegnato a un membro del team. Puoi utilizzare gli stessi AWS CLI comandi per stabilire se quel membro del team ha accesso remoto alle EC2 istanze Amazon associate al tuo progetto.

Per gestire le autorizzazioni per un membro del team

1. Apri un finestra dei comandi o di terminale.
2. Esegui il comando update-team-member con i parametri `--project-id`, `-user-arn` e `--project-role`. Puoi anche specificare se l'utente dispone di accesso remoto alle istanze del progetto includendo i parametri `--remote-access-allowed` oppure `--no-remote-access-allowed`. Ad esempio, per aggiornare il ruolo di progetto di un utente IAM di nome John_Doe e modificare le sue autorizzazioni in un visualizzatore senza accesso remoto alle istanze Amazon del progetto: EC2

   ```
   aws codestar update-team-member --project-id my-first-projec --user-arn
    arn:aws:iam:111111111111:user/John_Doe --project-role Viewer --no-remote-access-
   allowed
   ```

   Questo comando restituisce un output simile al seguente:

   ```
   {
    "projectRole":"Viewer",
    "remoteAccessAllowed":false,
    "userArn":"arn:aws:iam::111111111111:user/John_Doe"
   }
   ```

Rimuovere membri del team da un AWS CodeStar progetto

Dopo aver rimosso un utente da un AWS CodeStar progetto, l'utente appare ancora nella cronologia dei commit dell'archivio del progetto, ma non ha più accesso al CodeCommit repository o ad altre risorse del progetto, come la pipeline del progetto. (L'eccezione a questa regola è un utente IAM che dispone di altre politiche che garantiscono l'accesso a tali risorse.) L'utente non può accedere alla dashboard del progetto e il progetto non viene più visualizzato nell'elenco dei progetti che l'utente vede nella AWS CodeStar dashboard. Puoi utilizzare la AWS CodeStar console o AWS CLI rimuovere membri del team dal team di progetto.

> **Important**
>
> Sebbene la rimozione di un membro del team da un progetto neghi l'accesso remoto alle EC2 istanze Amazon del progetto, non chiude nessuna delle sessioni SSH attive dell'utente.
> La rimozione di un membro del team non influisce sull'accesso di tale membro del team a risorse esterne AWS (ad esempio, un GitHub repository o problemi in Atlassian JIRA). Queste autorizzazioni di accesso sono controllate dal fornitore di risorse, non. AWS CodeStar Per ulteriori informazioni, consultare la documentazione messa a disposizione dal fornitore delle risorse.
> La rimozione di un membro del team da un progetto non elimina automaticamente gli ambienti di AWS Cloud9 sviluppo correlati a quel membro del team né impedisce a quel membro di partecipare agli ambienti di AWS Cloud9 sviluppo correlati a cui è stato invitato. Per eliminare un ambiente di sviluppo, consultare Eliminare un AWS Cloud9 ambiente da un progetto. Per impedire a un membro del team di partecipare a un ambiente condiviso, consultare Condividi un AWS Cloud9 ambiente con un membro del team di progetto.

Per rimuovere un membro del team da un progetto, devi avere il ruolo di AWS CodeStar proprietario per quel progetto o avere la `AWSCodeStarFullAccess` politica applicata al tuo account.

Argomenti

- Rimozione dei membri del team (console)
- Rimozione dei membri del team (AWS CLI)

Rimozione dei membri del team (console)

Puoi utilizzare la AWS CodeStar console per rimuovere membri del team dal team di progetto.

Per rimuovere un membro del team da un progetto

1. Apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.
2. Scegli Progetti dal pannello di navigazione e scegli il tuo progetto.
3. Nel riquadro di navigazione laterale del progetto, scegli Team.
4. Nella pagina Membri del team, scegli il membro del team e scegli Rimuovi.

Rimozione dei membri del team (AWS CLI)

Puoi utilizzare il AWS CLI per rimuovere membri del team dal team di progetto.

Per rimuovere un membro del team

1. Apri un finestra dei comandi o di terminale.
2. Eseguire il comando disassociate-team-member con `--project-id` e `-user-arn`. Per esempio:

```
aws codestar disassociate-team-member --project-id my-first-projec --user-arn
 arn:aws:iam:111111111111:user/John_Doe
```

Questo comando restituisce un output simile al seguente:

```
{
    "projectId": "my-first-projec",
    "userArn": "arn:aws:iam::111111111111:user/John_Doe"
}
```

Lavorare con il tuo profilo AWS CodeStar utente

Il tuo profilo AWS CodeStar utente è associato al tuo utente IAM. Questo profilo contiene un nome visualizzato e un indirizzo e-mail che vengono utilizzati in tutti i AWS CodeStar progetti a cui appartieni. Puoi caricare una chiave pubblica SSH da associare al profilo. Questa chiave pubblica fa parte della coppia di chiavi pubblica-privata SSH che usi quando ti connetti a EC2 istanze Amazon associate ai AWS CodeStar progetti a cui appartieni.

> **Note**
>
> Le informazioni contenute in questi argomenti riguardano solo il tuo profilo utente. AWS CodeStar Se il progetto utilizza risorse esterne AWS (ad esempio, un GitHub repository o problemi in Atlassian JIRA), tali fornitori di risorse potrebbero utilizzare i propri profili utente, che potrebbero avere impostazioni diverse. Per ulteriori informazioni, consultare la documentazione messa a disposizione dal fornitore delle risorse.

Argomenti

Gestisci le informazioni di visualizzazione per il tuo profilo AWS CodeStar utente

Puoi utilizzare la AWS CodeStar console o AWS CLI modificare il nome visualizzato e l'indirizzo e-mail nel tuo profilo utente. Un profilo utente non è specifico di un progetto, È associato al tuo utente IAM e viene applicato a tutti i AWS CodeStar progetti a cui appartieni in una AWS regione. Se appartieni a progetti in più di una AWS regione, hai profili utente separati.

Puoi gestire il tuo profilo utente solo nella AWS CodeStar console. Se disponi della `AWSCodeStarFullAccess` politica, puoi utilizzarla AWS CLI per visualizzare e gestire altri profili.

> **Note**
>
> Le informazioni contenute in questo argomento riguardano solo il profilo AWS CodeStar utente. Se il progetto utilizza risorse esterne AWS (ad esempio, un GitHub repository

o problemi in Atlassian JIRA), tali fornitori di risorse potrebbero utilizzare i propri profili utente, che potrebbero avere impostazioni diverse. Per ulteriori informazioni, consultare la documentazione messa a disposizione dal fornitore delle risorse.

Argomenti

Gestione del profilo utente (console)

Puoi gestire il tuo profilo utente nella AWS CodeStar console accedendo a qualsiasi progetto in cui sei membro del team e modificando le informazioni del tuo profilo. Poiché i profili utente sono specifici dell'utente e non del progetto, le modifiche al profilo utente vengono visualizzate in ogni progetto in una AWS regione in cui sei membro del team.

Important

Per utilizzare la console per modificare le informazioni di visualizzazione per un utente, devi accedere come utente IAM. Nessun altro utente, nemmeno quelli con il ruolo di AWS CodeStar proprietario di un progetto o con la `AWSCodeStarFullAccess` politica applicata, può modificare le informazioni di visualizzazione.

Per modificare le informazioni di visualizzazione in tutti i progetti in una AWS regione

1. Apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.
2. Scegli Progetti dal pannello di navigazione e scegli un progetto in cui sei membro del team.
3. Nel riquadro di navigazione laterale del progetto, scegli Team.
4. Nella pagina Membri del team, scegli l'utente IAM, quindi scegli Modifica.
5. Modifica il nome visualizzato, l'indirizzo email o entrambi, quindi scegli Modifica membro del team.

> **Note**
>
> Sono richiesti un nome visualizzato e un indirizzo e-mail. Per ulteriori informazioni, consulta Limiti in AWS CodeStar.

Gestione dei profili utente (AWS CLI)

Puoi utilizzarlo AWS CLI per creare e gestire il tuo profilo utente in AWS CodeStar. Puoi anche utilizzare il AWS CLI per visualizzare le informazioni del tuo profilo utente e per visualizzare tutti i profili utente configurati per il tuo AWS account in una AWS regione.

Assicurati che il tuo AWS profilo sia configurato per la regione in cui desideri creare, gestire o visualizzare i profili utente.

Per creare un profilo utente

1. Apri un finestra dei comandi o di terminale.
2. Esegui il comando create-user-profile con i parametri `user-arn`, `display-name` e `email-address`. Per esempio:

```
aws codestar create-user-profile --user-arn arn:aws:iam:111111111111:user/
John_Stiles --display-name "John Stiles" --email-address "john_stiles@example.com"
```

Questo comando restituisce un output simile al seguente:

```
{
 "createdTimestamp":1.491439687681E9,"
 displayName":"John Stiles",
 "emailAddress":"john.stiles@example.com",
 "lastModifiedTimestamp":1.491439687681E9,
 "userArn":"arn:aws:iam::111111111111:user/Jane_Doe"
}
```

Per visualizzare le informazioni visualizzate

1. Apri un finestra dei comandi o di terminale.
2. Eseguire il comando describe-user-profile con il parametro `user-arn`. Per esempio:

```
aws codestar describe-user-profile --user-arn arn:aws:iam:111111111111:user/
Mary_Major
```

Questo comando restituisce un output simile al seguente:

```
{
 "createdTimestamp":1.490634364532E9,
 "displayName":"Mary Major",
 "emailAddress":"mary.major@example.com",
 "lastModifiedTimestamp":1.491001935261E9,
 "sshPublicKey":"EXAMPLE=",
 "userArn":"arn:aws:iam::111111111111:user/Mary_Major"
}
```

Per modificare le informazioni visualizzate

1. Apri un finestra dei comandi o di terminale.
2. Eseguire il comando update-user-profile con il parametro `user-arn` e i parametri del profilo che si desidera modificare, ad esempio `display-name` o `email-address`. Ad esempio, se un utente con il nome visualizzato Jane Doe vuole modificare il suo nome visualizzato in Jane Mary Doe:

```
aws codestar update-user-profile --user-arn arn:aws:iam:111111111111:user/Jane_Doe
 --display-name "Jane Mary Doe"
```

Questo comando restituisce un output simile al seguente:

```
{
 "createdTimestamp":1.491439687681E9,
 "displayName":"Jane Mary Doe",
 "emailAddress":"jane.doe@example.com",
 "lastModifiedTimestamp":1.491442730598E9,
 "sshPublicKey":"EXAMPLE1",
 "userArn":"arn:aws:iam::111111111111:user/Jane_Doe"
}
```

Per elencare tutti i profili utente di una AWS regione nel tuo AWS account

1. Apri un finestra dei comandi o di terminale.
2. Esegui il comando aws codestar list-user-profiles. Per esempio:

```
aws codestar list-user-profiles
```

Questo comando restituisce un output simile al seguente:

```
{
  "userProfiles":[
 {
  "displayName":"Jane Doe",
  "emailAddress":"jane.doe@example.com",
  "sshPublicKey":"EXAMPLE1",
  "userArn":"arn:aws:iam::111111111111:user/Jane_Doe"
 },
 {
  "displayName":"John Doe",
  "emailAddress":"john.doe@example.com",
  "sshPublicKey":"EXAMPLE2",
  "userArn":"arn:aws:iam::111111111111:user/John_Doe"
 },
 {
  "displayName":"Mary Major",
  "emailAddress":"mary.major@example.com",
  "sshPublicKey":"EXAMPLE=",
  "userArn":"arn:aws:iam::111111111111:user/Mary_Major"
 },
 {
  "displayName":"John Stiles",
  "emailAddress":"john.stiles@example.com",
  "sshPublicKey":"",
  "userArn":"arn:aws:iam::111111111111:user/John_Stiles"
 }
  ]
}
```

Aggiungi una chiave pubblica al tuo profilo AWS CodeStar utente

Puoi caricare una chiave SSH pubblica appartenente alla coppia di chiavi pubblica-privata che crei e gestisci. Utilizzi questa coppia di chiavi SSH pubblica-privata per accedere alle EC2 istanze Amazon che eseguono Linux. Se il proprietario di un progetto ti ha concesso l'autorizzazione per l'accesso da remoto, puoi accedere alle sole istanze associate al progetto. Puoi usare la AWS CodeStar console o gestire la tua AWS CLI chiave pubblica.

> **Important**
>
> AWS CodeStar Il proprietario di un progetto può concedere a proprietari, collaboratori e visualizzatori del progetto l'accesso SSH alle EC2 istanze Amazon per il progetto, ma solo l'individuo (proprietario, collaboratore o visualizzatore) può impostare la chiave SSH. Per eseguire questa operazione, l'utente deve essere registrato come proprietario, collaboratore o visualizzatore.
>
> AWS CodeStar non gestisce le chiavi SSH per gli ambienti. AWS Cloud9

Argomenti

Gestisci la tua chiave pubblica (Console)

Sebbene non sia possibile generare una coppia di chiavi pubblica-privata nella console, è possibile crearne una localmente e quindi aggiungerla o gestirla come parte del profilo utente tramite la AWS CodeStar console.

Per gestire la chiave SSH pubblica

1. Da un terminale o da una finestra con emulatore Bash, eseguire il comando ssh-keygen per generare una coppia di chiavi SSH pubblica-privata sul computer locale. Puoi generare una chiave in qualsiasi formato consentito da Amazon EC2. Per informazioni sui formati accettabili, consulta Importazione della propria chiave pubblica su Amazon EC2. L'ideale sarebbe generare una chiave SSH-2 RSA, in formato OpenSSH di 2048 bit di lunghezza. La chiave pubblica è memorizzata in un file con estensione .pub.

2. Apri la AWS CodeStar console all'indirizzo https://console.aws.amazon.com/codestar/.

   Scegliere un progetto in cui l'utente è un membro del team.

3. Nel riquadro di navigazione, scegli Team.
4. Nella pagina Membri del team, trova il nome del tuo utente IAM, quindi scegli Modifica.
5. Nella pagina Modifica membro del team, in Accesso remoto, abilita Consenti l'accesso SSH alle istanze del progetto.
6. Nella casella Chiave pubblica SSH, incolla la chiave pubblica, quindi scegli Modifica membro del team.

   > **Note**
   >
   > È possibile modificare la chiave pubblica eliminando la chiave precedente presente in questo campo e inserendone una nuova. Puoi eliminare una chiave pubblica eliminando il contenuto di questo campo e quindi scegliendo Modifica membro del team.

   Quando si modifica o si elimina una chiave pubblica, si sta modificando il proprio profilo utente. Non è una modifica a livello di progetto. Poiché la chiave è associata al profilo, questa si modifica (o viene eliminata) in tutti i progetti in cui si dispone dell'autorizzazione di accesso remoto.

