



Guida per l'utente

AWS Toolkit for JetBrains



AWS Toolkit for JetBrains: Guida per l'utente

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e il trade dress di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in qualsiasi modo che possa causare confusione tra i clienti o in qualsiasi modo che denigri o discreditì Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Che cosa è la AWS Toolkit for JetBrains?	1
Che cosa include il AWS Toolkit for JetBrains	1
Lavorare con AWS Toolkit for JetBrains	2
Informazioni correlate	2
Video correlati	2
Pagine Web correlate	3
Domande e supporto	3
Segnala un bug con Kit di strumenti AWS o effettua una richiesta di funzionalità	4
Contribuire a Kit di strumenti AWS	4
Nozioni di base	5
Installazione di Kit di strumenti AWS	5
Installazione del Kit di strumenti AWS dall'IDE JetBrains	5
Installazione di build e versioni personalizzate	6
Rimozione dei riferimenti ai repository AWS Toolkit for JetBrains EAP o personalizzati	6
Navigazione	7
Visualizzazione del kit di strumenti da JetBrains	7
AWS Explorer	8
Connessione ad AWS	9
Connessione ad AWS	10
Connessione ad AWS dal AWS Toolkit for JetBrains	11
Regioni AWS	12
Visualizzazione della regione AWS corrente	12
Modifica delle regioni AWS	12
Impostazione del proxy HTTP	13
Autenticazione e accesso	14
Centro identità AWS IAM	14
Accesso con Centro identità IAM dal AWS Toolkit for JetBrains	14
Credenziali IAM	15
Prerequisiti	16
Creazione di un file delle credenziali condiviso dal AWS Toolkit for JetBrains	16
Configurazione delle credenziali condivise	17
ID Builder AWS	18
Configurazione di un ID Builder AWS	19
Servizi di ID Builder AWS	19

Utilizzo dei servizi AWS	20
Funzionalità sperimentali	20
AWS App Runner	21
Prerequisiti	22
Prezzi	24
Creazione di servizi App Runner	25
Gestione dei servizi App Runner	27
Amazon CodeCatalyst	30
Cos'è Amazon CodeCatalyst?	30
Nozioni di base su CodeCatalyst	31
Utilizzo di CodeCatalyst	33
AWS CloudFormation	38
Visualizzazione dei log eventi per uno stack	39
Eliminazione di uno stack	41
File di log di Amazon CloudWatch	42
Visualizzazione dei gruppi di registro log e dei flussi di registro CloudWatch	42
Utilizzo dei log eventi di CloudWatch	45
Utilizzo di Logs Insights di CloudWatch	48
Amazon CodeWhisperer	51
Che cos'è CodeWhisperer?	51
Amazon DynamoDB	51
Utilizzo di Amazon DynamoDB	52
Utilizzo delle tabelle DynamoDB	53
Amazon ECS	54
Amazon ECS Exec	54
Amazon EventBridge	58
Utilizzo degli schemi Amazon EventBridge	58
AWS Lambda	61
Runtime Lambda	61
Creazione di una funzione	63
Esecuzione (richiamo) o debug di una funzione locale	65
Esecuzione (richiamo) di una funzione remota	67
Modifica (aggiornamento) delle impostazioni della funzione	68
Eliminazione di una funzione	71
Amazon RDS	72
Prerequisiti per l'accesso ai database Amazon RDS	73

Connessione a un database Amazon RDS	75
Amazon Redshift	81
Prerequisiti per l'accesso ai cluster Amazon Redshift	81
Connessione a un cluster Amazon Redshift	83
Amazon S3	89
Utilizzo dei bucket Amazon S3	89
Utilizzo degli oggetti Amazon S3	91
AWS Serverless	93
Creazione di un'applicazione	94
Sincronizzazione di un'applicazione	99
Modifica (aggiornamento) delle impostazioni dell'applicazione	102
Eliminazione di un'applicazione	105
Amazon SQS	107
Code Amazon SQS	107
Utilizzo di Lambda	109
Utilizzo di Amazon SNS	110
Risorse	110
Autorizzazioni IAM per l'accesso alle risorse	111
Aggiunta di risorse e interazione con le risorse esistenti	112
Creazione e aggiornamento delle risorse	114
Documentazione di riferimento per l'interfaccia utente	117
AWS Explorer	117
Finestra di dialogo Create Function (Crea funzione)	121
Finestra di dialogo Implementa applicazione serverless	123
Finestra di dialogo del nuovo progetto	125
Finestra di dialogo Nuovo progetto (IntelliJ IDEA, PyCharm e WebStorm)	125
Finestra di dialogo Nuovo progetto (JetBrains Rider)	127
Finestra di dialogo Configurazioni di esecuzione/debug	129
Configurazioni di esecuzione/debug (funzioni locali)	129
Configurazioni di esecuzione/debug (funzioni remote)	136
Modifica configurazione (cluster Amazon ECS)	139
Finestra di dialogo Aggiorna codice	146
Finestra di dialogo Aggiorna configurazione	147
Sicurezza	150
Protezione dei dati	150
Identity and Access Management	151

Destinatari	152
Autenticazione con identità	152
Gestione dell'accesso tramite policy	156
Funzionamento dei Servizi AWS con IAM	159
Risoluzione dei problemi di identità e accesso in AWS	159
Convalida della conformità	161
Resilienza	162
Sicurezza dell'infrastruttura	163
Cronologia dei documenti	164

Che cosa è la AWS Toolkit for JetBrains?

AWS Toolkit for JetBrains è un plug-in open source per gli ambienti di sviluppo integrati (IDE) di JetBrains. Questo kit di strumenti consente di sviluppare, sottoporre a debug e implementare applicazioni serverless con Amazon Web Services (AWS) rendendo le risorse AWS disponibili dal proprio IDE JetBrains.

Argomenti

- [Che cosa include il AWS Toolkit for JetBrains](#)
- [Lavorare con AWS Toolkit for JetBrains](#)
- [Informazioni correlate](#)

Che cosa include il AWS Toolkit for JetBrains

AWS Toolkit for JetBrains include i seguenti kit di strumenti:

- Kit di strumenti AWS per [CLion](#) (per lo sviluppo in C e C++)
- Kit di strumenti AWS per [GoLand](#) (per lo sviluppo in Go)
- Kit di strumenti AWS per [IntelliJ](#) (per lo sviluppo in Java)
- Kit di strumenti AWS per [WebStorm](#) (per lo sviluppo in Node.js)
- Kit di strumenti AWS per [Rider](#) (per lo sviluppo in .NET)
- Kit di strumenti AWS per [PhpStorm](#) (per lo sviluppo in PHP)
- Kit di strumenti AWS per [PyCharm](#) (per lo sviluppo in Python)
- Kit di strumenti AWS per [RubyMine](#) (per lo sviluppo in Ruby)
- Kit di strumenti AWS per [DataGrip](#) (per la gestione dei database)

Note

Quando esistono differenze significative di funzionalità tra i Kit di strumenti AWS per gli IDE JetBrains supportati, le segnaliamo in questa guida.

È inoltre possibile utilizzare il AWS Toolkit for JetBrains per lavorare con le funzioni AWS Lambda, gli stack AWS CloudFormation e i cluster Amazon Elastic Container Service (Amazon ECS). AWS

Toolkit for JetBrains include caratteristiche quali la gestione di credenziali AWS e la gestione di regioni AWS che semplificano la scrittura di applicazioni per AWS.

Lavorare con AWS Toolkit for JetBrains

Puoi usare AWS Toolkit for JetBrains per effettuare quanto segue:

- Crea, implementa, aggiorna ed elimina le applicazioni AWS Serverless Application Model (AWS SAM). Per ulteriori informazioni su come utilizzare AWS SAM con il AWS Toolkit for JetBrains, consulta l'argomento [AWS Serverless](#) di questa Guida per l'utente.
- Crea, aggiorna, esegui e sottponi a debug in remoto e localmente le funzioni AWS Lambda. Per ulteriori informazioni sull'utilizzo del servizio AWS Lambda con il AWS Toolkit for JetBrains, consulta l'argomento [AWS Lambda](#) di questa Guida per l'utente.
- Visualizza i log eventi ed elimina gli stack AWS CloudFormation. Per ulteriori informazioni sull'utilizzo di CloudFormation e del AWS Toolkit for JetBrains, consulta l'argomento [AWS CloudFormation](#) di questa Guida per l'utente.
- Sottponi a debug il codice nei cluster AWS che utilizzano Amazon Elastic Container Service. Per ulteriori informazioni sull'utilizzo di Amazon ECS con il AWS Toolkit for JetBrains, consulta l'argomento [Amazon Elastic Container Service](#) di questa Guida per l'utente.
- Lavora con gli schemi di Amazon EventBridge. Per ulteriori informazioni, consulta l'argomento [Pianificatore Amazon EventBridge](#) in questa Guida per l'utente.

Informazioni correlate

Video correlati

- [Annuncio | Presentazione del kit di strumenti AWS per IntelliJ IDEA](#) (16 minuti, aprile 2019, sito Web YouTube)
- [Nozioni di base su AWS Toolkit for JetBrains](#) (copre solo Kit di strumenti AWS per PyCharm, 2 minuti, novembre 2018, sito Web YouTube)
- [Compilazione di applicazioni serverless con AWS Toolkit for JetBrains](#) (copre solo Kit di strumenti AWS per PyCharm, 6 minuti, novembre 2018, sito Web YouTube)

Pagine Web correlate

- [Kit di strumenti AWS per IntelliJ è ora generalmente disponibile](#) (marzo 2019, post di blog, sito Web AWS)
- [Kit di strumenti AWS per IntelliJ è ora disponibile a livello generale](#) (marzo 2019, post del blog, sito Web di AWS)
- [Novità: Kit di strumenti AWS per PyCharm, IntelliJ \(anteprima\)](#) (novembre 2018, post del blog, sito Web di AWS)
- [Presentazione del Kit di strumenti AWS per PyCharm](#) (novembre 2018, post di blog, sito Web AWS)
- [Kit di strumenti AWS per IntelliJ](#) (parte di AWS Toolkit for JetBrains, sito Web AWS)
- [Kit di strumenti AWS per PyCharm](#) (parte di AWS Toolkit for JetBrains, sito Web AWS)
- [Kit di strumenti AWS](#) (sito Web di JetBrains)
- [Develop on AWS with JetBrains Tools](#) (sito Web di JetBrains)
- [All Developer Tools and Products by JetBrains](#) (sito Web di JetBrains)

Domande e supporto

Per porre domande o chiedere supporto alla community AWS per sviluppatori, consulta i seguenti forum di discussione AWS:

- [Sviluppo C e C++](#)
- [Sviluppo Go](#)
- [Sviluppo con Java](#)
- [Sviluppo con JavaScript](#)
- [Sviluppo con .NET](#)
- [Sviluppo PHP](#)
- [Sviluppo con Python](#)
- [Sviluppo Ruby](#)

Per entrare nel forum, è possibile che AWS ti richieda di effettuare l'accesso.

È inoltre possibile [contattarci](#) direttamente.

Segnala un bug con Kit di strumenti AWS o effettua una richiesta di funzionalità

Per segnalare un bug con AWS Toolkit for JetBrains o per effettuare una richiesta di funzionalità, vai alla scheda [Issues \(Problemi\)](#) nel repository [aws/aws-toolkit-jetbrains](#) sul sito Web GitHub. Scegli New issue (Nuovo problema), quindi segui le istruzioni visualizzate sullo schermo per completare la segnalazione di un bug o la richiesta di una funzionalità. Quando accedi a questo sito Web, GitHub ti potrebbe richiedere l'accesso.

Contribuire a Kit di strumenti AWS

Teniamo in grande considerazione il tuo contributo a Kit di strumenti AWS. Per iniziare, leggi le [linee guida del contributo](#) nel repository [aws/aws-toolkit-jetbrains](#) sul sito Web GitHub. Quando accedi a questo sito Web, GitHub ti potrebbe richiedere l'accesso.

Nozioni di base su AWS Toolkit for JetBrains

Il AWS Toolkit for JetBrains rende i tuoi servizi e le tue risorse AWS disponibili direttamente dall'ambiente di sviluppo integrato (IDE) di JetBrains.

Per iniziare, i seguenti argomenti illustrano i processi di installazione, impostazione e configurazione del AWS Toolkit for JetBrains.

Argomenti

- [Installazione di AWS Toolkit for JetBrains](#)
- [Installazione di build AWS Toolkit for JetBrains Early Access Program \(EAP\) e personalizzate](#)
- [Spostamento nel AWS Toolkit for JetBrains](#)
- [Connessione del AWS Toolkit for JetBrains all'account AWS](#)
- [Impostazione di una regione AWS per AWS Toolkit for JetBrains](#)
- [Configurazione del proxy HTTP per il AWS Toolkit for JetBrains](#)

Installazione di AWS Toolkit for JetBrains

Puoi scaricare, installare e configurare il AWS Toolkit for JetBrains dal Marketplace di JetBrains nel tuo IDE. In alternativa, puoi scaricare la versione più recente dei file di installazione del AWS Toolkit for JetBrains accedendo all'elenco [AWS Toolkit for JetBrains Marketplace](#) da un browser Web.

Nelle sezioni seguenti viene descritto come installare e configurare il AWS Toolkit for JetBrains direttamente dall'IDE JetBrains.

Installazione del Kit di strumenti AWS dall'IDE JetBrains

Per scaricare e installare il AWS Toolkit for JetBrains direttamente dal tuo IDE JetBrains preferito, completa la procedura seguente.

1. Dal menu principale di JetBrains, apri il menu Preferences; se utilizzi Windows, espandi File e scegli Settings.
2. Dal menu Preferences/Settings, scegli Plugins per aprire il menu Plugins.
3. Dal menu di navigazione Plugins, scegli Marketplace per aprire il Marketplace dei plug-in di JetBrains.

4. Nel campo di ricerca che appare, inserisci **AWS Toolkit**.
5. Dalla voce del plug-in AWS Toolkit, seleziona il pulsante verde Install accanto al titolo della voce.
6. Accetta la Third-party Plugins Privacy Notice per continuare con la procedura di installazione.
7. JetBrains richiede di riavviare l'IDE al termine dell'installazione.

Installazione di build AWS Toolkit for JetBrains Early Access Program (EAP) e personalizzate

Le versioni Early Access Program (EAP) del AWS Toolkit for JetBrains contengono anteprime di funzionalità nuove e sperimentali.

Per configurare il kit di strumenti, completa la procedura seguente:

1. Dal menu principale di JetBrains, apri il menu Preferences; se utilizzi Windows, espandi File e scegli Settings.
2. Dal menu Preferences/Settings, scegli Plugins per aprire il menu Plugins.
3. Dal menu di navigazione Plugins, espandi l'icona Settings (Manage Repositories, Configure Proxy or Install Plugin from Disk) e scegli Manage Plugin Repositories.
4. Dal menu Manage Plugin Repositories, seleziona l'icona + (Add) e inserisci **<https://plugins.jetbrains.com/plugins/eap/aws.toolkit>** nel campo EAP repository for the AWS Toolkit.
5. Scegli OK per avviare l'installazione EAP.
6. JetBrains richiede di riavviare l'IDE al termine dell'installazione.

Rimozione dei riferimenti ai repository AWS Toolkit for JetBrains EAP o personalizzati

Potrebbe essere necessario rimuovere un riferimento a un repository EAP o personalizzato per utilizzare una versione specifica del AWS Toolkit for JetBrains. Per rimuovere un riferimento a un repository, completa la procedura seguente.

Note

Dopo aver completato questa procedura, potrebbe essere comunque necessario disinstallare la versione corrente del AWS Toolkit for JetBrains prima di aggiornarla o installare una versione diversa.

Rimozione di un riferimento al repository EAP

1. Dal menu principale di JetBrains, apri il menu Preferences; se utilizzi Windows, espandi File e scegli Settings.
2. Dal menu Preferences/Settings, scegli Plugins per aprire il menu Plugins.
3. Dal menu di navigazione Plugins, espandi l'icona Settings (Manage Repositories, Configure Proxy or Install Plugin from Disk) e scegli Manage Plugin Repositories.
4. Dal menu Manage Plugin Repositories, seleziona l'icona - (Remove) e conferma la rimozione.

Spostamento nel AWS Toolkit for JetBrains

Negli argomenti seguenti vengono descritti le posizioni e i componenti di base del AWS Toolkit for JetBrains.

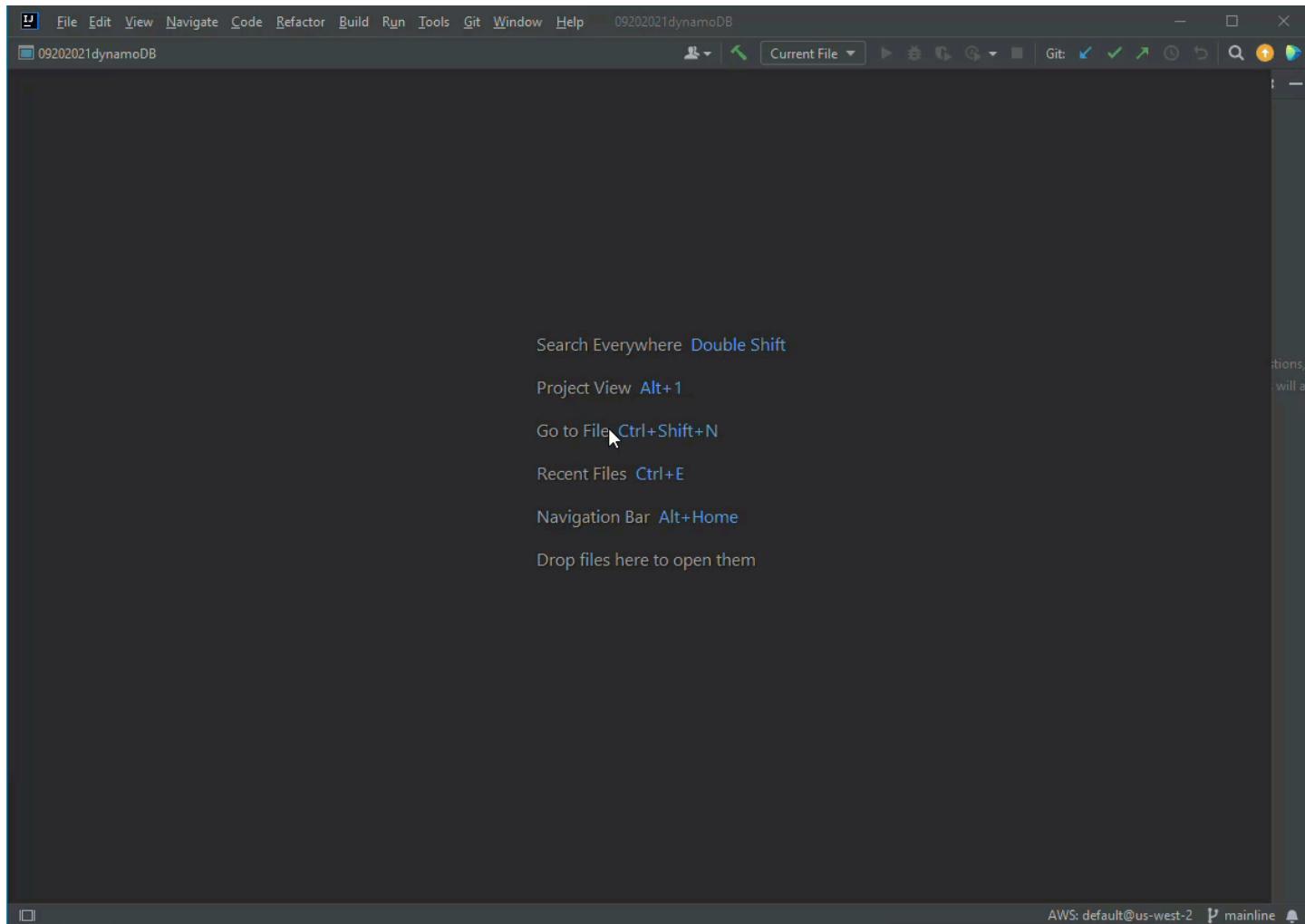
Argomenti

- [Visualizzazione del kit di strumenti da JetBrains](#)
- [AWS Explorer](#)
- [Connessione ad AWS](#)

Visualizzazione del kit di strumenti da JetBrains

Per visualizzare il kit di strumenti nell'IDE JetBrains, occorre eseguire le seguenti operazioni:

1. Dall'IDE JetBrains, espandi l'Active Toolbar utilizzando l'icona Active Toolbar nell'angolo in basso a sinistra dell'IDE JetBrains.
2. Da Active Toolbar, scegli AWS Toolkit.
3. Il AWS Toolkit for JetBrains è ora aperto nell'Active Toolbar.



AWS Explorer

I tuoi servizi e le tue risorse AWS sono disponibili tramite l'Esploratore AWS Toolkit for JetBrains.

Note

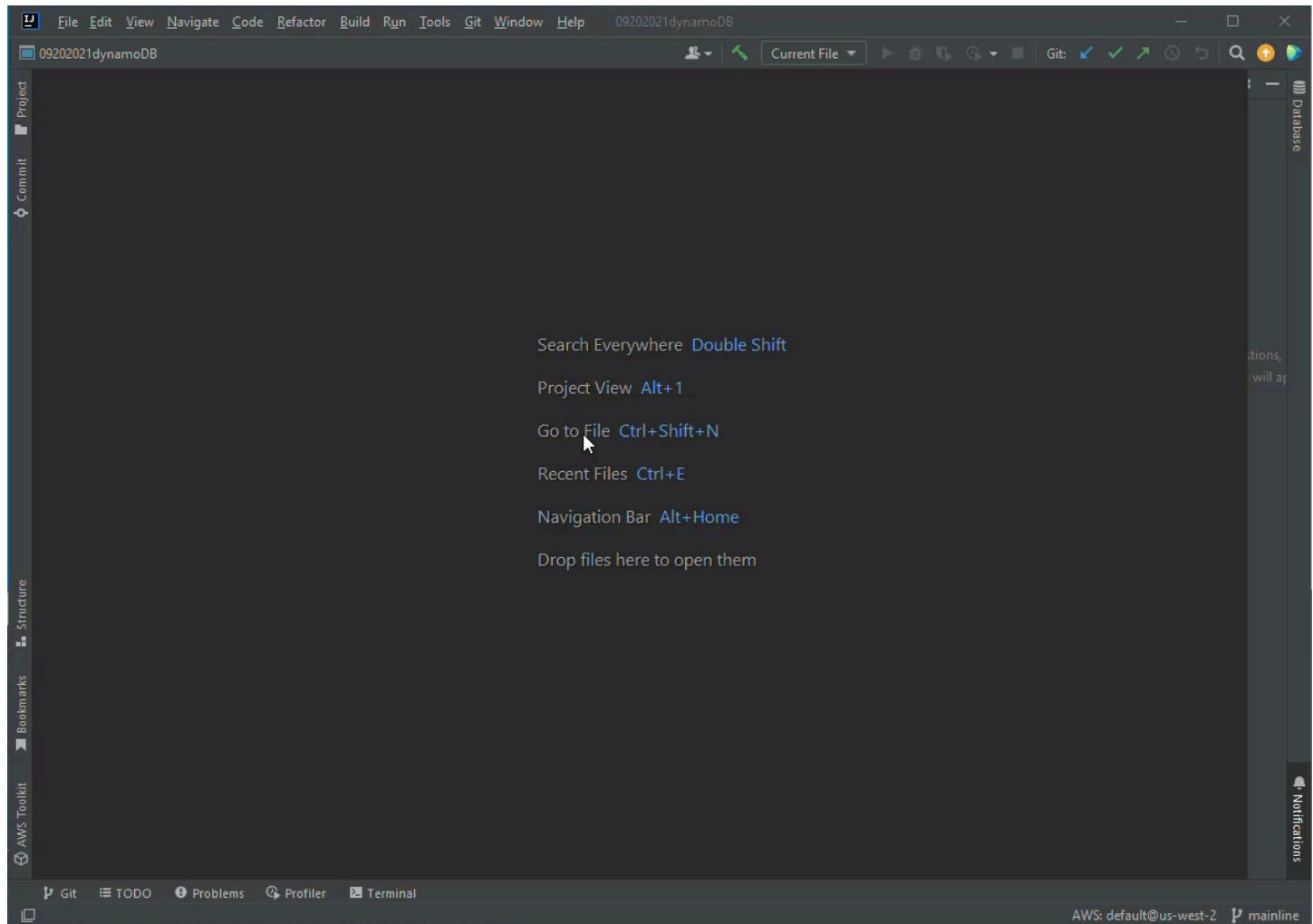
I servizi e le risorse AWS sono visibili dall'Esploratore AWS soltanto dopo aver configurato l'autenticazione e aver effettuato la connessione all'account AWS.

Per ulteriori informazioni sull'autenticazione e sul AWS Toolkit for JetBrains, consulta il sommario [Autenticazione e accesso](#) di questa Guida per l'utente.

Per ulteriori informazioni sulla connessione all'account AWS dal AWS Toolkit for JetBrains, consulta l'argomento [Connessione ad AWS](#) di questa Guida per l'utente.

Per visualizzare i servizi e le risorse AWS tramite l'Esploratore AWS Toolkit for JetBrains:

1. Dal AWS Toolkit for JetBrains, scegli la scheda Esploratore per visualizzare i servizi AWS associati al tuo account e alla tua regione.
2. Seleziona un servizio per espandere l'elenco delle tue risorse.
3. Apri il menu contestuale di una risorsa (facendo clic con il pulsante destro del mouse) per visualizzare un elenco di funzionalità per la modifica della risorsa.

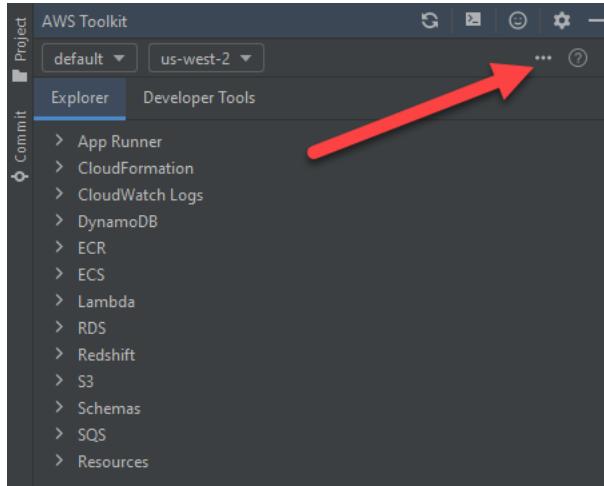


Connessione ad AWS

Le impostazioni di connessione si trovano nel menu dell'icona dei puntini di sospensione del riquadro di connessione del AWS Toolkit for JetBrains.

Note

Per ulteriori informazioni sulla connessione all'account AWS dal AWS Toolkit for JetBrains, consulta l'argomento [Connessione ad AWS](#) di questa Guida per l'utente.



Connessione del AWS Toolkit for JetBrains all'account AWS

La maggior parte delle risorse e dei servizi Amazon Web Services (AWS) è gestita tramite un account AWS. Per utilizzare la procedura il AWS Toolkit for JetBrains non è richiesto un account AWS, tuttavia le funzioni del kit di strumenti sono limitate in assenza di una connessione.

Se in precedenza hai configurato un account AWS e l'autenticazione tramite un altro servizio AWS (come la AWS Command Line Interface), AWS Toolkit for JetBrains rileva automaticamente le tue credenziali e ti guida attraverso il processo di connessione.

Se è la prima volta che utilizzi AWS o non hai creato un account, la procedura di connessione del AWS Toolkit for JetBrains al tuo account AWS prevede tre passaggi principali:

1. Creazione di un account AWS: puoi creare un account AWS dal portale [Iscriviti ad AWS](#). Per informazioni dettagliate sulla configurazione di un nuovo account AWS, consulta l'argomento [Panoramica](#) della Guida per l'utente alla configurazione di AWS.
2. Configurazione dell'autenticazione: esistono tre metodi principali per autenticarsi con l'account AWS dal AWS Toolkit for JetBrains. Per ulteriori informazioni su ciascuno di questi metodi, consulta l'argomento [Autenticazione e accesso](#) di questa Guida per l'utente.

3. Autenticazione con l'account AWS dal AWS Toolkit for JetBrains: dopo aver creato un account AWS e configurato l'autenticazione, puoi connettere il AWS Toolkit for JetBrains con il tuo account AWS completando la procedura Connessione ad AWS dal AWS Toolkit for JetBrains, riportata nella sezione seguente.

Connessione ad AWS dal AWS Toolkit for JetBrains

Completa la procedura seguente per eseguire l'autenticazione con l'account AWS utilizzando le credenziali Centro identità IAM esistenti dal AWS Toolkit for JetBrains.

Note

Questo processo avvia il portale Centro identità AWS IAM nel tuo browser Web preferito.

Ogni volta che le credenziali scadono, è necessario ripetere questo processo per rinnovare la connessione tra l'account AWS e il AWS Toolkit for JetBrains.

1. Dal AWS Toolkit for JetBrains, espandi il menu Impostazioni di connessione ad AWS selezionando l'icona ... (puntini di sospensione).
2. Dal menu Impostazioni di connessione di AWS, scegli Aggiungi nuova connessione... per aprire la finestra di dialogo Kit di strumenti AWS: aggiungi connessione.
3. Dalla finestra di dialogo Kit di strumenti AWS: aggiungi connessione, seleziona l'opzione di connessione con cui desideri autenticarti e scegli Connettiti per continuare.

Note

Per informazioni sulla configurazione di un metodo di autenticazione per l'account AWS specifiche per il AWS Toolkit for JetBrains, consulta l'argomento [Autenticazione e accesso](#) di questa Guida per l'utente.

4. Dopo aver selezionato il metodo di autenticazione, segui le istruzioni sullo schermo per connettere il AWS Toolkit for JetBrains con l'account AWS; JetBrains ti avvisa quando il processo di configurazione è completo.

Impostazione di una regione AWS per AWS Toolkit for JetBrains

Una regione AWS specifica il luogo in cui sono gestite le risorse AWS. La tua regione AWS predefinita viene rilevata quando ti connetti all'account AWS dal AWS Toolkit for JetBrains e viene visualizzata automaticamente nell'Esploratore AWS.

Nelle sezioni seguenti viene descritto come visualizzare e modificare la propria regione dall'Esploratore AWS Toolkit for JetBrains.

Visualizzazione della regione AWS corrente

Per verificare qual è la regione AWS attualmente selezionata, completa i seguenti passaggi.

1. Dall'Esploratore AWS, scegli l'icona Impostazioni per aprire Mostra il menu delle opzioni.
2. Da Mostra il menu delle opzioni, espandi Impostazioni di connessione ad AWS per visualizzare un elenco delle regioni AWS disponibili per il tuo account.
3. La tua regione AWS attuale riporta un'icona del segno di spunta accanto al nome.

Modifica delle regioni AWS

Per modificare la regione AWS attuale, completa i seguenti passaggi.

1. Dall'Esploratore AWS, scegli l'icona Impostazioni per aprire Mostra il menu delle opzioni.
2. Da Mostra il menu delle opzioni, espandi Impostazioni di connessione ad AWS per visualizzare un elenco delle regioni AWS.
3. Scegli la regione AWS a cui desideri connetterti dall'elenco.

Note

Se non vedi la regione a cui desideri connetterti, scegli Tutte le regioni per aprire un elenco completo di tutte le regioni AWS.

Configurazione del proxy HTTP per il AWS Toolkit for JetBrains

L'impostazione di un proxy HTTP per il AWS Toolkit for JetBrains viene gestita tramite l'ambiente di sviluppo integrato (IDE) di JetBrains. Per maggiori informazioni su come impostare un proxy HTTP, scegli il tuo IDE JetBrains dall'elenco seguente.

- CLion: consulta la pagina [Configure HTTP proxy](#) sul sito Web di assistenza di CLion.
- GoLand: consulta la pagina [Proxy HTTP](#) sul sito Web di assistenza di GoLand.
- IntelliJ IDEA: consulta la pagina [HTTP Proxy](#) sul sito Web di assistenza di IntelliJ IDEA.
- WebStorm: consulta la pagina [Proxy HTTP](#) sul sito Web di assistenza di WebStorm.
- JetBrains Rider: consulta la pagina [Configure HTTP Proxy](#) sul sito Web di assistenza di JetBrains Rider.
- PhpStorm: consulta la pagina [HTTP Proxy](#) sul sito Web di assistenza di PhpStorm.
- PyCharm: consulta la pagina [HTTP Proxy](#) sul sito Web di assistenza di PyCharm.
- RubyMine: consulta la pagina [HTTP Proxy](#) sul sito Web di assistenza di RubyMine.

Autenticazione e accesso per il AWS Toolkit for JetBrains

Non è necessario eseguire l'autenticazione con AWS per iniziare a lavorare con il AWS Toolkit for JetBrains. Tuttavia, la maggior parte delle risorse AWS viene gestita tramite un account AWS. Per accedere a tutti i servizi e le funzionalità di AWS Toolkit for JetBrains, avrai bisogno di almeno due tipi di autenticazione dell'account:

1. Autenticazione AWS Identity and Access Management (IAM) o AWS IAM Identity Center per gli account AWS. La maggior dei servizi e delle risorse AWS viene gestita tramite IAM e Centro identità IAM.
2. Un ID Builder AWS è facoltativo oppure obbligatorio per alcuni servizi AWS.

I seguenti argomenti contengono dettagli aggiuntivi e istruzioni di configurazione per ogni tipo di credenziale e metodo di autenticazione.

Argomenti

- [Centro identità AWS IAM](#)
- [Credenziali AWS IAM](#)
- [ID Builder AWS per sviluppatori](#)

Centro identità AWS IAM

AWS IAM Identity Center è la procedura consigliata per la gestione dell'autenticazione dell'account AWS.

Per istruzioni dettagliate su come configurare Centro identità IAM per i Software Development Kit (SDK) e il AWS Toolkit for JetBrains, consulta la sezione [IAM Identity Center authentication](#) della Guida di riferimento agli SDK e agli strumenti AWS.

Accesso con Centro identità IAM dal AWS Toolkit for JetBrains

Completa la procedura seguente per eseguire l'autenticazione con l'account AWS utilizzando le credenziali Centro identità IAM esistenti dal AWS Toolkit for JetBrains.

Note

Questo processo avvia il portale Centro identità AWS IAM nel tuo browser Web preferito.

Ogni volta che le credenziali scadono, è necessario ripetere questo processo per rinnovare la connessione tra l'account AWS e il AWS Toolkit for JetBrains.

1. Dal AWS Toolkit for JetBrains, apri il menu Impostazioni di connessione ad AWS selezionando l'icona ... (puntini di sospensione).
2. Dal menu Impostazioni di connessione di AWS, scegli Aggiungi nuova connessione... per aprire la finestra di dialogo Kit di strumenti AWS: aggiungi connessione.
3. Dalla finestra di dialogo Kit di strumenti AWS: aggiungi connessione, seleziona il pulsante di opzione Connottiti utilizzando Centro identità AWS IAM, inserisci l'URL del tuo portale Centro identità IAM nel campo di testo URL di avvio:, quindi scegli Connottiti per continuare.
4. Quando richiesto, conferma di voler aprire il portale Centro identità IAM nel tuo browser Web preferito e segui le istruzioni per completare il processo di autenticazione. Riceverai una notifica quando il processo di autenticazione sarà completo e potrai chiudere la finestra del browser in tutta sicurezza.

Credenziali AWS IAM

Le credenziali utente AWS IAM si autenticano con l'account AWS tramite chiavi di accesso memorizzate localmente.

Nelle seguenti sezioni viene descritto come configurare il AWS Toolkit for JetBrains per autenticarti con il tuo account AWS tramite le credenziali utente IAM.

Important

Prima di configurare le credenziali IAM per l'autenticazione con l'account AWS, tieni presente che:

- Se hai già impostato le credenziali IAM tramite un altro servizio AWS (come la AWS CLI), il AWS Toolkit for JetBrains rileva automaticamente tali credenziali e le rende disponibili.
- AWS consiglia di utilizzare l'autenticazione del Centro identità IAM. Per ulteriori informazioni sulle best practice di AWS IAM, consulta la sezione [Security best practice in IAM](#) della Guida per l'utente di AWS Identity and Access Management.

- Per evitare rischi per la sicurezza, non utilizzare gli utenti IAM per l'autenticazione quando sviluppi software creato ad hoc o lavori con dati reali. Utilizza invece la federazione con un provider di identità come [Che cos'è Centro identità IAM?](#) nella Guida per l'utente di AWS IAM Identity Center.

Prerequisiti

Prima di poter configurare il AWS Toolkit for JetBrains per l'autenticazione con le credenziali utente IAM, verifica che siano stati soddisfatti i prerequisiti seguenti. Se hai già configurato le credenziali utente IAM tramite un altro servizio (come la AWS Command Line Interface), puoi saltare i passaggi relativi ai prerequisiti e passare alle sezioni successive.

1. Crea un utente IAM. Per istruzioni dettagliate su come ottenere le chiavi di accesso di utente IAM, consulta la sezione [Step 1: Create your IAM user](#) della Guida di riferimento agli SDK e agli strumenti AWS.
2. Ottieni le chiavi di accesso utente IAM. Per istruzioni dettagliate su come ottenere le chiavi di accesso di utente IAM, consulta la sezione [Step 2: Get your access keys](#) della Guida di riferimento agli SDK e agli strumenti AWS.
3. Facoltativo: aggiorna il file delle credenziali condivise. Per istruzioni dettagliate su come aggiornare il file delle credenziali condivise, consulta la sezione [Step 3: Update the shared credentials file](#) della Guida di riferimento agli SDK e agli strumenti AWS.

Note

Se il prerequisto facoltativo Passaggio 3: aggiornamento del file di credenziali condivise è stato completato, il AWS Toolkit for JetBrains rileva automaticamente le tue credenziali durante la procedura di Creazione di un file di credenziali condiviso dal AWS Toolkit for JetBrains descritta nella sezione seguente.

Creazione di un file delle credenziali condiviso dal AWS Toolkit for JetBrains

Il file di configurazione condiviso e il file di credenziali condivise memorizzano le informazioni di configurazione e le credenziali per gli account AWS. Per ulteriori informazioni sulla configurazione e le credenziali condivise, consulta la sezione [Where are configuration settings stored?](#) della Guida per l'utente di AWS Command Line Interface.

Creazione di un file delle credenziali condiviso dal AWS Toolkit for JetBrains

1. Dal AWS Toolkit for JetBrains, scegli + Aggiungi connessione ad AWS per aprire la finestra di dialogo Kit di strumenti AWS: aggiungi connessione.
2. Dalla finestra di dialogo Kit di strumenti AWS: aggiungi connessione, scegli Modifica file di credenziali AWS per aprire la finestra di dialogo di conferma Crea file di credenziali.
3. Dalla finestra di dialogo di conferma Crea file di credenziali, scegli Crea per chiudere la finestra e creare il `credential File`.
4. Il `credential File` si apre automaticamente nell'IDE al termine della creazione.

Note

Durante il processo di creazione del `Credential File`:

- In caso di errore, JetBrains visualizza una notifica e apre i log di creazione contenenti i dettagli dell'errore.
- È possibile archiviare tutti i profili denominati in un unico file. Se utilizzi sia le credenziali sia i file di configurazione, le credenziali vengono aperte per impostazione predefinita nell'IDE.
- Se in entrambi i file sono presenti credenziali per un profilo che condivide lo stesso nome, le chiavi nel file delle credenziali hanno la precedenza.

Configurazione delle credenziali condivise

La procedura finale per autenticare il AWS Toolkit for JetBrains con l'account AWS serve per configurare le credenziali.

1. Dal AWS Toolkit for JetBrains, scegli + Aggiungi connessione ad AWS per aprire la finestra di dialogo Kit di strumenti AWS: aggiungi connessione.
2. Dalla finestra di dialogo Kit di strumenti AWS: aggiungi connessione, scegli Modifica file di credenziali AWS per aprire il File di credenziali.
3. Quando il `credentials file` si apre in JetBrains, individua la sezione etichettata `[default]`.
4. Dalla sezione `[default]`, individua la voce `#aws_access_key_id =`, rimuovi il `#` e inserisci la chiave di accesso AWS. La voce dovrebbe essere simile alla seguente:

aws_access_key_id = AKIAIOSFODNN7EXAMPLE

5. Dalla sezione [default], individua la voce `#aws_secret_access_key =`, rimuovi il `#` e inserisci la chiave di accesso segreta AWS. La voce dovrebbe essere simile alla seguente:

aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfCYEXAMPLEKEY

La versione finale del file di credenziali aggiornato è simile alla seguente:

```
[default]
# The access key and secret key pair identify your account and grant access to AWS.
# Treat your secret key like a password. Never share your secret key with anyone.
Do
# not post it in online forums, or store it in a source control system. If your
secret
# key is ever disclosed, immediately use IAM to delete the access key and secret
key
# and create a new key pair. Then, update this file with the replacement key
details.
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfCYEXAMPLEKEY
```

6. Salva le modifiche al file: il AWS Toolkit for JetBrains rileva automaticamente le credenziali aggiornate e si connette all'account AWS.

aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfCYEXAMPLEKEY

ID Builder AWS per sviluppatori

ID Builder AWS è un account AWS che è facoltativo o obbligatorio per alcuni servizi AWS. Per ulteriori informazioni su come configurare l'ID Builder AWS per servizi specifici, consulta la sezione [the section called “Servizi di ID Builder AWS”](#) di questa guida.

Le seguenti sezioni descrivono come creare ed eseguire l'autenticazione con l'ID Builder AWS dal AWS Toolkit for JetBrains.

Configurazione di un ID Builder AWS

Configurazione di un ID Builder AWS dal AWS Toolkit for JetBrains

1. Dall'Esploratore AWS, scegli + Aggiungi connessione ad AWS per aprire la finestra di dialogo Kit di strumenti AWS: aggiungi connessione.
2. Dalla finestra di dialogo Kit di strumenti AWS: aggiungi connessione, scegli Utilizza un indirizzo e-mail personale per registrarti e accedere con ID Builder AWS per aprire la finestra di dialogo Accedi con ID Builder AWS.
3. Dalla finestra di dialogo Accedi con un ID Builder AWS, seleziona il pulsante Apri e copia il codice per aprire il sito Richiesta di autorizzazione AWS in un browser Web.
4. Dal browser Web, incolla il codice di conferma nel campo apposito e scegli Successivo per procedere alla Creazione del sito ID Builder AWS.
5. Completa tutti i passaggi del tuo browser Web per continuare. Una volta completato il processo, riceverai una notifica che è sicuro chiudere il browser e tornare a JetBrains.
6. In JetBrains, il menu a discesa + Aggiungi connessione ad AWS viene aggiornato, indicando che sei connesso con l'ID Builder AWS.

Servizi di ID Builder AWS

La connessione di servizi specifici all'ID Builder AWS potrebbe richiedere una configurazione aggiuntiva. I seguenti servizi compatibili con ID Builder AWS sono accessibili tramite il AWS Toolkit for JetBrains:

- Amazon CodeCatalyst: per ulteriori informazioni su come configurare Amazon CodeCatalyst per Builder ID AWS, consulta la sezione [Setting up Amazon CodeCatalyst](#) della Guida per l'utente di Amazon CodeCatalyst.
- Amazon CodeWhisperer: per ulteriori informazioni su come configurare Amazon CodeWhisperer per Builder ID AWS, consulta la sezione [Setting up Amazon CodeWhisperer](#) della Guida per l'utente di Amazon CodeWhisperer.

Utilizzo dei servizi AWS tramite l'Esploratore del Kit di strumenti AWS

I tuoi servizi e le tue risorse AWS sono disponibili tramite l'Esploratore AWS Toolkit for JetBrains.

Per ulteriori informazioni su come utilizzare il AWS Toolkit for JetBrains e l'Esploratore AWS, consulta l'argomento [Navigazione](#) di questa Guida per l'utente.

Per ulteriori informazioni su come lavorare con un servizio AWS specifico tramite il AWS Toolkit for JetBrains, scegli dal seguente elenco degli argomenti.

Argomenti

- [Utilizzo delle funzionalità sperimentali](#)
- [Utilizzo del Kit di strumenti AWS per JetBrains con AWS App Runner](#)
- [Amazon CodeCatalyst per JetBrains](#)
- [Utilizzo di AWS CloudFormation tramite il AWS Toolkit for JetBrains](#)
- [Utilizzo di File di log CloudWatch tramite il AWS Toolkit for JetBrains](#)
- [Utilizzo di Amazon CodeWhisperer](#)
- [Amazon DynamoDB nel AWS Toolkit for JetBrains](#)
- [Utilizzo di Amazon Elastic Container Service tramite il AWS Toolkit for JetBrains](#)
- [Utilizzo di Amazon EventBridge tramite il AWS Toolkit for JetBrains](#)
- [Utilizzo di AWS Lambda tramite il AWS Toolkit for JetBrains](#)
- [Accesso ad Amazon RDS tramite il AWS Toolkit for JetBrains](#)
- [Accesso ad Amazon Redshift tramite il AWS Toolkit for JetBrains](#)
- [Utilizzo di Amazon S3 tramite il AWS Toolkit for JetBrains](#)
- [Utilizzo delle applicazioni serverless AWS tramite il AWS Toolkit for JetBrains](#)
- [Utilizzo di Amazon Simple Queue Service tramite il AWS Toolkit for JetBrains](#)
- [Utilizzo delle risorse](#)

Utilizzo delle funzionalità sperimentali

Le funzionalità sperimentali offrono l'accesso anticipato alle funzionalità del AWS Toolkit for JetBrains prima che vengano pubblicate ufficialmente.

