Guida per l'utente

AWS Toolkit con Amazon Q

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

AWS Toolkit con Amazon Q: 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 discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

AWS Toolkit con Amazon Q

Questa è la guida per l'utente del AWS Toolkit for Visual Studio with Amazon Q. Se stai cercando il AWS Toolkit for VS Code, consulta la Guida per AWS Toolkit for Visual Studio Code l'utente di.

Cos'è il AWS Toolkit for Visual Studio with Amazon Q

AWS Toolkit for Visual Studio with Amazon Q è un'estensione per l'IDE di Visual Studio che semplifica lo sviluppo, il debug e la distribuzione di applicazioni.NET che utilizzano Amazon Web Services. Il AWS Toolkit con Amazon Q è supportato per le versioni di Visual Studio 2022 e successive. Per informazioni dettagliate su come scaricare e installare il kit, consulta l'argomento Installazione e configurazione di questa Guida per l'utente.

> **Note**
>
> Il Toolkit for Visual Studio è stato rilasciato anche per le versioni di Visual Studio 2008, 2010, 2012, 2013, 2015, 2017 e 2019. Tuttavia, tali versioni non sono più supportate. Per ulteriori informazioni, consulta l'argomento Installazione e configurazione di questa Guida per l'utente.

Il AWS Toolkit con Amazon Q contiene le seguenti funzionalità per migliorare la tua esperienza di sviluppo.

AWS Explorer

La finestra degli strumenti AWS Explorer è accessibile dal menu Visualizza dell'IDE e consente di interagire con AWS i servizi di Visual Studio. Per un elenco dei AWS servizi e delle funzionalità supportati, consulta l'argomento Utilizzo AWS dei servizi in questa Guida per l'utente.

Amazon Q

Chatta con Amazon Q Developer in Visual Studio per porre domande sulla creazione AWS e sull'assistenza per lo sviluppo del software. Amazon Q può spiegare concetti e frammenti di codice, generare codice e test unitari e migliorare il codice tramite il debug o il refactoring.

Per installare e configurare Amazon Q for the Toolkit for Visual Studio, consulta l'argomento Guida introduttiva in questa Guida per l'utente. Per ulteriori informazioni su come lavorare con Amazon Q

Developer, consulta Amazon Q Developer nell' IDEsargomento della Amazon Q Developer User Guide. Per informazioni dettagliate sui piani e sui prezzi di Amazon Q, consulta la guida ai prezzi di Amazon Q.

Informazioni correlate

Per aprire un numero o visualizzare i problemi attualmente aperti, visita https://github.com/aws/aws-toolkit-visual-studio/issues.

Per ulteriori informazioni su Visual Studio, visita https://visualstudio.microsoft.com/vs/.

Amazon Q

Cos'è Amazon Q

A partire dal 30 aprile 2024, Amazon CodeWhisperer fa ora parte di Amazon Q Developer, che include suggerimenti di codice in linea e scansioni di sicurezza.

Per ulteriori informazioni su come lavorare con Amazon Q Developer in AWS Toolkit for Visual Studio, consulta Amazon Q Developer nell' IDEsargomento della Amazon Q Developer User Guide. Per informazioni dettagliate sui piani e sui prezzi di Amazon Q, consulta la guida ai prezzi di Amazon Q.

Scaricamento del Toolkit for Visual Studio

Puoi scaricare, installare e configurare il Toolkit for Visual Studio tramite Visual Studio Marketplace nel tuo IDE. Per istruzioni dettagliate, vedere la sezione Installazione del AWS Toolkit for Visual Studio nell'argomento Guida introduttiva di questa Guida per l'utente.

Download del Toolkit da Visual Studio Marketplace

Scarica i file di installazione di Toolkit for Visual Studio accedendo al sito AWS dei download di Visual Studio nel tuo browser web.

Toolkit IDE aggiuntivi da AWS

Oltre al Toolkit for Visual Studio AWS , offre anche Toolkit IDE per VS Code e. JetBrains

AWS Toolkit for Visual Studio Code link

- Segui questo link per scaricare il file AWS Toolkit for Visual Studio Code dal VS Code Marketplace.
- Per saperne di più AWS Toolkit for Visual Studio Code, consulta la Guida AWS Toolkit for Visual Studio Codeper l'utente.

AWS Toolkit for JetBrains link

- Segui questo link per scaricarlo AWS Toolkit for JetBrains dal JetBrains Marketplace.
- Per ulteriori informazioni AWS Toolkit for JetBrains, consulta la Guida per l'AWS Toolkit for JetBrainsutente.

Guida introduttiva

AWS Toolkit for Visual Studio rende disponibili i AWS servizi e le risorse dall'ambiente di sviluppo integrato (IDE) di Visual Studio.

Per aiutarti a iniziare, i seguenti argomenti descrivono come installare, configurare e configurare AWS Toolkit for Visual Studio.

Argomenti

Installazione e configurazione di AWS Toolkit for Visual Studio

Nei seguenti argomenti viene descritto come scaricare, installare, configurare e disinstallare AWS Toolkit for Visual Studio.

Argomenti

Prerequisiti

Di seguito sono riportati i prerequisiti per la configurazione delle versioni supportate di AWS Toolkit for Visual Studio.

- Visual Studio 19 o versione successiva
- Windows 10 o versione successiva di Windows
- Accesso da amministratore a Windows e Visual Studio
- Credenziali AWS IAM attive

> **Note**
>
> Le versioni non supportate di AWS Toolkit for Visual Studio sono disponibili per Visual Studio 2008, 2010, 2012, 2013, 2015 e 2017. Per scaricare una versione non supportata, vai alla pagina di AWS Toolkit for Visual Studiodestinazione e scegli la versione desiderata dall'elenco dei link per il download.
> Per saperne di più sulle credenziali IAM o per registrare un account, visita il gateway AWS Console.

Installazione del AWS Toolkit for Visual Studio

Per installare AWS Toolkit for Visual Studio, trova la tua versione di Visual Studio seguendo le seguenti procedure e completa i passaggi necessari. I link per il AWS Toolkit for Visual Studio download di tutte le versioni di sono disponibili nella pagina di AWS Toolkit for Visual Studiodestinazione.

> **Note**
>
> Se riscontri problemi durante l'installazione di AWS Toolkit for Visual Studio, consulta l'argomento Risoluzione dei problemi di installazione in questa guida.

Installazione di AWS Toolkit for Visual Studio per Visual Studio 2022

Per installare AWS Toolkit for Visual Studio 2022 da Visual Studio, completa i seguenti passaggi:

1. Dal menu principale, vai su Estensioni e scegli Gestisci estensioni.
2. Dalla casella di ricerca, cerca AWS.
3. Scegli il pulsante Download per la versione pertinente di Visual Studio 2022 e segui le istruzioni di installazione.

   > **Note**
   >
   > Potrebbe essere necessario chiudere e riavviare manualmente Visual Studio per completare il processo di installazione.

4. Una volta completati il download e l'installazione, puoi aprirli AWS Toolkit for Visual Studio scegliendo AWS Explorer dal menu Visualizza.

Installazione di AWS Toolkit for Visual Studio per Visual Studio 2019

Per installare AWS Toolkit for Visual Studio 2019 da Visual Studio, completa i seguenti passaggi:

1. Dal menu principale, vai su Estensioni e scegli Gestisci estensioni.
2. Dalla casella di ricerca, cerca AWS.
3. Scegli il pulsante Download per Visual Studio 2017 e 2019 e segui le istruzioni.

> **Note**
>
> Potrebbe essere necessario chiudere e riavviare manualmente Visual Studio per completare il processo di installazione.

4. Una volta completati il download e l'installazione, puoi aprirli AWS Toolkit for Visual Studio scegliendo AWS Explorer dal menu Visualizza.

Disinstallazione di AWS Toolkit for Visual Studio

Per disinstallarlo AWS Toolkit for Visual Studio, trova la tua versione di Visual Studio seguendo le seguenti procedure e completa i passaggi necessari.

Disinstallazione di AWS Toolkit for Visual Studio per Visual Studio 2022

Per disinstallare AWS Toolkit for Visual Studio 2022 da Visual Studio, completa i seguenti passaggi:

1. Dal menu principale, vai su Estensioni e scegli Gestisci estensioni.
2. Dal menu di navigazione Gestisci estensioni, espandi l'intestazione Installate.
3. Individua l'estensione AWS Toolkit for Visual Studio 2022 e scegli il pulsante Disinstalla.

> **Note**
>
> Se AWS Toolkit for Visual Studio non è visibile nella sezione Installato del menu di navigazione, potrebbe essere necessario riavviare Visual Studio.

4. Segui le istruzioni sullo schermo per completare il processo di disinstallazione.

Disinstallazione di per Visual Studio AWS Toolkit for Visual Studio 2019

Per disinstallare AWS Toolkit for Visual Studio 2019 da Visual Studio, completa i seguenti passaggi:

1. Dal menu principale, vai a Strumenti e scegli Gestisci estensioni.
2. Dal menu di navigazione Gestisci estensioni, espandi l'intestazione Installate.
3. Individua l'estensione AWS Toolkit for Visual Studio 2019 e scegli il pulsante Disinstalla.
4. Segui le istruzioni sullo schermo per completare il processo di disinstallazione.

Disinstallazione di per Visual Studio AWS Toolkit for Visual Studio 2017

Per disinstallare il AWS Toolkit for Visual Studio 2017 in Visual Studio, completa i seguenti passaggi:

1. Dal menu principale, vai a Strumenti e scegli Estensioni e aggiornamenti.
2. Dal menu di navigazione Estensioni e aggiornamenti, espandi l'intestazione Installati.
3. Individua l'estensione AWS Toolkit for Visual Studio 2017 e scegli il pulsante Disinstalla.
4. Segui le istruzioni sullo schermo per completare il processo di disinstallazione.

Disinstallazione di Visual Studio AWS Toolkit for Visual Studio 2013 o 2015

Per disinstallare il AWS Toolkit for Visual Studio 2013 o il 2015, completa i seguenti passaggi:

1. Dal Pannello di controllo di Windows, apri Programmi e funzionalità.

   > **Note**
   >
   > È possibile aprire immediatamente Programmi e funzionalità eseguendoli `appwiz.cpl` dal prompt dei comandi di Windows o dalla finestra di dialogo Esegui di Windows.

2. Dall'elenco dei programmi installati, apri il menu contestuale per (fare clic con il pulsante destro del mouse) AWS Strumenti per Windows.
3. Scegliete Disinstalla e seguite le istruzioni per completare il processo di disinstallazione.

> **Note**
>
> La tua directory Samples non viene eliminata durante il processo di disinstallazione. Questa directory viene conservata nel caso in cui siano stati modificati gli esempi. Questa cartella deve essere rimossa manualmente.

Connessione a AWS

Le seguenti sezioni descrivono come iniziare a usare AWS Toolkit for Visual Studio with Amazon Q. La prima volta che avvii Visual Studio dopo aver installato l'estensione, nella finestra dell'editor viene visualizzato un documento Getting Started. Dalla scheda Guida introduttiva puoi completare le seguenti azioni.

- Abilita o disabilita Amazon Q e il AWS Toolkit.
- Aggiungi e autentica con nuove credenziali.
- Effettua l'autenticazione con le credenziali esistenti.
- Accedi alla documentazione e ai tutorial per iniziare a lavorare con Amazon Q e il AWS Toolkit.

Prerequisiti

Per iniziare a lavorare con Amazon Q e AWS Toolkit, devi autenticarti con AWS le credenziali. Se in precedenza hai configurato un AWS account e l'autenticazione tramite un altro AWS strumento o servizio (come il AWS Command Line Interface), il AWS Toolkit rileva automaticamente le tue credenziali. Se sei nuovo utente AWS o non hai ancora creato un account, puoi registrarne uno dal AWS portale di AWS registrazione. Per informazioni dettagliate sulla configurazione di un nuovo AWS account, consulta l'argomento Panoramica nella Guida per l'utente alla AWS configurazione.

Connessione a AWS dal Toolkit

Per connetterti ai tuoi AWS account dal AWS Toolkit, apri la scheda Guida introduttiva in qualsiasi momento completando quanto segue.

Apertura della scheda Guida introduttiva in Visual Studio

1. Da Visual Studio, espandi Estensioni dal menu principale, quindi espandi il sottomenu Kit di strumenti AWS .

2. Selezionare Getting started (Nozioni di base).
3. La scheda Nozioni di base si apre nella finestra dell'editor di Visual Studio.

Nella scheda Guida introduttiva, ci sono 2 sezioni principali:

- Caratteristiche: in questa sezione puoi abilitare o disabilitare funzionalità come Amazon Q e AWS Toolkit.
- Documentazione e tutorial: una raccolta di riferimenti alle funzionalità abilitate.

> **Note**
>
> La sezione Documentazione e tutorial è visibile solo quando una o più funzionalità sono abilitate.

Amazon Q Developer

Dalla sezione Amazon Q della scheda Getting Started, puoi abilitare o disabilitare Amazon Q, aggiungere una nuova connessione o passare a una AWS connessione diversa. Prima di poter visualizzare o accedere a una di queste azioni, Amazon Q deve essere abilitato. Per abilitare Amazon Q, fai clic sul pulsante Abilita.

Quando Amazon Q è disabilitato, tutte le caratteristiche e le funzioni di Amazon Q vengono completamente rimosse da Visual Studio. L'abilitazione di Amazon Q apre automaticamente l'autenticazione di configurazione per Amazon Q nella scheda Getting Started. Per procedere, devi autenticarti con AWS IAM Identity Center le tue credenziali per accedere al livello Professional o il tuo ID AWS Builder per accedere al piano gratuito. Per informazioni dettagliate su ciascuna delle opzioni di livello, consulta l'argomento Understanding tiers of service for Amazon Q Developer Guide nella Amazon Q Developer User Guide.

Per procedere, completa una delle seguenti procedure.

Autenticazione di livello professionale con IAM Identity Center

> **Note**
>
> I campi Profile Name, Start URL, Profile Region o SSO Region necessari per l'autenticazione con il livello Professional sono in genere forniti da un amministratore dell'azienda o

dell'organizzazione. Per informazioni dettagliate sulle credenziali di IAM Identity Center, consulta l'argomento Cos'è IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center.

1. Dalla schermata Getting Started: AWS Toolkit with Amazon Q, scegli il pulsante Accedi nel riquadro Amazon Q per accedere alla schermata Setup authentication for Amazon Q
2. Dalla schermata Setup authentication for Amazon Q, accedi alla sezione Professional tier, compila i campi obbligatori e seleziona il pulsante Connect.
3. Conferma di voler aprire il portale di richiesta di AWS autorizzazione nel tuo browser web predefinito.
4. Completa i passaggi richiesti dal portale di richiesta di AWS autorizzazione, riceverai una notifica quando è sicuro chiudere il browser e tornare a Visual Studio
5. Nella scheda Getting Started, Amazon Q si aggiorna per mostrare che sei connesso a IAM Identity Center quando il processo è completo.

Autenticazione a livello gratuito con AWS Builder ID

> **Note**
>
> Per ulteriori dettagli su AWS Builder ID, consulta l'argomento Accedi con AWS Builder ID nella Guida per l'utente di AWS accesso.

1. Dalla schermata Getting Started: AWS Toolkit with Amazon Q, scegli il pulsante Accedi nel riquadro Amazon Q per accedere alla schermata Setup authentication for Amazon Q
2. Dalla schermata Configurazione dell'autenticazione per Amazon Q, vai alla sezione Piano gratuito e scegli il pulsante Registrati o Accedi.
3. Conferma di voler aprire il portale di richiesta di AWS autorizzazione nel tuo browser web predefinito.
4. Completa i passaggi richiesti dal portale di richiesta di AWS autorizzazione, riceverai una notifica quando è possibile chiudere il browser e tornare a Visual Studio.
5. Nella scheda Getting Started, Amazon Q si aggiorna per mostrare che sei connesso al tuo ID AWS Builder al termine del processo.

Dopo esserti autenticato con le credenziali IAM Identity Center o AWS Builder ID, puoi accedere ad Amazon Q in Visual Studio. Inoltre, puoi eseguire le seguenti azioni nella scheda Getting Started:

- Esci: disconnette la tua attuale connessione di credenziali da tutte le funzioni di Amazon Q. Amazon Q rimane abilitato, ma la maggior parte delle funzionalità non funziona.
- Disattiva Amazon Q: disattiva completamente tutte le funzionalità di Amazon Q in Visual Studio.

AWS Kit di strumenti

Dalla sezione AWS Toolkit della scheda Guida introduttiva al AWS Toolkit, puoi abilitare o disabilitare il AWS Toolkit, aggiungere una nuova connessione o passare a una connessione diversa. AWS Prima di poter visualizzare o accedere a una di queste azioni, è necessario abilitare il AWS Toolkit. Per abilitare il AWS Toolkit, fate clic sul pulsante Abilita.

Quando il AWS Toolkit è abilitato, Setup authentication for AWS Toolkit viene caricata automaticamente nella scheda Guida introduttiva al AWS Toolkit. Per procedere, devi autenticarti con le tue AWS IAM Identity Centercredenziali o con le credenziali IAM User Role.

> **Note**
>
> Per informazioni dettagliate sulle credenziali IAM Identity Center, consulta l'argomento Cos'è IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center. Per informazioni dettagliate sulle credenziali IAM User Role, consulta l'argomento Chiavi di AWS accesso: credenziali a lungo termine nella guida di riferimento AWS SDKs and Tools.

Autentica e connettiti con IAM Identity Center

1. Dalla schermata Getting Started: AWS Toolkit with Amazon Q, scegli il pulsante Accedi nel riquadro AWS Toolkit per accedere alla schermata Setup authentication for AWS Toolkit.
2. Dalla schermata Setup Authentication for AWS Toolkit, scegli IAM Identity Center (successore di Single Sign-on) dal menu a discesa Profile Type.
3. Dal menu a discesa Scegli da un profilo esistente o aggiungi nuovo, scegli un profilo esistente o seleziona Aggiungi nuovo profilo per aggiungere nuove informazioni sul profilo.

> **Note**
>
> Se scegli un profilo esistente, vai al passaggio 7.

4. Nel campo Nome profilo, inserisci l'account **`profile name`** associato all'account IAM Identity Center con cui desideri autenticarti.
5. Nel campo di testo Start URL, inserisci le **`Start URL`** credenziali allegate alle tue credenziali IAM Identity Center.
6. Dal menu a discesa Profile Region (l'impostazione predefinita è us-east-1), scegli la regione del profilo definita dal profilo utente IAM Identity Center con cui ti stai autenticando.
7. Dal menu a discesa Regione SSO (impostazione predefinita: us-east-1), scegli la regione SSO definita dalle tue credenziali IAM Identity Center.
8. Scegli il pulsante Connect per aprire il sito di richiesta di AWS autorizzazione nel tuo browser web predefinito.
9. Segui le istruzioni nel tuo browser web predefinito, riceverai una notifica quando il processo di autorizzazione è completo, puoi chiudere il browser e tornare a Visual Studio.
10. Nella scheda Guida introduttiva, la sezione AWS Toolkit si aggiorna per mostrare che sei connesso a IAM Identity Center quando il processo è completo.

Autentica e connettiti con le credenziali IAM User Role

1. Dalla schermata Getting Started: AWS Toolkit with Amazon Q, scegli il pulsante Accedi nel riquadro AWS Toolkit per accedere alla schermata Setup authentication for AWS Toolkit.
2. Dalla schermata Setup authentication for AWS Toolkit, scegli IAM User Role dal menu a discesa Profile Type.
3. Nel menu a discesa Scegli da un profilo esistente o aggiungi nuovo, scegli. **`Add new profile`**

> **Note**
>
> Se scegli un nome di profilo esistente dall'elenco, vai al passaggio 8.

4. Nel campo di testo Nome profilo, inserisci un nome per il tuo nuovo profilo.
5. Nel campo di testo Access Key ID, inserisci **`Access Key ID`** il nome del profilo con cui desideri autenticarti.

6. Nel campo di testo Secret Key, inserisci **`Secret Key`** il profilo con cui desideri autenticarti.
7. Dal menu a discesa Posizione di archiviazione (l'impostazione predefinita è Shared Credentials File), specifica se desideri archiviare le credenziali con un file di credenziali condivise o con.NET Encrypted Store.
8. Dai menu a discesa Regione profilo (impostazione predefinita: us-east-1), scegli la partizione e l'area del profilo allegate al profilo con cui desideri autenticarti.
9. Scegli il pulsante Connect per aggiungere questo profilo alla posizione di AWS archiviazione con AWS cui and/or effettuare l'autenticazione.
10. Nella scheda Getting Started, la sezione AWS Toolkit si aggiorna per mostrare che sei connesso alle credenziali del tuo ruolo utente IAM una volta completato il processo.

Dopo esserti autenticato con le tue credenziali IAM Identity Center o IAM User Role, puoi accedere a AWS Explorer nel Toolkit for Visual Studio. Inoltre, puoi disconnetterti e disabilitare il AWS Toolkit for Visual Studio with Amazon Q dalla scheda Getting Started.

Documentazione e tutorial

La sezione documentazione e tutorial si aggiorna automaticamente con suggerimenti di documentazione e tutorial in base alle preferenze di AWS servizio e funzionalità dell'utente. Questi riferimenti sono visibili solo quando è stata abilitata almeno una funzionalità.

Risoluzione dei problemi di installazione per AWS Toolkit for Visual Studio

Le seguenti informazioni sono note per risolvere i problemi di installazione più comuni durante la configurazione di AWS Toolkit for Visual Studio.

Se si verifica un errore durante l'installazione AWS Toolkit for Visual Studio o non è chiaro se l'installazione sia stata completata o meno, consulta le informazioni contenute in ciascuna delle seguenti sezioni.

Autorizzazioni di amministratore per Visual Studio

L' AWS Toolkit for Visual Studio estensione richiede le autorizzazioni di amministratore per garantire che tutti i AWS servizi e le funzionalità siano accessibili.

Se disponi delle autorizzazioni di amministratore locale, è possibile che le autorizzazioni di amministratore non si estendano direttamente all'istanza di Visual Studio.

Per avviare Visual Studio con le autorizzazioni di amministratore a livello locale:

1. Da Windows, individua l'icona di avvio delle applicazioni di Visual Studio.
2. Apri il menu contestuale (fai clic con il pulsante destro del mouse) sull'icona di Visual Studio per aprire il menu contestuale.
3. Seleziona Esegui come amministratore dal menu contestuale.

Per avviare Visual Studio con le autorizzazioni di amministratore in remoto:

1. Da Windows, individua il programma di avvio dell'applicazione che stai utilizzando per connetterti all'istanza remota di Visual Studio.
2. Apri il menu contestuale dell'applicazione (fai clic con il pulsante destro del mouse) per aprire il menu contestuale.
3. Seleziona Esegui come amministratore dal menu contestuale.

> **Note**
>
> Sia che stiate avviando il programma localmente o che vi stiate connettendo in remoto, Windows potrebbe richiedere di confermare le credenziali amministrative.

Ottenere un registro di installazione

Se hai completato i passaggi della precedente sezione Autorizzazioni di amministratore riportata sopra ed è confermato che stai eseguendo o ti connetti a Visual Studio con autorizzazioni di amministratore, ottenere un file di registro di installazione può aiutarti a diagnosticare altri problemi.

Per installare manualmente il file AWS Toolkit for Visual Studio da un `.vsix` file e generare un file di registro di installazione, completa i passaggi seguenti.

1. Dalla pagina di AWS Toolkit for Visual Studiodestinazione, segui il link Download e salva il `.vsix` file della AWS Toolkit for Visual Studio versione che desideri installare.
2. Dal menu principale di Visual Studio, espandi l'intestazione Strumenti, espandi il sottomenu della riga di comando, quindi scegli Visual Studio Developer Command Prompt.

3. Dal prompt dei comandi di Visual Studio Developer, inserisci il `vsixinstaller` comando con il seguente formato:

   ```
   vsixinstaller /logFile:[file path to log file] [file path to Toolkit installation file]
   ```

4. Sostituisci `[file path to log file]` con il nome del file e il percorso completo della directory in cui desideri creare il registro di installazione. Un esempio di `vsixinstaller` comando con il percorso e il nome di file specificati è simile al seguente:

   ```
   vsixinstaller /logFile:C:\Users\Documents\install-log.txt [file path to AWSToolkitPackage.vsix]
   ```

5. Sostituire `[file path to Toolkit installation file]` con il percorso completo del file della directory in cui si `AWSToolkitPackage.vsix` trova.

   Un esempio di `vsixinstaller` comando con il percorso completo del file di installazione di Toolkit dovrebbe essere simile al seguente:

   ```
   vsixinstaller /logFile:[file path to log file] C:\Users\Downloads\AWSToolkitPackage.vsix
   ```

6. Verifica che il nome e i percorsi del file siano corretti, quindi esegui il `vsixinstaller` comando.

   Un esempio di `vsixinstaller` comando completo è simile al seguente:

   ```
   vsixinstaller /logFile:C:\Users\Documents\install-log.txt C:\Users\Downloads\AWSToolkitPackage.vsix
   ```

Installazione di diverse estensioni di Visual Studio

Se hai ottenuto un file di registro di installazione e non riesci ancora a determinare il motivo per cui il processo di installazione non riesce, verifica se riesci a installare altre estensioni di Visual Studio. L'installazione di diverse estensioni di Visual Studio può fornire ulteriori informazioni sui problemi di installazione. Nel caso in cui non sia possibile installare alcuna estensione di Visual Studio, potrebbe essere necessario risolvere i problemi relativi a Visual Studio anziché. AWS Toolkit for Visual Studio

Contattare il supporto

Se hai esaminato tutte le sezioni contenute in questa guida e hai bisogno di risorse o supporto aggiuntivi, puoi visualizzare i problemi precedenti o aprire un nuovo problema dal sito AWS Toolkit for Visual Studio Github Issues.

Per contribuire a velocizzare la soluzione del problema:

- Controlla i problemi passati e attuali per vedere se altri hanno riscontrato una situazione simile.
- Tieni note dettagliate di ogni passaggio che hai intrapreso per risolvere il problema.
- Salva tutti i file di registro che hai ottenuto installando le AWS Toolkit for Visual Studio o altre estensioni.
- Allega i file di registro dell' AWS Toolkit for Visual Studio installazione al nuovo problema.

Profili e rilegatura per finestre

Profili e associazione di finestre per il Toolkit for Visual Studio

Quando utilizzi gli strumenti di pubblicazione, le procedure guidate e altre funzionalità del Toolkit for Visual Studio, tieni presente quanto segue:

- La finestra AWS Explorer è associata a un profilo e a una regione singoli alla volta. Windows è stato aperto dall'impostazione predefinita di AWS Explorer a quel profilo e area associati.
- Dopo l'apertura di una nuova finestra, puoi utilizzare quell'istanza di AWS Explorer per passare a un profilo o una regione diversi.
- Gli strumenti e le funzionalità di pubblicazione di Toolkit for Visual Studio utilizzano automaticamente per impostazione predefinita il profilo e l'area impostati in Explorer AWS .
- Se viene specificato un nuovo profilo o area in uno strumento di pubblicazione, una procedura guidata o una funzionalità: tutte le risorse create in seguito continueranno a utilizzare le nuove impostazioni del profilo e dell'area.
- Se hai più istanze di Visual Studio aperte, ogni istanza può essere associata a un profilo e a un'area diversi.
- AWS Explorer salva l'ultimo profilo e l'ultima area specificati e l'ultima istanza di Visual Studio chiusa avrà i suoi valori persistenti.

Autenticazione e accesso

Non è necessario autenticarsi con per iniziare AWS a lavorare con AWS Toolkit for Visual Studio with Amazon Q. Tuttavia, la AWS maggior parte delle risorse viene gestita tramite un account. AWS Per accedere a tutti i servizi e le funzionalità di AWS Toolkit for Visual Studio with Amazon Q, sono necessari almeno 2 tipi di autenticazione dell'account:

1. AWS Identity and Access Management (IAM) o AWS IAM Identity Centerautenticazione per i tuoi AWS account. La maggior parte AWS dei servizi e delle risorse viene gestita tramite IAM e IAM Identity Center.
2. Un AWS Builder ID è facoltativo per alcuni altri AWS servizi.

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

Argomenti

- AWS Credenziali IAM Identity Center in AWS Toolkit for Visual Studio
- AWS Credenziali IAM
- AWS ID del costruttore
- Autenticazione a più fattori (MFA) in Toolkit for Visual Studio
- Configurazione di credenziali esterne
- Aggiornamento di firewall e gateway per consentire l'accesso

AWS Credenziali IAM Identity Center in AWS Toolkit for Visual Studio

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

Per istruzioni dettagliate su come configurare IAM Identity Center for Software Development Kits (SDKs) e su come configurare IAM Identity Center AWS Toolkit for Visual Studio, consulta la sezione sull'autenticazione di IAM Identity Center della AWS SDKs and Tools Reference Guide.

Autenticazione con IAM Identity Center dal AWS Toolkit for Visual Studio

Per autenticarti con IAM Identity Center AWS Toolkit for Visual Studio aggiungendo un profilo IAM Identity Center al tuo `config` file `credentials` or, completa i seguenti passaggi.

1. Dal tuo editor di testo preferito, apri AWS le informazioni sulle credenziali memorizzate nel `<hone-directory>\.aws\credentials` file.
2. Nella sezione `credentials file` sottostante`[default]`, aggiungi un modello per un profilo denominato IAM Identity Center. Di seguito è riportato un modello di esempio:

> **Important**
>
> Non utilizzate la parola profilo quando create una voce nel `credential` file perché crea un conflitto con le convenzioni di denominazione dei `credential` file.
> Includete la parola di prefisso `profile_` solo quando configurate un profilo denominato nel file. `config`

```
[sso-user-1]
sso_start_url = https://example.com/start
sso_region = us-east-2
sso_account_id = 123456789011
sso_role_name = readOnly
region = us-west-2
```

- **`sso_start_url`**: L'URL che rimanda al portale utenti IAM Identity Center della tua organizzazione.
- **`sso_region`**: La AWS regione che contiene l'host del portale IAM Identity Center. Questa può essere diversa dalla AWS regione specificata più avanti nel `region` parametro predefinito.
- **`sso_account_id`**: L'ID dell' AWS account che contiene il ruolo IAM con l'autorizzazione che desideri concedere a questo utente di IAM Identity Center.
- **`sso_role_name`**: Il nome del ruolo IAM che definisce le autorizzazioni dell'utente quando utilizza questo profilo per ottenere credenziali tramite IAM Identity Center.
- **`region`**: La AWS regione predefinita a cui questo utente di IAM Identity Center accede.

> **Note**
>
> Puoi anche aggiungere un profilo abilitato per IAM Identity Center al tuo AWS CLI eseguendo il `aws configure sso` comando. Dopo aver eseguito questo comando, fornisci i valori per l'URL di avvio di IAM Identity Center (`sso_start_url`) e la AWS regione (`region`) che ospita la directory IAM Identity Center.
> Per ulteriori informazioni, consulta Configurazione della AWS CLI per l' AWS utilizzo del Single Sign-On nella Guida per l'utente.AWS Command Line Interface

Accesso con IAM Identity Center

Quando si accede con un profilo IAM Identity Center, il browser predefinito viene avviato nel modo `sso_start_url` specificato nel file`credential file`. È necessario verificare l'accesso a IAM Identity Center prima di poter accedere alle AWS risorse in AWS Toolkit for Visual Studio. Se le tue credenziali scadono, dovrai ripetere il processo di connessione per ottenere nuove credenziali temporanee.

AWS Credenziali IAM

AWS Le credenziali IAM si autenticano con il tuo AWS account tramite chiavi di accesso archiviate localmente.

Le seguenti sezioni descrivono come configurare le credenziali IAM per l'autenticazione con il tuo AWS account da. AWS Toolkit for Visual Studio

> **Important**
>
> Prima di configurare le credenziali IAM per l'autenticazione con il tuo AWS account, tieni presente che:
>
> - Se hai già impostato le credenziali IAM tramite un altro AWS servizio (come il AWS CLI), allora rileva AWS Toolkit for Visual Studio automaticamente tali credenziali.
> - AWS consiglia di utilizzare l'autenticazione. AWS IAM Identity Center Per ulteriori informazioni sulle best practice di AWS IAM, consulta la sezione Security best practice in IAM della AWS Identity and Access Management User Guide.
> - 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 AWS IAM Identity Center. Per ulteriori informazioni, consulta What is IAM Identity Center? nella Guida AWS IAM Identity Center per l'utente.

Creazione di un utente IAM

Prima di poter configurare l'autenticazione con il AWS Toolkit for Visual Studio tuo AWS account, devi completare il Passaggio 1: Crea il tuo utente IAM e il Passaggio 2: Ottieni le chiavi di accesso nell'argomento Autenticazione con credenziali a lungo termine nella Guida di riferimento agli strumenti AWS SDKs e agli strumenti.

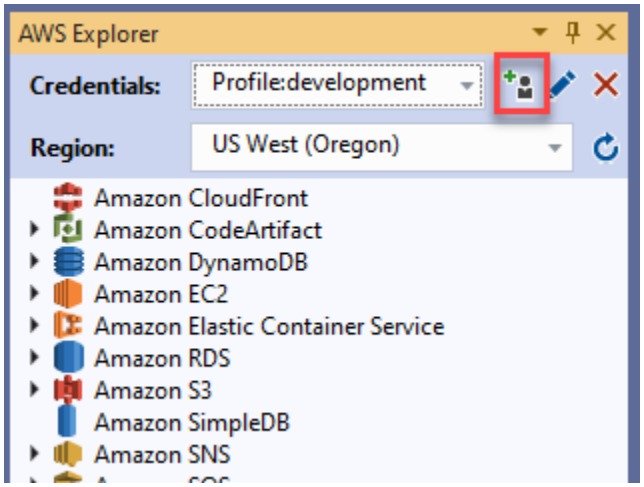
> **Note**
>
> Passaggio 3: L'aggiornamento delle credenziali condivise è facoltativo.
> Se completi il passaggio 3, rileva AWS Toolkit for Visual Studio automaticamente le tue credenziali da. `credentials file`
> Se non hai completato il Passaggio 3, ti AWS Toolkit for Visual Studio guiderà attraverso il processo di creazione di un file `credentials file` come descritto nella AWS Toolkit for Visual Studio sezione Creazione di un file di credenziali, riportata di seguito.

Creazione di un file di credenziali

Per aggiungere o creare un utente `credentials file` da: AWS Toolkit for Visual Studio

> **Note**
>
> Quando viene aggiunto un nuovo profilo utente dal toolkit:
>
> - Se esiste `credentials file` già un, le nuove informazioni utente vengono aggiunte al file esistente.
> - Se `credentials file` non esiste un file, viene creato un nuovo file.

1. Da AWS Explorer scegli l'icona Nuovo profilo dell'account per aprire la finestra di dialogo Nuovo profilo dell'account.



2. Completa i campi obbligatori nella finestra di dialogo Nuovo profilo dell'account e scegli il pulsante OK per creare l'utente IAM.

Modifica delle credenziali utente IAM dal toolkit

Per modificare le credenziali utente IAM dal toolkit, completa i seguenti passaggi:

1. Dal menu a discesa Credenziali in AWS Explorer, scegli la credenziale utente IAM che desideri modificare.
2. Scegli l'icona Modifica profilo per aprire la finestra di dialogo Modifica profilo.
3. Dalla finestra di dialogo Modifica profilo completa gli aggiornamenti e scegli il pulsante OK per salvare le modifiche.

Per eliminare le credenziali utente IAM dal toolkit, completa i seguenti passaggi:

1. Dal menu a discesa Credenziali in AWS Explorer, scegli la credenziale utente IAM che desideri eliminare.
2. Scegli l'icona Elimina profilo per aprire il prompt Elimina profilo.
3. Conferma di voler eliminare il profilo per rimuoverlo dal tuo`Credentials file`.

> **Important**
>
> I profili che supportano funzionalità di accesso avanzate, come IAM Identity Center o l'autenticazione a più fattori (MFA) nella finestra di dialogo Modifica profilo, non possono

essere modificati da. AWS Toolkit for Visual Studio Per apportare modifiche a questi tipi di profili, è necessario modificarli `credentials file` utilizzando un editor di testo.

Modifica delle credenziali utente IAM da un editor di testo

Oltre a gestire gli utenti IAM con AWS Toolkit for Visual Studio, puoi modificare `credential files` dal tuo editor di testo preferito. La posizione predefinita `credential file` di Windows è`C:\Users\`*`USERNAME`*`\.aws\credentials`.

Per maggiori dettagli sulla posizione e sulla struttura di`credential files`, consulta la sezione File di configurazione e credenziali condivisi della guida AWS SDKs and Tools Reference.

Creazione di utenti IAM da () AWS Command Line Interface AWS CLI

AWS CLI Questo è un altro strumento che puoi usare per creare un utente IAM in`credentials file`, utilizzando il comando`aws configure`.

Per informazioni dettagliate sulla creazione di utenti IAM da, AWS CLI consulta la sezione Configurazione degli AWS CLI argomenti nella Guida per l'AWS CLI utente.

Il Toolkit for Visual Studio supporta le seguenti proprietà di configurazione:

```
aws_access_key_id
aws_secret_access_key
aws_session_token
credential_process
credential_source
external_id
mfa_serial
role_arn
role_session_name
source_profile
sso_account_id
sso_region
sso_role_name
sso_start_url
```

AWS ID del costruttore

AWS Builder ID è un metodo di AWS autenticazione aggiuntivo che può essere necessario per utilizzare determinati servizi o funzionalità, come la clonazione di un repository di terze parti con Amazon. CodeCatalyst

Per informazioni dettagliate sul metodo di autenticazione AWS Builder ID, consulta l'argomento Accedi con AWS Builder ID nella Guida per l'utente di accesso.AWS

Per ulteriori informazioni sulla clonazione di un repository per CodeCatalyst from AWS Toolkit for Visual Studio, consulta l' CodeCatalystargomento Working with Amazon in questa Guida per l'utente.

Autenticazione a più fattori (MFA) in Toolkit for Visual Studio

L'autenticazione a più fattori (MFA) è una sicurezza aggiuntiva per AWS i tuoi account. La MFA richiede agli utenti di fornire credenziali di accesso e autenticazione univoca da un meccanismo AWS MFA supportato quando accedono a siti Web o servizi. AWS

AWS supporta una gamma di dispositivi virtuali e hardware per l'autenticazione MFA. Di seguito è riportato un esempio di dispositivo MFA virtuale abilitato tramite un'applicazione per smartphone. Per ulteriori informazioni sulle opzioni dei dispositivi MFA, consulta Using Multi-Factor Authentication (MFA) AWS nella IAM User Guide.

Fase 1: creazione di un ruolo IAM per delegare l'accesso agli utenti IAM

La procedura seguente descrive come impostare la delegazione dei ruoli per l'assegnazione delle autorizzazioni a un utente IAM. Per informazioni dettagliate sulla delega dei ruoli, consulta l'argomento Creazione di un ruolo per delegare le autorizzazioni a un utente IAM nella Guida per l'utente.AWS Identity and Access Management

1. Vai alla console IAM all'indirizzo /iam. https://console.aws.amazon.com
2. Scegli Ruoli nella barra di navigazione, quindi scegli Crea ruolo.
3. Nella pagina Crea ruolo, scegli Altro AWS account.
4. Inserisci l'ID account richiesto e contrassegna la casella di controllo Richiedi MFA.

> **Note**
>
> Per trovare il tuo numero di account (ID) a 12 cifre, vai alla barra di navigazione nella console, quindi scegli Support, Support Center.

5. Scegli Successivo: autorizzazioni.
6. Associa le politiche esistenti al tuo ruolo o creane una nuova. Le policy scelte in questa pagina determinano a quali AWS servizi l'utente IAM può accedere con il Toolkit.
7. Dopo aver associato le politiche, scegli Avanti: Tag per l'opzione di aggiungere tag IAM al tuo ruolo. Quindi scegli Avanti: Revisione per continuare.
8. Nella pagina Revisione, inserisci il nome del ruolo richiesto (toolkit-role, ad esempio). Puoi anche aggiungere una descrizione del ruolo facoltativa.
9. Scegli Crea ruolo.
10. Quando viene visualizzato il messaggio di conferma («The role toolkit-role has been created», ad esempio), scegli il nome del ruolo nel messaggio.
11. Nella pagina Riepilogo, scegliete l'icona di copia per copiare l'ARN del ruolo e incollarlo in un file. (È necessario questo ARN per configurare l'utente IAM per assumere il ruolo.).

Passaggio 2: creazione di un utente IAM che assuma le autorizzazioni del ruolo

Questo passaggio crea un utente IAM senza autorizzazioni in modo da poter aggiungere una policy in linea.

1. Vai alla console IAM all'indirizzo https://console.aws.amazon.com /iam.
2. Scegli Utenti nella barra di navigazione, quindi scegli Aggiungi utente.
3. Nella pagina Aggiungi utente, inserisci un nome utente richiesto (toolkit-user, ad esempio) e seleziona la casella di controllo Accesso programmatico.
4. Scegliete Avanti: Autorizzazioni, Avanti: Tag e Avanti: Revisione per passare alle pagine successive. Non stai aggiungendo autorizzazioni in questa fase perché l'utente assumerà le autorizzazioni del ruolo.
5. Nella pagina di revisione, vieni informato che Questo utente non dispone di autorizzazioni. Selezionare Create user (Crea utente).

6. Nella pagina Operazione completata, scegli Scarica .csv per scaricare il file contenente l'ID della chiave di accesso e la chiave di accesso segreta. (Sono necessari entrambi per definire il profilo dell'utente nel file delle credenziali).
7. Scegli Chiudi.

Fase 3: Aggiungere una policy per consentire all'utente IAM di assumere il ruolo

La procedura seguente crea una policy in linea che consente all'utente di assumere il ruolo (e le autorizzazioni di quel ruolo).

1. Nella pagina Utenti della console IAM, scegli l'utente IAM che hai appena creato (toolkit-user, ad esempio).
2. Nella scheda Autorizzazioni della pagina di riepilogo, scegli Aggiungi politica in linea.
3. Nella pagina Crea politica, scegli Scegli un servizio, inserisci STS in Trova un servizio, quindi scegli STS dai risultati.
4. Per Azioni, inizia a inserire il termine AssumeRole. Contrassegna la AssumeRolecasella di controllo quando viene visualizzata.
5. Nella sezione Risorsa, assicurati che sia selezionato Specifico e fai clic su Aggiungi ARN per limitare l'accesso.
6. Nella finestra di dialogo Aggiungi ARN, per Specificare ARN per ruolo aggiungere l'ARN del ruolo creato nel passaggio 1.

   Dopo aver aggiunto l'ARN del ruolo, l'account attendibile e il nome del ruolo associati a quel ruolo vengono visualizzati in Account e Nome ruolo con percorso.
7. Scegliere Aggiungi.
8. Tornando alla pagina Crea policy, scegli Specificare le condizioni di richiesta (opzionale), contrassegna la casella di controllo MFA obbligatoria, quindi scegli Chiudi per confermare.
9. Scegli Esamina policy.
10. Nella pagina Revisione della politica, inserisci un nome per la politica, quindi scegli Crea politica.

    La scheda Autorizzazioni mostra la nuova politica in linea allegata direttamente all'utente IAM.

Fase 4: Gestione di un dispositivo MFA virtuale per l'utente IAM

1. Scarica e installa un'applicazione MFA virtuale sul tuo smartphone.

   Per un elenco delle applicazioni supportate, consulta la pagina delle risorse sull'autenticazione a più fattori.
2. Nella console IAM, scegli Utenti dalla barra di navigazione, quindi scegli l'utente che assume un ruolo (toolkit-user, in questo caso).
3. Nella pagina Riepilogo, scegli la scheda Credenziali di sicurezza e per Dispositivo MFA assegnato scegli Gestisci.
4. Nel riquadro Gestisci dispositivo MFA, scegli Dispositivo MFA virtuale, quindi scegli Continua.
5. Nel riquadro Configura dispositivo MFA virtuale, scegli Mostra codice QR, quindi scansiona il codice utilizzando l'applicazione MFA virtuale installata sullo smartphone.
6. Dopo aver scansionato il codice QR, l'applicazione MFA virtuale genera codici MFA monouso. Inserisci due codici MFA consecutivi nel codice MFA 1 e nel codice MFA 2.
7. Scegliere Assign MFA (Assegna MFA).
8. Tornando alla scheda Credenziali di sicurezza per l'utente, copia l'ARN del nuovo dispositivo MFA assegnato.

   L'ARN include l'ID dell'account a 12 cifre e il formato è simile al seguente:. `arn:aws:iam::123456789012:mfa/toolkit-user` Questo ARN è necessario per definire il profilo MFA nel passaggio successivo.

Fase 5: Creazione di profili per consentire l'autenticazione a più fattori

La procedura seguente crea i profili che consentono l'autenticazione a più fattori quando si accede ai AWS servizi dal Toolkit for Visual Studio.

I profili che crei includono tre informazioni che hai copiato e archiviato durante i passaggi precedenti:

- Chiavi di accesso (ID della chiave di accesso e chiave di accesso segreta) per l'utente IAM
- ARN del ruolo che delega le autorizzazioni all'utente IAM
- ARN del dispositivo MFA virtuale assegnato all'utente IAM

Nel file di credenziali AWS condiviso o nell'SDK Store che contiene AWS le tue credenziali, aggiungi le seguenti voci:

```
[toolkit-user]
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

[mfa]
source_profile = toolkit-user
role_arn = arn:aws:iam::111111111111:role/toolkit-role
mfa_serial = arn:aws:iam::111111111111:mfa/toolkit-user
```

Nell'esempio fornito sono definiti due profili:

- `[toolkit-user]`il profilo include la chiave di accesso e la chiave di accesso segreta che sono state generate e salvate quando hai creato l'utente IAM nella fase 2.
- `[mfa]`profile definisce come è supportata l'autenticazione a più fattori. Sono disponibili tre voci:

  ◦`source_profile`: specifica il profilo le cui credenziali vengono utilizzate per assumere il ruolo specificato da questa `role_arn` impostazione in questo profilo. In questo caso, è il `toolkit-user` profilo.

  ◦`role_arn`: specifica l'Amazon Resource Name (ARN) del ruolo IAM che desideri utilizzare per eseguire le operazioni richieste utilizzando questo profilo. In questo caso, è l'ARN per il ruolo creato nella Fase 1.

  ◦`mfa_serial`: specifica l'identificazione o il numero di serie del dispositivo MFA che l'utente deve utilizzare quando assume un ruolo. In questo caso, è l'ARN del dispositivo virtuale configurato nel passaggio 3.

Configurazione di credenziali esterne

Se disponi di un metodo per generare o cercare credenziali che non è direttamente supportato da AWS, puoi aggiungere al file delle credenziali condivise un profilo che contiene l'impostazione. `credential_process` Questa impostazione specifica un comando esterno che viene eseguito per generare o recuperare le credenziali di autenticazione da utilizzare. Ad esempio, è possibile includere nel file una voce simile alla seguente: `config`

```
[profile developer]
credential_process = /opt/bin/awscreds-custom --username helen
```

Per ulteriori informazioni sull'utilizzo di credenziali esterne e sui rischi per la sicurezza associati, vedere Acquisizione di credenziali con un processo esterno nella Guida per l'AWS Command Line Interface utente.

Aggiornamento di firewall e gateway per consentire l'accesso

Se filtri l'accesso a AWS domini o endpoint URL specifici utilizzando una soluzione di filtraggio dei contenuti Web, è necessario che siano elencati i seguenti endpoint per accedere a tutti i servizi e le funzionalità disponibili tramite AWS Toolkit for Visual Studio Amazon Q. Per passaggi dettagliati su come risolvere le impostazioni firewall e proxy per il Toolkit AWS con Amazon Q, consulta la sezione Impostazioni firewall e proxy nell'argomento Risoluzione dei problemi in questa Guida per l'utente. Per informazioni dettagliate sulla configurazione di un proxy aziendale per Amazon Q, consulta l'argomento Configurazione di un proxy aziendale in Amazon Q nella Amazon Q Developer User Guide.

AWS Toolkit for Visual Studio Endpoint

Di seguito sono riportati gli elenchi di endpoint e riferimenti AWS Toolkit for Visual Studio specifici che devono essere consentiti.

Endpoints

```
https://idetoolkits-hostedfiles.amazonaws.com/*
https://idetoolkits.amazonwebservices.com/*
http://vstoolkit.amazonwebservices.com/*
https://aws-vs-toolkit.s3.amazonaws.com/*
https://raw.githubusercontent.com/aws/aws-toolkit-visual-studio/main/version.json
https://aws-toolkit-language-servers.amazonaws.com/*
```

Endpoint del plug-in Amazon Q

Di seguito è riportato un elenco di endpoint e riferimenti specifici del plug-in Amazon Q che devono essere elencati come consentiti.

```
https://idetoolkits-hostedfiles.amazonaws.com/*    (Plugin for configs)
https://idetoolkits.amazonwebservices.com/*   (Plugin for endpoints)
```

```
https://aws-toolkit-language-servers.amazonaws.com/*  (Language Server Process)
https://client-telemetry.us-east-1.amazonaws.com/ (Telemetry)
https://cognito-identity.us-east-1.amazonaws.com    (Telemetry)
https://aws-language-servers.us-east-1.amazonaws.com (Language Server Process)
```

Endpoint Amazon Q Developer

Di seguito è riportato un elenco di endpoint e riferimenti specifici di Amazon Q Developer che devono essere elencati.

```
https://codewhisperer.us-east-1.amazonaws.com (Inline,Chat, QSDA,...)
https://q.us-east-1.amazonaws.com (Inline,Chat, QSDA....)
https://desktop-release.codewhisperer.us-east-1.amazonaws.com/ (Download URL for CLI.)
https://specs.q.us-east-1.amazonaws.com (URL for auto-complete specs used by CLI)
* aws-language-servers.us-east-1.amazonaws.com (Local Workspace context)
```

Endpoint Amazon Q Code Transform

Di seguito è riportato un elenco di endpoint e riferimenti specifici di Amazon Q Code Transform che devono essere elencati.

```
https://docs.aws.amazon.com/amazonq/latest/qdeveloper-ug/security_iam_manage-access-
with-policies.html
```

Endpoint di autenticazione

Di seguito è riportato un elenco di endpoint e riferimenti di autenticazione che devono essere consentiti.

```
[Directory ID or alias].awsapps.com
* oidc.[Region].amazonaws.com
*.sso.[Region].amazonaws.com
*.sso-portal.[Region].amazonaws.com
*.aws.dev
```

```
*.awsstatic.com
*.console.aws.a2z.com
*.sso.amazonaws.com
```

Endpoint di identità

Gli elenchi seguenti contengono endpoint specifici dell'identità, come AWS Builder AWS IAM Identity Center ID.

AWS IAM Identity Center

Per i dettagli sugli endpoint richiesti per IAM Identity Center, consulta l'argomento Abilita IAM Identity Center nella Guida per l'AWS IAM Identity Centerutente.

Enterprise IAM Identity Center

```
https://[Center director id].awsapps.com/start (should be permitted to initiate auth)
https://us-east-1.signin.aws (for facilitating authentication, assuming IAM Identity
 Center is in IAD)
https://oidc.(us-east-1).amazonaws.com
https://log.sso-portal.eu-west-1.amazonaws.com
https://portal.sso.eu-west-1.amazonaws.com
```

AWS ID del costruttore

```
https://view.awsapps.com/start (must be blocked to disable individual tier)
https://codewhisperer.us-east-1.amazonaws.com and q.us-east-1.amazonaws.com (should be
 permitted)
```

Telemetria

Di seguito è riportato un endpoint specifico per la telemetria che deve essere elencato come consentito.

```
https://telemetry.aws-language-servers.us-east-1.amazonaws.com/
```

```
https://client-telemetry.us-east-1.amazonaws.com
```

Riferimenti

Di seguito è riportato un elenco di riferimenti agli endpoint.

```
idetoolkits-hostedfiles.amazonaws.com
cognito-identity.us-east-1.amazonaws.com
amazonwebservices.gallery.vsassets.io
eu-west-1.prod.pr.analytics.console.aws.a2z.com
prod.pa.cdn.uis.awsstatic.com
portal.sso.eu-west-1.amazonaws.com
log.sso-portal.eu-west-1.amazonaws.com
prod.assets.shortbread.aws.dev
prod.tools.shortbread.aws.dev
prod.log.shortbread.aws.dev
a.b.cdn.console.awsstatic.com
assets.sso-portal.eu-west-1.amazonaws.com
oidc.eu-west-1.amazonaws.com
aws-toolkit-language-servers.amazonaws.com
aws-language-servers.us-east-1.amazonaws.com
idetoolkits.amazonwebservices.com
```

Lavorare con AWS i servizi

I seguenti argomenti descrivono come iniziare a lavorare con AWS i servizi del AWS Toolkit for Visual Studio with Amazon Q.

Argomenti

Amazon CodeCatalyst per il AWS Toolkit per Visual Studio con Amazon Q

Che cos'è Amazon CodeCatalyst?

Amazon CodeCatalyst è uno spazio di collaborazione basato sul cloud per i team di sviluppo software. Utilizzando AWS Toolkit for Visual Studio with Amazon Q, puoi visualizzare e CodeCatalyst

gestire le risorse direttamente AWS da Toolkit for Visual Studio with Amazon Q. Per ulteriori CodeCatalyst informazioni, consulta la CodeCatalyst Amazon User Guide.

I seguenti argomenti descrivono come connettere il AWS Toolkit for Visual Studio CodeCatalyst con Amazon Q e come utilizzarlo tramite AWS il Toolkit for Visual Studio CodeCatalyst con Amazon Q.

Argomenti

Guida introduttiva ad Amazon CodeCatalyst e al AWS Toolkit for Visual Studio con Amazon Q

Per iniziare a lavorare con Amazon CodeCatalyst dal AWS Toolkit for Visual Studio with Amazon Q, completa quanto segue.

Argomenti

Installazione del AWS Toolkit for Visual Studio con Amazon Q

Prima di integrare AWS Toolkit for Visual Studio con Amazon Q con i CodeCatalyst tuoi account, assicurati di utilizzare una versione corrente AWS di Toolkit for Visual Studio con Amazon Q. Per dettagli su come installare e configurare la AWS versione più recente di Toolkit for Visual Studio con Amazon Q, consulta la sezione Configurazione del Toolkit for Visual Studio Q di questa Guida per AWS l'utente.

Creazione di un account e di un Builder ID CodeCatalyst AWS

Oltre a installare la versione più recente di AWS Toolkit for Visual Studio con Amazon Q, devi avere un Builder ID CodeCatalyst e un account AWS attivi per connetterti a Toolkit for Visual Studio AWS con Amazon Q. Se non disponi di un Builder ID CodeCatalyst o di un account AWS attivo, consulta la sezione CodeCatalyst Configurazione con nella Guida per l'utente. CodeCatalyst

> **Note**
>
> Un AWS Builder ID è diverso dalle tue credenziali. AWS Per istruzioni su come registrarsi e autenticarsi con un AWS Builder ID, consulta l'argomento Autenticazione e accesso: AWS Builder ID in questa guida utente.
> Per informazioni dettagliate su AWS Builder IDs, consulta l'argomento AWS Builder ID nella Guida utente di riferimento generale.AWS

Connessione di AWS Toolkit for Visual Studio con Amazon Q con CodeCatalyst

Per connettere AWS Toolkit for Visual Studio con Amazon Q con CodeCatalyst il tuo account, completa i seguenti passaggi.