   L'eliminazione della chiave pubblica rimuove l'accesso alle EC2 istanze Amazon che eseguono Linux in tutti i progetti in cui ti è stato concesso l'accesso remoto. Tuttavia, non chiude nessuna delle sessioni SSH già aperte che utilizzano tale chiave. Assicurarsi di chiudere tutte le sessioni aperte.

Gestire la chiave pubblica (AWS CLI)

Puoi usare il AWS CLI per gestire la tua chiave pubblica SSH come parte del tuo profilo utente.

Per gestire la chiave pubblica

1. Da un terminale o da una finestra con emulatore Bash, eseguire il comando ssh-keygen per generare una coppia di chiavi SSH pubblica-privata sul computer locale. Puoi generare una chiave in qualsiasi formato consentito da Amazon EC2. Per informazioni sui formati accettabili, consulta Importazione della propria chiave pubblica su Amazon EC2. L'ideale sarebbe generare

una chiave SSH-2 RSA, in formato OpenSSH di 2048 bit di lunghezza. La chiave pubblica è memorizzata in un file con estensione .pub.

2. Per aggiungere o modificare la chiave pubblica SSH nel tuo profilo AWS CodeStar utente, esegui il update-user-profile comando con il `--ssh-public-key` parametro. Per esempio:

```
aws codestar update-user-profile --user-arn arn:aws:iam:111111111111:user/Jane_Doe
 --ssh-key-id EXAMPLE1
```

Questo comando restituisce un output simile al seguente:

```
{
 "createdTimestamp":1.491439687681E9,
 "displayName":"Jane Doe",
 "emailAddress":"jane.doe@example.com",
 "lastModifiedTimestamp":1.491442730598E9,
 "sshPublicKey":"EXAMPLE1",
 "userArn":"arn:aws:iam::111111111111:user/Jane_Doe"
}
```

Connettiti ad Amazon EC2 Instance con la tua chiave privata

Assicurati di aver creato una coppia di EC2 chiavi Amazon. Aggiungi la tua chiave pubblica al tuo profilo utente in AWS CodeStar. Per creare una coppia di chiavi, consulta Fase 4: creare una coppia di EC2 chiavi Amazon per AWS CodeStar i progetti. Per aggiungere la chiave pubblica al profilo utente, consultare le precedenti istruzioni di questa sezione.

Per connetterti a un'istanza Amazon EC2 Linux utilizzando la tua chiave privata

1. Con il progetto aperto nella AWS CodeStar console, nel riquadro di navigazione, scegli Progetto.
2. In Project Resources, scegli il link ARN nella riga in cui Type è Amazon EC2 e Name inizia con instance.
3. Nella EC2 console Amazon, scegli Connect.
4. Seguire le istruzioni nella finestra di dialogo Connect To Your Instance (Collegati all'istanza).

   Per il nome utente, usa`ec2-user`. Inserendo il nome utente sbagliato, non è possibile connettersi all'istanza.

Per ulteriori informazioni, consulta le seguenti risorse nella Amazon EC2 User Guide.

- Connessione all'istanza Linux tramite SSH
- Connessione all'istanza Linux da Windows tramite PuTTY
- Connessione alla tua istanza Linux tramite MindTerm

Sicurezza in AWS CodeStar

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 aspetto 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 esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili AWS CodeStar, consulta Servizi AWS nell'ambito del programma di conformitàAWS .
- 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 durante l'utilizzo AWS CodeStar. I seguenti argomenti mostrano come eseguire la configurazione AWS CodeStar per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere AWS CodeStar le tue risorse.

Quando crei politiche personalizzate e utilizzi i limiti di autorizzazione in AWS CodeStar, assicurati l'accesso con il minimo privilegio concedendo solo le autorizzazioni necessarie per eseguire un'attività e definendo le autorizzazioni per le risorse mirate. Per impedire ai membri di altri progetti di accedere alle risorse del progetto, concedi ai membri dell'organizzazione autorizzazioni separate per ogni progetto. AWS CodeStar È consigliabile creare un account di progetto per ogni membro e quindi assegnare a tale account un accesso basato sui ruoli.

Ad esempio, puoi utilizzare un servizio come AWS Control Tower with AWS Organizations per fornire account per ogni ruolo di sviluppatore all'interno di un DevOps gruppo. Quindi puoi assegnare le autorizzazioni a tali account. Le autorizzazioni complessive si applicano all'account, ma l'utente ha un accesso limitato alle risorse esterne al progetto.

Per ulteriori informazioni sulla gestione dell'accesso con privilegi minimi alle AWS risorse utilizzando una strategia multi-account, consulta la strategia multi-account AWS per la tua landing zone nella Control Tower User Guide.AWS

Argomenti

Protezione dei dati in AWS CodeStar

Il modello di responsabilità AWS condivisa modello di si applica alla protezione dei dati in AWS CodeStar. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutto il 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
- 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 CodeStar o Servizi AWS utilizzi 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.

Crittografia dei dati in AWS CodeStar

Per impostazione predefinita, AWS CodeStar crittografa le informazioni memorizzate sul progetto. Tutti i dati inattivi, ad eccezione dell'ID del progetto, sono crittografati, ad esempio il nome del progetto, la descrizione e le e-mail degli utenti. Evita di inserire informazioni personali nel tuo progetto IDs. AWS CodeStar inoltre, per impostazione predefinita, crittografa le informazioni in transito. Non è necessaria alcuna azione del cliente per la crittografia dei dati inattivi o per la crittografia dei dati in transito.

Identity and Access Management per AWS CodeStar

AWS Identity and Access Management (IAM) è un software 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 le risorse AWS. CodeStar IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Risoluzione dei problemi di AWS CodeStar Identity and Access

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in AWS CodeStar.

Utente del servizio: se utilizzi il CodeStar servizio AWS per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più CodeStar funzionalità AWS 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 in AWS CodeStar, consultaRisoluzione dei problemi di AWS CodeStar Identity and Access.

Amministratore del servizio: se sei responsabile delle CodeStar risorse AWS della tua azienda, probabilmente hai pieno accesso ad AWS CodeStar. Spetta a te determinare a quali CodeStar funzionalità e risorse AWS 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 ulteriori informazioni su come la tua azienda può utilizzare IAM con AWS CodeStar, consultaCome CodeStar funziona AWS con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso ad AWS CodeStar. Per visualizzare esempi di policy AWS CodeStar basate sull'identità che puoi utilizzare in IAM, consulta. Esempi di policy CodeStar basate sull'identità di AWS

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 Console di gestione AWS 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 sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

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) in AWSnella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'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 Quando creare un utente IAM (invece di un ruolo) 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. Puoi assumere temporaneamente un ruolo IAM in Console di gestione AWS cambiando ruolo. 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 Creazione di un ruolo per un provider di identità di terza parte 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 operazioni. 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 Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella 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. È preferibile archiviare le 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 Usare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

Gestione dell'accesso tramite 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' Console di gestione AWS AWS CLI, dall'o dall' AWS API.

Policy basate sulle 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 azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM 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.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di

proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.

- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle policy nella IAM User Guide.

Come CodeStar funziona AWS con IAM

Prima di utilizzare IAM per gestire l'accesso ad AWS CodeStar, è necessario comprendere quali funzionalità IAM sono disponibili per l'uso con AWS CodeStar. Per avere una visione di alto livello di come AWS CodeStar e altri AWS servizi funzionano con IAM, consulta AWS Services That Work with IAM nella IAM User Guide.

Argomenti

- Policy AWS CodeStar basate sull'identità
- Policy AWS CodeStar basate sulle risorse
- Autorizzazione basata su CodeStar tag AWS
- Ruoli AWS CodeStar IAM
- Accesso utente IAM a AWS CodeStar
- Accesso utente federato a AWS CodeStar
- Utilizzo di credenziali temporanee con AWS CodeStar
- Ruoli collegati al servizio
- Ruoli dei servizi

Policy AWS CodeStar basate sull'identità

Con le policy basate sull'identità IAM, puoi specificare azioni e risorse consentite o negate e le condizioni in base alle quali le azioni sono consentite o negate. AWS CodeStar crea diverse politiche basate sull'identità per tuo conto, che consentono AWS CodeStar di creare e gestire risorse nell'ambito di un progetto. AWS CodeStar AWS CodeStar supporta 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.

Operazioni

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 azioni politiche in AWS CodeStar utilizzano il seguente prefisso prima dell'azione:`codestar:`. Per esempio, per consentire a un utente IAM specificato di modificare gli attributi di un AWS CodeStar progetto, come la descrizione del progetto, puoi utilizzare la seguente dichiarazione politica:

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar:UpdateProject"
      ],
      "Resource" : "arn:aws:codestar:us-east-2:project/my-first-projec"
    }
  ]
}
```

Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. AWS CodeStar definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

Per specificare più azioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

```
"Action": [
      "codestar:action1",
      "codestar:action2"
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `List`, includi la seguente azione:

```
"Action": "codestar:List*"
```

Per visualizzare un elenco di CodeStar azioni AWS, consulta Actions Defined by AWS CodeStar nella IAM User Guide.

Risorse

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 JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le operazioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

La risorsa AWS CodeStar del progetto ha il seguente ARN:

```
arn:aws:codestar:region:account:project/resource-specifier
```

Per ulteriori informazioni sul formato di ARNs, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces.

Ad esempio, quanto segue specifica il nome del AWS CodeStar progetto *my-first-projec* registrato sull' AWS account 111111111111 nella regione: AWS us-east-2

```
arn:aws:codestar:us-east-2:111111111111:project/my-first-projec
```

Quanto segue specifica qualsiasi AWS CodeStar progetto che inizia con il nome my-proj registrato sull' AWS account 111111111111 nella AWS Regione: us-east-2

```
arn:aws:codestar:us-east-2:111111111111:project/my-proj*
```

Alcune CodeStar azioni AWS, ad esempio quelle relative alla creazione di elenchi di progetti, non possono essere eseguite su una risorsa. In questi casi, è necessario utilizzare il carattere jolly (*).

```
"LisProjects": "*"
```

Per visualizzare un elenco dei tipi di CodeStar risorse AWS e relativi ARNs, consulta Resources Defined by AWS CodeStar nella IAM User Guide. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, consulta Actions Defined by AWS. CodeStar

Chiavi di condizione

AWS CodeStar non fornisce chiavi di condizione specifiche del servizio, ma supporta l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta AWS Global Condition Context Keys nella IAM User Guide.

Esempi

Per visualizzare esempi di policy CodeStar basate sull'identità di AWS, consulta. Esempi di policy CodeStar basate sull'identità di AWS

Policy AWS CodeStar basate sulle risorse

AWS CodeStar non supporta politiche basate sulle risorse.

Autorizzazione basata su CodeStar tag AWS

Puoi allegare tag ai CodeStar progetti AWS o passarli in una richiesta ad AWS CodeStar. Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy

utilizzando le chiavi di condizione `codestar:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. Per ulteriori informazioni sull'etichettatura CodeStar delle risorse AWS, consultathe section called “Utilizzo dei tag di progetto”.

Per visualizzare un esempio di politica basata sull'identità per limitare l'accesso a un AWS CodeStar progetto in base ai tag di quel progetto, consulta. Visualizzazione dei CodeStar progetti AWS in base ai tag

Ruoli AWS CodeStar IAM

Un ruolo IAM è un'entità nel tuo AWS account che dispone di autorizzazioni specifiche.

Puoi utilizzarlo AWS CodeStar come utente IAM, utente federato, utente root o ruolo presunto. Tutti i tipi di utenti con le autorizzazioni appropriate possono gestire le autorizzazioni di progetto relative alle proprie AWS risorse, ma AWS CodeStar gestiscono automaticamente le autorizzazioni del progetto per gli utenti IAM. Le politiche e i ruoli IAM concedono autorizzazioni e accesso a quell'utente in base al ruolo del progetto. Puoi utilizzare la console IAM per creare altre policy che AWS CodeStar assegnano altre autorizzazioni a un utente IAM.

Ad esempio, è possibile consentire a un utente di visualizzare ma non di modificare un progetto AWS CodeStar . In questo caso, aggiungi l'utente IAM a un AWS CodeStar progetto con il ruolo di spettatore. Ogni AWS CodeStar progetto ha una serie di politiche che ti aiutano a controllare l'accesso al progetto. Inoltre, puoi controllare a quali utenti hanno accesso AWS CodeStar.

AWS CodeStar l'accesso viene gestito in modo diverso per gli utenti IAM e gli utenti federati. Solo gli utenti IAM possono essere aggiunti ai team. Per concedere agli utenti IAM le autorizzazioni per i progetti, è possibile aggiungere l'utente al team del progetto e assegnargli un ruolo. Per concedere agli utenti federati le autorizzazioni per i progetti, alleghi manualmente la politica gestita del ruolo di AWS CodeStar progetto al ruolo dell'utente federato.

Questa tabella riepiloga gli strumenti disponibili per ogni tipo di accesso.

Caratteristica delle autorizzazioni	Utente IAM	Utente federato	Utente root
Gestione delle chiavi SSH per l'accesso remoto per progetti Amazon EC2 ed Elastic Beanstalk	✓		
AWS CodeCommit accesso SSH	✓		

Caratteristica delle autorizzazioni	Utente IAM	Utente federato	Utente root
Autorizzazioni utente IAM gestite da AWS CodeStar	✓		
Autorizzazioni del progetto gestite manualmente		✓	✓
Gli utenti possono essere aggiunti al progetto come membri del team	✓		

Accesso utente IAM a AWS CodeStar

Quando aggiungi un utente IAM a un progetto e scegli un ruolo per l'utente, AWS CodeStar applica automaticamente la policy appropriata all'utente IAM. Per gli utenti IAM, non è necessario allegare o gestire direttamente le policy o le autorizzazioni in IAM. Per informazioni sull'aggiunta di un utente IAM a un AWS CodeStar progetto, consultaAggiungere membri del team a un AWS CodeStar progetto . Per informazioni sulla rimozione di un utente IAM da un AWS CodeStar progetto, consultaRimuovere membri del team da un AWS CodeStar progetto .

Allega una politica in linea a un utente IAM

Quando aggiungi un utente a un progetto, allega AWS CodeStar automaticamente la politica gestita per il progetto che corrisponde al ruolo dell'utente. Non dovresti allegare manualmente una policy AWS CodeStar gestita per un progetto a un utente IAM. Ad eccezione di`AWSCodeStarFullAccess`, sconsigliamo di allegare policy che modificano le autorizzazioni di un utente IAM in un AWS CodeStar progetto. Se decidi di creare e allegare le tue policy, consulta Aggiungere e rimuovere le autorizzazioni di identità IAM nella Guida per l'utente IAM.