Warning

Dato che le funzionalità sperimentali vengono continuamente testate e aggiornate, potrebbero presentare problemi di usabilità. Inoltre, le funzionalità sperimentali potrebbero essere rimosse dal AWS Toolkit for JetBrains senza preavviso.

È possibile abilitare funzionalità sperimentali per servizi AWS specifici nella sezione AWS del riquadro Settings nell'IDE JetBrains.

1. Per modificare le impostazioni di AWS in JetBrains, scegli File, Settings oppure premi Ctrl+Alt+S.
2. Nel riquadro Settings, espandi Tools e scegli AWS, Experimental Features.
3. Seleziona le caselle di controllo relative alle funzionalità sperimentali a cui desideri accedere prima del rilascio. Se desideri disattivare una funzionalità sperimentale, deselecta la relativa casella di controllo.
4. Dopo aver abilitato le funzionalità sperimentali, puoi verificarne l'attivazione aprendo l'Esploratore AWS e scegliendo Opzioni (l'icona a forma di ingranaggio), Funzionalità sperimentali. Un segno di spunta accanto al nome della funzionalità indica che è disponibile per l'uso.

Utilizzo del Kit di strumenti AWS per JetBrains con AWS App Runner

[AWS App Runner](#) fornisce un modo rapido, semplice e conveniente per implementare dal codice sorgente o da un'immagine di container direttamente a un'applicazione Web scalabile e sicura in AWS Cloud. Non è necessario apprendere nuove tecnologie, decidere quale servizio di elaborazione utilizzare o sapere come eseguire il provisioning e la configurazione delle risorse AWS.

Puoi utilizzare AWS App Runner per creare e gestire servizi basati su una immagine sorgente o un codice sorgente. Se utilizzi un'immagine sorgente, puoi scegliere un'immagine di container pubblica o privata archiviata in un repository di immagini. App Runner supporta i seguenti provider di repository di immagini:

- Amazon Elastic Container Registry (Amazon ECR): archivia immagini private nell'account AWS.
- Amazon Elastic Container Registry Public (Amazon ECR Public): archivia le immagini leggibili pubblicamente.

Se scegli l'opzione del codice sorgente, puoi eseguire l'implementazione da un repository di codice sorgente gestito da un provider di repository supportato. Al momento, come provider di repository del codice sorgente, App Runner supporta [GitHub](#):

Prerequisiti

Questa sezione presuppone che tu abbia già un account AWS e disponga della versione più recente del AWS Toolkit for JetBrains completa di AWS App Runner. Oltre a questi requisiti fondamentali, assicurati che tutti gli utenti IAM pertinenti dispongano delle autorizzazioni per interagire con il servizio App Runner. Inoltre è necessario ottenere informazioni specifiche sull'origine del servizio, come l'URI dell'immagine di container o la connessione al repository GitHub. Queste informazioni sono necessarie per creare il servizio App Runner.

Configurazione delle autorizzazioni IAM per App Runner

Il modo più semplice per concedere le autorizzazioni necessarie per App Runner è collegare una policy gestita da AWS all'entità IAM pertinente, in particolare un utente o un gruppo. App Runner fornisce due policy gestite che è possibile allegare agli utenti IAM:

- **AWSAppRunnerFullAccess**: consente agli utenti di eseguire tutte le operazioni di App Runner.
- **AWSAppRunnerReadOnlyAccess**: consente agli utenti di elencare e visualizzare i dettagli relativi alle risorse di App Runner.

Inoltre, se scegli un repository privato da Amazon Elastic Container Registry (Amazon ECR) come origine del servizio, devi creare il seguente ruolo di accesso per il servizio App Runner:

- **AWSAppRunnerServicePolicyForECRAccess**: consente ad App Runner di accedere alle immagini Amazon Elastic Container Registry (Amazon ECR) nel tuo account.

È possibile utilizzare la finestra di dialogo Crea il servizio App Runner per creare questo ruolo IAM.

Note

Il ruolo collegato ai servizi `AWSServiceRoleForAppRunner` consente a AWS App Runner di completare i seguenti processi:

- Inviare i log ai gruppi di log di Amazon CloudWatch Logs.

- Creare regole di Amazon CloudWatch Events per eseguire la sottoscrizione all'invio delle immagini di Amazon Elastic Container Registry (Amazon ECR).

Non devi creare manualmente il ruolo collegato al servizio . Quando crei un AWS App Runner nella Console di gestione AWS oppure utilizzando le operazioni API che vengono chiamate dal kit di strumenti AWS Toolkit for JetBrains, AWS App Runner crea per tuo conto questo ruolo collegato al servizio.

Per ulteriori informazioni, consulta [Identity and Access Management per App Runner](#) nella Guida per gli sviluppatori di AWS App Runner.

Recupero delle origini di servizio per App Runner

AWS App Runner può essere utilizzato per implementare servizi da un'immagine sorgente o da un codice sorgente.

Source image

Se stai eseguendo l'implementazione da un'immagine sorgente, puoi ottenere un collegamento al repository dell'immagine interessata da un registro di immagini AWS privato o pubblico.

- Registro privato Amazon ECR: puoi copiare l'URI di un repository privato che utilizza la console Amazon ECR all'indirizzo <https://console.aws.amazon.com/ecr/repositories>.
- Registro pubblico Amazon ECR: puoi copiare l'URI di un repository pubblico che utilizza la galleria pubblica di Amazon ECR all'indirizzo <https://gallery.ecr.aws/>.

È possibile specificare l'URI del repository dell'immagine quando inserisci i dettagli della sorgente nella finestra di dialogo Crea il servizio App Runner.

Per ulteriori informazioni, consulta [Servizio App Runner basato su un'immagine sorgente](#) nella Guida per gli sviluppatori di AWS App Runner.

Source code

Per implementare il codice sorgente su un servizio AWS App Runner, tale codice deve essere archiviato in un repository Git gestito da un provider di repository supportato. Al momento, App Runner supporta un solo provider del repository del codice sorgente, ovvero [GitHub](#).

Per ulteriori informazioni sulla configurazione di un repository GitHub, consulta la [documentazione di base](#) su GitHub.

Per implementare il codice sorgente in un servizio App Runner da un repository GitHub, App Runner stabilisce una connessione a GitHub. Se il tuo repository è privato (cioè non è accessibile pubblicamente su GitHub), devi fornire ad App Runner i dettagli per la connessione.

Important

Per creare connessioni GitHub, utilizza la console App Runner (<https://console.aws.amazon.com/apprunner>) e crea una connessione che collega GitHub a AWS.

Quando utilizzi la finestra di dialogo Crea servizio App Runner per specificare i dettagli sul repository del codice sorgente, puoi selezionare le connessioni disponibili sulla pagina Connessioni GitHub.

Per ulteriori informazioni, consulta [Gestione delle connessioni di App Runner](#) nella Guida per gli sviluppatori di AWS App Runner.

L'istanza del servizio App Runner fornisce un runtime gestito che consente la creazione e l'esecuzione del codice. AWS App Runner al momento supporta i seguenti runtime:

- Runtime gestito da Python
- Runtime gestito da Node.js

Utilizzando la finestra di dialogo Crea il servizio App Runner disponibile nel AWS Toolkit for JetBrains, specifica le modalità in cui il servizio App Runner crea e avvia il servizio. È possibile inserire le informazioni direttamente nell'interfaccia o specificare un [file di configurazione App Runner](#) in formato YAML. I valori in questo file indicano ad App Runner come creare e avviare il servizio e forniscono il contesto di runtime. Sono incluse le impostazioni di rete e le variabili di ambiente pertinenti. Il file di configurazione è denominato `apprunner.yaml`. Viene aggiunto automaticamente alla directory principale del repository dell'applicazione.

Prezzi

Ti viene addebitato il costo delle risorse di calcolo e memoria utilizzate dall'applicazione. Inoltre, se automatizzi le implementazioni, paghi anche una tariffa mensile fissa per ogni applicazione che copre tutte le implementazioni automatiche per quel mese. Se scegli di eseguire l'implementazione

dal codice sorgente, paghi anche una tariffa di creazione per il periodo di tempo impiegato da App Runner per creare un container dal codice sorgente.

Per ulteriori informazioni, consultare [Prezzi di AWS App Runner](#).

Argomenti

- [Creazione di servizi App Runner](#)
- [Gestione dei servizi App Runner](#)

Creazione di servizi App Runner

È possibile specificare un servizio App Runner nel AWS Toolkit for JetBrains tramite la finestra di dialogo Crea servizio App Runner. È possibile utilizzare la relativa interfaccia per selezionare un repository di origine e configurare l'istanza del servizio su cui viene eseguita l'applicazione.

Prima di creare un servizio App Runner, verifica di aver soddisfatto tutti i [prerequisiti](#). Tra le altre cose, dovrai fornire le autorizzazioni IAM pertinenti e prendere nota delle informazioni specifiche del repository di origine che desideri implementare.

Creazione di un servizio App Runner

1. Aprire AWS Explorer, se non è già aperto.
2. Fai clic con il pulsante destro del mouse sul nodo App Runner e scegli Create Service (Crea servizio).

Viene visualizzata la finestra di dialogo Crea il servizio App Runner.

3. Inserisci il tuo Nome del servizio univoco.
4. Scegli il tipo di origine (ECR, ECR pubblico o Repository di codice sorgente) e configura le impostazioni pertinenti:

ECR/ECR public

Se utilizzi un registro privato, scegli il Tipo di implementazione:

- Manuale: utilizza l'implementazione manuale se desideri specificare esplicitamente ogni implementazione del tuo servizio.
- Automatico: utilizza l'implementazione automatica se desideri implementare il comportamento CI/CD (integrazione continua/implementazione continua) per il tuo servizio.

Se scegli questa opzione, significa che ogni volta che inserisci una nuova versione di immagine nel tuo repository di immagini o un esegui un commit nel tuo repository di codice, App Runner lo implementa automaticamente al tuo servizio senza che tu debba eseguire ulteriori operazioni.

Per URI dell'immagine del container, inserisci l'URI del repository di immagini che hai copiato dal tuo registro privato Amazon ECR o dalla Galleria pubblica Amazon ECR.

Per Comando di avvio, specifica il comando per avviare il processo del servizio.

Per Porta, inserisci la porta IP utilizzata dal servizio.

Se utilizzi un registro privato Amazon ECR, seleziona il Ruolo di accesso ECR richiesto e scegli Crea.

- La finestra di dialogo Crea ruolo IAM visualizza Nome, Policy gestite e Relazioni di fiducia per il ruolo IAM. Seleziona Crea.

Source code repository

Scegli il Tipo di implementazione:

- Manuale: utilizza l'implementazione manuale se desideri specificare esplicitamente ogni implementazione del tuo servizio.
- Automatico: utilizza l'implementazione automatica se desideri implementare il comportamento CI/CD (integrazione continua/implementazione continua) per il tuo servizio. Se scegli questa opzione, significa che ogni volta che inserisci una nuova versione di immagine nel tuo repository di immagini o esegui un commit nel tuo repository di codice, App Runner lo implementa automaticamente al tuo servizio senza che tu debba eseguire ulteriori operazioni.

Per Connessioni, seleziona una connessione disponibile dall'elenco sulla pagina Connessioni GitHub.

Per URL repository, inserisci il link al repository remoto ospitato su GitHub.

Per Selezione un ramo, scegli il ramo Git del codice sorgente che desideri implementare.

Per Configurazione, scegli come desideri specificare la configurazione del runtime:

- Configura tutte le impostazioni qui: scegli questa opzione se desideri specificare le seguenti impostazioni per l'ambiente di runtime dell'applicazione:
 - Runtime: scegli Python 3 o Nodejs 12.
 - Porta: inserisci la porta IP utilizzata dal servizio.
 - Build command (Comando build): immetti il comando per creare l'applicazione nell'ambiente di runtime dell'istanza del servizio.
 - Start command (Comando avvio): immetti il comando per avviare l'applicazione nell'ambiente di runtime dell'istanza del servizio.
- Fornisci qui le impostazioni del file di configurazione: scegli questa opzione per utilizzare le impostazioni definite dal file di configurazione `apprunner.yaml`. Questo file si trova nella directory principale del repository dell'applicazione.

5. Scegli i valori per specificare la configurazione di runtime dell'istanza del servizio App Runner:

- CPU: il numero di unità CPU riservate per ogni istanza del servizio App Runner (predefinito: 1 vCPU).
- Memoria: la quantità di memoria riservata per ogni istanza del servizio App Runner (predefinito: 2 GB)
- Configura variabili di ambiente: variabili di ambiente facoltative utilizzabili per personalizzare il comportamento nell'istanza del servizio. Crea variabili di ambiente definendo una chiave e un valore.

6. Scegli Create (Crea)

Quando il servizio viene creato, il suo stato cambia da Operazione in corso a In esecuzione.

7. Appena il servizio è in esecuzione, fai clic con il pulsante destro del mouse e scegli Copy Service URL (Copia URL del servizio).
8. Per accedere all'applicazione implementata, incolla l'URL copiato nella barra degli indirizzi del browser Web.

Gestione dei servizi App Runner

Dopo aver creato un servizio App Runner, potrai gestirlo utilizzando il riquadro AWS Explorer per completare le seguenti attività:

- [Sospensione e ripresa dei servizi App Runner](#)
- [Implementazione dei servizi App Runner](#)
- [Visualizzazione dei flussi di log per App Runner](#)
- [Eliminazione di servizi App Runner](#)

Sospensione e ripresa dei servizi App Runner

Se è necessario disabilitare temporaneamente l'applicazione Web e interrompere l'esecuzione del codice, puoi sospendere il servizio AWS App Runner. App Runner riduce a zero la capacità di calcolo del servizio. Quando vuoi eseguire nuovamente l'applicazione, puoi riprendere il servizio App Runner. App Runner fornisce una nuova capacità di calcolo, implementa l'applicazione su di essa ed esegue l'applicazione.

Important

App Runner ti verrà fatturato solo se è in esecuzione. Pertanto, potrai sospendere e riprendere l'applicazione secondo necessità per gestire i costi. Ciò è particolarmente utile negli scenari di sviluppo e test.

Sospensione del servizio App Runner

1. Aprire AWS Explorer, se non è già aperto.
2. Espandi App Runner per visualizzare l'elenco dei servizi.
3. Fai clic con il pulsante destro del mouse sul servizio e scegli Pause (Metti in pausa).
4. Nella finestra di dialogo visualizzata, scegli Sospendi.

Mentre il servizio viene messo in pausa, lo stato del servizio cambia da In esecuzione a In Operazione in corso e infine a Sospeso.

Come riprendere il servizio App Runner

1. Aprire AWS Explorer, se non è già aperto.
2. Espandi App Runner per visualizzare l'elenco dei servizi.
3. Fai clic con il pulsante destro del mouse sul servizio e scegli Resume (Riprendi).

4. Nella finestra di dialogo visualizzata, scegli Riprendi.

Mentre il servizio viene ripreso, lo stato del servizio cambia da Sospeso a In Operazione in corso e infine a In esecuzione.

Implementazione dei servizi App Runner

Se scegli l'opzione di implementazione manuale per il servizio, è necessario avviare esplicitamente ogni implementazione sul servizio.

1. Aprire AWS Explorer, se non è già aperto.
2. Espandi App Runner per visualizzare l'elenco dei servizi.
3. Fai clic con il pulsante destro del mouse sul servizio e scegli Implementa.
4. Mentre l'applicazione viene implementata, lo stato del servizio cambia da Operazione in corso a In esecuzione.
5. Per verificare che l'applicazione sia stata implementata correttamente, fai clic con il pulsante destro del mouse sullo stesso servizio e scegli Copy Service URL (Copia URL del servizio).
6. Per accedere all'applicazione Web implementata, incolla l'URL copiato nella barra degli indirizzi del browser Web.

Visualizzazione dei flussi di log per App Runner

Utilizza File di log CloudWatch per monitorare, archiviare e accedere ai flussi di log per servizi quali App Runner. File di log CloudWatch registra due tipi distinti di file di log: log eventi e flussi di log. I log eventi sono record di attività registrati dall'applicazione o dalla risorsa monitorata tramite File di log CloudWatch. Un flusso di log è una sequenza di log eventi che condividono la stessa origine.

È possibile accedere ai due seguenti tipi di flussi di log per App Runner:

- Flussi di log del servizio: contiene l'output di registrazione generato da App Runner. Per questo tipo di flusso di log, i log eventi sono record relativi al modo in cui App Runner gestisce il servizio e agisce su di esso.
- Flussi di log dell'applicazione: contiene l'output del codice dell'applicazione in esecuzione.

1. Espandi App Runner per visualizzare l'elenco dei servizi
2. Fai clic con il pulsante destro del mouse su un servizio e scegli una delle opzioni seguenti:

- Visualizza i flussi di log del servizio
- Visualizza i flussi di log dell'applicazione

Il riquadro Flussi di log visualizza i log eventi che costituiscono il flusso di log.

3. Per visualizzare ulteriori informazioni su un evento specifico, fai clic con il pulsante destro del mouse e scegli Esporta flusso di log, Apri nell'editor oppure Esporta flusso di log, Salva in un file.

Eliminazione di servizi App Runner

Important

Se elimini il servizio App Runner, questo viene rimosso in modo permanente e i dati archiviati vengono eliminati. Se devi ricreare il servizio, App Runner deve recuperare nuovamente il tuo sorgente e crearlo daccapo se si tratta di un repository di codice. La tua applicazione Web ottiene un nuovo dominio App Runner.

1. Aprire AWS Explorer, se non è già aperto.
2. Espandi App Runner per visualizzare l'elenco dei servizi.
3. Fai clic con il pulsante destro del mouse su un servizio e scegli Delete Service (Elimina servizio).
4. Nella finestra di dialogo di conferma, digita delete me, quindi scegli OK.

Il servizio eliminato si troverà nello stato Operazione in corso, poi scomparirà dall'elenco.

Amazon CodeCatalyst per JetBrains

Cos'è Amazon CodeCatalyst?

Amazon CodeCatalyst è uno spazio di collaborazione basato su cloud per i team di sviluppo software. Tramite il Kit di strumenti AWS per JetBrains Gateway, è possibile visualizzare e gestire le proprie risorse CodeCatalyst direttamente da JetBrains Gateway. È inoltre possibile utilizzare il Kit di strumenti per avviare, gestire e modificare gli ambienti di elaborazione virtuali di Ambienti di sviluppo. Per ulteriori informazioni su CodeCatalyst, consulta la Guida per l'utente di [Amazon CodeCatalyst](#).

Nei seguenti argomenti viene descritto come connettere il Kit di strumenti AWS per JetBrains Gateway con CodeCatalyst e come lavorare con CodeCatalyst tramite JetBrains Gateway.

Argomenti

- [Nozioni di base su CodeCatalyst e il AWS Toolkit for JetBrains](#)
- [Utilizzo di Amazon CodeCatalyst in JetBrains Gateway](#)

Nozioni di base su CodeCatalyst e il AWS Toolkit for JetBrains

Per iniziare a lavorare con CodeCatalyst da JetBrains Gateway, completa le operazioni seguenti.

Argomenti

- [Installazione di JetBrains Gateway](#)
- [Installazione del Kit di strumenti AWS per JetBrains Gateway](#)
- [Creazione di un account CodeCatalyst e un ID Builder AWS](#)
- [Connessione di JetBrains Gateway con CodeCatalyst](#)

Installazione di JetBrains Gateway

Prima di integrare il Kit di strumenti AWS con i tuoi account CodeCatalyst, assicurati di utilizzare una versione aggiornata di JetBrains Gateway. Per scaricare l'ultima versione di JetBrains Gateway, scegli la distribuzione JetBrains Gateway desiderata dai seguenti link:

- [JetBrains Gateway per Linux](#)
- [JetBrains Gateway per Windows](#)
- [JetBrains Gateway per macOS](#)
- [JetBrains Gateway per macOS Apple Silicon](#)

Installazione del Kit di strumenti AWS per JetBrains Gateway

Per connettere JetBrains al tuo account CodeCatalyst, devi installare l'ultima versione dell'estensione del kit di strumenti. È possibile trovare la versione più recente e completare l'installazione del kit di strumenti direttamente da Plugins Marketplace di JetBrains.

Per installare il plug-in del Kit di strumenti AWS da Plugins Marketplace di JetBrains, completa i seguenti passaggi:

1. Dalla schermata principale di JetBrains Gateway, scegli l'icona Settings/Preferences, che si trova nell'angolo in basso a sinistra dell'applicazione.
2. Scegli Settings/Preferences per aprire la visualizzazione Settings/Preferences.
3. Dalla visualizzazione Settings/Preferences, scegli Plugins per aprire il menu Plugins.

 Note

La visualizzazione Plugins può essere aperta sia nella visualizzazione Marketplace sia nella visualizzazione Installed.

- Se è la prima volta che installi il Kit di strumenti AWS per JetBrains Gateway, seleziona la visualizzazione Plugins Marketplace per continuare.
- Se disponi di una versione precedente del Kit di strumenti AWS per JetBrains Gateway, esegui l'aggiornamento dalla visualizzazione Installed.

4. Dalla visualizzazione del Marketplace, inserisci il testo AWS Toolkit e seleziona la voce del plug-in AWS Toolkit quando appare.
5. Scegli Install per scaricare e installare il Kit di strumenti AWS per JetBrains Gateway.

 Note

JetBrains Gateway mostra lo stato del download e dell'avanzamento dell'installazione. Dopo aver installato correttamente il kit di strumenti, l'esploratore Connections di JetBrains Gateway si aggiorna con l'icona del plug-in di Amazon CodeCatalyst.

Creazione di un account CodeCatalyst e un ID Builder AWS

Oltre a installare la versione più recente del AWS Toolkit for JetBrains, è necessario avere un ID Builder AWS e un account CodeCatalyst per eseguire la connessione con JetBrains Gateway. Se non disponi di un ID Builder AWS o un account CodeCatalyst attivo, consulta la sezione [Setting up CodeCatalyst](#) della Guida per l'utente di CodeCatalyst.

 Note

Un ID Builder AWS è diverso dalle credenziali di AWS. AWS La maggior parte dei Servizi AWS che sono accessibili dal Kit di strumenti AWS richiede le credenziali. Un ID Builder AWS è necessario per creare un nuovo account CodeCatalyst e utilizzare un account CodeCatalyst

esistente. Ciò include l'utilizzo di tutte le funzionalità di CodeCatalyst disponibili nel Kit di strumenti AWS.

Connessione di JetBrains Gateway con CodeCatalyst

Per connettere JetBrains Gateway con il tuo account CodeCatalyst, completa i seguenti passaggi.

1. Dall'esploratore Connections di JetBrains Gateway, scegli il plug-in Amazon CodeCatalyst per aprire la visualizzazione Amazon CodeCatalyst.
2. Dalla visualizzazione del plug-in CodeCatalyst, scegli Accedi con ID Builder AWS per aprire il prompt È richiesto l'accesso ad AWS.
3. Dal prompt È richiesto l'accesso ad AWS, scegli Apri il browser per aprire la schermata di accesso alla console CodeCatalyst nel tuo browser Web preferito.
4. Inserisci l'ID Builder AWS nell'apposito campo e segui le istruzioni per continuare.
5. Quando richiesto, scegli Consenti per confermare la connessione tra JetBrains e il tuo account CodeCatalyst. Quando il processo di connessione è completo, CodeCatalyst visualizza una conferma che indica che è possibile chiudere il browser.
6. Da JetBrains Gateway, la visualizzazione del plug-in CodeCatalyst viene aggiornata alla visualizzazione Dev Environments.

Utilizzo di Amazon CodeCatalyst in JetBrains Gateway

È possibile avviare un ambiente di elaborazione virtuale, noto come ambiente di sviluppo, da JetBrains. Gli ambienti di sviluppo sono ambienti di sviluppo cloud personalizzabili che puoi copiare e condividere tra i diversi membri del team nel tuo spazio. Per ulteriori informazioni sugli ambienti di sviluppo e su come accedervi da CodeCatalyst, consulta la sezione [Dev Environments](#) della Guida per l'utente di Amazon CodeCatalyst.

Nelle sezioni seguenti viene descritto come creare, aprire e utilizzare gli ambienti di sviluppo da JetBrains Gateway.

Argomenti

- [Apertura di un ambiente di sviluppo](#)
- [Creazione di un ambiente di sviluppo](#)
- [Creazione di un ambiente di sviluppo da un repository di terze parti](#)

- [Configurazione delle impostazioni dell'ambiente di sviluppo](#)
- [Sospensione di un ambiente di sviluppo](#)
- [Ripresa del lavoro in un ambiente di sviluppo](#)
- [Eliminazione di un ambiente di sviluppo](#)
- [Configurazione delle impostazioni predefinite degli ambienti di sviluppo](#)

Apertura di un ambiente di sviluppo

Per aprire un ambiente di sviluppo esistente da JetBrains Gateway, completa i seguenti passaggi.

1. Dall'esploratore Connections, scegli il plug-in Amazon CodeCatalyst.
2. Dal corpo della procedura guidata Sviluppo remoto, accedi allo spazio principale e progetta l'ambiente di sviluppo che desideri aprire.
3. Scegli l'ambiente di sviluppo che desideri aprire.
4. Verifica il processo di apertura dell'ambiente di sviluppo per continuare.

Note

JetBrains mostra l'avanzamento in una nuova finestra di stato. Quando il processo di apertura è completo, l'ambiente di sviluppo si apre in una nuova finestra.

Creazione di un ambiente di sviluppo

Per creare un nuovo ambiente di sviluppo:

1. Dall'esploratore Connections, scegli il plug-in CodeCatalyst.
2. Dalla sezione Sviluppo in remoto dell'intestazione della procedura guidata, seleziona il link Crea un ambiente di sviluppo per aprire la visualizzazione Nuovo ambiente di sviluppo CodeCatalyst.
3. Dalla visualizzazione Nuovo ambiente di sviluppo CodeCatalyst, utilizza i seguenti campi per configurare le preferenze dell'ambiente di sviluppo.
 - IDE: seleziona il tuo IDE JetBrains preferito da avviare all'interno dell'ambiente di sviluppo.
 - Progetto CodeCatalyst: scegli uno spazio e un progetto CodeCatalyst per l'ambiente di sviluppo.

- Alias dell'ambiente di sviluppo: inserisci un nome alternativo per l'ambiente di sviluppo.
 - Calcolo: scegli la configurazione hardware virtuale per l'ambiente di sviluppo.
 - Archiviazione persistente: scegli la quantità di archiviazione persistente per l'ambiente di sviluppo.
 - Timeout per inattività: scegli il tempo di inattività del sistema che può trascorrere prima che l'ambiente di sviluppo entri in standby.
4. Per creare l'ambiente di sviluppo, scegli Crea ambiente di sviluppo.

Note

Quando scegli Crea ambiente di sviluppo, la visualizzazione Nuovo ambiente di sviluppo si chiude e inizia il processo di creazione dell'ambiente di sviluppo. Il processo può richiedere diversi minuti e non è possibile utilizzare altre funzionalità di JetBrains Gateway finché la creazione dell'ambiente di sviluppo non viene ultimata. JetBrains mostra l'avanzamento in una nuova finestra di stato. Quando il processo è completo, l'ambiente di sviluppo si apre in una nuova finestra.

Creazione di un ambiente di sviluppo da un repository di terze parti

È possibile creare ambienti di sviluppo da un repository di terze parti connettendosi al repository come origine.

La connessione a un repository di terze parti come origine viene gestita a livello di progetto in CodeCatalyst. Per istruzioni e dettagli aggiuntivi su come connettere un repository di terze parti a un ambiente di sviluppo, consulta l'argomento [Linking a source repository](#) della Guida per l'utente di Amazon CodeCatalyst.

Configurazione delle impostazioni dell'ambiente di sviluppo

Per modificare le impostazioni per un ambiente di sviluppo esistente da JetBrains Gateway, completa i seguenti passaggi.

Note

Non è possibile modificare la quantità di spazio di archiviazione assegnata all'ambiente di sviluppo dopo averlo creato.

1. Dall'esploratore Connections, scegli il plug-in Amazon CodeCatalyst.
2. Dal corpo della procedura guidata Sviluppo remoto, accedi allo spazio principale e progetta l'ambiente di sviluppo che desideri configurare.
3. Scegli l'icona Impostazioni accanto all'ambiente di sviluppo che desideri configurare per aprire le impostazioni Configura l'ambiente di sviluppo:.
4. Dal menu delle impostazioni Configura l'ambiente di sviluppo:, configura l'ambiente di sviluppo modificando le seguenti opzioni:
 - Alias dell'ambiente di sviluppo: campo facoltativo per specificare un nome alternativo per l'ambiente di sviluppo.
 - IDE: scegli l'IDE JetBrains che desideri avviare all'interno del tuo ambiente di sviluppo.
 - Calcolo: scegli la configurazione hardware virtuale per l'ambiente di sviluppo.
 - Timeout per inattività: scegli il tempo di inattività del sistema che può trascorrere prima che l'ambiente di sviluppo entri in standby.

Sospensione di un ambiente di sviluppo

L'attività nel tuo ambiente di sviluppo viene archiviata in modo persistente. Ciò significa che puoi sospendere l'ambiente di sviluppo e riprendere l'attività in seguito senza perdere il lavoro.

Per sospendere l'ambiente di sviluppo, completa i seguenti passaggi.

1. Dall'esploratore Connections, scegli il plug-in Amazon CodeCatalyst.
2. Dal corpo della procedura guidata Sviluppo remoto, accedi allo spazio principale e al progetto dell'ambiente di sviluppo che desideri sospendere.
3. Scegli l'icona Sospendi accanto all'ambiente di sviluppo attivo per aprire la finestra di dialogo Conferma sospensione.
4. Scegli Sì per chiudere la finestra di dialogo Conferma sospensione e avviare il processo di sospensione.

Note

JetBrains mostra l'avanzamento del processo di sospensione in una nuova finestra di stato. Quando l'ambiente di sviluppo è stato arrestato, l'icona Sospendi viene rimossa dall'interfaccia utente.

Ripresa del lavoro in un ambiente di sviluppo

L'attività nel tuo ambiente di sviluppo viene archiviata in modo persistente. Ciò significa che puoi riprendere un ambiente di sviluppo precedentemente sospeso senza perdere il lavoro.

Per riprendere un ambiente di sviluppo sospeso, completa i seguenti passaggi.

1. Dall'esploratore Connections, scegli il plug-in Amazon CodeCatalyst.
2. Dal corpo della procedura guidata Sviluppo remoto, accedi allo spazio principale e progetta l'ambiente di sviluppo che desideri riprendere.
3. Scegli l'ambiente di sviluppo che desideri riprendere.

Note

JetBrains mostra l'avanzamento del processo di ripresa in una nuova finestra di stato. Quando l'ambiente di sviluppo è ripreso, l'icona Sospendi viene aggiunta accanto all'icona Impostazioni dell'ambiente di sviluppo.

Eliminazione di un ambiente di sviluppo

Per eliminare l'ambiente di sviluppo, completa i seguenti passaggi:

1. Dall'esploratore Connections, scegli il plug-in Amazon CodeCatalyst.
2. Dal corpo della procedura guidata Sviluppo remoto, accedi allo spazio principale e progetta l'ambiente di sviluppo che desideri eliminare.
3. Seleziona il pulsante icona X accanto al tuo ambiente di sviluppo per aprire la finestra di dialogo Conferma eliminazione.
4. Scegli Sì per chiudere la finestra di dialogo ed eliminare l'ambiente di sviluppo.

Important

Dopo aver scelto Sì, l'ambiente di sviluppo viene eliminato e non può essere recuperato. Prima di eliminare un ambiente di sviluppo, assicurati di eseguire il commit e inviare le modifiche al codice nel repository di origine iniziale. In caso contrario, le modifiche non salvate andranno perse definitivamente.

Dopo l'eliminazione di un ambiente di sviluppo, la procedura guidata Sviluppo in remoto si aggiorna e l'ambiente di sviluppo non è più elencato nelle tue risorse.

Configurazione delle impostazioni predefinite degli ambienti di sviluppo

È possibile configurare le impostazioni predefinite dell'ambiente di sviluppo nel **devfile** dell'ambiente di sviluppo. La specifica **devfile** è uno standard aperto che è possibile aggiornare in un documento YAML.

Per ulteriori informazioni su come definire e configurare i **devfile**, consulta la pagina [devfile.io](#).

Per aprire e modificare un **devfile** da un'istanza dell'ambiente di sviluppo di JetBrains Gateway, completa i seguenti passaggi.

1. Dalla Barra di navigazione nell'ambiente di sviluppo JetBrains attivo, espandi il nodo Ambiente di sviluppo Amazon CodeCatalyst per aprire il menu Dettagli sullo stato del back-end.
2. Scegli la scheda Configura l'ambiente di sviluppo, quindi scegli Apri Devfile per aprire il **devfile** nell'Editor di JetBrains.
3. Dall'Editor, apporta modifiche al **devfile** e salva il tuo lavoro.
4. Dopo aver salvato le modifiche, il nodo Ambiente di sviluppo Amazon CodeCatalyst visualizza un avviso che indica che l'ambiente di sviluppo richiede la ricostruzione.
5. Espandi il nodo Ambiente di sviluppo Amazon CodeCatalyst e scegli il nodo Ricostruisci l'ambiente di sviluppo dalla scheda Configura l'ambiente di sviluppo.

Utilizzo di AWS CloudFormation tramite il AWS Toolkit for JetBrains

Negli argomenti seguenti viene descritto come usare AWS Toolkit for JetBrains per utilizzare gli stack AWS CloudFormation in un account AWS.

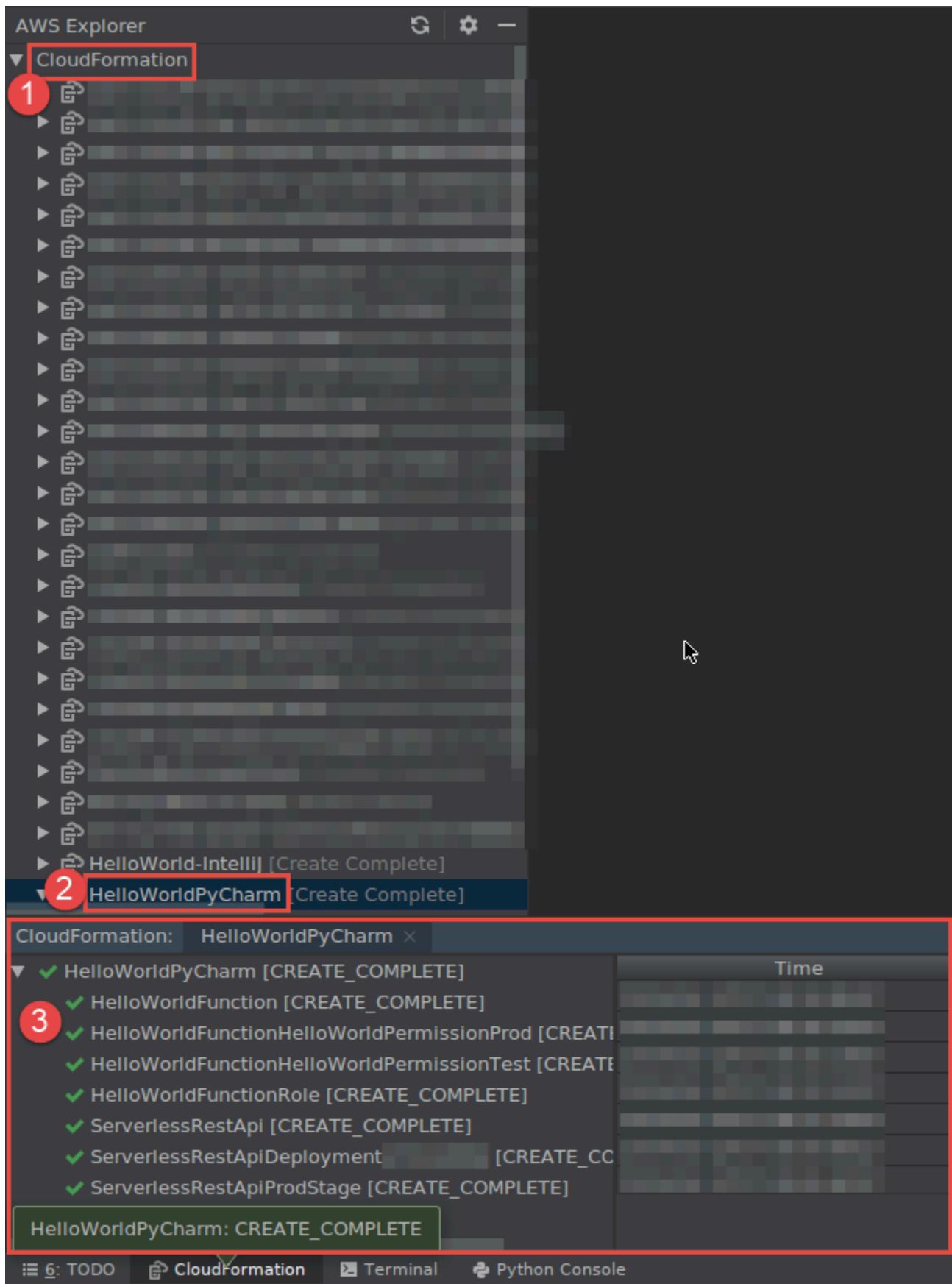
Argomenti

- [Visualizzazione dei log eventi per uno stack AWS CloudFormation tramite il AWS Toolkit for JetBrains](#)
- [Eliminazione di uno stack AWS CloudFormation tramite il AWS Toolkit for JetBrains](#)

Visualizzazione dei log eventi per uno stack AWS CloudFormation tramite il AWS Toolkit for JetBrains

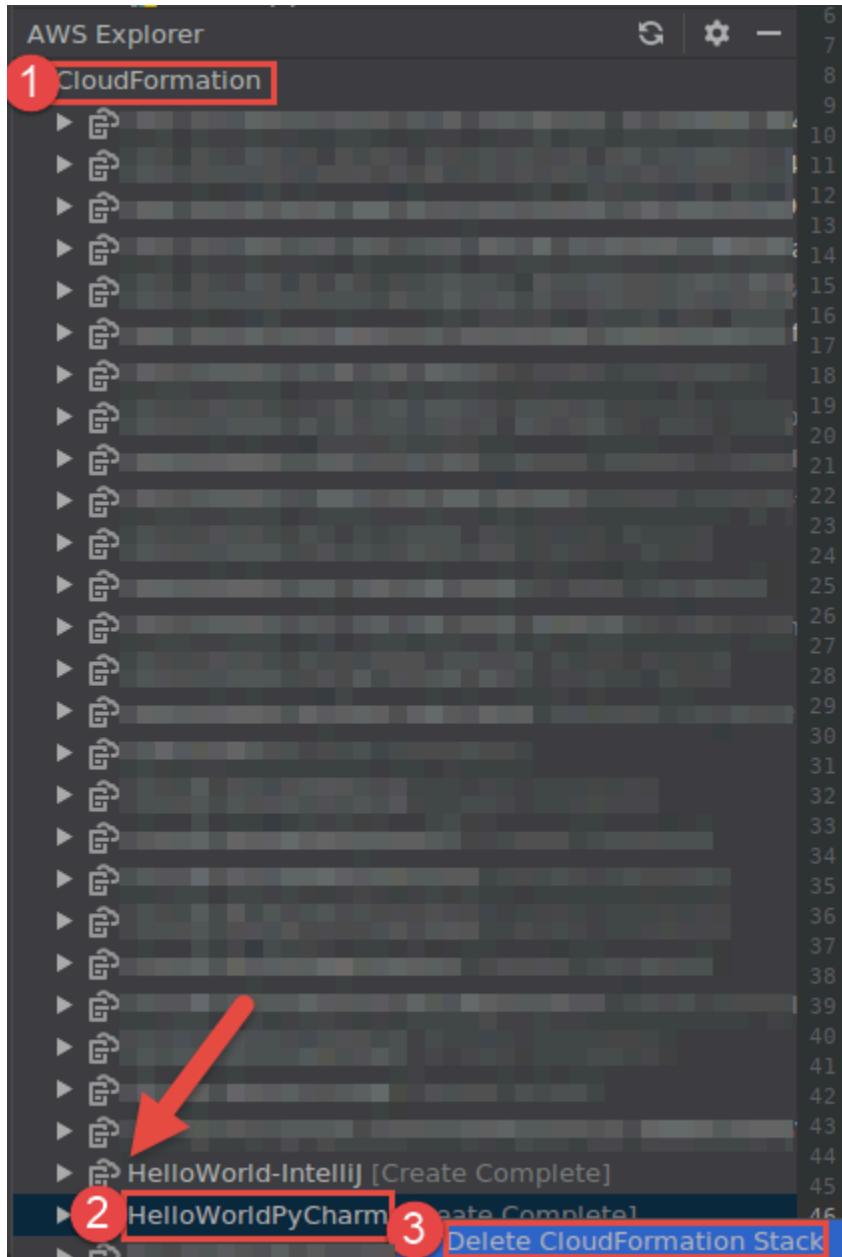
1. Aprire AWS Explorer, se non è già aperto. Se lo stack si trova in una regione AWS diversa da quella corrente, passa alla regione AWS che lo contiene.
2. Espandere CloudFormation.
3. Per visualizzare i registri eventi per lo stack, fare clic con il pulsante destro del mouse sul nome dello stack. AWS Toolkit for JetBrains visualizza i registri eventi nella finestra dello strumento CloudFormation.

Per nascondere o mostrare la finestra dello strumento CloudFormation nel menu principale, scegliere View (Visualizza), Tool Windows (Finestre degli strumenti), CloudFormation.



Eliminazione di uno stack AWS CloudFormation tramite il AWS Toolkit for JetBrains

1. Aprire AWS Explorer, se non è già aperto. Se devi passare alla regione AWS che contiene lo stack, esegui subito l'operazione.
2. Espandere CloudFormation.
3. Fare clic con il pulsante destro del mouse sul nome dello stack da eliminare, quindi scegliere Delete CloudFormation Stack (Elimina stack CloudFormation).



4. Immettere il nome dello stack per confermare che è stato eliminato, quindi scegliere OK. Se l'eliminazione dello stack ha esito positivo, AWS Toolkit for JetBrains rimuove il nome dello stack dall'elenco CloudFormation in AWS Explorer. Se l'eliminazione dello stack non riesce, è possibile risolvere i problemi visualizzando i registri eventi per lo stack.

Utilizzo di File di log CloudWatch tramite il AWS Toolkit for JetBrains

Amazon CloudWatch Logs consente di centralizzare i registri da tutti i sistemi, applicazioni e servizi AWS utilizzati in un unico servizio altamente scalabile. È quindi possibile visualizzarli facilmente, ricercarli per codici di errore o modelli specifici, filtrarli in base a campi specifici o archiviarli in modo sicuro per analisi future. Per ulteriori informazioni, consulta [Cos'è Amazon CloudWatch Logs](#) nella Guida per l'utente di Amazon CloudWatch.

Negli argomenti seguenti viene descritto come utilizzare il AWS Toolkit for JetBrains per lavorare con File di log CloudWatch in un account AWS.

Argomenti

- [Visualizzazione dei gruppi di log e dei flussi di log di CloudWatch tramite il AWS Toolkit for JetBrains](#)
- [Utilizzo dei log eventi di CloudWatch nei flussi di log tramite il AWS Toolkit for JetBrains](#)
- [Utilizzo di Logs Insights di CloudWatch tramite il AWS Toolkit for JetBrains](#)

Visualizzazione dei gruppi di log e dei flussi di log di CloudWatch tramite il AWS Toolkit for JetBrains

Un flusso di log è una sequenza di eventi di log che condividono la stessa origine. Ciascuna origine di registri separata in CloudWatch Logs costituisce un flusso di log distinto.

Un gruppo di log è un gruppo di flussi di log che condividono le stesse impostazioni di conservazione, monitoraggio e controllo degli accessi. Puoi definire i gruppi di log e specificare quali flussi inserire in ciascun gruppo. Non vi è alcun limite al numero di flussi di log che possono appartenere a un gruppo di log.

Per ulteriori informazioni, consulta la pagina [Working with Log Groups and Log Streams](#) della Guida per l'utente di Amazon CloudWatch.