1. Dalla voce di menu Git in Visual Studio, scegli Clone Repository... .
2. Nella sezione Sfoglia un repository, seleziona Amazon CodeCatalyst come provider.
3. Dalla sezione Connessione, scegli Connect with AWS Builder ID per aprire la CodeCatalyst console nel tuo browser web preferito.
4. Dal browser, inserisci il tuo ID AWS Builder nel campo fornito e segui le istruzioni per continuare.
5. Quando richiesto, scegli Consenti per confermare la connessione tra AWS Toolkit for Visual Studio with Amazon Q e CodeCatalyst il tuo account. Quando il processo di connessione è completo, CodeCatalyst visualizza una conferma che indica che la chiusura del browser è sicura.

Utilizzo CodeCatalyst delle risorse Amazon del AWS Toolkit for Visual Studio con Amazon Q

Le seguenti sezioni forniscono una panoramica delle funzionalità di gestione CodeCatalyst delle risorse di Amazon Amazon disponibili per AWS Toolkit for Visual Studio with Amazon Q.

Argomenti

Clonazione di un repository

CodeCatalyst è un servizio basato sul cloud che richiede la connessione al cloud per lavorare sui progetti. CodeCatalyst Per lavorare su un progetto localmente, puoi clonare gli CodeCatalyst archivi

sul tuo computer locale e sincronizzarli con il CodeCatalyst progetto la prossima volta che ti connetti al cloud.

Per clonare un repository sul computer locale, completa i seguenti passaggi.

1. Dalla voce di menu Git in Visual Studio, scegli Clone Repository... .
2. Nella sezione Sfoglia un repository, seleziona Amazon CodeCatalyst come provider.

> **Note**
>
> Se nella sezione Connessione viene visualizzato un `Not Connected` messaggio, completa i passaggi indicati nella sezione Autenticazione e accesso: AWS Builder ID di questa Guida per l'utente prima di procedere.

3. Scegli lo spazio e il progetto da cui vuoi clonare un repository.
4. Dalla sezione Repository, scegli il repository che desideri clonare.
5. Dalla sezione Percorso, scegli la cartella in cui vuoi clonare il tuo repository.

> **Note**
>
> Questa cartella deve inizialmente essere vuota per clonarla correttamente.

6. Seleziona Clone per iniziare a clonare il repository.
7. Dopo la clonazione del repository, Visual Studio caricherà la soluzione clonata

> **Note**
>
> Se Visual Studio non apre la soluzione nell'archivio clonato, le opzioni di Visual Studio possono essere modificate dall'impostazione Carica automaticamente la soluzione all'apertura di un repository Git, che si trova nelle Impostazioni globali Git, del menu Source Control.

Risoluzione dei problemi

Di seguito sono riportati gli argomenti per la risoluzione di problemi noti quando si lavora con Amazon CodeCatalyst dal AWS Toolkit for Visual Studio with Amazon Q.

Argomenti

Credenziali

Se incontri una finestra di dialogo che richiede le credenziali quando tenti di clonare un repository basato su git da CodeCatalyst, il tuo AWS CodeCommit Credential helper potrebbe essere configurato a livello globale, causando interferenze con. CodeCatalyst Per ulteriori informazioni sull'helper per le AWS CodeCommit credenziali, consulta la sezione Configurazione delle connessioni HTTPS ai AWS CodeCommit repository su Windows con l'helper delle credenziali AWS CLI della Guida per l'utente. AWS CodeCommit

Per limitare l'helper per le AWS CodeCommit credenziali alla sola gestione, completa i seguenti passaggi. CodeCommit URLs

1. apri il file di configurazione globale git in: `%userprofile%\.gitconfig`
2. Individua la sezione seguente nel tuo file:

```
[credential]
    helper = !aws codecommit credential-helper $@
    UseHttpPath = true
```

3. Modifica quella sezione come segue:

```
[credential "https://git-codecommit.*.amazonaws.com"]
    helper = !aws codecommit credential-helper $@
    UseHttpPath = true
```

4. Salva le modifiche, quindi completa i passaggi per clonare il tuo repository.

Integrazione con Amazon CloudWatch Logs per Visual Studio

L'integrazione di Amazon CloudWatch Logs di AWS Toolkit for Visual Studio con Amazon Q ti dà la possibilità di monitorare, archiviare e CloudWatch accedere alle risorse di Logs senza dover

uscire dal tuo IDE. Per ulteriori informazioni sulla configurazione del CloudWatch servizio e su come utilizzare le funzionalità di CloudWatch Logs, scegli uno dei seguenti argomenti.

Argomenti

Configurazione dell'integrazione CloudWatch dei log per Visual Studio

Prima di poter utilizzare l'integrazione di Amazon CloudWatch Logs con il AWS Toolkit con Amazon Q, è necessario un AWS account. Puoi creare un nuovo AWS account dal sito di AWS accesso. La maggior parte delle funzionalità di CloudWatch Logs disponibili nel AWS Toolkit con Amazon Q sono accessibili con credenziali attive AWS . Se una particolare funzionalità richiede una configurazione aggiuntiva, i requisiti sono inclusi nelle sezioni pertinenti della guida Working with CloudWatch Logs.

Per ulteriori informazioni e opzioni sulla configurazione CloudWatch dei log, consulta la sezione Come configurare la configurazione della guida Amazon CloudWatch Logs.

Utilizzo dei CloudWatch log in Visual Studio

L'integrazione con Amazon CloudWatch Logs ti consente di monitorare, archiviare e accedere ai CloudWatch log dal AWS Toolkit for Visual Studio con Amazon Q. L'accesso alle CloudWatch funzionalità di Logs, senza dover uscire dal tuo IDE, migliora l'efficienza semplificando CloudWatch il processo di sviluppo dei Logs e riducendo le interruzioni del flusso di lavoro. I seguenti argomenti descrivono come utilizzare le caratteristiche e le funzioni di base dell'integrazione Logs. CloudWatch

Argomenti

CloudWatch Gruppi di log

A `log group` è un gruppo `log streams` che condivide le stesse impostazioni di conservazione, monitoraggio e controllo degli accessi. Non vi è alcun limite al numero di flussi di log che possono appartenere a un gruppo di log.

Visualizzazione dei gruppi di log

La `View Log Groups` funzione visualizza un elenco di gruppi di log nel CloudWatch Log Groups Explorer.

Per accedere alla funzionalità Visualizza gruppi di log e aprire CloudWatch Log Groups Explorer, completa i seguenti passaggi.

1. Da AWS Explorer, espandi Amazon CloudWatch.
2. Fai doppio clic su Log Groups o apri il menu contestuale (fai clic con il pulsante destro del mouse) e seleziona Visualizza per aprire CloudWatch Log Groups Explorer.

> **Note**
>
> Il CloudWatch Log Groups Explorer si aprirà nella stessa finestra del Solutions Explorer.

Filtraggio dei gruppi di log

Il tuo account individuale è in grado di contenere migliaia di gruppi di log diversi. Per semplificare la ricerca di gruppi specifici, utilizza la `filtering` funzione descritta di seguito.

1. Da CloudWatch Log Groups Explorer, posiziona il cursore nella barra di ricerca situata nella parte superiore della finestra.
2. Inizia a digitare un prefisso relativo ai gruppi di log che stai cercando.
3. CloudWatch Log Groups Explorer viene aggiornato automaticamente per mostrare i risultati corrispondenti ai termini di ricerca specificati nel passaggio precedente.

Elimina i gruppi di log

Per eliminare un gruppo di log specifico, fare riferimento alla seguente procedura.

1. Da CloudWatch Log Groups Explorer, fate clic con il pulsante destro del mouse sul gruppo di log che desiderate eliminare.
2. Quando richiesto, confermate che desiderate eliminare il gruppo di log attualmente selezionato.
3. Scegliendo il pulsante Sì si elimina il gruppo di log selezionato, quindi si aggiorna il CloudWatch Log Groups Explorer.

Aggiorna i gruppi di log

Per aggiornare l'elenco corrente dei gruppi di log visualizzato in CloudWatch Log Groups Explorer, scegliete il pulsante con l'icona Aggiorna situato nella barra degli strumenti.

Copia l'ARN del gruppo di log

Per copiare l'ARN di un gruppo di log specifico, completare i passaggi descritti di seguito.

1. Da CloudWatch Log Groups Explorer, fai clic con il pulsante destro del mouse sul gruppo di log da cui vuoi copiare un ARN.
2. Scegli l'opzione Copia ARN dal menu.
3. L'ARN è ora copiato negli appunti locali e pronto per essere incollato.

CloudWatch Registra gli stream

Un flusso di log è una sequenza di log eventi che condividono la stessa origine.

> **Note**
>
> Durante la visualizzazione dei flussi di registro, tenete presente le seguenti proprietà:
>
> - Per impostazione predefinita, i flussi di registro sono ordinati in base al timestamp dell'evento più recente.
> - Le colonne associate a un flusso di log possono essere ordinate in ordine crescente o decrescente, spostando il cursore situato nelle intestazioni delle colonne.
> - Le voci filtrate possono essere ordinate solo in base al nome del flusso di registro.

Visualizzazione dei flussi di registro

1. In CloudWatch Log Groups Explorer, fate doppio clic su un gruppo di log oppure fate clic con il pulsante destro del mouse su un gruppo di log e selezionate View Log Stream dal menu contestuale.
2. Nella finestra del documento si aprirà una nuova scheda che contiene un elenco di flussi di log associati al gruppo di log.

Filtraggio dei flussi di log

1. Dalla scheda Log Streams, nella finestra del documento, posiziona il cursore nella barra di ricerca.
2. Inizia a digitare un prefisso relativo al flusso di log che stai cercando.
3. Durante la digitazione, la visualizzazione corrente si aggiorna automaticamente per filtrare i Log Stream in base ai dati inseriti.

Aggiorna Log Streams

Per aggiornare l'elenco corrente dei flussi di log visualizzati nella finestra del documento, scegliete il pulsante dell'icona Aggiorna, situato nella barra degli strumenti, accanto alla barra di ricerca.

Copia Log Streams ARN

Per copiare l'ARN di un flusso di log specifico, completare i passaggi descritti di seguito.

1. Nella scheda Log Streams, nella finestra del documento, fate clic con il pulsante destro del mouse sul flusso di log da cui desiderate copiare un ARN.
2. Scegli l'opzione Copia ARN dal menu.
3. L'ARN è ora copiato negli appunti locali e pronto per essere incollato.

Scarica Log Streams

La funzione Export Log Stream scarica e archivia il flusso di log selezionato localmente, dove è possibile accedervi tramite strumenti e software personalizzati per un'ulteriore elaborazione.

1. Nella scheda Log Streams, nella finestra del documento, fate clic con il pulsante destro del mouse sul flusso di log che desiderate scaricare.
2. Scegliete Esporta log Stream per aprire la finestra di dialogo Esporta in un file di testo.
3. Scegliete la posizione in cui desiderate archiviare il file localmente e specificate un nome nel campo di testo fornito.
4. Conferma il download selezionando OK. Lo stato del download viene visualizzato nel Visual Studio Task Status Center

CloudWatch Registra eventi

Gli eventi di registro sono registrazioni di attività registrate dall'applicazione o dalla risorsa monitorata da CloudWatch.

Registra le azioni degli eventi

Gli eventi di registro vengono visualizzati sotto forma di tabella. Per impostazione predefinita, gli eventi vengono ordinati dall'evento più vecchio a quello più recente.

Le seguenti azioni sono associate agli eventi di registro in Visual Studio:

- Modalità Wrapped-text: puoi attivare o disattivare il testo avvolto facendo clic su un evento.
- Pulsante di avvolgimento del testo: situato nella`document window` **`toolbar`**, questo pulsante attiva e disattiva la disposizione del testo per tutte le voci.
- Copia i messaggi negli appunti: seleziona i messaggi che desideri copiare, quindi fai clic con il pulsante destro del mouse sulla selezione e scegli Copia (scorciatoia da tastiera). `Ctrl + C`

Visualizzazione degli eventi del registro

1. Dalla finestra del documento, scegliete una scheda che contiene un elenco di flussi di log.
2. Fate doppio clic su un flusso di registro o fate clic con il pulsante destro del mouse su un flusso di registro e selezionate Visualizza flusso di registro dal menu.
3. Nella finestra del documento si aprirà una nuova scheda degli eventi di registro, che contiene una tabella degli eventi di registro associati al flusso di registro scelto.

Filtraggio degli eventi di registro

Esistono tre modi per filtrare gli eventi di registro: per contenuto, intervallo di tempo o entrambi. Per filtrare gli eventi di registro in base al contenuto e all'intervallo di tempo, inizia filtrando i messaggi in base al contenuto o all'intervallo di tempo, quindi filtra i risultati con l'altro metodo.

Per filtrare gli eventi di registro in base al contenuto:

1. Dalla scheda degli eventi di registro, nella finestra del documento, posiziona il cursore nella barra di ricerca, situata nella parte superiore della finestra.
2. Inizia a digitare un termine o una frase correlata agli eventi di registro che stai cercando.

3. Durante la digitazione, la visualizzazione corrente inizia automaticamente a filtrare gli eventi del registro.

> **Note**
>
> I modelli di filtro fanno distinzione tra maiuscole e minuscole. È possibile migliorare i risultati della ricerca racchiudendo termini e frasi esatti, con caratteri non alfanumerici tra virgolette doppie (*""*). Per informazioni più dettagliate sui modelli di filtro, consulta l'argomento Filtro e sintassi dei pattern nella CloudWatch guida di Amazon.

Per visualizzare gli eventi di registro generati in un intervallo di tempo specifico:

1. Dalla scheda degli eventi del registro, nella finestra del documento, scegliete il pulsante con l'icona Calendario, che si trova nella barra degli strumenti.
2. Utilizzando i campi forniti, specificate l'intervallo di tempo in cui desiderate effettuare la ricerca.
3. I risultati filtrati si aggiornano automaticamente quando si specificano i vincoli di data e ora.

> **Note**
>
> L'opzione Cancella filtro cancella tutte le selezioni dei filtri correnti. date-and-time

Aggiorna il registro degli eventi

Per aggiornare l'elenco corrente degli eventi di registro visualizzati nella scheda degli eventi di registro, scegliete il pulsante dell'icona Aggiorna, situato nella barra degli strumenti.

Accesso aggiuntivo ai registri CloudWatch

Puoi accedere ai CloudWatch log associati ad altri AWS servizi e risorse direttamente dal AWS Toolkit in Visual Studio.

Lambda

Per visualizzare i flussi di log associati a una funzione Lambda:

> **Note**
>
> Il ruolo di esecuzione Lambda deve disporre delle autorizzazioni appropriate per inviare i log ai registri. CloudWatch Per ulteriori informazioni sulle autorizzazioni Lambda richieste per i CloudWatch registri, consulta la https://docs.aws.amazon.com/lambda/latest/dg/monitoring-cloudwatchlogs.html#monitoring-cloudwatchlogs-prereqs

1. Da AWS Toolkit Explorer, espandi Lambda.
2. fate clic con il pulsante destro del mouse sulla funzione che desiderate visualizzare, quindi scegliete Visualizza registri per aprire i flussi di log associati nella finestra del documento.

Per visualizzare i flussi di log utilizzando l'integrazione `function view` Lambda:

1. Da AWS Toolkit Explorer, espandi Lambda.
2. fate clic con il pulsante destro del mouse sulla funzione che desiderate visualizzare, quindi scegliete Visualizza funzione per aprire la vista della funzione nella finestra del documento.
3. Dalla scheda Registri**`function view`**, vengono visualizzati i flussi di log associati alla funzione Lambda scelta.

ECS

Per visualizzare le risorse di registro associate a un Task Container ECS, completare la procedura seguente.

> **Note**
>
> Affinché il servizio Amazon ECS possa inviare i log CloudWatch, ogni contenitore per un determinato task Amazon ECS deve soddisfare la configurazione richiesta. Per ulteriori informazioni sulla configurazione e le configurazioni richieste, consulta la guida Using the Logs Log Driver. AWS

1. Da AWS Toolkit Explorer, espandi Amazon ECS.
2. Scegli il cluster Amazon ECS che desideri visualizzare per aprire una nuova scheda Cluster ECS, nella finestra del documento.

3. Dal menu di navigazione, situato sul lato sinistro della scheda ECS Cluster, scegli Attività per elencare tutte le attività associate al cluster.
4. Dalla schermata Attività, seleziona un'attività e scegli il link Visualizza registri, situato nell'angolo in basso a sinistra.

> **Note**
>
> Questa visualizzazione elenca tutte le attività contenute nel cluster, il `View Logs` collegamento è visibile solo per ogni attività che soddisfa la configurazione dei log richiesta.
>
> - Se un'attività è associata solo a un singolo contenitore, il link Visualizza registri apre il flusso di log di quel contenitore.
> - Se un'attività è associata a più contenitori, il link Visualizza registri apre la finestra di dialogo Visualizza CloudWatch registri per attività ECS, utilizza il menu a discesa Contenitore: per scegliere il contenitore per cui desideri visualizzare i registri, quindi scegli OK.

5. Nella finestra del documento si apre una nuova scheda che mostra i flussi di log associati alla selezione del contenitore.

Gestione delle istanze Amazon EC2

AWS Explorer fornisce viste dettagliate delle istanze Amazon Machine Images (AMI) e Amazon Elastic Compute Cloud (Amazon EC2). Da queste visualizzazioni, puoi avviare un'istanza Amazon EC2 da un'AMI, connetterti a quell'istanza e interrompere o terminare l'istanza, il tutto dall'interno dell'ambiente di sviluppo di Visual Studio. Puoi usare la visualizzazione delle istanze per creare a AMIs partire dalle tue istanze. Per ulteriori informazioni, consulta Creare un'AMI da un'istanza Amazon EC2.

Visualizzazioni delle immagini delle macchine Amazon e delle istanze Amazon EC2

Da AWS Explorer, puoi visualizzare le visualizzazioni delle AMI (Amazon Machine Images) e delle istanze Amazon EC2. In AWS Explorer, espandi il nodo Amazon EC2.

Per visualizzare la AMIs vista, nel primo sottonodo AMIs, apri il menu contestuale (fai clic con il pulsante destro del mouse) e scegli Visualizza.

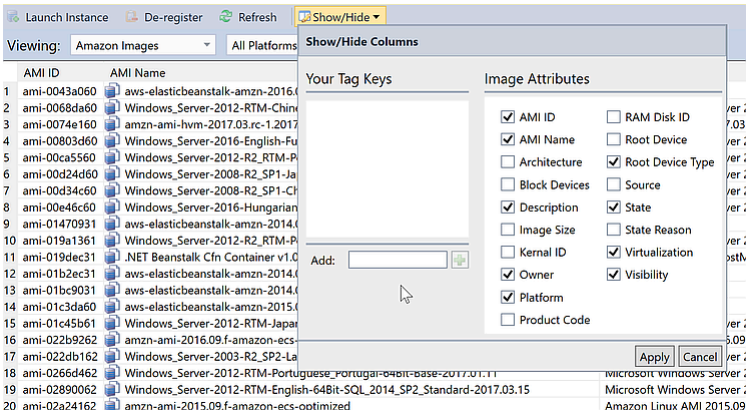
Per visualizzare la visualizzazione delle istanze Amazon EC2, nel nodo Istanze, apri il menu contestuale (fai clic con il pulsante destro del mouse) e scegli Visualizza.

Puoi anche visualizzare entrambe le viste facendo doppio clic sul nodo appropriato.

- Le visualizzazioni si riferiscono alla regione specificata in AWS Explorer (ad esempio, la regione Stati Uniti occidentali (California settentrionale)).
- È possibile ridisporre le colonne facendo clic e trascinando. Per ordinare i valori in una colonna, fate clic sull'intestazione della colonna.
- È possibile utilizzare gli elenchi a discesa e la casella di filtro in Visualizzazione per configurare le visualizzazioni. La visualizzazione iniziale mostra qualsiasi tipo AMIs di piattaforma (Windows o Linux) di proprietà dell'account specificato in AWS Explorer.

Mostra/nascondi colonne

Puoi anche scegliere il menu a discesa Mostra/Nascondi nella parte superiore della vista per configurare quali colonne visualizzare. La scelta delle colonne rimarrà invariata se chiudi la vista e la riapri.



Mostra/nascondi l'interfaccia utente delle colonne per le visualizzazioni AMI e istanze

Etichettatura AMIs, istanze e volumi

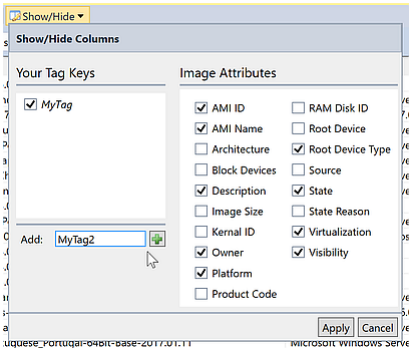
Puoi anche utilizzare l'elenco a discesa Mostra/Nascondi per aggiungere tag per AMI, istanze Amazon EC2 o volumi di tua proprietà. I tag sono coppie nome-valore che ti consentono di allegare metadati alle tue istanze e ai tuoi volumi. AMIs I nomi dei tag si riferiscono sia al tuo account che separatamente alle tue istanze. AMIs Ad esempio, non ci sarebbero conflitti se utilizzassi lo stesso

nome di tag per la tua istanza AMIs e quella per le tue. I nomi dei tag non fanno distinzione tra maiuscole e minuscole.

Per ulteriori informazioni sui tag, consulta Using Tags nella Amazon EC2 User Guide for Linux Instances.

Per aggiungere un tag

1. Nella casella Aggiungi, digita un nome per il tag. Scegli il pulsante verde con il segno più (+), quindi scegli Applica.



   Aggiungi un tag a un'istanza AMI o Amazon EC2

   Il nuovo tag viene visualizzato in corsivo, il che indica che nessun valore è stato ancora associato a quel tag.

   Nella visualizzazione a elenco, il nome del tag appare come una nuova colonna. Quando almeno un valore è stato associato al tag, il tag sarà visibile in Console di gestione AWS.
2. Per aggiungere un valore per il tag, fate doppio clic su una cella nella colonna relativa al tag e digitate un valore. Per eliminare il valore del tag, fate doppio clic sulla cella ed eliminate il testo.

   Se si cancella il tag nell'elenco a discesa Mostra/Nascondi, la colonna corrispondente scompare dalla visualizzazione. Il tag viene mantenuto, insieme a tutti i valori dei tag associati a AMIs, istanze o volumi.

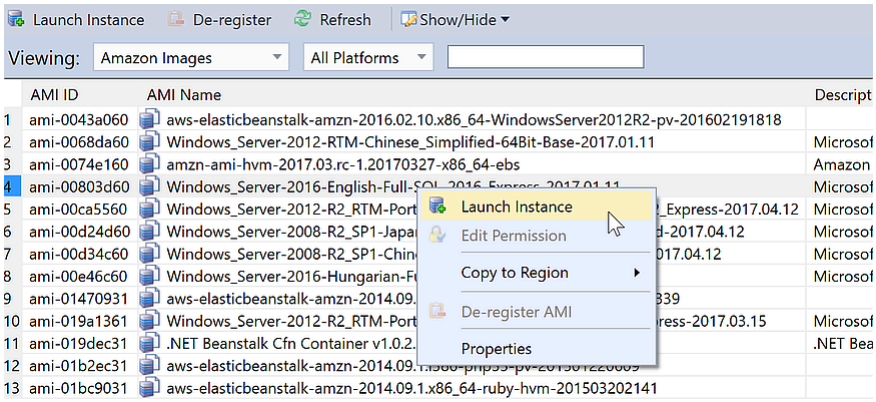
> **Note**
>
> Se si cancella un tag dall'elenco a discesa Mostra/Nascondi che non ha valori associati, il AWS Toolkit eliminerà completamente il tag. Non verrà più visualizzato nella visualizzazione a elenco o nell'elenco a discesa Mostra/Nascondi. Per utilizzare nuovamente quel tag, utilizzate la finestra di dialogo Mostra/Nascondi per ricrearlo.

Avvio di un'istanza Amazon EC2

AWS Explorer fornisce tutte le funzionalità necessarie per avviare un'istanza Amazon EC2. In questa sezione, selezioneremo un'Amazon Machine Image (AMI), la configureremo e la avvieremo come istanza Amazon EC2.

Per avviare un'istanza Amazon EC2 per Windows Server

1. Nella parte superiore della AMIs visualizzazione, nell'elenco a discesa a sinistra, scegli Amazon Images. Nell'elenco a discesa a destra, scegli Windows. Nella casella del filtro, digita `ebs` Elastic Block Storage. L'aggiornamento della visualizzazione potrebbe richiedere alcuni istanti.
2. Scegli un AMI nell'elenco, apri il menu contestuale (fai clic con il pulsante destro del mouse), quindi scegli Launch Instance.



Elenco AMI

3. Nella finestra di dialogo Launch New Amazon EC2 Instance, configura l'AMI per la tua applicazione.

   Tipo di istanza

   Scegli il tipo di istanza EC2 da avviare. Puoi trovare un elenco dei tipi di istanza e informazioni sui prezzi nella pagina dei Prezzi EC2.

   Nome

   Digita un nome per l'istanza. Questo nome non può contenere più di 256 caratteri.

   Coppia di chiavi

   Una key pair viene utilizzata per ottenere la password di Windows utilizzata per accedere all'istanza EC2 utilizzando Remote Desktop Protocol (RDP). Scegli una coppia di chiavi per la

quale hai accesso alla chiave privata o scegli l'opzione per creare una coppia di chiavi. Se crei la coppia di chiavi nel Toolkit, il Toolkit può memorizzare la chiave privata per te.

Le coppie di chiavi memorizzate nel Toolkit sono criptate. Le puoi trovare in (in genere:). `%LOCALAPPDATA%\AWSToolkit\keypairs` `C:\Users\<user>\AppData\Local\AWSToolkit\keypairs` È possibile esportare la coppia di chiavi crittografata in un `.pem` file.

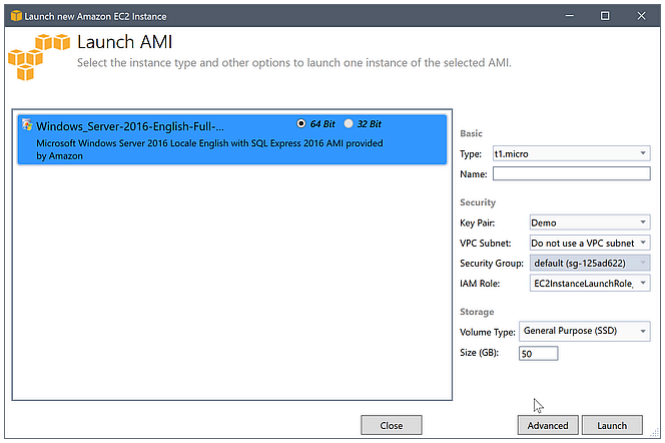
a. In Visual Studio, seleziona Visualizza e fai clic su AWS Explorer.
b. Fai clic su Amazon EC2 e seleziona Key Pairs.
c. Le coppie di chiavi verranno elencate e quelle created/managed del Toolkit contrassegnate come Archiviate in. AWSToolkit
d. Fai clic con il pulsante destro del mouse sulla coppia di chiavi che hai creato e seleziona Esporta chiave privata. La chiave privata non verrà crittografata e archiviata nella posizione specificata.

Gruppo di sicurezza

Il gruppo di sicurezza controlla il tipo di traffico di rete che l'istanza EC2 accetterà. Scegli un gruppo di sicurezza che consenta il traffico in entrata sulla porta 3389, la porta utilizzata da RDP, in modo da poterti connettere all'istanza EC2. Per informazioni su come utilizzare il Toolkit per creare gruppi di sicurezza, consulta Gestione dei gruppi di sicurezza da Explorer. AWS

Profilo dell'istanza

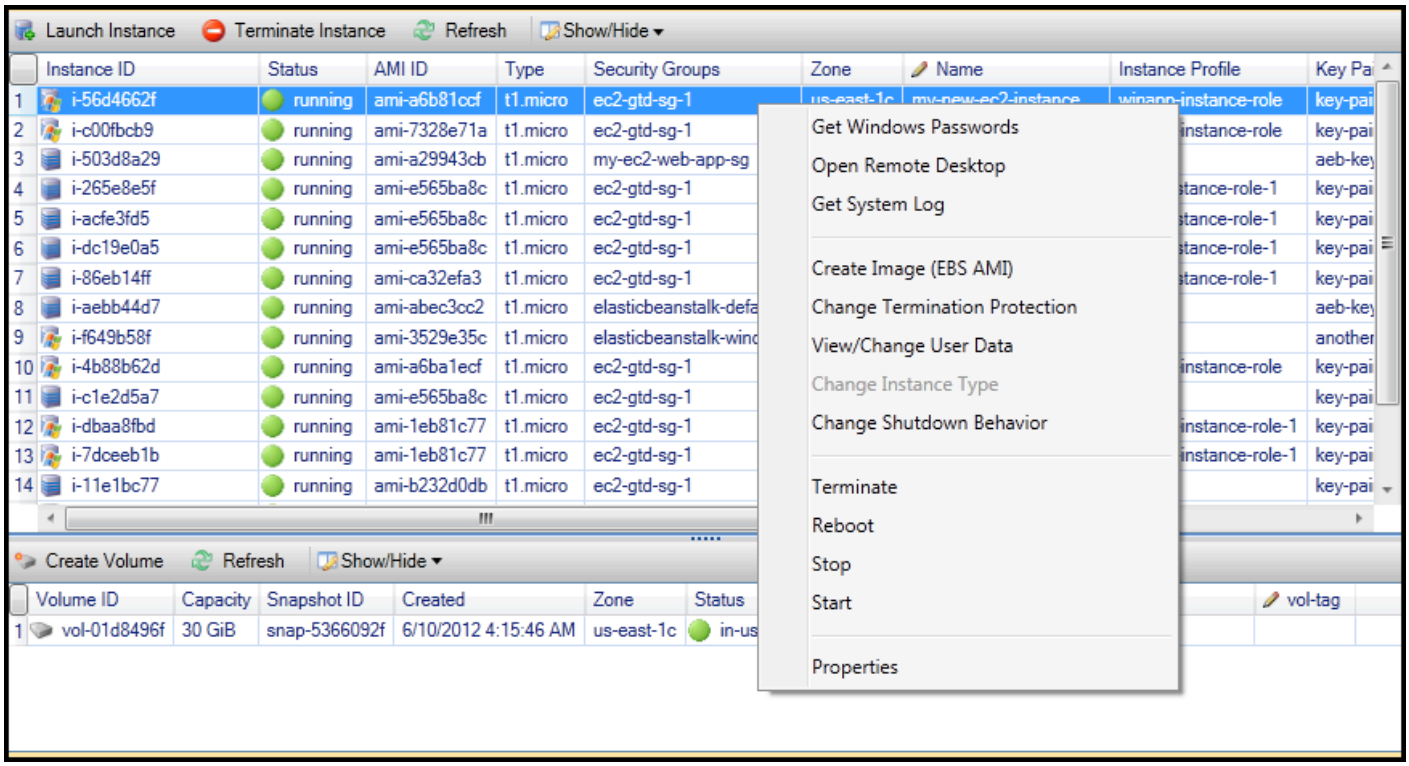
Il profilo dell'istanza è un container logico per un ruolo IAM. Quando scegli un profilo di istanza, associ il ruolo IAM corrispondente all'istanza EC2. I ruoli IAM sono configurati con policy che specificano l'accesso ad Amazon Web Services e alle risorse dell'account. Quando un'istanza EC2 è associata a un ruolo IAM, il software dell'applicazione eseguito sull'istanza viene eseguito con le autorizzazioni specificate dal ruolo IAM. Ciò consente al software applicativo di funzionare senza dover specificare alcuna AWS credenziale propria, il che rende il software più sicuro. Per ulteriori informazioni sui ruoli IAM, consulta la IAM User Guide.



Finestra di dialogo EC2 Launch AMI

4. Scegli Avvia.

In AWS Explorer, nel sottonodo Istanze di Amazon EC2, apri il menu contestuale (fai clic con il pulsante destro del mouse) e scegli Visualizza. Il AWS Toolkit visualizza l'elenco delle istanze Amazon EC2 associate all'account attivo. Potrebbe essere necessario scegliere Aggiorna per visualizzare la nuova istanza. Quando l'istanza viene visualizzata per la prima volta, potrebbe trovarsi in uno stato in sospeso, ma dopo alcuni istanti passa allo stato di esecuzione.



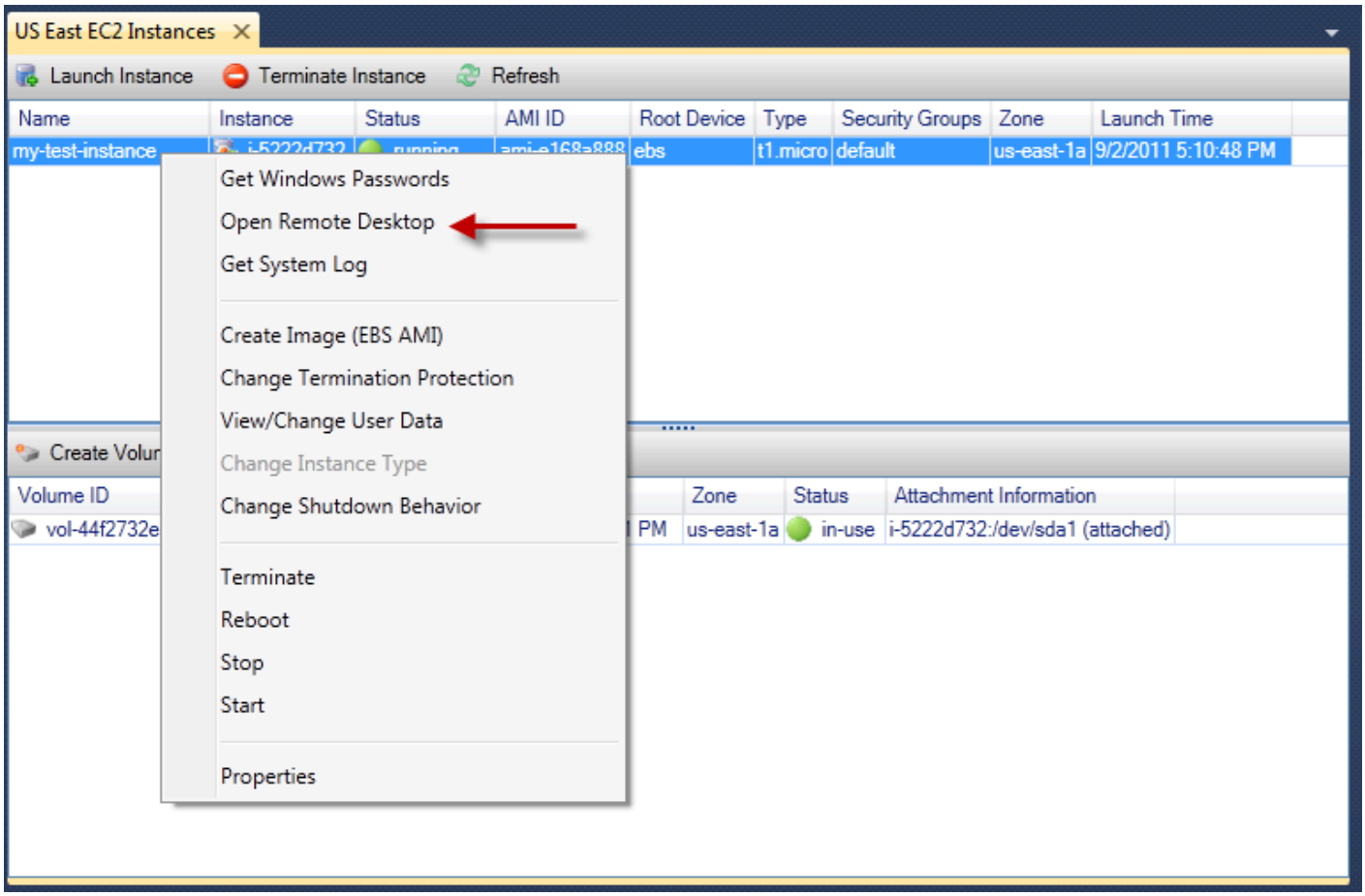
Connessione a un'istanza Amazon EC2

Puoi usare Windows Remote Desktop per connetterti a un'istanza di Windows Server. Per l'autenticazione, il AWS Toolkit consente di recuperare la password dell'amministratore per l'istanza oppure è possibile utilizzare semplicemente la coppia di chiavi memorizzata associata all'istanza. Nella procedura seguente, useremo la key pair memorizzata.

Per connettersi a un'istanza di Windows Server utilizzando Windows Remote Desktop

1. Nell'elenco delle istanze EC2, fai clic con il pulsante destro del mouse sull'istanza di Windows Server a cui desideri connetterti. Dal menu contestuale, scegli Apri desktop remoto.

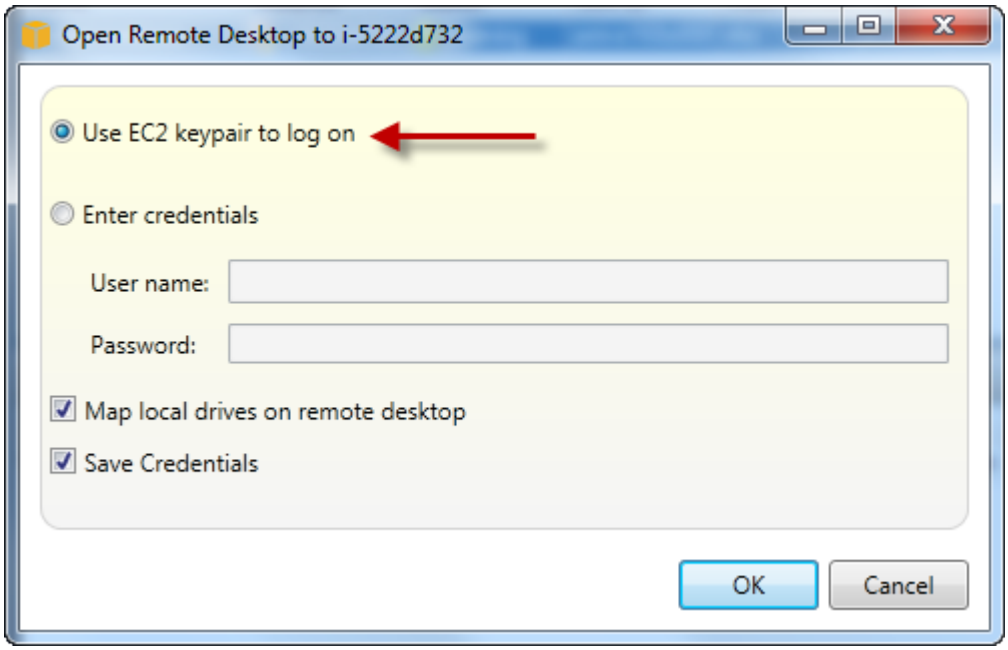
   Se desideri autenticarti utilizzando la password dell'amministratore, scegli Ottieni password di Windows.



   Menu contestuale dell'istanza EC2

2. Nella finestra di dialogo Open Remote Desktop, scegli Usa la coppia di chiavi EC2 per accedere, quindi scegli OK.

Se non hai memorizzato una coppia di chiavi con il AWS Toolkit, specifica il file PEM che contiene la chiave privata.

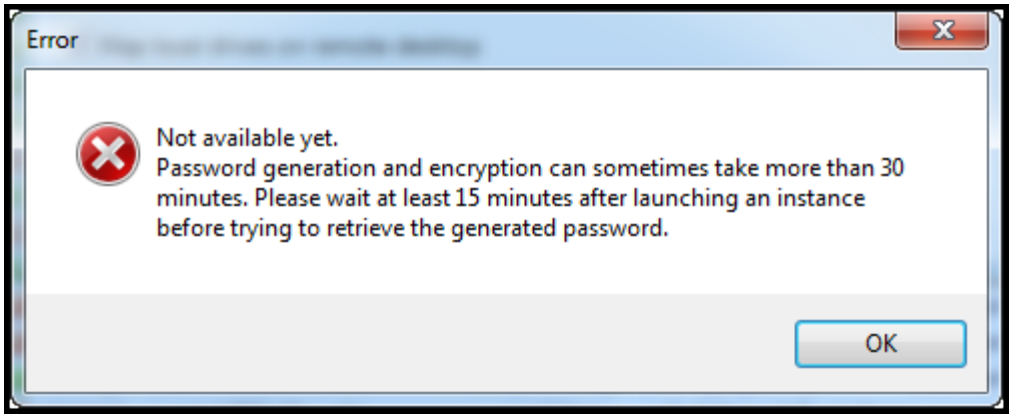


Apri la finestra di dialogo Desktop remoto

3. Si aprirà la finestra Remote Desktop. Non è necessario effettuare l'accesso perché l'autenticazione è avvenuta con la key pair. Eseguirai il ruolo di amministratore sull'istanza Amazon EC2.

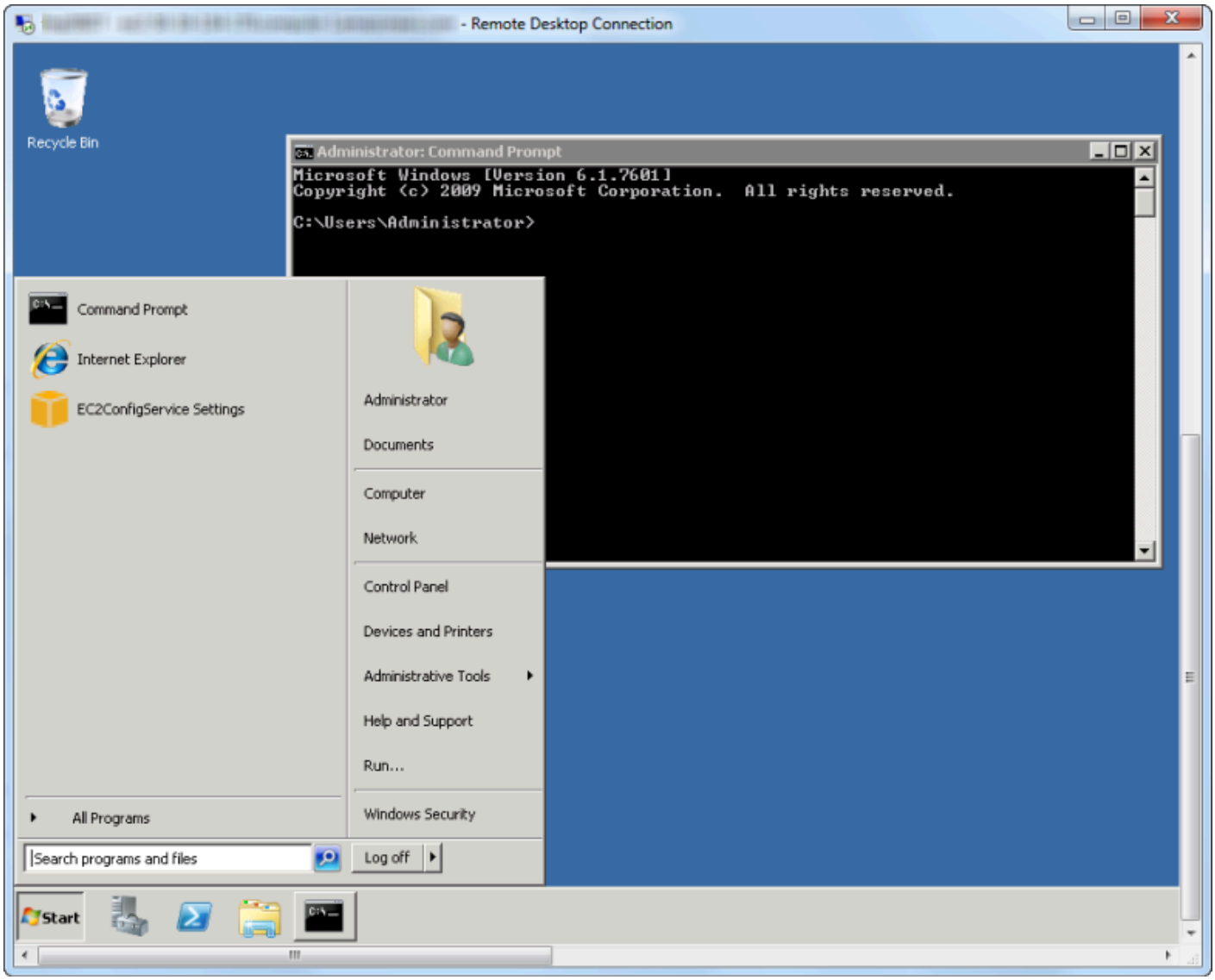
   Se l'istanza EC2 è stata avviata solo di recente, potresti non essere in grado di connetterti per due possibili motivi:

   - Il servizio Remote Desktop potrebbe non essere ancora attivo e funzionante. Attendere qualche minuto e riprovare.
   - Le informazioni sulla password potrebbero non essere ancora state trasferite all'istanza. In questo caso, verrà visualizzata una finestra di messaggio simile alla seguente.



Password non ancora disponibile

La schermata seguente mostra un utente connesso come amministratore tramite Remote Desktop.



Remote Desktop (Desktop remoto)

Terminare un'istanza Amazon EC2

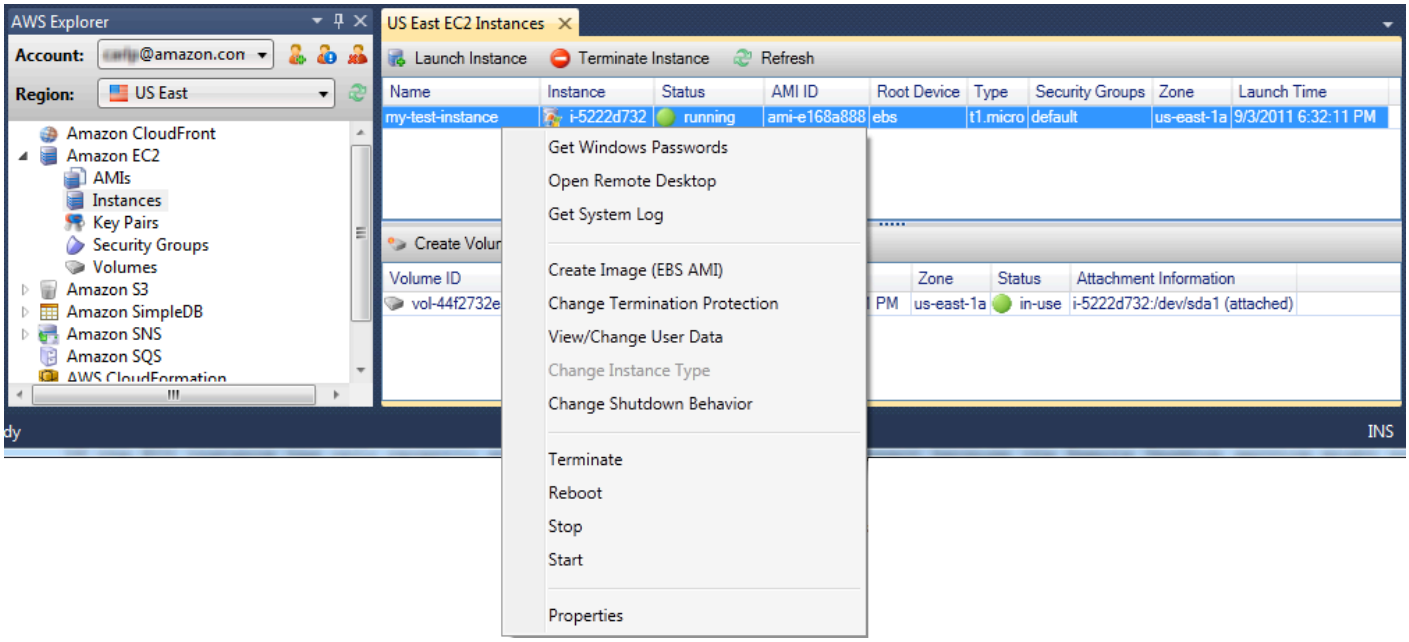
Utilizzando il AWS Toolkit, puoi interrompere o terminare un'istanza Amazon EC2 in esecuzione da Visual Studio. Per interrompere l'istanza, l'istanza EC2 deve utilizzare un volume Amazon EBS. Se l'istanza EC2 non utilizza un volume Amazon EBS, l'unica opzione è terminare l'istanza.

Se interrompi l'istanza, i dati archiviati nel volume EBS vengono conservati. Se si interrompe l'istanza, tutti i dati memorizzati sul dispositivo di archiviazione locale dell'istanza andranno persi. In entrambi i casi, che si tratti di interruzione o chiusura, non ti verrà addebitato alcun costo per l'istanza EC2. Tuttavia, se interrompi un'istanza, continuerai a ricevere addebiti per lo storage EBS che persiste dopo l'interruzione dell'istanza.

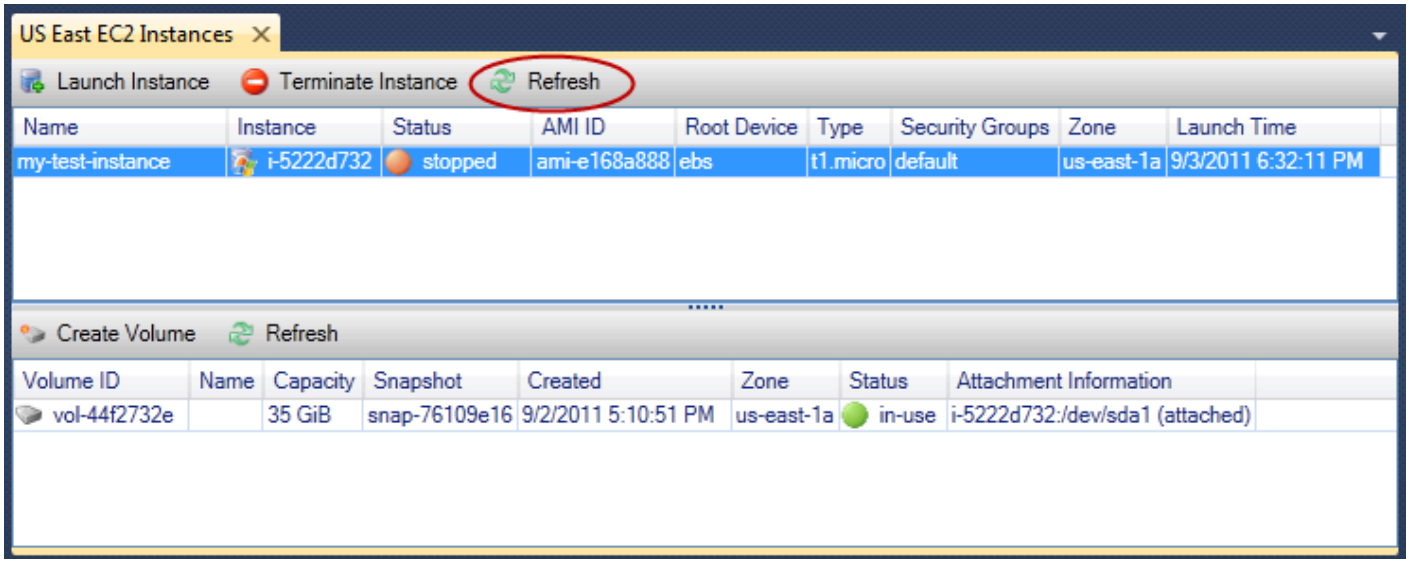
Un altro modo possibile per terminare un'istanza è utilizzare Remote Desktop per connettersi all'istanza e quindi, dal menu Start di Windows, utilizzare Shutdown. In questo scenario è possibile configurare l'istanza in modo che si interrompa o si chiuda.

Per interrompere un'istanza Amazon EC2

1. In AWS Explorer, espandi il nodo Amazon EC2, apri il menu contestuale (fai clic con il pulsante destro del mouse) per Istanze, quindi scegli Visualizza. Nell'elenco delle istanze, fai clic con il pulsante destro del mouse sull'istanza che desideri interrompere e scegli Stop dal menu contestuale. Scegli Sì per confermare che desideri interrompere l'istanza.

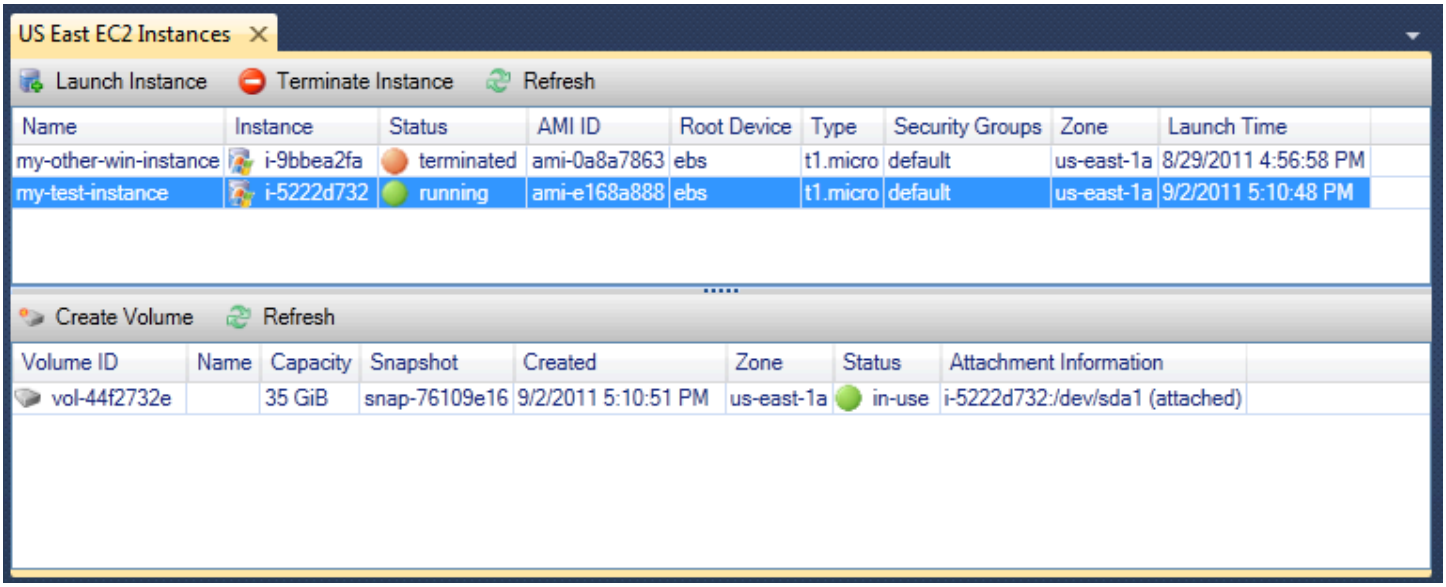


2. Nella parte superiore dell'elenco delle istanze, scegli Aggiorna per visualizzare la modifica dello stato dell'istanza Amazon EC2. Poiché l'istanza è stata interrotta anziché terminata, il volume EBS associato all'istanza è ancora attivo.