Accesso utente federato a AWS CodeStar

Invece di creare un utente IAM o utilizzare l'utente root, puoi utilizzare le identità utente di AWS Directory Service, la tua directory utenti aziendale, un provider di identità web o gli utenti IAM che assumono ruoli. Questi sono noti come utenti federati.

Concedi agli utenti federati l'accesso al tuo AWS CodeStar progetto allegando manualmente le politiche gestite descritte in Politiche e autorizzazioni a AWS CodeStar livello di progetto al ruolo IAM dell'utente. Alleghi la politica del proprietario, del collaboratore o del visualizzatore dopo aver AWS CodeStar creato le risorse del progetto e i ruoli IAM.

Prerequisiti:

- È necessario impostare un provider di identità. Ad esempio, puoi configurare un provider di identità SAML e impostare AWS l'autenticazione tramite il provider. Per ulteriori informazioni sull'impostazione di un provider di identità, consulta Creazione di provider di identità IAM. Per ulteriori informazioni sulla federazione SAML, consulta la pagina sulla federazione basata su SAML 2.0.
- Devi aver creato un ruolo per un utente federato da assumere quando è richiesto l'accesso tramite un provider di identità. Una policy di fiducia STS deve essere collegata al ruolo che consente agli utenti federati di assumere quel ruolo. Per ulteriori informazioni, consulta la sezione relativa agli utenti federati e ruoli nella guida per l'utente IAM.
- È necessario aver creato il AWS CodeStar progetto e conoscere l'ID del progetto.

Per ulteriori informazioni sulla creazione di un ruolo per provider di identità, consulta la pagina sulla creazione di un ruolo per un provider di identità di terze parti (federazione).

Allega la politica AWSCode StarFullAccess gestita al ruolo dell'utente federato

Concedi a un utente federato le autorizzazioni necessarie per creare un progetto collegando la policy gestita `AWSCodeStarFullAccess`. Per eseguire questi passaggi, è necessario aver effettuato l'accesso alla console come utente root, utente amministratore dell'account oppure utente IAM o utente federato con la policy `AdministratorAccess` gestita associata o equivalente.

> **Note**
>
> Dopo aver creato il progetto, le autorizzazioni del progetto proprietario non vengono applicate automaticamente. Utilizzando un ruolo con autorizzazioni amministrative per l'account, collega la policy gestita dal proprietario, come descritto in Allega la politica AWS CodeStar Viewer/Contributor/Owner gestita del tuo progetto al ruolo dell'utente federato.

1. Aprire la console IAM. Nel riquadro di navigazione, scegli Policy.
2. Inserisci `AWSCodeStarFullAccess` nel campo di ricerca. Viene visualizzato il nome della policy, con un tipo di policy AWS gestita. È possibile espandere la policy per visualizzare le autorizzazioni nella dichiarazione della policy.
3. Seleziona il pallino accanto alla policy e quindi, in Policy actions (Operazioni policy), seleziona Attach (Collega).

4. Nella pagina Summary (Riepilogo), seleziona la scheda Attached entities (Entità collegate). Scegli Collega.
5. Nella pagina Attach Policy (Collega policy), filtra il ruolo dell'utente federato nel campo di ricerca. Seleziona la casella accanto al nome del ruolo e quindi seleziona Attach policy (Collega policy). Nella scheda Attached entities (Collega entità) viene visualizzato il nuovo collegamento.

Allega la politica AWS CodeStar Viewer/Contributor/Owner gestita del tuo progetto al ruolo dell'utente federato

Concedere agli utenti federati l'accesso al progetto collegando la policy gestita dal proprietario, dal collaboratore o dal visualizzatore appropriata al ruolo dell'utente. La policy gestita offre il livello di autorizzazioni appropriato. A differenza degli utenti IAM, devi collegare e scollegare manualmente le policy gestite per gli utenti federati. Ciò equivale ad assegnare le autorizzazioni del progetto ai membri del team in. AWS CodeStar Per eseguire questi passaggi, devi aver effettuato l'accesso alla console come utente root, utente amministratore dell'account oppure utente IAM o utente federato con la policy `AdministratorAccess` gestita associata o equivalente.

Prerequisiti:

- È necessario aver creato un ruolo o disporre di un ruolo esistente assunto dall'utente federato.
- È necessario sapere quale livello di autorizzazioni si desidera concedere. Le policy gestite collegate ai ruoli del proprietario, collaboratore e visualizzatore forniscono autorizzazioni in base al ruolo per il progetto.
- Il AWS CodeStar progetto deve essere stato creato. La policy gestita non è disponibile in IAM fino alla creazione del progetto.

1. Aprire la console IAM. Nel riquadro di navigazione, scegli Policy.
2. Inserisci il tuo ID di progetto nel campo di ricerca. Viene visualizzato il nome della policy che si abbina al progetto, con un tipo di policy di Customer managed (Gestito dal cliente). È possibile espandere la policy per visualizzare le autorizzazioni nella dichiarazione della policy.
3. Seleziona una di queste policy gestite. Seleziona il pallino accanto alla policy e quindi, in Policy actions (Operazioni policy), seleziona Attach (Collega).
4. Nella pagina Summary (Riepilogo), seleziona la scheda Attached entities (Entità collegate). Scegli Collega.

5. Nella pagina Attach Policy (Collega policy), filtra il ruolo dell'utente federato nel campo di ricerca. Seleziona la casella accanto al nome del ruolo e quindi seleziona Attach policy (Collega policy). Nella scheda Attached entities (Collega entità) viene visualizzato il nuovo collegamento.

Scollega una policy AWS CodeStar gestita dal ruolo dell'utente federato

Prima di eliminare il AWS CodeStar progetto, è necessario scollegare manualmente tutte le politiche gestite associate al ruolo di un utente federato. Per eseguire questi passaggi, devi aver effettuato l'accesso alla console come utente root, utente amministratore dell'account oppure utente IAM o utente federato con la policy `AdministratorAccess` gestita associata o equivalente.

1. Aprire la console IAM. Nel riquadro di navigazione, scegli Policy.
2. Inserisci il tuo ID di progetto nel campo di ricerca.
3. Seleziona il pallino accanto alla policy e quindi, in Policy actions (Operazioni policy), seleziona Attach (Collega).
4. Nella pagina Summary (Riepilogo), seleziona la scheda Attached entities (Entità collegate).
5. Filtra il ruolo dell'utente federato nel campo di ricerca. Seleziona Scollega.

Allega una policy AWS Cloud9 gestita al ruolo dell'utente federato

Se utilizzi un ambiente di AWS Cloud9 sviluppo, concedi l'accesso agli utenti federati allegando la policy `AWSCloud9User` gestita al ruolo dell'utente. A differenza degli utenti IAM, devi collegare e scollegare manualmente le policy gestite per gli utenti federati. Per eseguire questi passaggi, devi aver effettuato l'accesso alla console come utente root, utente amministratore dell'account oppure utente IAM o utente federato con la policy `AdministratorAccess` gestita associata o equivalente.

Prerequisiti:

- È necessario aver creato un ruolo o disporre di un ruolo esistente assunto dall'utente federato.
- È necessario sapere quale livello di autorizzazioni si desidera concedere:
  - La policy gestita `AWSCloud9User` consente all'utente di:
    - Crea i propri ambienti di AWS Cloud9 sviluppo.
    - Ottieni le informazioni sugli ambienti.
    - Modifica le impostazioni per gli ambienti.
  - La policy gestita `AWSCloud9Administrator` consente all'utente di eseguire le seguenti azioni per sé o per gli altri:

- Crea ambienti.
- Ottieni informazioni sugli ambienti.
- Elimina gli ambienti.
- Modifica le impostazioni degli ambienti.

1. Aprire la console IAM. Nel riquadro di navigazione, scegli Policy.
2. Inserisci il nome della policy nel campo di ricerca. Viene visualizzata la policy gestita, con un tipo di policy AWS gestita. È possibile espandere la policy per visualizzare le autorizzazioni nella dichiarazione della policy.
3. Seleziona una di queste policy gestite. Seleziona il pallino accanto alla policy e quindi, in Policy actions (Operazioni policy), seleziona Attach (Collega).
4. Nella pagina Summary (Riepilogo), seleziona la scheda Attached entities (Entità collegate). Scegli Collega.
5. Nella pagina Attach Policy (Collega policy), filtra il ruolo dell'utente federato nel campo di ricerca. Scegli la casella accanto al nome del ruolo e quindi seleziona Attach policy (Collega policy). Nella scheda Attached entities (Collega entità) viene visualizzato il nuovo collegamento.

Scollegare una politica AWS Cloud9 gestita dal ruolo dell'utente federato

Se utilizzi un ambiente di AWS Cloud9 sviluppo, puoi rimuovere l'accesso di un utente federato ad esso scollegando la politica che concede l'accesso. Per eseguire questi passaggi, devi aver effettuato l'accesso alla console come utente root, utente amministratore dell'account oppure utente IAM o utente federato con la policy `AdministratorAccess` gestita associata o equivalente.

1. Aprire la console IAM. Nel riquadro di navigazione, scegli Policy.
2. Inserisci il nome del progetto nel campo di ricerca.
3. Seleziona il pallino accanto alla policy e quindi, in Policy actions (Operazioni policy), seleziona Attach (Collega).
4. Nella pagina Summary (Riepilogo), seleziona la scheda Attached entities (Entità collegate).
5. Filtra il ruolo dell'utente federato nel campo di ricerca. Seleziona Scollega.

Utilizzo di credenziali temporanee con AWS CodeStar

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. Puoi ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come AssumeRoleo. GetFederationToken

AWS CodeStar supporta l'uso di credenziali temporanee, ma la funzionalità dei membri del AWS CodeStar team non funziona per l'accesso federato. AWS CodeStar la funzionalità dei membri del team supporta solo l'aggiunta di un utente IAM come membro del team.

Ruoli collegati al servizio

I ruoli collegati ai AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore può visualizzare, ma non modificare le autorizzazioni dei ruoli collegati ai servizi.

AWS CodeStar non supporta ruoli collegati ai servizi.

Ruoli dei servizi

Questa caratteristica consente a un servizio di assumere un ruolo di servizio per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'azione per conto dell'utente. I ruoli dei servizi sono visualizzati nell'account IAM e sono di proprietà dell'account. Ciò significa che un amministratore può modificare le autorizzazioni per questo ruolo. Tuttavia, il farlo potrebbe pregiudicare la funzionalità del servizio.

AWS CodeStar supporta i ruoli di servizio. AWS CodeStar utilizza un ruolo di servizio quando crea e gestisce le risorse per il tuo progetto. aws-codestar-service-role Per ulteriori informazioni, consulta Roles Terms and Concepts nella IAM User Guide.

> **Important**
>
> È necessario essere registrati come utente amministratore di un o account radice per creare questo ruolo di servizio. Per ulteriori informazioni, consulta Solo accesso per la prima volta: le credenziali dell'utente root e Creazione del primo utente e gruppo di amministrazione nella Guida per l'utente IAM.

Questo ruolo viene creato per te la prima volta che crei un progetto in. AWS CodeStar Il ruolo di servizio agisce a nome di:

- Crea le risorse selezionate al momento della creazione di un progetto.
- Visualizza le informazioni su tali risorse nella dashboard AWS CodeStar del progetto.

Inoltre, agisce a tuo nome quando si gestiscono le risorse per un progetto. Per un esempio di questa dichiarazione di policy, consulta AWSCodeStarServiceRole Politica.

Inoltre, AWS CodeStar crea diversi ruoli di servizio specifici del progetto, a seconda del tipo di progetto. CloudFormation e i ruoli della toolchain vengono creati per ogni tipo di progetto.

- CloudFormation i ruoli AWS CodeStar consentono di accedere CloudFormation per creare e modificare gli stack del AWS CodeStar progetto.
- I ruoli della toolchain consentono AWS CodeStar di accedere ad altri AWS servizi per creare e modificare risorse per il AWS CodeStar progetto.

AWS CodeStar Politiche e autorizzazioni a livello di progetto

Quando crei un progetto, AWS CodeStar crea i ruoli e le policy IAM necessari per gestire le risorse del progetto. Le policy possono essere suddivise in tre categorie:

- Policy IAM per i membri del team di progetto.
- Policy IAM per i ruoli di dipendente.
- Policy IAM per un ruolo di esecuzione di runtime.

Policy IAM per i membri del team

Quando crei un progetto, AWS CodeStar crea tre politiche gestite dal cliente per l'accesso al progetto da parte del proprietario, del collaboratore e dello spettatore. Tutti i AWS CodeStar progetti contengono politiche IAM per questi tre livelli di accesso. Questi livelli di accesso sono specifici del progetto e definiti da una policy gestita da IAM con un nome standard, *`project-id`* dov'è l'ID del AWS CodeStar progetto (ad esempio,*`my-first-projec`*):

- `CodeStar_`*`project-id`*`_Owner`
- `CodeStar_`*`project-id`*`_Contributor`

- `CodeStar_project-id_Viewer`

> **Important**
>
> Queste politiche sono soggette a modifiche entro. AWS CodeStar Non devono essere modificate manualmente. Se desideri aggiungere o modificare le autorizzazioni, allega politiche aggiuntive all'utente IAM.

Quando aggiungi i membri del team (utenti IAM) al progetto e selezioni i loro livelli di accesso, la relativa policy viene collegata all'utente IAM, assicurando che questi abbia l'insieme corretto di autorizzazioni per agire sulle risorse del progetto. Nella maggior parte dei casi, non è necessario allegare o gestire direttamente le policy o le autorizzazioni in IAM. Non è consigliabile allegare manualmente una policy del livello di AWS CodeStar accesso a un utente IAM. Se assolutamente necessario, come supplemento a una policy sul livello di AWS CodeStar accesso, puoi creare policy gestite o in linea personalizzate per applicare il tuo livello di autorizzazioni a un utente IAM.

Le policy hanno un ambito rigidamente definito per risorse del progetto e azioni specifiche. Man mano che vengono aggiunte nuove risorse allo stack dell'infrastruttura, AWS CodeStar tenta di aggiornare le politiche dei membri del team per includere le autorizzazioni di accesso alla nuova risorsa, se si tratta di uno dei tipi di risorse supportati.

> **Note**
>
> Le politiche per i livelli di accesso in un AWS CodeStar progetto si applicano solo a quel progetto. Questo aiuta a garantire che gli utenti possano vedere e interagire solo con i AWS CodeStar progetti per i quali dispongono delle autorizzazioni, al livello determinato dal loro ruolo. Solo agli utenti che creano AWS CodeStar progetti deve essere applicata una politica che consenta l'accesso a tutte le AWS CodeStar risorse, indipendentemente dal progetto.