Argomenti

- [Visualizzazione dei gruppi di registro log e dei flussi di registro con il nodo CloudWatch Logs](#)
- [Visualizzazione dei flussi di log con il nodo Lambda](#)
- [Visualizzazione dei flussi di log con il nodo Amazon ECS](#)

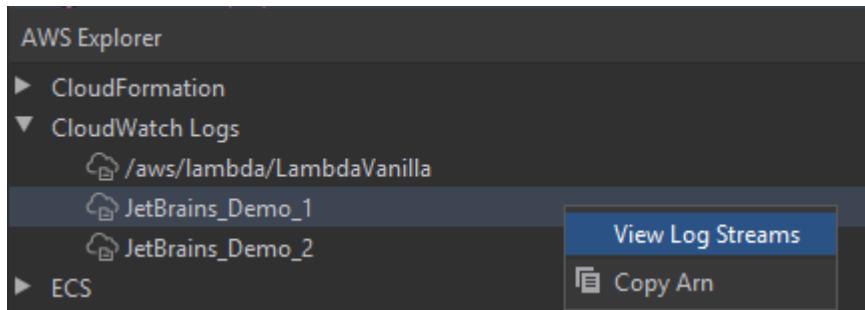
Visualizzazione dei gruppi di registro log e dei flussi di registro con il nodo CloudWatch Logs

1. Aprire AWS Explorer, se non è già aperto.
2. Fai clic sul nodo File di log CloudWatch per espandere l'elenco dei gruppi di log.

I gruppi di log per la [regione AWS corrente](#) vengono visualizzati sotto il nodo File di log CloudWatch.

3. Per visualizzare i flussi di log in un gruppo di log, effettua una delle seguenti operazioni:
 - Fai doppio clic sul gruppo di log.
 - Fai clic con il pulsante destro del mouse su un gruppo di log e scegli Visualizza flussi di log.

I contenuti del gruppo di log vengono visualizzati nel riquadro Flussi di log. Per informazioni sull'interazione con i log eventi in ogni flusso, consulta [Utilizzo dei log eventi di CloudWatch](#).



Visualizzazione dei flussi di log con il nodo Lambda

È possibile visualizzare File di log CloudWatch per le funzioni AWS Lambda tramite il nodo Lambda nell'Esploratore AWS.

Nota

È inoltre possibile visualizzare i flussi di log per tutti i servizi AWS, incluse le funzioni Lambda, che utilizzano il nodo File di log CloudWatch nell'Esploratore AWS. Tuttavia, per una panoramica dei dati di log specifici delle funzioni Lambda, ti consigliamo di utilizzare il nodo Amazon ECS.

1. Aprire AWS Explorer, se non è già aperto.
2. Fai clic sul nodo Lambda per espandere l'elenco delle funzioni Lambda.

Le funzioni Lambda per la [regione AWS corrente](#) vengono visualizzati sotto il nodo Lambda.

3. Fai clic con il pulsante destro del mouse su una funzione Lambda, quindi scegli Visualizza flussi di log.

I flussi di log relativi alla funzione vengono visualizzati nel riquadro Flussi di log. Per informazioni sull'interazione con i log eventi in ogni flusso, consulta [Utilizzo dei log eventi di CloudWatch](#).

Visualizzazione dei flussi di log con il nodo Amazon ECS

È possibile visualizzare File di log CloudWatch per cluster e container eseguiti e gestiti in Amazon Elastic Container Service tramite il nodo Amazon ECS nell'Esploratore AWS.

Nota

È inoltre possibile visualizzare i gruppi di log per tutti i servizi AWS, incluso Amazon ECS, che utilizzano il nodo File di log CloudWatch nell'Esploratore AWS. Tuttavia, per una panoramica dei dati di log specifici dei cluster e dei container Amazon ECS, ti consigliamo di utilizzare il nodo Amazon ECS.

1. Aprire AWS Explorer, se non è già aperto.
2. Fai clic sul nodo Amazon ECS per espandere l'elenco dei cluster Amazon ECS.

I cluster Amazon ECS per la [regione AWS corrente](#) vengono visualizzati sotto il nodo Amazon ECS.

3. Fai clic con il pulsante destro del mouse su un cluster, quindi scegli Visualizza flussi di log.

I flussi di log relativi al cluster vengono visualizzati nel riquadro Flussi di log.

4. Per visualizzare i flussi di log per un container specifico, fai clic su un cluster per espandere l'elenco dei container registrati.

I container registrati per il cluster sono visualizzati sotto.

5. Fai clic con il pulsante destro del mouse su un container, quindi scegli Visualizza flusso di log del container.

I flussi di log relativi al container vengono visualizzati nel riquadro Flussi di log. Per informazioni sull'interazione con i log eventi per cluster e container, consulta la pagina [Utilizzo dei log eventi di CloudWatch](#).

Utilizzo dei log eventi di CloudWatch nei flussi di log tramite il AWS Toolkit for JetBrains

Dopo aver aperto la finestra Flussi di log, puoi accedere ai log eventi in ogni flusso. Un log eventi è una serie di registri di attività registrate dall'applicazione o dalla risorsa monitorata.

Argomenti

- [Visualizzazione e filtraggio dei log eventi in un flusso](#)
- [Utilizzo delle operazioni sui log](#)
- [Esportazione dei log eventi di CloudWatch in un file o un editor](#)

Visualizzazione e filtraggio dei log eventi in un flusso

Quando apri un flusso di log, nella finestra Flusso di log, viene visualizzata la sequenza dei log eventi di tale flusso.

1. Per trovare un flusso di log da visualizzare, apri il riquadro Flusso di log (consulta la pagina [Visualizzazione dei gruppi di registro log e dei flussi di registro CloudWatch](#)).

Nota

È possibile utilizzare la corrispondenza del modello per individuare un flusso in un elenco. Fai clic sul riquadro Flussi di log e inizia a inserire il testo. Viene evidenziato il

primo flusso di log con il testo corrispondente al tuo. È inoltre possibile riordinare l'elenco facendo clic sulla parte superiore della colonna Ora dell'ultimo evento.

- Fai doppio clic su un flusso di log per visualizzarne la sequenza dei log eventi.

Il riquadro Log eventi visualizza i log eventi che costituiscono il flusso di log.

- Per filtrare i log eventi in base al contenuto, inserisci il testo nel campo Filtra flusso di log e premi Restituisci.

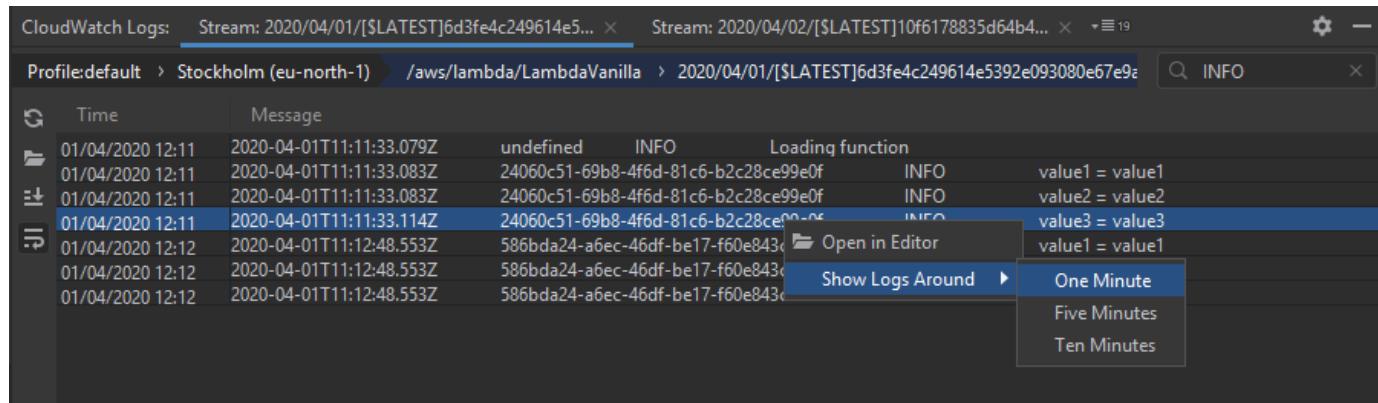
I risultati sono log eventi contenenti il testo corrispondente al testo del filtro che hai inserito, facendo distinzione tra maiuscole e minuscole. Il filtro esegue la ricerca nell'intero flusso di log, inclusi gli eventi non visualizzati sullo schermo.

Note

È inoltre possibile utilizzare la corrispondenza del modello per individuare un log eventi nel riquadro. Fai clic sul riquadro Log eventi e inizia a inserire il testo. Viene evidenziato il primo log eventi con il testo corrispondente al tuo. A differenza della ricerca Filtra flusso di log, vengono controllati solo gli eventi sullo schermo.

- Per filtrare i log eventi in base all'ora, fai clic con il pulsante destro del mouse su un log eventi, quindi scegli Mostra log.

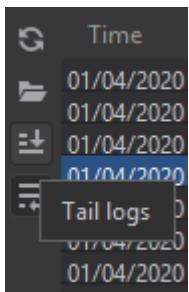
È possibile selezionare Un minuto, Cinque minuti oppure Dieci minuti. Ad esempio, se si seleziona Cinque minuti, l'elenco filtrato mostra solo i log eventi che si sono verificati cinque minuti prima e dopo la voce selezionata.



Sulla sinistra del riquadro Log eventi, le [operazioni sui log](#) offrono ulteriori modi per interagire con i log eventi.

Utilizzo delle operazioni sui log

Sulla sinistra del riquadro Log eventi, quattro operazioni di log consentono di aggiornare, modificare, aggiungere code e mandare a capo i log eventi di CloudWatch.



1. Per trovare i log eventi con cui interagire, [apri il riquadro Flussi di log](#).
2. Scegli una delle seguenti operazioni sui log:
 - Aggiorna: aggiorna l'elenco con i log eventi che si sono verificati dopo che è stato aperto il riquadro Log eventi.
 - Apri nell'editor: apre i log eventi sullo schermo nell'editor predefinito dell'IDE.

Note

Questa operazione esporta solo i log eventi visualizzati sullo schermo nell'editor IDE. Per visualizzare tutti gli eventi del flusso nell'editor, scegli l'opzione [Esporta flusso di log](#).

- Log di coda: trasmette i nuovi log eventi al riquadro Log eventi. Questa è una funzionalità utile per gli aggiornamenti continui su servizi a lunga durata come le istanze Amazon EC2 e le build AWS CodeBuild.
- Manda a capo i log: visualizza il testo dei log eventi su più righe se le dimensioni del riquadro nascondono voci più lunghe.

Esportazione dei log eventi di CloudWatch in un file o un editor

L'esportazione di un flusso di log di CloudWatch consente di aprire i log eventi nell'editor predefinito dell'IDE o di scaricarli in una cartella locale.

1. Per trovare un flusso di log a cui accedere, [apri il riquadro Flussi di log](#).

- Fai clic con il pulsante destro del mouse su un flusso di log, quindi scegli Esporta flusso di log, Apri nell'editor o Esporta flusso di log, Salva in un file.

- Apri nell'editor: apre i log eventi che costituiscono il flusso selezionato nell'editor predefinito dell'IDE.

 Note

Questa opzione esporta tutti gli eventi nel flusso di log nell'editor dell'IDE.

- Salva in un file: apre la finestra di dialogo Scarica flusso di log. Ciò consente di selezionare una cartella per il download e rinominare il file contenente i log eventi.

Utilizzo di Logs Insights di CloudWatch tramite il AWS Toolkit for JetBrains

È possibile utilizzare il AWS Toolkit for JetBrains per lavorare con Logs Insights di CloudWatch. Logs Insights di CloudWatch consente di eseguire ricerche interattive e analizzare i dati di log in File di log Amazon CloudWatch. Per ulteriori informazioni, consulta la pagina [Analyzing Log Data with CloudWatch Logs Insights](#) della Guida per l'utente di File di log Amazon CloudWatch.

Autorizzazioni IAM per Logs Insights di CloudWatch

Per eseguire e visualizzare i risultati delle query di Logs Insights di CloudWatch sono necessarie le seguenti autorizzazioni:

```
{  
    "Version": "2012-10-17",  
    "Statement" : [  
        {  
            "Effect" : "Allow",  
            "Action" : [  
                "logs:StartQuery",  
                "logs:GetQueryResults",  
                "logs:GetLogRecord",  
                "logs:describeLogGroups",  
                "logs:describeLogStreams"  
            ],  
            "Resource" : "*"  
        }  
    ]}
```

```
}
```

Le seguenti autorizzazioni non sono richieste, ma consentiranno al AWS Toolkit for JetBrains di interrompere automaticamente tutte le query attualmente in esecuzione quando si chiude il riquadro dei risultati o l'IDE associato.

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Utilizzo di Logs Insights di CloudWatch

Apertura dell'editor di query di Logs Insights di CloudWatch

1. Apri l'Esploratore AWS.
2. Fai doppio clic sul nodo File di log CloudWatch per espandere l'elenco dei gruppi di log.
3. Fate clic con il pulsante destro del mouse sul gruppo di log che desideri aprire, quindi scegli Apri editor di query.

Avvio di una query di Logs Insights di CloudWatch

1. Nella finestra Query sui gruppi di log, modifica i parametri di query come desiderato.

È possibile scegliere un intervallo di tempo per data oppure ora relativa.

Il campo Gruppi di log di query accetta la sintassi delle query di Logs Insights di CloudWatch. Per ulteriori informazioni, consulta la pagina [CloudWatch Logs Insights Query Syntax](#) della Guida per l'utente di File di log Amazon CloudWatch.

2. Scegli Esegui per iniziare la query.

Salvataggio di una query di Logs Insights di CloudWatch

1. Digita il nome della query.
2. Scegli Salva query.

I gruppi di log e la query selezionati vengono salvati nell'account AWS. Gli intervalli di tempo non vengono salvati.

È possibile recuperare e riutilizzare le query salvate dalla pagina della Console di gestione AWS di Logs Insights di CloudWatch.

Recupero di una query salvata di Logs Insights di CloudWatch

1. Nella finestra Query sui gruppi di log, scegli Recupera query salvate.
2. Scegli la query desiderata e seleziona OK.

I gruppi di log e la query selezionati sostituiscono ogni campo nella finestra di dialogo esistente.

Esplorazione dei risultati delle query

- Nella finestra Risultati delle query di Logs Insights di CloudWatch, nell'angolo in alto a destra, scegli Apri editor di query.

Visualizzazione di un singolo record di log

- Nel riquadro dei risultati della query, fai doppio clic su una riga per aprire una nuova scheda con i dettagli su tale record di log.

È inoltre possibile accedere al flusso di log associato al record di log scegliendo Visualizza flusso di log nell'angolo in alto a destra.

Utilizzo di Amazon CodeWhisperer

Che cos'è CodeWhisperer?

Amazon CodeWhisperer è un generatore di codice generico basato sul machine learning che fornisce suggerimenti di codice in tempo reale. Mentre scrivi codice, CodeWhisperer genera automaticamente suggerimenti basati sul codice e sui commenti esistenti. I tuoi suggerimenti personalizzati possono variare in termini di estensione e ambito, spaziando da un commento di una singola riga a intere funzioni.

CodeWhisperer può anche scansionare il codice per evidenziare e definire problemi di sicurezza.

CodeWhisperer è disponibile per i seguenti prodotti JetBrains:

- IntelliJ IDEA
- PyCharm
- WebStorm
- Rider

Per ulteriori informazioni, consulta la [Guida per l'utente di Amazon CodeWhisperer](#).

Amazon DynamoDB nel AWS Toolkit for JetBrains

Amazon DynamoDB è un servizio di database NoSQL interamente gestito che combina prestazioni prevedibili con una scalabilità ottimale. Per informazioni dettagliate sul servizio DynamoDB, consulta la Guida per l'utente di [Amazon DynamoDB](#).

Negli argomenti seguenti viene descritto come lavorare con il servizio DynamoDB dal AWS Toolkit for JetBrains.

Argomenti

- [Utilizzo di Amazon DynamoDB tramite il AWS Toolkit for JetBrains](#)
- [Utilizzo delle tabelle Amazon DynamoDB tramite il AWS Toolkit for JetBrains](#)

Utilizzo di Amazon DynamoDB tramite il AWS Toolkit for JetBrains

Il AWS Toolkit for JetBrains consente di visualizzare, copiare i nomi delle risorse Amazon (ARN) ed eliminare le risorse Amazon DynamoDB direttamente dall'IDE JetBrains.

Nelle sezioni seguenti viene descritto come utilizzare queste funzionalità del servizio tramite il AWS Toolkit for JetBrains.

Visualizzazione delle risorse DynamoDB

Al momento, le risorse DynamoDB non possono essere create direttamente dal kit di strumenti, ma le risorse sono ugualmente visibili. Per visualizzare le risorse DynamoDB, completa i seguenti passaggi:

1. Vai alla scheda Esploratore nel AWS Toolkit for JetBrains.
2. Espandi il nodo DynamoDB.
3. Le risorse DynamoDB vengono visualizzate sotto il nodo DynamoDB.

Copia degli ARN delle risorse DynamoDB

Un nome della risorsa Amazon (ARN) è un ID univoco che viene assegnato a tutte le risorse AWS, incluse le tabelle DynamoDB. Per copiare l'ID ARN di una risorsa DynamoDB, completa i seguenti passaggi:

1. Vai alla scheda Esploratore nel AWS Toolkit for JetBrains.
2. Espandi il nodo DynamoDB.
3. Apri il menu contestuale (facendo clic con il pulsante destro del mouse) della risorsa DynamoDB della quale desideri copiare l'ID ARN.
4. Scegli Copia ARN per copiare l'ID dell'ARN della risorsa negli appunti del sistema operativo.

Eliminazione delle risorse DynamoDB

Per eliminare una risorsa DynamoDB, completa i seguenti passaggi:

1. Vai alla scheda Esploratore nel AWS Toolkit for JetBrains.
2. Espandi il nodo DynamoDB.
3. Apri il menu contestuale (facendo clic con il pulsante destro del mouse) della risorsa DynamoDB che desideri eliminare.

4. Scegli Elimina tabella... per aprire la finestra di dialogo di conferma Elimina tabella....
5. Completa le istruzioni di conferma per eliminare la tabella DynamoDB.

Utilizzo delle tabelle Amazon DynamoDB tramite il AWS Toolkit for JetBrains

La risorsa principale di Amazon DynamoDB è una tabella di database. Negli argomenti seguenti viene descritto come lavorare con le tabelle DynamoDB tramite il AWS Toolkit for JetBrains.

Visualizzazione di una tabella DynamoDB

Per visualizzare una tabella DynamoDB, completa i seguenti passaggi:

1. Vai alla scheda Esploratore nel AWS Toolkit for JetBrains.
2. Espandi il nodo DynamoDB.
3. Dall'elenco di risorse DynamoDB, fai doppio clic su una tabella per visualizzarla nella finestra Editor.

Note

La prima volta che si visualizzano i dati della tabella, viene recuperata una scansione iniziale con un limite massimo di risultati di 50 elementi.

Impostazione del limite massimo di risultati

Per modificare il limite predefinito delle voci della tabella recuperate, completa i seguenti passaggi:

1. Dall'Esploratore AWS, fai clic con il pulsante destro del mouse su una tabella per visualizzarla nella finestra Editor di JetBrains.
2. Dalla visualizzazione della tabella, scegli l'icona Impostazioni, situata nell'angolo in alto a destra della finestra Editor.
3. Passa il pulsante destro del mouse sull'opzione Numero massimo di risultati per visualizzare un elenco dei valori del numero massimi di risultati disponibili.

Scansione di una tabella DynamoDB

Per eseguire la scansione di una tabella DynamoDB, completa i seguenti passaggi:

Note

Questa scansione genera una query PartiQL e richiede che siano applicate le corrette policy AWS Identity and Access Management (AWS IAM). Per ulteriori informazioni sui requisiti delle policy di sicurezza PartiQL, consulta l'argomento [IAM security policies with PartiQL for DynamoDB](#) della Guida per gli sviluppatori di Amazon DynamoDB.

1. Dall'Esploratore AWS, fai clic con il pulsante destro del mouse su una tabella per visualizzarla nella finestra Editor di JetBrains.
2. Dalla visualizzazione della tabella, espandi l'intestazione Scansiona.
3. Seleziona la voce Tabella/Indice per la quale desideri eseguire la scansione dal menu a discesa.
4. Scegli Esegui per procedere con la scansione. La scansione è completa quando i dati della tabella vengono restituiti nella finestra Editor.

Utilizzo di Amazon Elastic Container Service tramite il AWS Toolkit for JetBrains

Negli argomenti seguenti viene descritto come utilizzare il AWS Toolkit for JetBrains per lavorare con le risorse Amazon ECS in un account AWS.

Argomenti

- [Amazon Elastic Container Service \(Amazon ECS\) Exec nel Kit di strumenti AWS](#)

Amazon Elastic Container Service (Amazon ECS) Exec nel Kit di strumenti AWS

È possibile utilizzare la funzionalità Amazon ECS Exec per emettere comandi singoli o eseguire una shell (interprete di comandi) in un container Amazon Elastic Container Service (Amazon ECS) direttamente tramite il Kit di strumenti AWS.

Important

L'abilitazione e la disabilitazione di Amazon ECS Exec modificano lo stato delle risorse nell'account AWS. Sono inclusi l'arresto e il riavvio del servizio. Alterare lo stato delle risorse mentre Amazon ECS Exec è abilitato può portare a risultati imprevedibili. Per ulteriori informazioni su Amazon ECS Exec, consulta la pagina [Using Amazon ECS Exec for debugging](#) della Guida per gli sviluppatori.

Prerequisiti di Amazon ECS Exec

Prima di poter utilizzare la funzionalità Amazon ECS Exec, è necessario soddisfare alcune condizioni preliminari.

Important

Per abilitare Amazon ECS Exec per un particolare servizio, Amazon ECS Cloud Debugging deve essere disabilitato per tale servizio.

Requisiti di Amazon ECS

A seconda della posizione in cui sono ospitate le attività, Amazon EC2 o AWS Fargate, Amazon ECS Exec ha requisiti di versione differenti.

- Se utilizzi Amazon EC2, devi utilizzare un'AMI ottimizzata per Amazon ECS rilasciata dopo il 20 gennaio 2021, con una versione dell'agente 1.50.2 o successiva. Ulteriori informazioni sono disponibili nella guida per gli sviluppatori sulle [AMI ottimizzate per Amazon ECS](#).
- Se utilizzi AWS Fargate è necessario utilizzare la piattaforma versione 1.4.0 o successiva. Ulteriori informazioni sui requisiti di Fargate sono disponibili nella guida per gli sviluppatori sulle [versioni della piattaforma AWS Fargate](#).

Configurazione dell'account AWS e autorizzazioni IAM

Per utilizzare la funzionalità Amazon ECS Exec, è necessario disporre di un cluster Amazon ECS associato al proprio Account AWS. Amazon ECS Exec utilizza Systems Manager per stabilire una connessione con i container del cluster e richiede autorizzazioni dei ruoli IAM specifiche per le attività per comunicare con il servizio SSM.

Puoi trovare informazioni sui ruoli e sulle policy IAM specifiche per Amazon ECS Exec nella sezione [IAM permissions required for ECS Exec](#) della Guida per gli sviluppatori.

Utilizzo di Amazon ECS Exec

È possibile abilitare o disabilitare Amazon ECS Exec direttamente dall'Esploratore AWS nel AWS Toolkit for JetBrains. Una volta abilitato Amazon ECS Exec, è possibile scegliere i container dal menu Amazon ECS ed eseguirvi comandi.

Abilitazione di Amazon ECS Exec

1. Dall'Esploratore AWS, individua ed espandi il menu Amazon ECS.
2. Espandi la sezione Cluster e scegli il cluster che desideri modificare.
3. Apri il menu contestuale (facendo clic con il pulsante destro del mouse) del servizio e seleziona Abilita esecuzione dei comandi.

Note

Se Amazon ECS Cloud Debugging è abilitato per questo servizio, l'opzione Abilita esecuzione dei comandi non sarà disponibile. La disabilitazione di Cloud Debugging ripristinerà l'opzione, ma interromperà e riavvierà il servizio.

Important

Questa operazione avvia una nuova implementazione del servizio e potrebbe richiedere alcuni minuti. Per ulteriori informazioni, consulta la nota all'inizio di questa sezione.

Disabilitazione di Amazon ECS Exec

1. Dall'Esploratore AWS, individua ed espandi il menu Amazon ECS.
2. Espandi la sezione Cluster e scegli il cluster che desideri modificare.
3. Apri il menu contestuale (facendo clic con il pulsante destro del mouse) del servizio che desideri modificare e seleziona Disabilita esecuzione del comando.

Important

Questa operazione avvia una nuova implementazione del servizio e potrebbe richiedere alcuni minuti. Per ulteriori informazioni, consultare la nota all'inizio di questa sezione.

Esecuzione di comandi su un container

Per eseguire comandi su un container utilizzando AWS Explorer, Amazon ECS Exec deve essere abilitato. Se non è abilitato, consulta la procedura Abilitazione di Amazon ECS Exec descritta in questa sezione.

1. Dall'Esploratore AWS, individua ed espandi il menu Amazon ECS.
2. Espandi la sezione Cluster e scegli il cluster che desideri modificare.
3. Espandi un servizio per elencarne i container.
4. Apri il menu contestuale (facendo clic con il pulsante destro del mouse) del container che desideri modificare e scegli Esegui comando nel container.
5. Nella finestra di dialogo Esegui comando nel container, scegli l'ARN dell'attività che ti interessa.
6. È possibile digitare il comando che si desidera eseguire o selezionarlo da un elenco di comandi eseguiti durante la stessa sessione.
7. Scegli Execute (Esegui).

Esecuzione di comandi dall'interno di una shell (interprete di comandi)

Per eseguire comandi su un container all'interno di una shell utilizzando l'Esploratore AWS, Amazon ECS Exec deve essere abilitato. Se non è abilitato, consulta la procedura Abilitazione di Amazon ECS Exec descritta in questa sezione.

1. Dall'Esploratore AWS, individua ed espandi il menu Amazon ECS.
2. Espandi la sezione Cluster e scegli il cluster che desideri modificare.
3. Espandi il servizio per elencare i container associati.
4. Apri il menu contestuale (facendo clic con il pulsante destro del mouse) del container che desideri modificare e scegli Apri shell interattiva.
5. Nella finestra di dialogo Shell interattiva, scegli l'ARN dell'attività che ti interessa.
6. Scegli una shell dal menu a discesa corrispondente o inserisci il nome della shell con la quale vuoi interagire.

7. Quando le impostazioni ti soddisfano, scegli Esegui.
8. Quando la shell si apre in un terminale, puoi digitare dei comandi per interagire con il container.

Utilizzo di Amazon EventBridge tramite il AWS Toolkit for JetBrains

Nell'argomento seguente viene descritto come utilizzare il AWS Toolkit for JetBrains per lavorare con gli schemi di Amazon EventBridge in un account AWS.

Argomenti

- [Utilizzo degli schemi Amazon EventBridge](#)

Utilizzo degli schemi Amazon EventBridge

È possibile utilizzare il AWS Toolkit for JetBrains per lavorare con gli schemi Amazon EventBridge come descritto di seguito.

Note

L'utilizzo degli schemi EventBridge è attualmente supportato solo dal Kit di strumenti AWS per IntelliJ e dal Kit di strumenti AWS per PyCharm.

Le seguenti informazioni presuppongono che sia già stato [impostato AWS Toolkit for JetBrains](#).

Indice

- [Visualizzazione di uno schema disponibile](#)
- [Individuazione di uno schema disponibile](#)
- [Generazione del codice per uno schema disponibile](#)
- [Creazione di un'applicazione AWS Serverless Application Model che utilizza uno schema disponibile](#)

Visualizzazione di uno schema disponibile

1. Con la finestra dello strumento [AWS Explorer](#) visualizzata, espandere Schemas (Schemi).
2. Espandere il nome del registro che contiene lo schema da visualizzare. Ad esempio, molti degli schemi forniti da AWS si trovano nel registro aws.events.

3. Per visualizzare lo schema nell'editor, fare clic con il pulsante destro del mouse sul titolo dello schema e scegliere View Schema (Visualizza schema) dal menu contestuale.

Individuazione di uno schema disponibile

Con la finestra dello strumento [AWS Explorer](#) visualizzata, effettuare una delle seguenti operazioni:

- Iniziare a digitare il titolo dello schema che si desidera trovare. In AWS Explorer vengono evidenziati i titoli degli schemi che contengono una corrispondenza.
- Fare clic con il pulsante destro del mouse su Schemas (Schemi) e scegliere Search Schemas (Cerca schemi) dal menu di scelta rapida. Nella finestra di dialogo Cerca schemi EventBridge, inizia a digitare il titolo dello schema che desideri trovare. Nella finestra di dialogo vengono visualizzati i titoli degli schemi che contengono una corrispondenza.
- Espandere Schemas (Schemi). Fare clic con il pulsante destro del mouse sul nome del registro contenente lo schema che si desidera trovare e quindi scegliere Search Schemas in Registry (Cerca schemi nel registro). Nella finestra di dialogo Cerca schemi EventBridge, inizia a digitare il titolo dello schema che desideri trovare. Nella finestra di dialogo vengono visualizzati i titoli degli schemi che contengono una corrispondenza.

Per visualizzare uno schema nell'elenco delle corrispondenze, effettuare una delle seguenti operazioni:

- Per visualizzare lo schema nell'editor, in AWS Explorer, fare clic con il pulsante destro del mouse sul titolo dello schema e quindi scegliere View Schema (Visualizza schema).
- Nella finestra di dialogo Cerca schemi EventBridge, scegli il titolo dello schema che desideri visualizzare.

Generazione del codice per uno schema disponibile

1. Con la finestra dello strumento [AWS Explorer](#) visualizzata, espandere Schemas (Schemi).
2. Espandere il nome del registro che contiene lo schema per il quale si desidera generare codice.
3. Fare clic con il pulsante destro del mouse sul titolo dello schema, quindi scegliere Download code bindings (Scarica associazioni codice).
4. Nella finestra di dialogo Download code bindings (Scarica associazioni codice) scegliere quanto segue:

- La versione dello schema per cui generare il codice.
 - Il linguaggio di programmazione supportato e la versione del linguaggio per cui generare il codice.
 - Il percorso file in cui memorizzare il codice generato sul computer di sviluppo locale.
5. Scegli Download (Scarica).

Creazione di un'applicazione AWS Serverless Application Model che utilizza uno schema disponibile

1. Nel menu File scegli New (Nuovo), quindi Project (Progetto).
2. Nella finestra di dialogo New Project (Nuovo progetto) scegliere AWS.
3. Scegliere Applicazione Serverless AWS, quindi scegliere Next (Successivo).
4. Specificare le impostazioni seguenti:
 - Un nome per il progetto.
 - Un percorso del computer di sviluppo locale per il progetto.
 - Un runtime AWS Lambda supportato per il progetto.
 - Un modello SAM di AWS Serverless Application Model (AWS SAM) per il progetto. Le scelte attualmente includono quanto segue:
 - AWS SAM EventBridge Hello World (EC2 Instance State Change) : l'implementazione di questa funzionalità crea una funzione AWS Lambda e un endpoint Gateway Amazon API associato nell'account AWS. Per impostazione predefinita, questa funzione e l'endpoint rispondono solo a una modifica dello stato dell'istanza Amazon EC2.
 - App AWS SAM EventBridge da zero (per qualsiasi trigger di evento da un registro di schema): quando viene implementata, crea una funzione AWS Lambda e un endpoint Gateway Amazon API associato nell'account AWS. Questa funzione e l'endpoint possono rispondere agli eventi disponibili nello schema specificato.

Se scegli questo modello devi specificare anche quanto segue:

- Il profilo denominato e le credenziali da utilizzare.
 - La regione AWS da utilizzare.
 - Lo Schema dell'evento EventBridge da utilizzare.
- La versione dell'SDK da utilizzare per il progetto (Project SDK).

Dopo aver creato un progetto di applicazione serverless AWS, puoi effettuare le seguenti operazioni:

- [Distribuzione dell'applicazione](#)
- [Modifica \(aggiornamento\) delle impostazioni dell'applicazione](#)
- [Eliminazione dell'applicazione distribuita](#)

È inoltre possibile eseguire le seguenti operazioni con le funzioni Lambda che fanno parte dell'applicazione:

- [Esecuzione \(invocazione\) o debug della versione locale di una funzione](#)
- [Esecuzione \(invocazione\) della versione remota di una funzione](#)
- [Modifica delle impostazioni di una funzione](#)
- [Eliminazione di una funzione](#)

Utilizzo di AWS Lambda tramite il AWS Toolkit for JetBrains

Negli argomenti seguenti viene descritto come lavorare con le funzioni AWS Lambda tramite il AWS Toolkit for JetBrains.

Argomenti

- [Runtime e supporto di AWS Lambda nel AWS Toolkit for JetBrains](#)
- [Creazione di una funzione AWS Lambda tramite il AWS Toolkit for JetBrains](#)
- [Esecuzione \(richiamo\) o debug della versione locale di una funzione AWS Lambda tramite il AWS Toolkit for JetBrains](#)
- [Esecuzione \(richiamo\) della versione remota di una funzione AWS Lambda tramite il AWS Toolkit for JetBrains](#)
- [Modifica \(aggiornamento\) delle impostazioni della funzione AWS Lambda tramite il AWS Toolkit for JetBrains](#)
- [Eliminazione di una funzione AWS Lambda tramite il AWS Toolkit for JetBrains](#)

Runtime e supporto di AWS Lambda nel AWS Toolkit for JetBrains

AWS Lambda supporta più lingue attraverso l'uso di runtime. Un runtime fornisce un ambiente specifico del linguaggio che inoltra gli eventi di chiamata, le informazioni di contesto e le risposte

tra Lambda e la funzione. Per informazioni dettagliate sul servizio Lambda e sui runtime supportati, consulta l'argomento [Lambda runtimes](#) della Guida per l'utente di AWS Lambda.

Di seguito vengono descritti gli ambienti di runtime attualmente supportati per l'uso con il AWS Toolkit for JetBrains.

Nome	Identificatore	Sistema operativo	Architettura
Node.js 18	nodejs18.x	Amazon Linux 2	x86_64, arm64
Node.js 16	nodejs16.x	Amazon Linux 2	x86_64, arm64
Node.js 14	nodejs14.x	Amazon Linux 2	x86_64, arm64
Python 3.11	python3.11	Amazon Linux 2	x86_64, arm64
Python 3.10	python3.10	Amazon Linux 2	x86_64, arm64
Python 3.9	python3.9	Amazon Linux 2	x86_64, arm64
Python 3.8	python3.8	Amazon Linux 2	x86_64, arm64
Python 3.7	python3.7	Amazon Linux 2	x86_64
Java 17	java17	Amazon Linux 2	x86_64, arm64
Java 11	java11	Amazon Linux 2	x86_64, arm64
Java 8	java8.al2	Amazon Linux 2	x86_64, arm64
Java 8	java8	Amazon Linux 2	x86_64
.NET 6	dotnet6	Amazon Linux 2	x86_64, arm64
Go 1.x	go1.x	Amazon Linux 2	x86_64

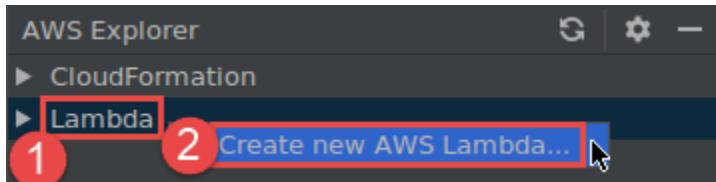
Creazione di una funzione AWS Lambda tramite il AWS Toolkit for JetBrains

Puoi utilizzare AWS Toolkit for JetBrains per creare una funzione AWS Lambda che fa parte di un'applicazione serverless AWS. In alternativa, puoi creare una funzione Lambda standalone.

Per creare una funzione Lambda che fa parte di un'applicazione serverless AWS, ignora il resto di questo argomento e consulta la pagina [Creazione di un'applicazione](#).

Per creare una funzione Lambda standalone, devi innanzitutto installare AWS Toolkit for JetBrains e, se non l'hai ancora fatto, connetterti a un account AWS per la prima volta. Quindi, con IntelliJ IDEA, PyCharm, WebStorm o JetBrains Rider già in esecuzione, esegui una delle seguenti operazioni:

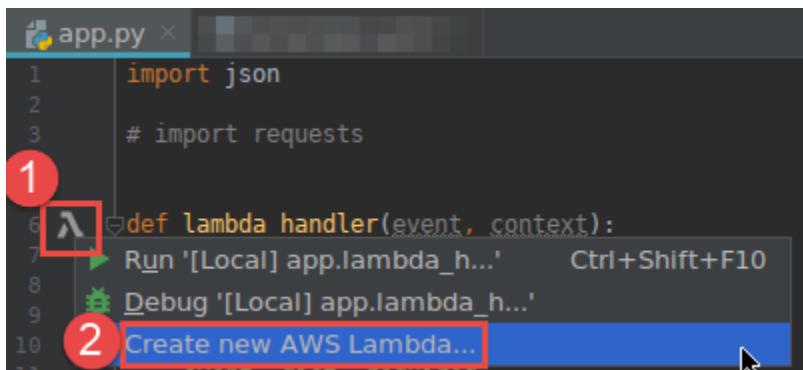
- Aprire AWS Explorer, se non è già aperto. Se devi passare a un'altra regione AWS per creare la funzione, esegui subito l'operazione. Quindi fai clic con il pulsante destro del mouse su Lambda e scegli Crea nuovo AWS Lambda.



Completa le operazioni nella finestra di dialogo [Create Function \(Crea funzione\)](#) e quindi scegliere Create Function (Crea funzione). AWS Toolkit for JetBrains crea uno stack AWS CloudFormation corrispondente per l'implementazione e aggiunge il nome della funzione all'elenco Lambda nell'Esploratore AWS. Se l'implementazione non riesce, puoi provare a comprendere il motivo visualizzando i log eventi per lo stack.

- Creare un file di codice che implementa un gestore di funzioni per [Java](#), [Python](#), [Node.js](#) o [C#](#).

Se devi passare a un'altra regione AWS per creare la funzione remota da eseguire (richiamare), esegui subito l'operazione. Quindi, nel file di codice, scegli l'icona Lambda nel margine accanto al gestore delle funzioni, quindi scegli Crea nuovo AWS Lambda. Completa le operazioni nella finestra di dialogo [Create Function \(Crea funzione\)](#) e quindi scegliere Create Function (Crea funzione).

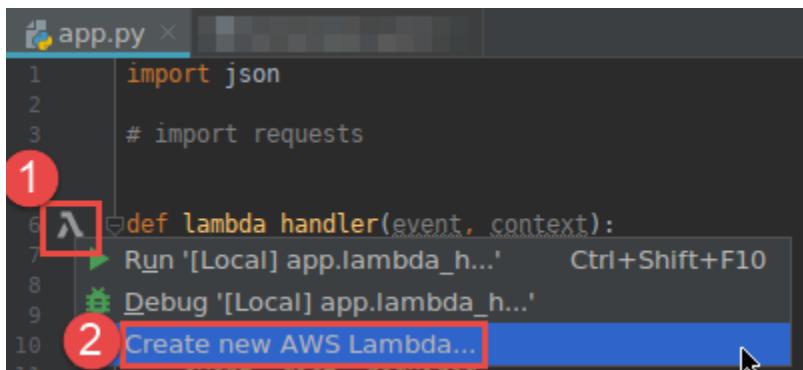


Note

Se l'icona Lambda non viene visualizzata nel margine accanto al gestore delle funzioni, prova a visualizzarla per il progetto corrente selezionando la seguente casella in Impostazioni/Preferenze: Strumenti, AWS, Impostazioni del progetto, Mostra le icone a margine per tutti i possibili gestori AWS Lambda. Inoltre, se il gestore della funzione è già definito nel modello AWS SAM corrispondente, il comando Crea nuovo AWS Lambda non verrà visualizzato.

Dopo aver scelto Crea funzione, AWS Toolkit for JetBrains crea una funzione corrispondente nel servizio Lambda per l'account AWS connesso. Se l'operazione ha esito positivo, dopo l'aggiornamento dell'Esploratore AWS, nell'elenco Lambda viene visualizzato il nome della nuova funzione.

- Se è già disponibile un progetto contenente una funzione AWS Lambda e devi prima passare a un'altra Regione AWS per creare la funzione, esegui subito l'operazione. Nel file di codice contenente il gestore di funzioni per [Java](#), [Python](#), [Node.js](#) oppure [C#](#), scegli l'icona Lambda a margine del gestore di funzioni. Scegli Crea nuovo AWS Lambda, completa le operazioni nella finestra di dialogo [Crea funzione](#), quindi scegli Crea funzione.



Note

Se l'icona Lambda non viene visualizzata nel margine accanto al gestore delle funzioni, prova a visualizzarla per il progetto corrente selezionando la seguente casella in Impostazioni/Preferenze: Strumenti, AWS, Impostazioni del progetto, Mostra le icone a margine per tutti i possibili gestori AWS Lambda. Inoltre, se il gestore della funzione è già definito nel modello AWS SAM corrispondente, il comando Crea nuovo AWS Lambda non verrà visualizzato.

Dopo aver scelto Crea funzione, AWS Toolkit for JetBrains crea una funzione corrispondente nel servizio Lambda per l'account AWS connesso. Se l'operazione ha esito positivo, dopo l'aggiornamento dell'Esploratore AWS, nell'elenco Lambda viene visualizzato il nome della nuova funzione.

Dopo aver creato la funzione, puoi eseguire (invocare) o eseguire il debug della versione locale della funzione o eseguire (invocare) la versione remota.

Esecuzione (richiamo) o debug della versione locale di una funzione AWS Lambda tramite il AWS Toolkit for JetBrains

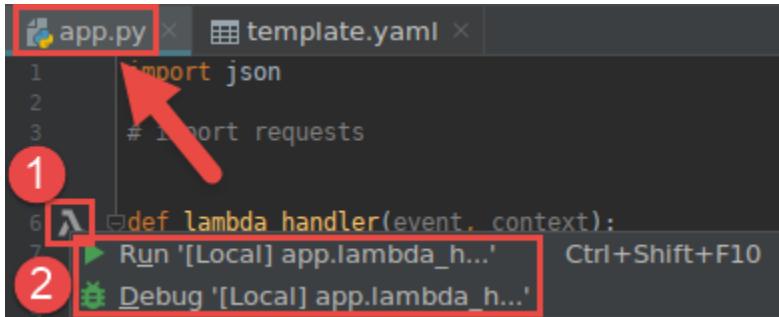
Per completare questa procedura, devi creare la funzione AWS Lambda che vuoi eseguire (richiamare) o sottoporre a debug, se non è già stata creata.

Note

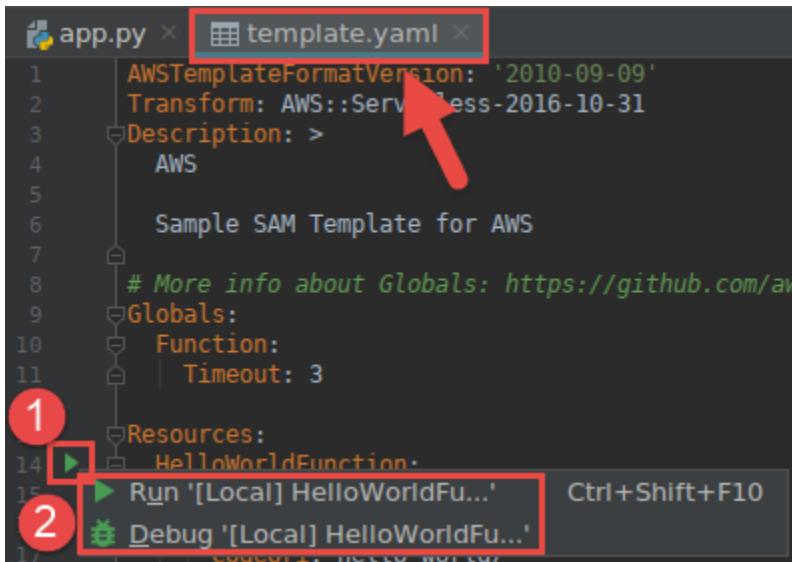
Se vuoi eseguire (richiamare) o sottoporre a debug la versione locale di una funzione Lambda ed eseguire (richiamare) o sottoporre a debug locale una funzione con proprietà non predefinite o facoltative, devi innanzitutto impostare tali proprietà nel file di modello AWS SAM corrispondente della funzione (ad esempio, in un file denominato `template.yaml` nel progetto). Per l'elenco delle impostazioni di proprietà disponibili, consulta [AWS::Serverless::Function](#) nel repository [awslabs/serverless-application-model](#) su GitHub.

1. Completa una delle seguenti operazioni:

- Nel file di codice contenente il gestore di funzioni per [Java](#), [Python](#), [Node.js](#) oppure [C#](#), scegli l'icona Lambda a margine del gestore di funzioni. Scegliere Run '[Local]' (Esegui '[Locale]') o Debug '[Local]' (Debug '[Locale]').



- Con la finestra dello strumento Project (Progetto) aperta con il progetto che contiene la funzione visualizzato, aprire il file template.yaml del progetto. Scegliere l'icona Run (Esegui) al margine della definizione della risorsa della funzione, quindi scegliere Run '[Local]' (Esegui '[Locale]') o Debug '[Local]' (Debug '[Locale]')).



- Completa le operazioni nella finestra di dialogo [Modifica configurazione \(impostazioni della funzione locale\)](#) se visualizzata, quindi scegli Esegui o Debug. I risultati vengono visualizzati nella finestra dello strumento Run (Esegui) o Debug.