Le istanze terminate rimangono visibili

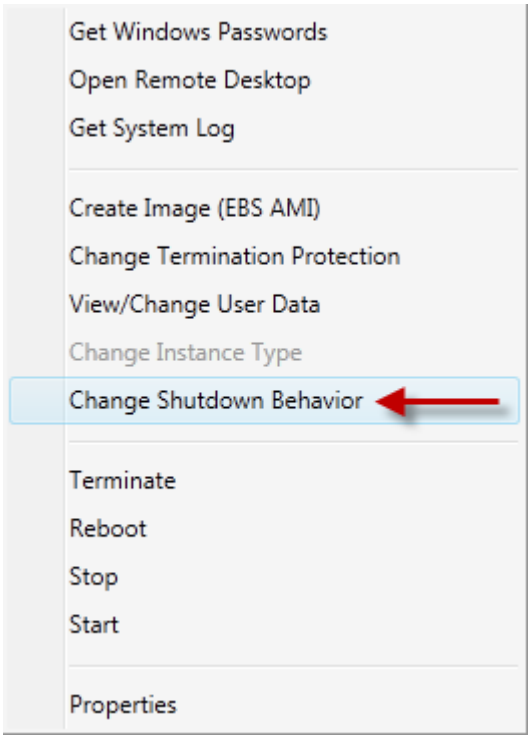
Se si interrompe un'istanza, questa continuerà a comparire nell'elenco delle istanze in esecuzione o interrotte. Alla fine, AWS recupera queste istanze e queste scompaiono dall'elenco. Non ti viene addebitato alcun costo per le istanze terminate.



Per specificare il comportamento di un'istanza EC2 all'arresto

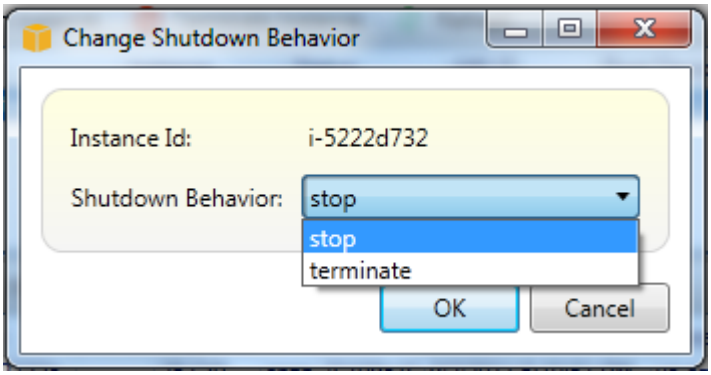
Il AWS Toolkit consente di specificare se un'istanza Amazon EC2 verrà interrotta o terminata se si seleziona Shutdown dal menu Start.

1. Nell'elenco Istanze, fai clic con il pulsante destro del mouse su un'istanza Amazon EC2, quindi scegli Modifica comportamento di chiusura.



Modifica la voce del menu Shutdown Behavior

2. Nella finestra di dialogo Modifica comportamento di spegnimento, dall'elenco a discesa Shutdown Behaviour, scegliete Arresta o Termina.



Gestione delle istanze Amazon ECS

AWS Explorer fornisce viste dettagliate dei cluster e dei repository di container di Amazon Elastic Container Service (Amazon ECS). Puoi creare, eliminare e gestire i dettagli di cluster e container dall'interno dell'ambiente di sviluppo di Visual Studio.

Modifica delle proprietà del servizio

È possibile visualizzare i dettagli del servizio, gli eventi e le proprietà del servizio dalla visualizzazione del cluster.

1. In AWS Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) per il cluster da gestire, quindi scegli Visualizza.
2. Nella vista Cluster ECS, fai clic su Servizi a sinistra, quindi fai clic sulla scheda Dettagli nella visualizzazione dei dettagli. Puoi fare clic su Eventi per visualizzare i messaggi relativi agli eventi e su Distribuzioni per visualizzare lo stato della distribuzione.
3. Fare clic su Edit (Modifica). È possibile modificare il numero di attività desiderato e la percentuale di integrità minima e massima.
4. Fate clic su Salva per accettare le modifiche o su Annulla per ripristinare i valori esistenti.

Interruzione di un'attività

È possibile visualizzare lo stato corrente delle attività e interrompere una o più attività nella visualizzazione cluster.

Come arrestare un'attività

1. In AWS Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) per il cluster con le attività che desideri interrompere, quindi scegli Visualizza.
2. Nella vista Cluster ECS, fai clic su Attività a sinistra.
3. Assicurati che Desired Task Status sia impostato su. `Running` Scegliete le singole attività da interrompere, quindi fate clic su Interrompi o su Arresta tutto per selezionare e interrompere tutte le attività in esecuzione.
4. Nella finestra di dialogo Interrompi attività, scegli Sì.

Eliminazione di un servizio

È possibile eliminare i servizi da un cluster dalla visualizzazione del cluster.

Per eliminare un servizio cluster

1. In AWS Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) per il cluster con un servizio che desideri eliminare, quindi scegli Visualizza.

2. Nella visualizzazione Cluster ECS, fai clic su Servizi a sinistra, quindi su Elimina.
3. Nella finestra di dialogo Elimina cluster, se nel cluster sono presenti un sistema di bilanciamento del carico e un gruppo target, puoi scegliere di eliminarli insieme al cluster. Non verranno utilizzati quando il servizio viene eliminato.
4. Nella finestra di dialogo Elimina cluster, scegliete OK. Quando il cluster viene eliminato, verrà rimosso da AWS Explorer.

Eliminazione di un cluster

Puoi eliminare un cluster Amazon Elastic Container Service da AWS Explorer.

Come eliminare un cluster

1. In AWS Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) per il cluster che desideri eliminare nel nodo Clusters di Amazon ECS, quindi scegli Elimina.
2. Nella finestra di dialogo Elimina cluster, scegli OK. Quando il cluster viene eliminato, verrà rimosso da AWS Explorer.

Creazione di un repository

Puoi creare un repository Amazon Elastic Container Registry da AWS Explorer.

Come creare un repository

1. In AWS Explorer, apri il menu contestuale (con il pulsante destro del mouse) del nodo Repositories in Amazon ECS, quindi scegli Create Repository.
2. Nella finestra di dialogo Crea repository, fornisci un nome per il repository, quindi scegli OK.

Eliminazione di un repository

Puoi eliminare un repository Amazon Elastic Container Registry da AWS Explorer.

Come eliminare un repository

1. In AWS Explorer, apri il menu contestuale (con il pulsante destro del mouse) del nodo Repositories in Amazon ECS, quindi scegli Delete Repository.

2. Nella finestra di dialogo Elimina repository, puoi scegliere di eliminare il repository anche se contiene immagini. Altrimenti, verrà eliminato solo se è vuoto. Fate clic su Sì.

Gestione dei gruppi di sicurezza da AWS Explorer

Il Toolkit for Visual Studio consente di creare e configurare gruppi di sicurezza da utilizzare con le istanze Amazon Elastic Compute Cloud (Amazon EC2) e. CloudFormation Quando avvii istanze Amazon EC2 o distribuisci un'applicazione CloudFormation, specifichi un gruppo di sicurezza da associare alle istanze Amazon EC2. (Implementazione per CloudFormation creare istanze Amazon EC2).

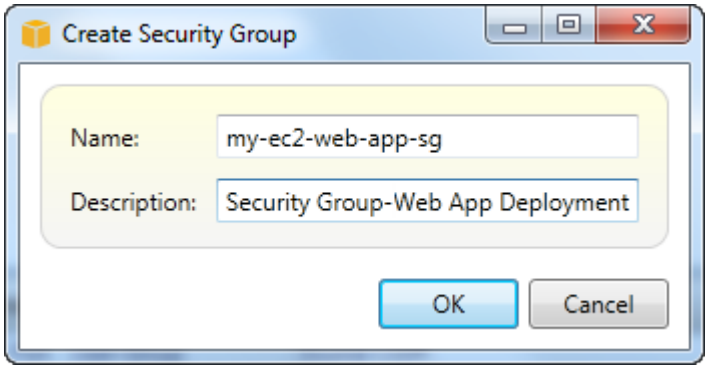
Un gruppo di sicurezza agisce come un firewall sul traffico di rete in entrata. Il gruppo di sicurezza specifica quali tipi di traffico di rete sono consentiti su un'istanza Amazon EC2. Può anche specificare che il traffico in entrata verrà accettato solo da determinati indirizzi IP o solo da utenti specifici o altri gruppi di sicurezza.

Creazione di un gruppo di sicurezza

In questa sezione, creeremo un gruppo di sicurezza. Dopo averlo creato, il gruppo di sicurezza non avrà alcuna autorizzazione configurata. La configurazione delle autorizzazioni viene gestita attraverso un'ulteriore operazione.

Per creare un gruppo di sicurezza

1. In AWS Explorer, sotto il nodo Amazon EC2, apri il menu contestuale (fai clic con il pulsante destro del mouse) sul nodo Security Groups, quindi scegli Visualizza.
2. Nella scheda Gruppi di sicurezza EC2, scegli Crea gruppo di sicurezza.
3. Nella finestra di dialogo Crea gruppo di sicurezza, digita un nome e una descrizione per il gruppo di sicurezza, quindi scegli OK.

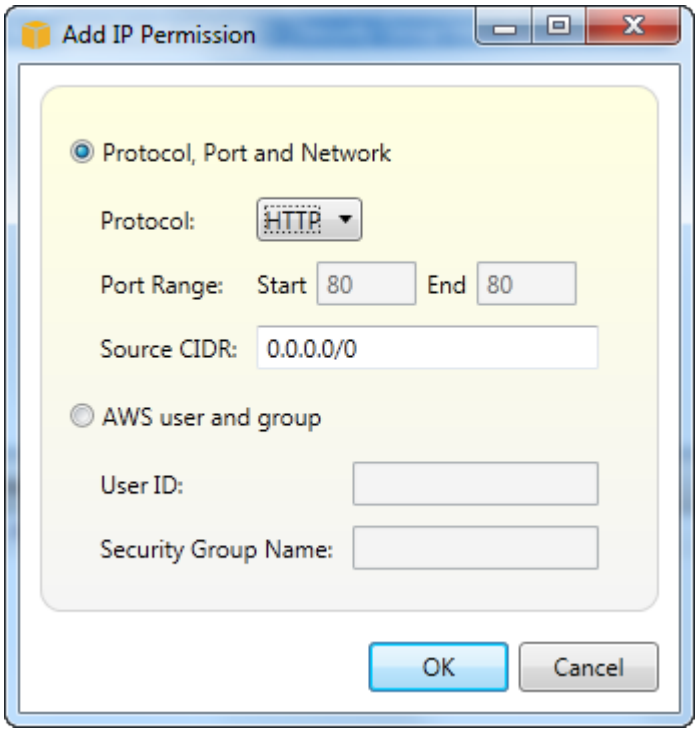


Aggiunta di autorizzazioni ai gruppi di sicurezza

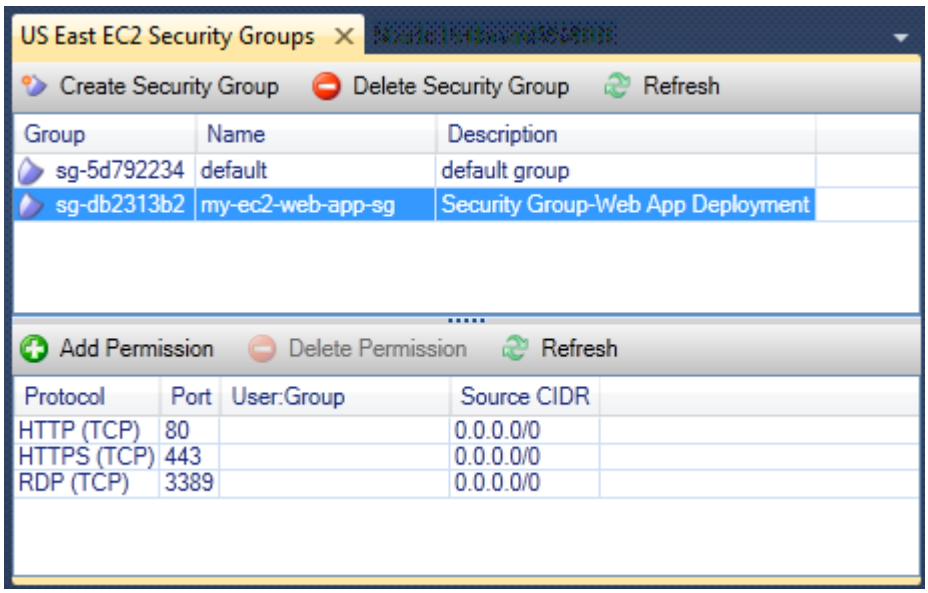
In questa sezione, aggiungeremo le autorizzazioni al gruppo di sicurezza per consentire il traffico web attraverso i protocolli HTTP e HTTPS. Consentiremo anche ad altri computer di connettersi utilizzando Windows Remote Desktop Protocol (RDP).

Per aggiungere autorizzazioni a un gruppo di sicurezza

1. Nella scheda Gruppi di sicurezza EC2, scegli un gruppo di sicurezza, quindi scegli il pulsante Aggiungi autorizzazione.
2. Nella finestra di dialogo Aggiungi autorizzazione IP, scegli il pulsante di opzione Protocollo, porta e rete, quindi dall'elenco a discesa Protocollo scegli HTTP. L'intervallo di porte si adatta automaticamente alla porta 80, la porta predefinita per HTTP. Il valore predefinito del campo Source CIDR è 0.0.0.0/0, che specifica che il traffico di rete HTTP verrà accettato da qualsiasi indirizzo IP esterno. Scegli OK.



   Apri la porta 80 (HTTP) per questo gruppo di sicurezza
3. Ripeti questo processo per HTTPS e RDP. Le autorizzazioni dei gruppi di sicurezza dovrebbero ora apparire come segue.



È inoltre possibile impostare le autorizzazioni nel gruppo di sicurezza specificando un ID utente e il nome del gruppo di sicurezza. In questo caso, le istanze Amazon EC2 in questo gruppo di sicurezza accetteranno tutto il traffico di rete in entrata dalle istanze Amazon EC2 nel gruppo di sicurezza specificato. È inoltre necessario specificare l'ID utente per disambiguare il nome del gruppo di sicurezza; non è necessario che i nomi dei gruppi di sicurezza siano univoci per tutti. AWS Per ulteriori informazioni sui gruppi di sicurezza, consulta la documentazione di EC2.

Creazione di un'AMI da un'istanza Amazon EC2

Puoi creare un'Amazon Machine Image (AMI) con AWS Toolkit for Visual Studio. Per informazioni più dettagliate AMIs, consulta l'argomento Amazon Machine Images (AMI) nella Guida per l'utente di Amazon Elastic Compute Cloud for Windows Instances.

Per creare un'AMI da un'istanza Amazon EC2 in uscita, completa la seguente procedura.

Creazione di un'AMI da un'istanza Amazon EC2 esistente

1. Da AWS Toolkit Explorer, espandi Amazon EC2 e scegli Istanze per visualizzare un elenco delle istanze esistenti.
2. Fate clic con il pulsante destro del mouse sull'istanza che desiderate utilizzare come base per l'AMI e scegliete Crea immagine (AMI ABS) per aprire la finestra di dialogo Crea immagine.
3. Dalla finestra di dialogo Crea immagine, aggiungi un nome e una descrizione per l'immagine nei campi forniti, quindi scegli il pulsante OK per continuare.

4. La finestra di conferma della creazione dell'immagine si apre in Visual Studio quando l'immagine viene creata, scegli il pulsante OK per continuare.

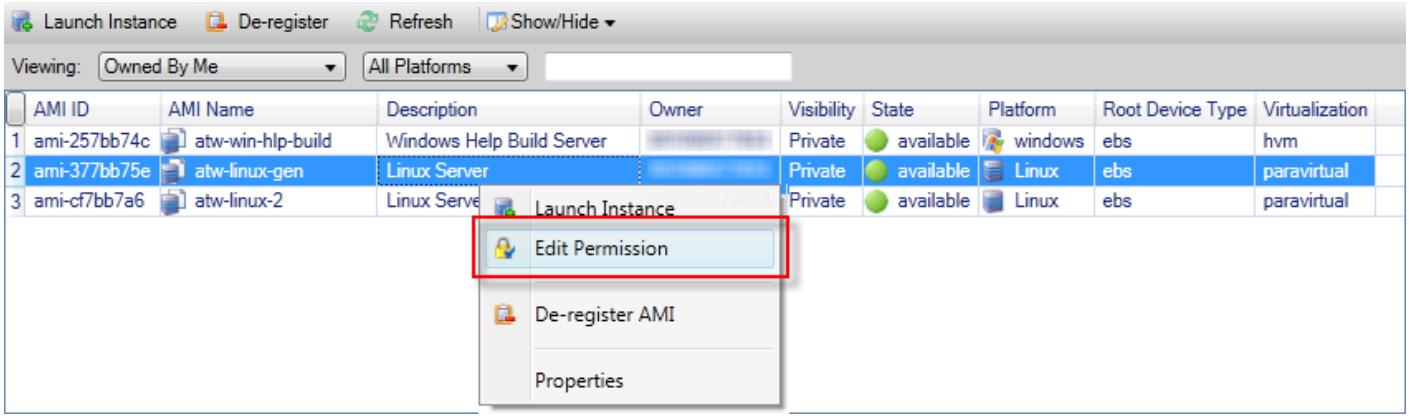
Per visualizzare la tua nuova AMI con il AWS Toolkit, espandi Amazon EC2 e AMIsfai doppio clic per aprire una finestra nel payne di Visual Studio Editor che mostra un elenco delle tue AMI esistenti. AMIs Se non vedi la tua nuova AMI nell'elenco, scegli il pulsante Aggiorna situato nella parte superiore della finestra AMI.

Impostazione delle autorizzazioni di avvio su un'immagine di macchina Amazon

Puoi impostare le autorizzazioni di avvio sulle tue Amazon Machine Images (AMIs) dalla AMIsvista in AWS Explorer. È possibile utilizzare la finestra di dialogo Imposta autorizzazioni AMI per copiare le autorizzazioni da. AMIs

Per impostare le autorizzazioni su un'AMI

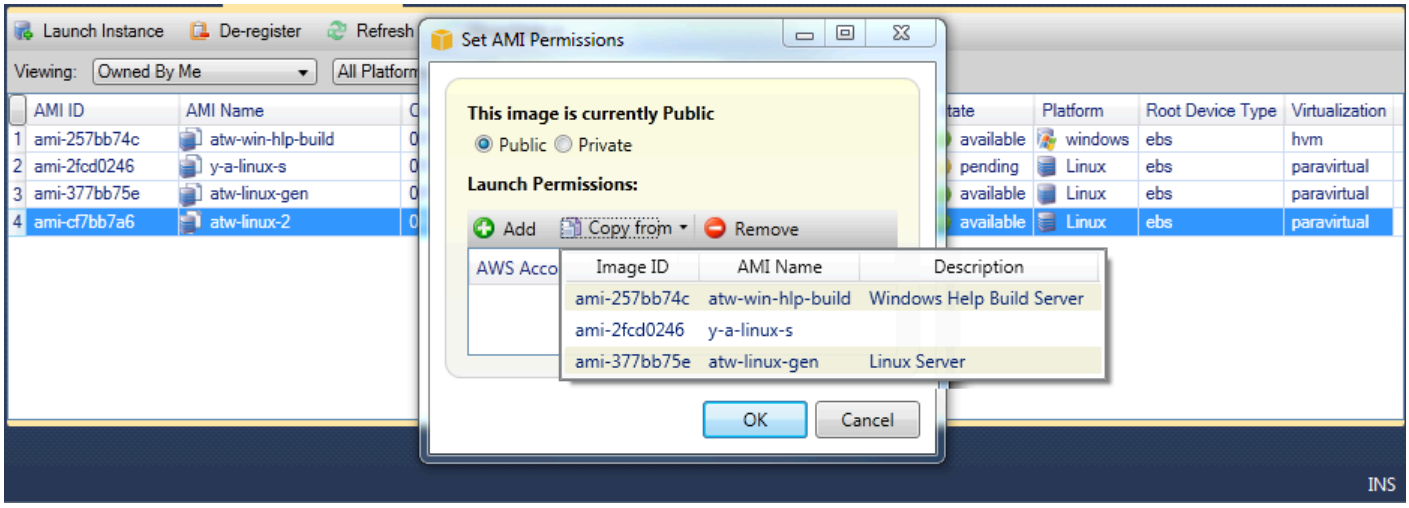
1. Nella AMIsvista in AWS Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) su un AMI, quindi scegli Modifica autorizzazione.



2. Nella finestra di dialogo Imposta autorizzazioni AMI sono disponibili tre opzioni:
   - Per concedere l'autorizzazione all'avvio, scegli Aggiungi e digita il numero di account dell' AWS utente a cui stai dando l'autorizzazione all'avvio.
   - Per rimuovere l'autorizzazione all'avvio, scegli il numero di account dell' AWS utente da cui stai rimuovendo l'autorizzazione all'avvio e scegli Rimuovi.
   - Per copiare le autorizzazioni da un'AMI all'altra, scegli un AMI dall'elenco e scegli Copia da. Agli utenti che dispongono delle autorizzazioni di avvio sull'AMI che hai scelto verranno concesse le

autorizzazioni di avvio sull'AMI corrente. Puoi ripetere questo processo con altri AMIs nell'elenco Copia da per copiare le autorizzazioni da più autorizzazioni AMIs all'AMI di destinazione.

L'elenco Copy-from contiene solo quelli di AMIs proprietà dell'account che era attivo quando la AMIsvisualizzazione veniva visualizzata da Explorer. AWS Di conseguenza, l'elenco Copy-from potrebbe non visualizzarne nessuno AMIs se nessun altro è di proprietà dell' AMIs account attivo.



Finestra di dialogo Copia autorizzazioni AMI

Amazon Cloud Privato Virtuale (VPC)

Amazon Virtual Private Cloud (Amazon VPC) ti consente di avviare le risorse di Amazon Web Services in una rete virtuale che hai definito. Questa rete virtuale è simile a una comune rete da gestire all'interno del proprio data center, ma con i vantaggi dell'infrastruttura scalabile di AWS. Per ulteriori informazioni, consulta la Amazon VPC User Guide.

Il Toolkit for Visual Studio consente a uno sviluppatore di accedere a funzionalità VPC simili a quelle esposte dal ma Console di gestione AWSdall'ambiente di sviluppo di Visual Studio. Il nodo Amazon VPC di AWS Explorer include sottonodi per le seguenti aree.

- VPCs
- Sottoreti
- Elastic IPs
- Internet Gateway
- Rete ACLs

- Tabelle di routing
- Gruppi di sicurezza

Creazione di un VPC pubblico-privato per l'implementazione con AWS Elastic Beanstalk

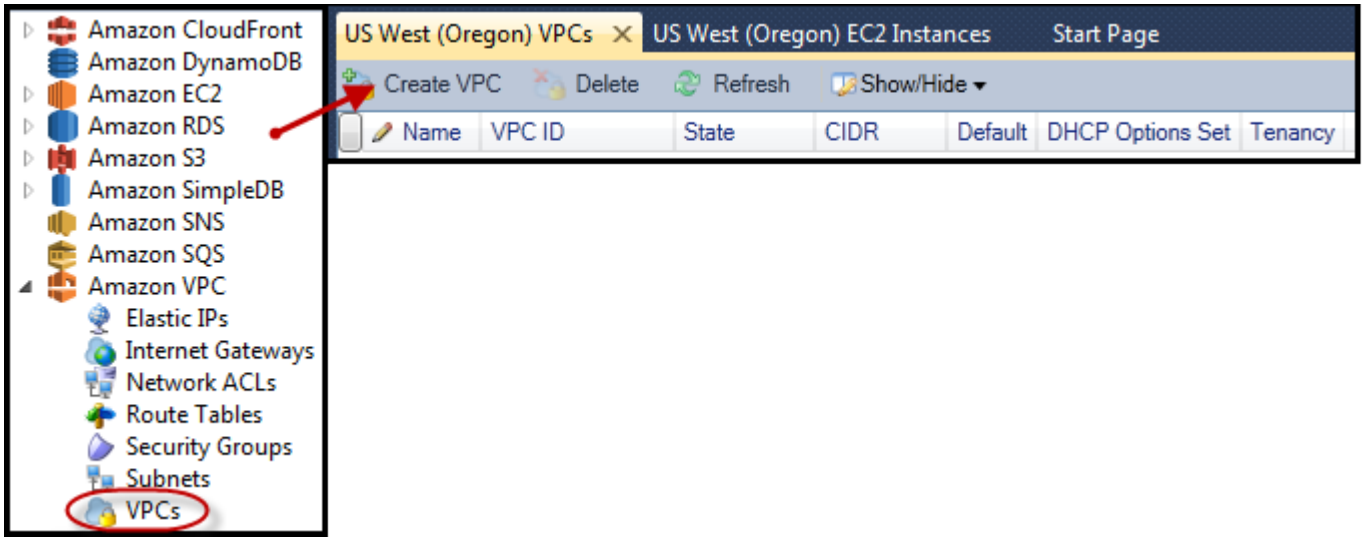
Questa sezione descrive come creare un Amazon VPC che contenga sottoreti pubbliche e private. La sottorete pubblica contiene un'istanza Amazon EC2 che esegue la traduzione degli indirizzi di rete (NAT) per consentire alle istanze nella sottorete privata di comunicare con la rete Internet pubblica. Le due sottoreti devono risiedere nella stessa zona di disponibilità (AZ).

Questa è la configurazione VPC minima richiesta per implementare un AWS Elastic Beanstalk ambiente in un VPC. In questo scenario, le istanze Amazon EC2 che ospitano l'applicazione risiedono nella sottorete privata; il sistema di bilanciamento del carico Elastic Load Balancing che indirizza il traffico in entrata verso l'applicazione risiede nella sottorete pubblica.

Per ulteriori informazioni sulla traduzione degli indirizzi di rete (NAT), consulta NAT Instances nella Amazon Virtual Private Cloud User Guide. Per un esempio di come configurare la distribuzione per l'utilizzo di un VPC, consulta Deploying to Elastic Beanstalk.

Per creare un VPC di sottorete pubblico-privato

1. Nel nodo Amazon VPC in AWS Explorer, apri il VPCssottonodo, quindi scegli Crea VPC.

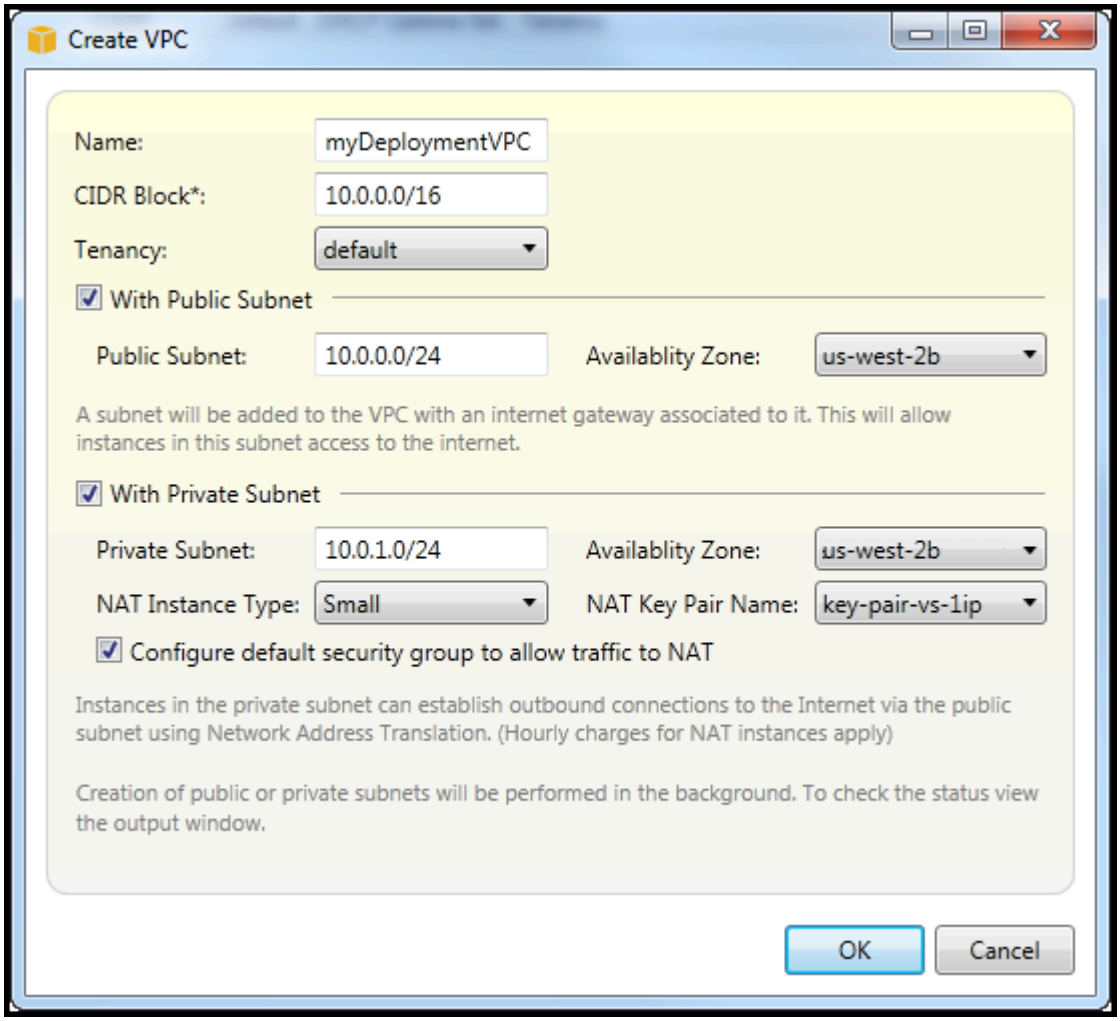


2. Configurare il VPC come segue:
   - Digita un nome per il tuo VPC.

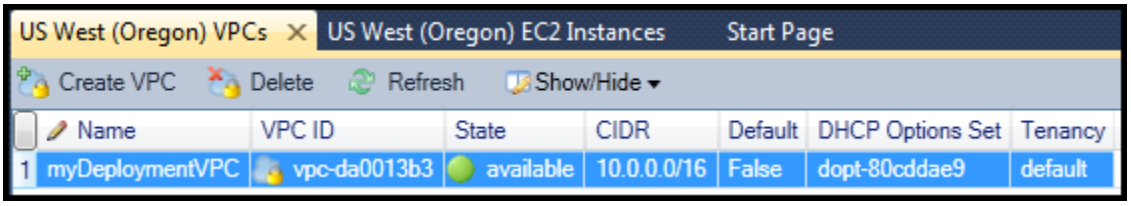
- Seleziona le caselle di controllo Con sottorete pubblica e Con sottorete privata.
- Dalla casella di riepilogo a discesa Zona di disponibilità per ogni sottorete, scegli una zona di disponibilità. Assicurati di utilizzare la stessa AZ per entrambe le sottoreti.
- Per la sottorete privata, in NAT Key Pair Name, fornire una coppia di chiavi. Questa coppia di chiavi viene utilizzata per l'istanza Amazon EC2 che esegue la traduzione degli indirizzi di rete dalla sottorete privata alla rete Internet pubblica.
- Seleziona la casella di controllo Configura il gruppo di sicurezza predefinito per consentire il traffico verso NAT.

Digita un nome per il tuo VPC. Seleziona le caselle di controllo Con sottorete pubblica e Con sottorete privata. Dalla casella di riepilogo a discesa Zona di disponibilità per ogni sottorete, scegli una zona di disponibilità. Assicurati di utilizzare la stessa AZ per entrambe le sottoreti. Per la sottorete privata, in NAT Key Pair Name, fornire una coppia di chiavi. Questa coppia di chiavi viene utilizzata per l'istanza Amazon EC2 che esegue la traduzione degli indirizzi di rete dalla sottorete privata alla rete Internet pubblica. Seleziona la casella di controllo Configura il gruppo di sicurezza predefinito per consentire il traffico verso NAT.

Scegli OK.

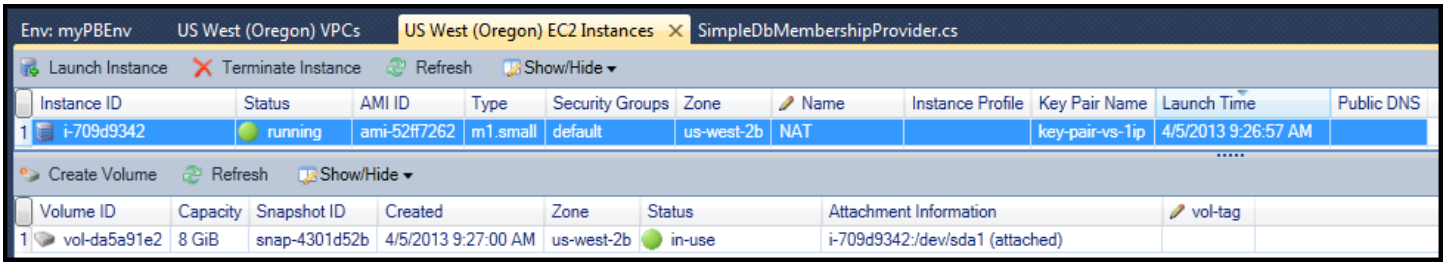


Puoi visualizzare il nuovo VPC nella VPCs AWS scheda di Explorer.



L'avvio dell'istanza NAT potrebbe richiedere alcuni minuti. Quando è disponibile, puoi visualizzarlo espandendo il nodo Amazon EC2 in AWS Explorer e quindi aprendo il sottonodo Instances.

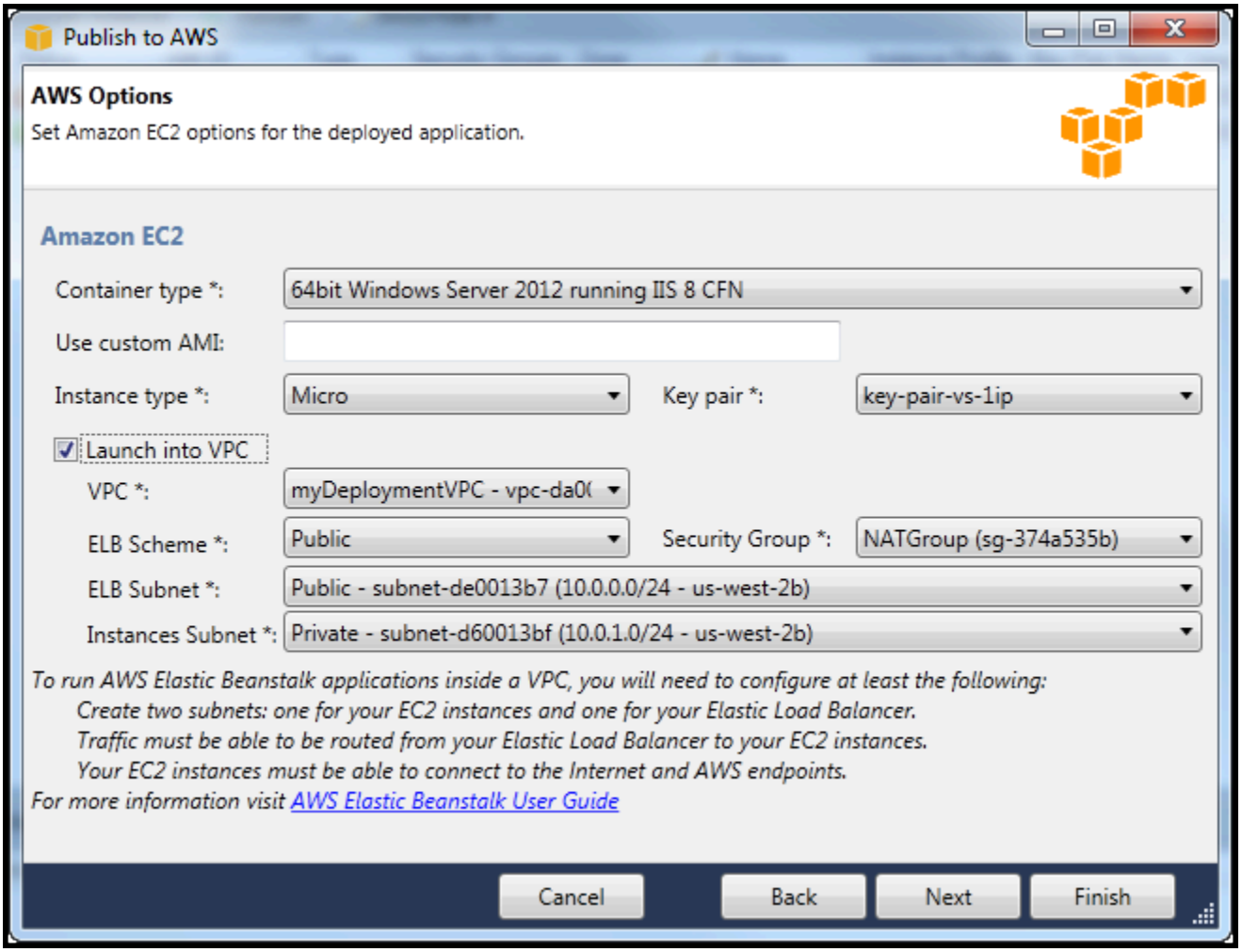
Un volume Amazon Elastic Block Store (Amazon EBS) Elastic Block Store (Amazon EBS) viene creato automaticamente per l'istanza NAT. Per ulteriori informazioni su Amazon EBS, consulta l'argomento Amazon Elastic Block Store (EBS) nella Amazon EC2 User Guide for Linux Instances.



Se distribuisci un'applicazione in un AWS Elastic Beanstalk ambiente e scegli di avviare l'ambiente in un VPC, il Toolkit popolerà la finestra di dialogo Pubblica su con le informazioni di Amazon Web Services configurazione per il tuo VPC.

Il Toolkit inserisce nella finestra di dialogo solo le informazioni VPCs che sono state create nel Toolkit, non quelle create utilizzando. VPCs Console di gestione AWS Questo perché quando il Toolkit crea un VPC, contrassegna i componenti del VPC in modo che possa accedere alle relative informazioni.

La seguente schermata della Deployment Wizard mostra un esempio di finestra di dialogo popolata con valori di un VPC creato nel Toolkit.



Come eliminare un VPC

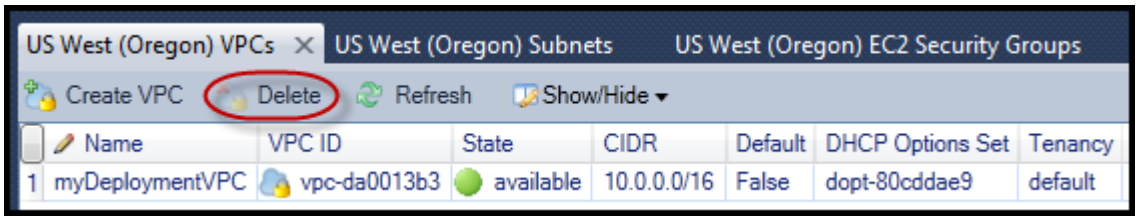
Per eliminare il VPC, devi prima terminare tutte le istanze Amazon EC2 nel VPC.

1. Se hai distribuito un'applicazione in un AWS Elastic Beanstalk ambiente nel VPC, elimina l'ambiente. Ciò interromperà tutte le istanze Amazon EC2 che ospitano l'applicazione insieme al sistema di bilanciamento del carico Elastic Load Balancing.

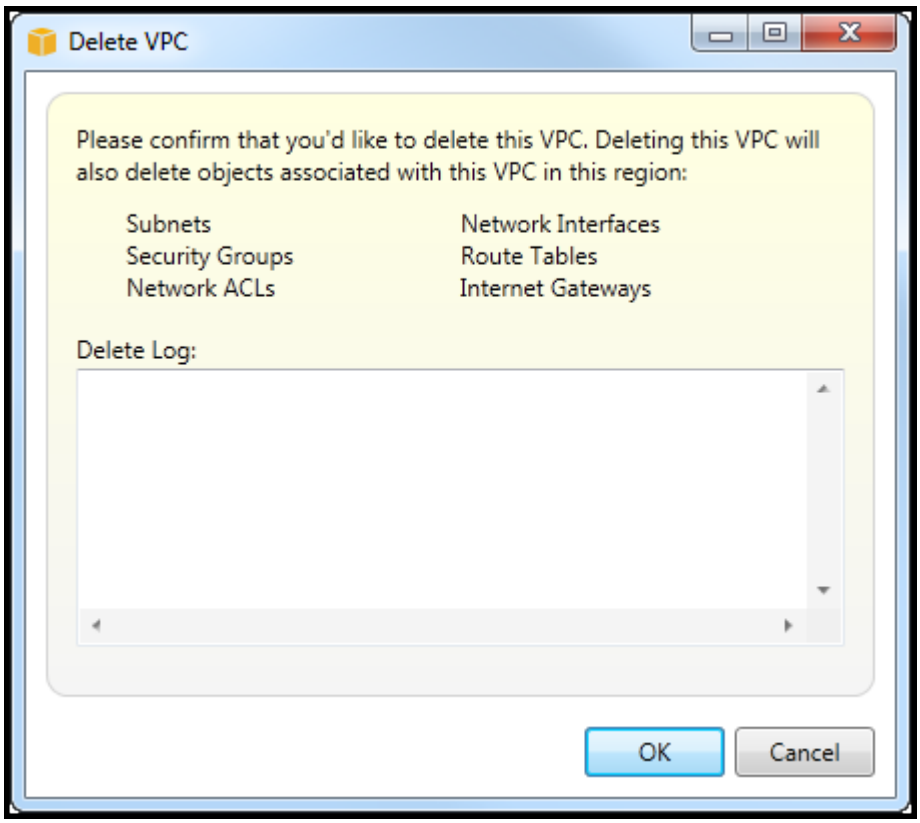
   Se si tenta di chiudere direttamente le istanze che ospitano l'applicazione senza eliminare l'ambiente, il servizio Auto Scaling creerà automaticamente nuove istanze per sostituire quelle eliminate. Per ulteriori informazioni, consulta la Guida per gli sviluppatori di Auto Scaling.
2. Eliminare l'istanza NAT per il VPC.

   Non è necessario eliminare il volume Amazon EBS associato all'istanza NAT per eliminare il VPC. Tuttavia, se non elimini il volume, ti verranno addebitati i costi anche se elimini l'istanza NAT e il VPC.

3. Nella scheda VPC, scegli il link Elimina per eliminare il VPC.



4. Nella finestra di dialogo Elimina VPC, scegli OK.



Utilizzo dell'editor CloudFormation di modelli per Visual Studio

Il Toolkit for Visual Studio include CloudFormation un editor di modelli CloudFormation e progetti modello per Visual Studio. Le funzionalità supportate includono:

- Creazione di nuovi modelli (vuoti o copiati da uno stack o modello di esempio esistente) utilizzando il tipo di progetto CloudFormation modello fornito.
- Modifica dei modelli con convalida JSON automatica, completamento automatico, piegatura del codice ed evidenziazione della sintassi.
- Suggerimento automatico di funzioni intrinseche e parametri di riferimento delle risorse per i valori dei campi nel modello.

- Voci di menu per eseguire azioni comuni per il modello di Visual Studio.

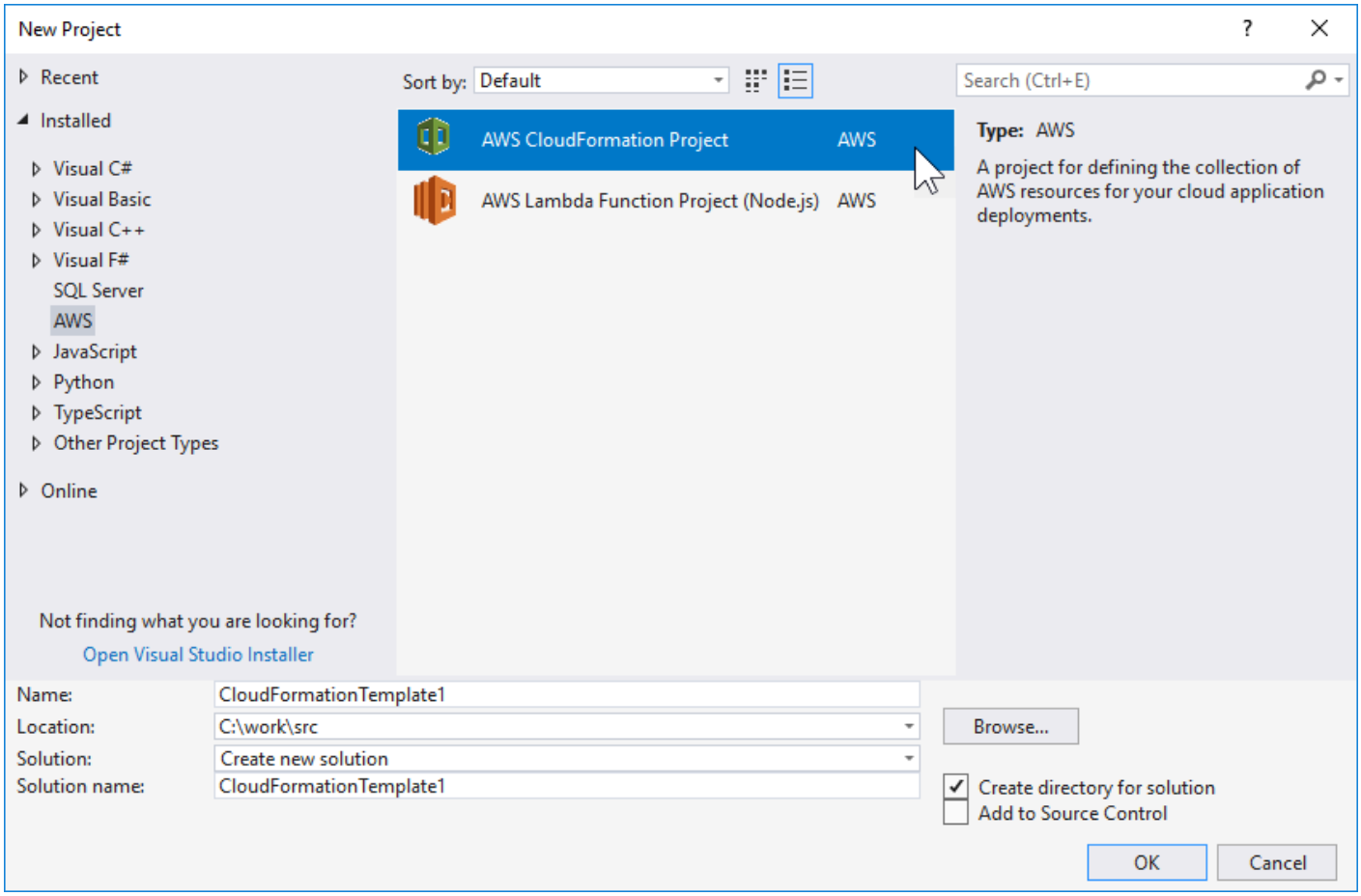
Argomenti

Creazione di un progetto CloudFormation modello in Visual Studio

Per creare un modello di progetto

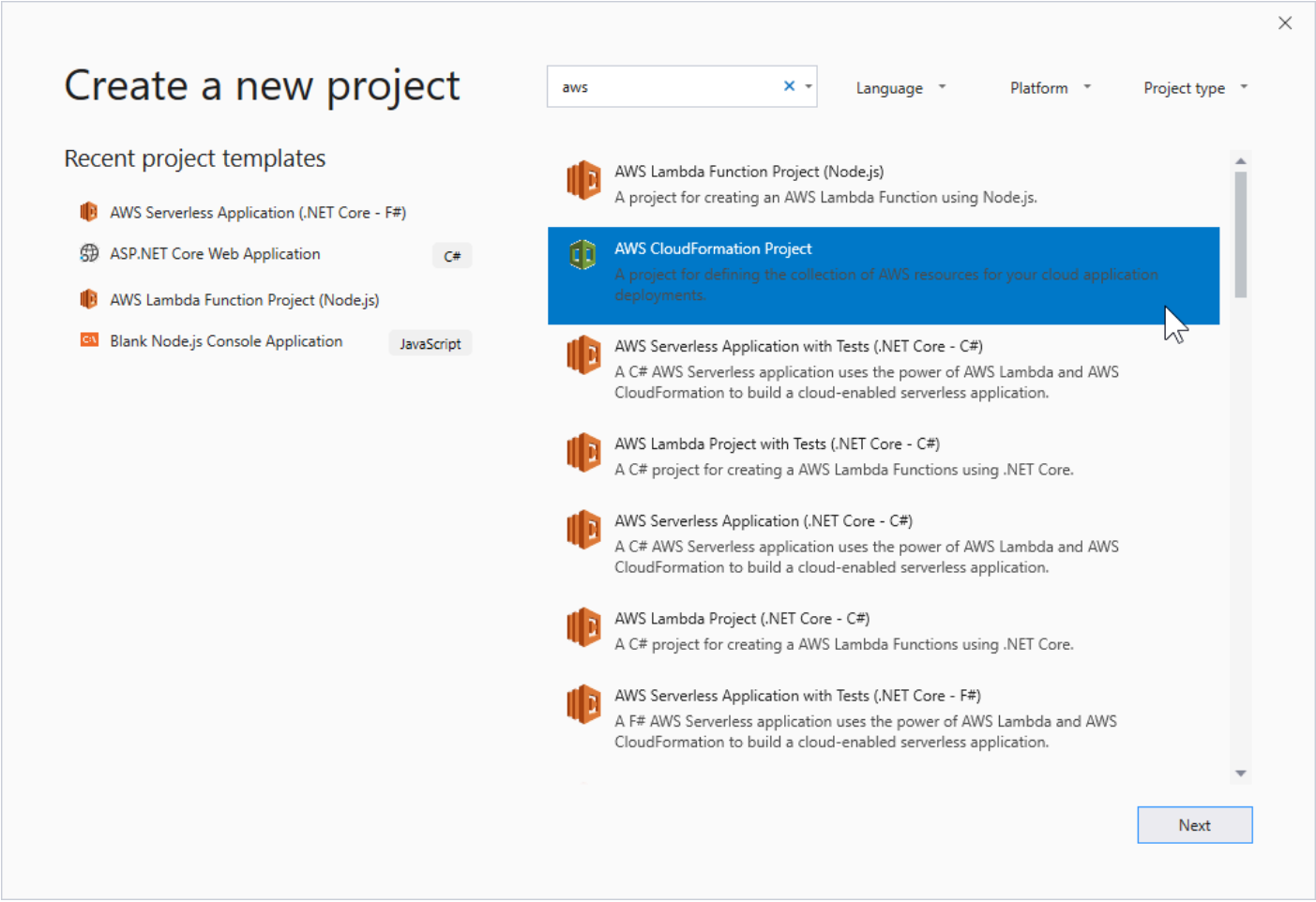
1. In Visual Studio, scegli File, scegli Nuovo e quindi scegli Progetto.
2. Per Visual Studio 2017:

   Nella finestra di dialogo Nuovo progetto, espandi Installato e seleziona AWS.



Per Visual Studio 2019:

Nella finestra di dialogo Nuovo progetto, assicurati che le caselle a discesa Lingua, Piattaforma e Tipo di progetto siano impostate su «Tutto...» e digita aws nel campo Cerca.



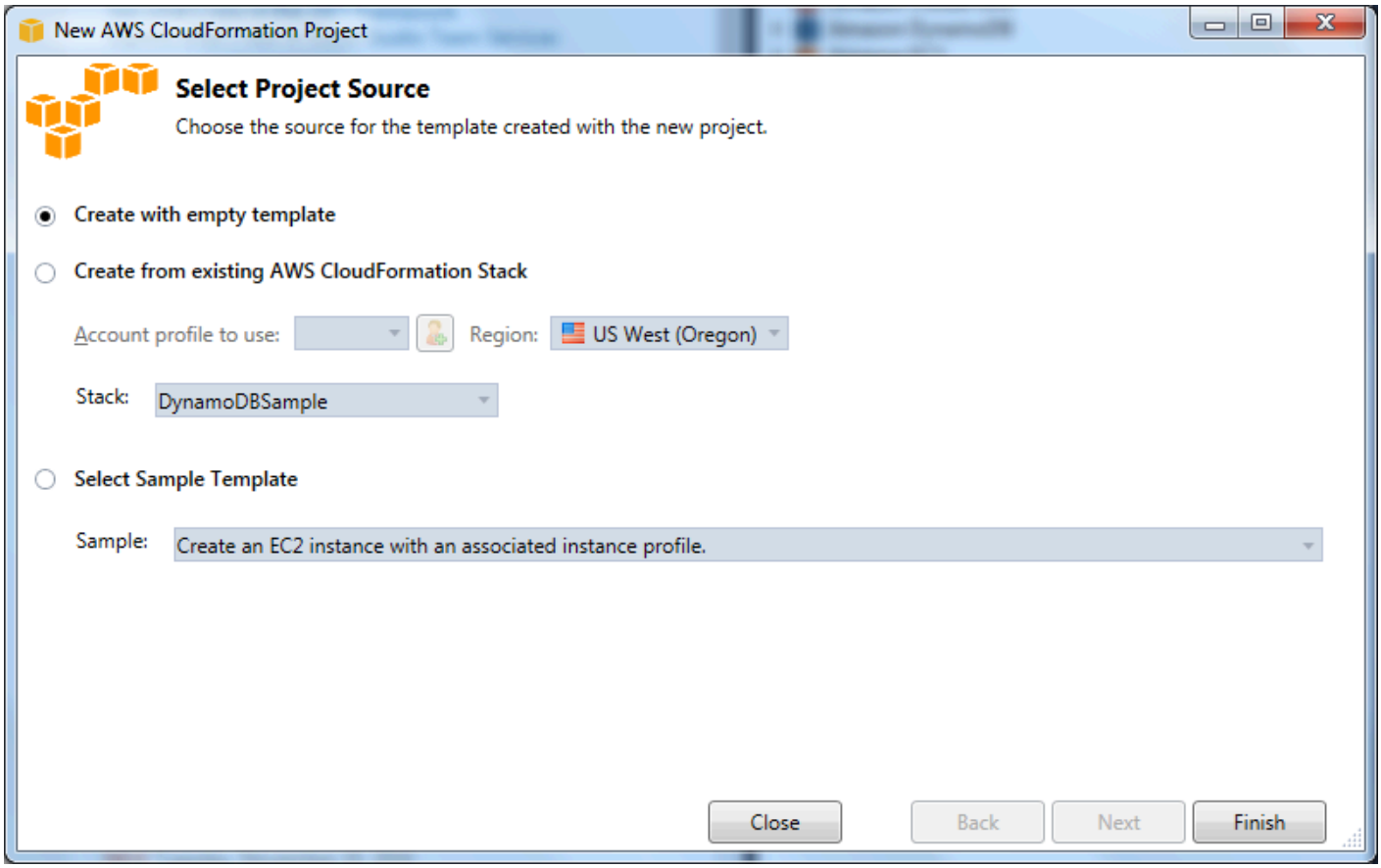
3. Seleziona il modello di AWS CloudFormation progetto.
4. Per Visual Studio 2017:

   Inserisci il nome, la posizione e così via desiderati per il tuo progetto modello, quindi fai clic su OK.