Tutte le politiche relative AWS CodeStar ai livelli di accesso variano a seconda delle AWS risorse associate al progetto a cui sono associati i livelli di accesso. A differenza di altri servizi AWS , queste policy sono personalizzate quando il progetto viene creato e aggiornato come modifica delle risorse del progetto. Pertanto, non vi è alcuna policy gestita dal proprietario canonico, dal collaboratore o dal visualizzatore.

AWS CodeStar Politica relativa al ruolo del proprietario

La politica gestita `CodeStar_project-id_Owner` dal cliente consente a un utente di eseguire tutte le azioni AWS CodeStar del progetto senza restrizioni. Questa è l'unica policy che consente a un utente di aggiungere o rimuovere i membri del team. I contenuti della policy variano a seconda delle risorse associate al progetto. Consulta AWS CodeStar Politica sul ruolo del proprietario per un esempio.

Un utente IAM con questa policy può eseguire tutte AWS CodeStar le azioni del progetto, ma a differenza di un utente IAM con la `AWSCodeStarFullAccess` policy, non può creare progetti. L'`codestar:*`autorizzazione è limitata a una risorsa specifica (il AWS CodeStar progetto associato a quell'ID di progetto).

AWS CodeStar Politica sul ruolo del collaboratore

La policy gestita dal cliente `CodeStar_project-id_Contributor` consente a un utente di contribuire al progetto e di modificare il pannello di controllo del progetto, ma non consente a un utente di aggiungere o rimuovere i membri del team. I contenuti della policy variano a seconda delle risorse associate al progetto. Consulta Policy del ruolo collaboratore AWS CodeStar per un esempio.

AWS CodeStar Politica sul ruolo del visualizzatore

La policy gestita dal cliente `CodeStar_project-id_Viewer` consente a un utente di visualizzare un progetto in AWS CodeStar, ma non di cambiare le risorse o di aggiungere o rimuovere i membri del team. I contenuti della policy variano a seconda delle risorse associate al progetto. Consulta AWS CodeStar Politica del ruolo del visualizzatore per un esempio.

Policy IAM per ruoli dipendente

Se crei il tuo AWS CodeStar progetto dopo il 6 dicembre 2018 PDT, AWS CodeStar crea due ruoli di lavoro `CodeStar-project-id-ToolChain` e`CodeStar-project-id-CloudFormation`. Un ruolo di lavoratore è un ruolo IAM specifico del progetto che viene AWS CodeStar creato per essere trasferito a un servizio. Concede le autorizzazioni in modo che il servizio possa creare risorse ed eseguire azioni nel contesto del progetto. AWS CodeStar Il ruolo di toolchain worker ha una relazione di fiducia stabilita con servizi di toolchain come, e CodeBuild. CodeDeploy CodePipeline Ai membri del team di progetto (proprietari e collaboratori) viene garantito l'accesso per passare il ruolo di dipendente ai servizi downstream affidabili. Per un esempio di istruzione della policy inline per questo ruolo, consulta AWS CodeStar Politica sul ruolo dei lavoratori di Toolchain (dopo il 6 dicembre 2018 PDT).

Il ruolo di CloudFormation lavoratore include le autorizzazioni per risorse selezionate supportate da CloudFormation, nonché le autorizzazioni per creare utenti, ruoli e policy IAM nello stack di applicazioni. Ha inoltre instaurato un rapporto di fiducia con. CloudFormation Per mitigare i rischi di escalation dei privilegi e di azioni distruttive, la policy relativa ai CloudFormation ruoli include una condizione che richiede il limite di autorizzazioni specifico del progetto per ogni entità IAM (utente o ruolo) creata nello stack dell'infrastruttura. Per un esempio di istruzione della policy inline per questo ruolo, consulta CloudFormation Politica sul ruolo dei lavoratori.

Per CodeStar i progetti AWS creati prima del 6 dicembre 2018, PDT AWS CodeStar crea ruoli di lavoro individuali per risorse della toolchain come CodePipeline CodeBuild, ed CloudWatch Events, e crea anche un ruolo di lavoratore CloudFormation che supporta un set limitato di risorse. Ognuno di questi ruoli ha una relazione di trust stabilita con il relativo servizio. Ai membri del team di progetto (proprietari e collaboratori) e ad alcuni degli altri ruoli dipendente viene garantito l'accesso per passare il ruolo ai servizi downstream affidabili. Le autorizzazioni per i ruoli dipendente sono definite in una policy inline con un insieme base di azioni eseguibili dal ruolo su un insieme di risorse del progetto. Queste autorizzazioni sono statiche. Includono le autorizzazioni alle risorse comprese nel progetto, ma non sono aggiornate in caso di aggiunta di nuove risorse. Per esempi di queste istruzioni della policy, consulta:

- CloudFormation Policy sul ruolo dei lavoratori (prima del 6 dicembre 2018 PDT)
- AWS CodePipeline Policy sul ruolo dei lavoratori (prima del 6 dicembre 2018 PDT)
- AWS CodeBuild Policy sul ruolo dei lavoratori (prima del 6 dicembre 2018 PDT)
- Policy sul ruolo dei lavoratori di Amazon CloudWatch Events (prima del 6 dicembre 2018 PDT)

Policy IAM per il ruolo di esecuzione

Per i progetti creati dopo il 6 dicembre 2018 PDT, AWS CodeStar crea un ruolo di esecuzione generico per il progetto di esempio nello stack di applicazioni. Il ruolo dispone di un numero limitato di risorse del progetto con la policy del limite di autorizzazioni. Man mano che espandi il progetto di esempio, puoi creare ruoli IAM aggiuntivi e la CloudFormation politica dei ruoli richiede che tali ruoli siano delimitati utilizzando il limite di autorizzazione per evitare l'aumento dei privilegi. Per ulteriori informazioni, consulta Aggiunta di un ruolo IAM a un progetto.

Per i progetti Lambda creati prima del 6 dicembre 2018 PDT, crea AWS CodeStar un ruolo di esecuzione Lambda a cui è associata una policy in linea con le autorizzazioni per agire sulle risorse nello stack del progetto. AWS SAM Man mano che vengono aggiunte nuove risorse al modello

SAM, AWS CodeStar tenta di aggiornare la politica del ruolo di esecuzione Lambda per includere le autorizzazioni per la nuova risorsa se si tratta di uno dei tipi di risorsa supportati.

Limite delle autorizzazioni IAM

Dopo il PDT del 6 dicembre 2018, quando crei un progetto, AWS CodeStar crea una policy gestita dai clienti e assegna tale policy come limite delle autorizzazioni IAM ai ruoli IAM nel progetto. AWS CodeStar richiede che tutte le entità IAM create nello stack di applicazioni abbiano un limite di autorizzazioni. Un limite di autorizzazioni controlla il numero massimo di autorizzazioni che il ruolo può avere, ma non riconosce al ruolo alcuna autorizzazione. Le policy di autorizzazione definiscono le autorizzazioni per il ruolo. Pertanto non contano le autorizzazioni ulteriori aggiunte a un ruolo: chiunque utilizzi il ruolo non potrà eseguire altre azioni rispetto a quelle incluse nel limite delle autorizzazioni. Per informazioni su come vengono valutate le policy e i limiti delle autorizzazioni, consulta Policy Evaluation Logic nella IAM User Guide.

AWS CodeStar utilizza un limite di autorizzazioni specifico del progetto per impedire l'escalation dei privilegi verso risorse esterne al progetto. Il limite delle CodeStar autorizzazioni AWS include ARNs le risorse del progetto. Per un esempio di questa dichiarazione di policy, consulta Politica sui limiti CodeStar delle autorizzazioni di AWS.

La CodeStar trasformazione AWS aggiorna questa policy quando aggiungi o rimuovi una risorsa supportata dal progetto tramite lo stack dell'applicazione (`template.yml`).

Aggiunta di un limite di autorizzazioni IAM ai progetti esistenti

Se hai un CodeStar progetto AWS creato prima del 6 dicembre 2018 PDT, devi aggiungere manualmente un limite di autorizzazione ai ruoli IAM nel progetto. Come best practice, consigliamo di utilizzare un limite specifico per il progetto che includa solo le risorse nel progetto per impedire l'escalation dei privilegi alle risorse al di fuori del progetto. Segui questi passaggi per utilizzare il limite delle autorizzazioni CodeStar gestite da AWS che viene aggiornato man mano che il progetto si evolve.

1. Accedi alla CloudFormation console e individua il modello per lo stack di toolchain nel tuo progetto. Questo modello è denominato `awscodestar-`*`project-id`*.
2. Scegliere il modello, scegliere Actions (Operazioni) e quindi scegliere View/Edit template in Designer (Visualizza/Modifica il modello in Designer).
3. Individuare la sezione `Resources` e includere il seguente frammento di codice nella parte superiore.

```
 PermissionsBoundaryPolicy:
   Description: Creating an IAM managed policy for defining the permissions boundary
for an AWS CodeStar project
   Type: AWS::IAM::ManagedPolicy
   Properties:
     ManagedPolicyName: !Sub 'CodeStar_${ProjectId }_PermissionsBoundary'
     Description: 'IAM policy to define the permissions boundary for IAM entities
created in an AWS CodeStar project'
     PolicyDocument:
       Version: '2012-10-17'
       Statement:
       - Sid: '1'
         Effect: Allow
         Action: ['*']
         Resource:
           - !Sub 'arn:${AWS::Partition}:cloudformation:${AWS::Region}:
${AWS::AccountId}:stack/awscodestar-${ProjectId}-*'
```

Potresti aver bisogno di autorizzazioni IAM aggiuntive per aggiornare lo stack dalla console. CloudFormation

4. (Facoltativo) Se desideri creare ruoli IAM specifici per l'applicazione, completa questo passaggio. Dalla console IAM, aggiorna la policy in linea allegata al CloudFormation ruolo per il tuo progetto in modo da includere il seguente frammento. Potresti aver bisogno di risorse IAM aggiuntive per aggiornare la policy.

```
      {
           "Action": [
               "iam:PassRole"
           ],
           "Resource": "arn:aws:iam::{AccountId}:role/CodeStar-{ProjectId}*",
           "Effect": "Allow"
       },
       {
           "Action": [
               "iam:CreateServiceLinkedRole",
               "iam:GetRole",
               "iam:DeleteRole",
               "iam:DeleteUser"
```

```
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:AttachRolePolicy",
                "iam:AttachUserPolicy",
                "iam:CreateRole",
                "iam:CreateUser",
                "iam:DeleteRolePolicy",
                "iam:DeleteUserPolicy",
                "iam:DetachUserPolicy",
                "iam:DetachRolePolicy",
                "iam:PutUserPermissionsBoundary",
                "iam:PutRolePermissionsBoundary"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PermissionsBoundary": "arn:aws:iam::{AccountId}:policy/
CodeStar_{ProjectId}_PermissionsBoundary"
                }
            },
            "Effect": "Allow"
        }
```

5. Immetti una modifica nella pipeline del tuo progetto in modo che AWS CodeStar aggiorni il limite delle autorizzazioni con le autorizzazioni appropriate.

Per ulteriori informazioni, consulta Aggiunta di un ruolo IAM a un progetto.

Esempi di policy CodeStar basate sull'identità di AWS

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificare CodeStar risorse AWS. Inoltre, non possono eseguire attività utilizzando l' AWS API Console di gestione AWS AWS CLI, o. Un amministratore deve creare le policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi allegare queste policy a utenti o IAM che richiedono tali autorizzazioni.

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.

Argomenti

Best practice delle policy

Le policy basate sull'identità determinano se qualcuno può creare, accedere o eliminare CodeStar risorse AWS nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

AWSCodeStarServiceRole Politica

La `aws-codestar-service-role` policy è allegata al ruolo di servizio che consente di AWS CodeStar eseguire azioni con altri servizi. La prima volta che accedi AWS CodeStar, crei il ruolo di

servizio. Devi crearlo solo una volta. La policy viene automaticamente collegata al ruolo del servizio dopo averlo creato.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ProjectEventRules",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets",
                "events:RemoveTargets",
                "events:PutRule",
                "events:DeleteRule",
                "events:DescribeRule"
            ],
            "Resource": [
                "arn:aws:events:*:*:rule/awscodestar-*"
            ]
        },
        {
            "Sid": "ProjectStack",
            "Effect": "Allow",
            "Action": [
                "cloudformation:*Stack*",
                "cloudformation:CreateChangeSet",
                "cloudformation:ExecuteChangeSet",
                "cloudformation:DeleteChangeSet",
                "cloudformation:GetTemplate"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/awscodestar-*",
                "arn:aws:cloudformation:*:*:stack/awseb-*",
                "arn:aws:cloudformation:*:*:stack/aws-cloud9-*",
                "arn:aws:cloudformation:*:aws:transform/CodeStar*"
            ]
        },
        {
            "Sid": "ProjectStackTemplate",
            "Effect": "Allow",
            "Action": [
                "cloudformation:GetTemplateSummary",
                "cloudformation:DescribeChangeSet"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "ProjectQuickstarts",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::awscodestar-*/*"
            ]
        },
        {
            "Sid": "ProjectS3Buckets",
            "Effect": "Allow",
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "arn:aws:s3:::aws-codestar-*",
                "arn:aws:s3:::elasticbeanstalk-*"
            ]
        },
        {
            "Sid": "ProjectServices",
            "Effect": "Allow",
            "Action": [
                "codestar:*",
                "codecommit:*",
                "codepipeline:*",
                "codedeploy:*",
                "codebuild:*",
                "autoscaling:*",
                "cloudwatch:Put*",
                "ec2:*",
                "elasticbeanstalk:*",
                "elasticloadbalancing:*",
                "iam:ListRoles",
                "logs:*",
                "sns:*",
                "cloud9:CreateEnvironmentEC2",
                "cloud9:DeleteEnvironment",
                "cloud9:DescribeEnvironment*",
```

```
                "cloud9:ListEnvironments"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ProjectWorkerRoles",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:PassRole",
                "iam:GetRolePolicy",
                "iam:PutRolePolicy",
                "iam:SetDefaultPolicyVersion",
                "iam:CreatePolicy",
                "iam:DeletePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:CreateInstanceProfile",
                "iam:DeleteInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile"
            ],
            "Resource": [
                "arn:aws:iam::*:role/CodeStarWorker*",
                "arn:aws:iam::*:policy/CodeStarWorker*",
                "arn:aws:iam::*:instance-profile/awscodestar-*"
            ]
        },
        {
            "Sid": "ProjectTeamMembers",
            "Effect": "Allow",
            "Action": [
                "iam:AttachUserPolicy",
                "iam:DetachUserPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "ArnEquals": {
                    "iam:PolicyArn": [
                        "arn:aws:iam::*:policy/CodeStar_*"
                    ]
```