- Se la finestra di dialogo Modifica configurazione non viene visualizzata e desideri modificare la configurazione esistente, prima modifica la configurazione e quindi ripeti questa procedura dall'inizio.
- Se i dettagli di configurazione sono mancanti, espandere Templates (Modelli), AWS Lambda e scegliere Local (Locale). Scegli OK, quindi ripeti questa procedura dall'inizio.

Esecuzione (richiamo) della versione remota di una funzione AWS Lambda tramite il AWS Toolkit for JetBrains

Una versione remota di una funzione AWS Lambda è una funzione il cui codice sorgente esiste già all'interno del servizio Lambda per un account AWS.

Per completare questa procedura, devi innanzitutto installare il AWS Toolkit for JetBrains e, se non l'hai ancora fatto, effettuare la prima connessione a un account AWS. Quindi, con IntelliJ IDEA, PyCharm, WebStorm o JetBrains Rider già in esecuzione, esegui le seguenti operazioni.

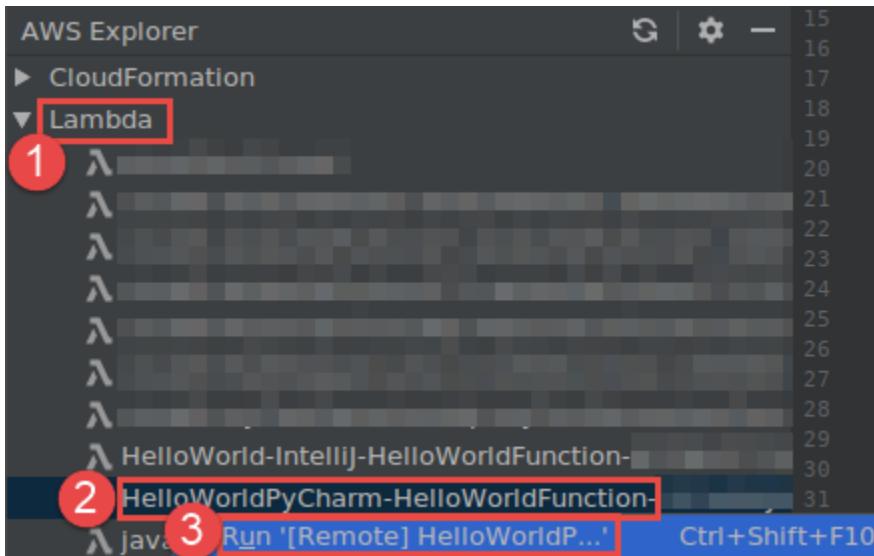
1. Aprire AWS Explorer, se non è già aperto. Se devi passare alla regione AWS che contiene la funzione, esegui subito l'operazione.
2. Espandi Lambda e verifica che il nome della funzione sia elencato. Se è presente, passare alla fase 3 in questa procedura.

Se il nome della funzione non è elencato, crea la funzione Lambda che desideri eseguire (richiamare).

Se la funzione è stata creata come parte di un'applicazione serverless AWS, è necessario implementare tale applicazione.

Se la funzione è stata creata con un file di codice che implementa un gestore di funzioni per [Java](#), [Python](#), [Node.js](#) oppure [C#](#), nel file di codice scegli l'icona Lambda accanto al gestore di funzioni. Quindi, scegli Crea nuovo AWS Lambda. Completare le operazioni nella finestra di dialogo [Create Function \(Crea funzione\)](#) e quindi scegliere Create Function (Crea funzione).

3. Con il menu Lambda aperto su Esploratore AWS, fai clic con il pulsante destro del mouse sul nome della funzione, quindi scegli Esegui '[Remoto]'



4. Completa le operazioni nella finestra di dialogo [Modifica configurazione \(impostazioni della funzione remota\)](#) se visualizzata, quindi scegli Esegui o Debug. I risultati vengono visualizzati nella finestra dello strumento Run (Esegui) o Debug.

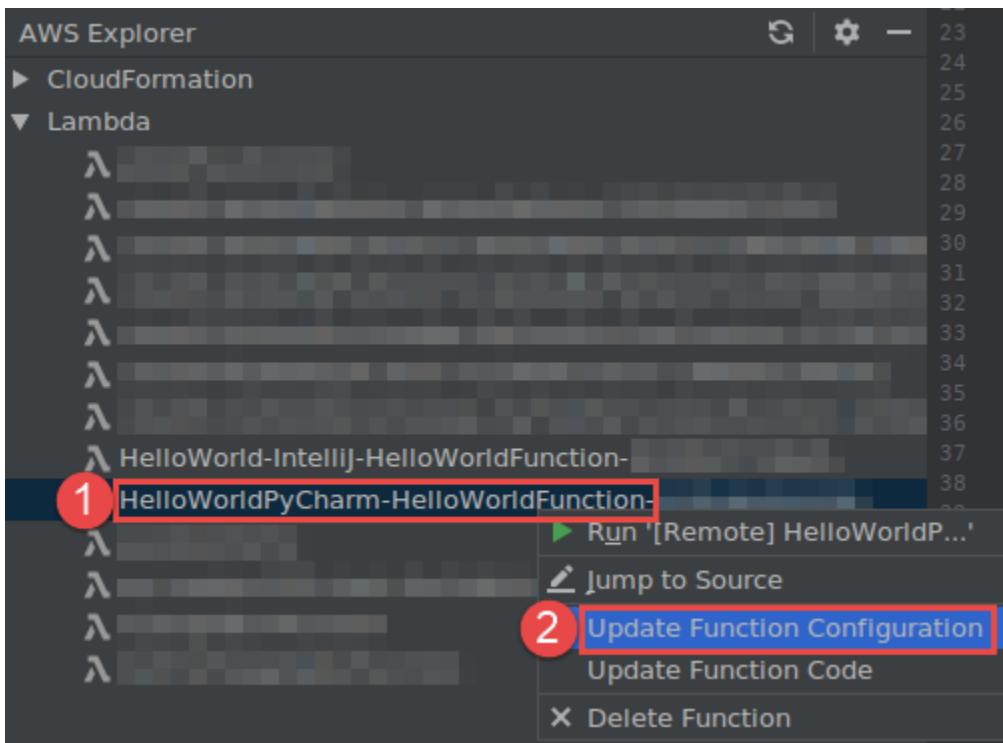
- Se la finestra di dialogo Modifica configurazione non viene visualizzata e desideri modificare la configurazione esistente, prima modifica la configurazione e quindi ripeti questa procedura dall'inizio.
- Se i dettagli di configurazione sono mancanti, espandere Templates (Modelli), AWS Lambda e scegliere Local (Locale). Scegli OK, quindi ripeti questa procedura dall'inizio.

Modifica (aggiornamento) delle impostazioni della funzione AWS Lambda tramite il AWS Toolkit for JetBrains

Per utilizzare AWS Toolkit for JetBrains per modificare (aggiornare) le impostazioni di una funzione AWS Lambda, effettua una delle seguenti operazioni.

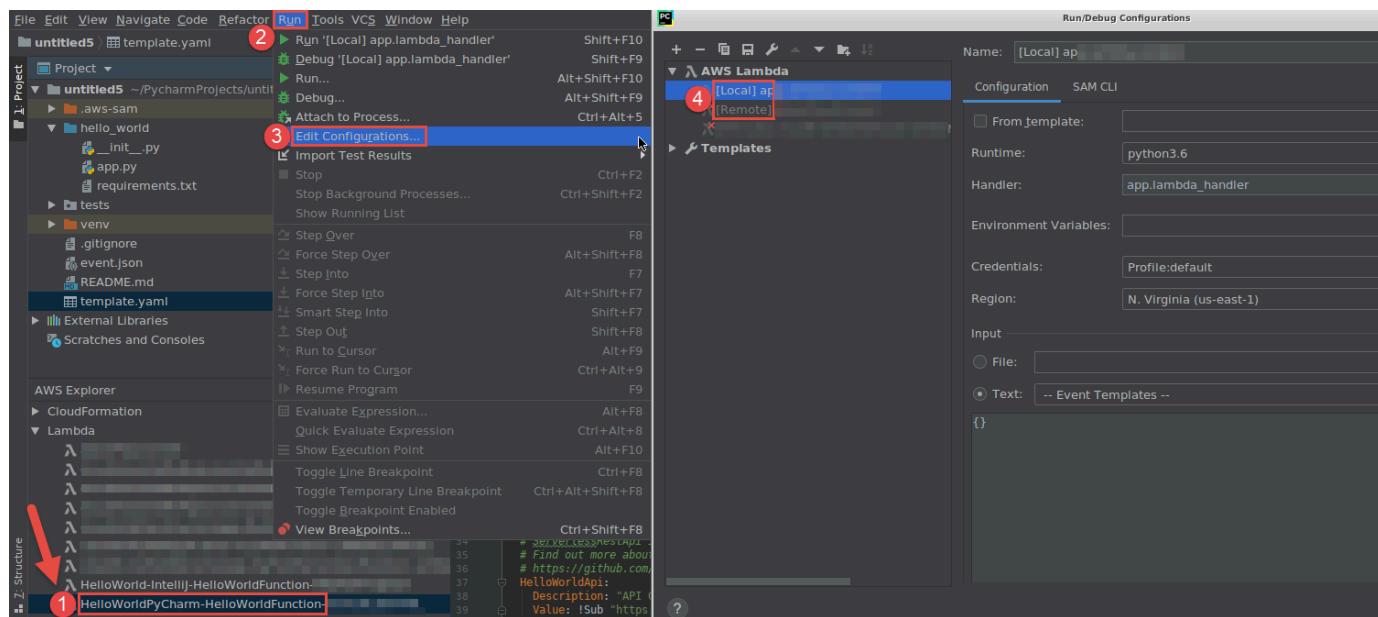
- Con il file di codice aperto contenente il gestore di funzioni per [Java](#), [Python](#), [Node.js](#) o [C#](#), scegliere nel menu principale Run (Esegui), Edit Configurations (Modifica configurazioni). Completare le operazioni nella finestra di dialogo [Run/Debug Configurations \(Esegui/Modifica configurazioni\)](#) e scegliere OK.
- Aprire AWS Explorer, se non è già aperto. Se devi passare alla regione AWS che contiene la funzione, esegui subito l'operazione. Espandi Lambda, scegli il nome della funzione per cui modificare la configurazione e quindi effettua una delle seguenti operazioni:

- Modifica impostazioni come il timeout, la memoria, le variabili di ambiente e il ruolo di esecuzione: fai clic con il pulsante destro del mouse sul nome della funzione, quindi scegli Aggiorna la configurazione della funzione.



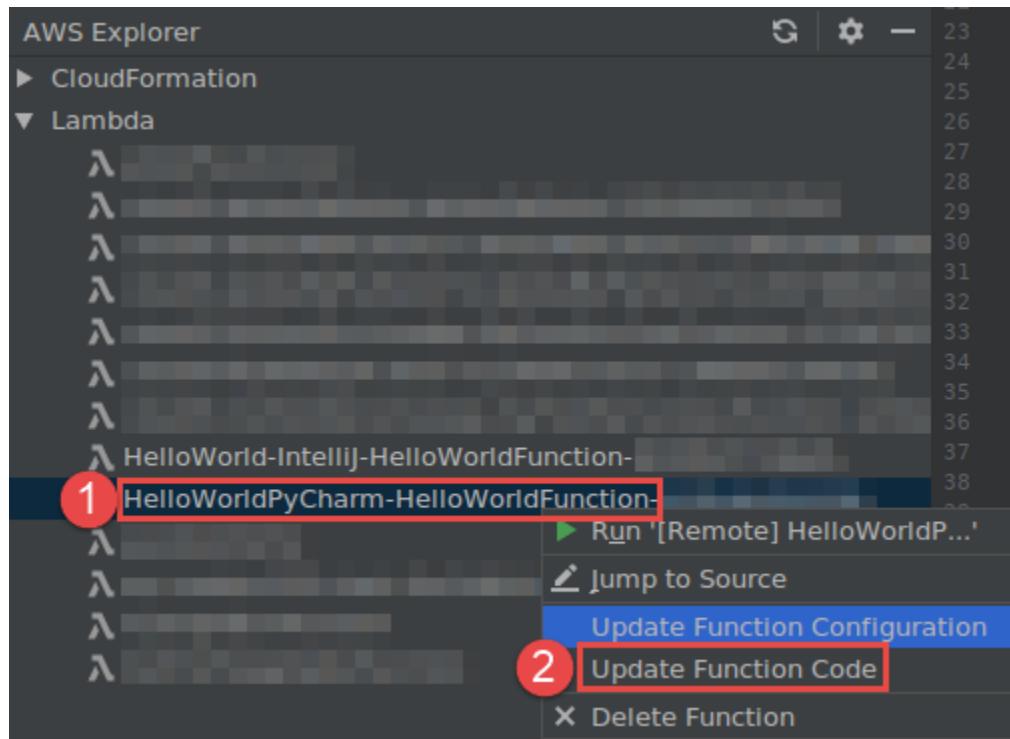
Completare le operazioni nella finestra di dialogo [Update Configuration \(Aggiorna configurazione\)](#) e scegliere Update (Aggiorna).

- Modifica le impostazioni come il payload di input: nel menu principale, scegli Esegui, Modifica configurazioni. Completare le operazioni nella finestra di dialogo [Run/Debug Configurations \(Esegui/Modifica configurazioni\)](#) e scegliere OK.



Se mancano i dettagli di configurazione, espandere Templates (Modelli), AWS Lambda e scegliere Local (Locale) (per la versione locale della funzione) o Remote (Remoto) (per la versione in remoto della stessa funzione). Scegliere OK, quindi ripetere questa procedura dall'inizio.

- Modifica le impostazioni, ad esempio il nome del gestore di funzioni o il bucket di origine Amazon Simple Storage Service (Amazon S3): fai clic con il pulsante destro del mouse sul nome della funzione e quindi scegli Aggiorna codice funzione.



Completa la finestra di dialogo [Update Code \(Aggiorna codice\)](#) e quindi scegliere Update (Aggiorna).

- Modifica le altre impostazioni di proprietà disponibili che non sono elencate nei punti precedenti: modifica tali impostazioni nel file di modello AWS SAM corrispondente della funzione (ad esempio, in un file denominato `template.yaml` nel progetto).

Per l'elenco delle impostazioni di proprietà disponibili, consulta [AWS::Serverless::Function](#) nel repository [awslabs/serverless-application-model](#) su GitHub.

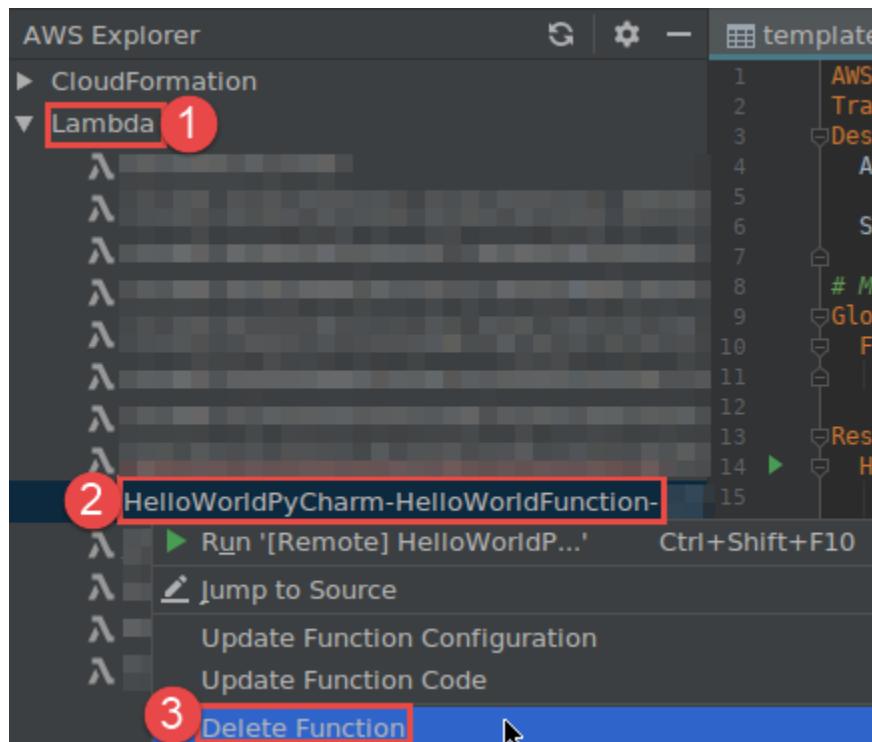
Eliminazione di una funzione AWS Lambda tramite il AWS Toolkit for JetBrains

È possibile utilizzare Kit di strumenti AWS per eliminare una funzione AWS Lambda che fa parte di un'applicazione serverless AWS oppure una funzione Lambda standalone.

Per eliminare una funzione Lambda che fa parte di un'applicazione serverless AWS, ignora il resto di questo argomento e consulta la pagina [Eliminazione di un'applicazione](#).

Per eliminare una funzione Lambda standalone, effettua le seguenti operazioni.

- Aprire AWS Explorer, se non è già aperto. Se devi passare alla regione AWS che contiene la funzione, esegui subito l'operazione.
- Espandi Lambda.
- Fare clic con il pulsante destro del mouse sul nome della funzione da eliminare, quindi scegliere Delete Function (Elimina funzione).



4. Immettere il nome della funzione per confermare l'eliminazione, quindi scegliere OK. Se l'eliminazione della funzione ha esito positivo, AWS Toolkit for JetBrains rimuove il nome della funzione dall'elenco Lambda.

Accesso ad Amazon RDS tramite il AWS Toolkit for JetBrains

Utilizzando Amazon Relational Database Service (Amazon RDS), è possibile eseguire il provisioning e gestire sistemi di database relazionali SQL nel cloud. Utilizzando il AWS Toolkit for JetBrains, è possibile connettersi ai seguenti motori di database Amazon RDS e interagire con essi:

- Aurora: è un database relazionale compatibile con MySQL e PostgreSQL creato per il cloud. Per ulteriori informazioni, consulta la [Guida per l'utente di Amazon Aurora](#).
- MySQL: Amazon RDS supporta diverse versioni principali del database relazionale open source. Per ulteriori informazioni, consulta la pagina [MySQL su Amazon RDS](#) della Guida per l'utente di Amazon RDS.
- PostgreSQL: Amazon RDS supporta diverse versioni principali del database relazionale a oggetti open source. Per ulteriori informazioni, consulta la pagina [PostgreSQL su Amazon RDS](#) della Guida per l'utente di Amazon RDS.

Negli argomenti seguenti vengono descritti i prerequisiti per accedere ai database RDS e come utilizzare il AWS Toolkit for JetBrains per connettersi a un'istanza di database.

Argomenti

- [Prerequisiti per l'accesso ai database Amazon RDS](#)
- [Connessione a un database Amazon RDS](#)

Prerequisiti per l'accesso ai database Amazon RDS

Prima di poter effettuare la connessione a un database Amazon RDS utilizzando AWS Toolkit for JetBrains, è necessario completare le seguenti attività:

- [Creazione di un'istanza di database e configurazione del relativo metodo di autenticazione](#)
- [Download e installazione di DataGrip](#)

Creazione di un'istanza di database Amazon RDS e configurazione del relativo metodo di autenticazione

AWS Toolkit for JetBrains consente di connettersi a un'istanza di database Amazon RDS già creata e configurata in AWS. Un'istanza di database è un ambiente di database isolato in esecuzione nel cloud che può contenere database multipli creati dall'utente. Per informazioni sulla creazione di istanze di database per i database supportati, consulta la pagina [Getting started with Amazon RDS resources](#) nella Guida per l'utente di Amazon RDS.

Quando ci si connette a un cluster tramite il AWS Toolkit for JetBrains, gli utenti possono scegliere di autenticarsi utilizzando le credenziali IAM oppure Secrets Manager. La tabella seguente descrive le funzionalità e le risorse informative principali per entrambe le opzioni:

Metodi di autenticazione	Come funziona	Ulteriori informazioni
Connessione con le credenziali IAM	Con l'autenticazione del database IAM, non occorre archiviare le credenziali dell'utente nel database, perché l'autenticazione è gestita esternamente utilizzando le credenziali AWS Identity	<ul style="list-style-type: none">• Gestione delle identità e degli accessi in Amazon RDS nella Guida per l'utente di Amazon RDS.• Articolo nell'AWS Knowledge Center: In che

Metodi di autenticazione	Come funziona	Ulteriori informazioni
	<p>and Access Management (IAM).</p> <p>Per impostazione predefinita, l'autenticazione al database mediante IAM è disabilitata nelle istanze di database. Puoi abilitare l'autenticazione database IAM (o disabilitarla di nuovo) tramite la Console di gestione AWS, l'AWS CLI o l'API.</p>	<p>modo è possibile consentire agli utenti di autenticarsi a un'istanza di database Amazon RDS utilizzando le credenziali IAM?</p>
Connessione con Gestione dei segreti AWS	<p>Un amministratore database può memorizzare le credenziali per un database come segreto in Secrets Manager. Secrets Manager crittografa e archivia le credenziali all'interno del segreto come testo segreto protetto.</p> <p>Quando un'applicazione dotata di autorizzazioni accede al database, Secrets Manager decripta il testo segreto protetto e lo restituisce su un canale protetto. Il client analizza le credenziali restituite, la stringa di connessione e qualsiasi altra informazione richiesta e utilizza tali informazioni per accedere al database.</p>	<ul style="list-style-type: none"> • Cos'è AWS Secrets Manager? nella Guida per l'utente di Gestione dei segreti AWS. • Tutorial: Rotazione di un segreto per un database AWS nella Guida per l'utente di Gestione dei segreti AWS. • Blog sulla sicurezza AWS: Rotazione automatica delle credenziali del database Amazon RDS con Secrets Manager.

Utilizzo dei database Amazon RDS con DataGrip

Dopo aver eseguito la connessione a un'origine dati Amazon RDS, puoi iniziare a interagire con essa. Utilizzando DataGrip di JetBrains, è possibile eseguire attività di database come la scrittura di SQL, l'esecuzione di query e l'importazione/esportazione di dati. Le funzionalità fornite da DataGrip sono disponibili anche nel plug-in del database per una serie di IDE JetBrains. Per informazioni su DataGrip, consulta la pagina <https://www.jetbrains.com/datagrip/>.

Connessione a un database Amazon RDS

Con l'Esploratore AWS, puoi selezionare un database Amazon RDS, scegliere un metodo di autenticazione e quindi configurare le impostazioni di connessione. Dopo aver verificato che la connessione funziona, puoi iniziare a interagire con l'origine dati utilizzando JetBrains DataGrip.

Important

Assicurati di aver completato i [prerequisiti](#) affinché gli utenti possano accedere ai database Amazon RDS e interagire con essi.

Seleziona una scheda per le istruzioni sulla connessione a un'istanza di database utilizzando il metodo di autenticazione preferito.

Connect with IAM credentials

1. Aprire AWS Explorer, se non è già aperto.
2. Fai clic sul nodo Amazon RDS per espandere l'elenco dei motori di database supportati.
3. Fai clic su un nodo del motore di database supportato (Aurora, MySQL o PostgreSQL) per espandere l'elenco delle istanze di database disponibili.

Note

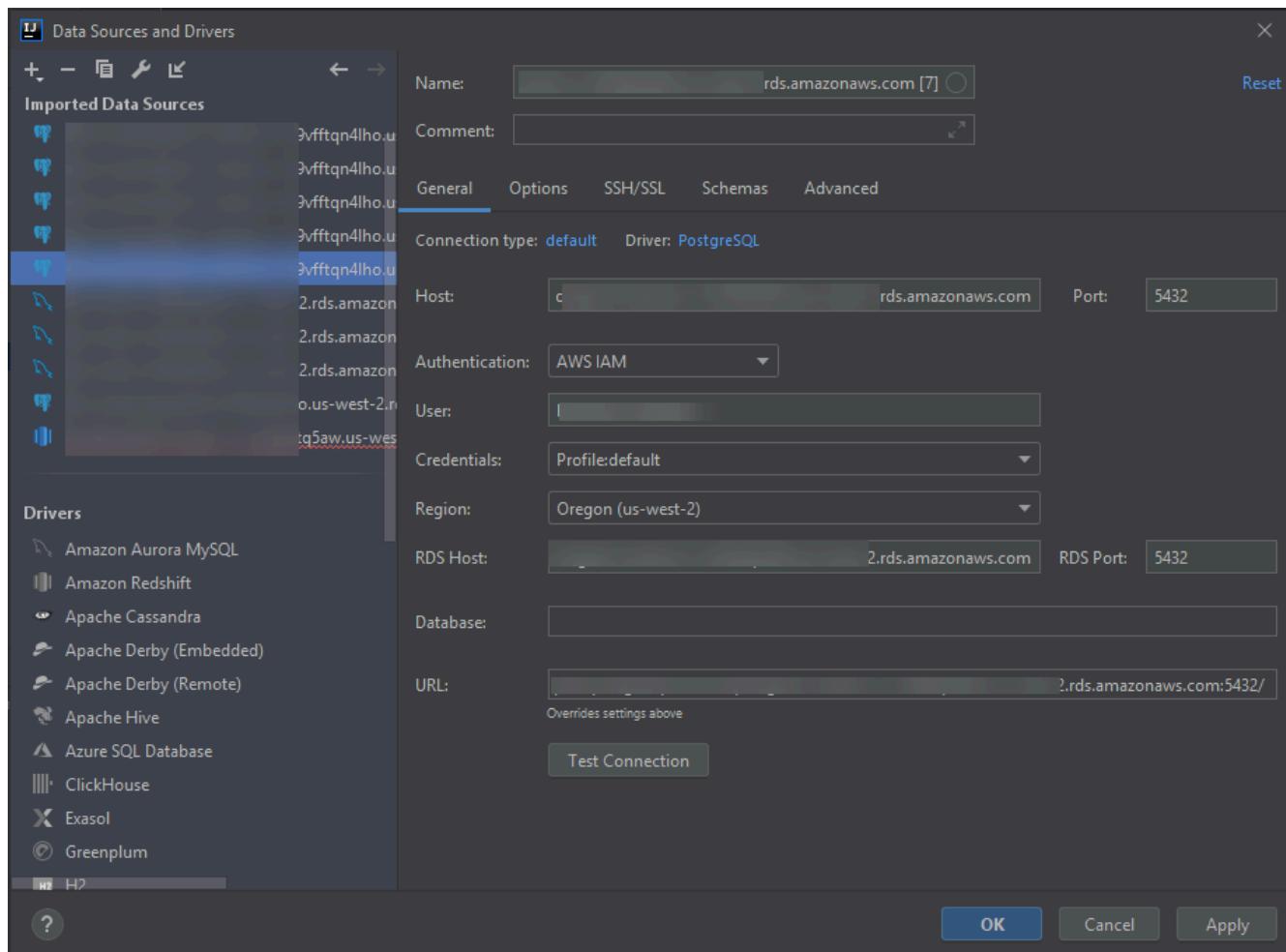
Se si seleziona Aurora, è possibile scegliere tra espandere un cluster MySQL e un cluster PostgreSQL.

4. Fai clic con il pulsante destro del mouse su un database e scegli Connottiti tramite credenziali IAM.

Note

È anche possibile scegliere Copia ARN per aggiungere il nome della risorsa Amazon (ARN) del database agli appunti.

5. Nella finestra di dialogo Origini dati e driver, esegui le operazioni seguenti per verificare che sia possibile stabilire una connessione al database:
 - Nel riquadro Origini dati importati, verifica che sia selezionata l'origine dati corretta.
 - Se appare il messaggio Scarica i file dei driver mancanti, scegli Vai al driver (l'icona a forma di chiave inglese) per scaricare i file richiesti.
6. Nella scheda Generale del riquadro Impostazioni, verifica che i seguenti campi visualizzino i valori corretti:
 - Host/Porta: l'endpoint e la porta utilizzati per le connessioni al database. Per i database Amazon RDS ospitati nel cloud AWS, gli endpoint terminano sempre con `rds.amazonaws.com`. Se ti connetti a un'istanza di database tramite un proxy, utilizza questi campi per specificare i dettagli di connessione del proxy.
 - Autenticazione: AWS IAM (autenticazione tramite credenziali IAM).
 - Utente: il nome dell'account dell'utente del database.
 - Credenziali: le credenziali utilizzate per accedere all'account AWS.
 - Regione: la regione AWS in cui è ospitato il database.
 - Host/Porta RDS: l'endpoint e la porta per il database come elencati nel Console di gestione AWS. Se utilizzi un endpoint diverso per connetterti a un'istanza di database, specifica i dettagli di connessione del proxy nei campi Host/Porta (descritti in precedenza).
 - Database: il nome del database.
 - URL: l'URL che l'IDE JetBrains utilizzerà per la connessione al database.



Note

Per una descrizione completa delle impostazioni di connessione che puoi configurare dalla finestra di dialogo Origini dati e driver, consulta la [documentazione relativa all'IDE JetBrains](#) che stai utilizzando.

7. Per verificare che le impostazioni di connessione siano corrette, scegli Testa la connessione.

Un segno di spunta verde indica che il test è andato a buon fine.

8. Scegli Applica per applicare le impostazioni, quindi seleziona OK per iniziare a utilizzare l'origine dati.

Si apre la finestra degli strumenti Database. Le origini dati disponibili vengono visualizzate sotto forma di albero con nodi che rappresentano elementi del database come schemi, tabelle e chiavi.

 **Important**

Per utilizzare la finestra degli strumenti Database, devi prima scaricare e installare DataGrip da JetBrains. Per ulteriori informazioni, consulta la pagina <https://www.jetbrains.com/datagrip/>.

Connect with Secrets Manager

1. Aprire AWS Explorer, se non è già aperto.
2. Fai clic sul nodo Amazon RDS per espandere l'elenco dei motori di database supportati.
3. Fai clic su un nodo del motore di database supportato (Aurora, MySQL o PostgreSQL) per espandere l'elenco delle istanze di database disponibili.

 **Note**

Se si seleziona Aurora, è possibile scegliere tra espandere un cluster MySQL e un cluster PostgreSQL.

4. Fai clic con il pulsante destro del mouse su un database e scegli Connottiti tramite Secrets Manager.

 **Note**

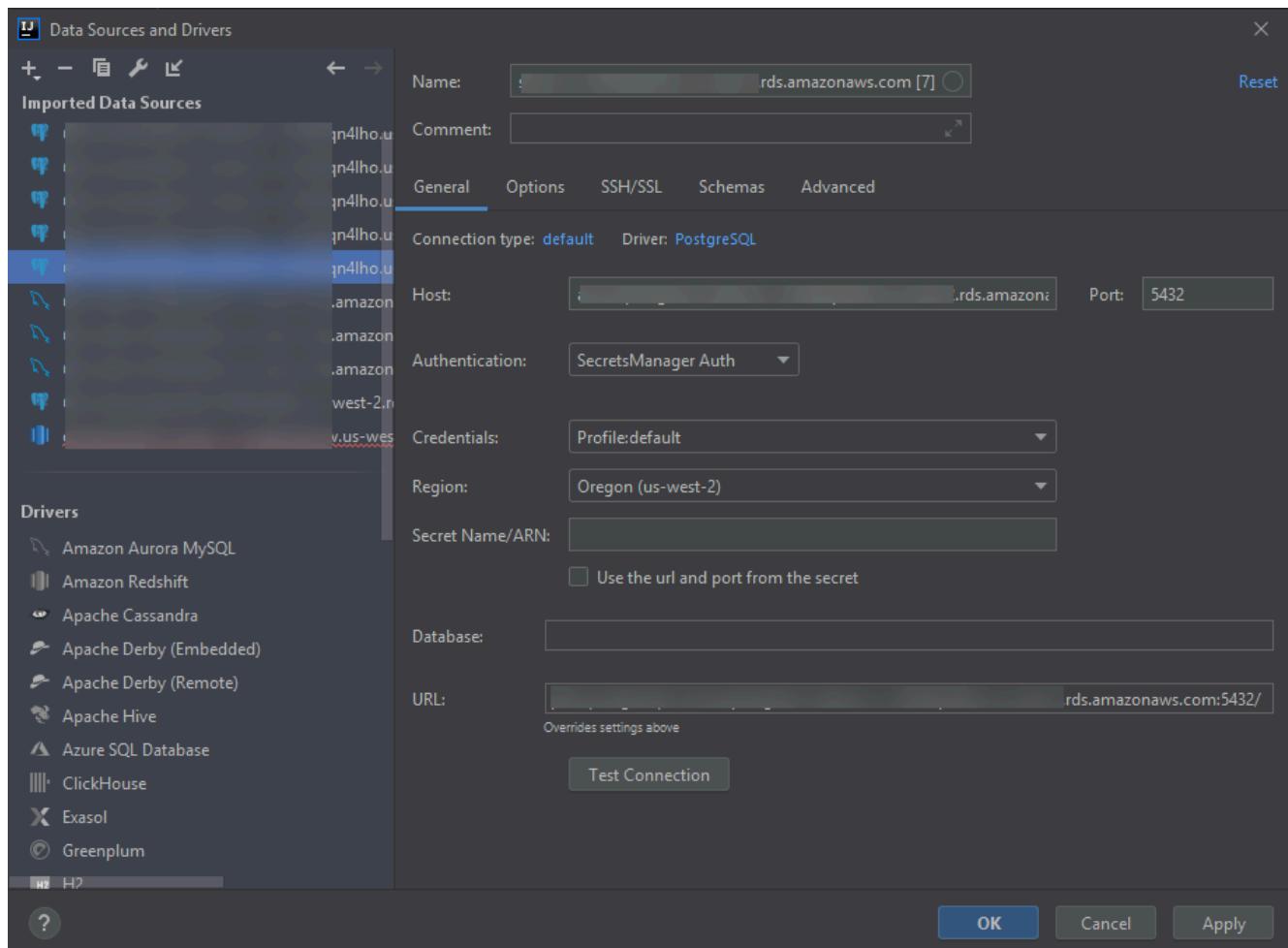
È anche possibile scegliere Copia ARN per aggiungere il nome della risorsa Amazon (ARN) del database agli appunti.

5. Nella finestra di dialogo Seleziona un segreto del database, utilizza il campo a discesa per selezionare le credenziali per il database, quindi scegli Crea.
6. Nella finestra di dialogo Origini dati e driver, esegui le operazioni seguenti per verificare che sia possibile stabilire una connessione al database:
 - Nel riquadro Origini dati importati, verifica che sia selezionata l'origine dati corretta.

- Se appare il messaggio Scarica i file dei driver mancanti, scegli Vai al driver (l'icona a forma di chiave inglese) per scaricare i file richiesti.
7. Nella scheda Generale del riquadro Impostazioni, verifica che i seguenti campi visualizzino i valori corretti:
- Host/Porta: l'endpoint e la porta utilizzati per le connessioni al database. Per i database Amazon RDS ospitati nel cloud AWS, gli endpoint terminano sempre con `rds.amazon.com`. Se ti connetti a un database tramite un proxy, utilizza questi campi per specificare i dettagli di connessione del proxy.
 - Autenticazione: SecretsManager Auth (autenticazione tramite Gestione dei segreti AWS).
 - Credenziali: le credenziali utilizzate per accedere all'account AWS.
 - Regione: la regione AWS in cui è ospitato il database.
 - Nome/ARN del segreto: il nome e l'ARN del segreto contenente le credenziali di autenticazione. Per sovrascrivere le impostazioni di connessione nei campi Host/Porta, seleziona la casella di controllo Utilizza l'URL e la porta del segreto.
 - Database: il nome dell'istanza di database selezionata dall'Esploratore AWS.
 - URL: l'URL che l'IDE JetBrains utilizzerà per la connessione al database.

 Note

Se utilizzi Secrets Manager per l'autenticazione, non sono presenti campi per il nome utente e la password per il database. Queste informazioni sono contenute nella parte relativa ai dati segreti crittografati di un segreto.



Note

Per una descrizione completa delle impostazioni di connessione che puoi configurare dalla finestra di dialogo Origini dati e driver, consulta la [documentazione relativa all'IDE JetBrains](#) che stai utilizzando.

8. Per verificare che le impostazioni di connessione siano corrette, scegli Testa la connessione.
Un segno di spunta verde indica che il test è andato a buon fine.
9. Scegli Applica per applicare le impostazioni, quindi seleziona OK per iniziare a utilizzare l'origine dati.

Si apre la finestra degli strumenti Database. Le origini dati disponibili vengono visualizzate sotto forma di albero con nodi che rappresentano elementi del database come schemi, tabelle e chiavi.

 **Important**

Per utilizzare la finestra degli strumenti Database, devi prima scaricare e installare DataGrip da JetBrains. Per ulteriori informazioni, consulta la pagina <https://www.jetbrains.com/datagrip/>.

Accesso ad Amazon Redshift tramite il AWS Toolkit for JetBrains

Un data warehouse di Amazon Redshift è un sistema di query e gestione di database relazionali di livello aziendale. Con il AWS Toolkit for JetBrains, è possibile connettersi ai cluster Amazon Redshift e interagire con essi. Un cluster Amazon Redshift è costituito da una raccolta di nodi che consente ai client di interrogare i database ospitati su quel cluster.

Negli argomenti seguenti vengono descritti i prerequisiti per accedere ai cluster Amazon Redshift e come utilizzare il AWS Toolkit for JetBrains per connettersi a un database in un cluster.

Argomenti

- [Prerequisiti per l'accesso ai cluster Amazon Redshift](#)
- [Connessione a un cluster Amazon Redshift](#)

Prerequisiti per l'accesso ai cluster Amazon Redshift

Prima di iniziare a interagire con un cluster Amazon Redshift utilizzando AWS Toolkit for JetBrains, è necessario completare le seguenti attività:

- [Creazione di un cluster Amazon Redshift e configurazione del relativo metodo di autenticazione](#)
- [Download e installazione di DataGrip](#)

Creazione di un cluster Amazon Redshift e configurazione del relativo metodo di autenticazione

AWS Toolkit for JetBrains consente di connettersi a un cluster Amazon Redshift già creato e configurato in AWS. Ciascun cluster contiene uno o più database. Per informazioni sulla creazione e sulla configurazione di cluster Amazon Redshift, consulta la pagina [Nozioni di base su Amazon Redshift](#) della Guida alle operazioni di base di Amazon Redshift.

Quando ci si connette a un cluster tramite il AWS Toolkit for JetBrains, gli utenti possono scegliere di autenticarsi utilizzando le credenziali IAM oppure Gestione dei segreti AWS. La tabella seguente descrive le funzionalità e le risorse informative principali per entrambe le opzioni:

Metodi di autenticazione	Come funziona	Ulteriori informazioni
Connessione con le credenziali IAM	<p>Con l'autenticazione del database IAM, non occorre archiviare le credenziali dell'utente nel database, perché l'autenticazione è gestita esternamente utilizzando le credenziali AWS Identity and Access Management (IAM).</p> <p>Per impostazione predefinita, l'autenticazione al database mediante IAM è disabilitata nelle istanze di database. Puoi abilitare l'autenticazione database IAM (o disabilitarla di nuovo) tramite la Console di gestione AWS, l'AWS CLI o l'API.</p>	<ul style="list-style-type: none"> • Gestione delle identità e degli accessi in Amazon Redshift nella Guida alla gestione di Amazon Redshift.
Connessione con Gestione dei segreti AWS;	<p>Un amministratore database può memorizzare le credenziali per un database come segreto in Secrets Manager.</p>	<ul style="list-style-type: none"> • Cos'è AWS Secrets Manager? nella Guida per l'utente di Gestione dei segreti AWS.

Metodi di autenticazione	Come funziona	Ulteriori informazioni
	<p>Secrets Manager crittografa e archivia le credenziali all'interno del segreto come testo segreto protetto.</p> <p>Quando un'applicazione dotata di autorizzazioni accede al database, Secrets Manager decripta il testo segreto protetto e lo restituisce su un canale protetto. Il client analizza le credenziali restituite, la stringa di connessione e qualsiasi altra informazione richiesta e utilizza tali informazioni per accedere al database.</p>	<ul style="list-style-type: none"> • Rotazione dei segreti per Amazon Redshift nella Guida per l'utente di Gestione dei segreti AWS. • Blog sulla sicurezza di AWS: Come ruotare le credenziali di Amazon DocumentDB e Amazon Redshift in Secrets Manager.

Utilizzo dei database Amazon RDS con DataGrip

Dopo aver eseguito la connessione a un database nel cluster Amazon Redshift, puoi iniziare a interagire con esso. Utilizzando DataGrip di JetBrains, è possibile eseguire attività di database come la scrittura di SQL, l'esecuzione di query e l'importazione/esportazione di dati. Le funzionalità fornite da DataGrip sono disponibili anche nel plug-in del database per una serie di IDE JetBrains. Per informazioni su DataGrip, consulta la pagina <https://www.jetbrains.com/datagrip/>.

Connessione a un cluster Amazon Redshift

Con l'Esploratore AWS, puoi selezionare un cluster Amazon Redshift, scegliere un metodo di autenticazione e quindi configurare le impostazioni di connessione. Dopo aver verificato che la connessione funziona, puoi iniziare a interagire con l'origine dati utilizzando JetBrains DataGrip.

Important

Assicurati di aver completato i [prerequisiti](#) affinché gli utenti possano accedere ai cluster Amazon Redshift e interagire con essi.

Seleziona una scheda per ottenere istruzioni sulla connessione a un cluster utilizzando il tuo metodo di autenticazione preferito.

Connect with IAM credentials

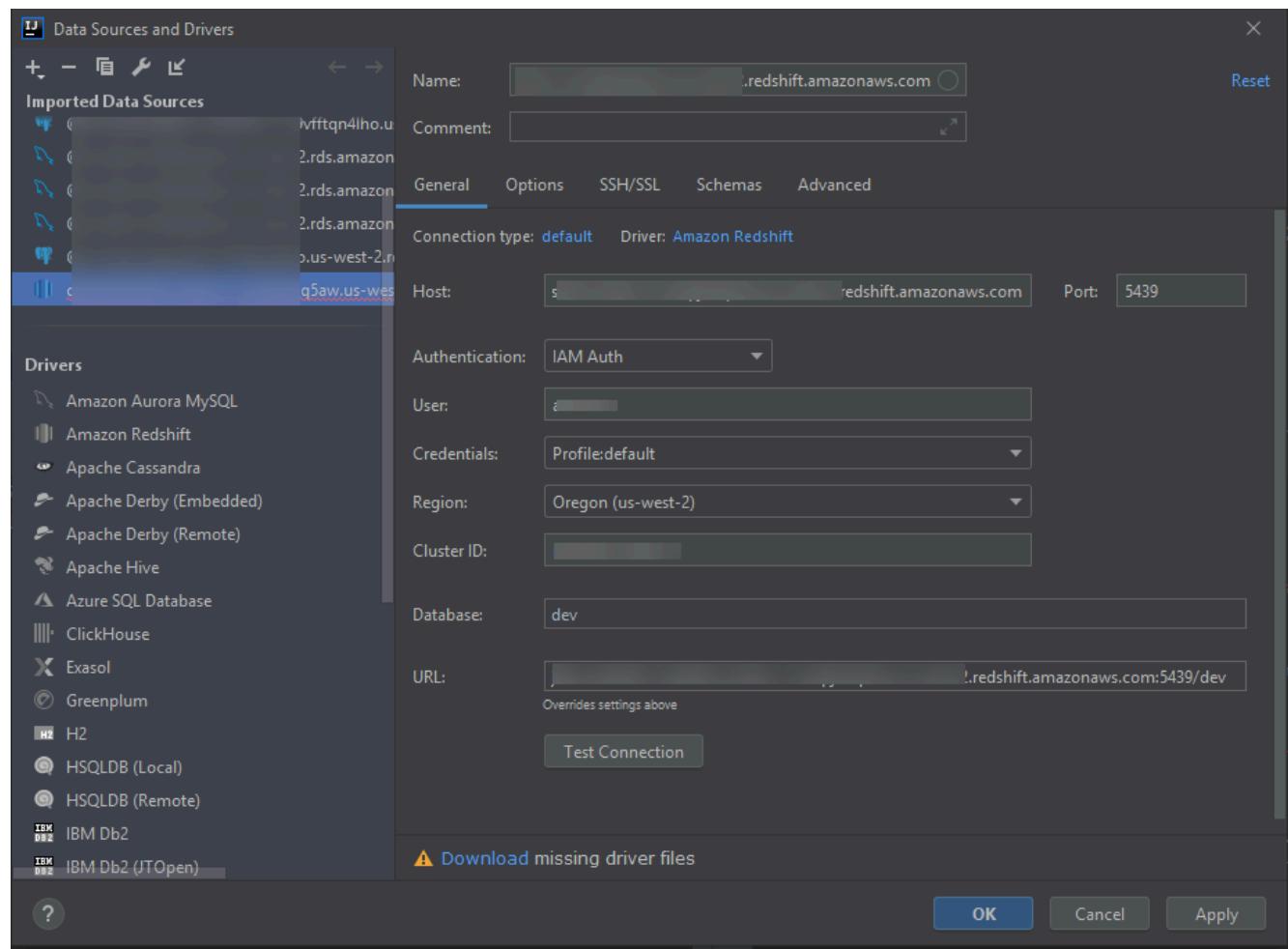
1. Aprire AWS Explorer, se non è già aperto.
2. Fai clic sul nodo Amazon Redshift per espandere l'elenco dei cluster disponibili.
3. Fai clic con il pulsante destro del mouse su un cluster e scegli Connottiti tramite credenziali IAM.