   Per Visual Studio 2019:

   Fare clic su Avanti. Nella finestra di dialogo successiva, inserisci il nome, la posizione, ecc. desiderati per il tuo progetto modello, quindi fai clic su Crea.
5. Nella pagina Seleziona l'origine del progetto, scegli la fonte del modello che creerai:
   - Crea con modello vuoto genera un nuovo CloudFormation modello vuoto.

- Lo stack Crea da AWS |CFN| esistente genera un modello da uno stack esistente nel tuo account. AWS (Non è necessario che lo stack abbia uno stato di.) `CREATE_COMPLETE`
- Seleziona un modello di esempio genera un modello da uno dei modelli di CloudFormation esempio.

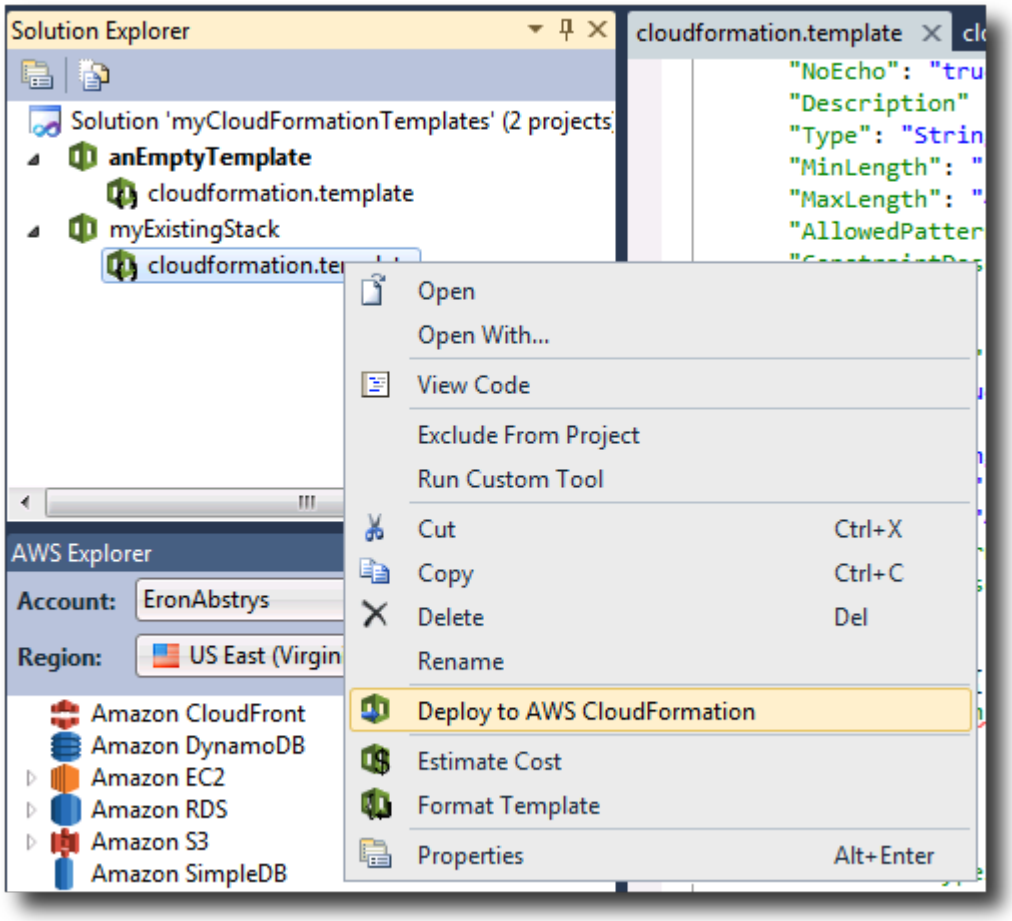


6. Per completare la creazione del CloudFormation modello di progetto, scegli Fine.

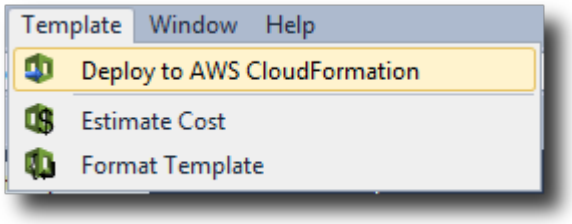
Distribuzione di un CloudFormation modello in Visual Studio

Per distribuire un modello CFN

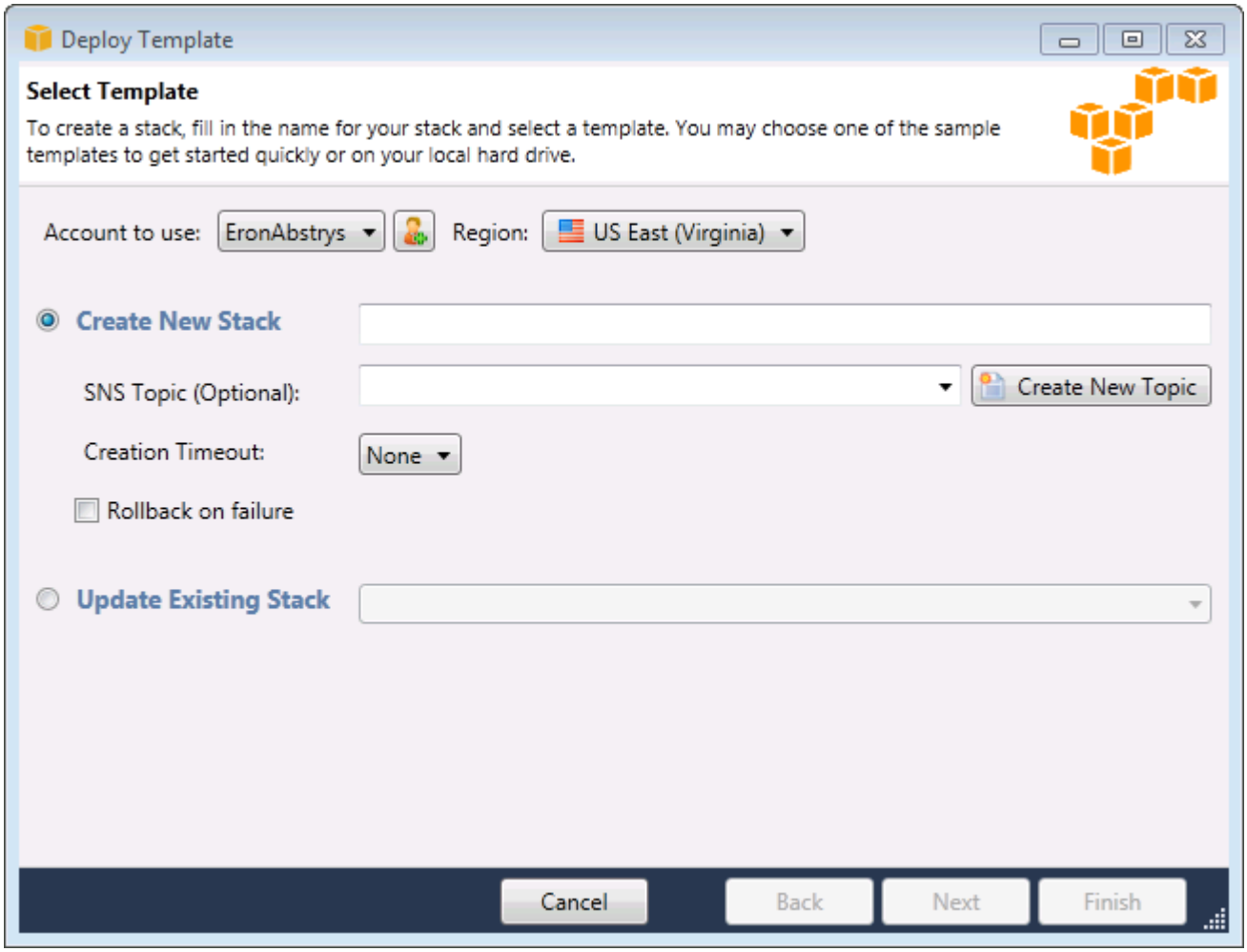
1. In Solution Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) per il modello che desideri distribuire e scegli Distribuisci su. AWS CloudFormation



In alternativa, per distribuire il modello che stai modificando, dal menu Modello, scegli Distribuisci su. AWS CloudFormation



2. Nella pagina Deploy Template, scegli Account AWS quello da usare per avviare lo stack e la regione in cui verrà lanciato.

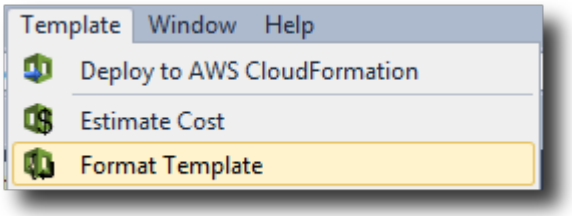


3. Scegli Crea nuovo stack e digita un nome per il tuo stack.
4. Seleziona una (o nessuna) delle seguenti opzioni:
   - Per ricevere notifiche sull'avanzamento dello stack, dall'elenco a discesa Argomento SNS, scegli un argomento SNS. Puoi anche creare un argomento SNS scegliendo Crea nuovo argomento e digitando un indirizzo email nella casella.
   - Utilizzate Creation Timeout per specificare per quanto tempo CloudFormation deve trascorrere la creazione dello stack prima che venga dichiarato fallito (e ripristinato, a meno che l'opzione Rollback on failure non sia deselezionata).
   - Usa Rollback in caso di errore se desideri che lo stack venga ripristinato (ovvero che si elimini da solo) in caso di errore. Lascia deselezionata questa opzione se desideri che lo stack rimanga attivo per scopi di debug, anche se non è riuscito a completare il lancio.
5. Scegli Fine per avviare lo stack.

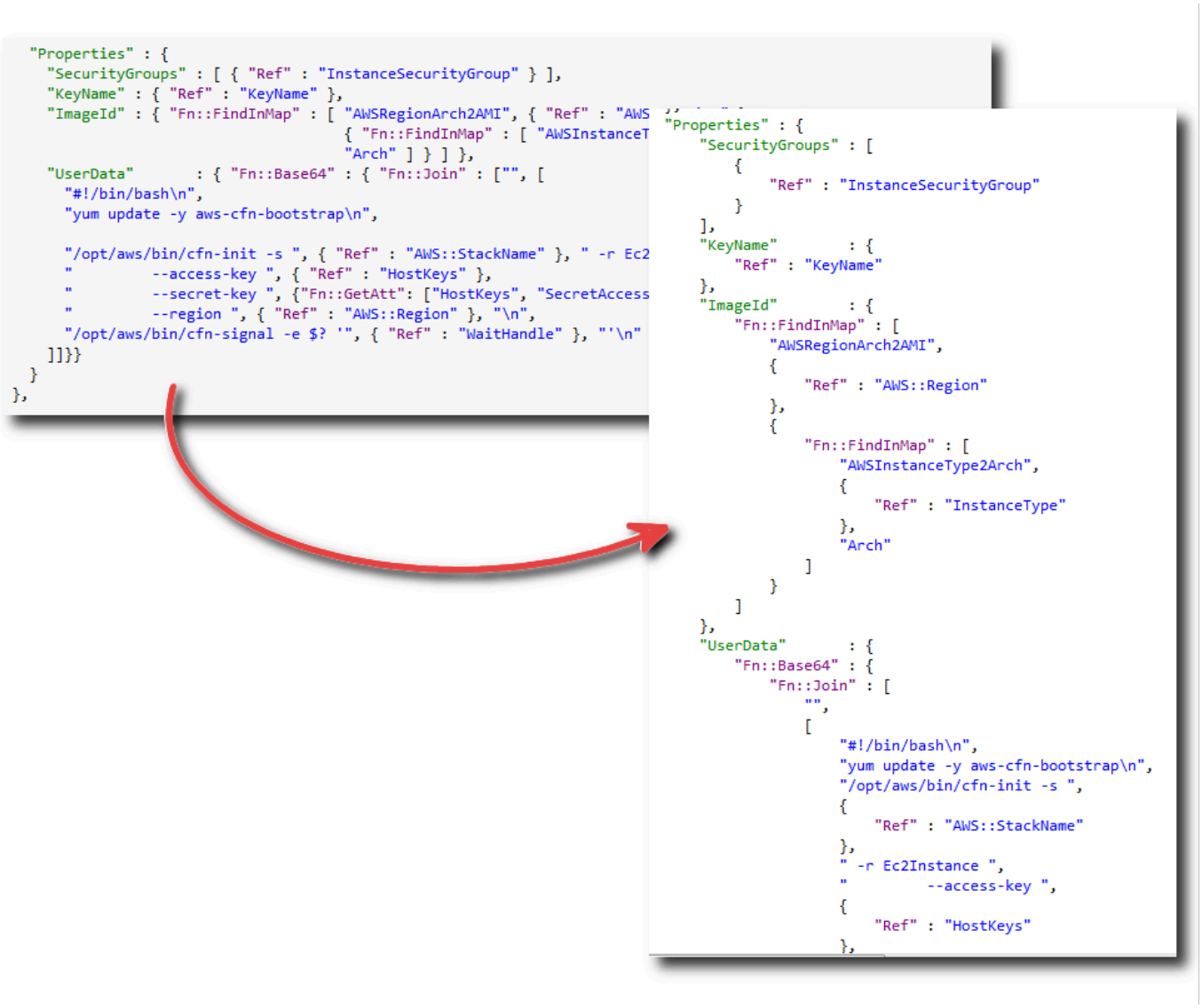
Formattazione di un CloudFormation modello in Visual Studio

- In Solution Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) per il modello e scegli Formato modello.

  In alternativa, per formattare il modello che stai modificando, dal menu Modello, scegli Formato modello.



  Il codice JSON verrà formattato in modo che la sua struttura sia presentata chiaramente.



Utilizzo di Amazon S3 di Explorer AWS

Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) consente di archiviare e recuperare dati da qualsiasi connessione a Internet. Tutti i dati archiviati su Amazon S3 sono associati al tuo account e, per impostazione predefinita, sono accessibili solo da te. Il Toolkit for Visual Studio consente di archiviare dati su Amazon S3 e di visualizzare, gestire, recuperare e distribuire tali dati.

Amazon S3 utilizza il concetto di bucket, che può essere considerato simile ai file system o alle unità logiche. I bucket possono contenere cartelle, simili alle directory, e oggetti, simili ai file. In questa sezione, utilizzeremo questi concetti per illustrare la funzionalità di Amazon S3 esposta dal Toolkit for Visual Studio.

> **Note**
>
> Per utilizzare questo strumento, la tua policy IAM deve concedere le autorizzazioni per le azioni `s3:GetBucketAcl` `es3:GetBucket`. `s3:ListBucket` Per ulteriori informazioni, consulta Panoramica delle politiche AWS IAM.

Creazione di un bucket Amazon S3

Il bucket è l'unità di storage più importante in Amazon S3.

Per creare un bucket S3

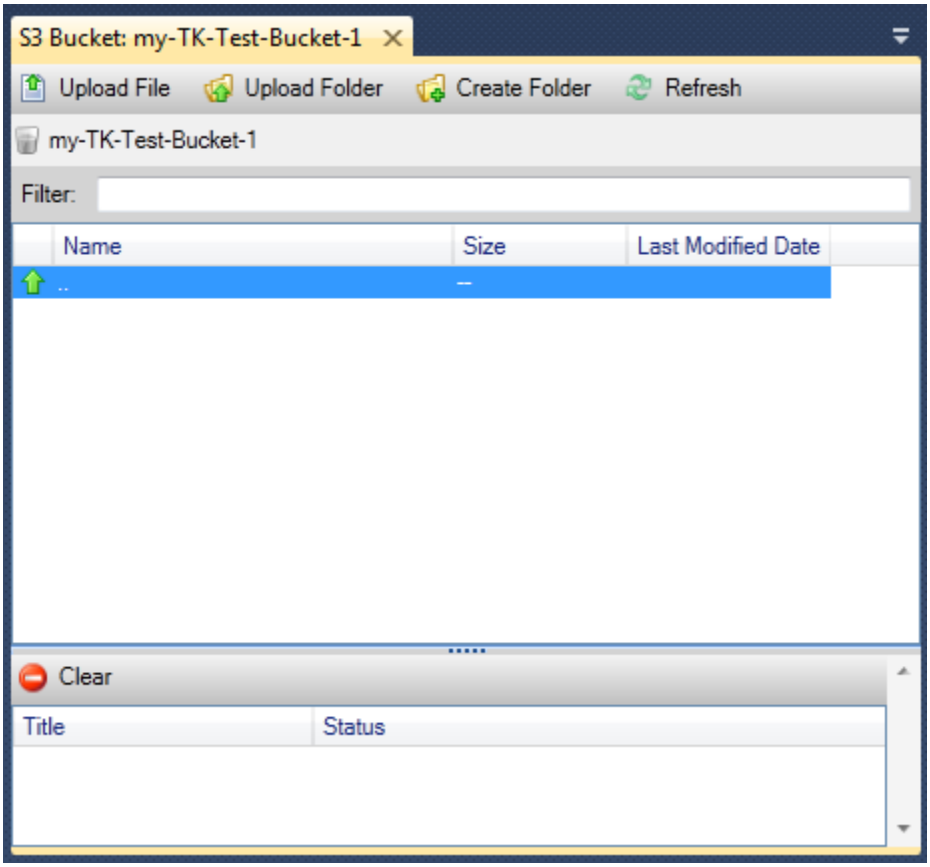
1. In AWS Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) per il nodo Amazon S3, quindi scegli Create Bucket.
2. Nella finestra di dialogo Crea bucket, digita un nome per il bucket. I nomi dei bucket devono essere univoci in tutto. AWS Per informazioni su altri vincoli, consulta la documentazione di Amazon S3.
3. Scegli OK.

Gestione dei bucket Amazon S3 da Explorer AWS

In AWS Explorer, le seguenti operazioni sono disponibili quando si apre un menu contestuale (facendo clic con il pulsante destro del mouse) per un bucket Amazon S3.

Sfoglia

Visualizza una vista degli oggetti contenuti nel bucket. Da qui, puoi creare cartelle o caricare file o intere directory e cartelle dal tuo computer locale. Il riquadro inferiore mostra i messaggi di stato relativi al processo di caricamento. Per cancellare questi messaggi, scegli l'icona Cancella. Puoi accedere a questa visualizzazione del bucket anche facendo doppio clic sul nome del bucket in Explorer. AWS



Proprietà

Visualizza una finestra di dialogo in cui è possibile effettuare le seguenti operazioni:

- Imposta le autorizzazioni Amazon S3 che coprono l'ambito per:
  - tu come proprietario del bucket.
  - tutti gli utenti che sono stati autenticati su. AWS
  - tutti coloro che hanno accesso a Internet.
- Attiva la registrazione per il bucket.
- Imposta una notifica utilizzando Amazon Simple Notification Service (Amazon SNS) in modo che se utilizzi Reduced Redundancy Storage (RRS), riceverai una notifica in caso di perdita di dati. RRS è un'opzione di storage Amazon S3 che offre una durata inferiore rispetto allo storage standard, ma a costi ridotti. Per ulteriori informazioni, consulta S3. FAQs
- Crea un sito Web statico utilizzando i dati nel bucket.

Policy

Ti consente di configurare politiche AWS Identity and Access Management (IAM) per il tuo bucket. Per ulteriori informazioni, consulta la documentazione IAM e i casi d'uso per IAM e S3.

Crea un URL prefirmato

Consente di generare un URL limitato nel tempo che è possibile distribuire per fornire l'accesso al contenuto del bucket. Per ulteriori informazioni, consulta Come creare un URL prefirmato.

Visualizza caricamenti in più parti

Consente di visualizzare caricamenti in più parti. Amazon S3 supporta la suddivisione in parti dei caricamenti di oggetti di grandi dimensioni per rendere il processo di caricamento più efficiente. Per ulteriori informazioni, consulta la discussione sui caricamenti in più parti nella documentazione di S3.

Elimina

Consente di eliminare il bucket. È possibile eliminare solo bucket vuoti.

Caricamento di file e cartelle su Amazon S3

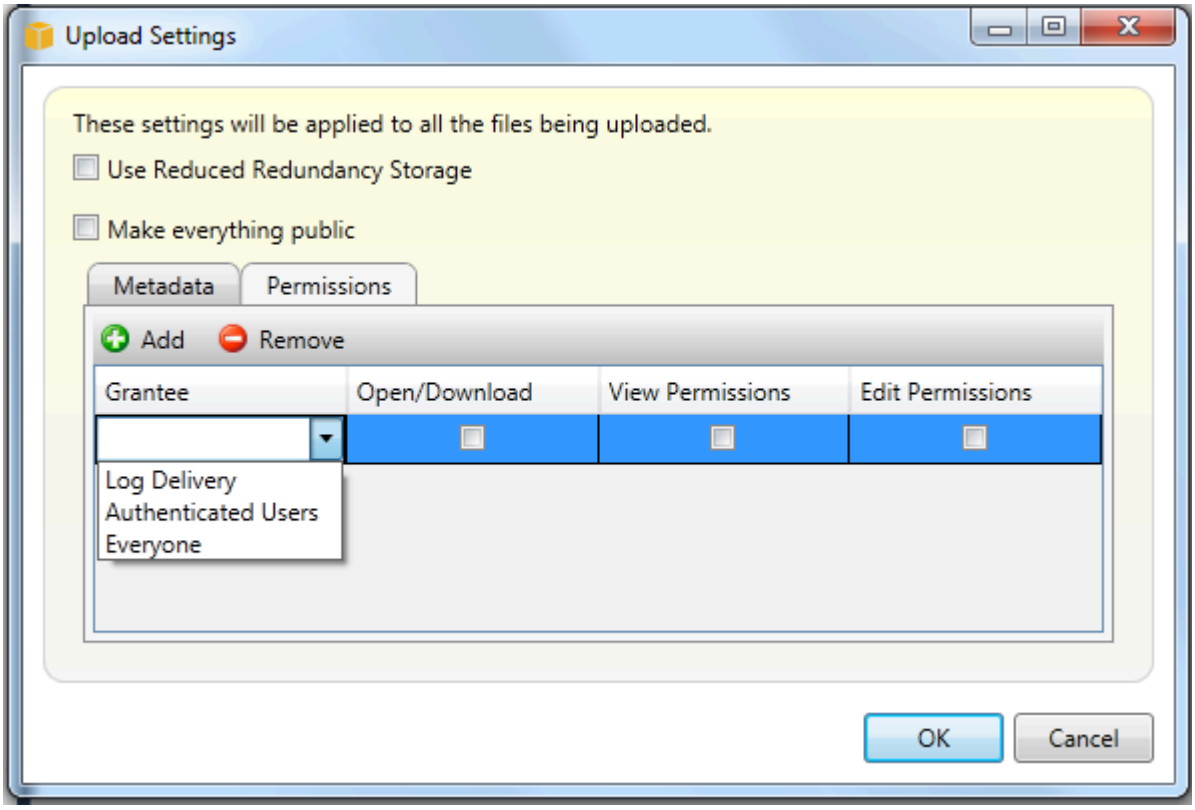
Puoi utilizzare AWS Explorer per trasferire file o intere cartelle dal tuo computer locale a qualsiasi bucket.

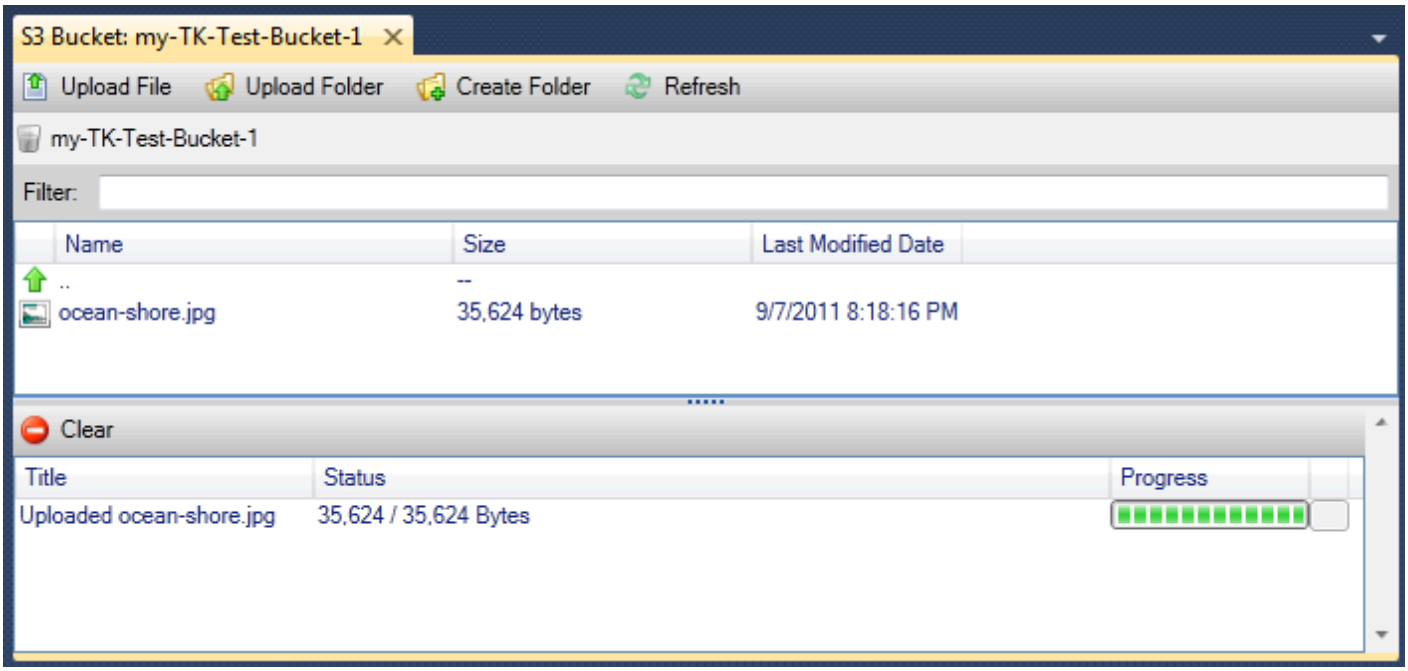
> **Note**
>
> Se carichi file o cartelle con lo stesso nome di file o cartelle già esistenti nel bucket Amazon S3, i file caricati sovrascriveranno i file esistenti senza preavviso.

Per caricare un file su S3

1. In AWS Explorer, espandi il nodo Amazon S3 e fai doppio clic su un bucket o apri il menu contestuale (fai clic con il pulsante destro del mouse) per il bucket e scegli Sfoglia.
2. Nella visualizzazione Sfoglia del tuo bucket, scegli Carica file o Carica cartella.
3. Nella finestra di dialogo Apri file, accedi ai file da caricare, sceglili e quindi scegli Apri. Se state caricando una cartella, accedete e scegliete quella cartella, quindi scegliete Apri.

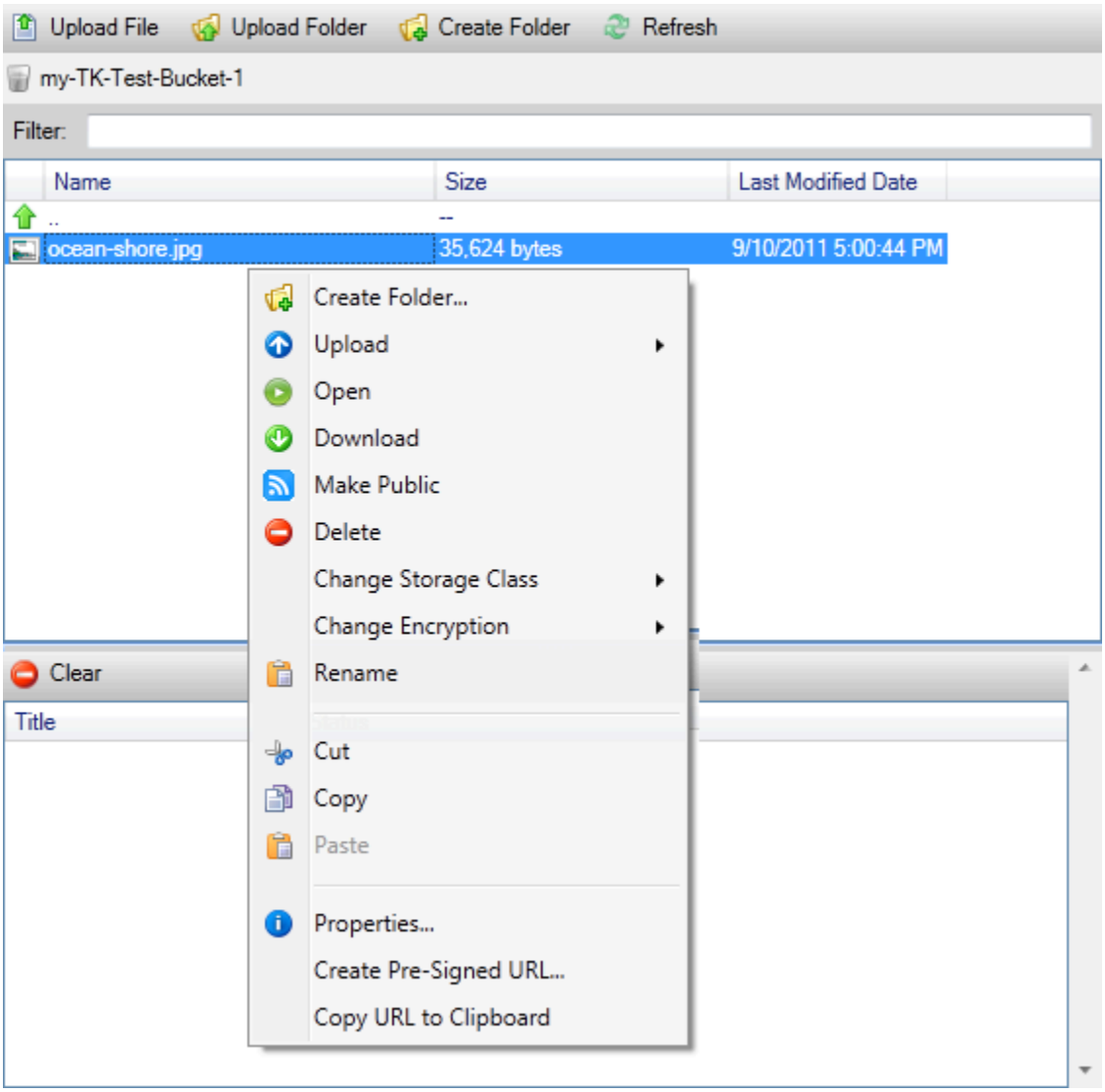
   La finestra di dialogo Impostazioni di caricamento consente di impostare i metadati e le autorizzazioni per i file o la cartella che state caricando. La selezione della casella di controllo Rendi tutto pubblico equivale a impostare le autorizzazioni di apertura/download su Tutti. È possibile selezionare l'opzione per utilizzare Reduced Redundancy Storage per i file caricati.





Operazioni sui file Amazon S3 di AWS Toolkit for Visual Studio

Se scegli un file nella vista di Amazon S3 e apri il menu contestuale (facendo clic con il pulsante destro del mouse), puoi eseguire diverse operazioni sul file.



Crea cartella

Consente di creare una cartella nel bucket corrente. (Equivalente a scegliere il link Crea cartella).

Caricamento

Consente di caricare file o cartelle. (Equivalente a scegliere i link Carica file o Carica cartella).

Open (Apertura)

Tenta di aprire il file selezionato nel browser predefinito. A seconda del tipo di file e delle funzionalità del browser predefinito, il file potrebbe non essere visualizzato. Potrebbe invece essere semplicemente scaricato dal tuo browser.

Scarica

Apre una finestra di dialogo Folder-Tree per consentire di scaricare il file selezionato.

Rendi pubblico

Imposta le autorizzazioni per il file selezionato su Apri/Scarica e Tutti. (Equivalente a selezionare la casella di controllo Rendi tutto pubblico nella finestra di dialogo Impostazioni di caricamento).

Elimina

Elimina i file o le cartelle selezionati. Puoi anche eliminare file o cartelle scegliendoli e premendo`Delete`.

Cambia classe di archiviazione

Imposta la classe di archiviazione su Standard o RRS (Reduced Redundancy Storage). Per visualizzare l'impostazione corrente della classe di archiviazione, scegli Proprietà.

Cambia crittografia

Consente di impostare la crittografia lato server sul file. Per visualizzare l'impostazione di crittografia corrente, scegli Proprietà.

Assegnazione di un nuovo nome

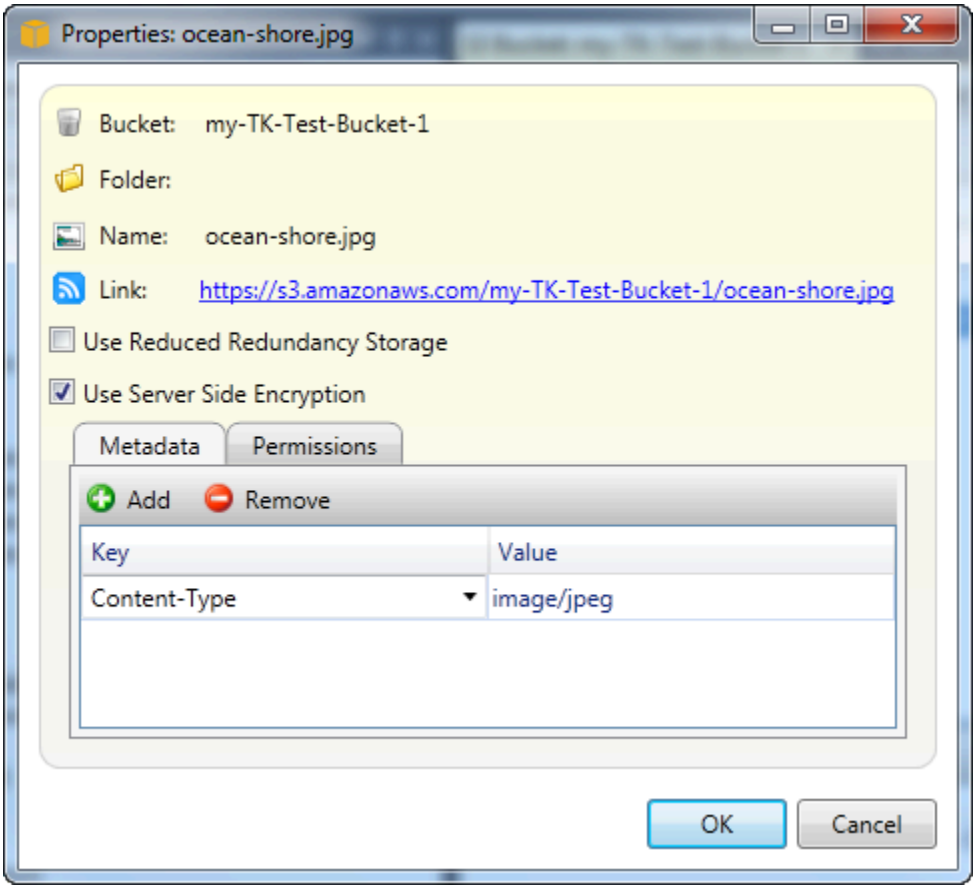
Consente di rinominare un file. Non è possibile rinominare una cartella.

Taglia | Copia | Incolla

Consente di tagliare, copiare e incollare file o cartelle tra cartelle o tra secchi.

Proprietà

Visualizza una finestra di dialogo che consente di impostare i metadati e le autorizzazioni per il file, nonché di alternare l'archiviazione del file tra Reduced Redundancy Storage (RRS) e Standard e di impostare la crittografia lato server per il file. Questa finestra di dialogo visualizza anche un collegamento https al file. Se scegli questo collegamento, Toolkit for Visual Studio apre il file nel browser predefinito. Se disponi delle autorizzazioni per il file impostate su Apri/Scarica e Tutti, altre persone potranno accedere al file tramite questo link. Piuttosto che distribuire questo link, ti consigliamo di creare e distribuire link prefirmati. URLs



Crea un URL prefirmato

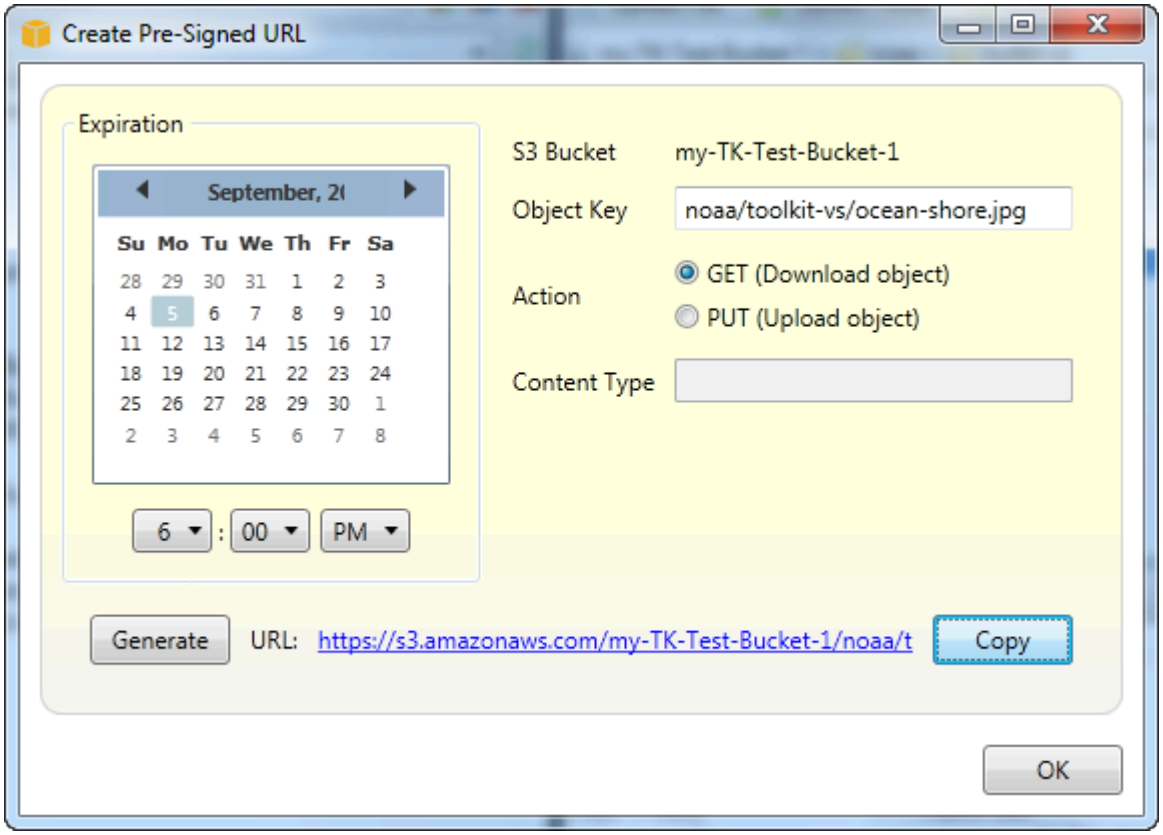
Ti consente di creare un URL prefirmato a tempo limitato che puoi distribuire per consentire ad altre persone di accedere ai contenuti che hai archiviato su Amazon S3.

Come creare un URL prefirmato

Puoi creare un URL prefirmato per uno o più file in un bucket. Altre persone possono quindi utilizzare questo URL per accedere al bucket o al file. L'URL scadrà dopo un periodo di tempo specificato al momento della creazione dell'URL.

Per creare un URL prefirmato

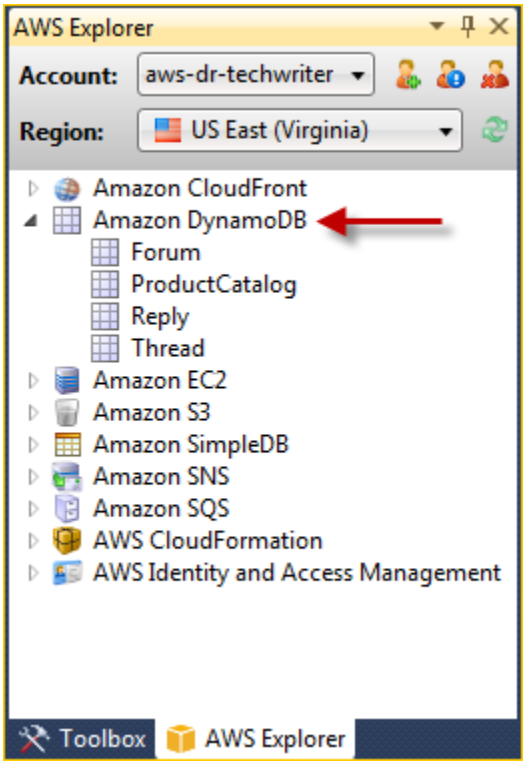
1. Nella finestra di dialogo Crea URL prefirmato, impostate la data e l'ora di scadenza dell'URL. L'impostazione predefinita è un'ora dall'ora corrente.
2. Scegli il pulsante Genera.
3. Per copiare l'URL negli appunti, scegliere Copia.



Utilizzo di DynamoDB da Explorer AWS

Amazon DynamoDB è un servizio di database non relazionale, conveniente, veloce e altamente scalabile e disponibile. DynamoDB rimuove le tradizionali limitazioni di scalabilità sullo storage dei dati mantenendo una bassa latenza e prestazioni prevedibili. Il Toolkit for Visual Studio offre funzionalità per lavorare con DynamoDB in un contesto di sviluppo. Per ulteriori informazioni su DynamoDB, consulta DynamoDB sul sito Web di Amazon Web Services.

Nel Toolkit for Visual Studio AWS , Explorer visualizza tutte le tabelle DynamoDB associate a quelle attive. Account AWS



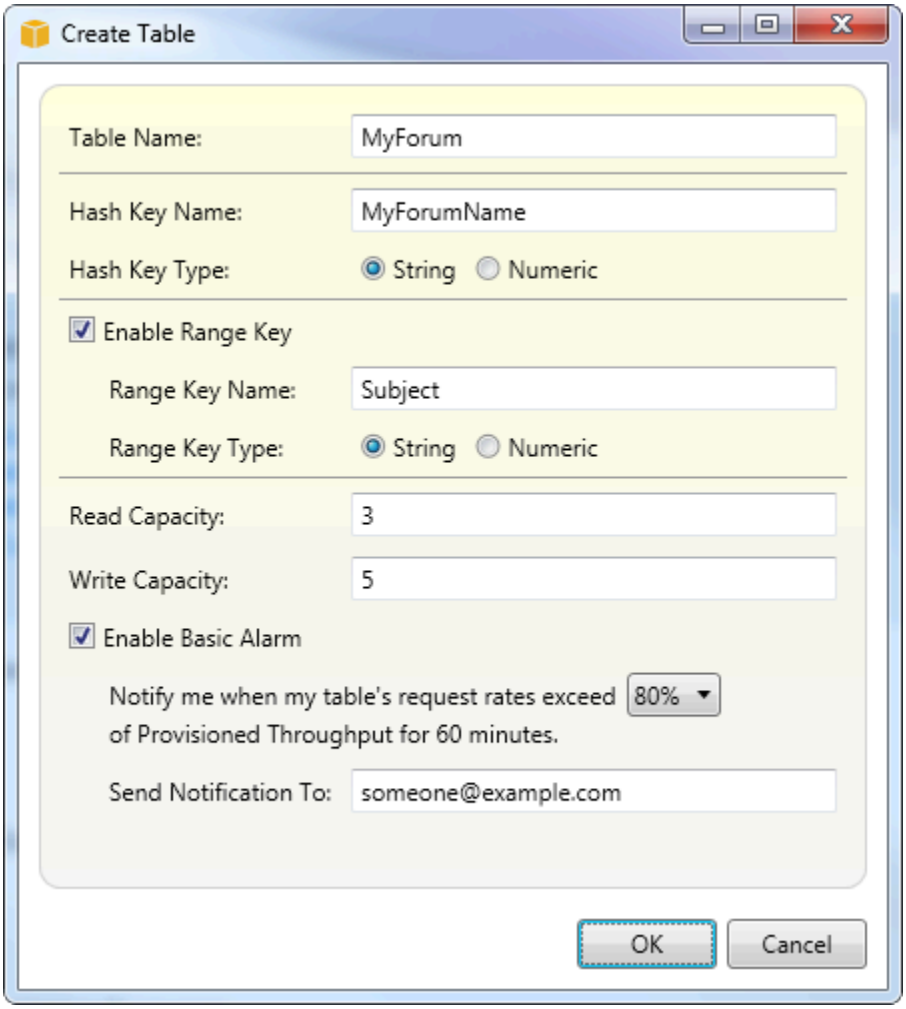
Creazione di una tabella DynamoDB

È possibile utilizzare il Toolkit for Visual Studio per creare una tabella DynamoDB.

Per creare una tabella in Explorer AWS

1. In AWS Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) per Amazon DynamoDB, quindi scegli Crea tabella.
2. Nella procedura guidata Crea tabella, in Nome tabella, digita un nome per la tabella.
3. Nel campo Hash Key Name, digitate un attributo di chiave hash principale e, tra i pulsanti Hash Key Type, scegliete il tipo di chiave hash. DynamoDB crea un indice hash non ordinato utilizzando l'attributo chiave primaria e un indice di intervallo ordinato opzionale utilizzando l'attributo range primary key. Per ulteriori informazioni sull'attributo della chiave hash primaria, vai alla sezione Primary Key della Amazon DynamoDB Developer Guide.
4. (Facoltativo) Seleziona Enable Range Key. Nel campo Range Key Name, digita un attributo chiave di intervallo, quindi dai pulsanti Range Key Type, scegli un tipo di chiave di intervallo.
5. Nel campo Capacità di lettura, digita il numero di unità di capacità di lettura. Nel campo Capacità di scrittura, digitare il numero di unità di capacità di scrittura. È necessario specificare un minimo di tre unità di capacità di lettura e cinque unità di capacità di scrittura. Per ulteriori informazioni sulle unità di capacità di lettura e scrittura, consulta Provisioned Throughput in DynamoDB.

6. (Facoltativo) Seleziona Abilita Basic Alarm per avvisarti quando i tassi di richiesta della tabella sono troppo alti. Scegli la percentuale di throughput assegnato per 60 minuti che deve essere superata prima dell'invio dell'avviso. In Invia notifiche a, digita un indirizzo email.
7. Fate clic su OK per creare la tabella.

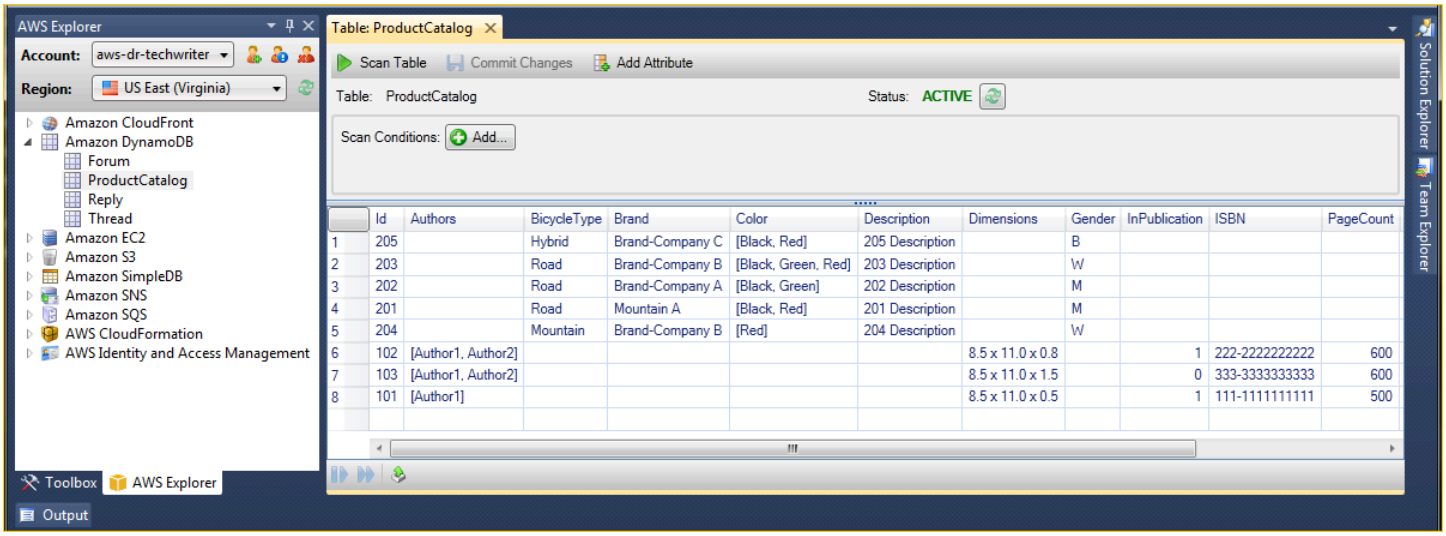


Per ulteriori informazioni sulle tabelle DynamoDB, vai a Data Model Concepts - Tables, Items and Attributes.

Visualizzazione di una tabella DynamoDB come griglia

Per aprire una visualizzazione a griglia di una delle tue tabelle DynamoDB, AWS in Explorer, fai doppio clic sul sottonodo corrispondente alla tabella. Dalla visualizzazione griglia, è possibile visualizzare le voci, gli attributi e i valori memorizzati nella tabella. Ogni riga corrisponde a una voce nella tabella. Le colonne della tabella corrispondono agli attributi. Ogni cella della tabella contiene i valori associati a tale attributo per quella voce.

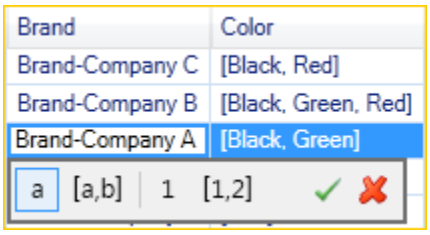
Un attributo può avere un valore che può essere una stringa o un numero. Alcuni attributi hanno un valore che è composto da un set di stringhe o numeri. I valori del set vengono visualizzati come un elenco separato da virgole racchiuso tra parentesi quadre.



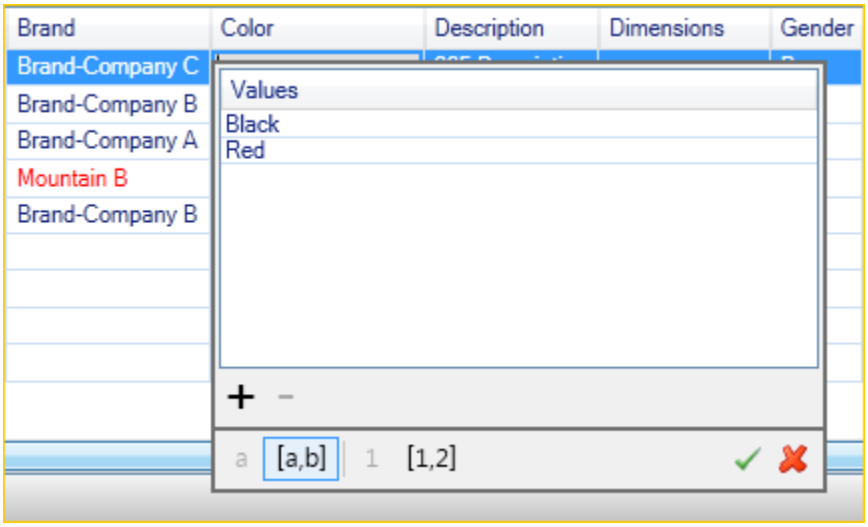
	Id	Authors	BicycleType	Brand	Color	Description	Dimensions	Gender	InPublication	ISBN	PageCount
1	205		Hybrid	Brand-Company C	[Black, Red]	205 Description		B			
2	203		Road	Brand-Company B	[Black, Green, Red]	203 Description		W			
3	202		Road	Brand-Company A	[Black, Green]	202 Description		M			
4	201		Road	Mountain A	[Black, Red]	201 Description		M			
5	204		Mountain	Brand-Company B	[Red]	204 Description		W			
6	102	[Author1, Author2]					8.5 x 11.0 x 0.8		1	222-2222222222	600
7	103	[Author1, Author2]					8.5 x 11.0 x 1.5		0	333-3333333333	600
8	101	[Author1]					8.5 x 11.0 x 0.5		1	111-1111111111	500

Modifica e aggiunta di attributi e valori

Facendo doppio clic su una cella, è possibile modificare i valori dell'attributo corrispondente dell'elemento. Per gli attributi con set di valori, è anche possibile aggiungere o eliminare singoli valori dal set.



Oltre a modificare il valore di un attributo, puoi anche, con alcune limitazioni, modificare il formato del valore di un attributo. Ad esempio, qualsiasi numero può essere convertito in una stringa. Se si dispone di un valore di stringa, il cui contenuto è un numero, ad esempio 125, l'editor di celle consente di convertire il formato del valore da stringa a numero. È inoltre possibile convertire un valore singolo in un valore impostato. Tuttavia, in genere non è possibile effettuare la conversione da un set di valori a un valore singolo; un'eccezione è quando il set di valori contiene un solo elemento.

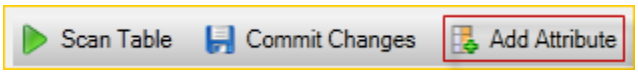


Dopo aver modificato il valore dell'attributo, scegli il segno di spunta verde per confermare le modifiche. Se desideri annullare le modifiche, scegli la X rossa.

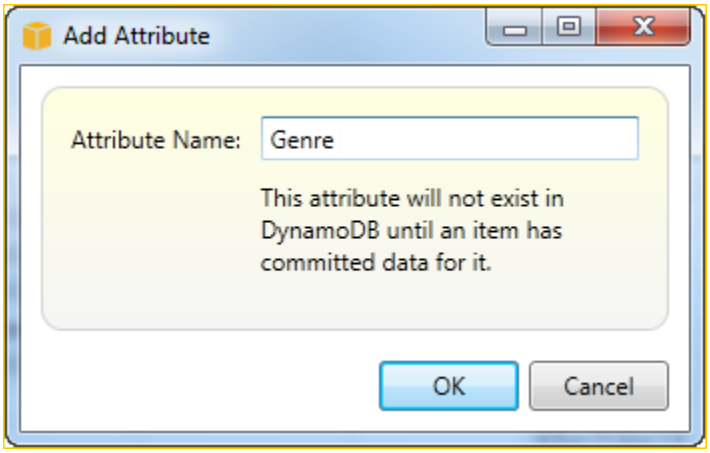
Dopo aver confermato le modifiche, il valore dell'attributo verrà visualizzato in rosso. Ciò indica che l'attributo è stato aggiornato, ma che il nuovo valore non è stato riscritto nel database DynamoDB. Per riscrivere le modifiche in DynamoDB, scegli Conferma modifiche. Per annullare le modifiche, scegli Scan Table e quando il Toolkit ti chiede se desideri salvare le modifiche prima della scansione, scegli No.