```
                }
            }
        },
        {
            "Sid": "ProjectRoles",
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:DeletePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:ListEntitiesForPolicy",
                "iam:ListPolicyVersions",
                "iam:GetPolicy",
                "iam:GetPolicyVersion"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/CodeStar_*"
            ]
        },
        {
            "Sid": "InspectServiceRole",
            "Effect": "Allow",
            "Action": [
                "iam:ListAttachedRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-codestar-service-role",
                "arn:aws:iam::*:role/service-role/aws-codestar-service-role"
            ]
        },
        {
            "Sid": "IAMLinkRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "cloud9.amazonaws.com"
                }
            }
        },
```

```
        {
            "Sid": "DescribeConfigRuleForARN",
            "Effect": "Allow",
            "Action": [
                "config:DescribeConfigRules"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "ProjectCodeStarConnections",
            "Effect": "Allow",
            "Action": [
                "codestar-connections:UseConnection",
                "codestar-connections:GetConnection"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ProjectCodeStarConnectionsPassConnections",
            "Effect": "Allow",
            "Action": "codestar-connections:PassConnection",
            "Resource": "*",
            "Condition": {
                "StringEqualsIfExists": {
                    "codestar-connections:PassedToService":
 "codepipeline.amazonaws.com"
                }
            }
        }
    ]
}
```

AWSCodeStarFullAccess Politica

Nelle Configurazione AWS CodeStar istruzioni, hai allegato una policy denominata `AWSCodeStarFullAccess` al tuo utente IAM. Questa informativa sulla politica consente all'utente di eseguire tutte le azioni disponibili AWS CodeStar con tutte le AWS CodeStar risorse disponibili associate all' AWS account. Ciò include la creazione e l'eliminazione di progetti. L'esempio seguente è un frammento di una policy `AWSCodeStarFullAccess` rappresentativa. La politica effettiva varia a seconda del modello selezionato quando si avvia un nuovo AWS CodeStar progetto.

AWS CloudFormation richiede `cloudformation::ListStacks` l'autorizzazione per le chiamate `cloudformation::DescribeStacks` senza uno stack di destinazione.

Dettagli dell'autorizzazione

Questa policy include le autorizzazioni per effettuare le seguenti operazioni:

- `ec2`—Recupera informazioni sulle EC2 istanze per creare un progetto. AWS CodeStar
- `cloud9`—Recupera informazioni sugli ambienti. AWS Command Line Interface
- `cloudformation`—Recupera informazioni sugli stack di progetti. AWS CodeStar
- `codestar`—Esegue azioni all'interno di un progetto. AWS CodeStar

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CodeStarEC2",
      "Effect": "Allow",
      "Action": [
        "codestar:*",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "cloud9:DescribeEnvironment*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CodeStarCF",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStack*",
        "cloudformation:ListStacks*",
        "cloudformation:GetTemplateSummary"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*"
      ]
    }
  ]
}
```

È possibile che non si desideri offrire a tutti gli utenti questo livello di accesso. È invece possibile aggiungere autorizzazioni a livello di progetto utilizzando i ruoli di progetto gestiti da. AWS CodeStar I ruoli garantiscono livelli specifici di accesso ai AWS CodeStar progetti e sono denominati come segue:

- Owner
- Collaboratore
- Visualizzatore

AWS CodeStar Politica sul ruolo del proprietario

La policy CodeStar del ruolo del proprietario di AWS consente a un utente di eseguire tutte le azioni in un CodeStar progetto AWS senza restrizioni. AWS CodeStar applica la `CodeStar_`*`project-id`*`_Owner` policy ai membri del team di progetto con il livello di accesso proprietario.

```
...
{
  "Effect": "Allow",
  "Action": [
    ...
    "codestar:*",
    ...
  ],
  "Resource": [
    "arn:aws:codestar:us-east-2:111111111111:project/project-id",
    "arn:aws:iam::account-id:policy/CodeStar_project-id_Owner"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "codestar:DescribeUserProfile",
    "codestar:ListProjects",
    "codestar:ListUserProfiles",
    "codestar:VerifyServiceRole",
    ...
  ],
  "Resource": [
    "*"
  ]
},
```

```
{
  "Effect": "Allow",
  "Action": [
    "codestar:*UserProfile",
    ...
  ],
  "Resource": [
    "arn:aws:iam::account-id:user/user-name"
  ]
}
...
```

Policy del ruolo collaboratore AWS CodeStar

La policy del ruolo di CodeStar contributore di AWS consente a un utente di contribuire al progetto e modificare la dashboard del progetto.AWS CodeStar applica la `CodeStar_project-id_Contributor` policy ai membri del team di progetto con il livello di accesso come contributore. Gli utenti con l'accesso di collaboratore possono contribuire al progetto e cambiare il pannello di controllo del progetto, ma non possono aggiungere o rimuovere membri del team.

```
...
{
  "Effect": "Allow",
  "Action": [
    ...
    "codestar:Describe*",
    "codestar:Get*",
    "codestar:List*",
    "codestar:PutExtendedAccess",
    ...
  ],
  "Resource": [
    "arn:aws:codestar:us-east-2:111111111111:project/project-id",
    "arn:aws:iam::account-id:policy/CodeStar_project-id_Contributor"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "codestar:DescribeUserProfile",
    "codestar:ListProjects",
    "codestar:ListUserProfiles",
    "codestar:VerifyServiceRole",
```

```
    ...
  ],
  "Resource": [
    "*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "codestar:*UserProfile",
    ...
  ],
  "Resource": [
    "arn:aws:iam::account-id:user/user-name"
  ]
}
...
```

AWS CodeStar Politica del ruolo del visualizzatore

La policy del ruolo del CodeStar visualizzatore di AWS consente a un utente di visualizzare un progetto in AWS CodeStar. AWS CodeStar applica la `CodeStar_project-id_Viewer` policy ai membri del team di progetto con il livello di accesso del visualizzatore. Gli utenti con accesso come visualizzatore possono visualizzare un progetto in AWS CodeStar, ma non modificarne le risorse o aggiungere o rimuovere membri del team.

```
...
{
  "Effect": "Allow",
  "Action": [
    ...
    "codestar:Describe*",
    "codestar:Get*",
    "codestar:List*",
    ...
  ],
  "Resource": [
    "arn:aws:codestar:us-east-2:111111111111:project/project-id",
    "arn:aws:iam::account-id:policy/CodeStar_project-id_Viewer"
  ]
},
{
  "Effect": "Allow",
```

```
  "Action": [
    "codestar:DescribeUserProfile",
    "codestar:ListProjects",
    "codestar:ListUserProfiles",
    "codestar:VerifyServiceRole",
    ...
  ],
  "Resource": [
    "*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "codestar:*UserProfile",
    ...
  ],
  "Resource": [
    "arn:aws:iam::account-id:user/user-name"
  ]
}
...
```

AWS CodeStar Politica sul ruolo dei lavoratori di Toolchain (dopo il 6 dicembre 2018 PDT)

Per AWS CodeStar i progetti creati dopo il 6 dicembre 2018 PDT, AWS CodeStar crea una policy in linea per un ruolo di lavoratore che crea risorse per il progetto in altri AWS servizi. Il contenuto della policy dipende dal tipo di progetto che stai creando. Di seguito ne viene riportato un esempio. Per ulteriori informazioni, consulta Policy IAM per ruoli dipendente.

```
{
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetBucketVersioning",
        "s3:PutObject*",
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
```

```
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:UploadArchive",
        "codebuild:StartBuild",
        "codebuild:BatchGetBuilds",
        "codebuild:StopBuild",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "codepipeline:StartPipelineExecution",
        "lambda:ListFunctions",
        "lambda:InvokeFunction",
        "sns:Publish"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
```

```
  ]
}
```

CloudFormation Politica sul ruolo dei lavoratori

Per AWS CodeStar i progetti creati dopo il 6 dicembre 2018 PDT, AWS CodeStar crea una policy in linea per un ruolo di lavoratore che crea CloudFormation risorse per il tuo progetto CodeStar AWS. Il contenuto della policy dipende dal tipo di risorse necessarie per il tuo progetto. Di seguito ne viene riportato un esempio. Per ulteriori informazioni, consulta Policy IAM per ruoli dipendente.

```
{
{
    "Statement": [
        {
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::aws-codestar-region-id-account-id-project-id",
                "arn:aws:s3:::aws-codestar-region-id-account-id-project-id/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "apigateway:DELETE",
                "apigateway:GET",
                "apigateway:PATCH",
                "apigateway:POST",
                "apigateway:PUT",
                "codedeploy:CreateApplication",
                "codedeploy:CreateDeployment",
                "codedeploy:CreateDeploymentConfig",
                "codedeploy:CreateDeploymentGroup",
                "codedeploy:DeleteApplication",
                "codedeploy:DeleteDeployment",
                "codedeploy:DeleteDeploymentConfig",
                "codedeploy:DeleteDeploymentGroup",
                "codedeploy:GetDeployment",
                "codedeploy:GetDeploymentConfig",
```

```
                "codedeploy:GetDeploymentGroup",
                "codedeploy:RegisterApplicationRevision",
                "codestar:SyncResources",
                "config:DeleteConfigRule",
                "config:DescribeConfigRules",
                "config:ListTagsForResource",
                "config:PutConfigRule",
                "config:TagResource",
                "config:UntagResource",
                "dynamodb:CreateTable",
                "dynamodb:DeleteTable",
                "dynamodb:DescribeContinuousBackups",
                "dynamodb:DescribeTable",
                "dynamodb:DescribeTimeToLive",
                "dynamodb:ListTagsOfResource",
                "dynamodb:TagResource",
                "dynamodb:UntagResource",
                "dynamodb:UpdateContinuousBackups",
                "dynamodb:UpdateTable",
                "dynamodb:UpdateTimeToLive",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AttachVolume",
                "ec2:CreateSecurityGroup",
                "ec2:createTags",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeInstances",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyInstanceCreditSpecification",
                "ec2:ModifyInstancePlacement",
                "ec2:MonitorInstances",
                "ec2:ReplaceIamInstanceProfileAssociation",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "events:DeleteRule",
                "events:DescribeRule",
                "events:ListTagsForResource",
                "events:PutRule",
                "events:PutTargets",
```

```
                "events:RemoveTargets",
                "events:TagResource",
                "events:UntagResource",
                "kinesis:AddTagsToStream",
                "kinesis:CreateStream",
                "kinesis:DecreaseStreamRetentionPeriod",
                "kinesis:DeleteStream",
                "kinesis:DescribeStream",
                "kinesis:IncreaseStreamRetentionPeriod",
                "kinesis:RemoveTagsFromStream",
                "kinesis:StartStreamEncryption",
                "kinesis:StopStreamEncryption",
                "kinesis:UpdateShardCount",
                "lambda:CreateAlias",
                "lambda:CreateFunction",
                "lambda:DeleteAlias",
                "lambda:DeleteFunction",
                "lambda:DeleteFunctionConcurrency",
                "lambda:GetFunction",
                "lambda:GetFunctionConfiguration",
                "lambda:ListTags",
                "lambda:ListVersionsByFunction",
                "lambda:PublishVersion",
                "lambda:PutFunctionConcurrency",
                "lambda:TagResource",
                "lambda:UntagResource",
                "lambda:UpdateAlias",
                "lambda:UpdateFunctionCode",
                "lambda:UpdateFunctionConfiguration",
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteBucketWebsite",
                "s3:PutAccelerateConfiguration",
                "s3:PutAnalyticsConfiguration",
                "s3:PutBucketAcl",
                "s3:PutBucketCORS",
                "s3:PutBucketLogging",
                "s3:PutBucketNotification",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutBucketVersioning",
                "s3:PutBucketWebsite",
                "s3:PutEncryptionConfiguration",
                "s3:PutInventoryConfiguration",
                "s3:PutLifecycleConfiguration",
```

```
                "s3:PutMetricsConfiguration",
                "s3:PutReplicationConfiguration",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListSubscriptionsByTopic",
                "sns:ListTopics",
                "sns:SetSubscriptionAttributes",
                "sns:Subscribe",
                "sns:Unsubscribe",
                "sqs:CreateQueue",
                "sqs:DeleteQueue",
                "sqs:GetQueueAttributes",
                "sqs:GetQueueUrl",
                "sqs:ListQueueTags",
                "sqs:TagQueue",
                "sqs:UntagQueue"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "lambda:AddPermission",
                "lambda:RemovePermission"
            ],
            "Resource": [
                "arn:aws:lambda:region-id:account-id:function:awscodestar-*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::account-id:role/CodeStar-project-id*"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "codedeploy.amazonaws.com"
```

```
                }
            },
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::account-id:role/CodeStarWorker-project-id-CodeDeploy"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudformation:CreateChangeSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:region-id:aws:transform/Serverless-2016-10-31",
                "arn:aws:cloudformation:region-id:aws:transform/CodeStar"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:GetRole",
                "iam:DeleteRole",
                "iam:DeleteUser"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringEquals": {
                    "iam:PermissionsBoundary": "arn:aws:iam::account-id:policy/
CodeStar_project-id_PermissionsBoundary"
                }
            },
            "Action": [
                "iam:AttachRolePolicy",
                "iam:AttachUserPolicy",
                "iam:CreateRole",
                "iam:CreateUser",
                "iam:DeleteRolePolicy",
                "iam:DeleteUserPolicy",
```

```
                "iam:DetachUserPolicy",
                "iam:DetachRolePolicy",
                "iam:PutUserPermissionsBoundary",
                "iam:PutRolePermissionsBoundary"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:CreateKey",
                "kms:CreateAlias",
                "kms:DeleteAlias",
                "kms:DisableKey",
                "kms:EnableKey",
                "kms:UpdateAlias",
                "kms:TagResource",
                "kms:UntagResource"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringEquals": {
                    "ssm:ResourceTag/awscodestar:projectArn":
 "arn:aws:codestar:project-id:account-id:project/project-id"
                }
            },
            "Action": [
                "ssm:GetParameter*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

CloudFormation Policy sul ruolo dei lavoratori (prima del 6 dicembre 2018 PDT)

Se il tuo CodeStar progetto AWS è stato creato prima del 6 dicembre 2018 PDT, AWS CodeStar ha creato una policy in linea per un ruolo di CloudFormation lavoratore. Di seguito è mostrato un esempio di istruzione della policy.