Note

È anche possibile scegliere Copia ARN per aggiungere il nome della risorsa Amazon (ARN) del cluster agli appunti.

4. Nella finestra di dialogo Origini dati e driver, esegui le operazioni seguenti per verificare che sia possibile stabilire una connessione al database:
 - Nel riquadro Origini dati importati, verifica che sia selezionata l'origine dati corretta.
 - Se appare il messaggio Scarica i file dei driver mancanti, scegli Vai al driver (l'icona a forma di chiave inglese) per scaricare i file richiesti.
5. Nella scheda Generale del riquadro Impostazioni, verifica che i seguenti campi visualizzino i valori corretti:
 - Host/Porta: l'endpoint e la porta utilizzati per le connessioni al cluster. Per i cluster Amazon Redshift ospitati nel cloud AWS, gli endpoint terminano sempre con `redshift.amazonaws.com`.
 - Autenticazione: AWS IAM (autenticazione tramite credenziali IAM).
 - Utente: il nome dell'account dell'utente del database.
 - Credenziali: le credenziali utilizzate per accedere all'account AWS.
 - Regione: la regione AWS in cui è ospitato il database.

- ID del cluster: l'ID del cluster in cui hai selezionato l'Esploratore AWS.
- Database: il nome del database nel cluster al quale ti connetterai.
- URL: l'URL che l'IDE JetBrains utilizzerà per la connessione al database del cluster.



Note

Per una descrizione completa delle impostazioni di connessione che puoi configurare dalla finestra di dialogo Origini dati e driver, consulta la [documentazione relativa all'IDE JetBrains](#) che stai utilizzando.

6. Per verificare che le impostazioni di connessione siano corrette, scegli Testa la connessione.

Un segno di spunta verde indica che il test è andato a buon fine.

7. Scegli Applica per applicare le impostazioni, quindi seleziona OK per iniziare a utilizzare l'origine dati.

Si apre la finestra degli strumenti Database. Le origini dati disponibili vengono visualizzate sotto forma di albero con nodi che rappresentano elementi del database come schemi, tabelle e chiavi.

 **Important**

Per utilizzare la finestra degli strumenti Database, devi prima scaricare e installare DataGrip da JetBrains. Per ulteriori informazioni, consulta la pagina <https://www.jetbrains.com/datagrip/>.

Connect with Secrets Manager

1. Aprire AWS Explorer, se non è già aperto.
2. Fai clic sul nodo Amazon Redshift per espandere l'elenco dei cluster disponibili.
3. Fai clic con il pulsante destro del mouse su un cluster e scegli Connottiti tramite Secrets Manager.

 **Note**

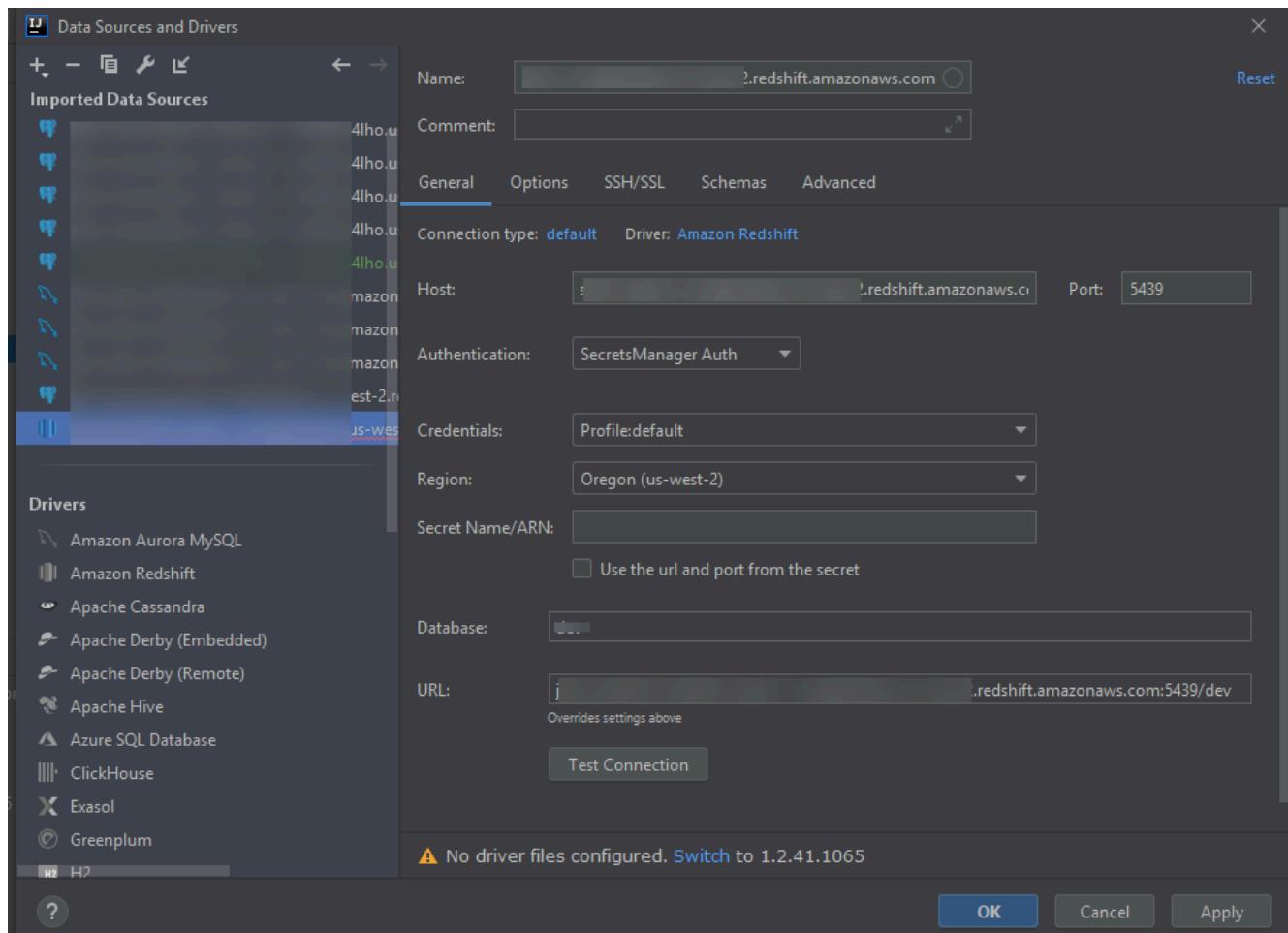
È anche possibile scegliere Copia ARN per aggiungere il nome della risorsa Amazon (ARN) del cluster agli appunti.

4. Nella finestra di dialogo Seleziona un segreto del database, utilizza il campo a discesa per selezionare le credenziali per il database, quindi scegli Crea.
5. Nella finestra di dialogo Origini dati e driver, esegui le operazioni seguenti per verificare che sia possibile stabilire una connessione al database:
 - Nel riquadro Origini dati importati, verifica che sia selezionata l'origine dati corretta.
 - Se nella finestra di dialogo viene visualizzato un messaggio per Scaricare i file dei driver mancanti, scegli Vai al driver (l'icona a forma di chiave inglese) per scaricare i file richiesti.
6. Nella scheda Generale del riquadro Impostazioni, verifica che i seguenti campi visualizzino i valori corretti:

- Host/Porta: l'endpoint e la porta utilizzati per le connessioni al cluster. Per i cluster Amazon Redshift ospitati nel cloud AWS, gli endpoint terminano sempre con `redshift.amazonaws.com`.
- Autenticazione: SecretsManager Auth (autenticazione tramite Gestione dei segreti AWS).
- Credenziali: le credenziali utilizzate per effettuare la connessione all'account AWS.
- Regione: la regione AWS in cui è ospitato il cluster.
- Nome/ARN del segreto: il nome e l'ARN del segreto contenente le credenziali di autenticazione. Se desideri sovrascrivere le impostazioni di connessione nei campi Host/ Porta, seleziona la casella di controllo Utilizza l'URL e la porta del segreto.
- Database: il nome del database nel cluster al quale ti connetterai.
- URL: l'URL che l'IDE JetBrains utilizzerà per la connessione al database.

 Note

Se utilizzi Gestione dei segreti AWS per l'autenticazione, non sono presenti campi per specificare il nome utente e la password per il cluster. Queste informazioni sono contenute nella parte relativa ai dati segreti crittografati di un segreto.



Note

Per una descrizione completa delle impostazioni di connessione che puoi configurare dalla finestra di dialogo Origini dati e driver, consulta la [documentazione relativa all'IDE JetBrains](#) che stai utilizzando.

7. Per verificare che le impostazioni di connessione siano corrette, scegli Testa la connessione.

Un segno di spunta verde indica che il test è andato a buon fine.

8. Scegli Applica per applicare le impostazioni, quindi seleziona OK per iniziare a utilizzare l'origine dati.

Si apre la finestra degli strumenti Database. Le origini dati disponibili vengono visualizzate sotto forma di albero con nodi che rappresentano elementi del database come schemi, tabelle e chiavi.

⚠ Important

Per utilizzare la finestra degli strumenti Database, devi prima scaricare e installare DataGrip da JetBrains. Per ulteriori informazioni, consulta la pagina <https://www.jetbrains.com/datagrip/>.

Utilizzo di Amazon S3 tramite il AWS Toolkit for JetBrains

Negli argomenti seguenti viene descritto come utilizzare il AWS Toolkit for JetBrains per lavorare con i bucket e gli oggetti di Amazon S3 in un account AWS.

Argomenti

- [Utilizzo dei bucket Amazon S3 tramite il AWS Toolkit for JetBrains](#)
- [Utilizzo degli oggetti Amazon S3 tramite il AWS Toolkit for JetBrains](#)

Utilizzo dei bucket Amazon S3 tramite il AWS Toolkit for JetBrains

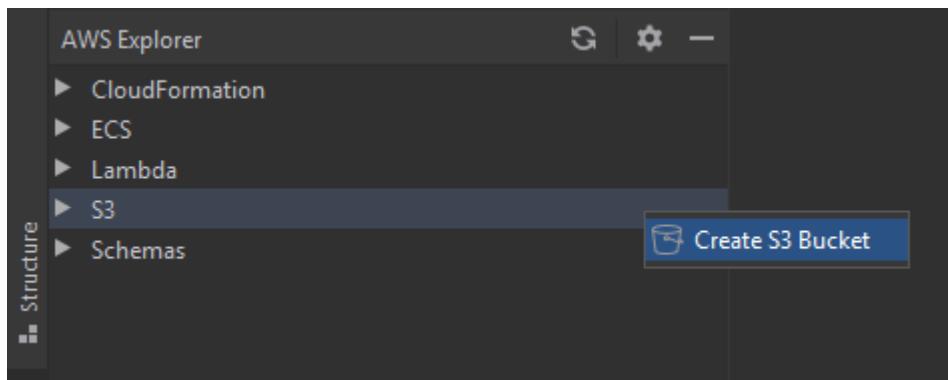
Ogni oggetto archiviato in Amazon S3 risiede in un bucket. I bucket consentono di raggruppare oggetti correlati nello stesso modo in cui si utilizza una directory per raggruppare i file in un file system.

Argomenti

- [Creazione di un bucket Amazon S3](#)
- [Visualizzazione dei bucket Amazon S3](#)
- [Eliminazione di un bucket Amazon S3](#)

Creazione di un bucket Amazon S3

1. Aprire AWS Explorer, se non è già aperto.
2. Fai clic con il pulsante destro del mouse sul nodo Amazon S3 e scegli Crea bucket S3.



3. Nella finestra di dialogo Create S3 Bucket (Crea bucket S3) immettere un nome per il bucket.

Nota

Poiché Amazon S3 supporta l'uso del bucket come URL a cui è possibile accedere pubblicamente, il nome di bucket selezionato deve essere univoco a livello globale. Se alcuni altri account hanno già creato un bucket con il nome scelto, devi utilizzare un altro nome. Per ulteriori informazioni, consulta [Restrizioni e limitazioni dei bucket](#) nella Guida per l'utente di Amazon Simple Storage Service.

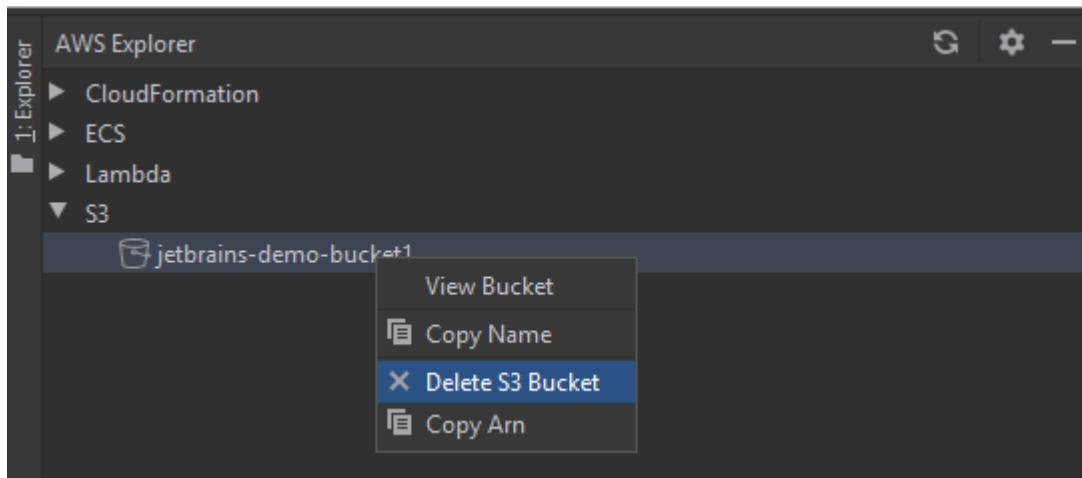
4. Seleziona Crea.

Visualizzazione dei bucket Amazon S3

1. Aprire AWS Explorer, se non è già aperto.
2. Fai clic sul nodo Amazon S3 per espandere l'elenco dei bucket.
 - I bucket S3 per la [regione AWS corrente](#) vengono visualizzati sotto il nodo Amazon S3.

Eliminazione di un bucket Amazon S3

1. Apri l'Esploratore AWS, se non lo hai già fatto.
2. Fai clic sul nodo Amazon S3 per espandere l'elenco dei bucket.
3. Fare clic con il pulsante destro del mouse sul bucket da eliminare, quindi scegliere Delete S3 Bucket (Elimina bucket S3).



4. Immettere il nome del bucket per confermare l'eliminazione, quindi scegliere OK.
 - Se il bucket contiene oggetti, il bucket viene svuotato prima dell'eliminazione. Una notifica viene visualizzata al termine dell'eliminazione.

Utilizzo degli oggetti Amazon S3 tramite il AWS Toolkit for JetBrains

Gli oggetti sono le entità fondamentali archiviate in Amazon S3 e sono composti da dati e metadata.

Argomenti

- [Visualizzazione di un oggetto in un bucket Amazon S3](#)
- [Apertura di un oggetto nell'IDE](#)
- [Caricamento di un oggetto](#)
- [Download di un oggetto](#)
- [Eliminazione di un oggetto](#)

Visualizzazione di un oggetto in un bucket Amazon S3

Questa procedura apre S3 Bucket Viewer (Visualizzatore bucket S3). È possibile utilizzarlo per visualizzare, caricare, scaricare ed eliminare oggetti raggruppati per cartelle in un bucket Amazon S3.

1. Aprire AWS Explorer, se non è già aperto.
2. Per visualizzare gli oggetti di un bucket, eseguire una delle operazioni seguenti:
 - Fare doppio clic sul nome del bucket.

- Fare clic con il pulsante destro del mouse sul nome del bucket e quindi scegliere View Bucket (Visualizza bucket).

In S3 Bucket Viewer (Visualizzatore bucket S3) vengono visualizzate le informazioni sul nome, sull'[Amazon Resource Name \(ARN\)](#) e sulla data di creazione del bucket. Gli oggetti e le cartelle nel bucket sono disponibili nel riquadro sottostante.

Apertura di un oggetto nell'IDE

Se l'oggetto in un bucket Amazon S3 è un tipo di file riconosciuto dall'IDE, puoi scaricare una copia di sola lettura e aprirlo nell'IDE.

1. Per trovare un oggetto da scaricare, aprire S3 Bucket Viewer (Visualizzatore bucket S3) (vedere [Visualizzazione di un oggetto in un bucket Amazon S3](#)).
2. Fare doppio clic sul nome dell'oggetto.

Il file viene aperto nella finestra IDE predefinita per quel tipo di file.

Caricamento di un oggetto

1. Per trovare la cartella in cui si desidera caricare gli oggetti, aprire S3 Bucket Viewer (Visualizzatore bucket S3) (vedere [Visualizzazione di un oggetto in un bucket Amazon S3](#)).
2. Fare clic con il pulsante destro del mouse sulla cartella e scegliere Upload (Carica).
3. Nella finestra di dialogo, selezionare i file da caricare.

 Nota

È possibile caricare più file contemporaneamente. Non puoi caricare le directory.

4. Scegli OK.

Download di un oggetto

1. Per trovare una cartella da cui scaricare oggetti, aprire S3 Bucket Viewer (Visualizzatore bucket S3) (vedere [Visualizzazione di un oggetto in un bucket Amazon S3](#)).
2. Scegliere una cartella per visualizzarne gli oggetti.
3. Fare clic con il pulsante destro del mouse su un oggetto, quindi scegliere Download (Scarica).

4. Nella finestra di dialogo, selezionare il percorso di download.

 Nota

Se stai scaricando più file, assicurati di selezionare il nome del percorso anziché la cartella. Non è possibile scaricare le directory.

5. Scegli OK.

 Nota

Se un file esiste già nel percorso di download, puoi sovrascriverlo o lasciarlo in posizione ignorando il download.

Eliminazione di un oggetto

1. Per trovare l'oggetto da eliminare, aprire S3 Bucket Viewer (Visualizzatore bucket S3) (vedere [Visualizzazione di un oggetto in un bucket Amazon S3](#)).
2. Dopo aver selezionato l'oggetto, eliminarlo eseguendo una delle seguenti operazioni:
 - Premere Delete (Elimina).
 - Fare clic con il pulsante destro del mouse, quindi scegliere Delete (Elimina).

 Nota

Puoi selezionare ed eliminare più oggetti contemporaneamente.

3. Per confermare l'eliminazione, scegliere Delete (Elimina).

Utilizzo delle applicazioni serverless AWS tramite il AWS Toolkit for JetBrains

Negli argomenti seguenti viene descritto come usare AWS Toolkit for JetBrains per utilizzare le applicazioni serverless AWS in un account AWS.

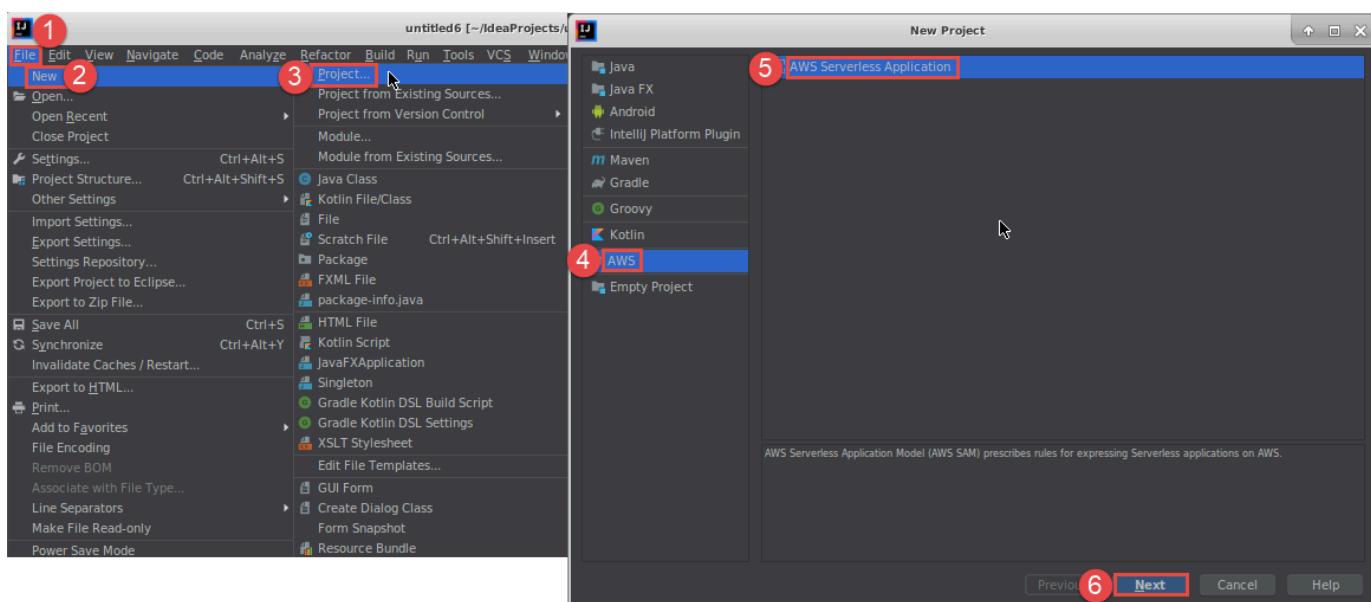
Argomenti

- [Creazione di un'applicazione serverless AWS tramite il AWS Toolkit for JetBrains](#)
- [Sincronizzazione delle applicazioni AWS SAM tramite il AWS Toolkit for JetBrains](#)
- [Modifica \(aggiornamento\) delle impostazioni dell'applicazione serverless AWS tramite il AWS Toolkit for JetBrains](#)
- [Eliminazione di un'applicazione serverless AWS tramite il AWS Toolkit for JetBrains](#)

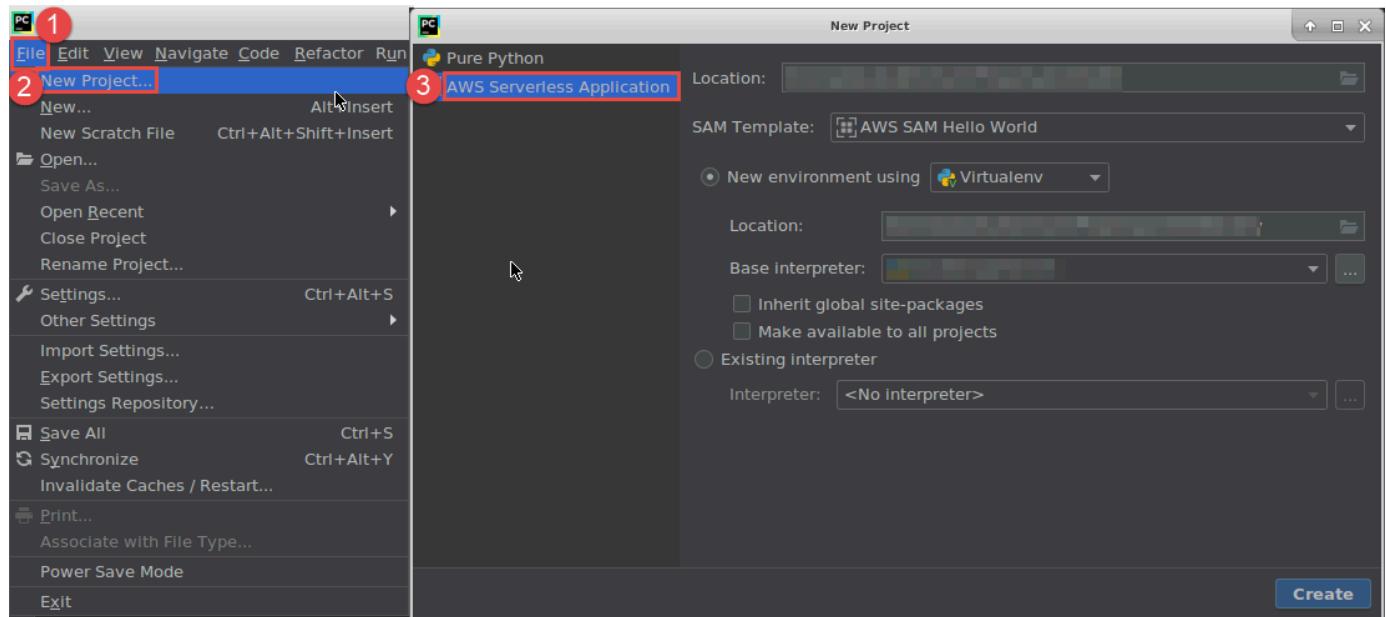
Creazione di un'applicazione serverless AWS tramite il AWS Toolkit for JetBrains

Per completare questa procedura, devi innanzitutto installare il Kit di strumenti AWS e, se non l'hai ancora fatto, effettuare la prima connessione a un account AWS. Quindi, con IntelliJ IDEA, PyCharm, WebStorm o JetBrains Rider già in esecuzione, effettua le seguenti operazioni."?>

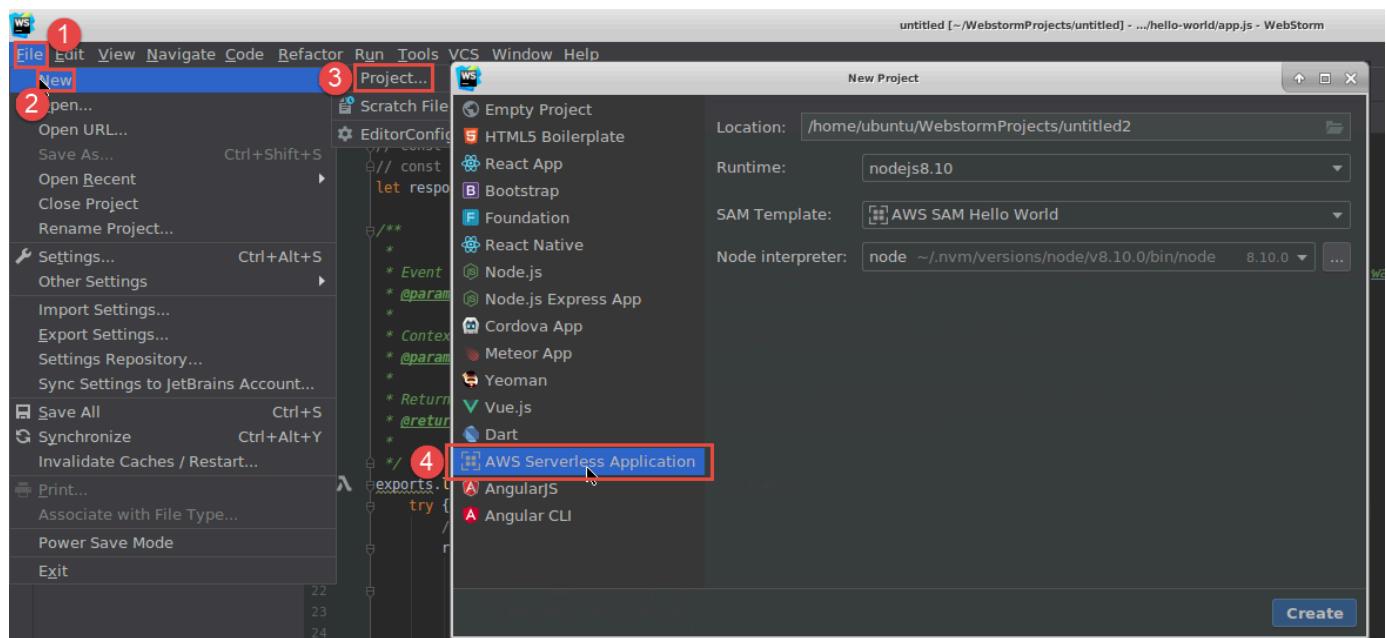
1. Con IntelliJ IDEA, PyCharm, WebStorm o JetBrains Rider già in esecuzione, effettua una delle seguenti operazioni:
 - Per IntelliJ IDEA o WebStorm, scegli File, Nuovo, Progetto.
 - Per PyCharm, scegli File, Nuovo progetto.
 - Per JetBrains Rider, scegli File, Nuovo per una nuova soluzione. In alternativa, fare clic con il pulsante destro del mouse su una soluzione esistente nella finestra dello strumento Explorer e scegliere Add (Aggiungi), New Project (Nuovo progetto).
2. Per IntelliJ IDEA, scegli AWS, Applicazione serverless AWS, quindi scegli Successivo.



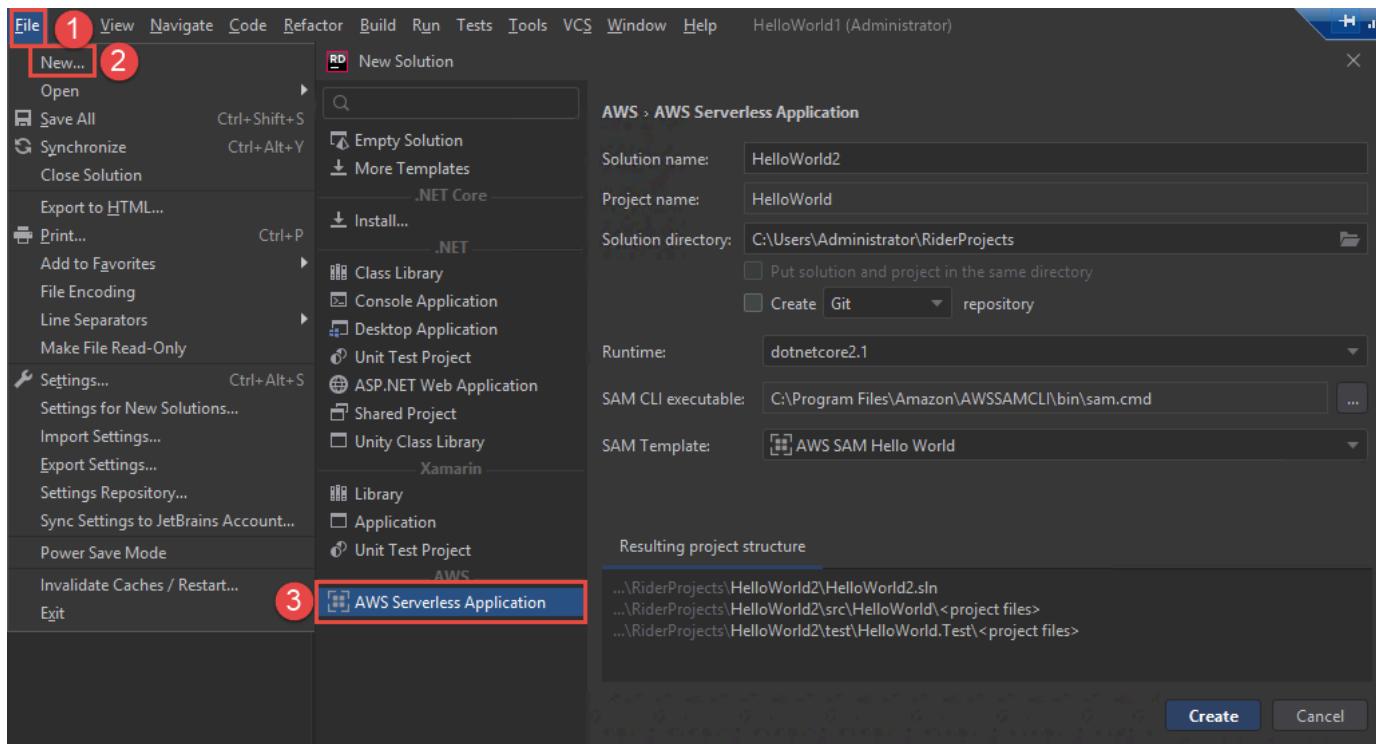
Per PyCharm, scegli Applicazione serverless AWS.



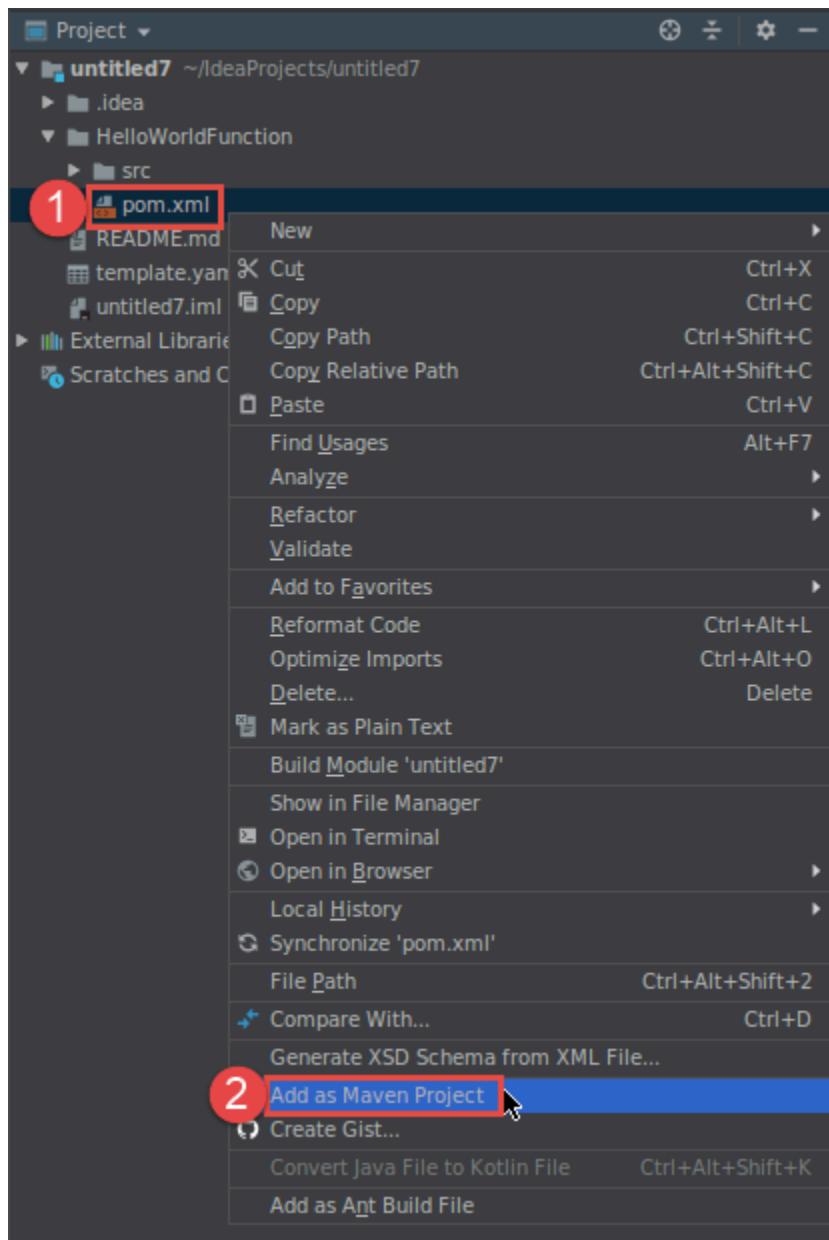
Per WebStorm, scegli Applicazione serverless AWS.



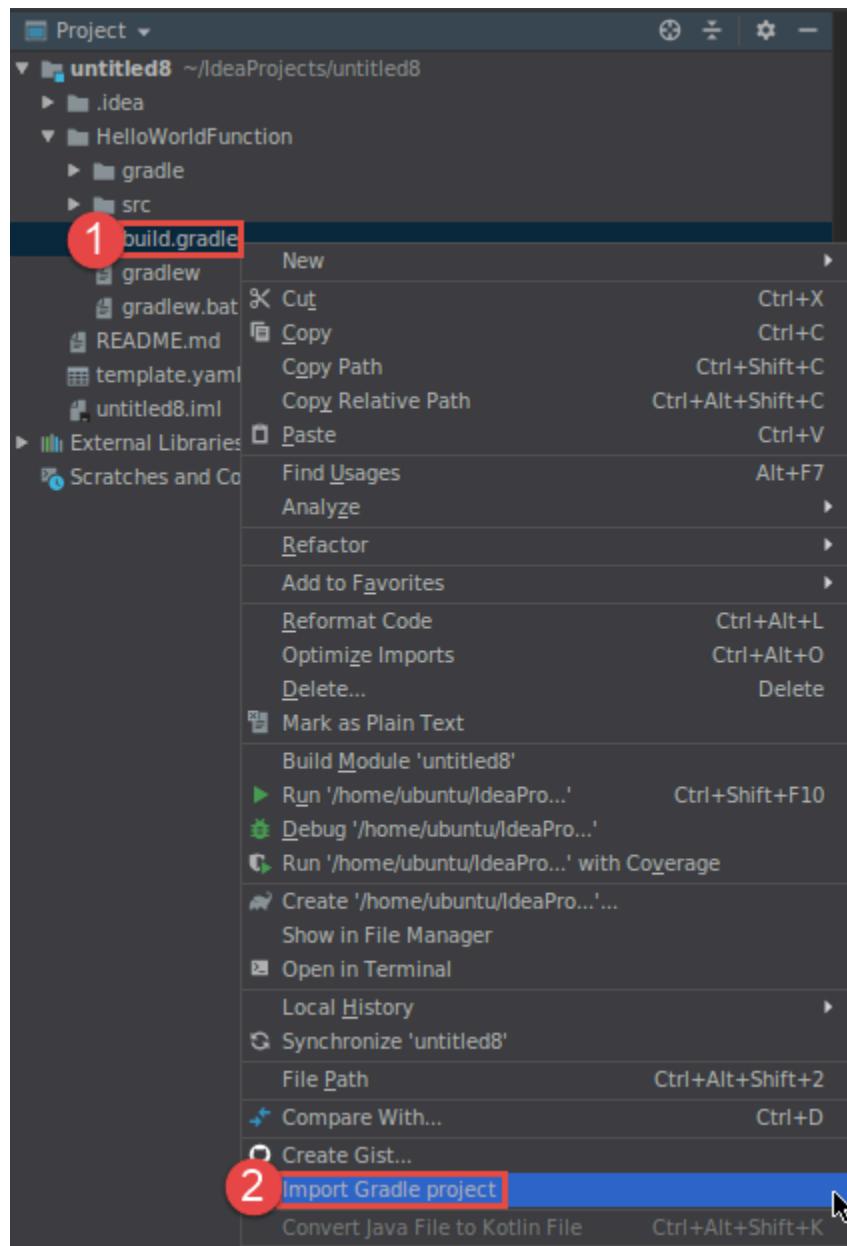
Per JetBrains Rider, scegli Applicazione serverless AWS.



- Completa le operazioni nella finestra di dialogo [Nuovo progetto o nella finestra di dialogo Nuova soluzione per JetBrains Rider](#), quindi scegli Fine (per IntelliJ IDEA) o Crea (per PyCharm, WebStorm o JetBrains). AWS Toolkit for JetBrains crea il progetto e aggiunge i file di codice dell'applicazione serverless al nuovo progetto.
- Se utilizzi IntelliJ IDEA, con la finestra dello strumento Progetto già aperta sul progetto che contiene i file dell'applicazione serverless, esegui una delle seguenti operazioni:
 - Per i progetti basati su Maven, fare clic con il pulsante destro del mouse sul file pom.xml del progetto e quindi scegliere Add as Maven Project (Aggiungi come progetto Maven).



- Per i progetti basati su Gradle, fare clic con il pulsante destro del mouse sul file build.gradle del progetto e quindi scegliere Import Gradle project (Importa progetto Gradle).



Completere le operazioni nella finestra di dialogo Import Module from Gradle (Importa modulo da Gradle) e quindi scegliere OK.

Dopo aver creato l'applicazione serverless, è possibile eseguire (richiamare) o sottoporre a debug della versione locale di una funzione AWS Lambda contenuta nell'applicazione.

È inoltre possibile distribuire l'applicazione serverless. Dopo averla implementata, è possibile eseguire (richiamare) la versione remota di una funzione Lambda che fa parte dell'applicazione implementata.

Sincronizzazione delle applicazioni AWS SAM tramite il AWS Toolkit for JetBrains

AWS Serverless Application Model (AWS SAM) `sam sync` è un processo di implementazione tramite comandi della CLI AWS SAM che identifica automaticamente le modifiche apportate alle applicazioni serverless, quindi sceglie il modo migliore per creare e implementare tali modifiche al Cloud AWS. Se hai apportato solo modifiche al codice dell'applicazione senza modificare l'infrastruttura, Sincronizzazione AWS SAM aggiorna la tua applicazione senza implementare nuovamente lo stack CloudFormation.

Per ulteriori informazioni sui comandi della CLI di `sam sync` e AWS SAM, consulta l'argomento [AWS SAM CLI command reference](#) della Guida per l'utente di AWS Serverless Application Model.

Nelle sezioni seguenti sono fornite le istruzioni per iniziare a lavorare con la sincronizzazione AWS SAM.

Prerequisiti

Prima di utilizzare la sincronizzazione AWS SAM devono essere soddisfatti i seguenti prerequisiti:

- Hai un'applicazione AWS SAM funzionante. Per ulteriori informazioni sulla creazione di un'applicazione AWS SAM, consulta l'argomento [Utilizzo di AWS SAM](#) di questa Guida per l'utente.
- Deve essere installata la versione 1.78.0 o successiva della CLI AWS SAM. Per ulteriori informazioni sull'installazione della CLI AWS SAM, consulta la pagina [Installing the AWS SAM CLI](#) della Guida per l'utente di AWS Serverless Application Model.
- L'applicazione è in esecuzione in un ambiente di sviluppo.

Note

Per sincronizzare e implementare un'applicazione serverless che contenga una funzione AWS Lambda con proprietà non predefinite, le proprietà facoltative devono essere impostate in un file di modello AWS SAM associato alla funzione AWS Lambda prima dell'implementazione.

Per ulteriori informazioni sulle proprietà di AWS Lambda, consulta la sezione [AWS::Serverless::Function](#) della Guida per l'utente di AWS Serverless Application Model su GitHub.

Nozioni di base

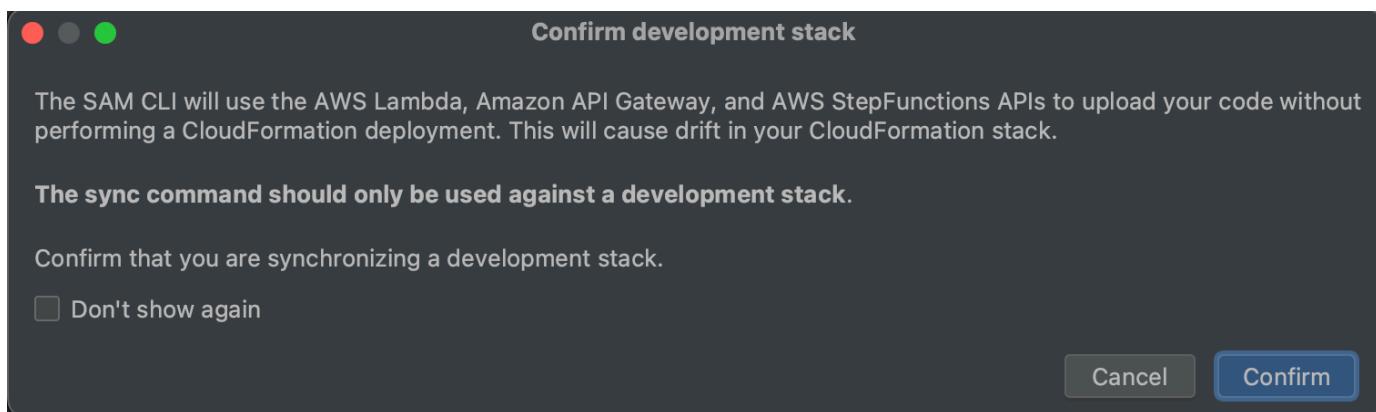
Per iniziare a lavorare con Sincronizzazione AWS SAM, completa la procedura seguente.

Note

Assicurati che la regione AWS sia impostata sulla posizione associata all'applicazione serverless.

Per ulteriori informazioni su come modificare la regione AWS dal AWS Toolkit for JetBrains, consulta l'argomento [Passare da una regione AWS all'altra](#) di questa Guida per l'utente.

1. Dal progetto dell'applicazione serverless, nella finestra degli strumenti di Progetto, apri il menu contestuale (con il pulsante destro del mouse) del file `template.yaml`.
2. Dal menu di scelta rapida `template.yaml`, scegli Sincronizza applicazioni serverless (precedentemente Implementa) per aprire la finestra di dialogo Verifica stack di sviluppo.
3. Verifica che stai lavorando da uno stack di sviluppo per aprire la finestra di dialogo Sincronizza applicazioni serverless.



4. Completa i passaggi indicati nella finestra di dialogo Sincronizza applicazioni serverless, quindi scegli Sincronizza per iniziare il processo di sincronizzazione di AWS SAM. Per ulteriori informazioni sulla finestra di dialogo Sincronizza applicazione serverless, consulta la sezione [the section called “Finestra di dialogo Sincronizza applicazioni serverless”](#) di seguito.
5. Durante il processo di sincronizzazione, la Run Window del AWS Toolkit for JetBrains viene aggiornata con lo stato dell'implementazione.
6. Se l'esito della sincronizzazione è positivo, il nome dello stack CloudFormation viene aggiunto all'Esploratore AWS.