Aggiungere un attributo

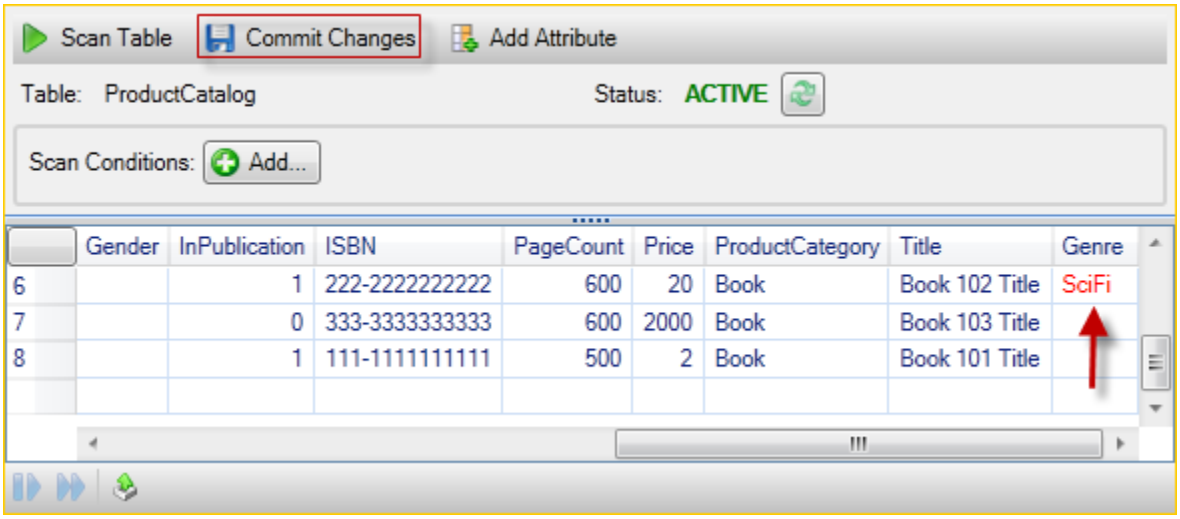
Dalla vista a griglia, puoi anche aggiungere attributi alla tabella. Per aggiungere un nuovo attributo, scegliete Aggiungi attributo.



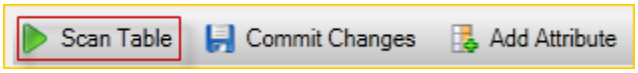
Nella finestra di dialogo Aggiungi attributo, digitate un nome per l'attributo, quindi scegliete OK.



Per fare in modo che il nuovo attributo diventi parte della tabella, è necessario aggiungere un valore per almeno un elemento e quindi scegliere il pulsante Conferma modifiche. Per eliminare il nuovo attributo, è sufficiente chiudere la visualizzazione a griglia della tabella senza scegliere Conferma modifiche.



Scansione di una tabella DynamoDB

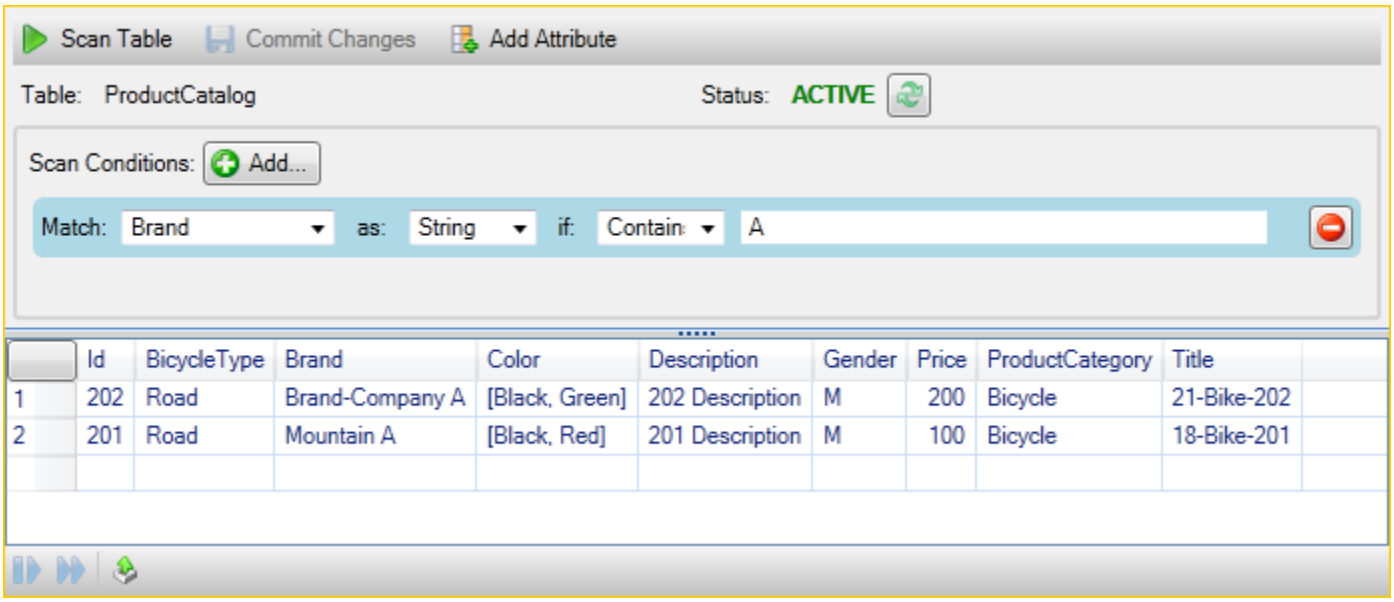


È possibile eseguire scansioni sulle tabelle DynamoDB dal Toolkit. In una scansione si definisce un set di criteri e la scansione restituisce tutte le voci della tabella che soddisfano i criteri specificati. Le scansioni sono operazioni costose e devono essere utilizzate con cautela per evitare di interrompere il traffico di produzione con priorità più elevata. Per ulteriori informazioni sull'utilizzo dell'operazione di scansione, consulta la Amazon DynamoDB Developer Guide.

Per eseguire una scansione su una tabella DynamoDB da Explorer AWS

1. Nella visualizzazione a griglia, scegli il pulsante Condizioni di scansione: aggiungi.
2. Nell'editor delle clausole Scan, scegli l'attributo con cui confrontare, come deve essere interpretato il valore dell'attributo (stringa, numero, valore impostato), come deve essere abbinato (ad esempio Begins With o Contains) e il valore letterale a cui deve corrispondere.
3. Aggiungi altre clausole Scan, se necessario, per la ricerca. La scansione restituirà solo le voci che soddisfano i criteri di tutte le clausole di scansione. Scan eseguirà un confronto con distinzione tra maiuscole e minuscole durante la corrispondenza con i valori delle stringhe.
4. Nella barra dei pulsanti nella parte superiore della visualizzazione a griglia, scegli Scansiona tabella.

Per rimuovere una clausola Scan, scegliete il pulsante rosso con la linea bianca a destra di ogni clausola.



Per tornare alla visualizzazione della tabella che include tutti gli elementi, rimuovete tutte le clausole Scan e scegliete nuovamente Scan Table.

Paginazione dei risultati della scansione

Nella parte inferiore della visualizzazione ci sono tre pulsanti.

I primi due pulsanti blu forniscono l'impaginazione dei risultati della scansione. Il primo pulsante mostrerà una pagina aggiuntiva di risultati. Il secondo pulsante mostrerà altre dieci pagine di risultati. In questo contesto, una pagina equivale a 1 MB di contenuto.

Esporta il risultato della scansione in formato CSV

Il terzo pulsante esporta i risultati della scansione corrente in un file CSV.

Utilizzo AWS CodeCommit con Visual Studio Team Explorer

Puoi utilizzare gli account utente AWS Identity and Access Management (IAM) per creare credenziali Git e utilizzarle per creare e clonare repository dall'interno di Team Explorer.

Tipi di credenziali per AWS CodeCommit

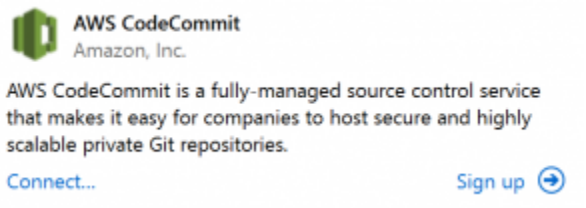
La maggior parte AWS Toolkit for Visual Studio degli utenti è a conoscenza della configurazione di profili di AWS credenziali che contengono le proprie chiavi di accesso e segrete. Questi profili di credenziali vengono utilizzati nel Toolkit for Visual Studio per abilitare le chiamate al APIs servizio, ad esempio per elencare i bucket Amazon S3 AWS in Explorer o per avviare un'istanza Amazon. EC2 L'integrazione di AWS CodeCommit con Team Explorer utilizza anche questi profili di credenziali. Tuttavia, per lavorare con Git stesso sono necessarie credenziali aggiuntive, in particolare credenziali Git per le connessioni HTTPS. Puoi leggere informazioni su queste credenziali (nome utente e password) nella sezione Configurazione per utenti HTTPS che utilizzano credenziali Git nella Guida per l'AWS CodeCommit utente.

Puoi creare le credenziali Git AWS CodeCommit solo per gli account utente IAM. Non è possibile crearle per un account root. È possibile creare fino a due set di queste credenziali per il servizio e, sebbene sia possibile contrassegnare un set di credenziali come inattivo, i set inattivi vengono comunque conteggiati ai fini del limite di due set. Tieni presente che puoi eliminare e ricreare le credenziali in qualsiasi momento. Quando si utilizza AWS CodeCommit dall'interno di Visual Studio, le AWS credenziali tradizionali vengono utilizzate per lavorare con il servizio stesso, ad esempio per creare ed elencare gli archivi. Quando si lavora con gli effettivi repository Git ospitati in AWS CodeCommit, si utilizzano le credenziali Git.

Come parte del supporto per AWS CodeCommit, il Toolkit for Visual Studio crea e gestisce automaticamente queste credenziali Git per te e le AWS associa al tuo profilo di credenziali. Non devi preoccuparti di avere a portata di mano il giusto set di credenziali per eseguire operazioni Git all'interno di Team Explorer. Una volta che ti connetti a Team Explorer con il tuo profilo di AWS credenziali, le credenziali Git associate vengono utilizzate automaticamente ogni volta che lavori con un telecomando Git.

Connessione a AWS CodeCommit

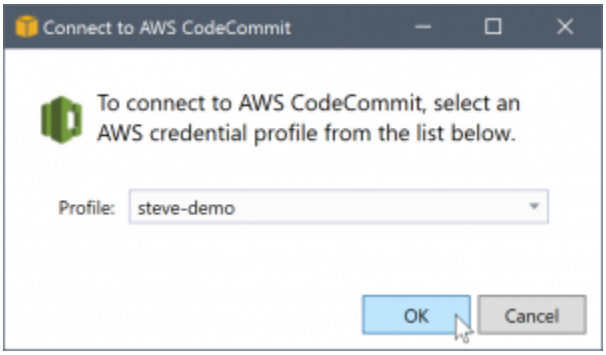
Quando apri la finestra Team Explorer in Visual Studio 2015 o versioni successive, vedrai una AWS CodeCommit voce nella sezione Hosted Service Provider di Gestisci connessioni.



Scegliendo Iscriviti si apre la home page di Amazon Web Services in una finestra del browser. Ciò che accade quando si sceglie Connect dipende dal fatto che Toolkit for Visual Studio sia in grado di trovare un profilo di credenziali AWS con chiavi di accesso e segrete per consentirgli di effettuare chiamate AWS per conto dell'utente. È possibile che sia stato impostato un profilo di credenziali utilizzando la nuova pagina Guida introduttiva visualizzata nell'IDE quando Toolkit for Visual Studio non riesce a trovare credenziali archiviate localmente. Oppure potresti aver utilizzato Toolkit for Visual Studio, o AWS Tools for Windows PowerShell il e AWS avere già profili di credenziali disponibili per AWS CLI l'utilizzo di Toolkit for Visual Studio.

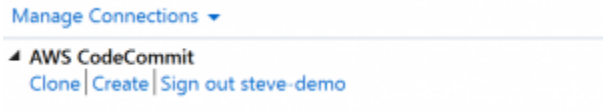
Quando scegli Connect, Toolkit for Visual Studio avvia il processo per trovare un profilo di credenziali da utilizzare nella connessione. Se Toolkit for Visual Studio non riesce a trovare un profilo di credenziali, apre una finestra di dialogo che invita a inserire le chiavi di accesso e segrete per il tuo. Account AWS Ti consigliamo vivamente di utilizzare un account utente IAM e non le tue credenziali root. Inoltre, come indicato in precedenza, le credenziali Git necessarie alla fine possono essere create solo per gli utenti IAM. Una volta fornite le chiavi di accesso e segrete e creato il profilo delle credenziali, la connessione tra Team Explorer e AWS CodeCommit è pronta per l'uso.

Se Toolkit for Visual Studio trova più di AWS un profilo di credenziali, ti viene richiesto di selezionare l'account che desideri utilizzare in Team Explorer.



Se disponi di un solo profilo di credenziali, Toolkit for Visual Studio ignora la finestra di dialogo di selezione del profilo e ti connetti immediatamente:

Quando viene stabilita una connessione tra Team Explorer e AWS CodeCommit tramite i profili delle credenziali, la finestra di dialogo di invito si chiude e viene visualizzato il pannello di connessione.



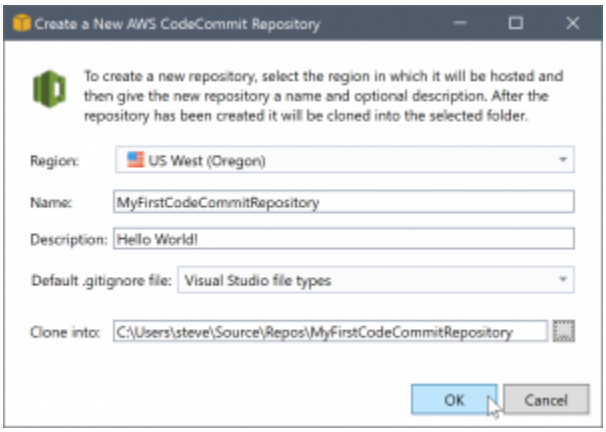
Poiché non sono presenti repository clonati localmente, il pannello mostra solo le operazioni che è possibile eseguire: Clona, Crea ed Esci. Come altri provider, AWS CodeCommit in Team Explorer

può essere associato a un solo profilo di AWS credenziali alla volta. Per cambiare account, usa Esci per rimuovere la connessione in modo da poter iniziare una nuova connessione utilizzando un account diverso.

Ora che hai stabilito una connessione, puoi creare un repository facendo clic sul link Crea.

Creazione di un repository

Quando fate clic sul link Crea, viene visualizzata la finestra di dialogo Crea un nuovo AWS CodeCommit deposito.



AWS CodeCommit I repository sono organizzati per regione, quindi in Regione è possibile selezionare la regione in cui ospitare il repository. L'elenco contiene tutte le regioni in cui AWS CodeCommit è supportato. Fornisci il nome (obbligatorio) e la descrizione (opzionale) per il nostro nuovo repository.

Il comportamento predefinito della finestra di dialogo consiste nel aggiungere il nome del repository alla posizione della cartella del nuovo repository (man mano che si immette il nome, anche la posizione della cartella viene aggiornata). Per utilizzare un nome di cartella diverso, modificate il percorso Clone in folder dopo aver inserito il nome del repository.

Puoi anche scegliere di creare automaticamente un `.gitignore` file iniziale per il repository. AWS Toolkit for Visual Studio Fornisce un valore predefinito integrato per i tipi di file di Visual Studio. Puoi anche scegliere di non avere alcun file o di utilizzare un file esistente personalizzato che desideri riutilizzare in più repository. Seleziona semplicemente Usa personalizzato nell'elenco e vai al file personalizzato da utilizzare.

Una volta che hai il nome e la posizione del repository, sei pronto per fare clic su OK e iniziare a creare il repository. Il Toolkit for Visual Studio richiede che il servizio crei il repository e quindi cloni il

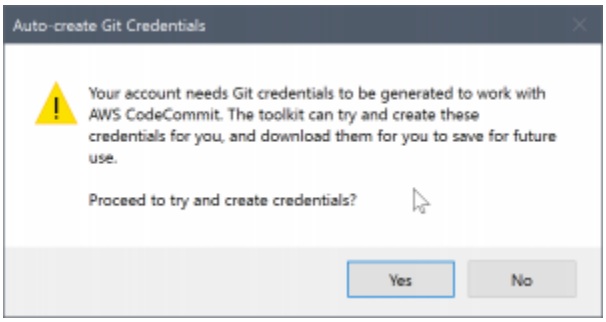
nuovo repository localmente, aggiungendo un commit iniziale per il file.gitignore, se ne stai utilizzando uno. È a questo punto che inizi a lavorare con il telecomando Git, quindi Toolkit for Visual Studio ora deve accedere alle credenziali Git descritte in precedenza.

Configurazione delle credenziali Git

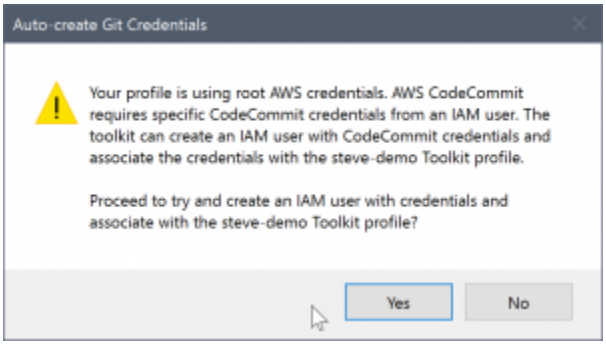
Fino a questo punto hai utilizzato chiavi di AWS accesso e chiavi segrete per richiedere al servizio di creare il tuo repository. Ora devi lavorare con Git stesso per eseguire l'effettiva operazione di clonazione e Git non comprende le chiavi di AWS accesso e segrete. Invece, devi fornire a Git il nome utente e la password per utilizzarli su una connessione HTTPS con il telecomando.

Come indicato in Configurazione delle credenziali Git, le credenziali Git che utilizzerai devono essere associate a un utente IAM. Non è possibile generarle per le credenziali root. Dovresti sempre configurare i tuoi profili di AWS credenziali in modo che contengano le chiavi segrete e di accesso utente IAM e non le chiavi root. Il Toolkit for Visual Studio può tentare di configurare le credenziali Git AWS CodeCommit per te e AWS associarle al profilo di credenziali che hai usato per connetterti in Team Explorer in precedenza.

Quando scegli OK nella finestra di dialogo Crea un nuovo AWS CodeCommit repository e crei correttamente il repository, Toolkit for Visual Studio controlla AWS il profilo delle credenziali connesso in Team Explorer per determinare se le credenziali Git AWS CodeCommit for esistono e sono associate localmente al profilo. In tal caso, il Toolkit for Visual Studio indica a Team Explorer di iniziare l'operazione di clonazione sul nuovo repository. Se le credenziali Git non sono disponibili localmente, il Toolkit for Visual Studio controlla il tipo di credenziali dell'account utilizzate nella connessione in Team Explorer. Se le credenziali sono per un utente IAM, come consigliato, viene visualizzato il seguente messaggio.

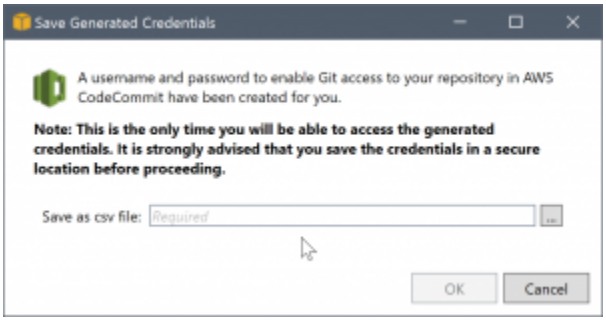


Se le credenziali sono credenziali root, viene invece visualizzato il seguente messaggio.



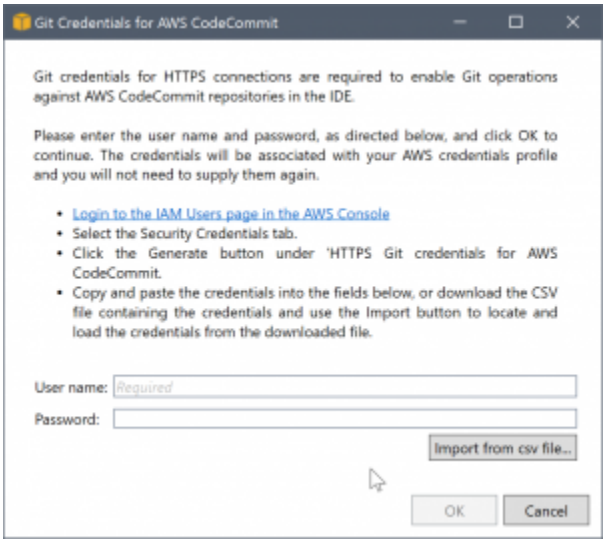
In entrambi i casi, il Toolkit for Visual Studio offre la possibilità di provare a creare le credenziali Git necessarie all'utente. Nel primo scenario, tutto ciò che deve creare è un set di credenziali Git per l'utente IAM. Quando è in uso un account root, Toolkit for Visual Studio tenta prima di creare un utente IAM e poi procede a creare le credenziali Git per quel nuovo utente. Se Toolkit for Visual Studio deve creare un nuovo utente, applica AWS CodeCommit la politica gestita da Power User a quel nuovo account utente. Questa politica consente l'accesso solo a AWS CodeCommit e consente di eseguire tutte le operazioni ad AWS CodeCommit eccezione dell'eliminazione del repository.

Quando crei le credenziali, puoi visualizzarle solo una volta. Pertanto, Toolkit for Visual Studio richiede di salvare le credenziali appena create come `.csv` file prima di continuare.



Anche questo è qualcosa che consigliamo vivamente e assicurati di salvarle in un luogo sicuro!

Potrebbero verificarsi casi in cui Toolkit for Visual Studio non è in grado di creare automaticamente le credenziali. Ad esempio, potresti aver già creato il numero massimo di set di credenziali Git per AWS CodeCommit (due) oppure potresti non avere diritti programmatici sufficienti per consentire a Toolkit for Visual Studio di eseguire il lavoro al posto tuo (se hai effettuato l'accesso come utente IAM). In questi casi, puoi accedere Console di gestione AWS a per gestire le credenziali o ottenerle dal tuo amministratore. È quindi possibile inserirle nella finestra di AWS CodeCommit dialogo Git Credentials for, visualizzata da Toolkit for Visual Studio.

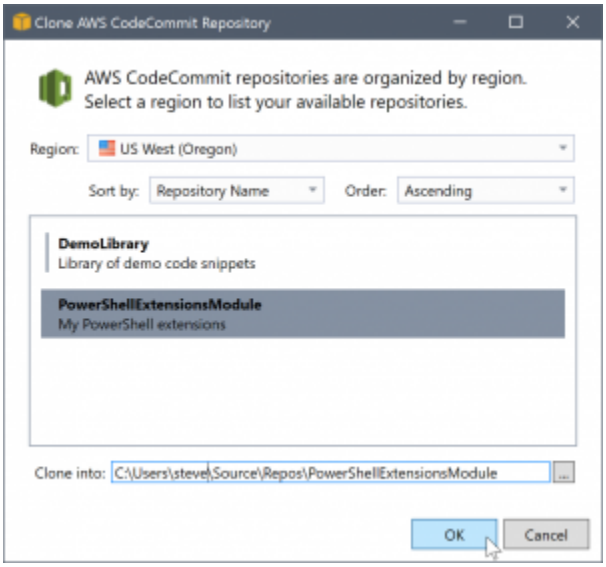


Ora che le credenziali per Git sono disponibili, l'operazione di clonazione per il nuovo repository procede (vedi l'indicazione di avanzamento per l'operazione all'interno di Team Explorer). Se hai scelto di applicare un `.gitignore` file predefinito, questo viene salvato nel repository con un commento di «Initial Commit».

Questo è tutto ciò che serve per impostare le credenziali e creare un repository all'interno di Team Explorer. Una volta inserite le credenziali richieste, quando creerete nuovi repository in futuro, tutto ciò che vedrete sarà la finestra di dialogo Create a New AWS CodeCommit Repository.

Clonazione di un repository

Per clonare un repository esistente, torna al pannello di connessione di Team Explorer. AWS CodeCommit Fai clic sul link Clone per aprire la finestra di dialogo Clone AWS CodeCommit Repository, quindi seleziona il repository da clonare e la posizione sul disco in cui desideri posizionarlo.



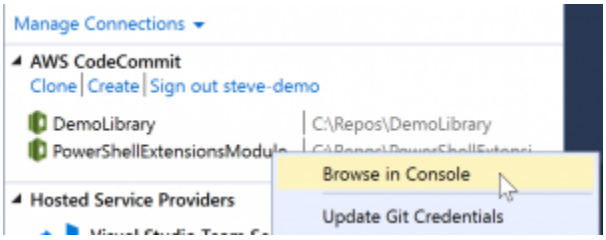
Una volta scelta la regione, Toolkit for Visual Studio interroga il servizio per individuare i repository disponibili in quell'area e li visualizza nell'elenco centrale della finestra di dialogo. Vengono inoltre visualizzati il nome e la descrizione facoltativa di ogni repository. È possibile riordinare l'elenco in base al nome del repository o alla data dell'ultima modifica e ordinarlo in ordine crescente o decrescente.

Dopo aver selezionato il repository, puoi scegliere la posizione in cui clonare. L'impostazione predefinita è la stessa posizione del repository utilizzata in altri plugin di Team Explorer, ma puoi cercare o inserire qualsiasi altra posizione. Per impostazione predefinita, il nome del repository ha il suffisso sul percorso selezionato. Tuttavia, se desideri un percorso specifico, modifica semplicemente la casella di testo dopo aver selezionato la cartella. Qualunque testo sia presente nella casella quando fai clic su OK sarà la cartella in cui troverai il repository clonato.

Dopo aver selezionato il repository e la posizione della cartella, fate clic su OK per procedere con l'operazione di clonazione. Proprio come con la creazione di un repository, puoi vedere lo stato di avanzamento dell'operazione di clonazione riportata in Team Explorer.

Utilizzo dei repository

Quando cloni o crei repository, nota che i repository locali per la connessione sono elencati nel pannello di connessione in Team Explorer sotto i link operativi. Queste voci offrono un modo comodo per accedere al repository per sfogliare i contenuti. Basta fare clic con il pulsante destro del mouse sul repository e scegliere Browse in Console.



Puoi anche usare Update Git Credentials per aggiornare le credenziali Git memorizzate associate al profilo delle credenziali. Questo è utile se hai ruotato le credenziali. Il comando apre la finestra di AWS CodeCommit dialogo Git Credentials for in cui è possibile inserire o importare le nuove credenziali.

Le operazioni Git sui repository funzionano come previsto. Puoi effettuare commit locali e, quando sei pronto per la condivisione, usi l'opzione Sync in Team Explorer. Poiché le credenziali Git sono già archiviate localmente e associate al nostro profilo di AWS credenziali connesso, non ci verrà richiesto di fornirle nuovamente per le operazioni sul telecomando. AWS CodeCommit

Utilizzo CodeArtifact in Visual Studio

AWS CodeArtifact è un servizio di archiviazione di artefatti completamente gestito che consente alle organizzazioni di archiviare e condividere in modo semplice e sicuro i pacchetti software utilizzati per lo sviluppo di applicazioni. È possibile utilizzarlo CodeArtifact con i più diffusi strumenti di compilazione e gestori di pacchetti come e.NET Core NuGet CLIs e Visual Studio. Puoi anche configurare CodeArtifact per estrarre i pacchetti da un archivio pubblico esterno come NuGet.org.

In CodeArtifact, i pacchetti vengono archiviati in repository che vengono poi archiviati all'interno di un dominio. AWS Toolkit for Visual Studio Semplifica la configurazione di Visual Studio con i tuoi CodeArtifact repository, semplificando l'utilizzo dei pacchetti in Visual Studio sia CodeArtifact direttamente che dal sito .org. NuGet

Aggiungi il tuo CodeArtifact repository come sorgente del pacchetto NuGet

Per utilizzare i pacchetti dal tuo CodeArtifact, dovrai aggiungere il tuo repository come sorgente di pacchetti in Package Manager in NuGet Visual Studio

Per aggiungere il tuo repository come sorgente del pacchetto

1. In AWS Explorer, accedi al tuo repository nel AWS CodeArtifactnodo.
2. Apri il menu contestuale (fai clic con il pulsante destro del mouse) per il repository che desideri aggiungere, quindi scegli Copy NuGet Source Endpoint.

3. Vai a Package Sources sotto il nodo NuGet Package Manager nel menu Strumenti > Opzioni.
4. In Package Sources, seleziona il segno più (+), modifica il nome e incolla l'URL dell'endpoint di NuGet origine che hai copiato in precedenza nel campo Source.
5. Seleziona la casella di controllo accanto alla fonte del pacchetto appena aggiunto per abilitarla.

> **Note**
>
> Ti consigliamo di aggiungere una connessione esterna a NuGet.org al tuo CodeArtifact e di disabilitare l'origine del pacchetto nuget.org in Visual Studio. Quando si utilizza una connessione esterna, tutte le dipendenze estratte da .org vengono archiviate in. NuGet CodeArtifact Se NuGet.org non funziona per qualsiasi motivo, i pacchetti necessari saranno ancora disponibili. Per ulteriori informazioni sulle connessioni esterne, consulta Aggiungere una connessione esterna nella Guida per l'AWS CodeArtifact utente.

6. Scegli OK per chiudere il menu.

Per ulteriori informazioni sull'utilizzo CodeArtifact con Visual Studio, vedi Uso CodeArtifact con Visual Studio nella Guida per l'AWS CodeArtifact utente.

Amazon RDS di Explorer AWS

Amazon Relational Database Service (Amazon RDS) è un servizio che consente di fornire e gestire sistemi di database relazionali SQL nel cloud. Amazon RDS supporta tre tipi di sistemi di database:

- MySQL Community Edition
- Oracle Database Enterprise edizione
- Microsoft SQL Server (edizioni Express, Standard o Web)

Per ulteriori informazioni, consultare la Guida per l'utente di Amazon RDS.

Molte delle funzionalità discusse qui sono disponibili anche tramite la console di AWS gestione per Amazon RDS.

Argomenti

- Avvia un'istanza di database Amazon RDS
- Creare un database Microsoft SQL Server in un'istanza RDS

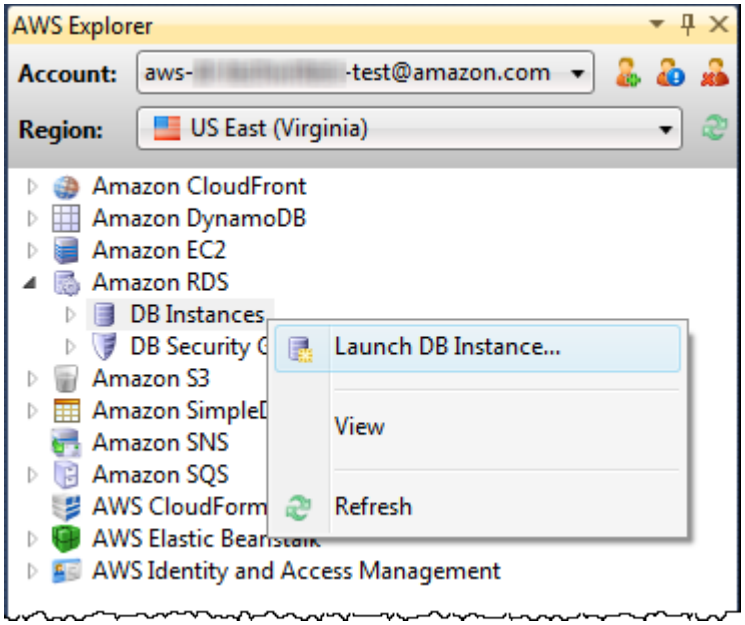
- Gruppi di sicurezza Amazon RDS

Avvia un'istanza di database Amazon RDS

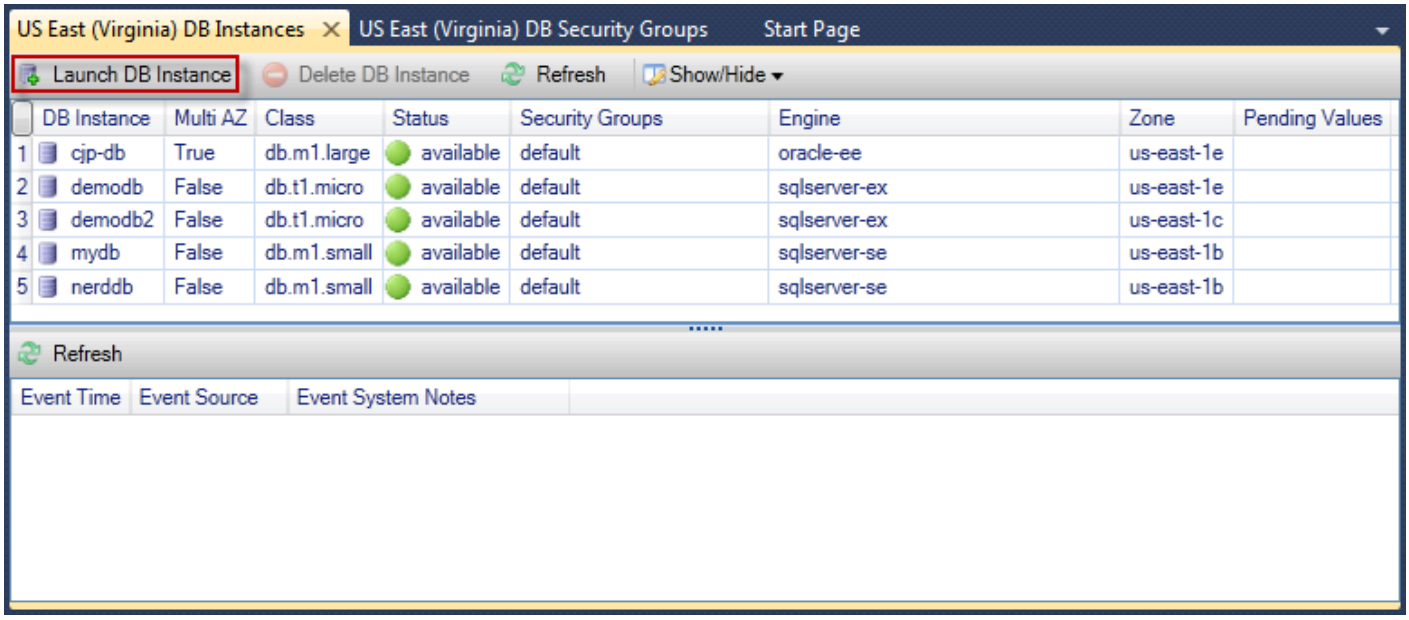
Con AWS Explorer, puoi avviare un'istanza di qualsiasi motore di database supportato da Amazon RDS. La procedura dettagliata seguente mostra l'esperienza utente per l'avvio di un'istanza di Microsoft SQL Server Standard Edition, ma l'esperienza utente è simile per tutti i motori supportati.

Per avviare un'istanza Amazon RDS

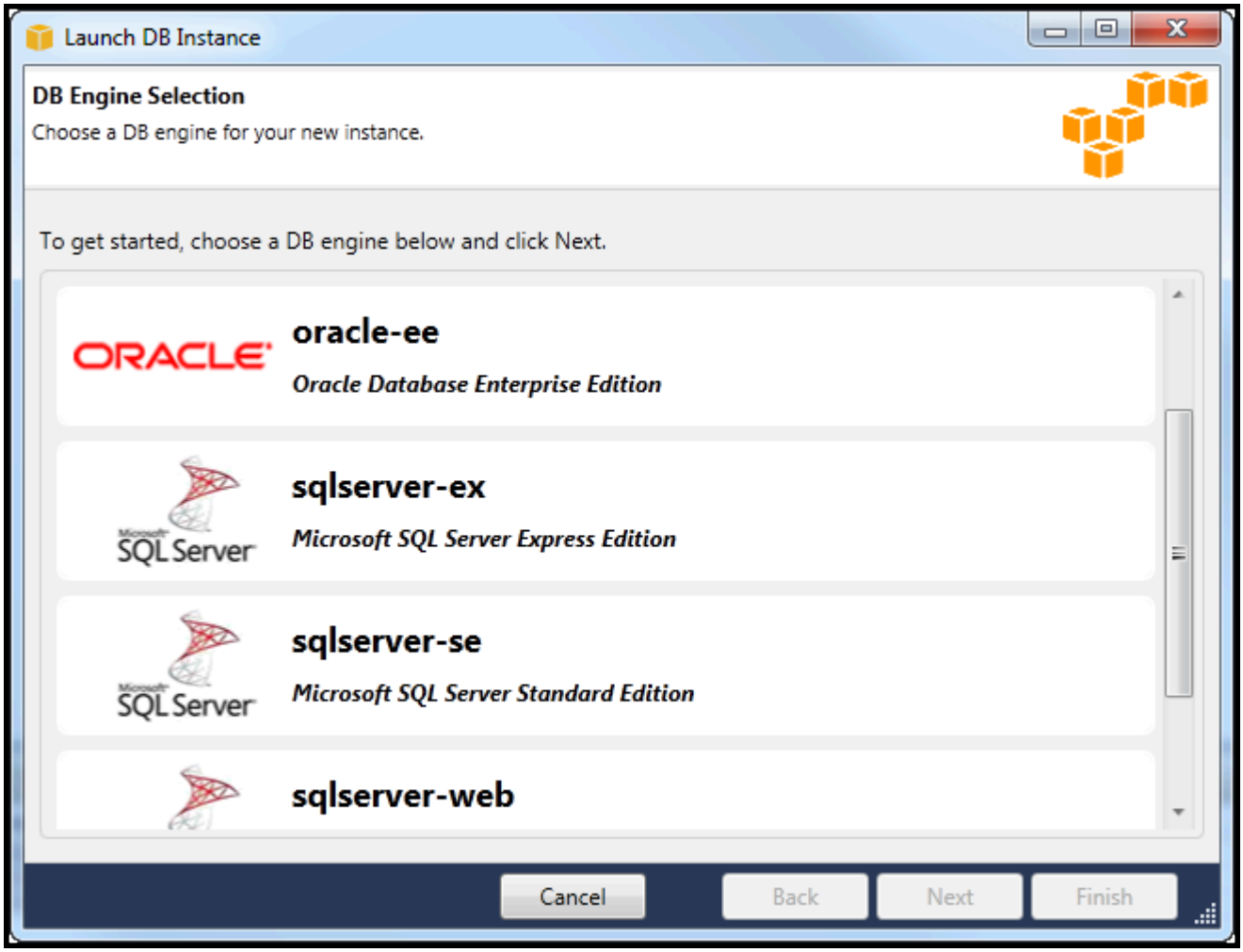
1. In AWS Explorer, apri il menu contestuale (con il pulsante destro del mouse) per il nodo Amazon RDS e scegli Launch DB Instance.



   In alternativa, nella scheda Istanze DB, scegli Launch DB Instance.



2. Nella finestra di dialogo DB Engine Selection, scegli il tipo di motore di database da avviare. Per questa procedura dettagliata, scegli Microsoft SQL Server Standard Edition (sqlserver-se), quindi scegli Avanti.



3. Nella finestra di dialogo DB Engine Instance Options, scegli le opzioni di configurazione.

   Nella sezione Opzioni e classe dell'istanza di DB Engine, puoi specificare le seguenti impostazioni.

   License Model (Modello di licenza)

Tipo di motore	Licenza
Microsoft SQL Server	licenza inclusa
MySql	general-public-license
Oracle	bring-your-own-license

Il modello di licenza varia a seconda del tipo di motore di database. Tipo di motore Licenza Microsoft SQL Server inclusa Oracle MySql general-public-license bring-your-own-license

Versione dell'istanza DB

Scegli la versione del motore di database che desideri utilizzare. Se è supportata solo una versione, viene selezionata per te.

Classe di istanza database

Scegli la classe di istanza per il motore di database. I prezzi per esempio le classi variano. Per ulteriori informazioni, consulta i prezzi di Amazon RDS.

Esegui una distribuzione multi-AZ

Seleziona questa opzione per creare un'implementazione Multi-AZ per una maggiore durabilità e disponibilità dei dati. Amazon RDS fornisce e mantiene una copia in standby del database in una zona di disponibilità diversa per il failover automatico in caso di interruzione pianificata o non pianificata. Per informazioni sui prezzi delle implementazioni Multi-AZ, consulta la sezione sui prezzi della pagina dei dettagli di Amazon RDS. Questa opzione non è supportata per Microsoft SQL Server.

Aggiorna automaticamente le versioni secondarie

Seleziona questa opzione per fare in AWS modo che esegua automaticamente gli aggiornamenti delle versioni minori sulle tue istanze RDS per te.

Nella sezione Istanza del database RDS, puoi specificare le seguenti impostazioni.

Allocated Storage (Storage allocato)

Motore	Minimo (GB)	Massimo (GB)
MySQL	5	1.024
Oracle Enterprise Edition	10	1.024
Edizione Microsoft SQL Server Express	30	1.024

Motore	Minimo (GB)	Massimo (GB)
Microsoft SQL Server Standard Edition	250	1.024
Edizione Web Microsoft SQL Server	30	1.024

I valori minimi e massimi per lo storage allocato dipendono dal tipo di motore di database. Motore minimo (GB) Massimo (GB) MySQL 5 1024 Oracle Enterprise Edition 10 1024 Microsoft SQL Server Express Edition 30 1024 Microsoft SQL Server Standard Edition 250 1024 Microsoft SQL Server Web Edition 30 1024 Microsoft SQL Server Web Edition 30 1024

DB Instance Identifier (Identificatore istanza database)

Specificare un nome per l'istanza del database. Questo nome non fa distinzione tra maiuscole e minuscole. Verrà visualizzato in formato minuscolo in Explorer. AWS

Master User Name (Nome utente master)

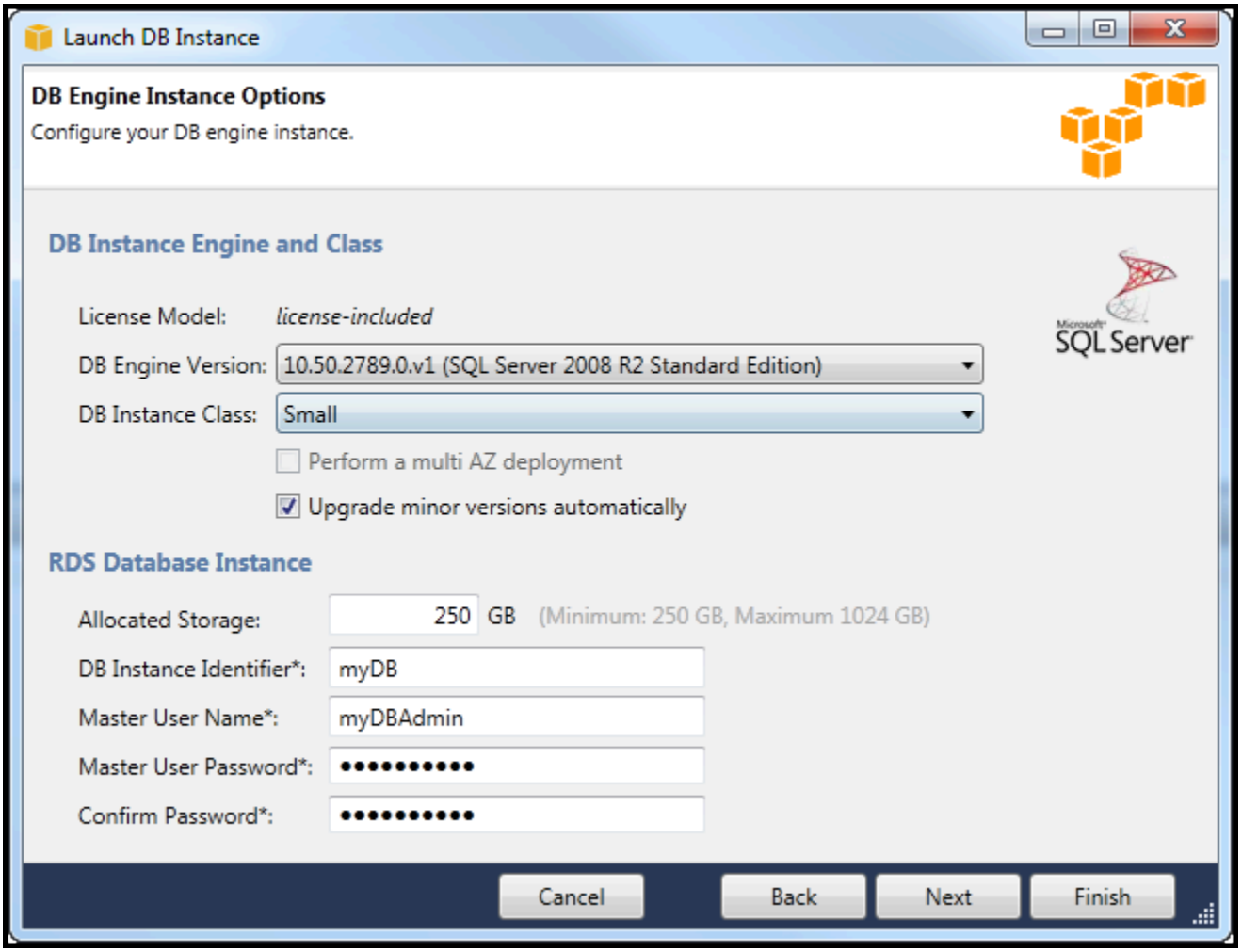
Digita un nome per l'amministratore dell'istanza del database.

Password utente master

Digitare una password per l'amministratore dell'istanza del database.

Conferma la password

Digita nuovamente la password per verificare che sia corretta.



1. Nella finestra di dialogo Opzioni aggiuntive, è possibile specificare le seguenti impostazioni.

   Database Port (Porta database)

   Questa è la porta TCP che l'istanza utilizzerà per comunicare sulla rete. Se il computer accede a Internet tramite un firewall, imposta questo valore su una porta attraverso la quale il firewall consente il traffico.

   Zona di disponibilità

   Utilizzate questa opzione se desiderate che l'istanza venga avviata in una particolare zona di disponibilità nella vostra regione. L'istanza di database specificata potrebbe non essere disponibile in tutte le zone di disponibilità di una determinata regione.

   Gruppo di sicurezza RDS

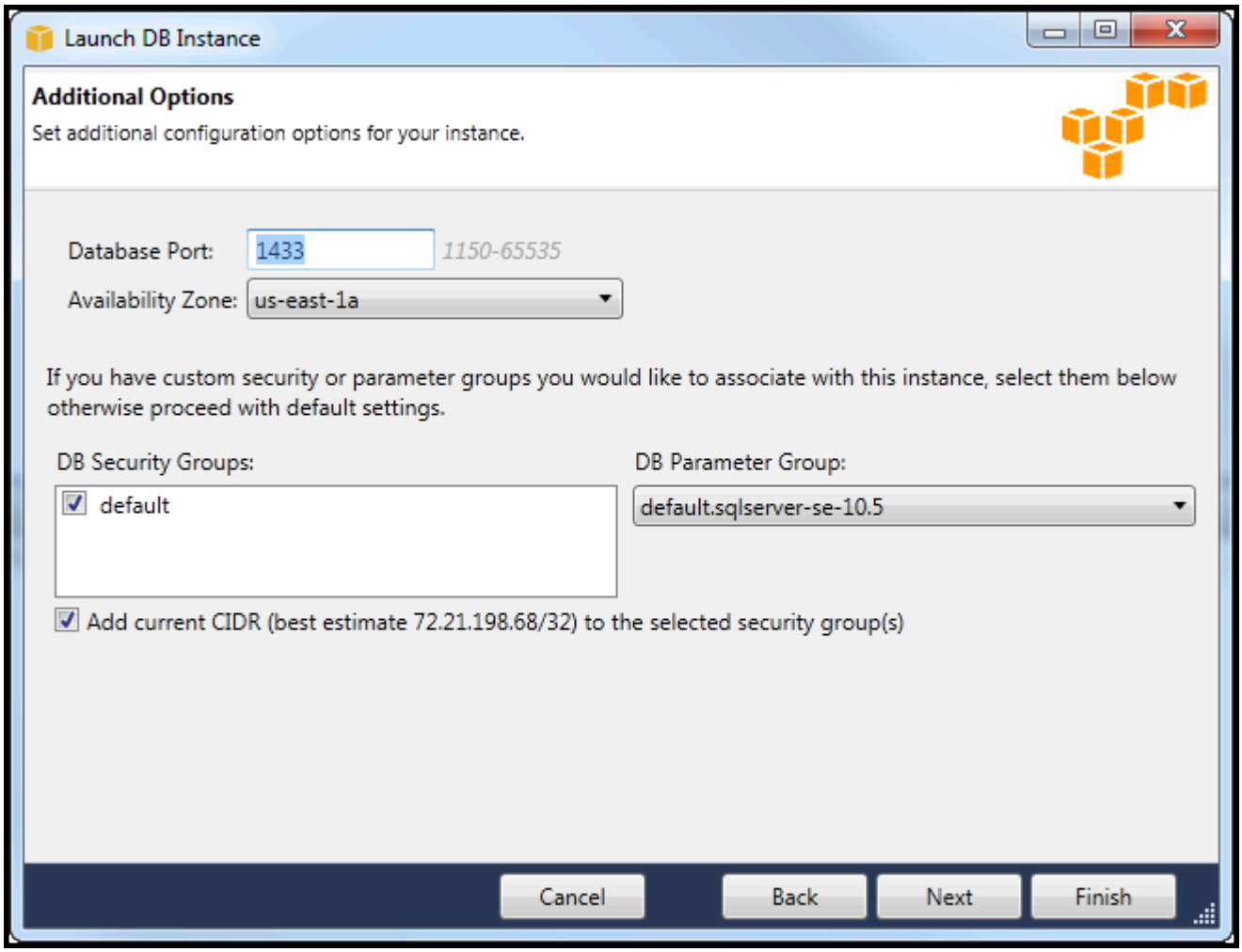
   Seleziona uno o più gruppi di sicurezza RDS da associare alla tua istanza. I gruppi di sicurezza RDS specificano l'indirizzo IP, le istanze Amazon EC2 Account AWS e a chi è consentito

accedere all'istanza. Per ulteriori informazioni sui gruppi di sicurezza RDS, consulta Amazon RDS Security Groups. Il Toolkit for Visual Studio tenta di determinare l'indirizzo IP corrente e offre la possibilità di aggiungere questo indirizzo ai gruppi di sicurezza associati all'istanza. Tuttavia, se il computer accede a Internet tramite un firewall, l'indirizzo IP generato dal Toolkit per il computer potrebbe non essere preciso. Per determinare l'indirizzo IP da utilizzare, rivolgetevi all'amministratore di sistema.

DB Parameter Group (Gruppo di parametri database)

(Facoltativo) Da questo elenco a discesa, scegliete un gruppo di parametri DB da associare all'istanza. I gruppi di parametri DB consentono di modificare la configurazione predefinita per l'istanza. Per ulteriori informazioni, consulta la Amazon Relational Database Service User Guide e questo articolo.

Dopo aver specificato le impostazioni in questa finestra di dialogo, scegli Avanti.

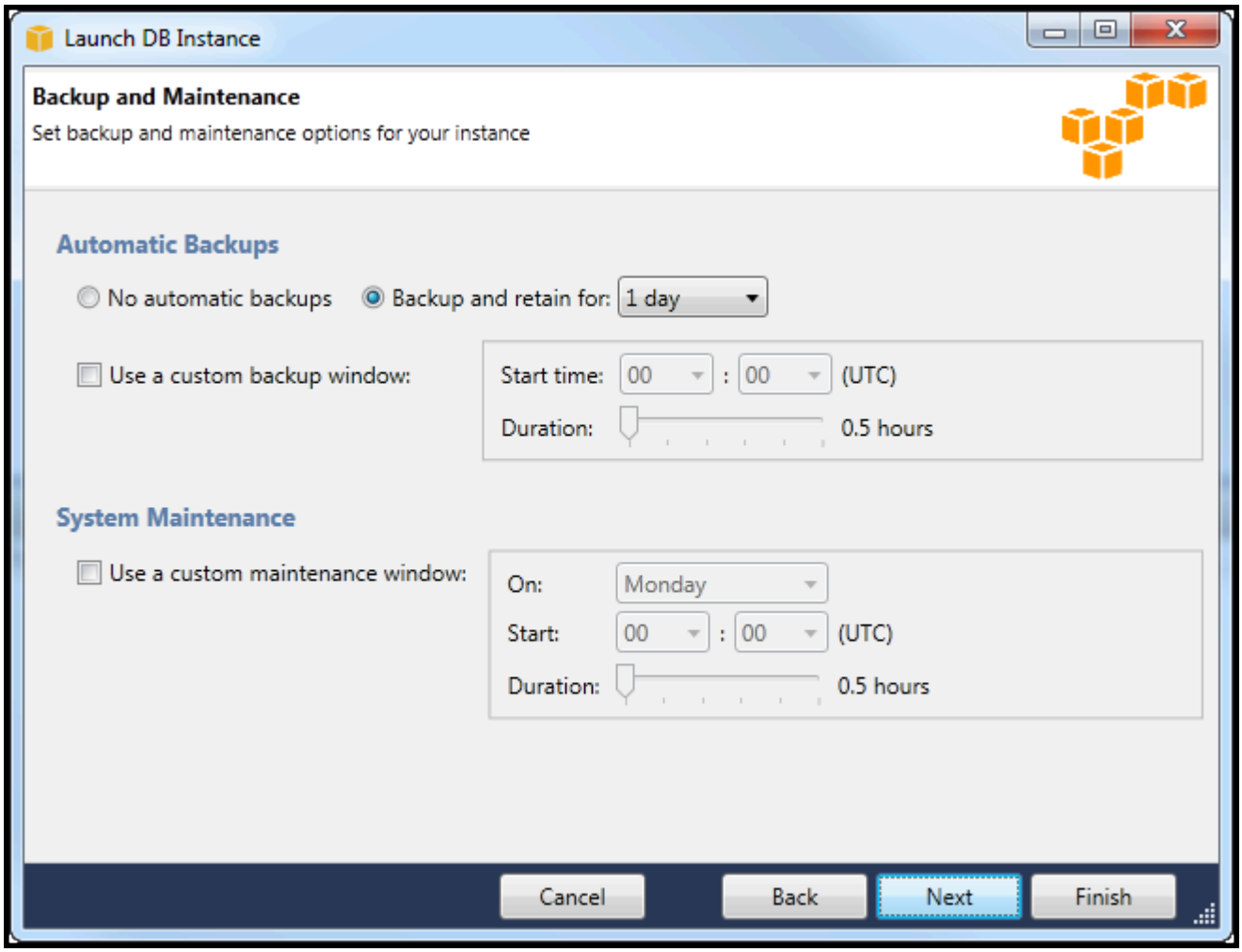


2. La finestra di dialogo Backup e manutenzione consente di specificare se Amazon RDS deve eseguire il backup dell'istanza e, in caso affermativo, per quanto tempo il backup deve essere conservato. Puoi anche specificare un intervallo di tempo durante il quale devono essere eseguiti i backup.