```
{
    "Statement": [
        {
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::aws-codestar-us-east-1-account-id-project-id-pipe",
                "arn:aws:s3:::aws-codestar-us-east-1-account-id-project-id-pipe/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "codestar:SyncResources",
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:AddPermission",
                "lambda:UpdateFunction",
                "lambda:UpdateFunctionCode",
                "lambda:GetFunction",
                "lambda:GetFunctionConfiguration",
                "lambda:UpdateFunctionConfiguration",
                "lambda:RemovePermission",
                "lambda:listTags",
                "lambda:TagResource",
                "lambda:UntagResource",
                "apigateway:*",
                "dynamodb:CreateTable",
                "dynamodb:DeleteTable",
                "dynamodb:DescribeTable",
                "kinesis:CreateStream",
                "kinesis:DeleteStream",
                "kinesis:DescribeStream",
                "sns:CreateTopic",
```

```
                "sns:DeleteTopic",
                "sns:ListTopics",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "config:DescribeConfigRules",
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "ec2:*",
                "autoscaling:*",
                "elasticloadbalancing:*",
                "elasticbeanstalk:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::account-id:role/CodeStarWorker-project-id-Lambda"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudformation:CreateChangeSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:us-east-1:aws:transform/Serverless-2016-10-31",
                "arn:aws:cloudformation:us-east-1:aws:transform/CodeStar"
            ],
            "Effect": "Allow"
        }
    ]
}
```

AWS CodePipeline Policy sul ruolo dei lavoratori (prima del 6 dicembre 2018 PDT)

Se il tuo CodeStar progetto AWS è stato creato prima del 6 dicembre 2018 PDT, AWS CodeStar ha creato una policy in linea per un ruolo di CodePipeline lavoratore. Di seguito è mostrato un esempio di istruzione della policy.

```
{
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:GetBucketVersioning",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-codestar-us-east-1-account-id-project-id-pipe",
                "arn:aws:s3:::aws-codestar-us-east-1-account-id-project-id-pipe/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "codecommit:CancelUploadArchive",
                "codecommit:GetBranch",
                "codecommit:GetCommit",
                "codecommit:GetUploadArchiveStatus",
                "codecommit:UploadArchive"
            ],
            "Resource": [
                "arn:aws:codecommit:us-east-1:account-id:project-id"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "codebuild:StartBuild",
                "codebuild:BatchGetBuilds",
                "codebuild:StopBuild"
            ],
            "Resource": [
                "arn:aws:codebuild:us-east-1:account-id:project/project-id"
            ],
```

```
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeChangeSet",
                "cloudformation:CreateChangeSet",
                "cloudformation:DeleteChangeSet",
                "cloudformation:ExecuteChangeSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:us-east-1:account-id:stack/awscodestar-project-
id-lambda/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::account-id:role/CodeStarWorker-project-id-CloudFormation"
            ],
            "Effect": "Allow"
        }
    ]
}
```

AWS CodeBuild Policy sul ruolo dei lavoratori (prima del 6 dicembre 2018 PDT)

Se il tuo CodeStar progetto AWS è stato creato prima del 6 dicembre 2018 PDT, AWS CodeStar ha creato una policy in linea per un ruolo di CodeBuild lavoratore. Di seguito è mostrato un esempio di istruzione della policy.

```
{
    "Statement": [
        {
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "*",
```

```
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::aws-codestar-us-east-1-account-id-project-id-pipe",
                "arn:aws:s3:::aws-codestar-us-east-1-account-id-project-id-pipe/*",
                "arn:aws:s3:::aws-codestar-us-east-1-account-id-project-id-app",
                "arn:aws:s3:::aws-codestar-us-east-1-account-id-project-id-app/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "codecommit:GitPull"
            ],
            "Resource": [
                "arn:aws:codecommit:us-east-1:account-id:project-id"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Encrypt",
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:account-id:alias/aws/s3"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Policy sul ruolo dei lavoratori di Amazon CloudWatch Events (prima del 6 dicembre 2018 PDT)

Se il tuo CodeStar progetto AWS è stato creato prima del 6 dicembre 2018 PDT, AWS CodeStar ha creato una policy in linea per un ruolo di worker CloudWatch Events. Di seguito è mostrato un esempio di istruzione della policy.

```
{
    "Statement": [
        {
            "Action": [
                "codepipeline:StartPipelineExecution"
            ],
            "Resource": [
                "arn:aws:codepipeline:us-east-1:account-id:project-id-Pipeline"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Politica sui limiti CodeStar delle autorizzazioni di AWS

Se crei un CodeStar progetto AWS dopo il 6 dicembre 2018 PDT, AWS CodeStar crea una policy sui limiti delle autorizzazioni per il tuo progetto. La policy impedisce l'escalation dei privilegi alle risorse al di fuori del progetto. Si tratta di una policy dinamica che si aggiorna con l'evolvere del progetto. Il contenuto della policy dipende dal tipo di progetto che stai creando. Di seguito ne viene riportato un esempio. Per ulteriori informazioni, consulta Limite delle autorizzazioni IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "1",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::*/AWSLogs/*/Config/*"
      ]
```

```
    },
    {
      "Sid": "2",
      "Effect": "Allow",
      "Action": [
        "*"
      ],
      "Resource": [
        "arn:aws:codestar:us-east-1:account-id:project/project-id",
        "arn:aws:cloudformation:us-east-1:account-id:stack/awscodestar-project-id-
lambda/eefbbf20-c1d9-11e8-8a3a-500c28b4e461",
        "arn:aws:cloudformation:us-east-1:account-id:stack/awscodestar-project-
id/4b80b3f0-c1d9-11e8-8517-500c28b236fd",
        "arn:aws:codebuild:us-east-1:account-id:project/project-id",
        "arn:aws:codecommit:us-east-1:account-id:project-id",
        "arn:aws:codepipeline:us-east-1:account-id:project-id-Pipeline",
        "arn:aws:execute-api:us-east-1:account-id:7rlst5mrgi",
        "arn:aws:iam::account-id:role/CodeStarWorker-project-id-CloudFormation",
        "arn:aws:iam::account-id:role/CodeStarWorker-project-id-CloudWatchEventRule",
        "arn:aws:iam::account-id:role/CodeStarWorker-project-id-CodeBuild",
        "arn:aws:iam::account-id:role/CodeStarWorker-project-id-CodePipeline",
        "arn:aws:iam::account-id:role/CodeStarWorker-project-id-Lambda",
        "arn:aws:lambda:us-east-1:account-id:function:awscodestar-project-id-lambda-
GetHelloWorld-KFKTXYNH9573",
        "arn:aws:s3:::aws-codestar-us-east-1-account-id-project-id-app",
        "arn:aws:s3:::aws-codestar-us-east-1-account-id-project-id-pipe"
      ]
    },
    {
      "Sid": "3",
      "Effect": "Allow",
      "Action": [
        "apigateway:GET",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:PutLogEvents"
      ],
      "Resource": [
        "*"
```

```
      ]
    }
  ]
}
```

Elenco delle risorse per un progetto

In questo esempio, vuoi concedere a un utente IAM specificato nel tuo AWS account l'accesso per elencare le risorse di un progetto. AWS CodeStar

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar:ListResources",
      ],
      "Resource" : "arn:aws:codestar:us-east-2:project/my-first-projec"
    }
  ]
}
```

Utilizzo della CodeStar console AWS

Non sono richieste autorizzazioni specifiche per accedere alla CodeStar console AWS, ma non puoi fare nulla di utile se non disponi della `AWSCodeStarFullAccess` policy o di uno dei ruoli a AWS CodeStar livello di progetto: Proprietario, Collaboratore o Visualizzatore. Per ulteriori informazioni su `AWSCodeStarFullAccess`, consulta AWSCodeStarFullAccess Politica. Per ulteriori informazioni sulle policy a livello di progetto, consulta Policy IAM per i membri del team.

Non è necessario consentire autorizzazioni minime di console per gli utenti che effettuano chiamate solo verso o l'API. AWS CLI AWS Al contrario, è possibile accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Consenti 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": "*"
        }
    ]
}
```

Aggiornamento di un progetto AWS CodeStar

In questo esempio, vuoi concedere a un utente IAM specificato nel tuo AWS account l'accesso per modificare gli attributi di un AWS CodeStar progetto, come la descrizione del progetto.

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

```
      "Action" : [
        "codestar:UpdateProject"
      ],
      "Resource" : "arn:aws:codestar:us-east-2:project/my-first-projec"
    }
  ]
}
```

Aggiunta di un membro del team a un progetto

In questo esempio, vuoi concedere a un utente IAM specifico la possibilità di aggiungere membri del team a un AWS CodeStar progetto con l'ID del progetto*my-first-projec*, ma negare esplicitamente a quell'utente la possibilità di rimuovere membri del team:

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar:AssociateTeamMember",
      ],
      "Resource" : "arn:aws:codestar:us-east-2:project/my-first-projec"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "codestar:DisassociateTeamMember",
      ],
      "Resource" : "arn:aws:codestar:us-east-2:project/my-first-projec"
    }
      ]

  ]
}
```

Elenco dei profili utente associati a un account AWS

In questo esempio, consenti a un utente IAM a cui è associata questa policy di elencare tutti i profili AWS CodeStar utente associati a un AWS account:

```
{
```

```
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar:ListUserProfiles",
              ],
      "Resource" : "*"
    }
  ]
}
```

Visualizzazione dei CodeStar progetti AWS in base ai tag

Puoi utilizzare le condizioni nella tua policy basata sull'identità per controllare l'accesso ai CodeStar progetti AWS in base ai tag. Questo esempio mostra come creare una policy che consente di visualizzare un progetto. Tuttavia, l'autorizzazione viene concessa solo se il valore del tag `Owner` del progetto corrisponde a quello del nome utente. Questa policy concede anche le autorizzazioni necessarie per completare questa azione nella console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListProjectsInConsole",
            "Effect": "Allow",
            "Action": "codestar:ListProjects",
            "Resource": "*"
        },
        {
            "Sid": "ViewProjectIfOwner",
            "Effect": "Allow",
            "Action": "codestar:GetProject,
            "Resource": "arn:aws:codestar:*:*:project/*",
            "Condition": {
                "StringEquals": {"codestar:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Puoi allegare questa policy agli utenti IAM nel tuo account. Se un utente denominato `richard-roe` tenta di visualizzare un CodeStar progetto AWS, il progetto deve essere taggato `0wner=richard-roe` o`owner=richard-roe`. In caso contrario l'accesso è negato. La chiave di tag di condizione `0wner` corrisponde a `0wner` e `owner` perché i nomi delle chiavi di condizione non effettuano la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.

AWS CodeStar aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle policy AWS gestite per AWS CodeStar da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei CodeStar documenti AWS.

Modifica	Descrizione	Data
AWSCodeStarFullAccess Policy: aggiorna la policy AWSCode StarFullAccess	La politica del ruolo di AWS CodeStar accesso è stata aggiornata. L'esito della policy è lo stesso, ma cloudformation richiede qualcosa ListStacks in più rispetto a DescribeStacks quanto già richiesto.	24 marzo 2023
AWSCodeStarServiceRole Politica: aggiorna la politica AWSCode StarServiceRole	La policy per il ruolo del CodeStar servizio AWS è stata aggiornata per correggere le azioni ridondanti contenute nella policy policy. La policy del ruolo del servizio consente al CodeStar servizio AWS di eseguire azioni per tuo conto.	23 settembre 2021
AWS CodeStar ha iniziato a tracciare le modifiche	AWS CodeStar ha iniziato a tracciare le modifiche per le sue policy AWS gestite.	23 settembre 2021

Risoluzione dei problemi di AWS CodeStar Identity and Access

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS CodeStar e IAM.

Argomenti

Non sono autorizzato a eseguire un'azione in AWS CodeStar

Se ti Console di gestione AWS dice che non sei autorizzato a eseguire un'azione, contatta l'amministratore per ricevere assistenza. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` tenta di utilizzare la console per visualizzare i dettagli relativi a *`widget`*, ma non dispone delle autorizzazioni `codestar:`*`GetWidget`*.

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

In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *`my-example-widget`* utilizzando l'azione `codestar:`*`GetWidget`*.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue policy devono essere aggiornate per consentirti di trasferire un ruolo ad AWS CodeStar.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in AWS CodeStar. Tuttavia, l'azione richiede che il

servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie CodeStar risorse AWS

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 policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS CodeStar supporta queste funzionalità, consultaCome CodeStar funziona AWS con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, 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.

Registrazione delle chiamate AWS CodeStar API con AWS CloudTrail

AWS CodeStar è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, un ruolo o un AWS servizio in AWS CodeStar. CloudTrail acquisisce tutte le chiamate API AWS CodeStar come eventi. Le chiamate acquisite includono chiamate dalla AWS CodeStar console e chiamate di codice alle operazioni AWS CodeStar API. Se crei un trail, puoi abilitare la consegna continua di CloudTrail eventi a un bucket S3, inclusi gli eventi per. AWS CodeStar 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 CodeStar, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli.

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

AWS CodeStar Informazioni in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in AWS CodeStar, 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 la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi di AWS CodeStar, crea un percorso. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il percorso registra gli eventi di tutte le regioni della AWS partizione e consegna i file di registro al bucket S3 specificato. 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 trail
- 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 vengono registrate CloudTrail e documentate nell'AWS CodeStar API Reference. Ad esempio, le chiamate a `DescribeProject`, `UpdateProject`, e `AssociateTeamMember` le 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 dell'utente 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 AWS CodeStar voci dei file di registro

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 chiamata di un'`CreateProject`operazione: AWS CodeStar

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJLIN2OF3UBEXAMPLE:role-name",
    "arn": "arn:aws:sts::account-ID:assumed-role/role-name/role-session-name",
    "accountId": "account-ID",
    "accessKeyId": "ASIAJ44LFQS5XEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2017-06-04T23:56:57Z"
      },
      "sessionIssuer": {
```

```
        "type": "Role",
        "principalId": "AROAJLIN2OF3UBEXAMPLE",
        "arn": "arn:aws:iam::account-ID:role/service-role/role-name",
        "accountId": "account-ID",
        "userName": "role-name"
      }
    },
    "invokedBy": "codestar.amazonaws.com"
  },
  "eventTime": "2017-06-04T23:56:57Z",
  "eventSource": "codestar.amazonaws.com",
  "eventName": "CreateProject",
  "awsRegion": "region-ID",
  "sourceIPAddress": "codestar.amazonaws.com",
  "userAgent": "codestar.amazonaws.com",
  "requestParameters": {
    "clientRequestToken": "arn:aws:cloudformation:region-ID:account-ID:stack/stack-
name/additional-ID",
    "id": "project-ID",
    "stackId": "arn:aws:cloudformation:region-ID:account-ID:stack/stack-
name/additional-ID",
    "description": "AWS CodeStar created project",
    "name": "project-name",
    "projectTemplateId": "arn:aws:codestar:region-ID::project-template/project-
template-name"
  },
  "responseElements": {
    "projectTemplateId": "arn:aws:codestar:region-ID::project-template/project-
template-name",
    "arn": "arn:aws:codestar:us-east-1:account-ID:project/project-ID",
    "clientRequestToken": "arn:aws:cloudformation:region-ID:account-ID:stack/stack-
name/additional-ID",
    "id": "project-ID"
  },
  "requestID": "7d7556d0-4981-11e7-a3bc-dd5daEXAMPLE",
  "eventID": "6b0d6e28-7a1e-4a73-981b-c8fdbEXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "account-ID"
}
```


Convalida della conformità per AWS CodeStar

AWS CodeStar non rientra nell'ambito di alcun programma di AWS conformità.