Se la sincronizzazione fallisce, i dettagli per la risoluzione dei problemi sono indicati nella Run Window di JetBrains o nel log eventi di CloudFormation. Per ulteriori informazioni sulla visualizzazione dei log eventi di CloudFormation, consulta l'argomento [Visualizzazione dei log di eventi per uno stack](#) di questa Guida per l'utente.

Finestra di dialogo Sincronizza applicazioni serverless

La finestra di dialogo Sincronizza applicazioni serverless ti assiste nel processo di sincronizzazione di AWS SAM. Le seguenti sezioni sono descrizioni e dettagli per ciascuno dei diversi componenti della finestra di dialogo.

Crea stack o Aggiorna stack

Obbligatorio: per creare e configurare un nuovo stack CloudFormation di implementazione di applicazioni serverless, inserisci un nome nel campo fornito.

In alternativa, per eseguire l'implementazione su uno stack CloudFormation esistente, seleziona il nome dello stack dall'elenco degli stack associati al tuo account AWS che viene compilato automaticamente.

Parametri del modello

Facoltativo: viene compilato con un elenco di parametri rilevati dal file `template.yaml` di progetto. Per specificare i valori dei parametri, inserisci un nuovo valore di parametro nell'apposito campo di testo situato nella colonna valore.

Bucket S3

Obbligatorio: per scegliere un bucket Amazon Simple Storage Service (Amazon S3) per archiviare il modello CloudFormation, selezionalo dall'elenco.

Per creare un nuovo bucket Amazon S3 e utilizzarlo per l'archiviazione, scegli Crea e segui le istruzioni.

Repository ECR

Obbligatorio, visibile solo quando si lavora con un tipo di pacchetto Immagine: scegli l'URI di un repository Amazon Elastic Container Registry (Amazon ECR) esistente per l'implementazione dell'applicazione serverless.

Per ulteriori informazioni sulla differenza tra i tipi di pacchetto AWS Lambda, consulta la pagina [Generating sample event payloads](#) della Guida per gli sviluppatori di AWS Lambda.

Funzionalità di CloudFormation

Obbligatorio: scegli le funzionalità che CloudFormation è autorizzato a utilizzare durante la creazione di stack.

Tag

Facoltativo: inserisci i tag preferiti nei campi di testo forniti per etichettare un parametro.

Funzione build all'interno di un container

Facoltativo, Docker richiesto: la selezione di queste opzioni consente di creare le funzioni delle applicazioni serverless all'interno di un container Docker locale prima dell'implementazione. Questa opzione è utile se la funzione dipende da pacchetti con dipendenze o programmi compilati in modo nativo.

Per ulteriori informazioni, consulta l'argomento [Building applications](#) della Guida per gli sviluppatori di AWS Serverless Application Model.

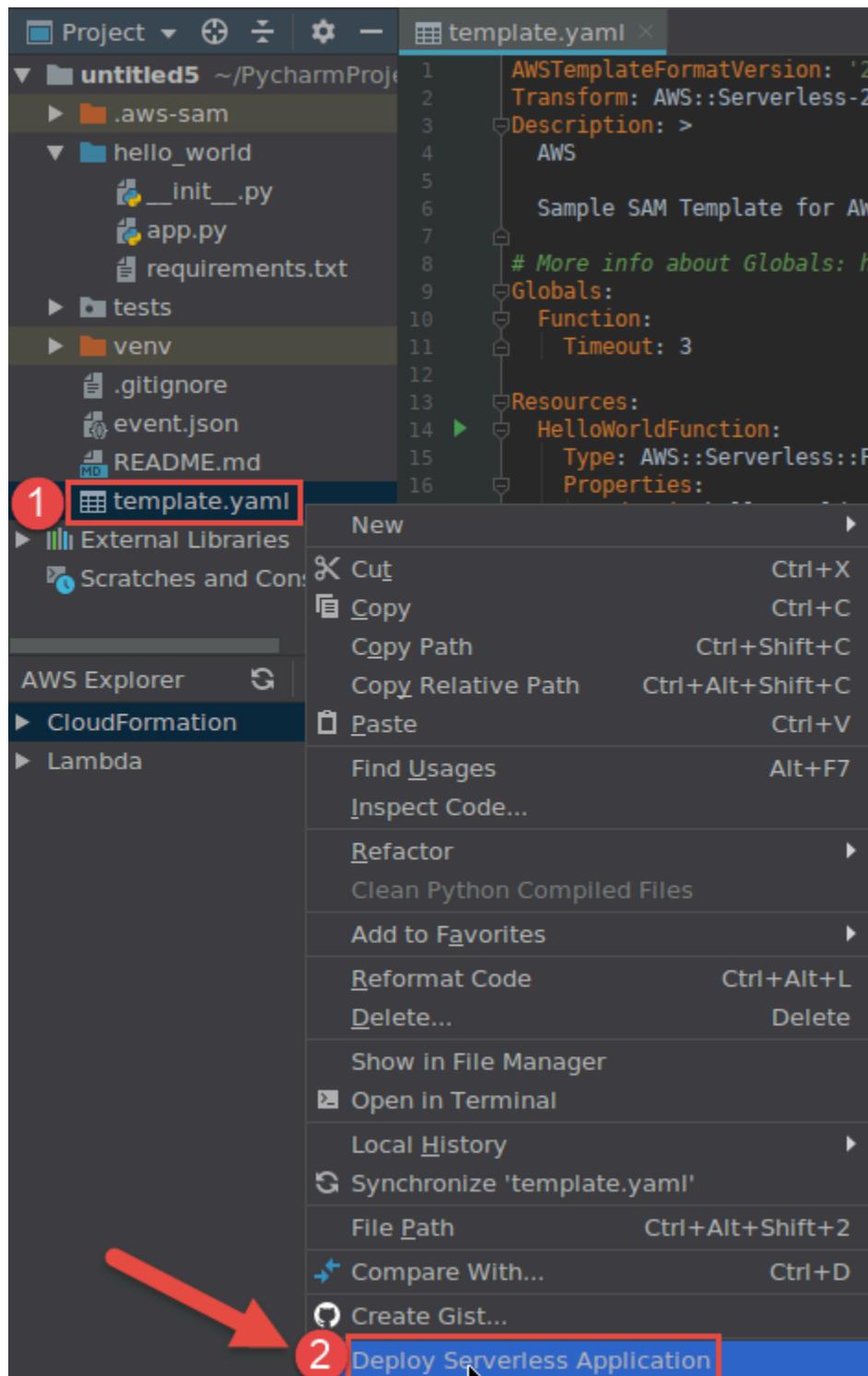
Modifica (aggiornamento) delle impostazioni dell'applicazione serverless AWS tramite il AWS Toolkit for JetBrains

Per prima cosa devi implementare l'applicazione serverless AWS che vuoi modificare, se non è ancora stato fatto.

Note

Per distribuire un'applicazione serverless contenente una funzione AWS Lambda e distribuirla con proprietà non predefinite o facoltative, è necessario innanzitutto impostare tali proprietà nel file modello AWS SAM corrispondente della funzione (ad esempio, in un file denominato `template.yaml` nel progetto). Per l'elenco delle impostazioni di proprietà disponibili, consulta [AWS::Serverless::Function](#) nel repository [awslabs/serverless-application-model](#) su GitHub.

1. Con la finestra dello strumento Project (Progetto) aperta con il progetto che contiene i file dell'applicazione serverless, aprire il file `template.yaml` del progetto. Modificare il contenuto del file per riflettere le nuove impostazioni, quindi salvare e chiudere il file.
2. Se devi passare a un'altra regione AWS per implementare l'applicazione serverless, esegui subito l'operazione.
3. Fare clic con il pulsante destro del mouse sul file `template.yaml` del progetto e quindi scegliere Deploy Serverless Application (Distribuisci applicazione serverless).



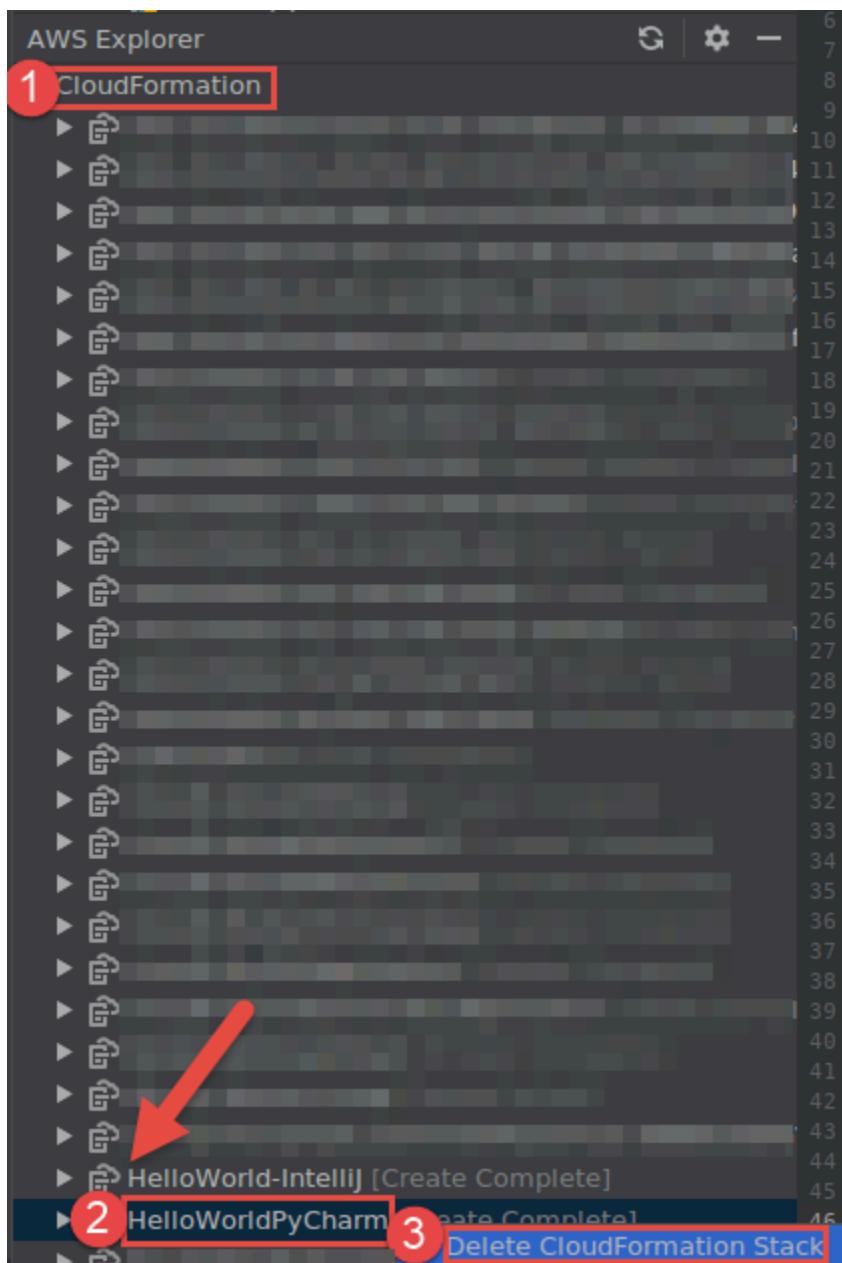
4. Completare le operazioni nella finestra di dialogo [Deploy Serverless Application \(Distribuisci applicazione serverless\)](#) e quindi scegliere Deploy (Distribuisci). AWS Toolkit for JetBrains aggiorna lo stack AWS CloudFormation corrispondente per la distribuzione.

Se l'implementazione non riesce, puoi provare a comprenderne il motivo visualizzando i log eventi per lo stack.

Eliminazione di un'applicazione serverless AWS tramite il AWS Toolkit for JetBrains

Prima di eliminare un'applicazione serverless AWS, è necessario implementarla.

1. Aprire AWS Explorer, se non è già aperto. Se devi passare alla regione AWS che contiene l'applicazione serverless, esegui subito l'operazione.
2. Espandere CloudFormation.
3. Fare clic con il pulsante destro del mouse sul nome dello stack AWS CloudFormation contenente l'applicazione serverless che si desidera eliminare e quindi scegliere Delete CloudFormation Stack (Elimina stack CloudFormation).



4. Immettere il nome dello stack per confermare l'eliminazione, quindi scegliere OK. Se l'eliminazione dello stack ha esito positivo, AWS Toolkit for JetBrains rimuove il nome dello stack dall'elenco CloudFormation in AWS Explorer. Se l'eliminazione dello stack non riesce, puoi provare a comprenderne il motivo visualizzando i log eventi per lo stack.

Utilizzo di Amazon Simple Queue Service tramite il AWS Toolkit for JetBrains

Negli argomenti seguenti viene descritto come utilizzare il servizio Amazon Simple Queue Service tramite il AWS Toolkit for JetBrains.

Argomenti

- [Utilizzo delle code Amazon Simple Queue Service](#)
- [Utilizzo di Amazon SQS con AWS Lambda nel AWS Toolkit for JetBrains](#)
- [Utilizzo di Amazon SQS con Amazon SNS nel AWS Toolkit for JetBrains](#)

Utilizzo delle code Amazon Simple Queue Service

Negli argomenti seguenti viene descritto come utilizzare il AWS Toolkit for JetBrains per lavorare con le code e i messaggi Amazon Simple Queue Service.

I due tipi di messaggi che puoi inviare utilizzando Amazon SQS nel AWS Toolkit for JetBrains sono Standard e FIFO (First-In-Last-Out).

Creazione di una coda Amazon SQS

1. Dal AWS Toolkit for JetBrains, espandi l'Esploratore AWS per visualizzare i servizi AWS.
2. Dall'Esploratore AWS, apri il menu contestuale (facendo clic con il pulsante destro del mouse) del servizio Amazon SQS e scegli Crea coda....
3. Fornisci un nome per la coda e scegli il tipo di coda.

Note

Per ulteriori informazioni sui tipi di coda, consulta gli argomenti [Amazon SQS standard queues](#) e [Amazon SQS FIFO \(First-In-First-Out\) queues](#) della Guida per gli sviluppatori di Amazon Simple Queue Service.

4. Seleziona Crea.

Visualizzazione dei messaggi Amazon SQS

1. Dal AWS Toolkit for JetBrains, espandi l'Esploratore AWS per visualizzare i servizi AWS.

2. Dall'Esploratore AWS, espandi il servizio Amazon SQS per visualizzare un elenco delle code esistenti.
3. Fai clic con il pulsante destro del mouse sulla coda che desideri visualizzare e scegli Visualizza messaggi.
4. Scegli Visualizza messaggi per visualizzare i messaggi in questa coda.

Modifica delle proprietà della coda Amazon SQS

1. Dal AWS Toolkit for JetBrains, espandi l'Esploratore AWS per visualizzare i servizi AWS.
2. Dall'Esploratore AWS, espandi il servizio Amazon SQS per visualizzare un elenco delle code esistenti.
3. Fai clic con il pulsante destro del mouse sulla coda che desideri modificare e scegli Modifica proprietà della coda....
4. Nella finestra di dialogo Modifica proprietà della coda che si apre, rivedi e modifica le proprietà della coda. Per ulteriori informazioni sulle proprietà di Amazon SQS, consulta la pagina [Configuring queue parameters \(console\)](#) della Guida per gli sviluppatori di Amazon Simple Queue Service.

Invio di messaggi standard

1. Dal AWS Toolkit for JetBrains, espandi l'Esploratore AWS per visualizzare i servizi AWS.
2. Dall'Esploratore AWS, espandi il servizio Amazon SQS per visualizzare un elenco delle code esistenti.
3. Fai clic con il pulsante destro del mouse sulla coda per inviare il messaggio e scegli Invia un messaggio.
4. Compila il messaggio e scegli Invia. Dopo aver inviato il messaggio, viene visualizzata una conferma che include l'ID del messaggio.

Invio di messaggi FIFO

1. Dal AWS Toolkit for JetBrains, espandi l'Esploratore AWS per visualizzare i servizi AWS.
2. Dall'Esploratore AWS, espandi il servizio Amazon SQS per visualizzare un elenco delle code esistenti.

3. Fai clic con il pulsante destro del mouse sulla coda per inviare il messaggio e scegli Invia un messaggio.
4. Inserisci il messaggio, l'ID del gruppo e un ID di deduplicazione facoltativo.

 Note

Se non viene fornito alcun ID di deduplicazione, ne verrà generato uno.

5. Scegliere Send (Invia). Dopo aver inviato il messaggio, viene visualizzata una conferma che include l'ID del messaggio.

Eliminazione di una coda Amazon SQS

1. Verifica che una coda sia vuota prima di eliminarla. Per ulteriori informazioni, consulta la pagina [Confirming that a queue is empty](#) della Guida per gli sviluppatori di Amazon Simple Queue Service.
2. Dal AWS Toolkit for JetBrains, espandi l'Esploratore AWS per visualizzare i servizi AWS.
3. Dall'Esploratore AWS, espandi il servizio Amazon SQS per visualizzare un elenco delle code esistenti.
4. Fai clic con il pulsante destro del mouse su Amazon SQS e scegli Elimina coda....
5. Conferma di voler eliminare la coda e scegli OK nella finestra di dialogo di eliminazione.

Utilizzo di Amazon SQS con AWS Lambda nel AWS Toolkit for JetBrains

La procedura seguente descrive nel dettaglio come configurare le code Amazon SQS come trigger Lambda nel AWS Toolkit for JetBrains.

Configurazione di una coda Amazon SQS come trigger Lambda

1. Dal AWS Toolkit for JetBrains, espandi l'Esploratore AWS per visualizzare i servizi AWS.
2. Dall'Esploratore AWS, espandi il servizio Amazon SQS per visualizzare un elenco delle code esistenti.
3. Fai clic con il pulsante destro del mouse sulla coda con cui desideri lavorare e scegli Configura trigger Lambda.
4. Nella finestra di dialogo, dal menu a discesa, scegli la funzione Lambda che desideri attivare.
5. Scegliere Configure (Configura).

6. Se la funzione Lambda non dispone delle autorizzazioni IAM necessarie affinché Amazon SQS possa eseguirla, il kit di strumenti genera una policy minima che puoi aggiungere al ruolo IAM per la funzione Lambda.

Scegli Aggiungi policy.

Dopo aver configurato la coda, riceverai un messaggio di stato sulle modifiche applicate, inclusi eventuali messaggi di errore applicabili.

Utilizzo di Amazon SQS con Amazon SNS nel AWS Toolkit for JetBrains

La procedura seguente descrive nel dettaglio come sottoscrivere le code Amazon SQS Standard agli argomenti Amazon SNS utilizzando il AWS Toolkit for JetBrains.

 Note

Non è possibile sottoscrivere le code Amazon SQS FIFO agli argomenti Amazon SNS.

Sottoscrizione di una coda Amazon SQS Standard a un argomento Amazon SNS

1. Dal AWS Toolkit for JetBrains, espandi l'Esploratore AWS per visualizzare i servizi AWS.
2. Dall'Esploratore AWS, espandi il servizio Amazon SQS per visualizzare un elenco delle code esistenti.
3. Fai clic con il pulsante destro del mouse sulla coda con cui desideri lavorare e scegli Sottoscrivi all'argomento SNS....
4. Nella finestra di dialogo, dal menu a discesa, scegli un argomento Amazon SNS, quindi scegli Sottoscrivi.

Utilizzo delle risorse

Oltre ad accedere ai servizi AWS elencati per impostazione predefinita in AWS Explorer, puoi passare a Resources (Risorse) e scegliere tra centinaia di risorse da aggiungere all'interfaccia. In AWS, una risorsa è un'entità che può essere utilizzata. Alcune delle risorse aggiunte includono distribuzioni Amazon CloudFront, Amazon AppFlow, Flusso di dati Amazon Kinesis, ruoli AWS IAM e Amazon VPC.

Dopo aver effettuato la selezione, puoi andare a Risorse ed espandere il tipo di risorsa per elencare le risorse disponibili per quel tipo. Ad esempio, se selezioni il tipo di risorsa AWS::Lambda::Function, potrai accedere alle risorse che definiscono funzioni diverse, le loro proprietà e i relativi attributi.

Dopo aver aggiunto un tipo di risorsa a Resources (Risorse), potrai interagire con quel tipo e le relative risorse nei seguenti modi:

- Potrai visualizzare un elenco di risorse esistenti disponibili nella regione AWS corrente per questo tipo di risorsa.
- Potrai visualizzare una versione di sola lettura del file JSON che descrive una risorsa.
- Potrai copiare l'identificatore della risorsa per la risorsa.
- Potrai visualizzare la documentazione AWS che spiega lo scopo del tipo di risorsa e lo schema (nei formati JSON e YAML) per la modellazione di una risorsa.
- Crea una nuova risorsa modificando e salvando un modello in formato JSON conforme a uno schema.*
- Aggiorna o elimina una risorsa esistente.*

Important

*Nella versione attuale del AWS Toolkit for JetBrains, l'opzione per creare, modificare ed eliminare le risorse è una funzionalità sperimentale. Dato che le funzionalità sperimentali vengono continuamente testate e aggiornate, potrebbero presentare problemi di usabilità. Inoltre, le funzionalità sperimentali potrebbero essere rimosse dal AWS Toolkit for JetBrains senza preavviso.

Per consentire l'uso di funzionalità sperimentali per le risorse, apri il riquadro Settings nell'IDE JetBrains, espandi Tools, quindi scegli AWS, Experimental Features. Seleziona Modifica risorse JSON per ottenere l'autorizzazione a creare, aggiornare ed eliminare risorse.

Per ulteriori informazioni, consulta [Utilizzo delle funzionalità sperimentali](#).

Autorizzazioni IAM per l'accesso alle risorse

Per accedere alle risorse associate ai servizi AWS, hai bisogno di autorizzazioni AWS Identity and Access Management specifiche. Ad esempio, un'entità IAM, come un utente o un ruolo, per accedere alle risorse AWS::Lambda::Function richiede le autorizzazioni Lambda.

Oltre alle autorizzazioni per le risorse di servizio, un'entità IAM richiede autorizzazioni per consentire al AWS Toolkit for JetBrains di chiamare le operazioni API di AWS Control Cloud per suo conto. Le operazioni API di Cloud Control consentono all'utente o al ruolo IAM di accedere e aggiornare le risorse remote.

Il modo più semplice per concedere le autorizzazioni è quello di allegare la policy gestita AWS, PowerUserAccess, all'entità IAM che chiama queste operazioni API tramite l'interfaccia Toolkit. Questa [policy gestita](#) concede una serie di autorizzazioni per l'esecuzione di attività di sviluppo applicazioni, inclusa la chiamata delle operazioni API.

Per autorizzazioni specifiche che definiscono le operazioni API consentite su risorse remote, consulta la [Guida per l'utente dell'API AWS Cloud Control](#).

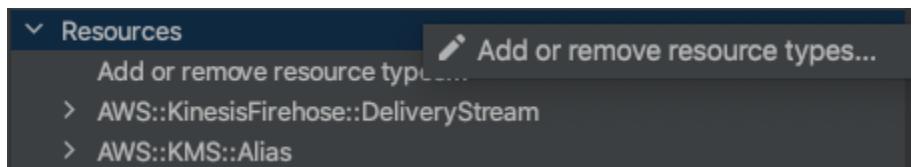
Aggiunta di risorse e interazione con le risorse esistenti

- Nell'Esploratore AWS, fai clic con il pulsante destro del mouse su Risorse e scegli Aggiungi o rimuovi risorse.

Risorse aggiuntive per l'Esploratore nel riquadro Impostazioni mostra un elenco di tipi di risorse disponibili per la selezione.

Note

È inoltre possibile visualizzare l'elenco dei tipi di risorse facendo doppio clic sul nodo Aggiungi o rimuovi risorse, che si trova sotto Risorse.



- In Risorse aggiuntive per l'Esploratore, seleziona i tipi di risorse da aggiungere all' Esploratore AWS e premi Invio oppure scegli OK per confermare.

I tipi di risorse selezionati sono elencati sotto Risorse.

i Note

Se hai già aggiunto un tipo di risorsa all'Esploratore AWS e hai deselezionato la relativa casella di controllo, tale tipo non è più elencato sotto Risorse dopo aver scelto OK. Solo i tipi di risorse attualmente selezionati sono visibili nell'Esploratore AWS.

3. Per visualizzare le risorse già esistenti per un tipo di risorsa, espandi la voce per quel tipo.

Un elenco di risorse disponibili viene visualizzato sotto il tipo di risorse.

4. Per interagire con una risorsa specifica, fai clic con il pulsante destro del mouse sul suo nome e quindi seleziona una delle opzioni seguenti:

- Visualizza risorsa: visualizza una versione di sola lettura del modello formattato in JSON che descrive la risorsa.

Dopo aver visualizzato il modello, puoi modificarlo scegliendo Modifica se la [??? richiesta](#) è abilitata.

i Note

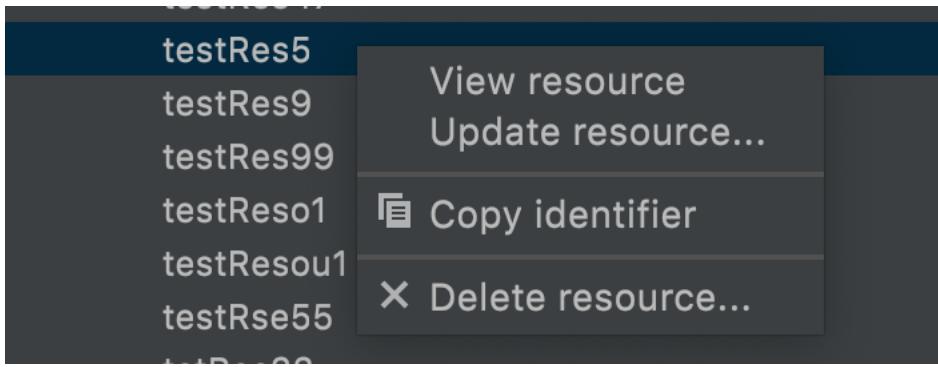
È inoltre possibile visualizzare la risorsa facendo doppio clic su di essa.

- Copia identificatore: copia l'identificatore della risorsa specifica negli appunti. Ad esempio, la risorsa AWS :: DynamoDB :: Table può essere identificata utilizzando la proprietà TableName.
- Aggiorna risorsa: modifica il modello in formato JSON per la risorsa in un editor JetBrains. Per ulteriori informazioni, consulta [Creazione e aggiornamento delle risorse](#).
- Elimina risorse: elimina la risorsa confermando l'eliminazione in una finestra di dialogo visualizzata. L'eliminazione delle risorse è attualmente una [??? in questa versione del AWS Toolkit for JetBrains](#).

⚠ Warning

Se si elimina una risorsa, qualsiasi stack AWS CloudFormation che utilizza tale risorsa non verrà aggiornato. Per correggere questo errore di aggiornamento, è necessario ricreare la risorsa o rimuovere il riferimento ad essa nel modello dello stack

CloudFormation. Per ulteriori informazioni, consulta [questo articolo nel Knowledge Center](#).



Creazione e aggiornamento delle risorse

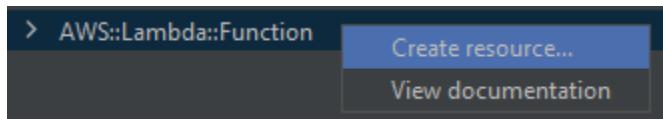
⚠ Important

La creazione e l'aggiornamento delle risorse sono attualmente una funzionalità [???](#) in questa versione del AWS Toolkit for JetBrains.

La creazione di una nuova risorsa comporta l'aggiunta di un tipo di risorsa all'elenco delle Risorse e la successiva modifica di un modello in formato JSON che definisce la risorsa, le sue proprietà e i suoi attributi.

Ad esempio, una risorsa che appartiene al tipo di risorsa AWS::SageMaker::UserProfile è definita con un modello che crea un profilo utente per Amazon SageMaker Studio. Il modello che definisce questa risorsa del profilo utente deve essere conforme allo schema del tipo di risorsa per AWS::SageMaker::UserProfile. Se il modello non è conforme allo schema, ad esempio a causa di proprietà mancanti o errate, la risorsa non può essere creata o aggiornata.

1. Aggiungi il tipo di risorsa per la risorsa che desideri creare facendo clic con il pulsante destro del mouse su Risorse e scegliendo Aggiungi o rimuovi risorse.
2. Dopo aver aggiunto il tipo di risorsa in Risorse, fai clic con il pulsante destro del mouse sul nome e scegli Crea risorsa. È inoltre possibile accedere alle informazioni su come modellare la risorsa scegliendo Visualizza la documentazione.



- Nell'editor, inizia a definire le proprietà che costituiscono il modello di risorsa. La funzionalità di completamento automatico suggerisce nomi di proprietà conformi allo schema del modello. Quando il modello è completamente conforme alla sintassi JSON, il conteggio degli errori viene sostituito da un segno di spunta verde. Per informazioni dettagliate sullo schema, scegli Visualizza la documentazione.

Note

Oltre a essere conforme alla sintassi JSON di base, il modello deve essere conforme allo schema che modella il tipo di risorsa. Quando tenti di creare o aggiornare la risorsa remota, il modello viene convalidato mediante il confronto con il modello di schema.

The screenshot shows a code editor window titled 'Create new AWS::Lambda::Function'. The status bar indicates 'Creating a resource: Enter resource properties, click Create'. The code itself is a JSON object:

```
1  {
2      "Role": "arn:aws:iam::488247187723:role/service-role/HelloWorld-role-p22slq36",
3      "Code": {"Z"},
4      "File": ZipFile      The source code of your Lambda function.
5      "FunctionName": Press Enter to insert. Tab to replace. Next Tip
6      "MemorySize": 128,
7      "Runtime": "nodejs12.x",
8      "Description": "",
9      "TracingConfig": {
10          "Mode": "PassThrough"
11      },
12      "Timeout": 3,
13      "PackageType": "Zip",
14      "Handler": "index.handler",
15      "Arn": "arn:aws:lambda:us-west-2:488247187723:function:HelloWorld14"
16  }
```

The 'File' field is highlighted with a tooltip: 'ZipFile The source code of your Lambda function.'. The status bar at the bottom shows 'Code > Z'.

- Dopo aver finito di dichiarare la risorsa, scegli Crea per convalidare il modello e salvare la risorsa nel cloud AWS remoto. Scegli Aggiorna se stai modificando una risorsa esistente.

Se il modello definisce la risorsa in base al relativo schema, viene visualizzato un messaggio per confermare che la risorsa è stata creata. Se la risorsa esiste già, il messaggio conferma che la risorsa è stata aggiornata.

Dopo la creazione, la risorsa viene aggiunta all'elenco sotto l'intestazione del tipo di risorse.

5. Se il file contiene errori, viene visualizzato un messaggio che spiega che la risorsa non può essere creata o aggiornata. Apri il Log eventi per identificare gli elementi del modello da correggere.

Documentazione di riferimento per l'interfaccia utente per il AWS Toolkit for JetBrains

Per assistenza nell'utilizzo dell'interfaccia utente del AWS Toolkit for JetBrains, consulta i seguenti argomenti.

Argomenti

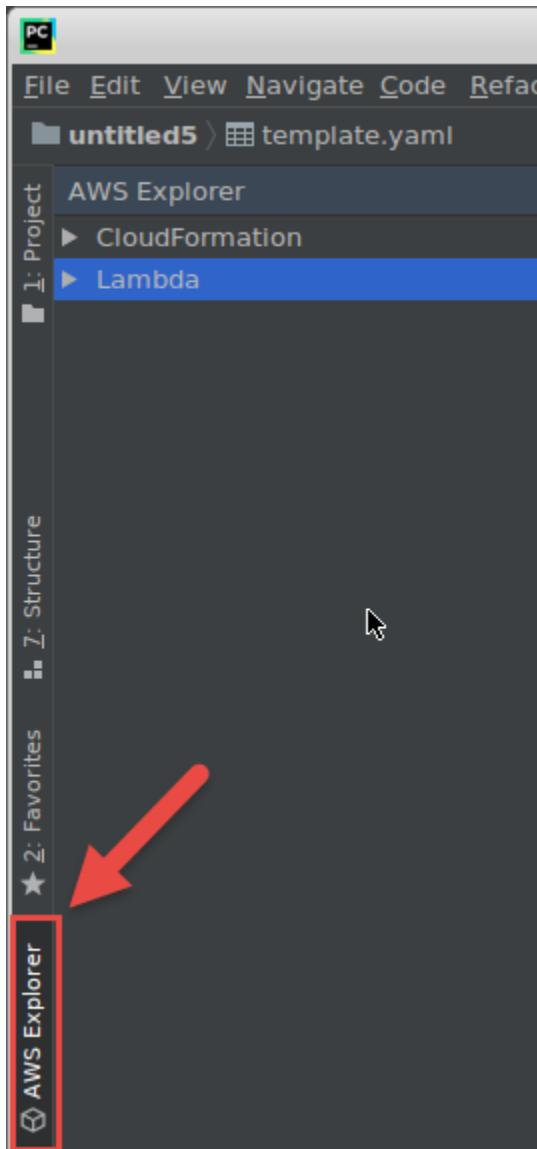
- [AWS Explorer](#)
- [Finestra di dialogo Create Function \(Crea funzione\)](#)
- [Finestra di dialogo Implementa applicazione serverless](#)
- [Finestra di dialogo del nuovo progetto](#)
- [Finestra di dialogo Configurazioni di esecuzione/debug](#)
- [Finestra di dialogo Aggiorna codice](#)
- [Finestra di dialogo Aggiorna configurazione](#)

AWS Explorer

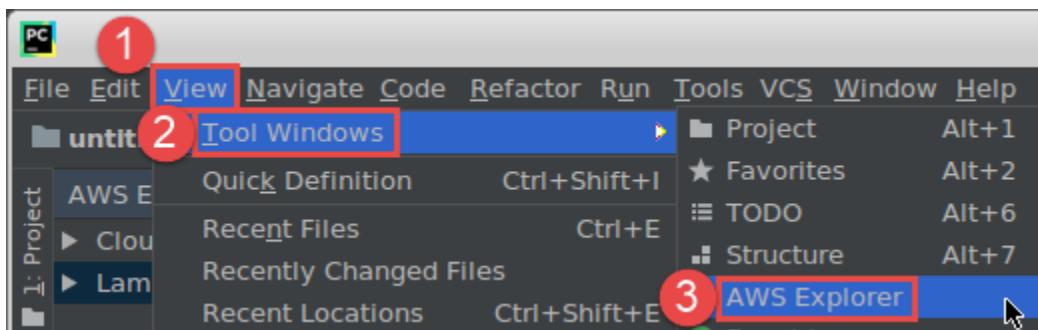
L'Esploratore AWS fornisce un comodo accesso a diverse funzionalità nel AWS Toolkit for JetBrains. Queste includono la gestione delle connessioni dal toolkit agli account AWS, il passaggio di regioni AWS, l'utilizzo di funzioni AWS Lambda e stack AWS CloudFormation negli account e altro ancora.

Per aprire l'Esploratore AWS, con il AWS Toolkit for JetBrains già installato e IntelliJ IDEA, PyCharm, WebStorm o JetBrains Rider in esecuzione, effettua una delle seguenti operazioni:

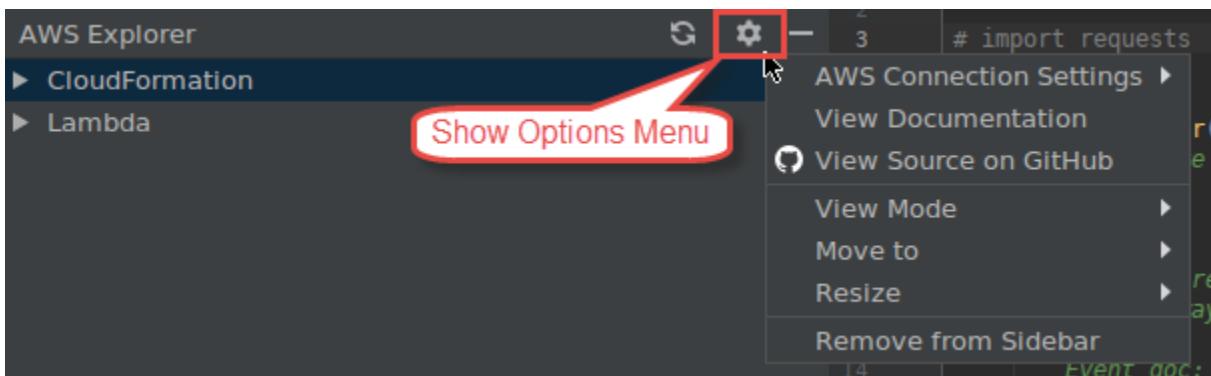
- Nella barra della finestra degli strumenti scegliere AWS Explorer.



- Nel menu principale scegliere View (Visualizza), Tool Windows (Finestre degli strumenti), AWS Explorer.



Nell'Esploratore AWS, scegli l'icona delle impostazioni (Mostra il menu delle opzioni) per le seguenti opzioni:



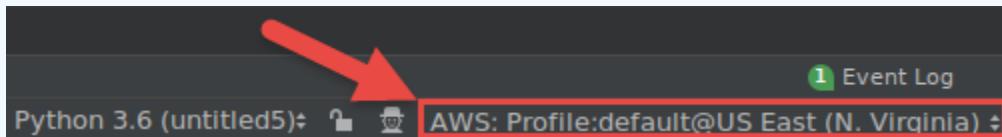
Impostazioni della connessione ad AWS

Contiene le seguenti opzioni:

- Elenco delle regioni AWS: il AWS Toolkit for JetBrains utilizza la regione selezionata. Affinché il kit di strumenti utilizzi una regione diversa, scegli un'altra regione elencata.
- Elenco delle credenziali recenti: elenca le connessioni recenti effettuate dal AWS Toolkit for JetBrains agli account AWS. Il toolkit utilizza la connessione selezionata. Affinché il kit di strumenti utilizzi una connessione recente diversa, scegli il nome della connessione.
- Tutte le credenziali: elenca tutte le connessioni disponibili che puoi stabilire dal AWS Toolkit for JetBrains agli account AWS. Il toolkit utilizza la connessione selezionata. Affinché il kit di strumenti utilizzi una connessione diversa, scegli il nome della rispettiva connessione. Per eseguire altre attività di connessione, scegli Modifica file di credenziali AWS.

Note

L'area Impostazioni di connessione ad AWS nella barra di stato mostra la connessione all'account AWS e la regione che AWS Toolkit for JetBrains sta attualmente utilizzando.



Scegli quest'area per visualizzare le medesime opzioni di Impostazioni di connessione ad AWS come Mostra il menu delle opzioni.

View Documentation (Visualizza documentazione)

Va alla [Guida per l'utente di AWS Toolkit for JetBrains](#) (questa guida).

View Source on GitHub (Visualizza sorgente su GitHub)

Va al repository [aws/aws-toolkit-jetbrains](#) sul sito Web GitHub.

View Mode (Modalità di visualizzazione)

Consente di regolare la finestra dello strumento AWS Explorer in modo che sia possibile accedervi rapidamente e risparmiare spazio quando si lavora nell'editor o in altre finestre degli strumenti.

Per le modalità di visualizzazione di IntelliJ IDEA, consulta la pagina [Tool window view modes](#) sul sito Web di assistenza di IntelliJ IDEA.

Per le modalità di visualizzazione di PyCharm, consulta la pagina [Tool window view modes](#) sul sito Web di assistenza di PyCharm.

Per le modalità di visualizzazione di WebStorm, consulta la pagina [Tool window view modes](#) sul sito Web di assistenza di WebStorm.

Per le modalità di visualizzazione di JetBrains Rider, consulta la pagina [Tool window view modes](#) sul sito Web di assistenza di JetBrains Rider.

Move to (Vai a)

Sposta la finestra degli strumenti Esploratore AWS in una posizione diversa in IntelliJ IDEA, PyCharm, WebStorm o JetBrains Rider.

Ridimensiona

Modifica le dimensioni della finestra dello strumento AWS Explorer.

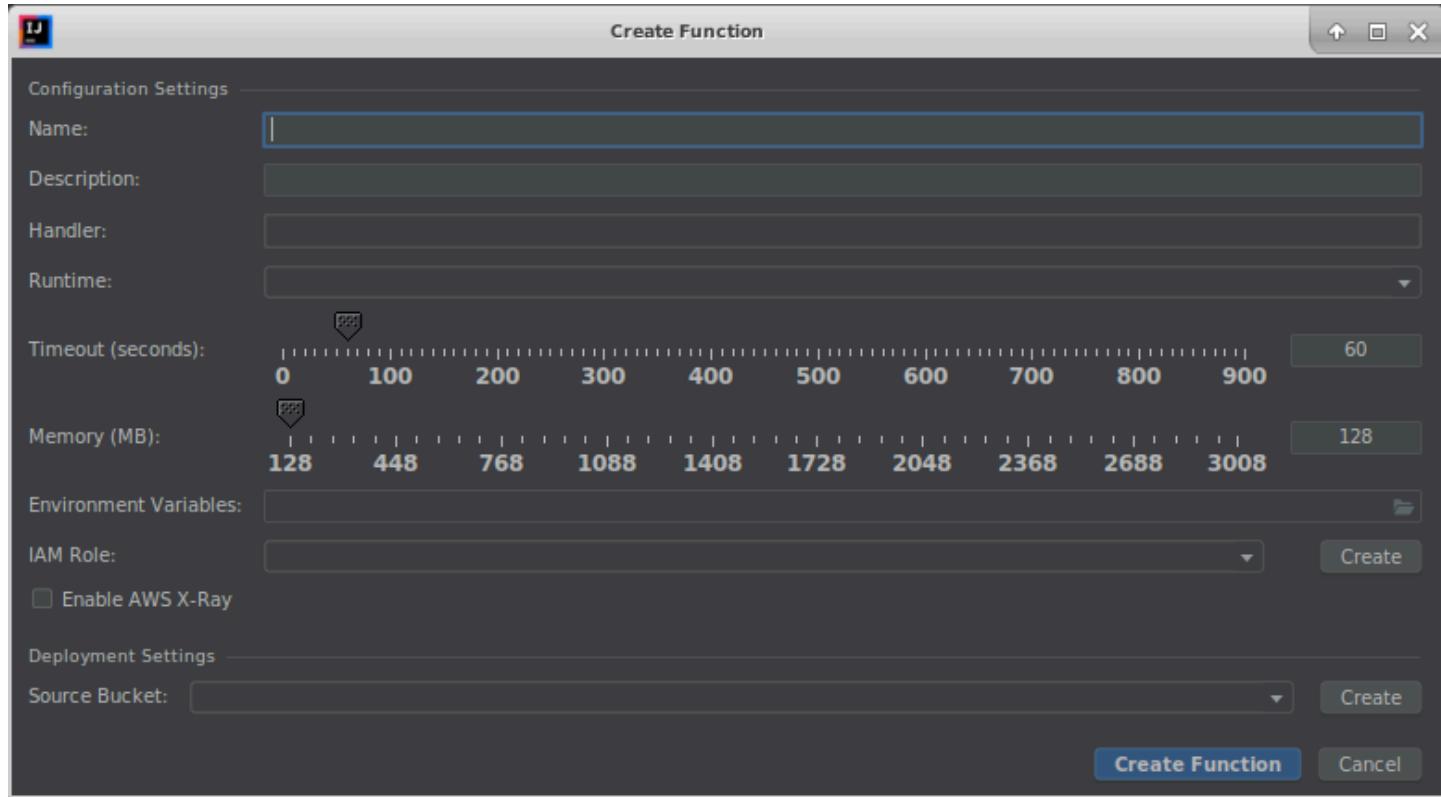
Remove from Sidebar (Rimuovi dalla barra laterale)

Rimuove la finestra degli strumenti Esploratore AWS dalla barra della finestra degli strumenti. Per visualizzarla di nuovo, nella barra dei menu principale, scegli View (Visualizza), Tool Windows (Finestre degli strumenti), AWS Explorer.

È inoltre possibile utilizzare l'Esploratore AWS per lavorare con le funzioni Lambda e gli stack AWS CloudFormation negli account AWS.

Finestra di dialogo Create Function (Crea funzione)

La finestra di dialogo Crea funzione viene visualizzata nel AWS Toolkit for JetBrains quando crei una funzione AWS Lambda standalone.



La finestra di dialogo Crea funzione contiene i seguenti elementi:

Nome

(Obbligatorio) Il nome della funzione. Può contenere solo le lettere maiuscole dalla A alla Z, le lettere minuscole dalla a alla z, i numeri da 0 a 9, trattini (-) e caratteri di sottolineatura (_). Il nome non può contenere più di 64 caratteri.

Descrizione

(Facoltativo) Qualsiasi descrizione significativa della funzione.

Gestore

(Obbligatorio) L'identificatore del gestore di funzioni corrispondente per [Java](#), [Python](#), [Node.js](#) o [C#](#).

Runtime

(Obbligatorio) L'ID del [runtime Lambda](#) da utilizzare.

Timeout (secondi)

(Obbligatorio) La quantità di tempo di esecuzione consentita a una funzione da Lambda prima che venga arrestata. Specifica un valore fino a un massimo di 900 secondi (15 minuti).