   Questa finestra di dialogo consente inoltre di specificare se desideri che Amazon RDS esegua la manutenzione del sistema sulla tua istanza. La manutenzione include patch di routine e aggiornamenti di versioni minori.

   La finestra temporale specificata per la manutenzione del sistema non può sovrapporsi alla finestra specificata per i backup.

   Scegli Next (Successivo).



3. L'ultima finestra di dialogo della procedura guidata consente di rivedere le impostazioni dell'istanza. Se è necessario modificare le impostazioni, utilizzare il pulsante Indietro. Se tutte le impostazioni sono corrette, scegli Avvia.

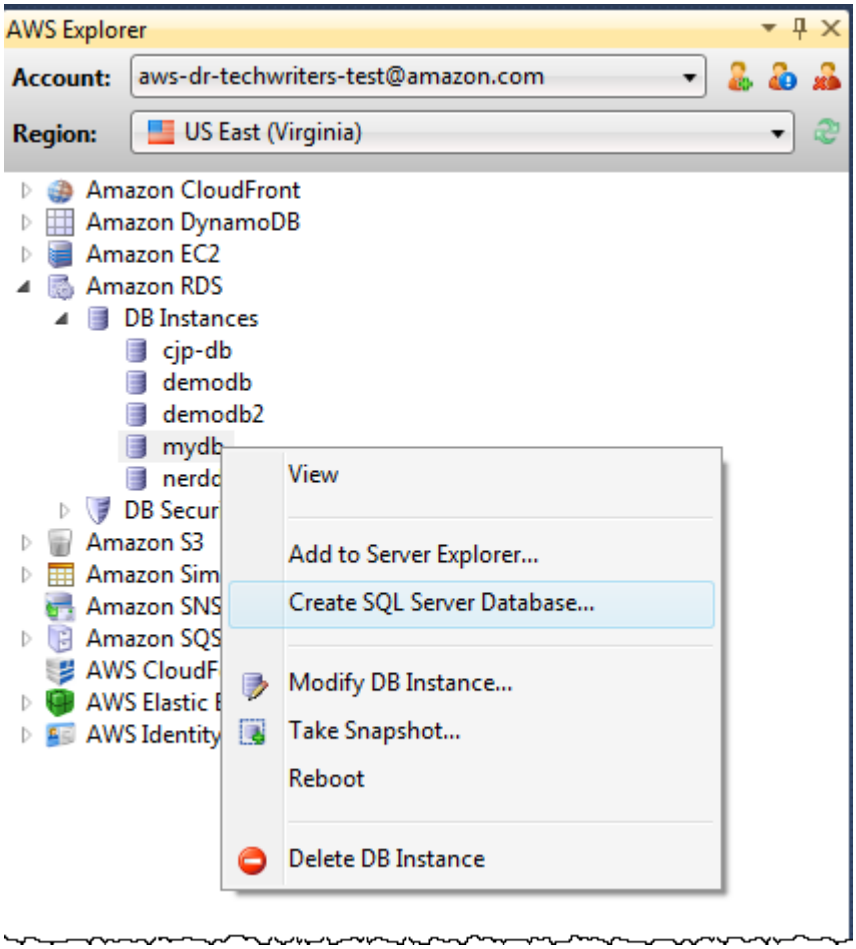
Creare un database Microsoft SQL Server in un'istanza RDS

Microsoft SQL Server è progettato in modo tale che, dopo aver avviato un'istanza Amazon RDS, sia necessario creare un database SQL Server nell'istanza RDS.

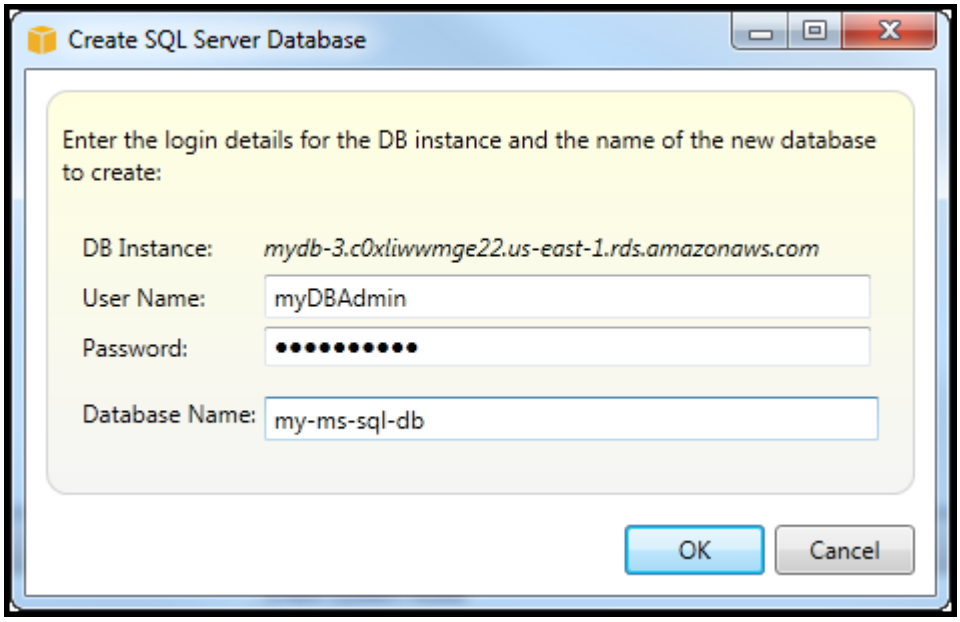
Per informazioni su come creare un'istanza Amazon RDS, consulta Launch an Amazon RDS Database Instance.

Per creare un database Microsoft SQL Server

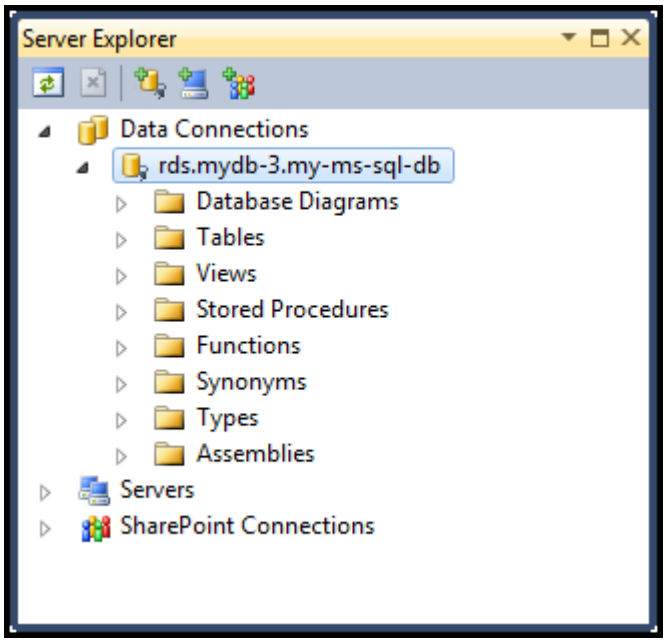
1. In AWS Explorer, apri il menu contestuale (con il pulsante destro del mouse) per il nodo che corrisponde all'istanza RDS per Microsoft SQL Server e scegli Crea database SQL Server.



2. Nella finestra di dialogo Crea database SQL Server, digita la password specificata al momento della creazione dell'istanza RDS, digita un nome per il database Microsoft SQL Server e quindi scegli OK.



3. Il Toolkit for Visual Studio crea il database Microsoft SQL Server e lo aggiunge a Visual Studio Server Explorer.



Gruppi di sicurezza Amazon RDS

I gruppi di sicurezza Amazon RDS consentono di gestire l'accesso di rete alle istanze Amazon RDS. Con i gruppi di sicurezza, specifichi set di indirizzi IP utilizzando la notazione CIDR e solo il traffico di rete proveniente da questi indirizzi viene riconosciuto dall'istanza Amazon RDS.

Sebbene funzionino in modo simile, i gruppi di sicurezza Amazon RDS sono diversi dai gruppi di sicurezza Amazon EC2. È possibile aggiungere un gruppo di sicurezza EC2 al gruppo di sicurezza RDS. Tutte le istanze EC2 che sono membri del gruppo di sicurezza EC2 sono quindi in grado di accedere alle istanze RDS che sono membri del gruppo di sicurezza RDS.

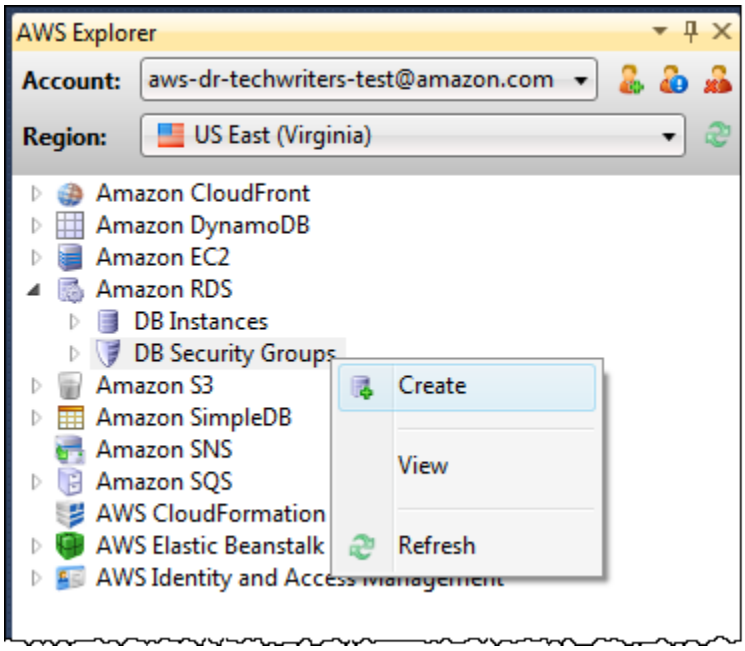
Per ulteriori informazioni sui gruppi di sicurezza Amazon RDS, consulta i gruppi di sicurezza RDS. Per ulteriori informazioni sui gruppi di sicurezza di Amazon EC2, consulta la Guida per l'utente di EC2.

Crea un gruppo di sicurezza Amazon RDS

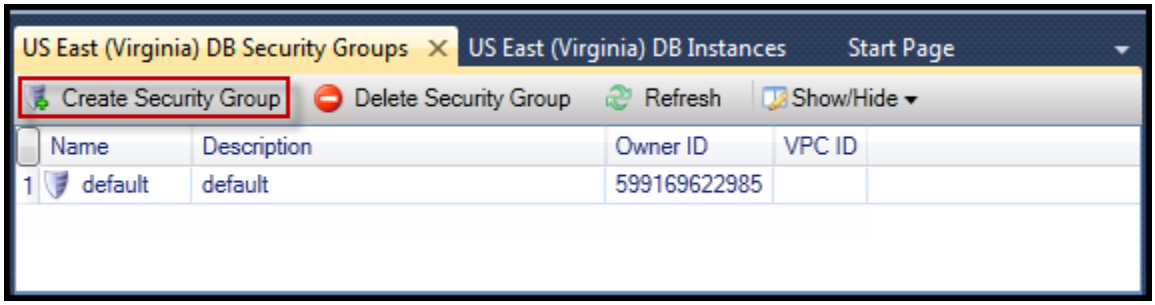
È possibile utilizzare Toolkit for Visual Studio per creare un gruppo di sicurezza RDS. Se si utilizza il AWS Toolkit per avviare un'istanza RDS, la procedura guidata consentirà di specificare un gruppo di sicurezza RDS da utilizzare con l'istanza. È possibile utilizzare la procedura seguente per creare il gruppo di sicurezza prima di avviare la procedura guidata.

Per creare un gruppo di sicurezza Amazon RDS

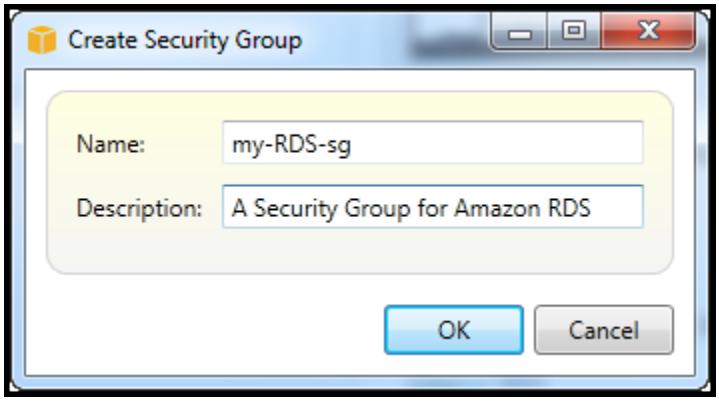
1. In AWS Explorer, espandi il nodo Amazon RDS, apri il menu contestuale (fai clic con il pulsante destro del mouse) per il sottonodo DB Security Groups e scegli Crea.



   In alternativa, nella scheda Gruppi di sicurezza, scegli Crea gruppo di sicurezza. Se questa scheda non è visualizzata, apri il menu contestuale (fai clic con il pulsante destro del mouse) per il sottonodo DB Security Groups e scegli Visualizza.



2. Nella finestra di dialogo Crea gruppo di sicurezza, digitate un nome e una descrizione per il gruppo di sicurezza, quindi scegliete OK.



Impostazione delle autorizzazioni di accesso per un gruppo di sicurezza Amazon RDS

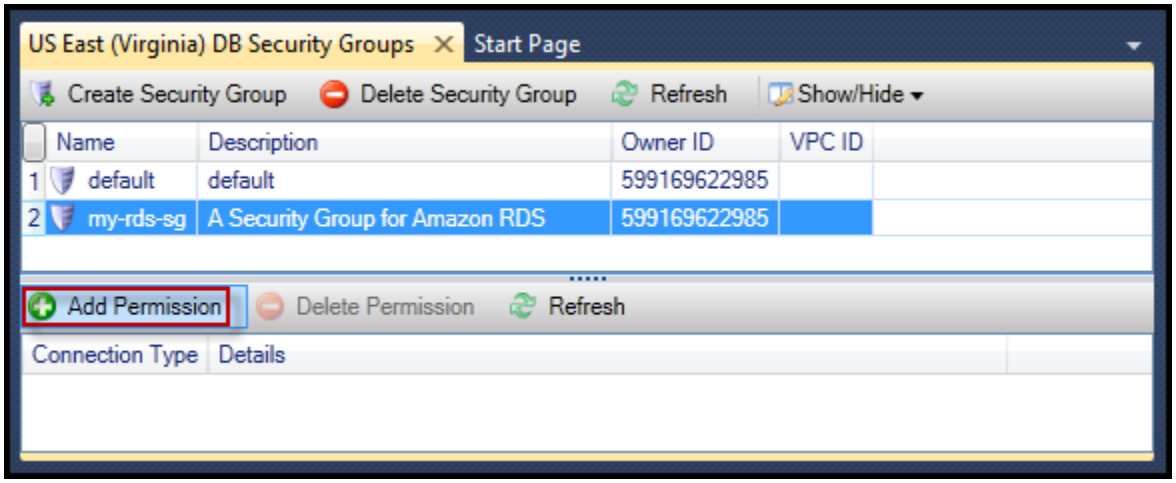
Per impostazione predefinita, un nuovo gruppo di sicurezza Amazon RDS non fornisce accesso alla rete. Per abilitare l'accesso alle istanze Amazon RDS che utilizzano il gruppo di sicurezza, utilizza la seguente procedura per impostarne le autorizzazioni di accesso.

Per impostare l'accesso per un gruppo di sicurezza Amazon RDS

1. Nella scheda Gruppi di sicurezza, scegli il gruppo di sicurezza dalla visualizzazione a elenco. Se il gruppo di sicurezza non compare nell'elenco, scegli Aggiorna. Se il gruppo di sicurezza continua a non apparire nell'elenco, verifica di visualizzare l'elenco per l' AWS area corretta. Le schede dei gruppi di sicurezza nel AWS Toolkit sono specifiche della regione.

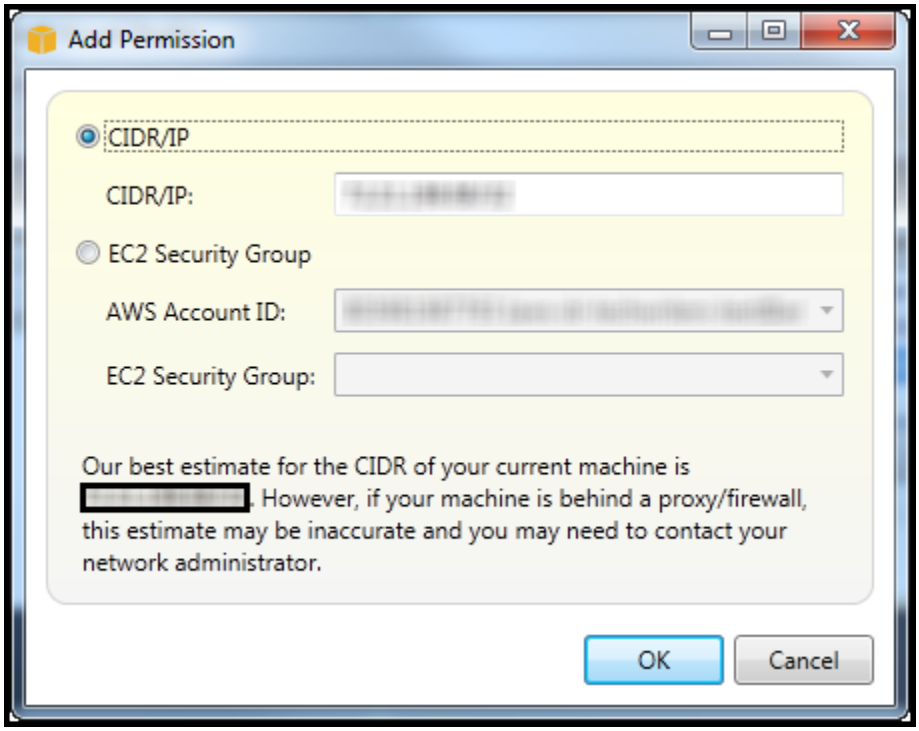
   Se non viene visualizzata alcuna scheda del gruppo di sicurezza, in AWS Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) per il sottonodo DB Security Groups e scegli Visualizza.

2. Scegli Add Permission (Aggiungi autorizzazioni).



pulsante Aggiungi autorizzazioni nella scheda Gruppi di sicurezza

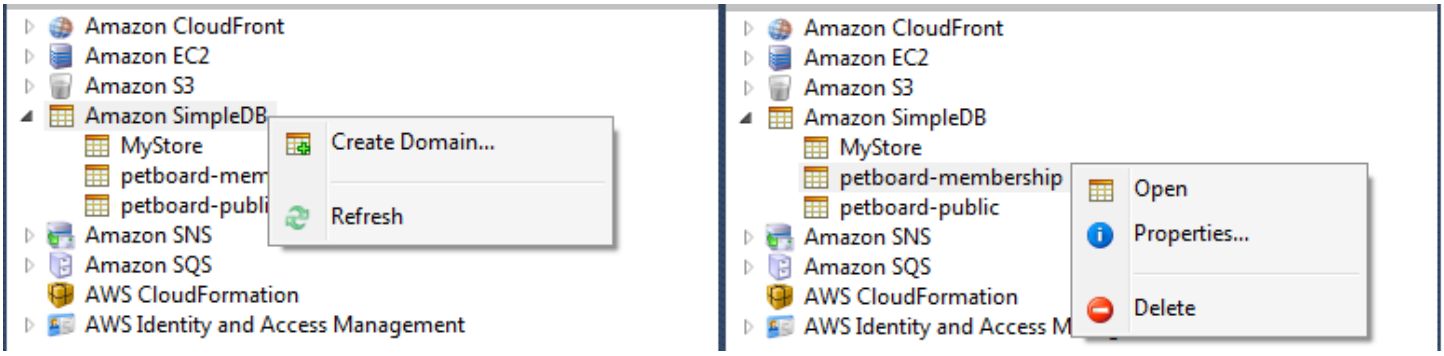
3. Nella finestra di dialogo Aggiungi autorizzazione, puoi utilizzare la notazione CIDR per specificare quali indirizzi IP possono accedere alla tua istanza RDS oppure puoi specificare quali gruppi di sicurezza EC2 possono accedere alla tua istanza RDS. Quando scegli EC2 Security Group, puoi specificare l'accesso per tutte le istanze EC2 associate a un Account AWS have access oppure puoi scegliere un gruppo di sicurezza EC2 dall'elenco a discesa.



Il AWS Toolkit tenta di determinare l'indirizzo IP dell'utente e di compilare automaticamente la finestra di dialogo con le specifiche CIDR appropriate. Tuttavia, se il computer accede a Internet tramite un firewall, il CIDR determinato dal Toolkit potrebbe non essere preciso.

Utilizzo di Amazon SimpleDB di AWS Explorer

AWS Explorer visualizza tutti i domini Amazon SimpledB associati all'account attivo. AWS Da AWS Explorer, puoi creare o eliminare domini Amazon SimpleDB.

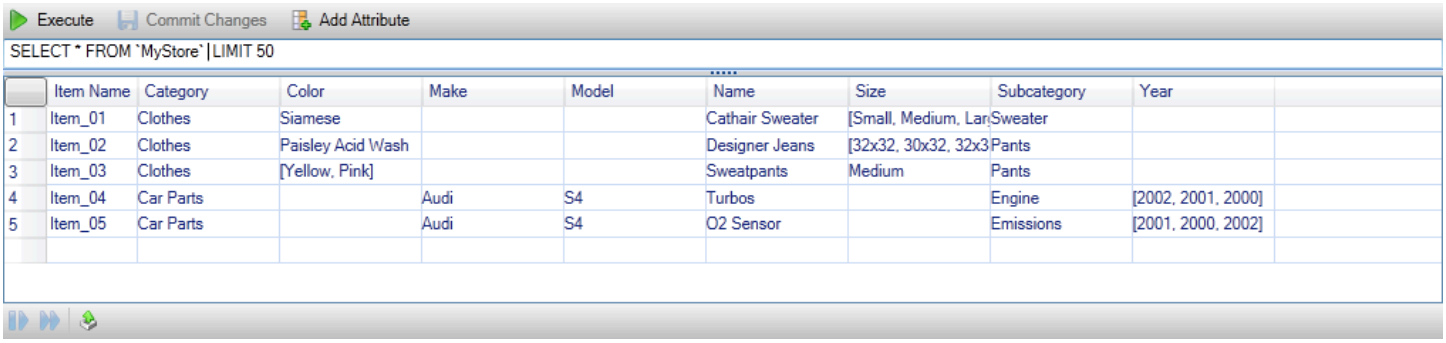


Create, delete, or open Amazon SimpleDB domains associated with your account

Esecuzione di interrogazioni e modifica dei risultati

AWS Explorer può anche visualizzare una visualizzazione a griglia di un dominio Amazon SimpledB da cui è possibile visualizzare gli elementi, gli attributi e i valori in quel dominio. Puoi eseguire query in modo che venga visualizzato solo un sottoinsieme degli elementi del dominio. Facendo doppio clic su una cella, è possibile modificare i valori dell'attributo corrispondente dell'elemento. Puoi anche aggiungere nuovi attributi al dominio.

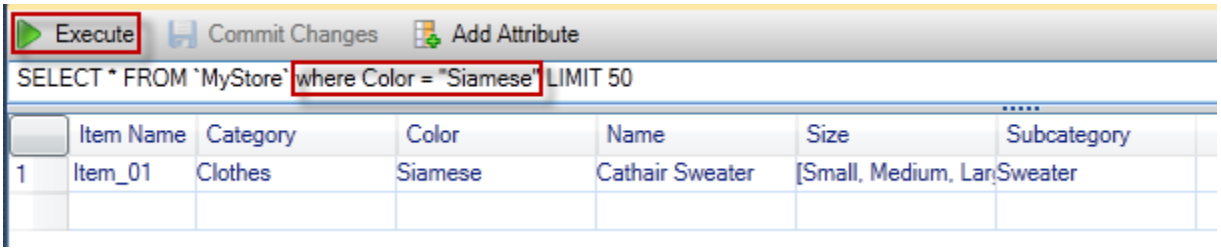
Il dominio visualizzato qui proviene dall'esempio di Amazon SimpleDB incluso in. AWS SDK per .NET



	Item Name	Category	Color	Make	Model	Name	Size	Subcategory	Year
1	Item_01	Clothes	Siamese			Cathair Sweater	[Small, Medium, Lar	Sweater	
2	Item_02	Clothes	Paisley Acid Wash			Designer Jeans	[32x32, 30x32, 32x3	Pants	
3	Item_03	Clothes	[Yellow, Pink]			Sweatpants	Medium	Pants	
4	Item_04	Car Parts		Audi	S4	Turbos		Engine	[2002, 2001, 2000]
5	Item_05	Car Parts		Audi	S4	O2 Sensor		Emissions	[2001, 2000, 2002]

Amazon SimpleDB grid view

Per eseguire un'interrogazione, modificatela nella casella di testo nella parte superiore della visualizzazione a griglia, quindi scegliete Esegui. La visualizzazione viene filtrata per mostrare solo gli elementi che corrispondono alla query.

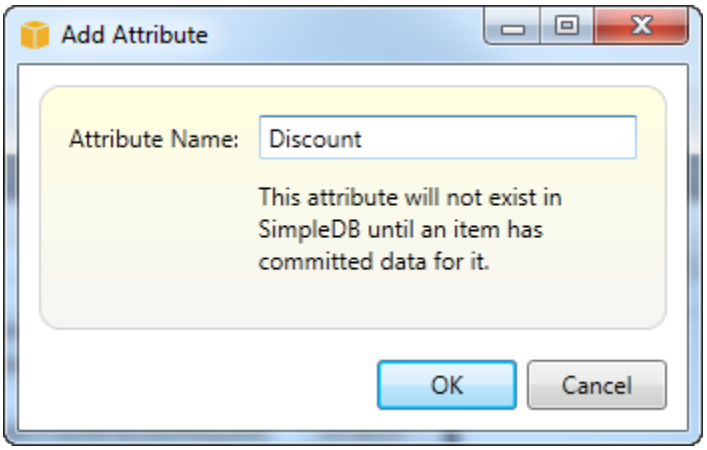


Execute query from AWS Explorer

Per modificare i valori associati a un attributo, fai doppio clic sulla cella corrispondente, modifica i valori e quindi scegli Conferma modifiche.

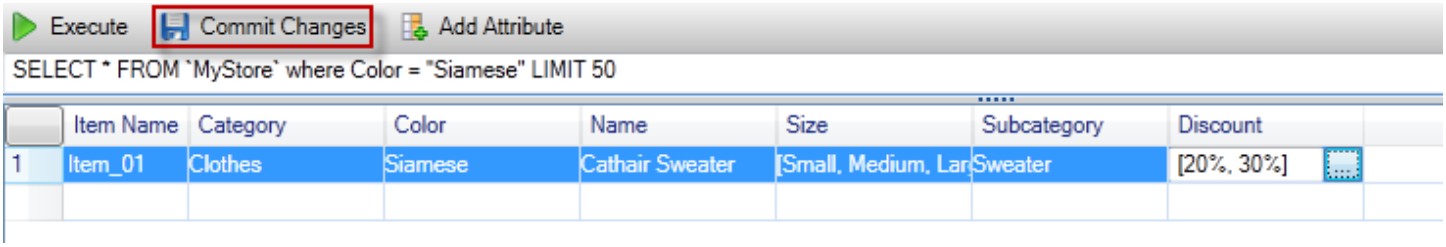
Aggiungere un attributo

Per aggiungere un attributo, nella parte superiore della vista, scegli Aggiungi attributo.



Aggiungi attributo dialog box

Per rendere l'attributo parte del dominio, devi aggiungere un valore ad almeno un elemento e quindi scegliere Conferma modifiche.



Commit changes for a new attribute

Impaginazione dei risultati delle query

Nella parte inferiore della visualizzazione sono presenti tre pulsanti.

Paginate and export buttons

I primi due pulsanti forniscono l'impaginazione dei risultati delle query. Per visualizzare una pagina aggiuntiva di risultati, scegliete il primo pulsante. Per visualizzare altre dieci pagine di risultati, scegli il secondo pulsante. In questo contesto, una pagina è uguale a 100 righe o al numero di risultati specificato dal valore LIMIT, se è incluso nella query.

Esporta in formato CSV

L'ultimo pulsante esporta i risultati correnti in un file CSV.

Utilizzo di Amazon SQS di Explorer AWS

Amazon Simple Queue Service (Amazon SQS) è un servizio di coda flessibile che consente lo scambio di messaggi tra diversi processi di esecuzione in un'applicazione software. Le code di Amazon SQS si trovano nell' AWS infrastruttura, ma i processi che trasmettono i messaggi possono essere localizzati localmente, su istanze Amazon EC2 o su una combinazione di queste. Amazon SQS è ideale per coordinare la distribuzione del lavoro su più computer.

Il Toolkit for Visual Studio consente di visualizzare le code Amazon SQS associate all'account attivo, creare ed eliminare code e inviare messaggi tramite code. (Per account attivo, intendiamo l'account selezionato in Explorer.) AWS

Per ulteriori informazioni su Amazon SQS, consulta la sezione Introduzione a SQS nella documentazione. AWS

Creazione di una coda

Puoi creare una coda Amazon SQS da Explorer. AWS L'ARN e l'URL della coda si baseranno sul numero di account dell'account attivo e sul nome della coda specificato al momento della creazione.

Come creare una coda

1. In AWS Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) per il nodo Amazon SQS, quindi scegli Crea coda.
2. Nella finestra di dialogo Crea coda, specifica il nome della coda, il timeout di visibilità predefinito e il ritardo di consegna predefinito. Il timeout di visibilità e il ritardo di consegna predefiniti sono

specificati in secondi. Il timeout di visibilità predefinito è il periodo di tempo in cui un messaggio sarà invisibile ai potenziali processi di ricezione dopo che un determinato processo lo ha acquisito. Il ritardo di recapito predefinito è il periodo di tempo che intercorre tra il momento in cui il messaggio viene inviato al momento in cui diventa visibile per la prima volta ai potenziali processi di ricezione.

3. Scegli OK. La nuova coda verrà visualizzata come sottonodo nel nodo Amazon SQS.

Eliminazione di una coda

Puoi eliminare le code esistenti da Explorer. AWS Se si elimina una coda, tutti i messaggi associati alla coda non sono più disponibili.

Come eliminare una coda

1. In AWS Explorer, apri i menu contestuali (fai clic con il pulsante destro del mouse) per la coda che desideri eliminare, quindi scegli Elimina.

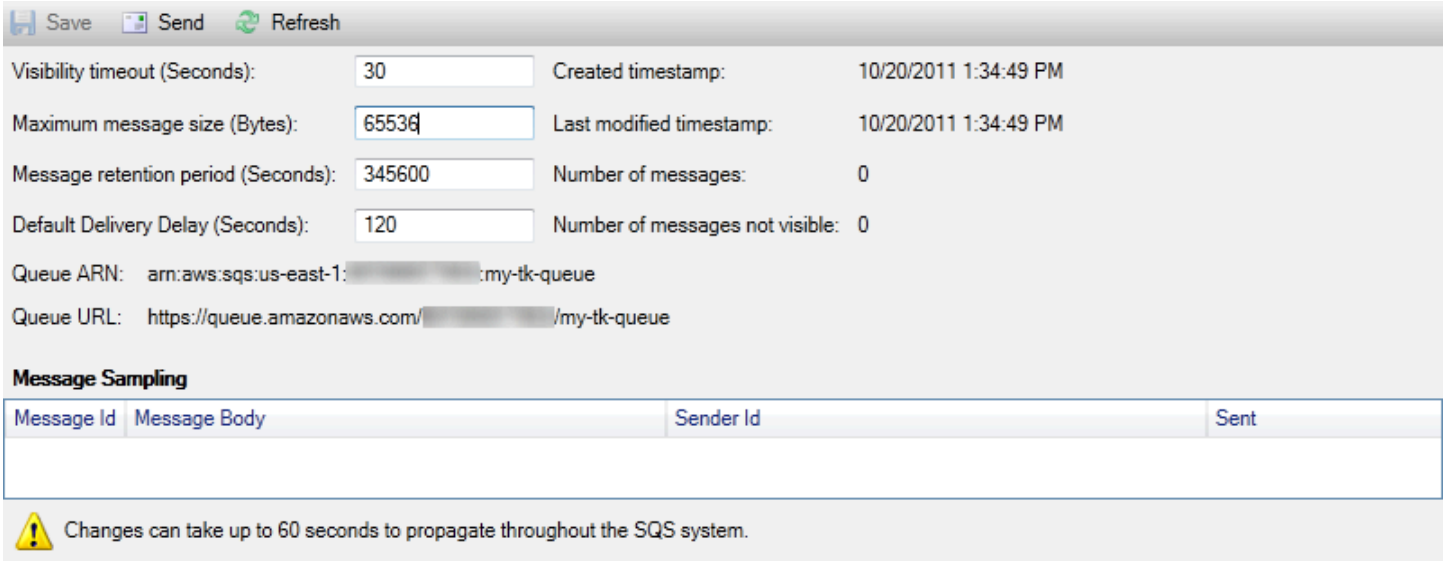
Gestione delle proprietà della coda

È possibile visualizzare e modificare le proprietà di qualsiasi coda visualizzata in AWS Explorer. È inoltre possibile inviare messaggi alla coda da questa visualizzazione delle proprietà.

Per gestire le proprietà della coda

- In AWS Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) per la coda di cui desideri gestire le proprietà, quindi scegli Visualizza coda.

  Dalla visualizzazione delle proprietà della coda, puoi modificare il timeout di visibilità, la dimensione massima dei messaggi, il periodo di conservazione dei messaggi e il ritardo di consegna predefinito. Il ritardo di recapito predefinito può essere ignorato quando si invia un messaggio. Nella schermata seguente, il testo oscurato è il componente del numero di account dell'ARN e dell'URL della coda.



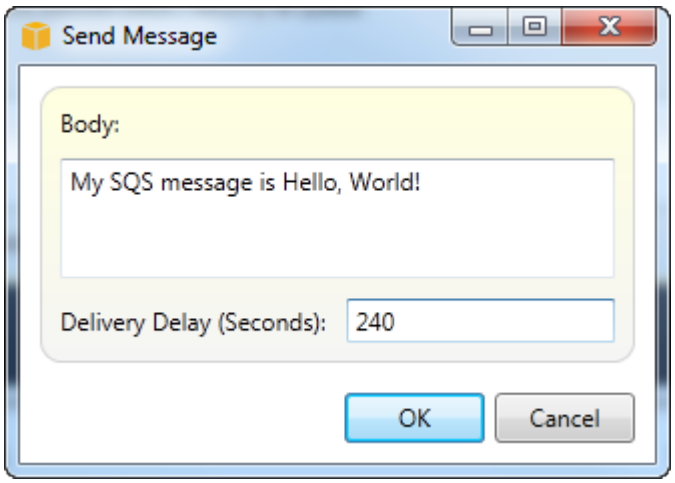
SQS queue properties view

Invio di un messaggio a una coda

Dalla vista delle proprietà della coda, è possibile inviare un messaggio alla coda.

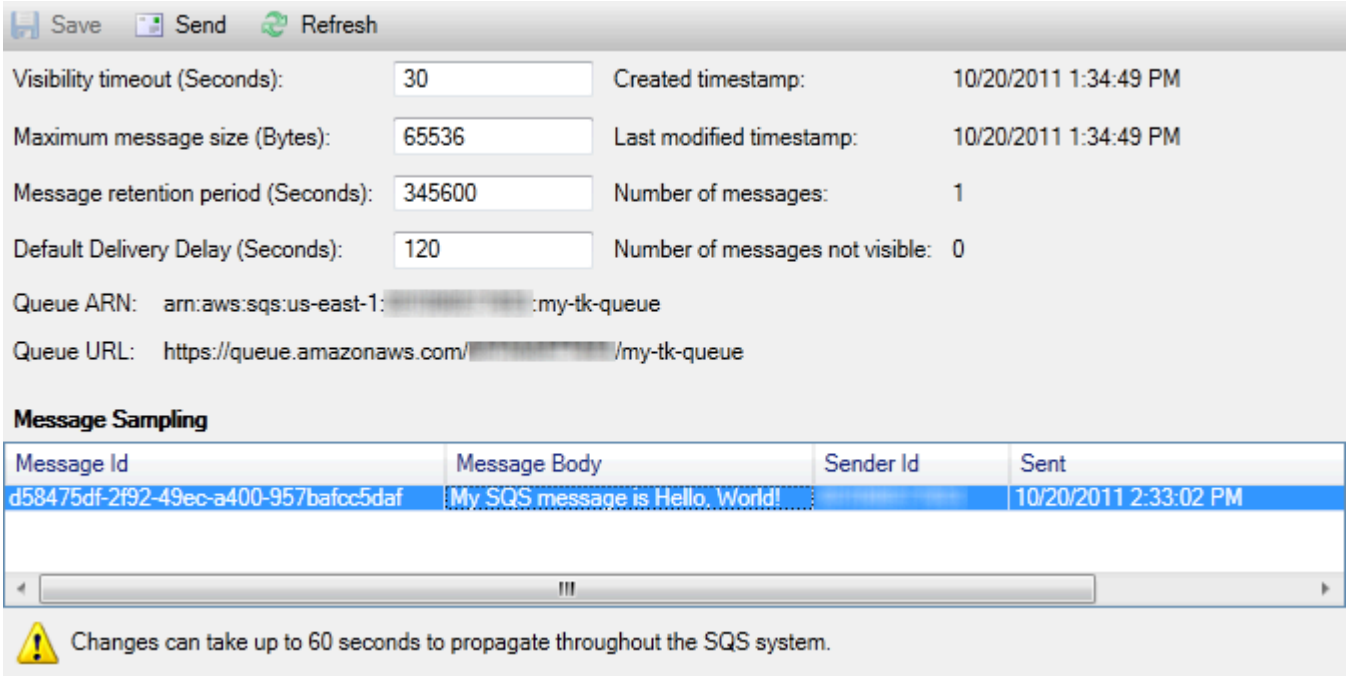
Come inviare un messaggio

1. Nella parte superiore della visualizzazione delle proprietà della coda, scegli il pulsante Invia.
2. Digita il messaggio. (Facoltativo) Inserisci un ritardo di consegna che sostituirà il ritardo di consegna predefinito per la coda. Nell'esempio seguente, abbiamo sostituito il ritardo con un valore di 240 secondi. Scegli OK.



Invia messaggio dialog box

3. Attendere circa 240 secondi (quattro minuti). Il messaggio verrà visualizzato nella sezione Message Sampling della vista delle proprietà della coda.



SQS properties view with sent message

Il timestamp nella vista delle proprietà della coda indica l'ora in cui hai scelto il pulsante Invia. Non include il ritardo. Pertanto, l'ora in cui il messaggio appare nella coda ed è disponibile per i destinatari potrebbe essere successiva a questo timestamp. Il timestamp viene visualizzato nell'ora locale del computer.

Identity and Access Management

AWS Identity and Access Management (IAM) ti consente di gestire in modo più sicuro l'accesso alle tue risorse Account AWS e alle tue risorse. Con IAM, puoi creare più utenti nella tua directory principale (root). Account AWS Questi utenti possono avere le proprie credenziali: password, ID della chiave di accesso e chiave segreta, ma tutti gli utenti IAM condividono un unico numero di account.

Puoi gestire il livello di accesso alle risorse di ogni utente IAM allegando le policy IAM all'utente. Ad esempio, puoi allegare una policy a un utente IAM che consente all'utente di accedere al servizio Amazon S3 e alle risorse correlate nel tuo account, ma che non fornisce l'accesso ad altri servizi o risorse.

Per una gestione degli accessi più efficiente, puoi creare gruppi IAM, che sono raccolte di utenti. Quando alleghi una policy al gruppo, questa avrà effetto su tutti gli utenti che fanno parte di quel gruppo.

Oltre a gestire le autorizzazioni a livello di utente e gruppo, IAM supporta anche il concetto di ruoli IAM. Come utenti e gruppi, puoi allegare policy ai ruoli IAM. Puoi quindi associare il ruolo IAM a un'istanza Amazon EC2. Le applicazioni eseguite sull'istanza EC2 sono in grado di accedere AWS utilizzando le autorizzazioni fornite dal ruolo IAM. Per ulteriori informazioni sull'utilizzo dei ruoli IAM con il Toolkit, consulta Create an IAM Role. Per ulteriori informazioni su IAM, consulta la IAM User Guide.

Crea e configura un utente IAM

Gli utenti IAM ti consentono di concedere ad altri l'accesso al tuo Account AWS. Poiché sei in grado di associare policy agli utenti IAM, puoi limitare con precisione le risorse a cui un utente IAM può accedere e le operazioni che può eseguire su tali risorse.

Come best practice, tutti gli utenti che accedono a un Account AWS dovrebbero farlo come utenti IAM, anche il proprietario dell'account. Ciò garantisce che, se le credenziali di uno degli utenti IAM vengono compromesse, solo tali credenziali possano essere disattivate. Non è necessario disattivare o modificare le credenziali root dell'account.

Dal Toolkit for Visual Studio, puoi assegnare le autorizzazioni a un utente IAM allegando una policy IAM all'utente o assegnando l'utente a un gruppo. Gli utenti IAM assegnati a un gruppo ottengono le proprie autorizzazioni dalle politiche allegate al gruppo. Per ulteriori informazioni, consultare Creazione di un gruppo IAM e Aggiunta di un utente IAM a un gruppo IAM.

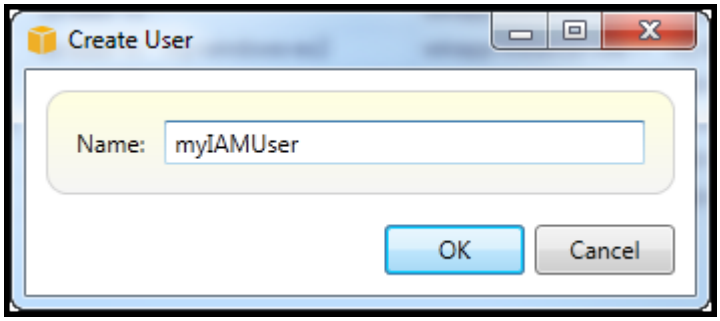
Dal Toolkit for Visual Studio, puoi anche AWS generare credenziali (ID chiave di accesso e chiave segreta) per l'utente IAM. Per ulteriori informazioni, consulta Generare credenziali per un utente IAM

Il Toolkit for Visual Studio supporta la specificazione delle credenziali utente IAM per l'accesso ai servizi tramite Explorer. AWS Poiché gli utenti IAM in genere non hanno accesso completo a tutti gli Amazon Web Services, alcune funzionalità di AWS Explorer potrebbero non essere disponibili. Se utilizzi AWS Explorer per modificare le risorse mentre l'account attivo è un utente IAM e poi passi l'account attivo all'account root, le modifiche potrebbero non essere visibili finché non aggiorni la vista in AWS Explorer. Per aggiornare la vista, scegli il pulsante refresh ().

Per informazioni su come configurare gli utenti IAM da Console di gestione AWS, consulta Working with Users and Groups nella IAM User Guide.

Per creare un utente IAM

1. In AWS Explorer, espandi il AWS Identity and Access Managementnodo, apri il menu contestuale (fai clic con il pulsante destro del mouse) per Utenti, quindi scegli Crea utente.
2. Nella finestra di dialogo Crea utente, digita un nome per l'utente IAM e scegli OK. Questo è il nome descrittivo di IAM. Per informazioni sui vincoli sui nomi per gli utenti IAM, consulta la IAM User Guide.



Create an IAM user

Il nuovo utente verrà visualizzato come sottonodo in Utenti sotto il AWS Identity and Access Managementnodo.

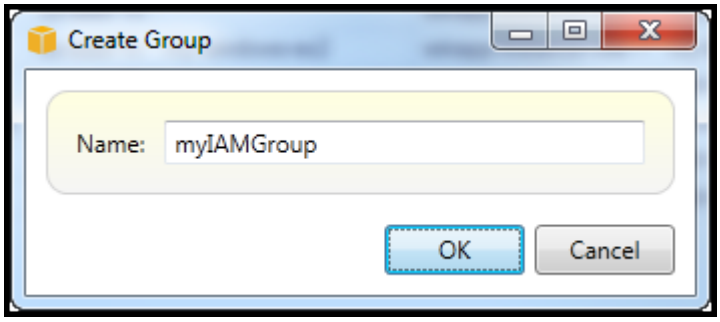
Per informazioni su come creare una policy e collegarla all'utente, consulta Create an IAM Policy.

Creazione di un gruppo IAM

I gruppi forniscono un modo per applicare le policy IAM a una raccolta di utenti. Per informazioni su come gestire utenti e gruppi IAM, consulta Working with Users and Groups nella IAM User Guide.

Come creare un gruppo IAM

1. In AWS Explorer, in Identity and Access Management, apri il menu contestuale (fai clic con il pulsante destro del mouse) per Gruppi e scegli Crea gruppo.
2. Nella finestra di dialogo Crea gruppo, digita un nome per il gruppo IAM e scegli OK.



Create IAM group

Il nuovo gruppo IAM verrà visualizzato nel sottonodo Groups di Identity and Access Management.

Per informazioni su come creare una policy e collegarla al gruppo IAM, consulta Create an IAM Policy.

Aggiunta di un utente IAM a un gruppo IAM

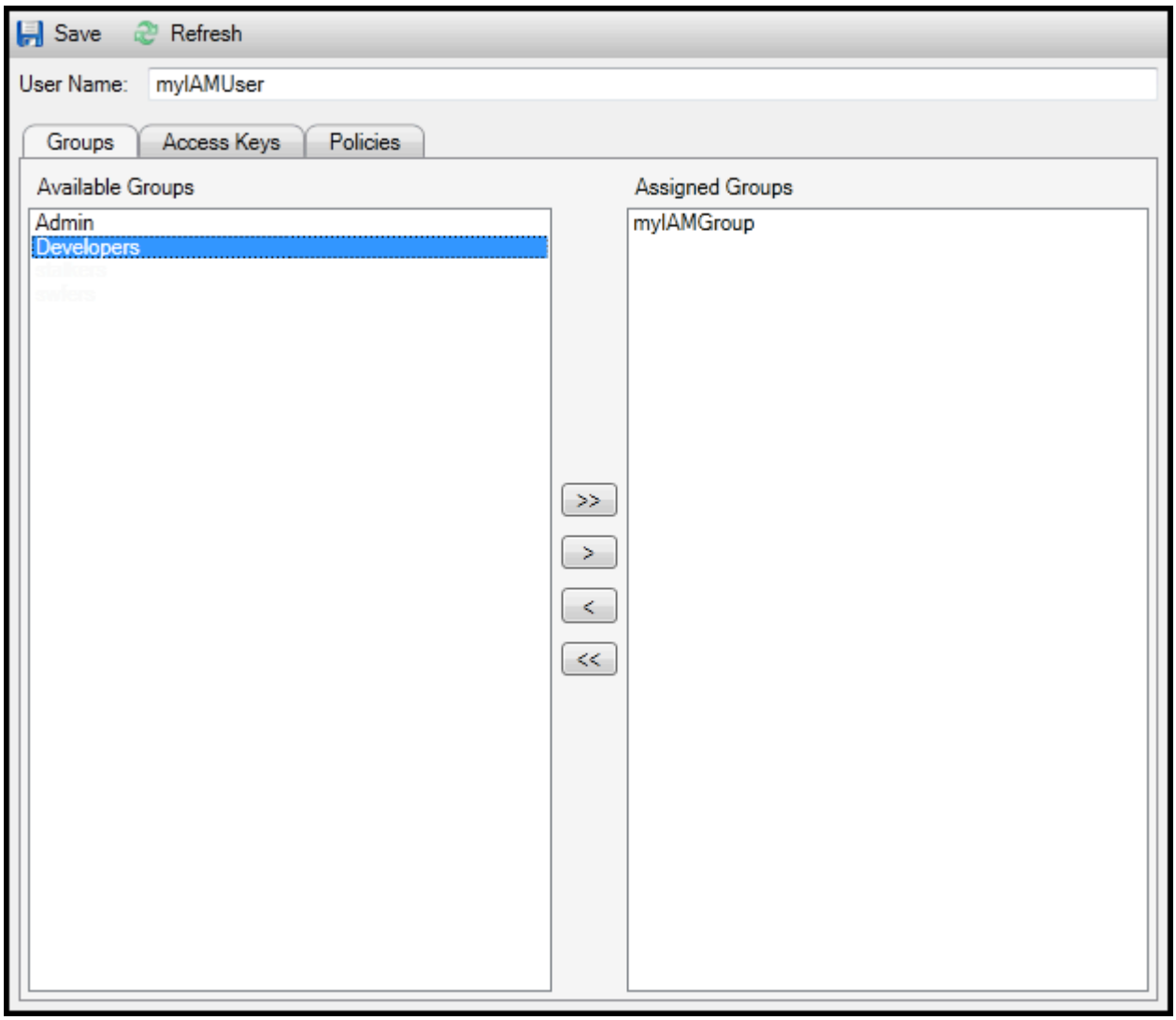
Gli utenti IAM che sono membri di un gruppo IAM ottengono le autorizzazioni di accesso dalle policy allegate al gruppo. Lo scopo di un gruppo IAM è semplificare la gestione delle autorizzazioni tra una raccolta di utenti IAM.

Per informazioni su come le policy collegate a un gruppo IAM interagiscono con le policy associate agli utenti IAM che sono membri di quel gruppo IAM, consulta Managing IAM Policies nella IAM User Guide.

In AWS Explorer, aggiungi gli utenti IAM ai gruppi IAM dal sottonodo Users, non dal sottonodo Groups.

Per aggiungere un utente IAM a un gruppo IAM

1. In AWS Explorer, in Identity and Access Management, apri il menu contestuale (fai clic con il pulsante destro del mouse) per Utenti e scegli Modifica.



Assign an IAM user to a IAM group

2. Il riquadro sinistro della scheda Gruppi mostra i gruppi IAM disponibili. Il riquadro di destra mostra i gruppi di cui l'utente IAM specificato è già membro.

   Per aggiungere l'utente IAM a un gruppo, nel riquadro di sinistra, scegli il gruppo IAM, quindi scegli il pulsante **>**.

   Per rimuovere l'utente IAM da un gruppo, nel riquadro di destra, scegli il gruppo IAM, quindi scegli il pulsante **<**.

   Per aggiungere l'utente IAM a tutti i gruppi IAM, scegli il pulsante **>>**. Allo stesso modo, per rimuovere l'utente IAM da tutti i gruppi, scegli il pulsante **<<**.

   Per scegliere più gruppi, sceglili in sequenza. Non è necessario tenere premuto il tasto Ctrl. Per cancellare un gruppo dalla selezione, è sufficiente sceglierlo una seconda volta.

3. Quando hai finito di assegnare l'utente IAM ai gruppi IAM, scegli Salva.

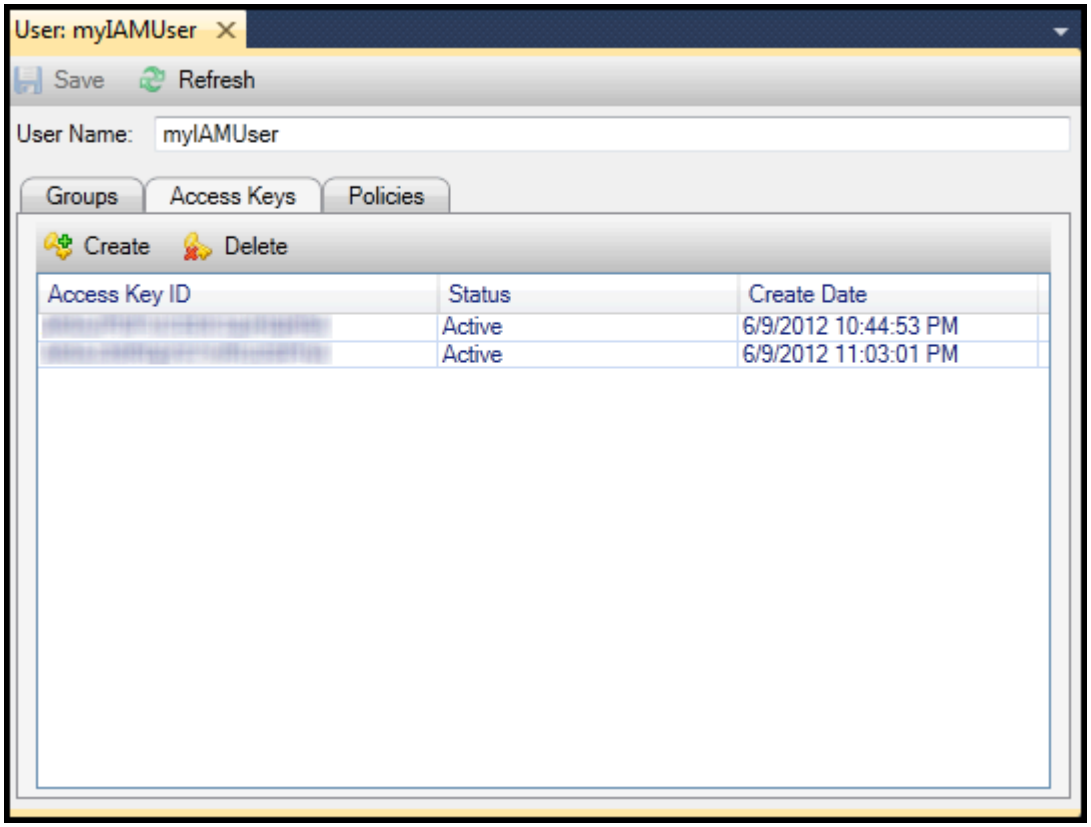
Genera credenziali per un utente IAM

Con Toolkit for Visual Studio, puoi generare l'ID della chiave di accesso e la chiave segreta utilizzati per effettuare chiamate AWS API a. Queste chiavi possono anche essere specificate per accedere ad Amazon Web Services tramite il Toolkit. Per ulteriori informazioni su come specificare le credenziali da utilizzare con il Toolkit, consulta creds. Per ulteriori informazioni su come gestire in modo sicuro le credenziali, consulta Best Practices for Managing Access Keys. AWS

Il Toolkit non può essere utilizzato per generare una password per un utente IAM.