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, vedere AWS Servizi compresi nell'ambito del programma di conformità. Per informazioni generali, consulta Programmi di 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.

Resilienza in AWS CodeStar

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 Global Infrastructure.AWS

Sicurezza dell'infrastruttura in AWS CodeStar

In quanto servizio gestito, AWS CodeStar è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere CodeStar attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Per impostazione predefinita, AWS CodeStar non isola il traffico di servizio. I progetti creati utilizzando AWS CodeStar sono aperti alla rete Internet pubblica a meno che non si modifichino manualmente le impostazioni di accesso tramite Amazon EC2, API Gateway o Elastic Beanstalk. Questo è intenzionale. Puoi modificare le impostazioni di accesso in Amazon EC2, API Gateway o Elastic Beanstalk nella misura che desideri, inclusa la prevenzione di tutti gli accessi a Internet.

AWS CodeStar non fornisce il supporto per gli endpoint VPC (AWS PrivateLink) per impostazione predefinita, ma è possibile configurare tale supporto direttamente sulle risorse del progetto.

Limiti in AWS CodeStar

La tabella seguente descrive i limiti in AWS CodeStar. AWS CodeStar dipende da altri AWS servizi per le risorse del progetto. È possibile modificare alcune di queste restrizioni dei servizi. Per informazioni sulle restrizioni modificabili, consulta la pagina relativa alle restrizioni dei servizi AWS.

Numero di progetti	Massimo 333 progetti in un AWS account. Il limite effettivo varia a seconda del livello delle altre dipendenze del servizio (ad esempio, il numero massimo di pipeline CodePipeline consentito per l' AWS account).
Numero di AWS CodeStar progetti a cui un utente IAM può appartenere	Massimo 10 per singolo utente IAM.
Progetto IDs	Il progetto IDs deve essere unico in un AWS account. Il progetto IDs deve contenere almeno 2 caratteri e non può superare i 15 caratteri. I caratteri consentiti includono: Lettere dalla a alla z incluse. Numeri da 0 a 9 inclusi. Carattere speciale - (segno meno). Tutti gli altri caratteri, come lettere maiuscole , spazi, . (punto), @ (chiocciola) o _ (sottolin eatura), non sono consentiti.
Nomi di progetto	I nomi di progetto non possono superare i 100 caratteri di lunghezza e non possono iniziare o finire con uno spazio vuoto.
Descrizioni del progetto	Qualsiasi combinazione di caratteri, per una lunghezza compresa tra 0 e 1.024 caratteri. Le descrizioni dei progetti sono facoltative.

Membri del team in un AWS CodeStar progetto	100
Nome visualizzato in un profilo utente	Qualsiasi combinazione di caratteri, per una lunghezza compresa tra 1 e 100 caratteri. I nomi visualizzati devono includere almeno un carattere che non sia uno spazio. I nomi visualizzati non possono iniziare né finire con uno spazio.
Indirizzo e-mail di un profilo utente	L'indirizzo e-mail deve includere il simbolo @e terminare con un'estensione di dominio valida.
Accesso federato, accesso all'account root o accesso temporaneo a AWS CodeStar	AWS CodeStar supporta gli utenti federati e l'uso di credenziali di accesso temporanee. L'utilizzo AWS CodeStar con un account root non è consigliato.
Ruoli IAM	Un massimo di 5.120 caratteri in qualsiasi policy gestita associata a un ruolo IAM.

Risoluzione dei problemi AWS CodeStar

Le informazioni seguenti possono risultare utili per risolvere i problemi comuni di AWS CodeStar.

Argomenti

Errore di creazione del progetto: un progetto non è stato creato

Problema: quando provi a creare un progetto, viene visualizzato un messaggio indicante che la creazione non è riuscita.

Possibili correzioni: i motivi più comuni per gli errori sono:

- Un progetto con quell'ID esiste già nel tuo AWS account, probabilmente in un'altra AWS regione.
- L'utente IAM con cui hai effettuato l'accesso Console di gestione AWS non dispone delle autorizzazioni necessarie per creare un progetto.
- Al ruolo AWS CodeStar di servizio mancano una o più autorizzazioni richieste.
- Hai raggiunto il limite massimo per una o più risorse per un progetto (ad esempio il limite per le policy gestite dai clienti in IAM, i bucket Amazon S3 o le pipeline in). CodePipeline

Prima di creare un progetto, verifica di avere applicato la `AWSCodeStarFullAccess` policy al tuo utente IAM. Per ulteriori informazioni, consulta AWSCodeStarFullAccess Politica.

Quando si crea un progetto, assicurati che l'ID sia univoco e soddisfi i requisiti AWS CodeStar . Assicurati di aver selezionato la casella di controllo AWS CodeStar Desidero l'autorizzazione ad amministrare AWS le risorse per tuo conto.

Per risolvere altri problemi, apri la CloudFormation console, scegli lo stack per il progetto che hai cercato di creare e scegli la scheda Eventi. Non potrebbe essere presente più di uno stack per un progetto. I nomi dello stack iniziano con `awscodestar-` seguiti dall'ID del progetto. Gli stack potrebbero essere sotto la visualizzazione filtro Deleted (Eliminati). Esamina eventuali messaggi di errore negli eventi dello stack e correggi il problema elencato come causa di tali errori.

Creazione di un progetto: visualizzo un errore quando provo a modificare la EC2 configurazione di Amazon durante la creazione di un progetto

Problema: quando modifichi le opzioni di EC2 configurazione di Amazon durante la creazione del progetto, visualizzi un messaggio di errore o un'opzione disattivata e non puoi continuare con la creazione del progetto.

Possibili correzioni: i motivi più comuni per un messaggio di errore sono:

- Il VPC nel modello di AWS CodeStar progetto (il VPC predefinito o quello utilizzato per la modifica della EC2 configurazione di Amazon) ha una tenancy dedicata e il tipo di istanza non è supportato per le istanze dedicate. Scegli un tipo di istanza diverso o un Amazon VPC diverso.
- Il tuo AWS account non ha Amazon VPCs. È possibile che la VPC di default sia stata eliminata senza che ne sia stata creata un'altra. Apri la console Amazon VPC all'indirizzo https://

console.aws.amazon.com/vpc/, scegli Your VPCs e assicurati di avere almeno un VPC configurato. In caso contrario, è necessario crearne uno. Per ulteriori informazioni, consulta la panoramica di Amazon Virtual Private Cloud nella Amazon VPC Getting Started Guide.

- Amazon VPC non dispone di sottoreti. Scegli un altra VPC o crea una sottorete per la VPC. Per ulteriori informazioni, consulta la sezione relativa alle informazioni di base su VPC e sottoreti.

Eliminazione del progetto: un AWS CodeStar progetto è stato eliminato, ma le risorse esistono ancora

Problema: un AWS CodeStar progetto è stato eliminato, ma le risorse create per quel progetto esistono ancora. Per impostazione predefinita, AWS CodeStar elimina le risorse del progetto quando il progetto viene eliminato. Alcune risorse, come i bucket Amazon S3, vengono conservate anche se l'utente seleziona la casella di controllo Elimina risorse, poiché i bucket potrebbero contenere dati.

Possibili correzioni: apri la CloudFormation console e trova uno o più CloudFormation stack usati per creare il progetto. I nomi dello stack iniziano con `awscodestar-` seguiti dall'ID del progetto. Gli stack potrebbero essere sotto la visualizzazione filtro Deleted (Eliminati). Esamina gli eventi associati con lo stack per scoprire le risorse create per il progetto. Apri la console per ciascuna di queste risorse nella AWS regione in cui hai creato il AWS CodeStar progetto, quindi elimina manualmente le risorse.

Le risorse del progetto che potrebbero restare includono:

- Uno o più bucket di progetto in Amazon S3. A differenza di altre risorse di progetto, i bucket di progetto in Amazon S3 non vengono eliminati quando è selezionata la casella di controllo Elimina risorse AWS AWS CodeStar associate insieme al progetto.

  Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
- Un repository di sorgenti per il tuo progetto in. CodeCommit

  Apri la CodeCommit console all'indirizzo https://console.aws.amazon.com/codecommit/.
- Una pipeline per il tuo progetto in CodePipeline.

  Apri la CodePipeline console all'indirizzo https://console.aws.amazon.com/codepipeline/.
- Un'applicazione e i gruppi di distribuzione associati in CodeDeploy.

  Apri la CodeDeploy console all'indirizzo https://console.aws.amazon.com/codedeploy/.
- Un'applicazione e gli ambienti associati in AWS Elastic Beanstalk.

Apri la console Elastic Beanstalk all'indirizzo. https://console.aws.amazon.com/elasticbeanstalk/

- Una funzione in AWS Lambda.

  Apri la console all' AWS Lambda indirizzo. https://console.aws.amazon.com/lambda/

- Uno o più APIs in API Gateway.

  Apri la console API Gateway all'indirizzo https://console.aws.amazon.com/apigateway/.

- Una o più politiche o ruoli IAM in IAM.

  Accedi a Console di gestione AWS e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.

- Un'istanza in Amazon EC2.

  Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.

- Uno o più ambienti di sviluppo in AWS Cloud9.

  Per visualizzare, accedere e gestire gli ambienti di sviluppo, apri la AWS Cloud9 console all'indirizzo https://console.aws.amazon.com/cloud9/.

Se il progetto utilizza risorse esterne AWS (ad esempio, un GitHub repository o problemi in Atlassian JIRA), tali risorse non vengono eliminate, anche se è selezionata la casella Elimina AWS risorse associate insieme al CodeStar progetto.

Errore di gestione del team: non è stato possibile aggiungere un utente IAM a un team in un progetto AWS CodeStar

Problema: quando provi ad aggiungere un utente a un progetto, viene visualizzato un messaggio di errore indicante che l'aggiunta non è riuscita.

Possibili correzioni: il motivo più comune di questo errore è che l'utente ha raggiunto il limite di policy gestite che possono essere applicate a un utente in IAM. Potresti ricevere questo errore anche se non hai il ruolo di proprietario nel AWS CodeStar progetto in cui hai cercato di aggiungere l'utente o se l'utente IAM non esiste o è stato eliminato.

Assicurati di aver effettuato l'accesso come utente proprietario di quel AWS CodeStar progetto. Per ulteriori informazioni, consulta Aggiungere membri del team a un AWS CodeStar progetto .

Per risolvere altri problemi, apri la console IAM, scegli l'utente che hai provato ad aggiungere e controlla quante policy gestite vengono applicate a quell'utente IAM.

Per ulteriori informazioni, consulta Limitations on IAM Entities and Objects (Limitazioni per entità e oggetti &IAM;). Per le restrizioni modificabili, consulta la pagina sulle restrizioni dei servizi AWS.

Errore di accesso: un utente federato non può accedere a un progetto AWS CodeStar

Problema: un utente federato non è in grado di visualizzare i progetti nella AWS CodeStar console.

Possibili correzioni: se si è effettuato l'accesso come utente federato, assicurati di avere l'opportuna policy gestita associata al ruolo che assumi per poter accedere. Per ulteriori informazioni, consulta Allega la politica AWS CodeStar Viewer/Contributor/Owner gestita del tuo progetto al ruolo dell'utente federato.

Aggiungi utenti federati al tuo AWS Cloud9 ambiente allegando manualmente le policy. Per informazioni, consulta Allega una policy AWS Cloud9 gestita al ruolo dell'utente federato.

Errore di accesso: un utente federato non può accedere o creare un ambiente AWS Cloud9

Problema: un utente federato non è in grado di visualizzare o creare un AWS Cloud9 ambiente nella AWS Cloud9 console.

Possibili correzioni: se si è effettuato l'accesso come utente federato, assicurati di avere l'opportuna policy gestita associata al ruolo dell'utente federato.

Puoi aggiungere utenti federati al tuo AWS Cloud9 ambiente allegando manualmente le politiche al ruolo dell'utente federato. Per informazioni, consulta Allega una policy AWS Cloud9 gestita al ruolo dell'utente federato.

Errore di accesso: un utente federato può creare un AWS CodeStar progetto, ma non può visualizzare le risorse del progetto

Problemi: un utente federato era in grado di creare un progetto, ma non è in grado di visualizzare le risorse del progetto, ad esempio la pipeline del progetto.

Possibili correzioni: se hai allegato la politica **`AWSCodeStarFullAccess`**gestita, disponi delle autorizzazioni per creare un progetto in. AWS CodeStar Tuttavia, per accedere a tutte le risorse del progetto, è necessario collegare la policy gestita dal proprietario.

Dopo aver AWS CodeStar creato le risorse del progetto, le autorizzazioni di progetto per tutte le risorse del progetto sono disponibili nelle politiche gestite per proprietario, collaboratore e visualizzatore. Per accedere a tutte le risorse, è necessario collegare manualmente la policy del proprietario per il ruolo. Per informazioni, consulta Fase 3: Configurare le autorizzazioni IAM per l'utente.

Problema del ruolo del servizio: non è stato possibile creare il ruolo del servizio

Problema: quando si tenta di creare un progetto in AWS CodeStar, viene visualizzato un messaggio che richiede di creare il ruolo di servizio. Quando scegli la possibilità di crearlo, verrà visualizzato un messaggio di errore.

Possibili correzioni: il motivo più comune di questo errore è che hai effettuato l'accesso AWS con un account che non dispone di autorizzazioni sufficienti per creare il ruolo di servizio. Per creare il ruolo di AWS CodeStar servizio (`aws-codestar-service-role`), è necessario accedere come utente amministrativo o con un account root. Esci dalla console e accedi con un utente IAM a cui è stata applicata la policy `AdministratorAccess` gestita.

Problema del ruolo del servizio: il ruolo di servizio non è valido o è mancante

Problema: quando apri la AWS CodeStar console, viene visualizzato un messaggio che indica che il ruolo di AWS CodeStar servizio è mancante o non valido.