Memoria (MB)

(Obbligatorio) La quantità di memoria disponibile per la funzione in fase di esecuzione. Specifica una quantità [compresa tra 128 MB e 3.008 MB](#) in incrementi di 64 MB.

Variabili di ambiente

(Facoltativo) Qualsiasi [variabile di ambiente](#) che la funzione Lambda può utilizzare, specificata come coppia chiave-valore. Per aggiungere, modificare o eliminare le variabili di ambiente, scegli l'icona della cartella e quindi segui le istruzioni visualizzate.

Ruolo IAM

(Obbligatorio) Scegli un [ruolo di esecuzione Lambda](#) disponibile nell'account AWS connesso per consentire a Lambda di utilizzare la funzione. Per creare un ruolo di esecuzione nell'account e consentire a Lambda di utilizzarlo, scegli Crea, quindi segui le istruzioni visualizzate.

Abilitazione di AWS X-Ray

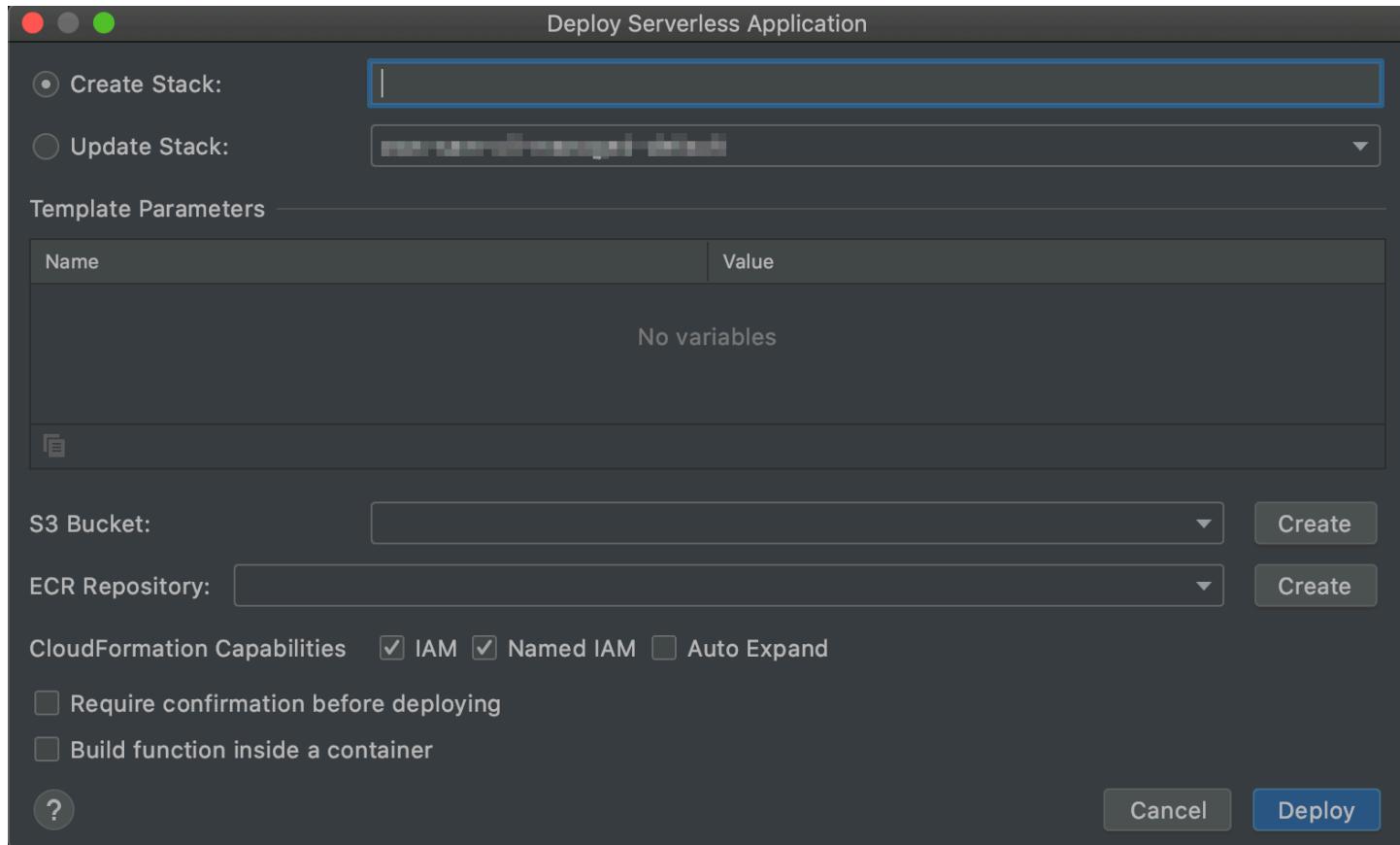
(Facoltativo) Se selezionato, [Lambda abilita AWS X-Ray](#) al rilevamento, all'analisi e all'ottimizzazione dei problemi di prestazioni della funzione. X-Ray raccoglie metadati da Lambda e da qualsiasi servizio a monte o a valle che costituisce l'applicazione. X-Ray utilizza questi metadati per generare un grafico dettagliato dei servizi, che mostra colli di bottiglia nelle prestazioni, picchi di latenza e altri problemi che influiscono sulle prestazioni della funzione.

Bucket di origine

(Obbligatorio) Scegli un bucket Amazon Simple Storage Service (Amazon S3) disponibile nell'account AWS connesso che l'interfaccia della linea di comando AWS Serverless Application Model (AWS SAM) possa utilizzare per implementare la funzione in Lambda. Per creare un bucket Amazon S3 nell'account e fare in modo che la CLI AWS SAM lo usi, scegli Crea e quindi segui le istruzioni visualizzate sullo schermo.

Finestra di dialogo Implementa applicazione serverless

La finestra di dialogo Implementa applicazione serverless nel AWS Toolkit for JetBrains viene visualizzata quando si implementa un'applicazione serverless AWS.



La finestra di dialogo Implementa applicazione serverless contiene i seguenti elementi:

Create Stack (Crea stack)

(Obbligatorio) Fornisci il nome dello stack che l'interfaccia della linea di comando AWS Serverless Application Model (CLI AWS SAM) deve creare in AWS CloudFormation per l'account AWS connesso. L'interfaccia a riga di comando AWS SAM utilizza quindi questo stack per distribuire l'applicazione serverless AWS.

Aggiornamento dello stack

(Obbligatorio) Scegli il nome di uno stack CloudFormation esistente per l'account AWS connesso che la CLI AWS SAM possa utilizzare per implementare l'applicazione serverless AWS.

Note

È necessario specificare uno dei due campi Crea stack o Aggiorna stack.

Parametri del modello

(Facoltativo) Tutti i parametri rilevati dal AWS Toolkit for JetBrains nel file `template.yaml` del progetto corrispondente. Per specificare un valore per un parametro, scegli la casella nella colonna Value (Valore) accanto al parametro, immetti il valore e quindi premi INVIO. Per ulteriori informazioni, consulta [Parametri](#) nella Guida per l'utente AWS CloudFormation.

Bucket S3

(Obbligatorio) Scegli un bucket Amazon Simple Storage Service (Amazon S3) esistente nell'account AWS connesso che la CLI AWS SAM possa utilizzare per implementare l'applicazione serverless AWS. Per creare un bucket Amazon S3 nell'account e fare in modo che la CLI AWS SAM lo utilizzi, scegli Crea e quindi segui le istruzioni visualizzate sullo schermo.

Repository ECR

(Obbligatorio solo per il tipo di pacchetto Image) Scegli l'URI di un repository Amazon Elastic Container Registry (Amazon ECR) esistente nell'account AWS connesso che la CLI AWS SAM possa utilizzare per implementare l'applicazione serverless AWS. Per ulteriori informazioni sulla differenza tra i tipi di pacchetto AWS Lambda, consulta la pagina [Lambda deployment packages](#) della Guida per gli sviluppatori di AWS Lambda.

Richiesta di conferma prima della distribuzione

(Facoltativo) Se selezionato, indica ad CloudFormation di attendere il completamento della creazione o dell'aggiornamento dello stack corrispondente [eseguendo il set di modifiche corrente dello stack in CloudFormation](#). Se non si esegue questo set di modifiche, l'applicazione serverless AWS non passa alla fase di implementazione.

Funzione build all'interno di un container

(Facoltativo) Se selezionato, la CLI AWS SAM crea una qualsiasi delle funzioni dell'applicazione serverless all'interno di un container Docker di tipo Lambda localmente prima dell'implementazione. Questo è utile se la funzione dipende da pacchetti che hanno compilato in modo nativo dipendenze o programmi. Per ulteriori informazioni, consulta [Creazione di applicazioni](#) nella Guida per gli sviluppatori di AWS Serverless Application Model.

Finestra di dialogo del nuovo progetto

La finestra di dialogo Nuovo progetto nel AWS Toolkit for JetBrains viene visualizzata quando crei un'applicazione serverless AWS.

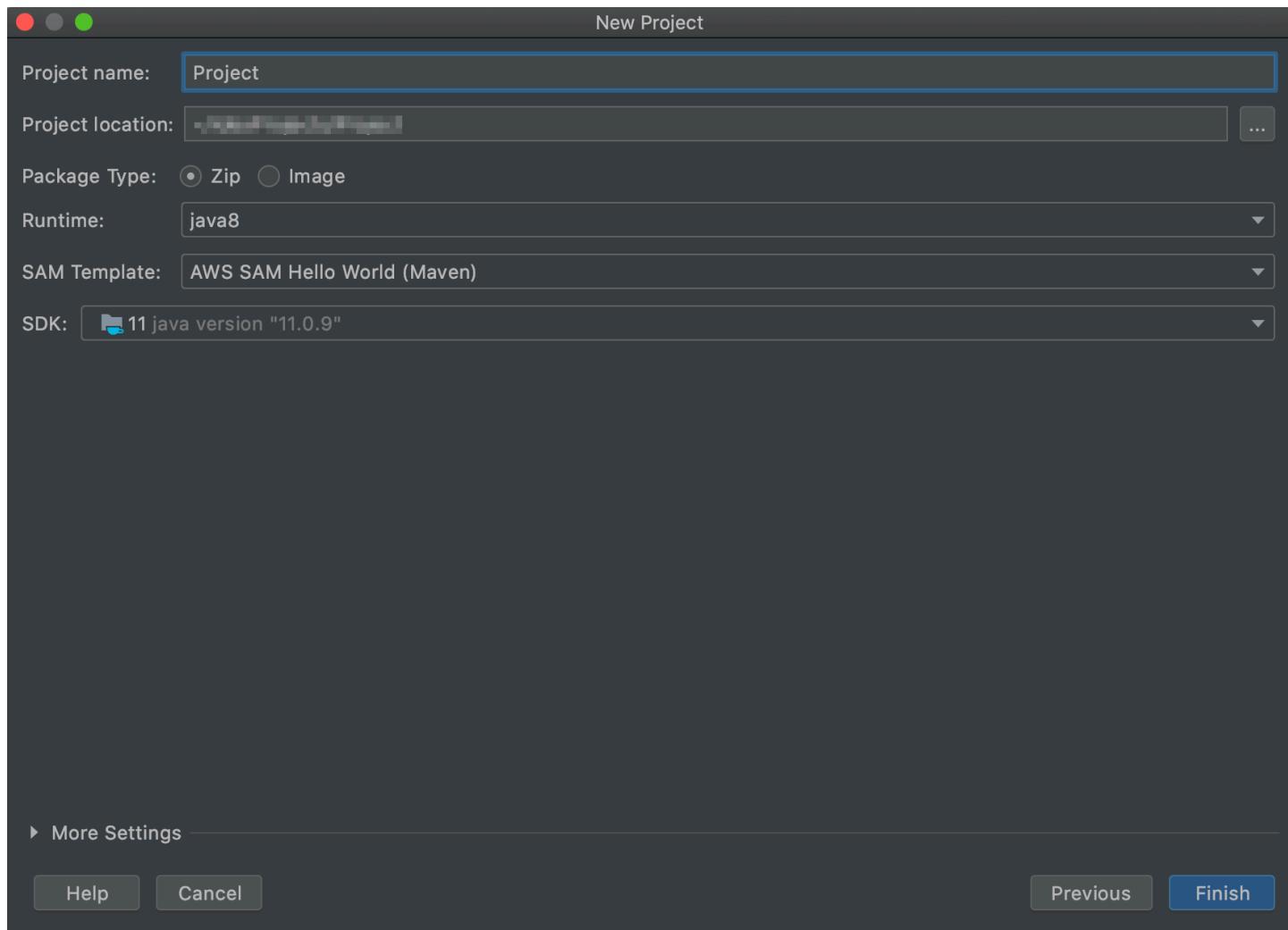
Argomenti

- [Finestra di dialogo Nuovo progetto \(IntelliJ IDEA, PyCharm e WebStorm\)](#)
- [Finestra di dialogo Nuovo progetto \(JetBrains Rider\)](#)

Finestra di dialogo Nuovo progetto (IntelliJ IDEA, PyCharm e WebStorm)

Note

L'immagine seguente mostra la finestra di dialogo Nuovo progetto per IntelliJ IDEA, ma le descrizioni dei campi si applicano anche a PyCharm e WebStorm.



La finestra di dialogo Nuovo progetto contiene i seguenti elementi:

Nome progetto

(Obbligatorio) Il nome del progetto.

Posizione del progetto

(Obbligatorio) La posizione in cui IntelliJ IDEA crea il progetto.

Tipo di pacchetto

(Obbligatorio) Il tipo di pacchetto di implementazione della funzione AWS Lambda, che può essere Zip oppure Image. Per informazioni sulla differenza tra tipi di pacchetto Zip e Image, consulta la pagina [Lambda deployment packages](#) della Guida per gli sviluppatori di AWS Lambda.

Runtime

(Obbligatorio) L'ID del [runtime Lambda](#) da utilizzare.

Modello SAM

(Obbligatorio) Il nome del modello AWS Serverless Application Model (AWS SAM) da utilizzare.

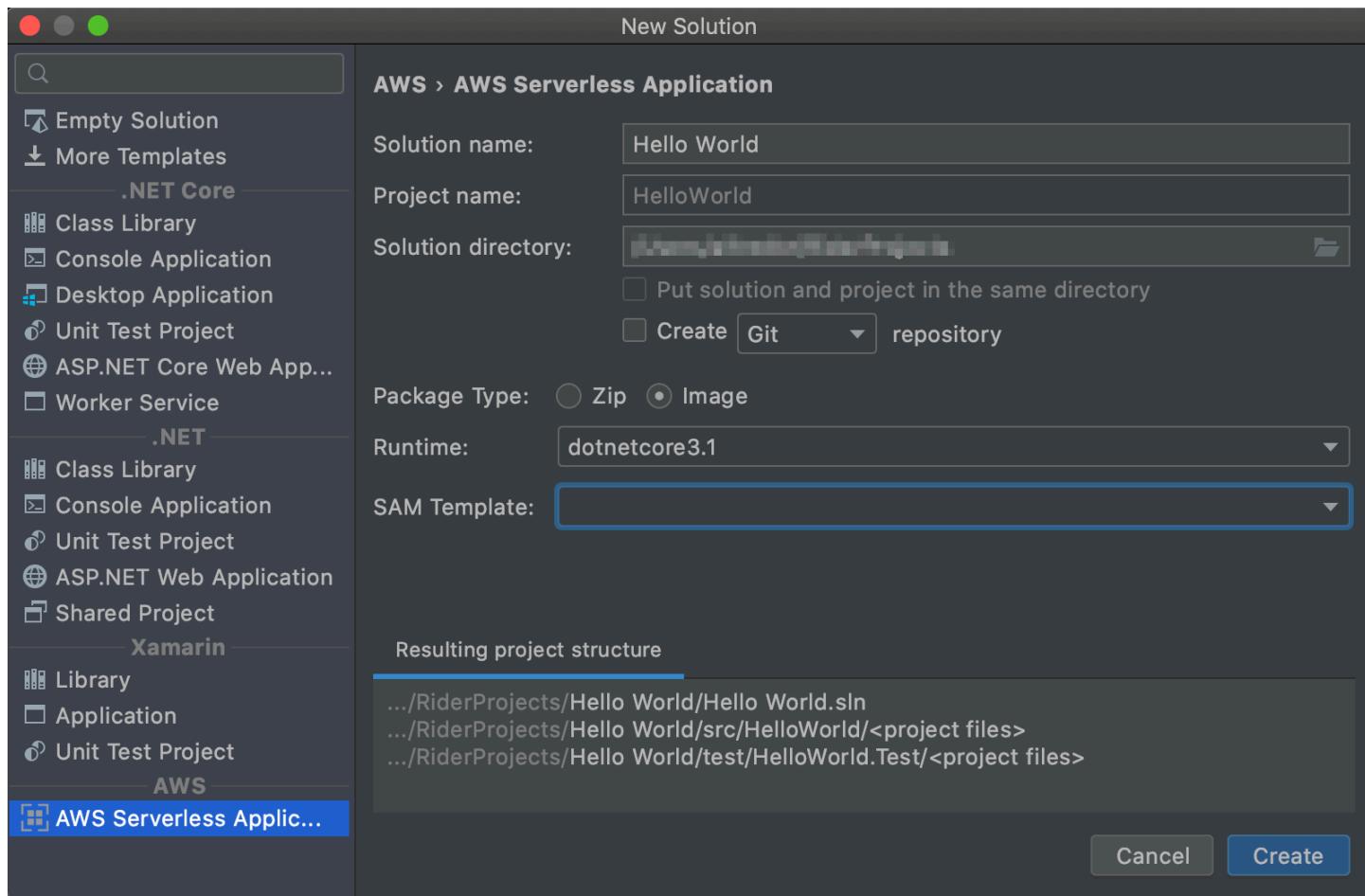
SDK del progetto

(Obbligatorio) Il kit di sviluppo Java (JDK) da utilizzare. Per ulteriori informazioni, consulta la pagina [Java Development Kit \(JDK\)](#) sul sito Web di assistenza di IntelliJ IDEA.

Finestra di dialogo Nuovo progetto (JetBrains Rider)

Note

Quando crei una nuova soluzione, questa finestra di dialogo contiene il titolo Nuova soluzione anziché Nuovo progetto. Tuttavia, il contenuto della finestra di dialogo è lo stesso.



La finestra di dialogo Nuovo progetto contiene i seguenti elementi:

Nome della soluzione

(Obbligatorio) Il nome della soluzione.

Nome progetto

(Obbligatorio) Il nome del progetto.

Directory della soluzione

(Obbligatorio) Il percorso della directory della soluzione.

Inserisci soluzione e progetto nella stessa directory

(Facoltativo) Se selezionato, inserisce i file della soluzione nella stessa posizione dei file del progetto.

Crea repository

(Facoltativo) Se selezionato, crea un repository remoto per il progetto con il provider specificato.

Tipo di pacchetto

(Obbligatorio) Il tipo di pacchetto della funzione Lambda, che può essere Zip oppure Image.

Per informazioni sulla differenza tra tipi di pacchetto Zip e Image, consulta la pagina [Lambda deployment packages](#) della Guida per gli sviluppatori di AWS Lambda.

Runtime

(Obbligatorio) L'ID del runtime Lambda da utilizzare.

Modello SAM

(Obbligatorio) Il nome del modello AWS SAM da utilizzare.

Struttura del progetto risultante

(Non modificabile) I percorsi delle directory e dei file del progetto che verranno creati.

Finestra di dialogo Configurazioni di esecuzione/debug

La finestra di dialogo Configurazioni di esecuzione/debug nel AWS Toolkit for JetBrains viene mostrata ogni volta che desideri modificare le configurazioni di esecuzione/debug, in locale, in remoto o in un cluster Amazon Elastic Container Service (Amazon ECS).

Argomenti

- [Finestra di dialogo Configurazioni di esecuzione/debug \(impostazioni della funzione locale\)](#)
- [Finestra di dialogo Configurazioni di esecuzione/debug \(impostazioni della funzione remota\)](#)
- [Finestra di dialogo Modifica configurazione \(cluster Amazon ECS\)](#)

Finestra di dialogo Configurazioni di esecuzione/debug (impostazioni della funzione locale)

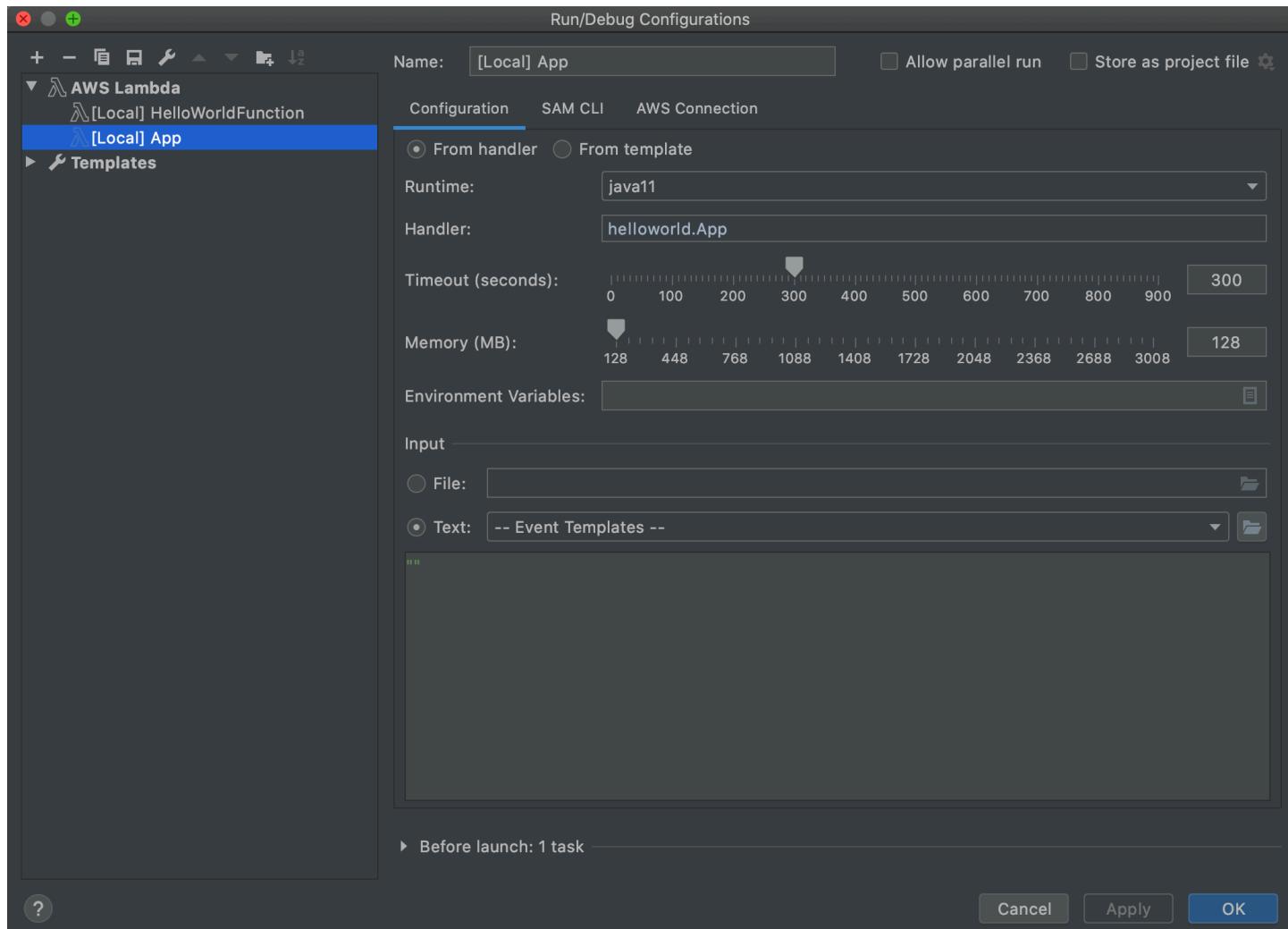
Questa finestra di dialogo viene visualizzata ogni volta che si aggiornano le impostazioni per la versione locale di una funzione AWS Lambda.

Note

Per aggiornare le impostazioni per la versione remota di quella stessa funzione (il codice sorgente della funzione è all'interno del servizio Lambda per l'account AWS), consulta invece

la pagina [Finestra di dialogo Configurazioni di esecuzione/debug \(impostazioni della funzione remota\)](#).

Questa finestra di dialogo contiene tre schede: Configurazione, CLI SAM e Connessione ad AWS.



La scheda Configurazione della finestra di dialogo Configurazioni di esecuzione/debug per le impostazioni delle funzioni locali contiene i seguenti elementi:

Nome

(Obbligatorio) Il nome di questa configurazione.

Consenti esecuzione parallela/Consenti esecuzione in parallelo

(Facoltativo) Se selezionato, consente a IntelliJ IDEA, PyCharm, WebStorm o JetBrains Rider di avviare tutte le istanze della configurazione da eseguire in parallelo necessarie.¹

Dal gestore//Dal modello

(Obbligatorio) A seconda dell'opzione scelta, è necessario configurare impostazioni aggiuntive.

Runtime

(Obbligatorio) L'ID del [runtime Lambda](#) da utilizzare.

Gestore

(Obbligatorio per l'opzione Dal gestore) L'identificatore del gestore di funzioni corrispondente per [Java](#), [Python](#), [Node.js](#) o [C#](#).

Timeout (secondi)

(Obbligatorio per l'opzione Dal gestore) La quantità di tempo di esecuzione consentita a una funzione da Lambda prima che venga arrestata. Specifica un valore fino a un massimo di 900 secondi (15 minuti).

Memoria (MB)

(Obbligatorio per l'opzione Dal gestore) La quantità di memoria disponibile per la funzione in fase di esecuzione. Specifica una quantità [compresa tra 128 MB e 3.008 MB](#) in incrementi di 64 MB.

Variabili di ambiente

(Facoltativo per l'opzione Da gestore) Qualsiasi [variabile di ambiente](#) che la funzione Lambda può utilizzare, specificata come coppia chiave-valore. Per aggiungere, modificare o eliminare le variabili di ambiente, scegli l'icona della cartella e quindi segui le istruzioni visualizzate.

Modello

(Obbligatorio per l'opzione Dal gestore) Il percorso e il nome file del modello AWS Serverless Application Model (AWS SAM) (ad esempio, `template.yaml`) da utilizzare per questa configurazione e la risorsa nel modello da associare a questa configurazione.

File

(Obbligatorio) Il percorso e il nome del file dei dati dell'evento da passare nella funzione in formato JSON. Per esempi di dati degli eventi, consulta le pagine [Invoke the Lambda function](#) della Guida per gli sviluppatori di AWS Lambda e [Generating sample event payloads](#) della Guida per gli sviluppatori di AWS Serverless Application Model.

Text

(Obbligatorio) I dati dell'evento da passare nella funzione in formato JSON. Per esempi di dati degli eventi, consulta le pagine [Invoke the Lambda function](#) della Guida per gli sviluppatori di AWS

Lambda e [Generating sample event payloads](#) della Guida per gli sviluppatori di AWS Serverless Application Model.

 Note

È necessario specificare uno dei due campi File o Testo.

Prima dell'avvio: finestra

(Facoltativo) Elenca tutte le attività che devono essere eseguite prima di avviare questa configurazione.²

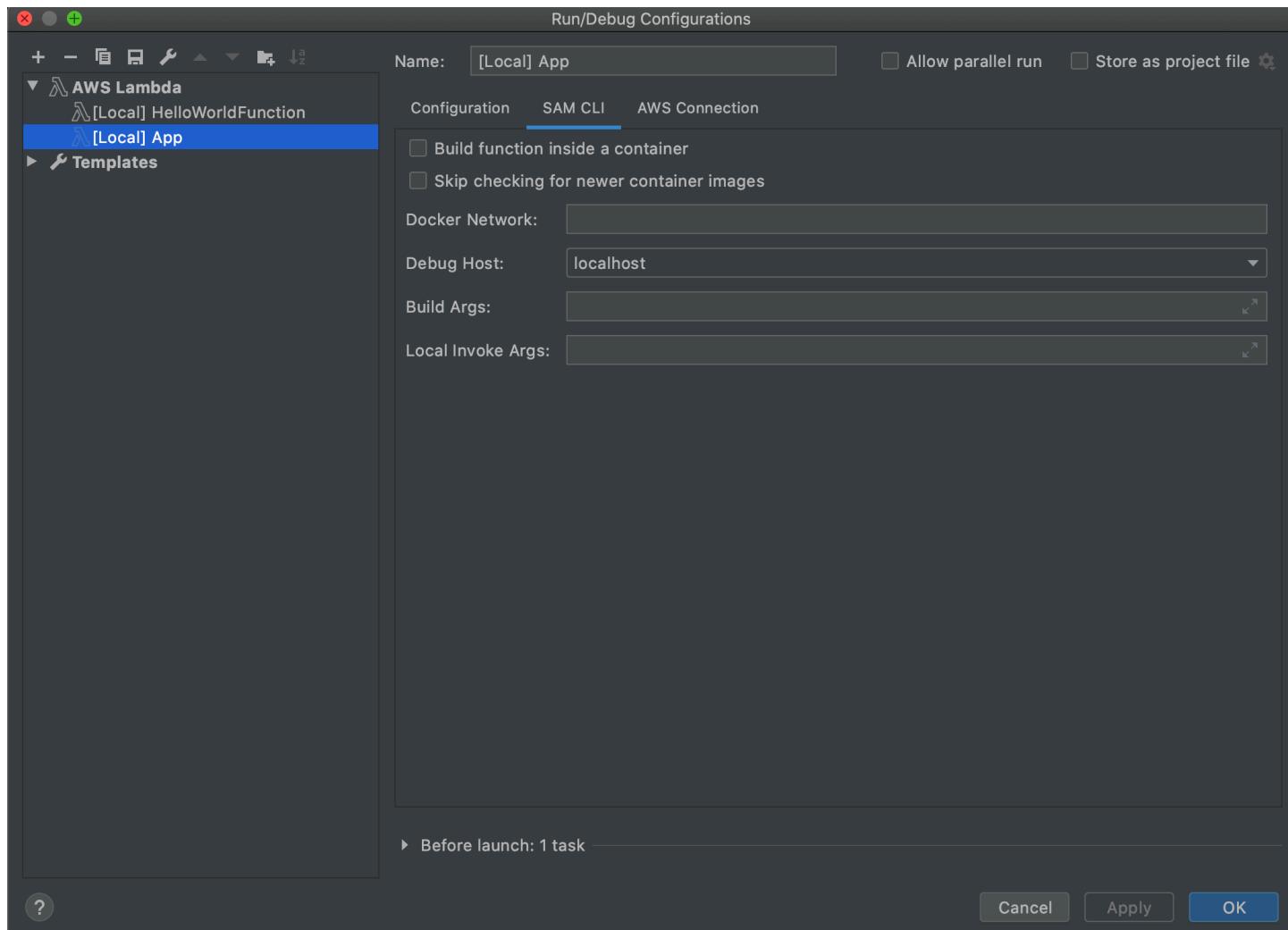
Note

¹ Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per IntelliJ IDEA, consulta la pagina [Common options](#) sul sito Web di assistenza di IntelliJ IDEA.
- Per PyCharm consulta la pagina [Common options](#) sul sito Web di assistenza di PyCharm.
- Per WebStorm, consulta la pagina [Common options](#) sul sito Web di assistenza di WebStorm.
- Per JetBrains Rider, consulta la pagina [Common options](#) sul sito Web di assistenza di JetBrains Rider.

² Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per IntelliJ IDEA, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di IntelliJ IDEA.
- Per PyCharm consulta la pagina [Before Launch options](#) sul sito Web di assistenza di PyCharm.
- Per WebStorm, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di WebStorm.
- Per JetBrains Rider, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di JetBrains Rider.



La scheda CLI SAM della finestra di dialogo Configurazioni di esecuzione/debug per le impostazioni delle funzioni locali contiene i seguenti elementi:

Nome

(Obbligatorio) Il nome di questa configurazione.

Consenti esecuzione parallela/Consenti esecuzione in parallelo

(Facoltativo) Se selezionato, consente a IntelliJ IDEA, PyCharm, WebStorm o JetBrains Rider di avviare tutte le istanze della configurazione da eseguire in parallelo necessarie.¹

Funzione build all'interno di un container

(Facoltativo) Se selezionato, la CLI AWS SAM crea una qualsiasi delle funzioni dell'applicazione serverless all'interno di un container Docker di tipo Lambda localmente prima dell'implementazione. Questo è utile se la funzione dipende da pacchetti che hanno compilato

in modo nativo dipendenze o programmi. Per ulteriori informazioni, consulta [Creazione di applicazioni](#) nella Guida per gli sviluppatori di AWS Serverless Application Model.

Ignora il controllo delle immagini dei container più recenti

(Facoltativo) Se selezionato, la CLI AWS SAM ignora l'inserimento dell'immagine Docker più recente per il [runtime](#) specificato nella scheda Configurazione.

Rete Docker

(Facoltativo) Il nome o l'ID di una rete Docker esistente a cui devono connettersi i container Lambda Docker con la rete bridge predefinita. Se non specificato, i container Lambda si connettono solo alla rete Docker bridge predefinita.

Prima dell'avvio: finestra

(Facoltativo) Elenca tutte le attività che devono essere eseguite prima di avviare questa configurazione.²

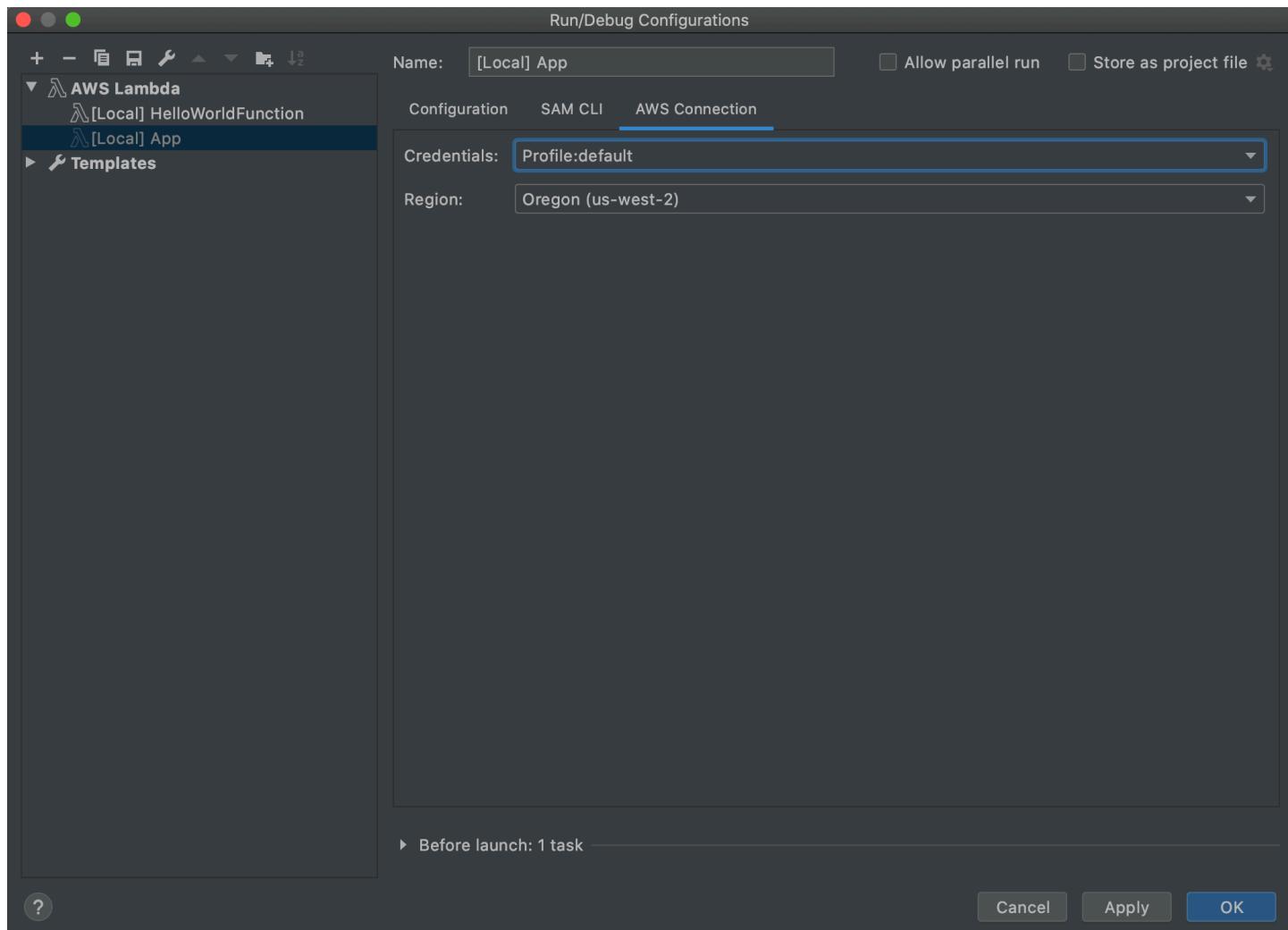
Note

¹ Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per IntelliJ IDEA, consulta la pagina [Common options](#) sul sito Web di assistenza di IntelliJ IDEA.
- Per PyCharm consulta la pagina [Common options](#) sul sito Web di assistenza di PyCharm.
- Per WebStorm, consulta la pagina [Common options](#) sul sito Web di assistenza di WebStorm.
- Per JetBrains Rider, consulta la pagina [Common options](#) sul sito Web di assistenza di JetBrains Rider.

² Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per IntelliJ IDEA, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di IntelliJ IDEA.
- Per PyCharm consulta la pagina [Before Launch options](#) sul sito Web di assistenza di PyCharm.
- Per WebStorm, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di WebStorm.
- Per JetBrains Rider, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di JetBrains Rider.



La scheda Connessione ad AWS della finestra di dialogo Configurazioni di esecuzione/debug per le impostazioni delle funzioni locali contiene i seguenti elementi:

Credenziali

(Obbligatorio) Il nome della connessione all'account AWS esistente da utilizzare.

Regione

(Obbligatorio) Il nome della regione AWS da utilizzare per l'account connesso.

Note

¹ Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per IntelliJ IDEA, consulta la pagina [Common options](#) sul sito Web di assistenza di IntelliJ IDEA.

- Per PyCharm consulta la pagina [Common options](#) sul sito Web di assistenza di PyCharm.
- Per WebStorm, consulta la pagina [Common options](#) sul sito Web di assistenza di WebStorm.
- Per JetBrains Rider, consulta la pagina [Common options](#) sul sito Web di assistenza di JetBrains Rider.

² Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per IntelliJ IDEA, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di IntelliJ IDEA.
- Per PyCharm consulta la pagina [Before Launch options](#) sul sito Web di assistenza di PyCharm.
- Per WebStorm, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di WebStorm.
- Per JetBrains Rider, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di JetBrains Rider.

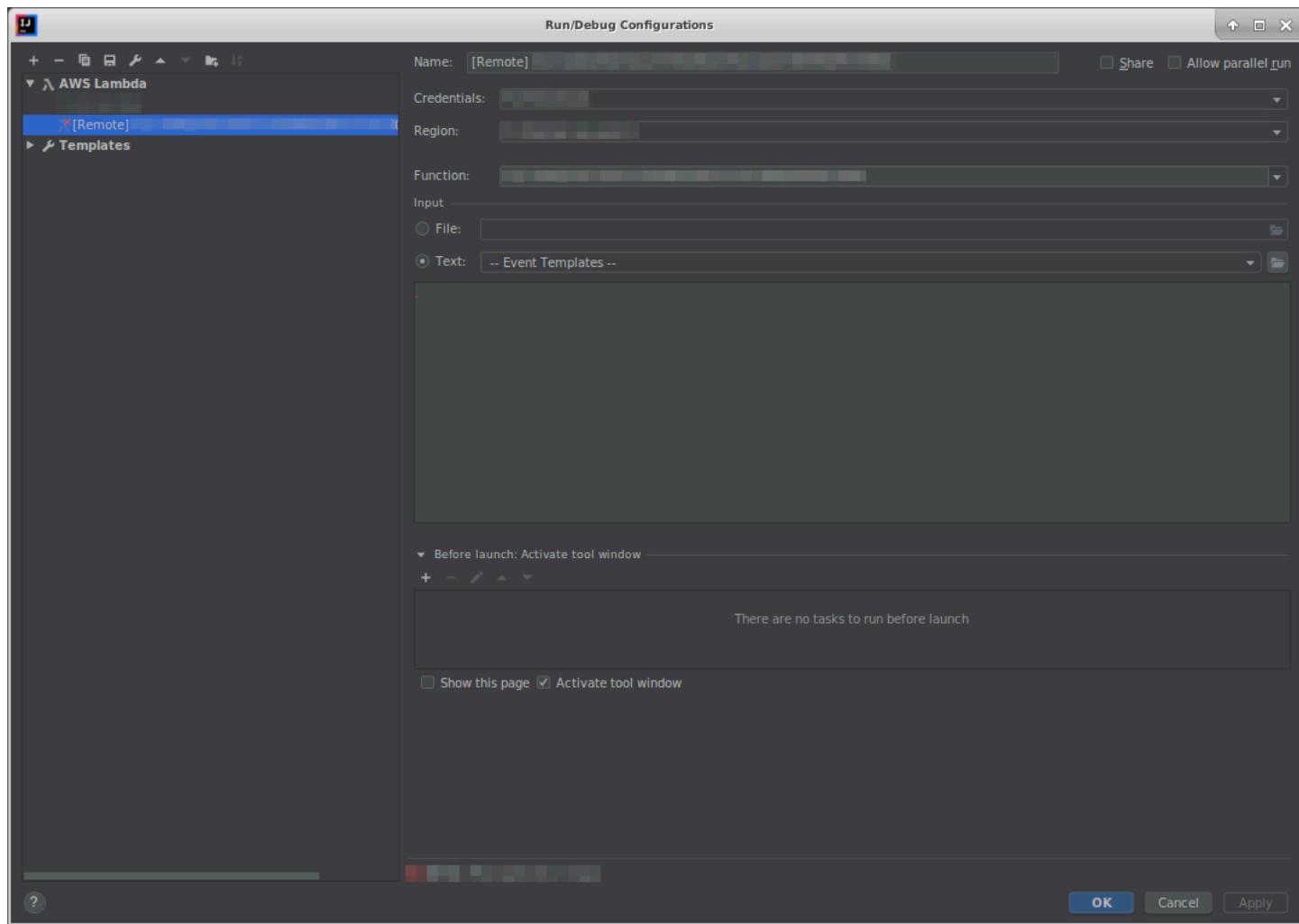
Finestra di dialogo Configurazioni di esecuzione/debug (impostazioni della funzione remota)

Questa finestra di dialogo viene visualizzata ogni volta che modifichi le impostazioni per la versione remota di una funzione AWS Lambda (il codice sorgente della funzione è all'interno di Lambda nell'account AWS).

Note

Per aggiornare le impostazioni per la versione locale della stessa funzione, consulta la pagina [Finestra di dialogo Configurazioni di esecuzione/debug \(impostazioni della funzione locale\)](#).

Sebbene il nome della finestra di dialogo sia Configurazioni di esecuzione/debug, non è possibile utilizzare il AWS Toolkit for JetBrains per sottoporre a debug la versione remota di una funzione Lambda. È possibile eseguire solo la funzione.



La finestra di dialogo Configurazioni di esecuzione/debug per le impostazioni delle funzioni remote contiene i seguenti elementi:

Nome

(Obbligatorio) Il nome di questa configurazione.

Condividi/Condividi tramite VCS

(Facoltativo) Se selezionato, rende questa configurazione disponibile agli altri membri del team.¹

Consenti esecuzione parallela/Consenti esecuzione in parallelo

(Facoltativo) Se selezionato, consente a IntelliJ IDEA, PyCharm, WebStorm o JetBrains Rider di avviare tutte le istanze della configurazione da eseguire in parallelo necessarie.¹

Credenziali

(Obbligatorio) Il nome della connessione all'account AWS esistente da utilizzare.

Regione

(Obbligatorio) Il nome della regione AWS da utilizzare per l'account connesso.

Funzione

(Obbligatorio) Il nome della funzione Lambda da utilizzare.

File

(Obbligatorio) Il percorso e il nome del file dei dati dell'evento da passare nella funzione in formato JSON. Per esempi di dati degli eventi, consulta le pagine [Invoke the Lambda function](#) della Guida per gli sviluppatori di AWS Lambda e [Generating sample event payloads](#) della Guida per gli sviluppatori di AWS Serverless Application Model.

Text

(Obbligatorio) I dati dell'evento da passare nella funzione in formato JSON. Per esempi di dati degli eventi, consulta le pagine [Invoke the Lambda function](#) della Guida per gli sviluppatori di AWS Lambda e [Generating sample event payloads](#) della Guida per gli sviluppatori di AWS Serverless Application Model.

Note

È necessario specificare uno dei due campi File o Testo.