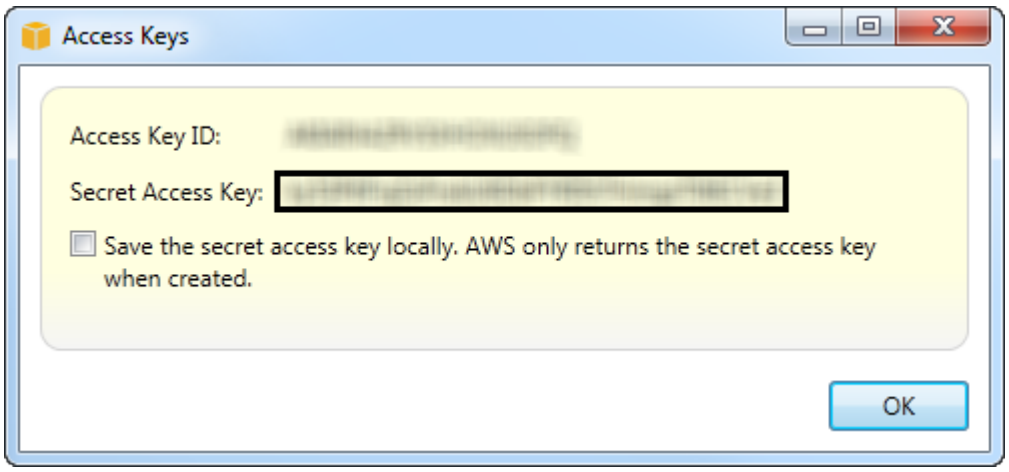
Per generare credenziali per un utente IAM

1. In AWS Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) per un utente IAM e scegli Modifica.



2. Per generare credenziali, nella scheda Access Keys, scegli Crea.

   Puoi generare solo due set di credenziali per ogni utente IAM. Se disponi già di due set di credenziali e devi crearne uno aggiuntivo, devi eliminare uno dei set esistenti.

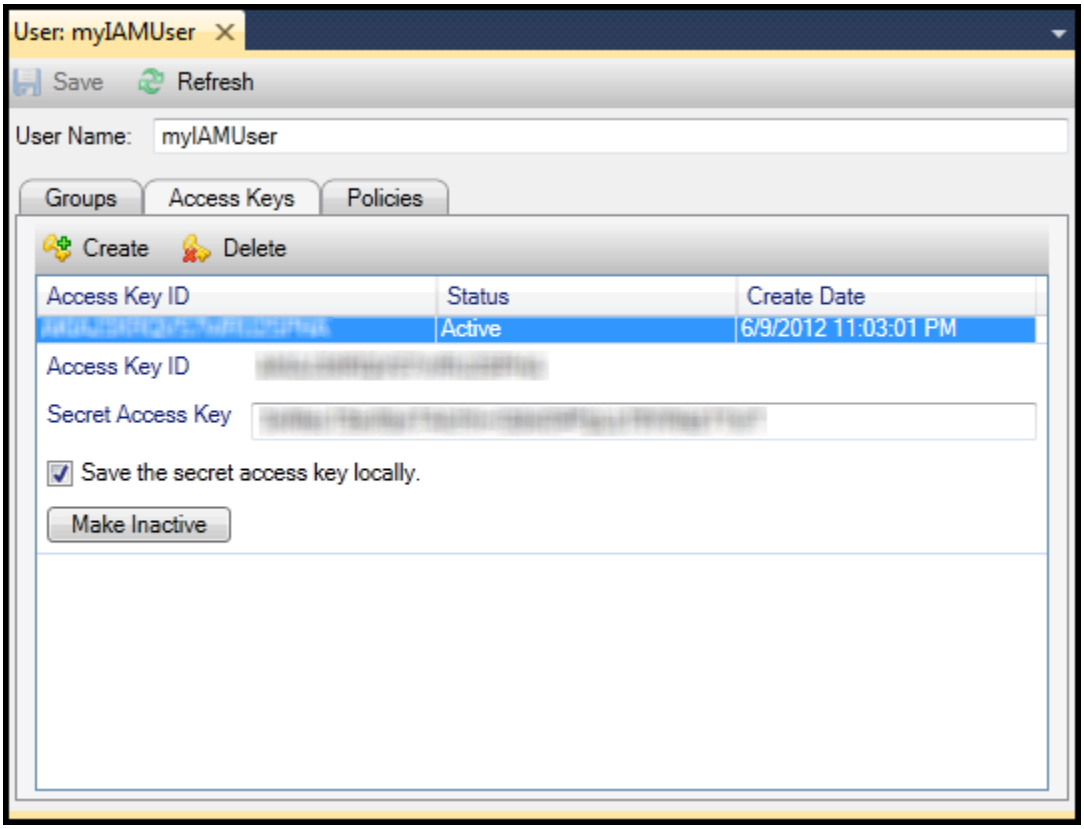


reate credentials for IAM user

Se desideri che il Toolkit salvi una copia crittografata della chiave di accesso segreta sull'unità locale, seleziona Salva la chiave di accesso segreta localmente. AWS restituisce la chiave di accesso segreta solo quando viene creata. È inoltre possibile copiare la chiave di accesso segreta dalla finestra di dialogo e salvarla in una posizione sicura.

3. Scegli OK.

Dopo aver generato le credenziali, è possibile visualizzarle dalla scheda Access Keys. Se hai selezionato l'opzione per fare in modo che il Toolkit salvi la chiave segreta localmente, questa verrà visualizzata qui.



Create credentials for IAM user

Se hai salvato tu stesso la chiave segreta e desideri che venga salvata anche dal Toolkit, nella casella Chiave di accesso segreta, digita la chiave di accesso segreta, quindi seleziona Salva la chiave di accesso segreta localmente.

Per disattivare le credenziali, scegli Rendi inattivo. (Puoi farlo se sospetti che le credenziali siano state compromesse. Puoi riattivare le credenziali se ti viene assicurato che siano sicure.)

Creazione di un ruolo IAM

Il Toolkit for Visual Studio supporta la creazione e la configurazione di ruoli IAM. Proprio come con utenti e gruppi, puoi collegare le policy ai ruoli IAM. Puoi quindi associare il ruolo IAM a un'istanza Amazon EC2. L'associazione con l'istanza EC2 viene gestita tramite un profilo di istanza, che è un contenitore logico per il ruolo. Alle applicazioni eseguite sull'istanza EC2 viene automaticamente concesso il livello di accesso specificato dalla policy associata al ruolo IAM. Questo è vero anche quando l'applicazione non ha specificato altre AWS credenziali.

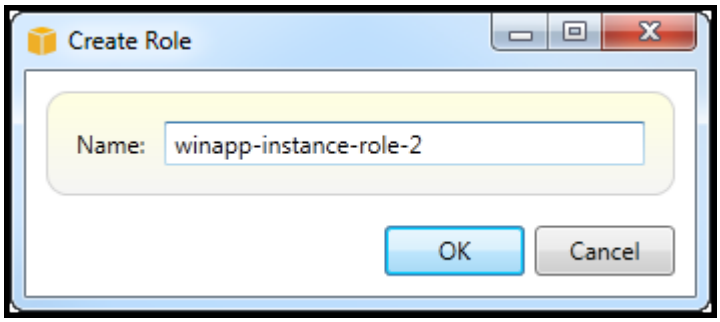
Ad esempio, puoi creare un ruolo e allegare a quel ruolo una policy che limiti l'accesso solo ad Amazon S3. Dopo aver associato questo ruolo a un'istanza EC2, puoi eseguire un'applicazione su quell'istanza e l'applicazione avrà accesso ad Amazon S3, ma non ad altri servizi o risorse. Il

vantaggio di questo approccio è che non devi preoccuparti di trasferire e archiviare in modo sicuro le AWS credenziali sull'istanza EC2.

Per ulteriori informazioni sui ruoli IAM, consulta Working with IAM Roles nella IAM User Guide. Per esempi di programmi che accedono AWS utilizzando il ruolo IAM associato a un'istanza Amazon EC2, consulta le guide per AWS sviluppatori per Java, .NET, PHP e Ruby (Impostazione delle credenziali tramite IAM, Creazione di un ruolo IAM e Utilizzo delle politiche IAM).

Per creare un ruolo IAM

1. In AWS Explorer, in Identity and Access Management, apri il menu contestuale (fai clic con il pulsante destro del mouse) per Ruoli, quindi scegli Crea ruoli.
2. Nella finestra di dialogo Crea ruolo, digita un nome per il ruolo IAM e scegli OK.



Create IAM role

Il nuovo ruolo IAM verrà visualizzato in Ruoli in Identity and Access Management.

Per informazioni su come creare una policy e collegarla al ruolo, consulta Create an IAM Policy.

Creare una policy IAM

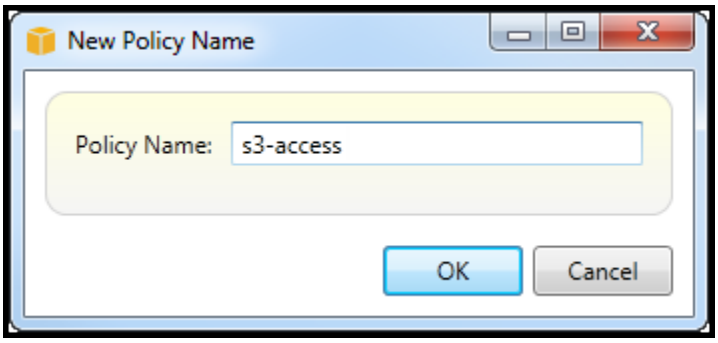
Le policy sono fondamentali per IAM. Le policy possono essere associate a entità IAM come utenti, gruppi o ruoli. Le policy specificano il livello di accesso abilitato per un utente, un gruppo o un ruolo.

Per creare una policy IAM

In AWS Explorer, espandi il AWS Identity and Access Managementnodo, quindi espandi il nodo per il tipo di entità (gruppi, ruoli o utenti) a cui allegherai la policy. Ad esempio, apri un menu contestuale per un ruolo IAM e scegli Modifica.

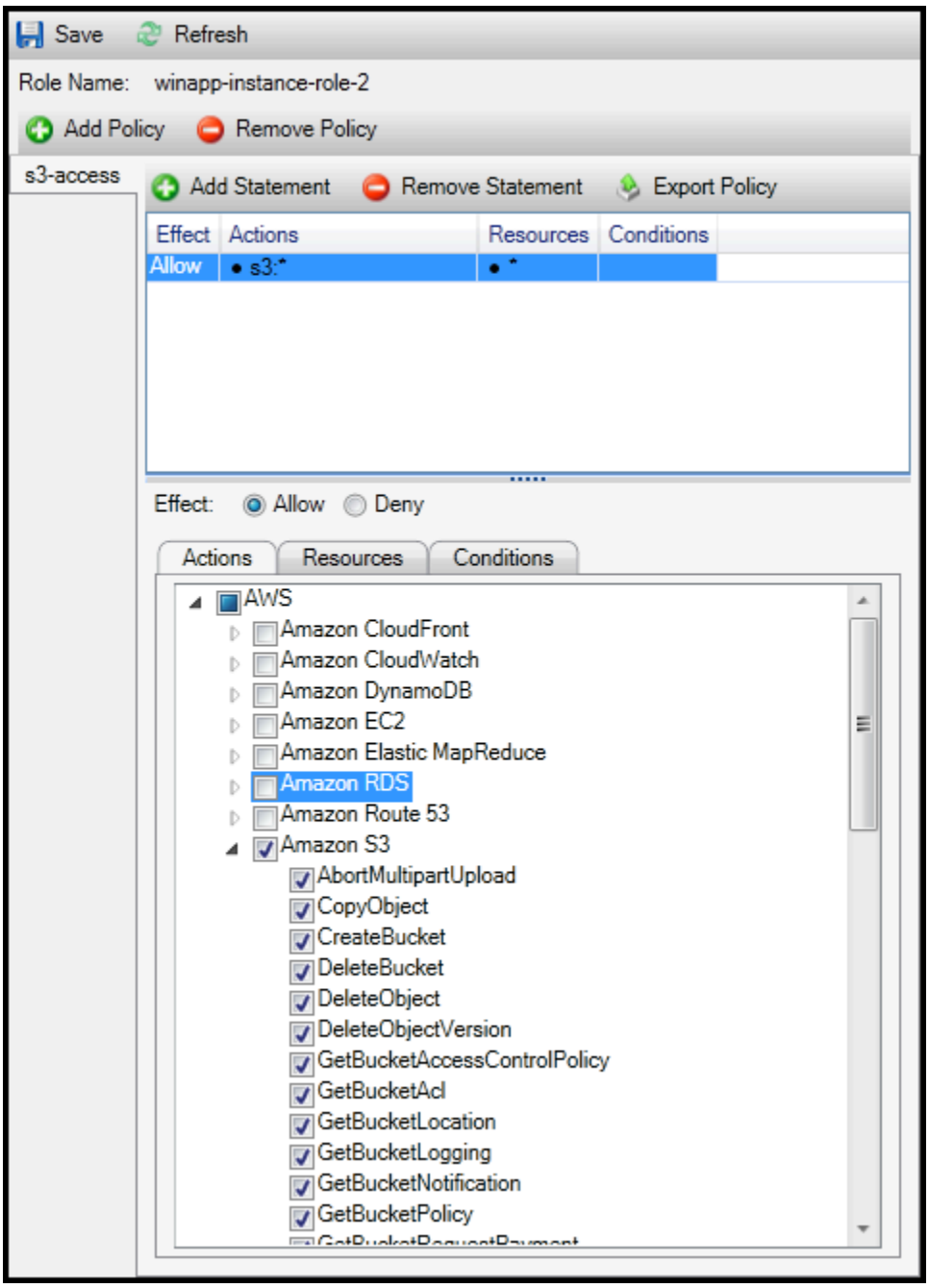
Una scheda associata al ruolo verrà visualizzata in AWS Explorer. Scegli il link Aggiungi politica.

Nella finestra di dialogo New Policy Name, digitate un nome per la policy (ad esempio, s3-access).



New Policy Name dialog box

Nell'editor delle politiche, aggiungi le istruzioni relative alle policy per specificare il livello di accesso da fornire al ruolo (in questo esempio, winapp-instance-role -2) associato alla policy. In questo esempio, una policy fornisce l'accesso completo ad Amazon S3, ma nessun accesso ad altre risorse.



Specify IAM policy

Per un controllo degli accessi più preciso, puoi espandere i sottonodi nell'editor delle politiche per consentire o impedire azioni associate ad Amazon Web Services.

Dopo aver modificato la policy, scegli il link Salva.

AWS Lambda

Sviluppa e distribuisci le tue funzioni Lambda in C# basate su .NET Core con. AWS Toolkit for Visual Studio AWS Lambda è un servizio di elaborazione che consente di eseguire codice senza eseguire il provisioning o la gestione di server. Il Toolkit for Visual Studio AWS Lambda include modelli di progetto.NET Core per Visual Studio.

Per ulteriori informazioni AWS Lambda, consulta la AWS Lambda Developer Guide.

Per ulteriori informazioni su.NET Core, vedere la guida di Microsoft.NET Core. Per i prerequisiti.NET Core e le istruzioni di installazione per le piattaforme Windows, macOS e Linux, consulta Download di.NET Core.

Negli argomenti seguenti viene descritto come AWS Lambda utilizzare il Toolkit for Visual Studio.

Argomenti

AWS Lambda Progetto base

È possibile creare una funzione Lambda utilizzando i modelli di progetto Microsoft.NET Core, in. AWS Toolkit for Visual Studio

Creare un progetto Lambda di Visual Studio .NET Core

Puoi usare modelli e blueprint Lambda-Visual Studio per velocizzare l'inizializzazione del progetto. I blueprint Lambda contengono funzioni predefinite che semplificano la creazione di una base di progetto flessibile.

> **Note**
>
> Il servizio Lambda ha limiti di dati su diversi tipi di pacchetti. Per informazioni dettagliate sui limiti dei dati, consulta l'argomento sulle quote Lambda nella Lambda User AWS Guide.

Per creare un progetto Lambda in Visual Studio

1. Da Visual Studio espandi il menu File, espandi Nuovo, quindi scegli Progetto.
2. Dalla finestra di dialogo Nuovo progetto, imposta le caselle a discesa Lingua, Piattaforma e Tipo di progetto su «Tutto», quindi digita aws lambda nel campo Cerca. Scegli il modello AWS Lambda Project (.NET Core - C#).
3. Nel campo Nome, inserisci**`AWSLambdaSample`**, specifica la posizione del file desiderata, quindi scegli Crea per procedere.
4. Dalla pagina Seleziona Blueprint, seleziona il blueprint Empty Function, quindi scegli Finish per creare il progetto Visual Studio.

Esamina i file di progetto

Ci sono due file di progetto da esaminare: `aws-lambda-tools-defaults.json` e `Function.cs`.

L'esempio seguente mostra il `aws-lambda-tools-defaults.json` file, che viene creato automaticamente come parte del progetto. È possibile impostare le opzioni di compilazione utilizzando i campi di questo file.

> **Note**
>
> I modelli di progetto in Visual Studio contengono molti campi diversi, prendi nota di quanto segue:
>
> - function-handler: specifica il metodo che viene eseguito quando viene eseguita la funzione Lambda
> - Se si specifica un valore nel campo function-handler, tale valore viene precompilato nella procedura guidata di pubblicazione.
> - Se rinominate la funzione, la classe o l'assieme, dovete aggiornare anche il campo corrispondente nel file. `aws-lambda-tools-defaults.json`

```
{
  "Information": [
    "This file provides default values for the deployment wizard inside Visual Studio
 and the AWS Lambda commands added to the .NET Core CLI.",
    "To learn more about the Lambda commands with the .NET Core CLI execute the
 following command at the command line in the project root directory.",
```

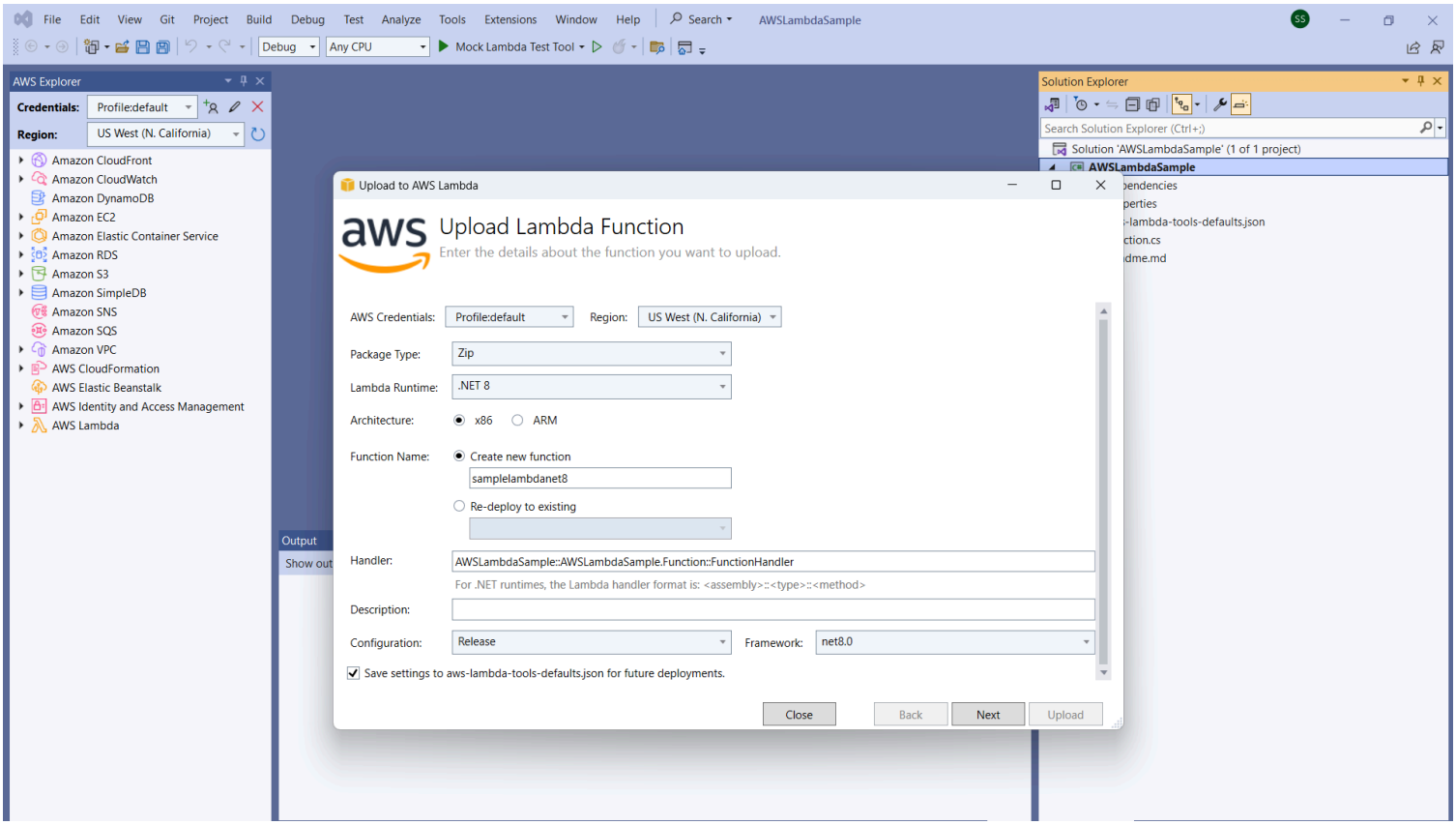
```
    "dotnet lambda help",
    "All the command line options for the Lambda command can be specified in this
 file."
  ],
  "profile": "default",
  "region": "us-west-2",
  "configuration": "Release",
  "function-architecture": "x86_64",
  "function-runtime": "dotnet8",
  "function-memory-size": 512,
  "function-timeout": 30,
  "function-handler": "AWSLambdaSample::AWSLambdaSample.Function::FunctionHandler"
}
```

Esamina il `Function.cs` file. `Function.cs`definisce le funzioni c# da esporre come funzioni Lambda. Questa `FunctionHandler` è la funzionalità Lambda che viene eseguita quando viene eseguita la funzione Lambda. In questo progetto, è definita una funzione:`FunctionHandler`, che richiama `ToUpper()` il testo di input.

Il tuo progetto è ora pronto per la pubblicazione su Lambda.

Pubblicazione su Lambda

La procedura e l'immagine seguenti mostrano come caricare la funzione su Lambda utilizzando il. AWS Toolkit for Visual Studio



Pubblicazione della funzione su Lambda

1. Passa a AWS Explorer espandendo View e scegliendo AWS Explorer.
2. In Solution Explorer, apri il menu contestuale per (fai clic con il pulsante destro del mouse) per il progetto che desideri pubblicare, quindi scegli Pubblica su AWS Lambda per aprire la finestra Carica funzione Lambda.
3. Dalla finestra Upload Lambda Function, completa i seguenti campi:

    a. Tipo di pacchetto: a scelta**`Zip`**. Un file ZIP verrà creato come risultato del processo di compilazione e verrà caricato su Lambda. In alternativa, puoi scegliere Package Type**`Image`**. Il tutorial: Basic Lambda Project Creating Docker Image descrive come pubblicare usando Package Type. **`Image`**

    b. Lambda Runtime: scegli Lambda Runtime dal menu a discesa.

    c. Architettura: seleziona il radiale per la tua architettura preferita.

    d. Nome funzione: seleziona il radiale per Crea nuova funzione, quindi inserisci un nome visualizzato per l'istanza Lambda. A questo nome fanno riferimento sia l' AWS Explorer che i display. Console di gestione AWS

e. Gestore: utilizzare questo campo per specificare un gestore di funzioni. Ad esempio: **`AWSLambdaSample::AWSLambdaSample.Function::FunctionHandler`**.

f. (Facoltativo) Descrizione: inserisci il testo descrittivo da visualizzare con l'istanza, dall'interno di. Console di gestione AWS

g. Configurazione: scegli la configurazione preferita dal menu a discesa.

h. Framework: scegli il tuo framework preferito dal menu a discesa.

i. Salva impostazioni: seleziona questa casella per salvare le impostazioni correnti `aws-lambda-tools-defaults.json` come predefinite per le distribuzioni future.

j. Scegliete Avanti per passare alla finestra Dettagli avanzati delle funzioni.

4. Nella finestra Dettagli delle funzioni avanzate, completare i seguenti campi:

   a. Nome del ruolo: scegli un ruolo associato al tuo account. Il ruolo fornisce credenziali temporanee per tutte le chiamate di AWS servizio effettuate dal codice della funzione. Se non disponi di un ruolo, scorri fino a individuare Nuovo ruolo basato su AWS Managed Policy nel selettore a discesa, quindi scegli. AWSLambdaBasicExecutionRole Questo ruolo ha autorizzazioni di accesso minime.

   > **Note**
   >
   > Il tuo account deve disporre dell'autorizzazione per eseguire l' ListPolicies azione IAM, altrimenti l'elenco dei nomi dei ruoli sarà vuoto e non potrai continuare.

   b. (Facoltativo) Se la funzione Lambda accede alle risorse su un Amazon VPC, seleziona le sottoreti e i gruppi di sicurezza.

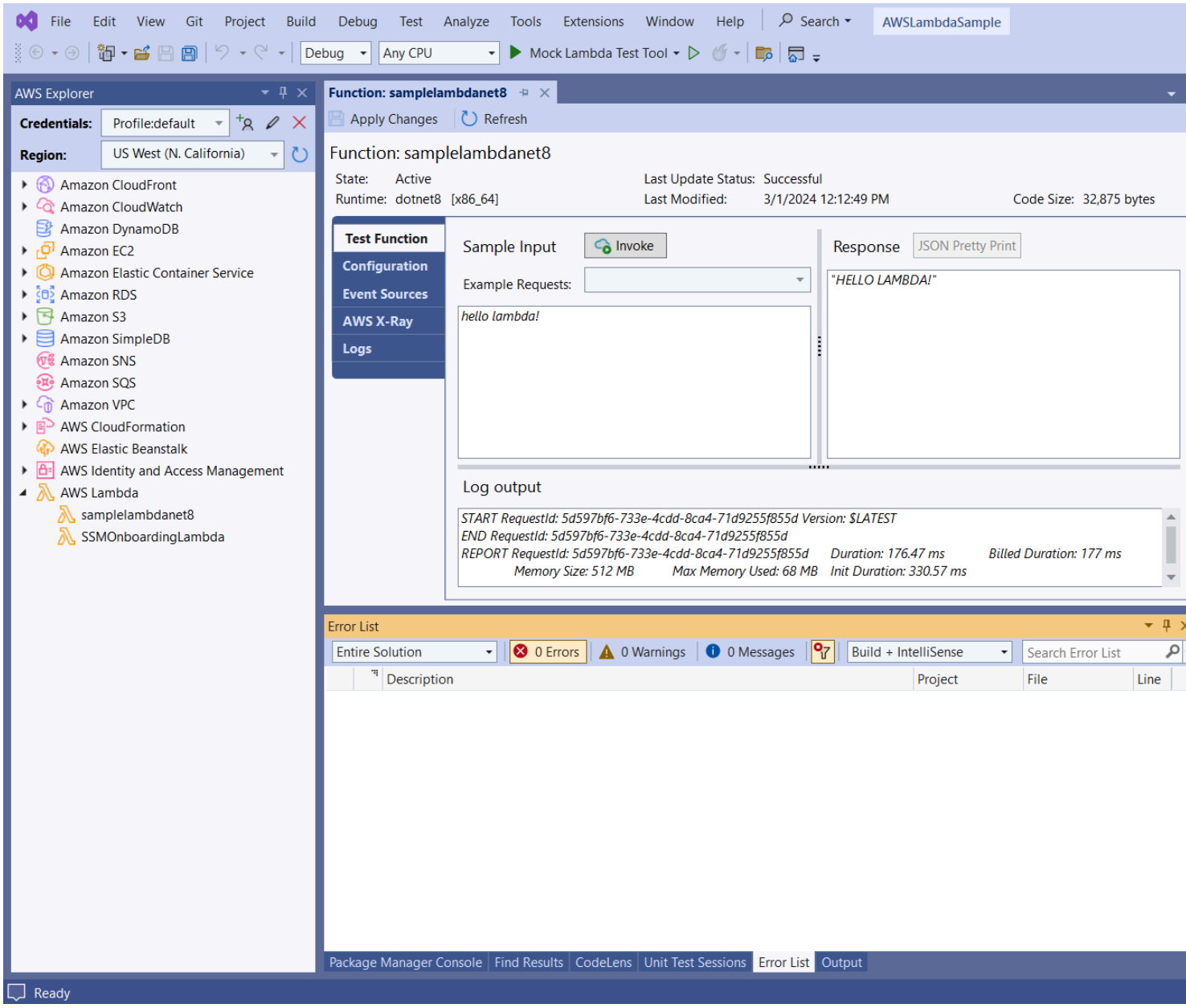
   c. (Facoltativo) Imposta tutte le variabili di ambiente necessarie alla funzione Lambda. Le chiavi vengono crittografate automaticamente dalla chiave di servizio predefinita, che è gratuita. In alternativa, puoi specificare una AWS KMS chiave, per la quale è previsto un costo. KMS è un servizio gestito che puoi utilizzare per creare e controllare le chiavi di crittografia utilizzate per crittografare i dati. Se hai una AWS KMS chiave, puoi selezionarla dall'elenco.

5. Scegli Carica per aprire la finestra della funzione di caricamento e iniziare il processo di caricamento.

> **Note**
>
> La pagina Funzione di caricamento viene visualizzata durante il caricamento della funzione su. AWS Per mantenere aperta la procedura guidata dopo il caricamento in modo da poter visualizzare il rapporto, deseleziona Chiudi automaticamente la procedura guidata in caso di completamento con successo nella parte inferiore del modulo prima del completamento del caricamento.
> Dopo il caricamento della funzione, la funzione Lambda è attiva. La pagina Funzione: visualizza si apre e mostra la configurazione della nuova funzione Lambda.

6. Dalla scheda Funzione di test, inserisci `hello lambda!` il campo di immissione del testo, quindi scegli Invoke per richiamare manualmente la funzione Lambda. Il testo viene visualizzato nella scheda Risposta, convertito in lettere maiuscole.

> **Note**
>
> Puoi riaprire la Funzione: visualizza in qualsiasi momento facendo doppio clic sull'istanza distribuita situata nell'Explorer sotto il AWS nodo. AWS Lambda



7. (Facoltativo) Per confermare di aver pubblicato correttamente la funzione Lambda, accedi a Console di gestione AWS e scegli Lambda. La console mostra tutte le funzioni Lambda pubblicate, inclusa quella appena creata.

Pulizia

Se non intendi continuare a sviluppare utilizzando questo esempio, elimina la funzione che hai implementato in modo da non farti addebitare le risorse non utilizzate nel tuo account.

> **Note**
>
> Lambda monitora automaticamente le funzioni Lambda per te, riportando i parametri tramite Amazon. CloudWatch Per monitorare e risolvere i problemi della tua funzione, consulta l' CloudWatchargomento Troubleshooting and Monitoring AWS Lambda Functions with Amazon nella Developer Guide. AWS Lambda

Per eliminare la tua funzione

1. Dall'AWS Explorer espandi il AWS Lambdanodo.
2. Fai clic con il pulsante destro del mouse sull'istanza distribuita, quindi scegli Elimina.

AWS Lambda Progetto di base per la creazione di un'immagine Docker

Puoi usare Toolkit for Visual Studio per distribuire la AWS Lambda tua funzione come immagine Docker. Usando Docker, hai un maggiore controllo sul tuo runtime. Ad esempio, puoi scegliere runtime personalizzati come .NET 8.0. L'immagine Docker viene distribuita allo stesso modo di qualsiasi altra immagine del contenitore. Questo tutorial imita da vicino Tutorial: Basic Lambda Project, con due differenze:

- Un Dockerfile è incluso nel progetto.
- Viene scelta una configurazione di pubblicazione alternativa.

Per informazioni sulle immagini dei container Lambda, consulta Lambda Deployment Packages nella Developer Guide.AWS Lambda

Per ulteriori informazioni sull'utilizzo di Lambda AWS Toolkit for Visual Studio, consulta la sezione Utilizzo dei AWS Lambda modelli nell' AWS Toolkit for Visual Studioargomento di questa Guida per l'utente.

Creare un progetto Lambda di Visual Studio .NET Core

Puoi utilizzare modelli e blueprint di Lambda Visual Studio per velocizzare l'inizializzazione del progetto. I blueprint Lambda contengono funzioni predefinite che semplificano la creazione di una base di progetto flessibile.

Per creare un progetto Lambda di Visual Studio .NET Core

1. Da Visual Studio espandi il menu File, espandi Nuovo, quindi scegli Progetto.
2. Dalla finestra di dialogo Nuovo progetto, imposta le caselle a discesa Lingua, Piattaforma e Tipo di progetto su «Tutto», quindi digita **`aws lambda`** nel campo Cerca. Scegli il modello AWS Lambda Project (.NET Core - C#).
3. Nel campo Nome progetto, inserisci**`AWSLambdaDocker`**, specifica la posizione del file, quindi scegli Crea.
4. Nella pagina Seleziona Blueprint, scegli il blueprint .NET 8 (Container Image), quindi scegli Fine per creare il progetto Visual Studio. Ora puoi rivedere la struttura e il codice del progetto.

Revisione dei file di progetto

Le seguenti sezioni esaminano i tre file di progetto creati dal blueprint .NET 8 (Container Image):

1. `Dockerfile`
2. `aws-lambda-tools-defaults.json`
3. `Function.cs`

1. Dockerfile

A `Dockerfile` esegue tre azioni principali:

- `FROM`: stabilisce l'immagine di base da utilizzare per questa immagine. Questa immagine di base fornisce .NET Runtime, Lambda runtime e uno script di shell che fornisce un punto di ingresso per il processo Lambda .NET.
- `WORKDIR`: stabilisce la directory di lavoro interna dell'immagine come. `/var/task`
- `COPY`: Copierà i file generati dal processo di compilazione dalla loro posizione locale nella directory di lavoro dell'immagine.

Di seguito sono riportate `Dockerfile` le azioni opzionali che è possibile specificare:

- `ENTRYPOINT`: L'immagine di base include già un`ENTRYPOINT`, che è il processo di avvio eseguito all'avvio dell'immagine. Se desideri specificare il tuo, stai sovrascrivendo quel punto di ingresso di base.

- `CMD`: Indica AWS quale codice personalizzato si desidera eseguire. Si aspetta un nome completo per il metodo personalizzato. Questa riga deve essere inclusa direttamente nel Dockerfile o può essere specificata durante il processo di pubblicazione.

```
# Example of alternative way to specify the Lambda target method rather than during
 the publish process.
CMD [ "AWSLambdaDocker::AWSLambdaDocker.Function::FunctionHandler"]
```

Di seguito è riportato un esempio di Dockerfile creato dal blueprint .NET 8 (Container Image).

```
FROM public.ecr.aws/lambda/dotnet:8

WORKDIR /var/task

# This COPY command copies the .NET Lambda project's build artifacts from the host
 machine into the image.
# The source of the COPY should match where the .NET Lambda project publishes its build
 artifacts. If the Lambda function is being built
# with the AWS .NET Lambda Tooling, the `--docker-host-build-output-dir` switch
 controls where the .NET Lambda project
# will be built. The .NET Lambda project templates default to having `--docker-host-
build-output-dir`
# set in the aws-lambda-tools-defaults.json file to "bin/Release/lambda-publish".
#
# Alternatively Docker multi-stage build could be used to build the .NET Lambda project
 inside the image.
# For more information on this approach checkout the project's README.md file.
COPY "bin/Release/lambda-publish"  .
```

2. aws-lambda-tools-defaults.json

Il `aws-lambda-tools-defaults.json` file viene utilizzato per specificare i valori predefiniti per la procedura guidata di distribuzione di Toolkit for Visual Studio e.NET Core CLI. L'elenco seguente descrive i campi che è possibile impostare nel file. `aws-lambda-tools-defaults.json`

- `profile`: imposta il tuo AWS profilo.
- `region`: imposta la AWS regione in cui sono archiviate le risorse.
- `configuration`: imposta la configurazione utilizzata per pubblicare la funzione.

- `package-type`: imposta il tipo di pacchetto di distribuzione su un'immagine del contenitore o su un archivio di file.zip.
- `function-memory-size`: imposta l'allocazione della memoria per la funzione in MB.
- `function-timeout`: Il timeout è la quantità massima di tempo in secondi che una funzione Lambda può essere eseguita. Puoi regolarlo con incrementi di 1 secondo fino a un valore massimo di 15 minuti.
- `docker-host-build-output-dir`: imposta la directory di output del processo di compilazione correlata alle istruzioni contenute in. `Dockerfile`
- `image-command`: è un nome completo per il tuo metodo, il codice che vuoi che venga eseguita dalla funzione Lambda. La sintassi è:. `{Assembly}::{Namespace}.{ClassName}::{MethodName}` Per ulteriori informazioni, consulta Handler signatures. L'impostazione `image-command` qui precompila questo valore nella procedura guidata di pubblicazione di Visual Studio in un secondo momento.

Di seguito è riportato un esempio di un aws-lambda-tools-defaults file .json creato dal blueprint .NET 8 (Container Image).

```
{
  "Information": [
    "This file provides default values for the deployment wizard inside Visual Studio
 and the AWS Lambda commands added to the .NET Core CLI.",
    "To learn more about the Lambda commands with the .NET Core CLI execute the
 following command at the command line in the project root directory.",
    "dotnet lambda help",
    "All the command line options for the Lambda command can be specified in this
 file."
  ],
  "profile": "default",
  "region": "us-west-2",
  "configuration": "Release",
  "package-type": "image",
  "function-memory-size": 512,
  "function-timeout": 30,
  "image-command": "AWSLambdaDocker::AWSLambdaDocker.Function::FunctionHandler",
  "docker-host-build-output-dir": "./bin/Release/lambda-publish"
}
```

3. Function.cs

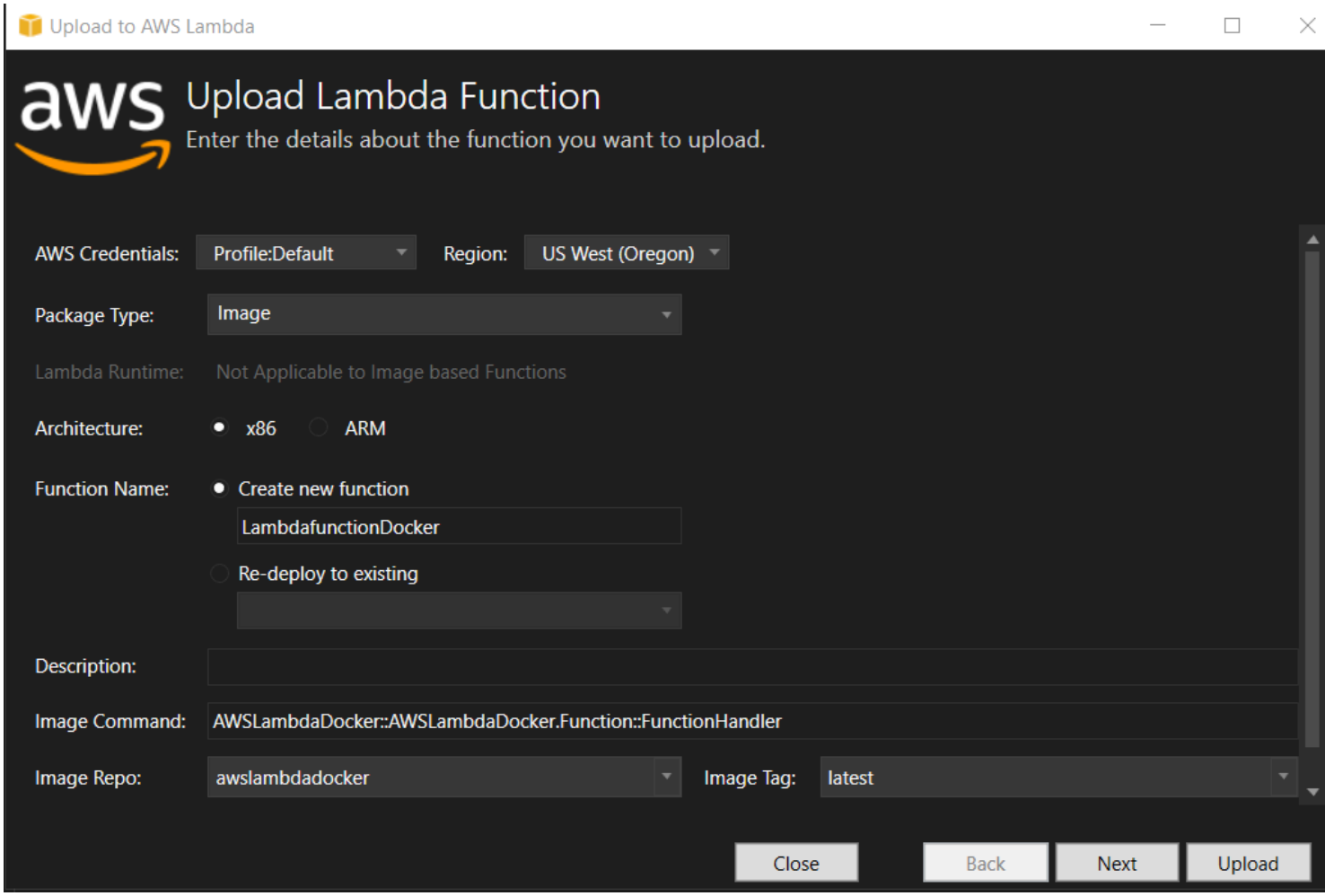
Il `Function.cs` file definisce le funzioni c# da esporre come funzioni Lambda. `FunctionHandler`È la funzionalità Lambda che viene eseguita quando viene eseguita la funzione Lambda. In questo progetto, `FunctionHandler` richiama `ToUpper()` il testo di input.

Pubblica su Lambda

Le immagini Docker generate dal processo di compilazione vengono caricate su Amazon Elastic Container Registry (Amazon ECR). Amazon ECR è un registro di container Docker completamente gestito che utilizzi per archiviare, gestire e distribuire immagini di container Docker. Amazon ECR ospita l'immagine, a cui Lambda fa quindi riferimento per fornire la funzionalità Lambda programmata quando viene richiamata.

Per pubblicare la tua funzione su Lambda

1. Da Solution Explorer, apri il menu contestuale (fai clic con il pulsante destro del mouse) per il progetto, quindi scegli Pubblica per AWS Lambda aprire la finestra Upload Lambda Function.
2. Dalla pagina Upload Lambda Function, procedi come segue:



a. Per Tipo di pacchetto, **`Image`** è stato selezionato automaticamente come tipo di pacchetto perché la procedura guidata di pubblicazione ha rilevato un elemento `Dockerfile` all'interno del progetto.

b. Per Function Name, inserisci un nome visualizzato per l'istanza Lambda. Questo nome è il nome di riferimento visualizzato sia in AWS Explorer in Visual Studio che in. Console di gestione AWS

c. Per Descrizione, inserisci il testo da visualizzare con l'istanza in Console di gestione AWS.

d. Per Image Command, inserisci un percorso completo del metodo che desideri venga eseguita dalla funzione Lambda: **`AWSLambdaDocker::AWSLambdaDocker.Function::FunctionHandler`**

> **Note**
>
> Qualsiasi nome di metodo inserito qui sovrascriverà qualsiasi istruzione CMD all'interno del Dockerfile. L'immissione di Image Command è facoltativa solo SE `CMD` si `Dockerfile` include un'istruzione su come avviare la funzione Lambda.

e. Per Image Repo, inserisci il nome di un Amazon Elastic Container Registry nuovo o esistente. L'immagine Docker creata dal processo di compilazione viene caricata in questo registro. La definizione Lambda che viene pubblicata farà riferimento all'immagine Amazon ECR.

f. Per Image Tag, inserisci un tag Docker da associare all'immagine nel repository.

g. Scegli Next (Successivo).

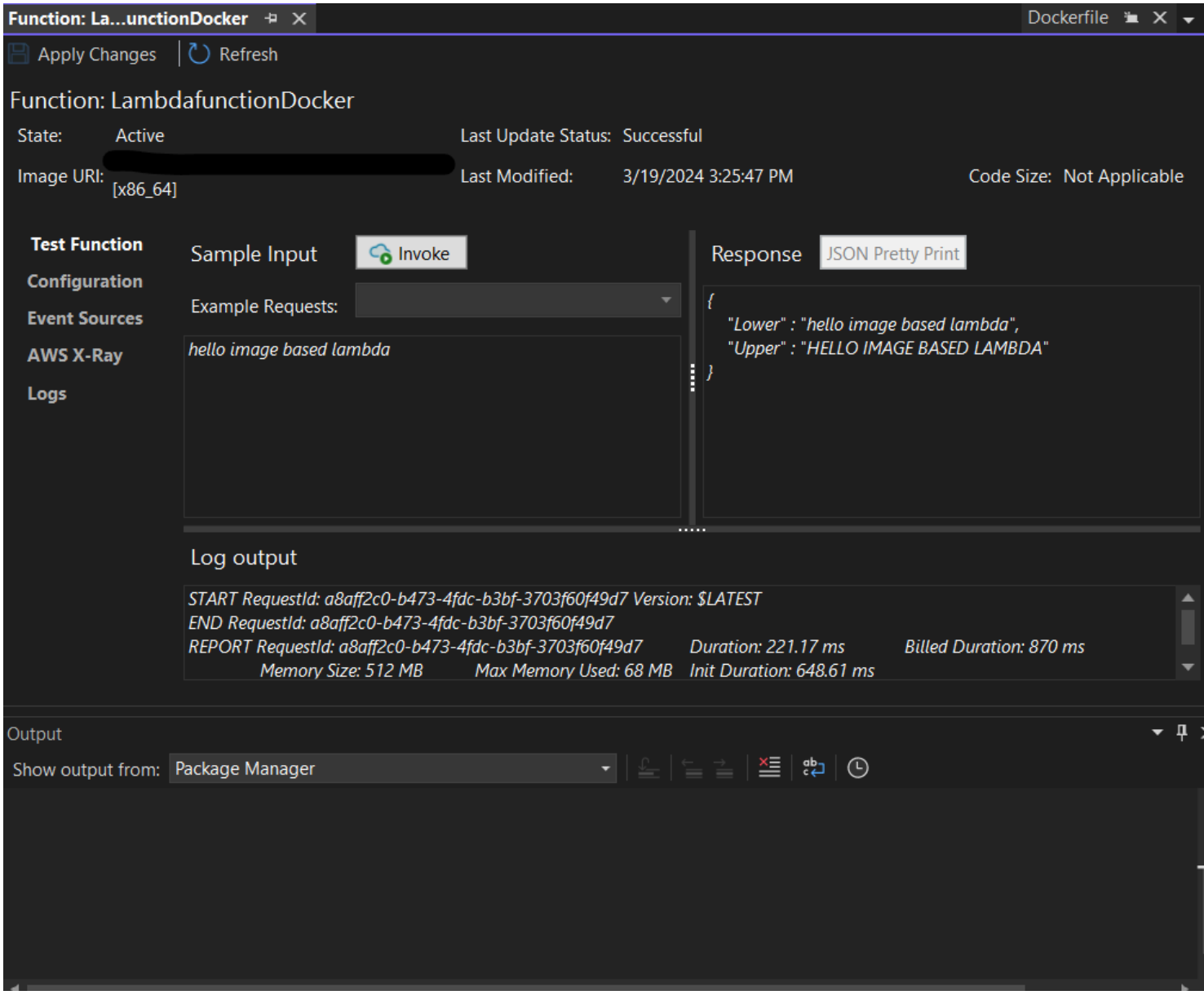
3. Nella pagina Dettagli delle funzioni avanzate, in Nome ruolo scegli un ruolo associato al tuo account. Il ruolo viene utilizzato per fornire credenziali temporanee per tutte le chiamate Amazon Web Services effettuate dal codice nella funzione. Se non disponi di un ruolo, scegli Nuovo ruolo basato su AWS Managed Policy e poi scegli AWSLambdaBasicExecutionRole.

> **Note**
>
> Il tuo account deve disporre dell'autorizzazione per eseguire l' ListPolicies azione IAM, altrimenti l'elenco dei nomi dei ruoli sarà vuoto.

4. Scegli Carica per avviare i processi di caricamento e pubblicazione.

> **Note**
>
> La pagina Funzione di caricamento viene visualizzata durante il caricamento della funzione. Il processo di pubblicazione crea quindi l'immagine in base ai parametri di configurazione, crea il repository Amazon ECR se necessario, carica l'immagine nel repository e crea la Lambda che fa riferimento a quel repository con quell'immagine. Dopo il caricamento della funzione, si apre la pagina Funzione che mostra la configurazione della nuova funzione Lambda.

5. Per richiamare manualmente la funzione Lambda, nella scheda Funzione di test, **`hello image based lambda`** inserisci il campo di immissione a testo libero della richiesta e quindi scegli Invoke. Il testo, convertito in lettere maiuscole, verrà visualizzato in Response.



6. Per visualizzare il repository, in AWS Explorer, in Amazon Elastic Container Service, scegli Repositories.

   Puoi riaprire la funzione: visualizzala in qualsiasi momento facendo doppio clic sull'istanza distribuita situata nell'Explorer sotto il AWS nodo. AWS Lambda

> **Note**
>
> Se la finestra di AWS Explorer non è aperta, puoi agganciarla tramite Visualizza -> Explorer AWS

7. Nota le opzioni di configurazione aggiuntive specifiche dell'immagine nella scheda Configurazione. Questa scheda fornisce un modo per sovrascrivere il `ENTRYPOINTCMD`, e `WORKDIR` che potrebbe essere stato specificato all'interno del Dockerfile. Descrizione è la descrizione che hai inserito (se presente) durante il caricamento/pubblicazione.

Pulizia

Se non hai intenzione di continuare a sviluppare con questo esempio, ricordati di eliminare la funzione e l'immagine ECR che sono state implementate in modo da non farti addebitare le risorse non utilizzate nel tuo account.

- Le funzioni possono essere eliminate facendo clic con il pulsante destro del mouse sull'istanza distribuita situata in Explorer sotto il nodo.AWS AWS Lambda
- I repository possono essere eliminati in AWS Explorer in Amazon Elastic Container Service -> Repositories.

Fasi successive

Per informazioni sulla creazione e il test di immagini Lambda, consulta Using Container Images with Lambda.

Per informazioni sulla distribuzione delle immagini dei container, sulle autorizzazioni e sulla sovrascrittura delle impostazioni di configurazione, vedi Configurazione delle funzioni.

Tutorial: crea e testa un'applicazione serverless con AWS Lambda

È possibile creare un'applicazione Lambda serverless utilizzando AWS Toolkit for Visual Studio un modello. I modelli di progetto Lambda ne includono uno per un'applicazione AWS serverless, che è l' AWS Toolkit for Visual Studio implementazione del AWS Serverless Application Model (SAM).AWS Utilizzando questo tipo di progetto è possibile sviluppare una raccolta di AWS Lambda funzioni e distribuirle con tutte le AWS risorse necessarie come intera applicazione, utilizzandole per AWS CloudFormation orchestrare la distribuzione.

Per i prerequisiti e informazioni sulla configurazione di AWS Toolkit for Visual Studio, vedi Uso dei modelli AWS Lambda nel Toolkit for AWS Visual Studio.

Argomenti

- Crea un nuovo progetto di applicazione serverless AWS

- Revisione dei file dell'applicazione Serverless
- Distribuzione dell'applicazione serverless
- Prova l'applicazione serverless

Crea un nuovo progetto di applicazione serverless AWS

AWS I progetti di applicazioni serverless creano funzioni Lambda con un CloudFormation modello serverless. CloudFormation i modelli consentono di definire risorse aggiuntive come database, aggiungere ruoli IAM e distribuire più funzioni contemporaneamente. Ciò differisce dai progetti AWS Lambda, che si concentrano sullo sviluppo e l'implementazione di una singola funzione Lambda.

La procedura seguente descrive come creare un nuovo AWS progetto di applicazione Serverless.

1. Da Visual Studio espandi il menu File, espandi Nuovo, quindi scegli Progetto.
2. Nella finestra di dialogo Nuovo progetto, assicurati che le caselle a discesa Lingua, Piattaforma e Tipo di progetto siano impostate su «Tutto...» e inseriscile **`aws lambda`** nel campo Cerca.
3. Seleziona il modello AWS Serverless Application with Tests (.NET Core - C#).

   > **Note**
   >
   > È possibile che il modello AWS Serverless Application with Tests (.NET Core - C#) non compili nella parte superiore dei risultati.

4. Fate clic su Avanti per aprire la finestra di dialogo Configura il nuovo progetto.
5. Dalla finestra di dialogo Configura il tuo nuovo progetto, inserisci **`ServerlessPowertools`** il nome, quindi completa i campi rimanenti secondo le tue preferenze. Scegli il pulsante Crea per passare alla finestra di dialogo Seleziona Blueprint.
6. Dalla finestra di dialogo Seleziona Blueprint scegli Powertools per il AWS Lambda blueprint, quindi scegli Fine per creare il progetto Visual Studio.

Revisione dei file dell'applicazione Serverless

Le seguenti sezioni forniscono una panoramica dettagliata di tre file di applicazioni serverless creati per il progetto:

1. serverless.template
2. Functions.cs

3. aws-lambda-tools-defaults.json

1. template senza server

Un `serverless.template` file è un AWS CloudFormation modello per dichiarare le funzioni Serverless e altre risorse. AWS Il file incluso in questo progetto contiene una dichiarazione per una singola funzione Lambda che verrà esposta tramite Amazon API Gateway come operazioneHTTP `*Get*`. Puoi modificare questo modello per personalizzare la funzione esistente o aggiungere altre funzioni e altre risorse richieste dall'applicazione.