Possibili correzioni: il motivo più comune di questo errore è che un utente amministrativo ha modificato o eliminato il ruolo del servizio (`aws-codestar-service-role`). Se il ruolo del servizio è stato eliminato, ti viene chiesto di crearlo. È necessario essere registrati come utente amministratore o con un account root per creare il ruolo. Se il ruolo è stato modificato, ma non è più valido. Accedi alla console IAM come utente amministrativo, trova il ruolo di servizio nell'elenco dei ruoli ed eliminalo. Passa alla AWS CodeStar console e segui le istruzioni per creare il ruolo di servizio.

Problema relativo al ruolo del progetto: AWS Elastic Beanstalk i controlli dello stato di integrità non riescono per le istanze di un AWS CodeStar progetto

Problema: se hai creato un AWS CodeStar progetto che include Elastic Beanstalk prima del 22 settembre 2017, i controlli dello stato di salute di Elastic Beanstalk potrebbero non riuscire. Se non hai modificato la configurazione di Elastic Beanstalk da quando hai creato il progetto, il controllo dello stato di integrità ha esito negativo e riporta uno stato grigio. Nonostante l'errore di controllo dello stato di integrità, l'applicazione dovrebbe ancora essere eseguita come previsto. Se hai modificato la configurazione di Elastic Beanstalk dopo aver creato il progetto, il controllo dello stato di integrità ha esito negativo e l'applicazione potrebbe non funzionare correttamente.

Correzione: in uno o più ruoli IAM mancano le istruzioni di policy IAM richieste. Aggiungi le policy mancanti per i ruoli interessati nell'account AWS .

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.

   (Se non riesci a farlo, rivolgiti all'amministratore AWS del tuo account per ricevere assistenza.)
2. Nel riquadro di navigazione, seleziona Ruoli.
3. Nell'elenco dei ruoli, scegli CodeStarWorker- ***Project-ID*** -EB, dove *Project-ID* è l'ID di uno dei progetti interessati. (Se non è possibile trovare facilmente un ruolo nell'elenco, digita alcuni o tutti i nomi del ruolo nella casella Search (Cerca).)
4. Nella scheda Permissions (Autorizzazioni), scegli Attach Policy (Associa policy).
5. Nell'elenco delle politiche, seleziona AWSElasticBeanstalkEnhancedHealthe AWSElasticBeanstalkService. (Se non è possibile trovare facilmente una policy nell'elenco, digita alcuni o tutti i nomi della policy nella casella di ricerca.)
6. Scegli Attach Policy (Collega policy).
7. Ripeti i passaggi da 3 a 6 per ogni ruolo interessato il cui nome segue lo schema CodeStarWorker- ***Project-ID*** -EB.

Problema del ruolo del progetto: il ruolo del progetto non è valido o è mancante

Problema: quando si tenta di aggiungere un utente a un progetto, viene visualizzato un messaggio di errore che segnala che l'aggiunta non è riuscita perché la policy per un ruolo di progetto è mancante o non valido.

Possibili correzioni: il motivo più comune di questo errore è che una o più politiche di progetto sono state modificate o eliminate da IAM. Le politiche di progetto sono specifiche AWS CodeStar dei progetti e non possono essere ricreate. Il progetto non può essere utilizzato. Crea un progetto in AWS CodeStar, quindi migra i dati nel nuovo progetto. Clona il codice del progetto dal repository del progetto inutilizzabile e invia il codice al nuovo repository del progetto. Copia le informazioni wiki del team dal vecchio al nuovo progetto. Aggiungi gli utenti al nuovo progetto. Quando sei sicuro di aver migrato tutti i dati e le impostazioni, elimina il progetto inutilizzabile.

Estensioni del progetto: impossibile connettersi a JIRA

Problema: quando si utilizza l'estensione Atlassian JIRA per provare a connettere un AWS CodeStar progetto a un'istanza JIRA, viene visualizzato il seguente messaggio: «L'URL non è un URL JIRA valido. Verificare che l'URL sia corretto."

Possibili soluzioni.

- Verifica che l'URL JIRA sia corretto, quindi riprova a connetterti.
- L'stanza JIRA autogestita potrebbe non essere accessibile tramite Internet pubblico. Contatta l'amministratore di rete per verificare che sia possibile accedere all'istanza JIRA tramite Internet pubblico, quindi riprovare a connettersi.

GitHub: Impossibile accedere alla cronologia dei commit, ai problemi o al codice di un repository

Problema: nella dashboard di un progetto in cui è memorizzato il codice GitHub, i riquadri Cronologia dei commit e GitHubProblemi visualizzano un errore di connessione, oppure scegliendo Apri in GitHub o Crea problema in questi riquadri viene visualizzato un errore.

Possibili cause:

- Il AWS CodeStar progetto potrebbe non avere più accesso al GitHub repository.
- Il repository potrebbe essere stato eliminato o rinominato in. GitHub

AWS CloudFormation: la creazione di stack è stata sottoposta a rollback per autorizzazioni mancanti

Una volta aggiunta una risorsa per il file `template.yml`, visualizza l'aggiornamento di uno stack AWS CloudFormation per qualsiasi messaggio di errore. L'aggiornamento dello stack ha esito negativo se determinati criteri non sono soddisfatti (per esempio, quando le necessarie autorizzazioni a livello di risorsa sono mancanti).

> **Note**
>
> A partire dal 2 maggio 2019, abbiamo aggiornato la politica sul ruolo dei CloudFormation lavoratori per tutti i progetti esistenti. Questo aggiornamento consente di ridurre l'ambito delle autorizzazioni di accesso concesse alla pipeline per migliorare la sicurezza dei progetti.

Per risolvere i problemi, visualizza lo stato dell'errore nella visualizzazione del AWS CodeStar dashboard relativa alla pipeline del progetto.

Quindi, scegli il CloudFormationlink nella fase di distribuzione della pipeline per risolvere l'errore nella console. AWS CloudFormation Per visualizzare i dettagli di creazione dello stack, espandere l'elenco Events (Eventi) per il progetto e visualizza qualsiasi messaggio di errore. Il messaggio indica che l'autorizzazione è mancante. Correggere la policy del ruolo lavoratore CloudFormation e quindi eseguire nuovamente la pipeline.

AWS CloudFormation non è autorizzato a eseguire iam: PassRole on Lambda execution role

Se hai un progetto creato prima del 6 dicembre 2018 PDT che crea funzioni Lambda, potresti visualizzare CloudFormation un errore come questo:

```
User: arn:aws:sts::id:assumed-role/CodeStarWorker-project-id-CloudFormation/
AWSCloudFormation is not authorized to perform: iam:PassRole on resource:
```

```
arn:aws:iam::id:role/CodeStarWorker-project-id-Lambda (Service: AWSLambdaInternal;
Status Code: 403; Error Code: AccessDeniedException; Request ID: id)
```

Questo errore si verifica perché il ruolo di CloudFormation lavoratore non è autorizzato a passare un ruolo per il provisioning della nuova funzione Lambda.

Per correggere questo errore, dovrai aggiornare la politica relativa al ruolo di CloudFormation lavoratore con il seguente frammento.

```
{
        "Action":[ "iam:PassRole" ],
        "Resource": [
           "arn:aws:iam::account-id:role/CodeStarWorker-project-id-Lambda",
           ],

        "Effect": "Allow"
}
```

Dopo aver aggiornato la policy, eseguire nuovamente la pipeline.

In alternativa, puoi utilizzare un ruolo personalizzato per la tua funzione Lambda aggiungendo un limite di autorizzazioni al tuo progetto, come descritto in Aggiunta di un limite di autorizzazioni IAM ai progetti esistenti

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

AWS CodeStar Guida per l'utente e note di rilascio

La tabella seguente descrive le modifiche importanti in ogni versione della Guida per l' AWS CodeStar utente. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile sottoscrivere un feed RSS.

Modifica	Descrizione	Data
Aggiornamenti delle politiche di accesso	La politica del ruolo di AWS CodeStar accesso è stata aggiornata. L'esito della policy è lo stesso, ma cloudformation richiede qualcosa ListStack s in più rispetto a DescribeS tacks quanto già richiesto . Per fare riferimento alla politica aggiornata, consulta la sezione Policy. AWSCode StarFullAccess	24 marzo 2023
Aggiornamenti delle politiche relative ai ruoli di servizio	La politica del ruolo di AWS CodeStar servizio è stata aggiornata. Per fare riferimen to alla politica aggiornata, fare riferimento alla AWSCodeSt arServiceRole Politica.	23 settembre 2021
Utilizza una risorsa di connessione per progetti con un repository di GitHub sorgenti	Quando usi la console per creare un progetto AWS CodeStar con un GitHub repository, viene utilizzata una risorsa di connessione per gestire le tue GitHub azioni. Le connessioni utilizzano GitHub le app, mentre veniva utilizzata OAuth l' GitHub autorizzazione precedente. Per un tutorial	27 aprile 2021

	che mostra come creare un progetto che utilizza una connessione a GitHub, vedi Tutorial: Create a Project with a GitHub Source Repository. Il tutorial mostra anche come creare, rivedere e unire una pull request per il repository dei sorgenti del progetto.	
AWS CodeStar supporta AWS Cloud9 nella regione Stati Uniti occidentali (California settentrionale)	AWS CodeStar ora supporta l'utilizzo AWS Cloud9 nella regione Stati Uniti occidentali (California settentrionale). Per ulteriori informazioni, consulta Configurazione di Cloud9.	16 febbraio 2021
Aggiorna la documentazione per adattarla alla nuova esperienza con la console	Il 12 agosto 2020 il AWS CodeStar servizio è passato a una nuova esperienza utente nella AWS console. La guida per l'utente è stata aggiornat a per adattarsi alla nuova esperienza della console.	12 agosto 2020
AWS CodeStar i progetti possono essere creati con la AWS CodeStar CLI	AWS CodeStar i progetti possono essere creati con il comando CLI. AWS CodeStar crea il progetto e l'infrastruttura utilizzando il codice sorgente e un modello di toolchain fornito dall'utente. Vedi Creare un progetto in AWS CodeStar (AWS CLI).	24 ottobre 2018

Tutti i modelli di AWS CodeStar progetto ora includono CloudFormation file per gli aggiornamenti dell'infrastruttura	AWS CodeStar funziona con CloudFormation per consentire di utilizzare il codice per creare servizi di supporto e server o piattaforme serverless nel cloud. Il CloudFormation file è ora disponibile per tutti i tipi di modelli di AWS CodeStar progetto (modelli con la piattaforma di calcolo Lambda o Elastic Beanstalk). EC2 Il file è memorizzato in `template.yml` nel repository di origine del progetto. È possibile visualizzare e modificare il file per aggiungere risorse al progetto. Consulta Modelli di progetto.	3 agosto 2018
AWS CodeStar Le notifiche di aggiornamento della Guida per l'utente sono ora disponibili tramite RSS	La versione HTML della Guida per l' AWS CodeStar utente ora supporta un feed RSS di aggiornamenti documentati nella pagina Documentation Update Release Notes. Il feed RSS include gli aggiornamenti effettuati dopo il 30 giugno 2018. Gli aggiornamenti annunciati in precedenza sono ancora disponibili nella pagina delle note di rilascio degli aggiornamenti della documentazione. Utilizza il pulsante RSS nel pannello del menu in alto per registrarti al feed.	30 giugno 2018

La tabella seguente descrive le modifiche importanti apportate in ogni versione della Guida per l' AWS CodeStar utente prima del 30 giugno 2018.

Modifica	Descrizione	Data della modifica
La Guida per AWS CodeStar l'utente è ora disponibile su GitHub	Questa guida è ora disponibile su GitHub. Puoi anche utilizzarla GitHub per inviare feedback e richieste di modifica del contenuto di questa guida. Per ulteriori informazioni, scegli l' GitHubicona Modifica nella barra di navigazione della guida o consulta il aws-codestar-user-guide repository awsdocs/ sul sito web. GitHub	22 febbraio 2018
AWS CodeStar è ora disponibile in Asia Pacifico (Seoul)	AWS CodeStar è ora disponibile nella regione Asia Pacifico (Seoul). Per ulteriori informazioni, consulta AWS CodeStar nella Riferimenti generali di Amazon Web Services.	14 febbraio 2018
AWS CodeStar è ora disponibile in Asia Pacifico (Tokyo) e Canada (Centrale)	AWS CodeStar è ora disponibile nelle regioni Asia Pacifico (Tokyo) e Canada (Centrale). Per ulteriori informazioni, consulta AWS CodeStar nella Riferimenti generali di Amazon Web Services.	20 dicembre 2017
AWS CodeStar ora supporta AWS Cloud9	AWS CodeStar ora supporta l'utilizzo AWS Cloud9 di un IDE online basato su browser Web per lavorare con il codice del progetto. Per ulteriori informazioni, consulta Usare AWS Cloud9 con AWS CodeStar. Per un elenco delle AWS regioni supportate, AWS Cloud9consulta. Riferimenti generali di Amazon Web Services	30 novembre 2017
AWS CodeStar ora supporta GitHub	AWS CodeStar ora supporta la memorizzazione del codice del progetto in GitHub. Per ulteriori informazioni, consulta Creare un progetto.	12 ottobre 2017

Modifica	Descrizione	Data della modifica
AWS CodeStar ora disponibile negli Stati Uniti occidentali (California settentrionale) e in Europa (Londra)	AWS CodeStar è ora disponibile nelle regioni Stati Uniti occidentali (California settentrionale) ed Europa (Londra). Per ulteriori informazioni, consulta AWS CodeStar nella Riferimenti generali di Amazon Web Services.	17 agosto 2017
AWS CodeStar ora disponibile in Asia Pacifico (Sydney), Asia Pacifico (Singapore) ed Europa (Francoforte)	AWS CodeStar è ora disponibile nelle regioni Asia Pacifico (Sydney), Asia Pacifico (Singapore) ed Europa (Francoforte). Per ulteriori informazioni, consulta AWS CodeStar nella Riferimenti generali di Amazon Web Services.	25 luglio 2017
AWS CloudTrail ora supporta AWS CodeStar	AWS CodeStar è ora integrato con CloudTrail, un servizio che acquisisce le chiamate API effettuate da o per conto del AWS CodeStar tuo AWS account e invia i file di registro a un bucket Amazon S3 da te specificato. Per ulteriori informazioni, consulta Registrazione delle chiamate AWS CodeStar API con AWS CloudTrail.	14 giugno 2017
Rilascio iniziale	La prima versione della Guida per l'utente di AWS CodeStar .	19 aprile 2017

AWS Glossario

Per la AWS terminologia più recente, consultate il AWS glossario nella sezione Reference.Glossario AWS