Prima dell'avvio: finestra degli strumenti di attivazione

(Facoltativo) Elenca tutte le attività che devono essere eseguite prima di avviare questa configurazione.²

Mostra questa pagina

(Facoltativo) Se selezionato, visualizza queste impostazioni di configurazione prima di avviare la configurazione.²

Finestra strumenti di attivazione

(Facoltativo) Se selezionato, viene visualizzata la finestra dello strumento Esegui o Debug all'avvio della configurazione.²

Note

¹ Per ulteriori informazioni, consulta gli argomenti seguenti:

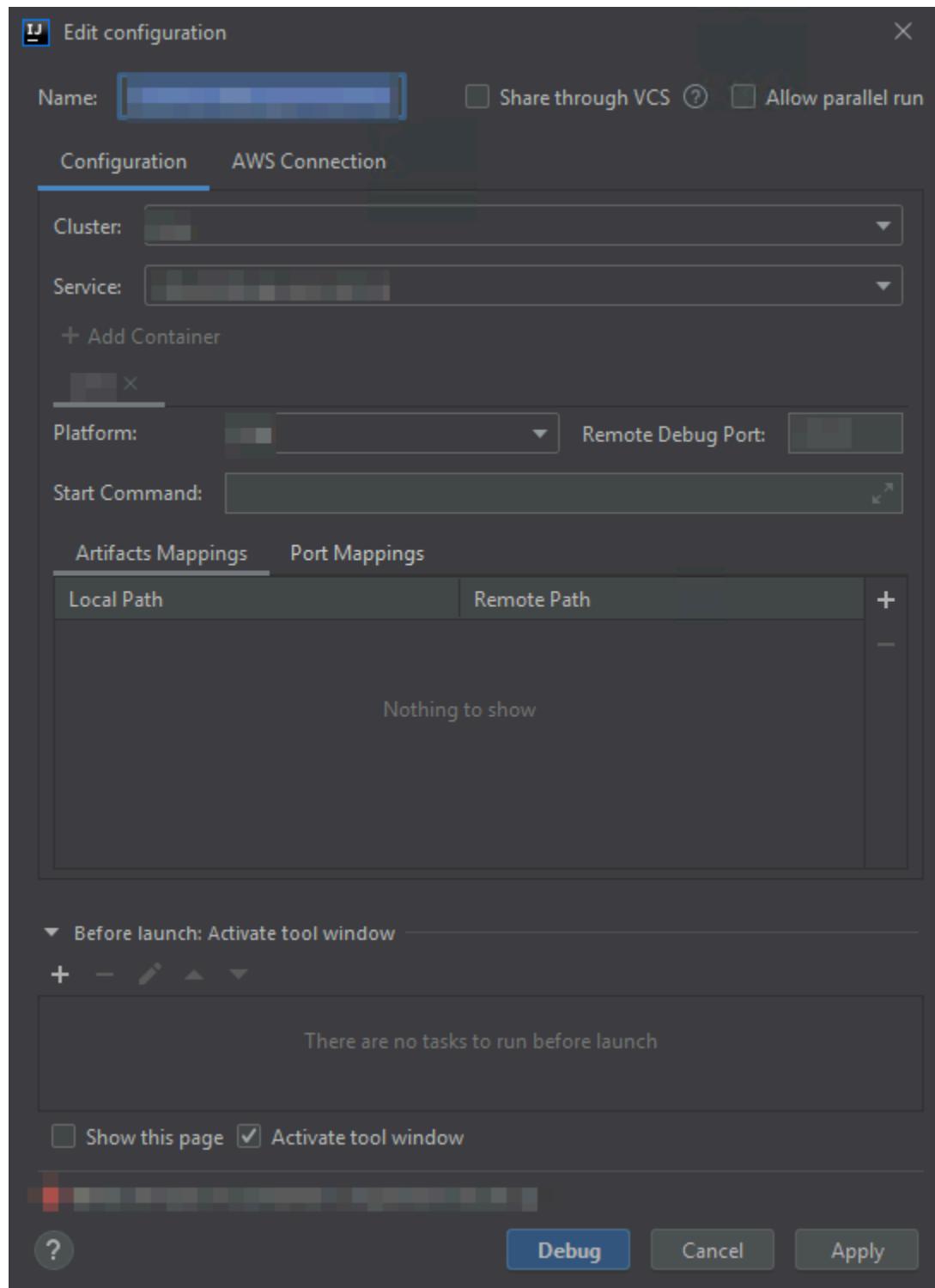
- Per IntelliJ IDEA, consulta la pagina [Common options](#) sul sito Web di assistenza di IntelliJ IDEA.
- Per PyCharm consulta la pagina [Common options](#) sul sito Web di assistenza di PyCharm.
- Per WebStorm, consulta la pagina [Common options](#) sul sito Web di assistenza di WebStorm.
- Per JetBrains Rider, consulta la pagina [Common options](#) sul sito Web di assistenza di JetBrains Rider.

² Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per IntelliJ IDEA, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di IntelliJ IDEA.
- Per PyCharm consulta la pagina [Before Launch options](#) sul sito Web di assistenza di PyCharm.
- Per WebStorm, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di WebStorm.
- Per JetBrains Rider, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di JetBrains Rider.

Finestra di dialogo Modifica configurazione (cluster Amazon ECS)

La finestra di dialogo Modifica configurazione contiene due schede: Configurazione e Connessione ad AWS.



La scheda Configurazione della finestra di dialogo Modifica configurazione contiene i seguenti elementi:

Nome

(Obbligatorio) Il nome di questa configurazione.

Condividi/Condividi tramite VCS

(Facoltativo) Se selezionato, rende questa configurazione disponibile agli altri membri del team.¹

Consenti esecuzione parallela/Consenti esecuzione in parallelo

(Facoltativo) Se selezionato, consente a IntelliJ IDEA, PyCharm, WebStorm o JetBrains Rider di avviare tutte le istanze della configurazione da eseguire in parallelo necessarie.¹

Cluster

(Obbligatorio) Il nome del cluster Amazon Elastic Container Service (Amazon ECS) da sottoporre a debug.

Servizio

(Obbligatorio) Il nome del servizio Amazon ECS nel cluster da sottoporre a debug.

Aggiungi container

Aggiunge un container a questa configurazione. Facoltativo se almeno una scheda è già visibile. Ogni scheda rappresenta un container separato.

I seguenti elementi si applicano al container selezionato: Piattaforma, Porta di debug remota, Comando Avvia, Mappature artefatti e Mappature porte.

Piattaforma

(Obbligatorio) La piattaforma di debug da utilizzare.

Porta di debug remota

(Facoltativo) La porta da collegare allo strumento di debug. In genere, non è necessario specificarla a meno che il servizio non utilizzi le porte 20020-20030. In tal caso, specifica la porta in questo ambito in modo che il container non provi ad associare porte che potrebbero essere in uso altrove.

Comando Avvia

(Obbligatorio) Il comando per avviare il programma in modo che il debugger vi si possa collegare. Per Java, deve iniziare con `java` e non contenere informazioni sul debugger, come `-Xdebug`. Per

Python, deve iniziare con `python`, `python2` o `python3`, seguito dal percorso e dal nome del file da eseguire.

Mappature artefatti

(Obbligatorio) Il percorso locale del computer di sviluppo locale che esegue la mappatura a un percorso remoto nel container. Devi eseguire la mappatura di tutti i codici e gli artefatti che intendi eseguire. Per specificare una mappatura del percorso locale e remoto, scegli Aggiungi (l'icona +).

Mappature porte

(Facoltativo) Una porta locale sul computer di sviluppo locale che esegue la mappatura a una porta remota nel container. Ciò consente alle porte locali di comunicare direttamente con le porte su una risorsa remota. Ad esempio, per il comando `curl localhost:3422`, la porta 3422 è mappata al servizio. Per specificare una mappatura della porta locale e remota, scegli Aggiungi (l'icona +).

Prima dell'avvio: finestra degli strumenti di attivazione

(Facoltativo) Elenca tutte le attività che devono essere eseguite prima di avviare questa configurazione.²

Mostra questa pagina

(Facoltativo) Se selezionato, visualizza queste impostazioni di configurazione prima di avviare la configurazione.²

Finestra strumenti di attivazione

(Facoltativo) Se selezionato, viene visualizzata la finestra dello strumento Esegui o Debug all'avvio della configurazione.²

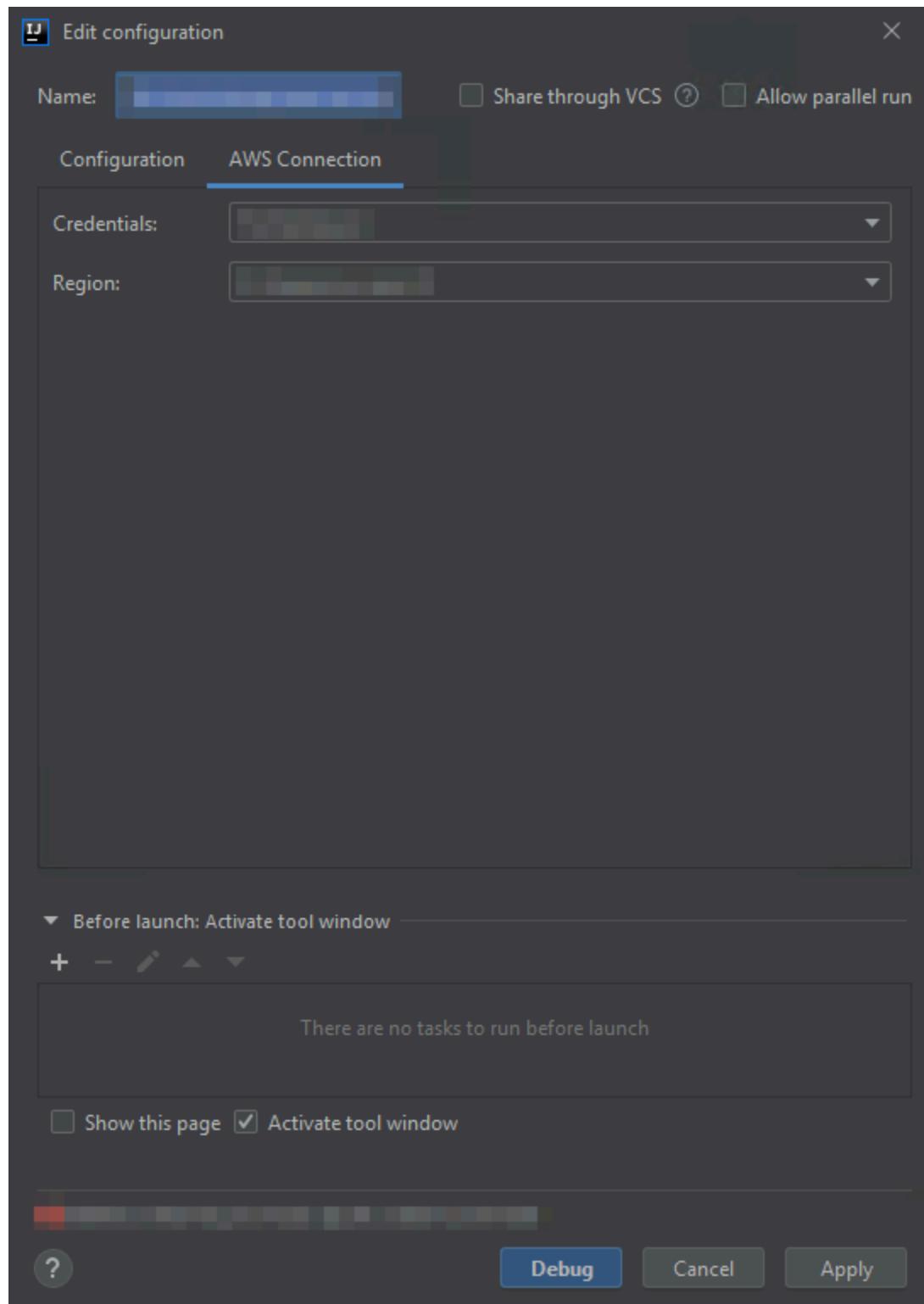
Note

¹ Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per IntelliJ IDEA, consulta la pagina [Common options](#) sul sito Web di assistenza di IntelliJ IDEA.
- Per PyCharm consulta la pagina [Common options](#) sul sito Web di assistenza di PyCharm.
- Per WebStorm, consulta la pagina [Common options](#) sul sito Web di assistenza di WebStorm.
- Per JetBrains Rider, consulta la pagina [Common options](#) sul sito Web di assistenza di JetBrains Rider.

² Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per IntelliJ IDEA, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di IntelliJ IDEA.
- Per PyCharm consulta la pagina [Before Launch options](#) sul sito Web di assistenza di PyCharm.
- Per WebStorm, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di WebStorm.
- Per JetBrains Rider, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di JetBrains Rider.



La scheda Connessione ad AWS della finestra di dialogo Modifica configurazione contiene i seguenti elementi:

Nome

(Obbligatorio) Il nome di questa configurazione.

Credenziali

(Obbligatorio) Il nome della connessione all'account AWS esistente da utilizzare.

Regione

(Obbligatorio) Il nome della regione AWS da utilizzare per l'account connesso.

Condividi/Condividi tramite VCS

(Facoltativo) Se selezionato, rende questa configurazione disponibile agli altri membri del team.¹

Consenti esecuzione parallela/Consenti esecuzione in parallelo

(Facoltativo) Se selezionato, consente a IntelliJ IDEA, PyCharm, WebStorm o JetBrains Rider di avviare tutte le istanze della configurazione da eseguire in parallelo necessarie.¹

Prima dell'avvio: finestra degli strumenti di attivazione

(Facoltativo) Elenca tutte le attività che devono essere eseguite prima di avviare questa configurazione.²

Mostra questa pagina

(Facoltativo) Se selezionato, visualizza queste impostazioni di configurazione prima di avviare la configurazione.²

Finestra strumenti di attivazione

(Facoltativo) Se selezionato, viene visualizzata la finestra dello strumento Esegui o Debug all'avvio della configurazione.²

Note

¹ Per ulteriori informazioni, consulta gli argomenti seguenti:

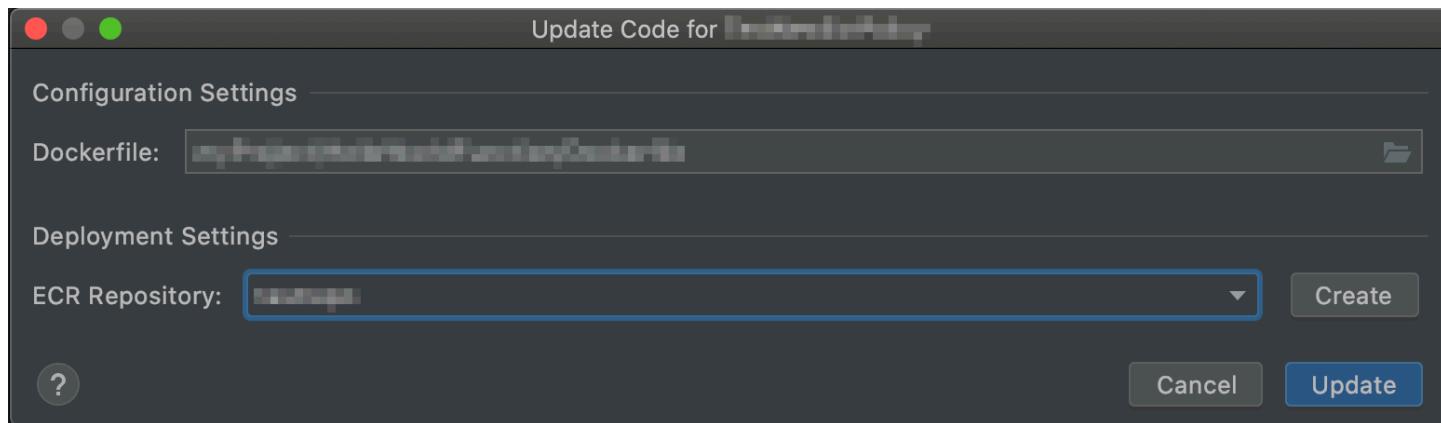
- Per IntelliJ IDEA, consulta la pagina [Common options](#) sul sito Web di assistenza di IntelliJ IDEA.
- Per PyCharm consulta la pagina [Common options](#) sul sito Web di assistenza di PyCharm.
- Per WebStorm, consulta la pagina [Common options](#) sul sito Web di assistenza di WebStorm.
- Per JetBrains Rider, consulta la pagina [Common options](#) sul sito Web di assistenza di JetBrains Rider.

² Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per IntelliJ IDEA, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di IntelliJ IDEA.
- Per PyCharm consulta la pagina [Before Launch options](#) sul sito Web di assistenza di PyCharm.
- Per WebStorm, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di WebStorm.
- Per JetBrains Rider, consulta la pagina [Before Launch options](#) sul sito Web di assistenza di JetBrains Rider.

Finestra di dialogo Aggiorna codice

Ogni volta che si aggiorna una funzione AWS Lambda, nel AWS Toolkit for JetBrains viene visualizzata la finestra di dialogo Aggiorna codice.



La finestra di dialogo Aggiorna codice contiene i seguenti elementi:

Gestore

(Obbligatorio) L'identificatore del gestore di funzioni Lambda corrispondente per [Java](#), [Python](#), [Node.js](#) o [C#](#).

Bucket di origine

(Obbligatorio solo per il tipo di pacchetto Zip) Scegli un bucket Amazon Simple Storage Service (Amazon S3) disponibile nell'account AWS connesso che l'interfaccia della linea di comando AWS Serverless Application Model (AWS SAM) possa utilizzare per implementare la funzione in Lambda. Per creare un bucket Amazon S3 nell'account e fare in modo che la CLI AWS SAM lo utilizzi, scegli Crea e quindi segui le istruzioni visualizzate sullo schermo. Per ulteriori informazioni

sulla differenza tra i tipi di pacchetto Lambda, consulta la pagina [Lambda deployment packages](#) della Guida per gli sviluppatori di AWS Lambda.

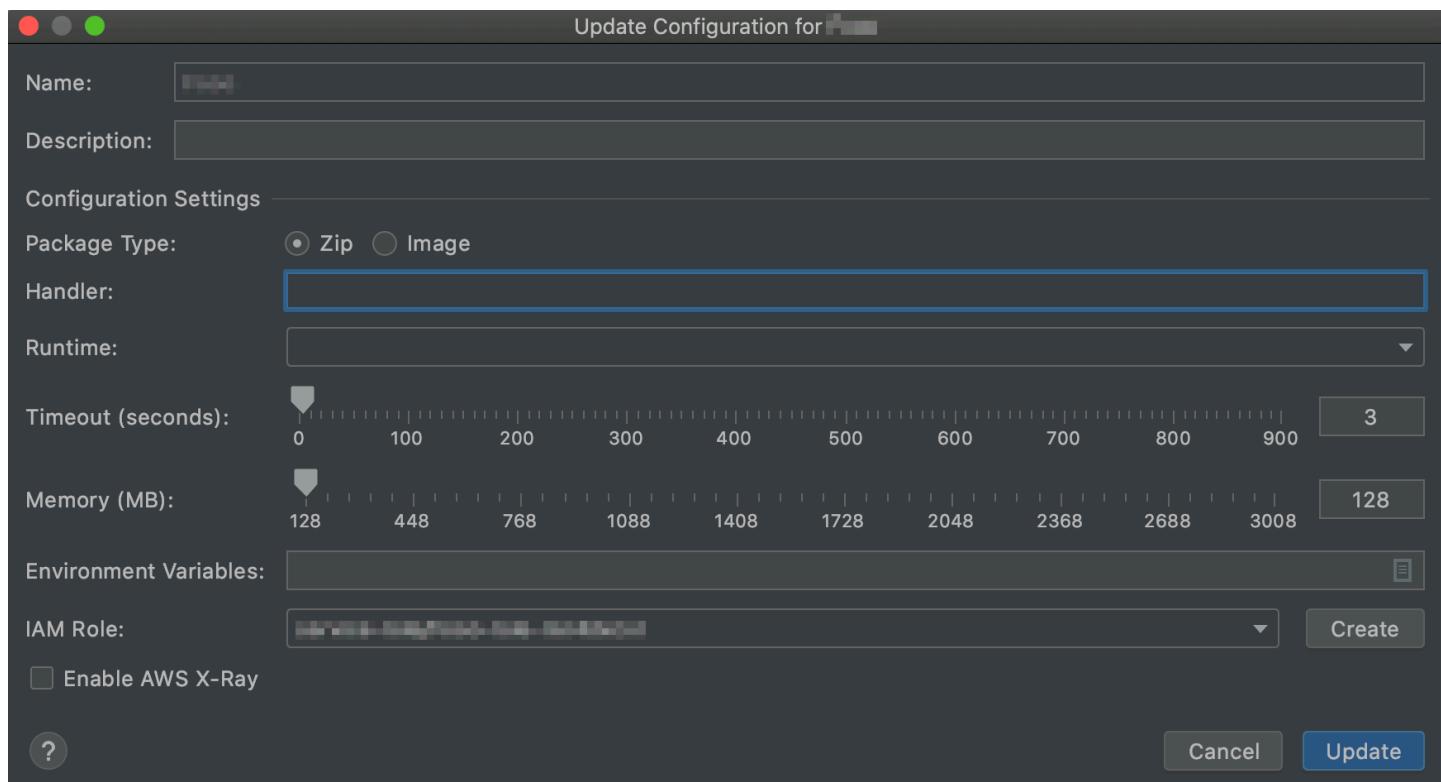
Repository ECR

(Obbligatorio solo per il tipo di pacchetto Image) Scegli un repository Amazon Elastic Container Registry (Amazon ECR) esistente nell'account AWS connesso che la CLI AWS SAM possa utilizzare per implementare la funzione in Lambda.

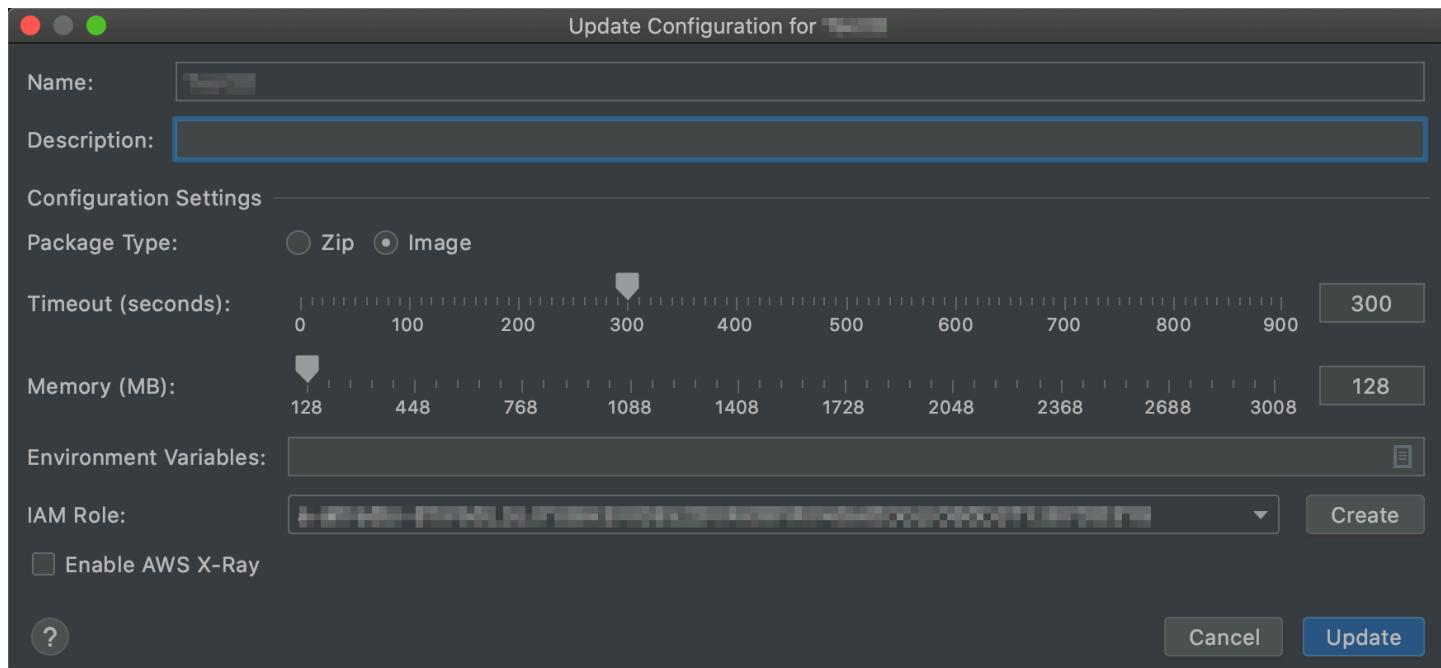
Finestra di dialogo Aggiorna configurazione

Ogni volta che si modifica la configurazione di una funzione AWS Lambda, nel AWS Toolkit for JetBrains viene visualizzata la finestra di dialogo Aggiorna configurazione. Le informazioni fornite differiscono leggermente a seconda che la funzione Lambda del progetto sia del tipo di pacchetto Zip o Image.

La finestra di dialogo Aggiorna configurazione per il tipo di pacchetto Zip:



La finestra di dialogo Aggiorna configurazione per il tipo di pacchetto Image:



La finestra di dialogo Aggiorna configurazione contiene i seguenti elementi:

Nome

(Obbligatorio) Il nome della funzione. Può contenere solo le lettere maiuscole dalla A alla Z, le lettere minuscole dalla a alla z, i numeri da 0 a 9, trattini (-) e caratteri di sottolineatura (_). Il nome non può contenere più di 64 caratteri.

Descrizione

(Facoltativo) Qualsiasi descrizione significativa della funzione.

Tipo di pacchetto

(Obbligatorio) Il tipo di pacchetto della funzione Lambda, che può essere Zip oppure Image.

Gestore

(Obbligatorio soltanto per i pacchetti Zip) L'identificatore del gestore di funzioni Lambda corrispondente per [Java](#), [Python](#), [Node.js](#) o [C#](#).

Runtime

(Obbligatorio solo per i pacchetti Zip) L'ID del [runtime Lambda](#) da utilizzare.

Timeout (secondi)

(Obbligatorio) La quantità di tempo di esecuzione consentita a una funzione da Lambda prima che venga arrestata. Specifica un valore fino a un massimo di 900 secondi (15 minuti).

Memoria (MB)

(Obbligatorio) La quantità di memoria disponibile per la funzione in fase di esecuzione. Specifica una quantità [compresa tra 128 MB e 3.008 MB](#) in incrementi di 64 MB.

Variabili di ambiente

(Facoltativo) Qualsiasi [variabile di ambiente](#) che la funzione Lambda può utilizzare, specificata come coppia chiave-valore. Per aggiungere, modificare o eliminare le variabili di ambiente, scegli l'icona della cartella e quindi segui le istruzioni visualizzate.

Ruolo IAM

(Obbligatorio) Scegli un [ruolo di esecuzione Lambda](#) disponibile nell'account AWS connesso per consentire a Lambda di utilizzare la funzione. Per creare un ruolo di esecuzione nell'account e consentire a Lambda di utilizzarlo, scegli Crea, quindi segui le istruzioni visualizzate.

Abilitazione di AWS X-Ray

(Facoltativo) Se selezionato, [Lambda abilita AWS X-Ray](#) al rilevamento, all'analisi e all'ottimizzazione dei problemi di prestazioni della funzione. X-Ray raccoglie metadati da Lambda e da qualsiasi servizio a monte o a valle che costituisce l'applicazione. X-Ray utilizza questi metadati per generare un grafico dettagliato dei servizi, che mostra colli di bottiglia nelle prestazioni, picchi di latenza e altri problemi che influiscono sulle prestazioni della funzione.

Sicurezza per questo prodotto o servizio AWS

La sicurezza cloud di Amazon Web Services (AWS) è la priorità più alta. In quanto cliente AWS, è possibile trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza. La sicurezza è una responsabilità condivisa tra te e AWS. Il [modello di responsabilità condivisa](#) descrive questo come sicurezza del cloud e sicurezza nel cloud.

Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue tutti i servizi offerti nel cloud AWS e fornisce inoltre i servizi che è possibile utilizzare in modo sicuro. La nostra responsabilità in termini di sicurezza in AWS è la massima priorità e l'efficacia dei nostri processi viene testata regolarmente e verificata da auditor di terze parti, in base ai [programmi di conformità AWS](#).

Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi e da altri fattori, tra cui il livello di riservatezza dei tuoi dati, i requisiti della tua organizzazione, le leggi e le normative applicabili.

Questo prodotto o servizio AWS segue il [modello di responsabilità condivisa](#) attraverso gli specifici servizi Amazon Web Services (AWS) supportati. Per informazioni sulla sicurezza del servizio AWS, consulta la [pagina relativa alla documentazione della sicurezza dei servizi AWS](#) e i [Servizi AWS coperti dal programma di compliance che rientrano nell'ambito delle attività di conformità AWS in base al programma di compliance](#).

Argomenti

- [Protezione dei dati nel Kit di strumenti AWS per JetBrains](#)
- [Identity and Access Management](#)
- [Convalida della conformità per questo prodotto o servizio AWS](#)
- [Resilienza per questo prodotto o servizio AWS](#)
- [Sicurezza dell'infrastruttura per questo prodotto o servizio AWS](#)

Protezione dei dati nel Kit di strumenti AWS per JetBrains

Il [modello di responsabilità condivisa](#) di AWS si applica alla protezione dei dati nel Kit di strumenti AWS per JetBrains. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile di mantenere

il controllo sui contenuti ospitati su questa infrastruttura. Questi contenuti comprendono la configurazione della protezione e le 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.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare i singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In questo modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere il suo lavoro. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura la registrazione delle API e delle attività degli utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza di default all'interno dei Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, ad esempio Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se si richiedono moduli crittografici convalidati FIPS 140-2 quando si accede ad AWS tramite una CLI o un'API, utilizzare un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-2](#).

Ti consigliamo vivamente di non inserire mai informazioni identificative sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio un campo Name (Nome). Questo include il lavoro con il Kit di strumenti AWS per JetBrains o altri Servizi AWS utilizzando la console, l'API, la AWS CLI o gli SDK AWS. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i log di fatturazione o 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.

Identity and Access Management

AWS Identity and Access Management (IAM) è un Servizio AWS che consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) a utilizzare risorse AWS. IAM è un Servizio AWS che è possibile utilizzare senza alcun costo aggiuntivo.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso tramite policy](#)
- [Funzionamento dei Servizi AWS con IAM](#)
- [Risoluzione dei problemi di identità e accesso in AWS](#)

Destinatari

Le modalità di utilizzo di AWS Identity and Access Management (IAM) cambiano in base alle operazioni eseguite in AWS.

Utente del servizio: se utilizzi i Servizi AWS per eseguire il tuo lavoro, l'amministratore fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità AWS utilizzate per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. 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, consulta la pagina [Risoluzione dei problemi di identità e accesso in AWS](#) oppure la guida per l'utente del Servizio AWS che stai utilizzando.

Amministratore del servizio: se sei il responsabile delle risorse AWS presso la tua azienda, probabilmente disponi dell'accesso completo a AWS. Il tuo compito è determinare le caratteristiche e le risorse AWS a cui gli utenti del servizio devono accedere. 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, consulta la guida per l'utente del Servizio AWS che stai utilizzando.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a AWS. Per visualizzare esempi di policy basate sull'identità di AWS che puoi utilizzare in IAM, consulta la guida per l'utente del Servizio AWS che stai utilizzando.

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWS utilizzando le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWS come identità federata utilizzando le credenziali fornite tramite un'origine di identità. AWS IAM Identity Center Gli esempi di identità federate comprendono gli utenti del centro identità IAM, l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWS tramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla Console di gestione AWS o al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione [Come accedere al tuo Account AWS](#) nella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia della linea di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consultare [Firma delle richieste AWS](#) nella Guida per l'utente IAM.

Indipendentemente dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'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 AWS](#) nella Guida per l'utente di IAM.

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi 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 [Tasks that require root user credentials](#) (Attività che richiedono le credenziali dell'utente root) nella Guida di riferimento di Gestione dell'account AWS.

Identità federata

Come best practice, richiedere agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory degli utenti aziendali, un provider di identità Web, Directory Service, la directory Identity Center o qualsiasi utente che accede ad Servizi AWS utilizzando le credenziali fornite tramite un'origine di identità. Quando le identità federate accedono ad Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni e gli Account AWS. Per ulteriori informazioni su IAM Identity Center, consulta [Cos'è IAM Identity Center?](#) nella Guida per l'utente di AWS IAM Identity Center.

Utenti e gruppi IAM

Un [utente IAM](#) è una identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche per un singolo utente 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 [Ruota regolarmente le 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, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale 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 di IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità all'interno di Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella Console di gestione AWS mediante lo [scambio di ruoli](#). È possibile assumere un ruolo chiamando un'operazione AWS CLI o API AWS oppure utilizzando un

URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta [Utilizzo di ruoli IAM](#) nella Guida per l'utente di 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 una serie 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 sulle serie di autorizzazioni, consulta [Serie 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 (entità di sicurezza attendibile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso tra account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare 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 [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.
- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità che eseguono in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale 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.
 - Autorizzazioni principale: quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Le policy concedono autorizzazioni a un'entità. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per verificare se un'operazione richiede ulteriori operazioni dipendenti in una policy, consulta [Operazioni, risorse e chiavi di condizione per Servizi AWS](#) nella Guida di riferimento per l'autorizzazione del servizio.
 - Ruolo di servizio: un ruolo di servizio è un [ruolo IAM](#) assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un

ruolo di servizio da IAM. Per ulteriori informazioni, consulta la sezione [Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS](#) nella Guida per l'utente di 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 conto dell'utente. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.
- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLI o dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta [Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2](#) nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta [Quando creare un ruolo IAM \(invece di un utente\)](#) nella Guida per l'utente di IAM.

Gestione dell'accesso tramite policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS.

Una policy è un oggetto in AWS che, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nella policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWS sotto forma di 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 di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare l'accesso ai diversi elementi. Cioè, quale principale può eseguire azioni 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. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, indipendentemente 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 dalla Console di gestione AWS, la AWS CLI o l'API AWS.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWS e le policy gestite dal cliente. 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 di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di trust 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 allegata a una risorsa, una policy definisce le azioni 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 è possibile utilizzare le policy gestite da AWS da IAM in una policy basata su risorse.

Liste di controllo accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta [Panoramica della lista di controllo accessi](#) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta altri tipi di policy 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 funzione 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 di IAM.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata degli Account AWS multipli di proprietà dell'azienda. Se si abilitano tutte le caratteristiche in un'organizzazione, è possibile applicare le policy di controllo dei servizi (SCP) a uno o tutti i propri account. L'SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su Organizations e le policy SCP, consulta [Utilizzo delle SCP](#) nella Guida per l'utente di AWS Organizations.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono passate 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 sull'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 di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle policy](#) nella Guida per l'utente di IAM.

Funzionamento dei Servizi AWS con IAM

Per ottenere un quadro generale del funzionamento dei Servizi AWS con la maggior parte delle funzionalità di IAM, consulta la pagina [AWS services that work with IAM](#) della Guida per l'utente IAM.

Per ulteriori informazioni su come utilizzare uno specifico Servizio AWS con IAM, consulta la sezione sulla sicurezza della guida per l'utente del servizio pertinente.

Risoluzione dei problemi di identità e accesso in AWS

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di AWS e di IAM.

Argomenti

- [Non sono autorizzato a eseguire un'operazione in AWS](#)
- [Non sono autorizzato a eseguire iam:PassRole](#)
- [Voglio consentire alle persone esterne al mio account Account AWS di accedere alle mie risorse AWS](#)

Non sono autorizzato a eseguire un'operazione in AWS

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM mateojackson prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *my-example-widget* fittizia ma non dispone di autorizzazioni awes:*GetWidget* fittizie.

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

In questo caso, la policy per l'utente mateojackson deve essere aggiornata per consentire l'accesso alla risorsa *my-example-widget* utilizzando l'azione awes:*GetWidget*.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è colui che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam:PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a AWS.

Alcuni Servizi AWS consentono di passare un ruolo esistente a tale servizio, invece di creare un nuovo ruolo di servizio o un ruolo collegato ai servizi. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per passare il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS. Tuttavia, l'operazione 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`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è colui che ti ha fornito le credenziali di accesso.

Voglio consentire alle persone esterne al mio account Account AWS di accedere alle mie 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 servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se AWS supporta queste funzionalità, consulta [Funzionamento dei Servizi AWS con IAM](#).

- Per informazioni su come garantire l'accesso alle risorse negli Account AWS che possiedi, consulta [Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso](#) nella Guida per l'utente di IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta [Fornire l'accesso agli Account AWS di proprietà di terze parti](#) nella Guida per l'utente di 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 di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.

Convalida della conformità per questo prodotto o servizio AWS

Per sapere se il Servizio AWS è coperto da programmi di conformità specifici, consulta i [Servizi AWS coperti dal programma di conformità](#) e scegli il programma di conformità desiderato. Per informazioni generali, consulta [Programmi per la conformità di AWS](#).

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Download di report in AWS Artifact](#).

La responsabilità di conformità durante l'utilizzo dei Servizi AWS è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. Per semplificare il rispetto della conformità, AWS mette a disposizione le seguenti risorse:

- [Guide Quick Start per la sicurezza e conformità](#): queste guide all'implementazione illustrano considerazioni relative all'architettura e forniscono la procedura per l'implementazione di ambienti di base su AWS incentrati sulla sicurezza e sulla conformità.
- [Architetture per la sicurezza e la conformità HIPAA su Amazon Web Services](#): questo whitepaper descrive come le aziende possono utilizzare AWS per creare applicazioni conformi alla normativa HIPAA.

Note

Non tutti i Servizi AWS sono conformi ai requisiti HIPAA. Per ulteriori informazioni, consulta la sezione [Riferimenti sui servizi conformi ai requisiti HIPAA](#).

- [Risorse per la conformità AWS](#): una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- [Valutazione delle risorse con le regole](#) nella Guida per lo sviluppatore di AWS Config: il servizio AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- [AWS Security Hub CSPM](#): questo Servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS. La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina [Documentazione di riferimento sui controlli della Centrale di sicurezza](#).
- [AWS Audit Manager](#): questo Servizio AWS aiuta a verificare continuamente l'utilizzo di AWS per semplificare la gestione dei rischi e della conformità alle normative e agli standard di settore.

Questo prodotto o servizio AWS segue il [modello di responsabilità condivisa](#) attraverso gli specifici servizi Amazon Web Services (AWS) supportati. Per informazioni sulla sicurezza del servizio AWS, consulta la [pagina relativa alla documentazione della sicurezza dei servizi AWS](#) e i [Servizi AWS coperti dal programma di compliance che rientrano nell'ambito delle attività di conformità AWS in base al programma di compliance](#).

Resilienza per questo prodotto o servizio AWS

L'infrastruttura globale di AWS è basata su Regioni AWS e zone di disponibilità.

Le regioni Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato.

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 a data center singolo o multiplo.

Per ulteriori informazioni sulle Regioni AWS e sulle zone di disponibilità, consulta [Infrastruttura globale di AWS](#).

Questo prodotto o servizio AWS segue il [modello di responsabilità condivisa](#) attraverso gli specifici servizi Amazon Web Services (AWS) supportati. Per informazioni sulla sicurezza del servizio AWS, consulta la [pagina relativa alla documentazione della sicurezza dei servizi AWS](#) e i [Servizi AWS coperti dal programma di compliance che rientrano nell'ambito delle attività di conformità AWS in base al programma di compliance](#).

Sicurezza dell'infrastruttura per questo prodotto o servizio AWS

Questo prodotto o servizio AWS utilizza servizi gestiti ed è pertanto protetto dalla sicurezza di rete globale di AWS. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina [Sicurezza del cloud AWS](#). Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina [Protezione dell'infrastruttura](#) nel Pilastro della sicurezza di AWS Well-Architected Framework.

Utilizza le chiamate API pubblicate da AWS per accedere a questo prodotto o servizio AWS tramite la rete. I clienti 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. In alternativa, è possibile utilizzare [AWS Security Token Service](#) (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Questo prodotto o servizio AWS segue il [modello di responsabilità condivisa](#) attraverso gli specifici servizi Amazon Web Services (AWS) supportati. Per informazioni sulla sicurezza del servizio AWS, consulta la [pagina relativa alla documentazione della sicurezza dei servizi AWS](#) e i [Servizi AWS coperti dal programma di compliance che rientrano nell'ambito delle attività di conformità AWS in base al programma di compliance](#).

Cronologia dei documenti per la Guida per l'utente di AWS Toolkit for JetBrains

Nella tabella seguente sono elencati gli aggiornamenti importanti della documentazione della Guida per l'utente di AWS Toolkit for JetBrains.

Per un elenco dettagliato delle modifiche apportate a AWS Toolkit for JetBrains, vedere la directory [.changes](#) nel repository [aws/aws-toolkit-jetbrains](#) sul sito Web GitHub.

Modifica	Descrizione	Data
Creato la Guida per l'utente per Amazon Elastic Container Service Exec	Questa è una panoramica di Amazon ECS Exec.	16 dicembre 2021
Supporto per funzionalità sperimentali	È stato aggiunto il supporto per l'attivazione di funzionalità sperimentali per i servizi AWS.	14 ottobre 2021
Supporto per le risorse AWS	È stato aggiunto il supporto per accedere ai tipi di risorse e alle opzioni di interfaccia per creare, modificare e cancellare risorse.	14 ottobre 2021
Supporto di AWS App Runner ora disponibile	Utilizza AWS Toolkit for JetBrains per lavorare con App Runner e implementare dal codice sorgente o da un'immagine di container direttamente a un'applicazione Web scalabile e sicura nel Cloud AWS.	26 maggio 2021
Supporto delle immagini di container di Lambda con	Ora è possibile utilizzare il Kit di strumenti AWS per lavorare con le immagini di container di	1° dicembre 2020

<u>applicazioni serverless ora disponibile</u>	AWS Lambda con applicazioni serverless.	
<u>Supporto di Logs Insights di CloudWatch ora disponibile</u>	Ora è possibile utilizzare il AWS Toolkit for JetBrains per lavorare con Logs Insights di CloudWatch.	24 novembre 2020
<u>Supporto di Amazon SQS ora disponibile</u>	Ora è possibile utilizzare il AWS Toolkit for JetBrains per lavorare con Amazon Simple Queue Service (Amazon SQS).	24 novembre 2020
<u>Supporto di Amazon RDS e Amazon Redshift ora disponibile</u>	Ora è possibile utilizzare il Kit di strumenti AWS per lavorare con Amazon Relational Database Service (Amazon RDS) e Amazon Redshift.	23 settembre 2020
<u>Supporto per Centro identità IAM ora disponibile</u>	Il supporto per AWS IAM Identity Center è ora disponibile nel Kit di strumenti AWS.	23 settembre 2020

<u>Kit di strumenti AWS ora disponibili per altri quattro IDE JetBrains</u>	Sono ora disponibili i Kit di strumenti AWS come plug-in per quattro IDE JetBrains aggiuntivi: <ul style="list-style-type: none">• <u>Kit di strumenti AWS per CLion</u> (per lo sviluppo in C e C++)• <u>Kit di strumenti AWS per GoLand</u> (per lo sviluppo in Go)• <u>Kit di strumenti AWS per PhpStorm</u> (per lo sviluppo in PHP)• <u>Kit di strumenti AWS per RubyMine</u> (per lo sviluppo in Ruby)	28 maggio 2020
<u>Supporto di File sui log CloudWatch ora disponibile</u>	Ora è possibile utilizzare il Kit di strumenti AWS per lavorare con File di log Amazon CloudWatch.	15 aprile 2020
<u>Supporto di bucket e oggetti Amazon S3 ora disponibile</u>	Ora è possibile utilizzare il Kit di strumenti AWS per lavorare con i bucket e gli oggetti Amazon Simple Storage Service (Amazon S3).	27 marzo 2020
<u>Supporto degli schemi EventBridge ora disponibile</u>	Ora è possibile utilizzare il Kit di strumenti AWS per lavorare con gli schemi di Amazon EventBridge.	2 dicembre 2019

<u>Debug del codice nei cluster</u>	Ora è possibile utilizzare il Kit di strumenti AWS per sottoporre a debug il codice nei cluster Amazon Elastic Container Service (Amazon ECS) in versione beta.	25 novembre 2019
<u>Kit di strumenti AWS per Rider ora disponibile</u>	Il Kit di strumenti AWS per Rider è ora disponibile.	25 novembre 2019
<u>Kit di strumenti AWS per WebStorm ora disponibile</u>	Il Kit di strumenti AWS per WebStorm è ora disponibile.	23 ottobre 2019
<u>Il Kit di strumenti AWS per IntelliJ è ora disponibile a livello generale</u>	Il Kit di strumenti AWS per IntelliJ è ora disponibile a livello generale. La documentazione corrispondente è stata aggiornata di conseguenza.	27 marzo 2019
<u>Versione iniziale</u>	Questa è la versione iniziale della Guida per l'utente di AWS Toolkit for JetBrains. Il Kit di strumenti AWS per PyCharm è ora disponibile a livello generale. Il Kit di strumenti AWS per IntelliJ per IntelliJ è ancora nell'anteprima per sviluppatori.	27 Novembre 2018