Di seguito è riportato un esempio di un file `serverless.template`:

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Transform": "AWS::Serverless-2016-10-31",
  "Description": "An AWS Serverless Application.",
  "Resources": {
    "Get": {
      "Type": "AWS::Serverless::Function",
      "Properties": {
         "Architectures": [
            "x86_64"
            ],
         "Handler": "ServerlessPowertools::ServerlessPowertools.Functions::Get",
         "Runtime": "dotnet8",
         "CodeUri": "",
         "MemorySize": 512,
         "Timeout": 30,
         "Role": null,
         "Policies": [
            "AWSLambdaBasicExecutionRole"
            ],
         "Environment": {
            "Variables": {
               "POWERTOOLS_SERVICE_NAME": "ServerlessGreeting",
               "POWERTOOLS_LOG_LEVEL": "Info",
               "POWERTOOLS_LOGGER_CASE": "PascalCase",
               "POWERTOOLS_TRACER_CAPTURE_RESPONSE": true,
               "POWERTOOLS_TRACER_CAPTURE_ERROR": true,
               "POWERTOOLS_METRICS_NAMESPACE": "ServerlessGreeting"
               }
            },
```

```
         "Events": {
            "RootGet": {
               "Type": "Api",
               "Properties": {
                  "Path": "/",
                  "Method": "GET"
                  }
               }
            }
         }
      }
   },
  "Outputs": {
    "ApiURL": {
      "Description": "API endpoint URL for Prod environment",
      "Value": {
        "Fn::Sub": "https://${ServerlessRestApi}.execute-api.
${AWS::Region}.amazonaws.com/Prod/"
      }
    }
  }
}
```

Nota che molti dei campi di `...AWS:: Serverless::Function...` dichiarazione sono simili ai campi della distribuzione di un progetto Lambda. Powertools Logging, Metrics and Tracing sono configurati tramite le seguenti variabili di ambiente:

- POWERTOOLS_SERVICE_NAME= ServerlessGreeting
- powertools_log_level=Informazioni
- POWERTOOLS_LOGGER_CASE= PascalCase
- PowerTools_Tracer_Capture_Response=Vero
- powertools_tracer_capture_error=Vero
- SPAZIO DEI NOMI POWERTOOLS_METRICS= ServerlessGreeting

Per definizioni e dettagli aggiuntivi sulle variabili di ambiente, consultate il sito Web Powertools for References. AWS Lambda

2. Functions.cs

`Functions.cs`è un file di classe contenente un metodo C# mappato a una singola funzione dichiarata nel file modello. La funzione Lambda risponde ai `HTTP Get` metodi di API Gateway. Di seguito è riportato un esempio del `Functions.cs` file:

```
public class Functions
{
    [Logging(LogEvent = true, CorrelationIdPath = CorrelationIdPaths.ApiGatewayRest)]
    [Metrics(CaptureColdStart = true)]
    [Tracing(CaptureMode = TracingCaptureMode.ResponseAndError)]
    public APIGatewayProxyResponse Get(APIGatewayProxyRequest request, ILambdaContext
 context)
    {
        Logger.LogInformation("Get Request");

        var greeting = GetGreeting();

        var response = new APIGatewayProxyResponse
        {
            StatusCode = (int)HttpStatusCode.OK,
            Body = greeting,
            Headers = new Dictionary (string, string) { { "Content-Type", "text/
plain" } }
        };

        return response;
    }

    [Tracing(SegmentName = "GetGreeting Method")]
    private static string GetGreeting()
    {
        Metrics.AddMetric("GetGreeting_Invocations", 1, MetricUnit.Count);

        return "Hello Powertools for AWS Lambda (.NET)";
    }
}
```

3. aws-lambda-tools-defaults.json

`aws-lambda-tools-defaults.json`fornisce i valori predefiniti per la procedura guidata di AWS distribuzione all'interno di Visual Studio e i AWS Lambda comandi aggiunti al.NET Core CLI. Di

seguito è riportato un esempio del `aws-lambda-tools-defaults.json` file incluso in questo progetto:

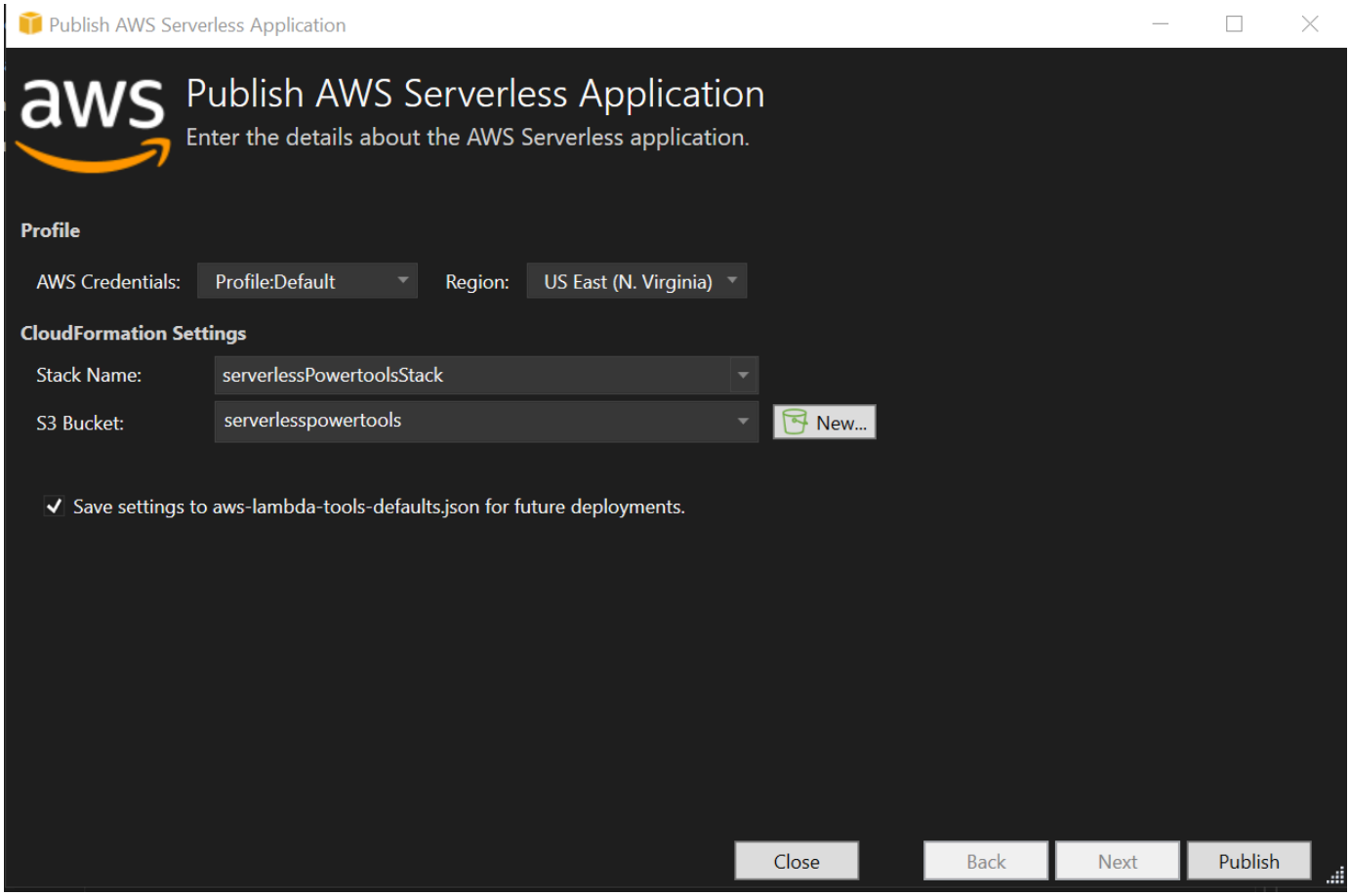
```
{
  "profile": "Default",
  "region": "us-east-1",
  "configuration": "Release",
  "s3-prefix": "ServerlessPowertools/",
  "template": "serverless.template",
  "template-parameters": ""
}
```

Distribuzione dell'applicazione serverless

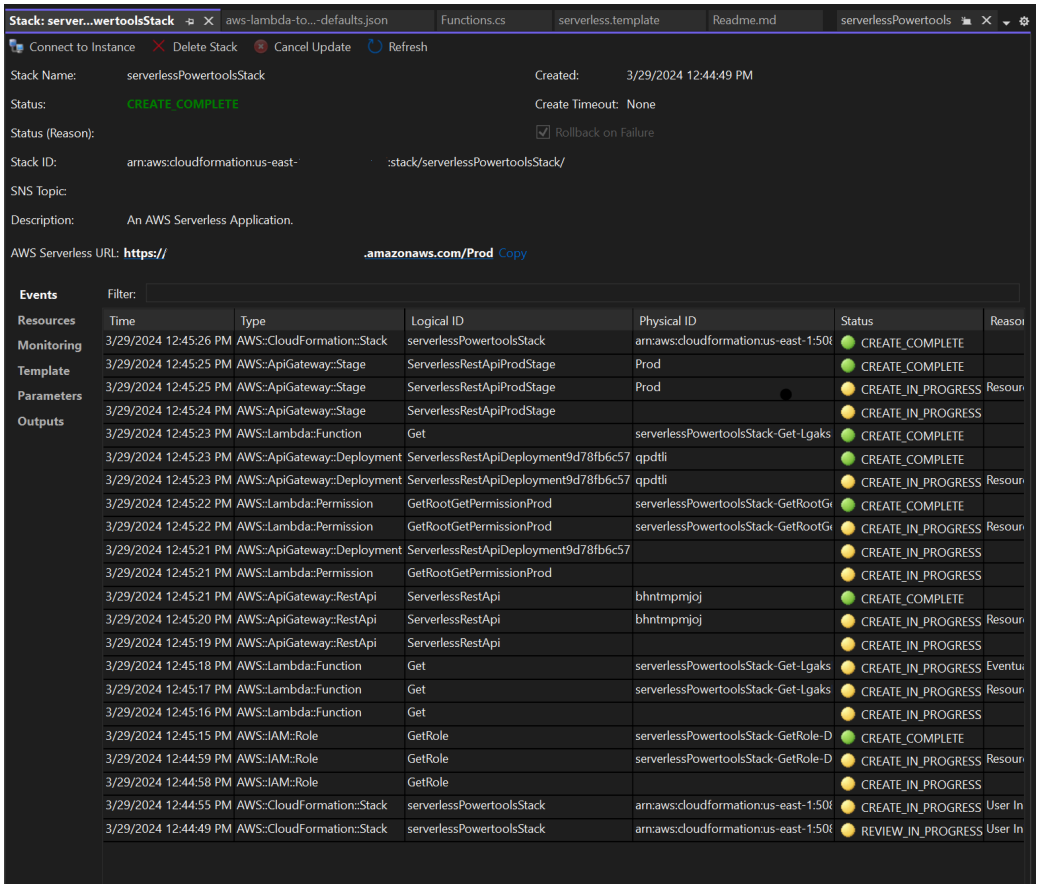
Per distribuire un'applicazione serverless, completa i seguenti passaggi

1. Da Solution Explorer, apri il menu contestuale del progetto (fai clic con il pulsante destro del mouse) e scegli Pubblica su AWS Lambda per aprire la finestra di dialogo Pubblica applicazione AWS serverless.
2. Nella finestra di dialogo Pubblica applicazione AWS serverless, inserisci un nome per il contenitore dello CloudFormation stack nel campo Stack Name.
3. Nel campo S3 Bucket, scegli un bucket Amazon S3 su cui caricare il pacchetto di applicazioni o scegli il Nuovo... pulsante e inserisci il nome di un nuovo bucket Amazon S3. Quindi scegli Pubblica per pubblicare per distribuire la tua applicazione.

> **Note**
>
> CloudFormation Lo stack e Amazon S3 Bucket devono esistere nella stessa regione. AWS Le impostazioni rimanenti per il progetto sono definite nel file. `serverless.template`



4. La finestra di visualizzazione dello stack si apre durante il processo di pubblicazione. Una volta completata la distribuzione, viene visualizzato il campo Status:. `CREATE_COMPLETE`



Prova l'applicazione serverless

Una volta completata la creazione dello stack, puoi visualizzare l'applicazione utilizzando l'URL AWS Serverless. Se hai completato questo tutorial senza aggiungere funzioni o parametri aggiuntivi, accedendo al tuo URL AWS serverless viene visualizzata la seguente frase nel tuo browser web:. `Hello Powertools for AWS Lambda (.NET)`

Tutorial: creazione di un'applicazione Amazon Rekognition Lambda

Questo tutorial mostra come creare un'applicazione Lambda che utilizzi Amazon Rekognition per etichettare gli oggetti Amazon S3 con le etichette rilevate.

Per i prerequisiti e informazioni sulla configurazione di AWS Toolkit for Visual Studio, consulta Using the AWS Lambda Templates in AWS the Toolkit for Visual Studio.

Creare un progetto di Rekognition Lambda Image Rekognition di Visual Studio.NET Core

La procedura seguente descrive come creare un'applicazione Amazon Rekognition Lambda da. AWS Toolkit for Visual Studio

> **Note**
>
> Al momento della creazione, l'applicazione dispone di una soluzione con due progetti: il progetto sorgente che contiene il codice della funzione Lambda da distribuire su Lambda e un progetto di test che utilizza xUnit per testare la funzione localmente.
> A volte Visual Studio non riesce a trovare tutti i NuGet riferimenti per i tuoi progetti. Questo perché i blueprint richiedono dipendenze da cui è necessario recuperare. NuGet Quando vengono creati nuovi progetti, Visual Studio inserisce solo riferimenti locali e non riferimenti remoti da. NuGet Per correggere gli NuGet errori: fai clic con il pulsante destro del mouse sui riferimenti e scegli Ripristina pacchetti.

1. Da Visual Studio espandi il menu File, espandi Nuovo, quindi scegli Progetto.
2. Nella finestra di dialogo Nuovo progetto, assicurati che le caselle a discesa Lingua, Piattaforma e Tipo di progetto siano impostate su «Tutto...» e inseriscile **`aws lambda`** nel campo Cerca.
3. Seleziona il modello AWS Lambda with Tests (.NET Core - C#).
4. Fai clic su Avanti per aprire la finestra di dialogo Configura il tuo nuovo progetto.
5. Nella finestra di dialogo Configura il nuovo progetto, inserisci ImageRekognition "" come nome, quindi completa i campi rimanenti secondo le tue preferenze. Scegli il pulsante Crea per passare alla finestra di dialogo Seleziona Blueprint.
6. Nella finestra di dialogo Seleziona progetto, scegli il progetto Detect Image Labels, quindi scegli Fine per creare il progetto Visual Studio.

> **Note**
>
> Questo modello fornisce codice per ascoltare gli eventi di Amazon S3 e utilizza Amazon Rekognition per rilevare le etichette e aggiungerle all'oggetto S3 come tag.

Revisione dei file di progetto

Le seguenti sezioni esaminano questi file di progetto:

1. `Function.cs`
2. `aws-lambda-tools-defaults.json`

1. Function.cs

All'interno del `Function.cs` file, il primo segmento di codice è l'attributo assembly, situato nella parte superiore del file. Per impostazione predefinita, Lambda accetta solo parametri di input e tipi di tipo restituiti. `System.IO.Stream` È necessario registrare un serializzatore per utilizzare le classi tipizzate per i parametri di input e i tipi restituiti. L'attributo assembly registra il serializzatore JSON Lambda, che viene `Newtonsoft.Json` utilizzato per convertire i flussi in classi tipizzate. È possibile impostare il serializzatore a livello di assembly o metodo.

Di seguito è riportato un esempio dell'attributo assembly:

```
// Assembly attribute to enable the Lambda function's JSON input to be converted into
 a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer
```

La classe ha due costruttori. Il primo è un costruttore predefinito che viene utilizzato quando Lambda richiama la tua funzione. Questo costruttore crea i client di servizi Amazon S3 e Amazon Rekognition. Il costruttore recupera anche le AWS credenziali per questi client dal ruolo IAM assegnato alla funzione al momento della distribuzione. La AWS regione per i client è impostata sulla regione in cui è in esecuzione la funzione Lambda. In questo modello, desideri aggiungere tag all'oggetto Amazon S3 solo se il servizio Amazon Rekognition ha un livello minimo di fiducia sull'etichetta. Questo costruttore controlla la variabile di ambiente per determinare il livello di confidenza `MinConfidence` accettabile. È possibile impostare questa variabile di ambiente quando si distribuisce la funzione Lambda.

Di seguito è riportato un esempio del costruttore di prima classe in: `Function.cs`

```
public Function()
{
    this.S3Client = new AmazonS3Client();
    this.RekognitionClient = new AmazonRekognitionClient();
```

```
    var environmentMinConfidence =
 System.Environment.GetEnvironmentVariable(MIN_CONFIDENCE_ENVIRONMENT_VARIABLE_NAME);
    if(!string.IsNullOrWhiteSpace(environmentMinConfidence))
    {
        float value;
        if(float.TryParse(environmentMinConfidence, out value))
        {
            this.MinConfidence = value;
            Console.WriteLine($"Setting minimum confidence to {this.MinConfidence}");
        }
        else
        {
            Console.WriteLine($"Failed to parse value {environmentMinConfidence} for
 minimum confidence. Reverting back to default of {this.MinConfidence}");
        }
    }
    else
    {
        Console.WriteLine($"Using default minimum confidence of {this.MinConfidence}");
    }
}
```

L'esempio seguente dimostra come il secondo costruttore può essere utilizzato per i test. Il progetto di test configura i propri client S3 e Rekognition e li trasmette:

```
public Function(IAmazonS3 s3Client, IAmazonRekognition rekognitionClient, float
 minConfidence)
{
    this.S3Client = s3Client;
    this.RekognitionClient = rekognitionClient;
    this.MinConfidence = minConfidence;
}
```

Di seguito è riportato un esempio del metodo all'interno del `FunctionHandler` file. `Function.cs`

```
public async Task FunctionHandler(S3Event input, ILambdaContext context)
{
    foreach(var record in input.Records)
    {
        if(!SupportedImageTypes.Contains(Path.GetExtension(record.S3.Object.Key)))
        {
            Console.WriteLine($"Object {record.S3.Bucket.Name}:{record.S3.Object.Key}
 is not a supported image type");
```

```
            continue;
        }

        Console.WriteLine($"Looking for labels in image {record.S3.Bucket.Name}:
{record.S3.Object.Key}");
        var detectResponses = await this.RekognitionClient.DetectLabelsAsync(new
 DetectLabelsRequest
        {
            MinConfidence = MinConfidence,
            Image = new Image
            {
                S3Object = new Amazon.Rekognition.Model.S3Object
                {
                    Bucket = record.S3.Bucket.Name,
                    Name = record.S3.Object.Key
                }
            }
        });

        var tags = new List();
        foreach(var label in detectResponses.Labels)
        {
            if(tags.Count < 10)
            {
                Console.WriteLine($"\tFound Label {label.Name} with confidence
 {label.Confidence}");
                tags.Add(new Tag { Key = label.Name, Value =
 label.Confidence.ToString() });
            }
            else
            {
                Console.WriteLine($"\tSkipped label {label.Name} with confidence
 {label.Confidence} because maximum number of tags reached");
            }
        }

        await this.S3Client.PutObjectTaggingAsync(new PutObjectTaggingRequest
        {
            BucketName = record.S3.Bucket.Name,
            Key = record.S3.Object.Key,
            Tagging = new Tagging
            {
                TagSet = tags
            }
```

```
        });
    }
    return;
}
```

`FunctionHandler`è il metodo che Lambda chiama dopo aver costruito l'istanza. Notate che il parametro di input è di tipo `S3Event` e non a. `Stream` Puoi farlo grazie al serializzatore JSON Lambda registrato. `S3Event`Contiene tutte le informazioni sull'evento attivato in Amazon S3. La funzione esegue un ciclo su tutti gli oggetti S3 che facevano parte dell'evento e indica a Rekognition di rilevare le etichette. Dopo che le etichette sono state rilevate, vengono aggiunte come tag all'oggetto S3.

> **Note**
>
> Il codice contiene chiamate a. `Console.WriteLine()` Quando la funzione è in esecuzione in Lambda, tutte le chiamate vengono `Console.WriteLine()` reindirizzate ad Amazon Logs. CloudWatch

2. aws-lambda-tools-defaults.json

Il `aws-lambda-tools-defaults.json` file contiene i valori predefiniti che il blueprint ha impostato per precompilare alcuni campi nella procedura guidata di distribuzione. È anche utile per impostare le opzioni della riga di comando per l'integrazione con.NET Core CLI.

Per accedere all'integrazione CLI.NET Core, accedi alla directory del progetto della funzione e digita. **`dotnet lambda help`**

> **Note**
>
> Il gestore di funzioni indica quale metodo Lambda deve chiamare in risposta alla funzione richiamata. Il formato di questo campo è:. `<assembly-name>::<full-type-name>::<method-name>` Il namespace deve essere incluso nel nome del tipo.

Implementa la funzione

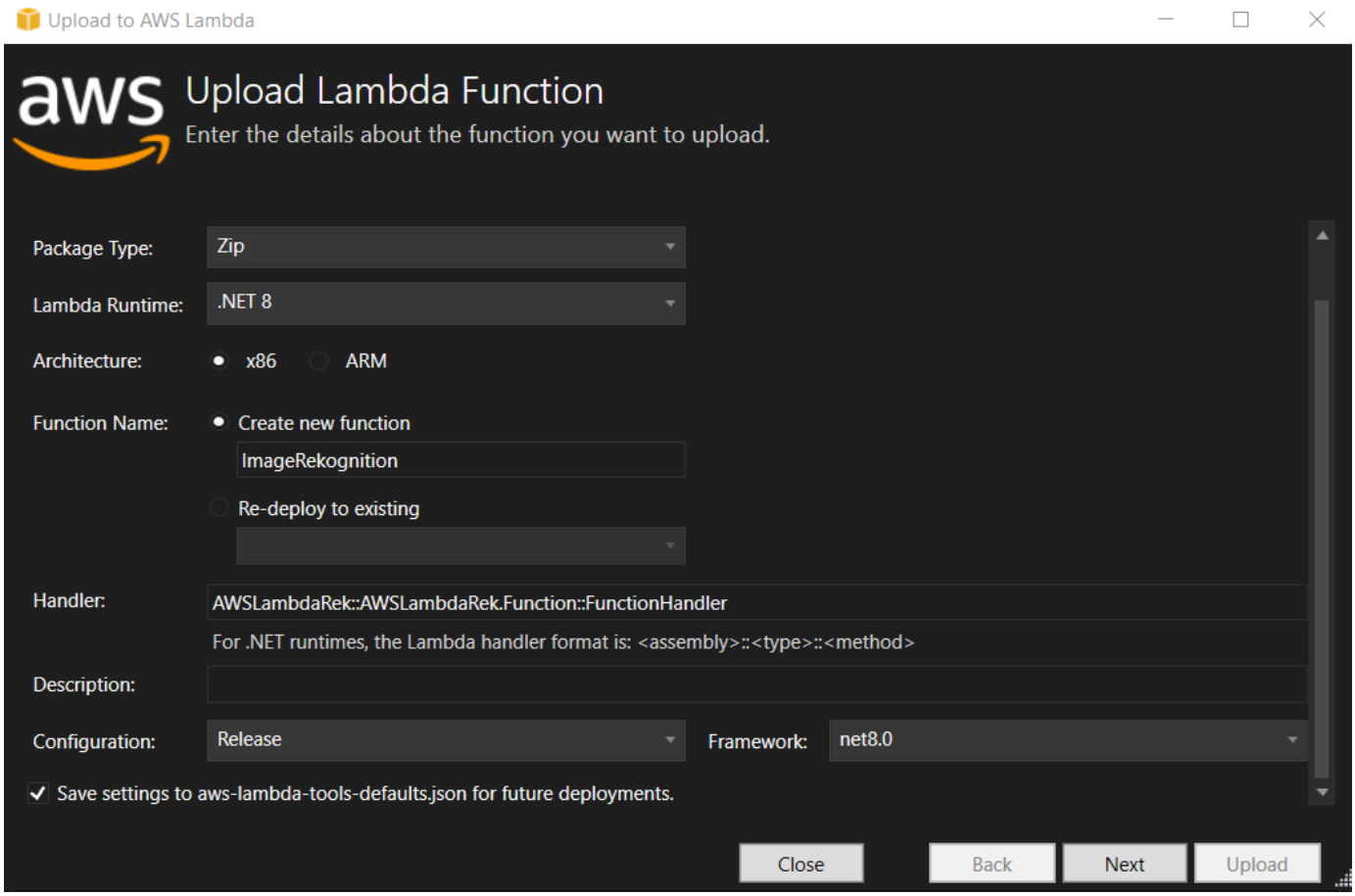
La procedura seguente descrive come distribuire la funzione Lambda.

1. Da Solution Explorer, fai clic con il pulsante destro del mouse sul progetto Lambda e scegli Pubblica su AWS Lambda per aprire la finestra Carica su. AWS Lambda

> **Note**
>
> I valori preimpostati vengono recuperati dal file. `aws-lambda-tools-defaults.json`

2. Dalla AWS Lambda finestra Carica su, inserisci un nome nel campo Nome funzione, quindi scegli il pulsante Avanti per passare alla finestra Dettagli della funzione avanzata.

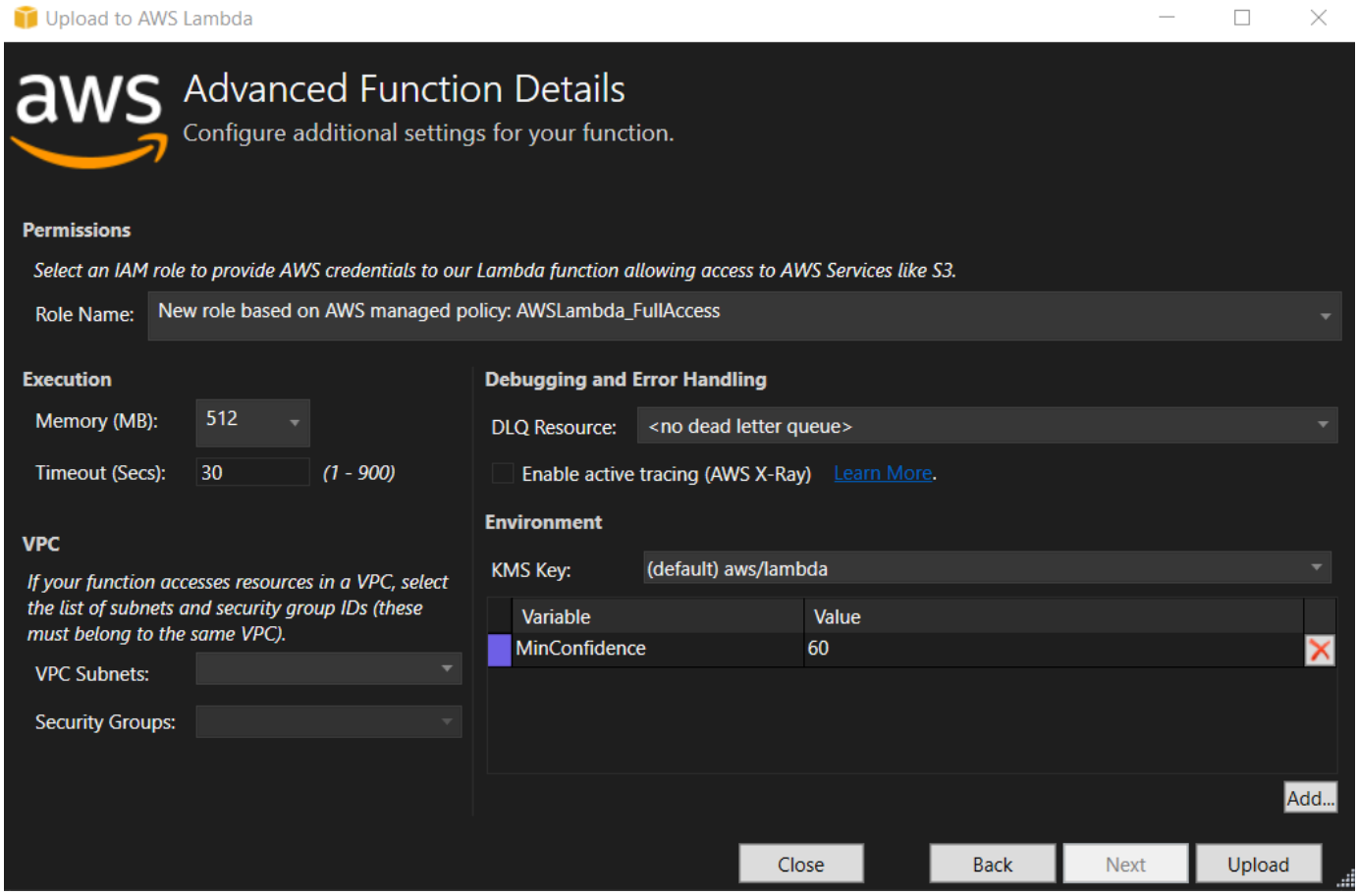
> **Note**
>
> Questo esempio utilizza il nome della funzione**`ImageRekognition`**.



3. Dalla finestra Advanced Function Details, seleziona un ruolo IAM che autorizzi il codice ad accedere alle tue risorse Amazon S3 e Amazon Rekognition.

> **Note**
>
> Se stai seguendo questo esempio, seleziona il ruolo. `AWSLambda_FullAccess`

4. Imposta la variabile `MinConfidence` di ambiente su 60, quindi scegli Carica per avviare il processo di distribuzione. Il processo di pubblicazione è completo quando la vista Function viene visualizzata in AWS Explorer.



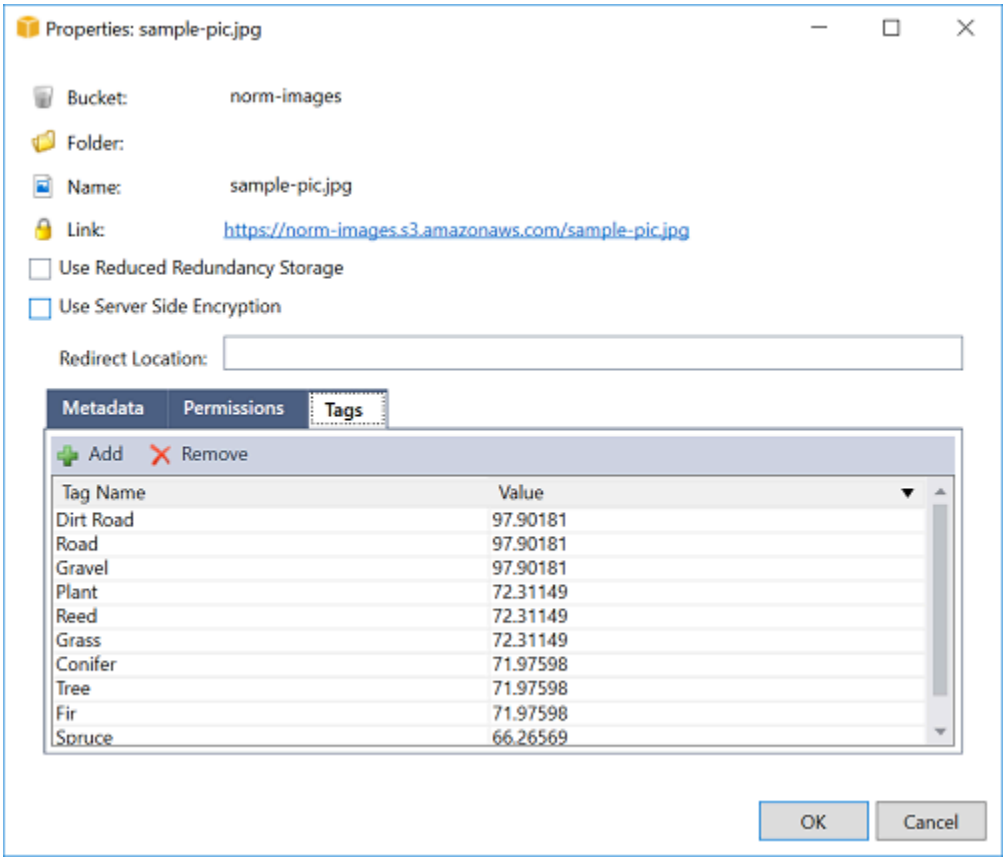
5. Dopo una distribuzione riuscita, configura Amazon S3 per inviare i suoi eventi alla tua nuova funzione accedendo alla scheda Event Sources.
6. Dalla scheda Event Sources, scegli il pulsante Aggiungi, quindi seleziona il bucket Amazon S3 per connetterti alla tua funzione Lambda.

> **Note**
>
> Il bucket deve trovarsi nella stessa AWS regione della funzione Lambda.

Esegui il test della funzione

Ora che la funzione è stata implementata e un bucket S3 è configurato come sorgente di eventi, apri il browser del bucket S3 dall'Explorer per il AWS bucket selezionato. Quindi carica alcune immagini.

Una volta completato il caricamento, puoi confermare che la tua funzione è stata eseguita guardando i log dalla visualizzazione delle funzioni. In alternativa, fate clic con il pulsante destro del mouse sulle immagini nel browser bucket e scegliete Proprietà. Nella scheda Tag, puoi visualizzare i tag applicati all'oggetto.



Tutorial: Utilizzo di Amazon Logging Frameworks AWS Lambda per creare log di applicazioni

Puoi usare Amazon CloudWatch Logs per monitorare, archiviare e accedere ai log della tua applicazione. Per inserire i dati di log in CloudWatch Logs, usa un AWS SDK o installa l'agente CloudWatch Logs per monitorare determinate cartelle di log. CloudWatch Logs è integrato con diversi framework di logging.NET diffusi, semplificando i flussi di lavoro.

Per iniziare a utilizzare i framework di registrazione CloudWatch Logs e.NET, aggiungi il NuGet pacchetto e la sorgente di output CloudWatch Logs appropriati all'applicazione, quindi usa la tua

libreria di registrazione come faresti normalmente. Ciò consente all'applicazione di registrare i messaggi con il framework.NET, inviarli a CloudWatch Logs e visualizzare i messaggi di registro dell'applicazione nella console Logs. CloudWatch Puoi anche configurare metriche e allarmi dalla console CloudWatch Logs, in base ai messaggi di registro dell'applicazione.

I framework di logging.NET supportati includono:

- NLog: Per visualizzarlo, consulta il pacchetto nuget.org. NLog
- Log4net: per visualizzarlo, vedi il pacchetto Log4net di nuget.org.
- ASP.NET Core Logging Framework: per visualizzare, consulta il pacchetto nuget.org ASP.NET Core logging Framework.

Di seguito è riportato un esempio di `NLog.config` file che abilita sia CloudWatch i log che la console come output per i messaggi di registro aggiungendo il pacchetto e la destinazione. `AWS.Logger.NLog` NuGet AWS `NLog.config`

```
<?xml version="1.0" encoding="utf-8" ?>
<nlog xmlns="http://www.nlog-project.org/schemas/NLog.xsd"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      throwExceptions="true">
  <targets>
    <target name="aws" type="AWSTarget" logGroup="NLog.ConfigExample" region="us-
east-1"/>
    <target name="logfile" xsi:type="Console" layout="${callsite} ${message}" />
  </targets>
  <rules>
    <logger name="*" minlevel="Info" writeTo="logfile,aws" />
  </rules>
</nlog>
```

I plugin di registrazione sono tutti basati su AWS SDK per .NET e autenticano le AWS credenziali in un processo simile all'SDK. L'esempio seguente descrive in dettaglio le autorizzazioni richieste dalle credenziali del plug-in di registrazione per accedere ai registri: CloudWatch

> **Note**
>
> I plugin di AWS logging.NET sono un progetto open source. Per ulteriori informazioni, esempi e istruzioni, consultate gli argomenti relativi agli esempi e alle istruzioni nel repository AWS Logging .NET. GitHub

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

Distribuzione su AWS

Il Toolkit for Visual Studio supporta la distribuzione delle applicazioni AWS Elastic Beanstalk in contenitori CloudFormation o stack.

> **Note**
>
> Se usi Visual Studio Express Edition:
>
> - Puoi utilizzare la CLI Docker per distribuire applicazioni in contenitori Amazon ECS.
> - Puoi utilizzare la console di AWS gestione per distribuire applicazioni nei contenitori Elastic Beanstalk.
>
> Per le distribuzioni di Elastic Beanstalk, devi prima creare un pacchetto di distribuzione web. Per ulteriori informazioni, vedi Procedura: creare un pacchetto di distribuzione Web in Visual Studio. Per la distribuzione di Amazon ECS, è necessario disporre di un'immagine Docker. Per ulteriori informazioni, consulta Visual Studio Tools for Docker.

Argomenti

Utilizzo di Publish to AWS in Visual Studio

Publish to AWS è un'esperienza di distribuzione interattiva che consente di pubblicare le applicazioni.NET su obiettivi di AWS distribuzione, supportando applicazioni destinate a .NET Core 3.1 e versioni successive. La collaborazione con Publish consente di AWS mantenere il flusso di lavoro all'interno di Visual Studio rendendo disponibili queste funzionalità di distribuzione direttamente dal tuo IDE:

- La possibilità di distribuire l'applicazione con un solo clic.

- Consigli di implementazione basati sull'applicazione in uso.
- Creazione automatica di Dockerfile, in base a quanto pertinente e richiesto dall'ambiente della destinazione di distribuzione (obiettivo di distribuzione).
- Impostazioni ottimizzate per la creazione e il pacchetto delle applicazioni, come richiesto dall'obiettivo di distribuzione.

> **Note**
>
> Per ulteriori informazioni sulla pubblicazione di applicazioni.NET Framework, consulta la guida Creazione e distribuzione di applicazioni.NET su Elastic Beanstalk
> Puoi accedere a Publish to anche AWS dall'interfaccia della riga di comando .NET. Per ulteriori informazioni, consulta la guida Deploy .NET applications on AWS.

Argomenti

Prerequisiti

Per pubblicare correttamente le applicazioni.NET su un AWS servizio, installa quanto segue sul tuo dispositivo locale:

- .NET Core 3.1+ (che include. NET5 e. NET6): Per ulteriori informazioni su questi prodotti e sul download, visita il sito di download di Microsoft.
- Node.js 14.x o versione successiva: per l'esecuzione AWS Cloud Development Kit (AWS CDK)è necessario Node.js. Per scaricare o ottenere ulteriori informazioni su Node.js, visita il sito di download di Node.js.

> **Note**
>
> Publish to AWS utilizza AWS CDK per distribuire l'applicazione e tutta la relativa infrastruttura di distribuzione come un unico progetto. Per ulteriori informazioni, AWS CDK consulta la guida Cloud Development Kit.

- (Facoltativo) Docker viene utilizzato durante la distribuzione su un servizio basato su container come Amazon ECS. Per ulteriori informazioni e per scaricare Docker, consulta il sito di download di Docker.

Tipi di applicazioni supportati

Prima di pubblicare su una destinazione nuova o uscire, inizia creando o aprendo uno dei seguenti tipi di progetto in Visual Studio:

- Applicazione ASP.NET Core
- applicazione.NET Console
- Applicazione Blazor WebAssembly

Pubblicazione di applicazioni su obiettivi AWS

Quando pubblicate su una nuova destinazione, Publish to vi AWS guiderà attraverso il processo formulando consigli e utilizzando impostazioni comuni. Se devi pubblicare su una destinazione impostata in precedenza, le tue preferenze vengono archiviate e possono essere modificate oppure sono immediatamente disponibili per la distribuzione con un solo clic.

> **Note**
>
> Integrazione dei toolkit con il server CLI DI.NET:
> Publishing avvia un processo server.NET sull'host locale per eseguire il processo di pubblicazione.

Pubblica su una nuova destinazione

Di seguito viene descritto come configurare le preferenze di pubblicazione su Publish to AWS deployment, quando si pubblica su una nuova destinazione.

1. Da AWS Explorer, espandi il menu a discesa Credenziali, quindi scegli il AWS profilo corrispondente alla regione e AWS ai servizi necessari per la distribuzione.
2. Espandi il menu a discesa Regione, quindi scegli la AWS regione che contiene AWS i servizi necessari per la distribuzione.

3. Dal riquadro Visual Studio Solutions Explorer, apri il menu contestuale per (fai clic con il pulsante destro del mouse) sul nome del progetto e scegli Pubblica su. AWS Si aprirà Pubblica su AWS.
4. Da Pubblica a AWS, scegli Pubblica su nuova destinazione per configurare una nuova distribuzione.

> **Note**
>
> Per modificare le credenziali di distribuzione predefinite, scegli o fai clic sul link Modifica situato accanto alla sezione Credenziali, in Pubblica su. AWS
> Per aggirare il processo di configurazione della destinazione, scegli Pubblica su destinazione esistente, quindi scegli la configurazione preferita dall'elenco degli obiettivi di distribuzione precedenti.

5. Dal riquadro Publish Targets, scegli un AWS servizio per gestire la distribuzione dell'applicazione.
6. Quando sei soddisfatto della configurazione, scegli Pubblica per avviare il processo di distribuzione.

> **Note**
>
> Dopo aver avviato una distribuzione, Publish to AWS visualizza i seguenti aggiornamenti di stato:
>
> - Durante il processo di distribuzione, Publish to AWS visualizza informazioni sull'avanzamento della distribuzione.
> - Dopo il processo di distribuzione, Publish to AWS indica se la distribuzione è riuscita o meno.
> - Dopo una distribuzione riuscita, il pannello Risorse offre informazioni aggiuntive sulla risorsa che è stata creata. Queste informazioni varieranno a seconda del tipo di applicazione e della configurazione di distribuzione.

Pubblica su una destinazione esistente

Di seguito viene descritto come ripubblicare l'applicazione.NET su una AWS destinazione esistente.

1. Da AWS Explorer, espandi il menu a discesa Credenziali, quindi scegli il AWS profilo che corrisponde alla regione e AWS ai servizi necessari per la distribuzione.
2. Espandi il menu a discesa Regione, quindi scegli la AWS regione che contiene AWS i servizi necessari per la distribuzione.
3. Dal riquadro Visual Studio Solutions Explorer, fai clic con il pulsante destro del mouse sul nome del progetto e scegli Pubblica su per AWS aprire Pubblica su. AWS
4. Da Pubblica a AWS, scegli Pubblica su destinazione esistente per selezionare l'ambiente di distribuzione da un elenco di destinazioni esistenti.

   > **Note**
   >
   > Se di recente hai pubblicato delle applicazioni sul AWS Cloud, tali applicazioni vengono visualizzate in Pubblica su AWS.

5. Seleziona la destinazione di pubblicazione su cui vuoi distribuire l'applicazione, quindi fai clic su Pubblica per avviare il processo di distribuzione.

Distribuzione di un AWS Lambda progetto con la CLI.NET Core

AWS Toolkit for Visual Studio Include modelli di AWS Lambda progetto.NET Core per Visual Studio. Puoi distribuire funzioni Lambda integrate in Visual Studio utilizzando l'interfaccia a riga di comando (CLI) .NET Core.

Argomenti

Prerequisiti

Prima di utilizzare l'interfaccia CLI.NET Core per distribuire le funzioni Lambda, è necessario soddisfare i seguenti prerequisiti:

- Assicurati che Visual Studio 2015 Update 3 sia installato.

- Installa .NET Core per Windows.
- Configura la CLI.NET Core per l'utilizzo con Lambda. Per ulteriori informazioni, consulta.NET Core CLI nella AWS Lambda Developer Guide.
- Installa il Toolkit for Visual Studio. Per ulteriori informazioni, consulta Installazione del AWS Toolkit for Visual Studio.

Argomenti correlati

I seguenti argomenti correlati possono essere utili quando utilizzi la CLI.NET Core per distribuire le funzioni Lambda:

- Per ulteriori informazioni sulle funzioni Lambda, vedi Cos'è AWS Lambda? nella Guida per gli AWS Lambda sviluppatori.
- Per informazioni sulla creazione di funzioni Lambda in Visual Studio, vedi. AWS Lambda
- Per ulteriori informazioni su Microsoft.NET Core, consulta.NET Core nella documentazione online di Microsoft.

Elenco dei comandi Lambda disponibili tramite la CLI.NET Core

Per elencare i comandi Lambda disponibili tramite la CLI.NET Core, procedi come segue.

1. Apri una finestra del prompt dei comandi e accedi alla cartella contenente un progetto Lambda di Visual Studio .NET Core.
2. Specificare `dotnet lambda --help`.

```
C:\Lambda\AWSLambda1\AWSLambda1>dotnet lambda --help AWS Lambda Tools for .NET Core
 functions
    Project Home: https://github.com/aws/aws-lambda-dotnet
    .
    Commands to deploy and manage Lambda functions:
    .
            deploy-function         Deploy the project to Lambda
            invoke-function         Invoke the function in Lambda with an optional
 input
            list-functions          List all of your Lambda functions
            delete-function         Delete a Lambda function
```

```
            get-function-config     Get the current runtime configuration for a Lambda
function
            update-function-config  Update the runtime configuration for a Lambda
function
   .
   Commands to deploy and manage AWS serverless applications using AWS CloudFormation:
   .
            deploy-serverless       Deploy an AWS serverless application
            list-serverless         List all of your AWS serverless applications
            delete-serverless       Delete an AWS serverless application
   .
   Other Commands:
   .
            package                 Package a Lambda project into a .zip file ready for
deployment
   .
   To get help on individual commands, run the following:

            dotnet lambda help <command>
```

Pubblicazione di un progetto.NET Core Lambda da.NET Core CLI

Le seguenti istruzioni presuppongono che tu abbia creato una AWS Lambda funzione.NET Core in Visual Studio.

1. Apri una finestra del prompt dei comandi e accedi alla cartella contenente il tuo progetto Visual Studio .NET Core Lambda.
2. Specificare `dotnet lambda deploy-function`.
3. Quando richiesto, inserisci il nome della funzione da distribuire. Può essere un nuovo nome o il nome di una funzione esistente.
4. Quando richiesto, inserisci la AWS regione (la regione in cui verrà distribuita la funzione Lambda).
5. Quando richiesto, seleziona o crea il ruolo IAM che Lambda assumerà durante l'esecuzione della funzione.

Una volta completato con successo, viene visualizzato il messaggio Nuova funzione Lambda creata.

```
C:\Lambda\AWSLambda1\AWSLambda1>dotnet lambda deploy-function
Executing publish command
... invoking 'dotnet publish', working folder 'C:\Lambda\AWSLambda1\AWSLambda1\bin
\Release\netcoreapp1.0\publish'
```

```
... publish: Publishing AWSLambda1 for .NETCoreApp,Version=v1.0
... publish: Project AWSLambda1 (.NETCoreApp,Version=v1.0) will be compiled because
 expected outputs are missing
... publish: Compiling AWSLambda1 for .NETCoreApp,Version=v1.0
... publish: Compilation succeeded.
... publish:     0 Warning(s)
... publish:     0 Error(s)
... publish: Time elapsed 00:00:01.2479713
... publish:
... publish: publish: Published to C:\Lambda\AWSLambda1\AWSLambda1\bin\Release
\netcoreapp1.0\publish
... publish: Published 1/1 projects successfully
Zipping publish folder C:\Lambda\AWSLambda1\AWSLambda1\bin\Release
\netcoreapp1.0\publish to C:\Lambda\AWSLambda1\AWSLamb
da1\bin\Release\netcoreapp1.0\AWSLambda1.zip
Enter Function Name: (AWS Lambda function name)
DotNetCoreLambdaTest
Enter AWS Region: (The region to connect to AWS services)
us-west-2
Creating new Lambda function
Select IAM Role that Lambda will assume when executing function:
    1) lambda_exec_LambdaCoreFunction
    2) *** Create new IAM Role ***
1
New Lambda function created
```

Se si distribuisce una funzione esistente, la funzione di distribuzione richiede solo la regione. AWS

```
C:\Lambda\AWSLambda1\AWSLambda1>dotnet lambda deploy-function
Executing publish command
Deleted previous publish folder
... invoking 'dotnet publish', working folder 'C:\Lambda\AWSLambda1\AWSLambda1\bin
\Release\netcoreapp1.0\publish'
... publish: Publishing AWSLambda1 for .NETCoreApp,Version=v1.0
... publish: Project AWSLambda1 (.NETCoreApp,Version=v1.0) was previously compiled.
 Skipping compilation.
... publish: publish: Published to C:\Lambda\AWSLambda1\AWSLambda1\bin\Release
\netcoreapp1.0\publish
... publish: Published 1/1 projects successfully
Zipping publish folder C:\Lambda\AWSLambda1\AWSLambda1\bin\Release
\netcoreapp1.0\publish to C:\Lambda\AWSLambda1\AWSLamb
da1\bin\Release\netcoreapp1.0\AWSLambda1.zip
Enter Function Name: (AWS Lambda function name)
```

```
DotNetCoreLambdaTest
Enter AWS Region: (The region to connect to AWS services)
us-west-2
Updating code for existing function
```

Una volta implementata, la funzione Lambda è pronta per l'uso. Per ulteriori informazioni, consulta Esempi di utilizzo di AWS Lambda.

Lambda monitora automaticamente le funzioni Lambda per te, riportando i parametri tramite Amazon. CloudWatch Per monitorare e risolvere i problemi della tua funzione Lambda, consulta Risoluzione dei problemi e monitoraggio delle funzioni AWS Lambda con Amazon. CloudWatch

Distribuzione AWS Elastic Beanstalk in Visual Studio utilizzando AWS Toolkit for Visual Studio con Amazon Q

AWS Elastic Beanstalk è un servizio che semplifica il processo di approvvigionamento AWS delle risorse per l'applicazione. Elastic Beanstalk fornisce tutta l'infrastruttura necessaria per AWS distribuire l'applicazione. Questa infrastruttura include:

- Istanze Amazon EC2 che ospitano i file eseguibili e i contenuti per la tua applicazione.
- Un gruppo Auto Scaling per mantenere il numero appropriato di istanze Amazon EC2 per supportare la tua applicazione.
- Un sistema di bilanciamento del carico Elastic Load Balancing che indirizza il traffico in entrata verso l'istanza Amazon EC2 con la maggiore larghezza di banda.

Questo argomento della guida per l'utente descrive come utilizzare la procedura guidata Elastic Beanstalk AWS nel Toolkit with Amazon Q. Per informazioni dettagliate specifiche su Elastic Beanstalk, consulta la Developer Guide. AWS Elastic Beanstalk La procedura guidata Elastic Beanstalk AWS per il Toolkit con Amazon Q è descritta nelle seguenti sezioni degli argomenti.

Argomenti

- Distribuisci un'applicazione ASP.NET tradizionale su Elastic Beanstalk
- Distribuzione di un'applicazione ASP.NET Core su Elastic Beanstalk (Legacy)
- Come specificare le credenziali AWS di sicurezza per l'applicazione
- Come ripubblicare l'applicazione in un ambiente Elastic Beanstalk (Legacy)
- Implementazioni di applicazioni Elastic Beanstalk personalizzate

- Distribuzioni personalizzate di ASP.NET Core Elastic Beanstalk
- Supporto di più applicazioni per.NET ed Elastic Beanstalk

Distribuisci un'applicazione ASP.NET tradizionale su Elastic Beanstalk

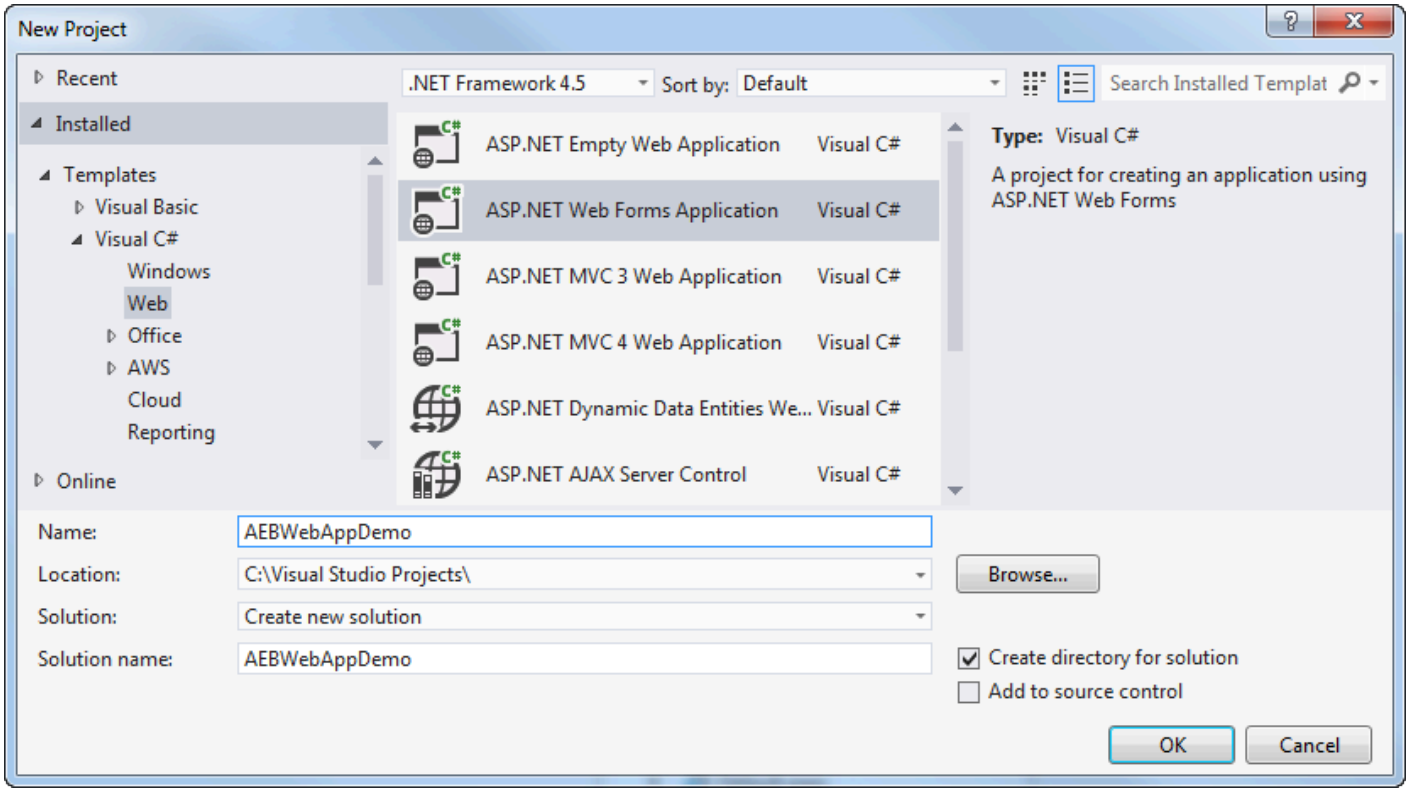
Questa sezione descrive come utilizzare la procedura guidata di pubblicazione su Elastic Beanstalk, fornita come parte del Toolkit for Visual Studio, per distribuire un'applicazione tramite Elastic Beanstalk. Per esercitarti, puoi usare un'istanza di un progetto di avvio di un'applicazione Web integrato in Visual Studio oppure puoi usare il tuo progetto.

> **Note**
>
> La procedura guidata supporta anche la distribuzione di applicazioni ASP.NET Core. Per informazioni su ASP.NET Core, consulta la guida agli strumenti di AWS distribuzione.NET e il sommario Deploying to aggiornato. AWS

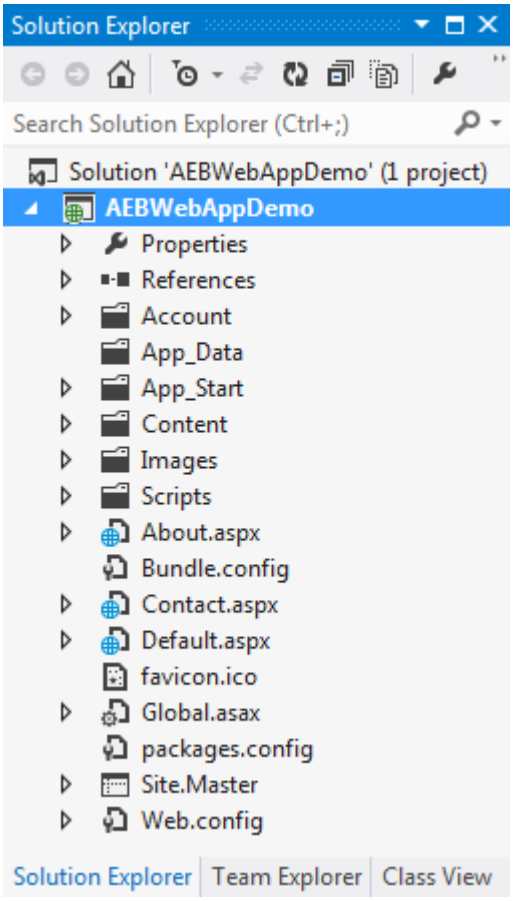
> **Note**
>
> Prima di poter utilizzare la procedura guidata di pubblicazione su Elastic Beanstalk, è necessario scaricare e installare Web Deploy. La procedura guidata si basa su Web Deploy per distribuire applicazioni Web e siti Web sui server Web di Internet Information Services (IIS).

Per creare un esempio di progetto di avvio di un'applicazione Web

1. In Visual Studio, dal menu File, scegli Nuovo, quindi scegli Progetto.
2. Nel riquadro di navigazione della finestra di dialogo New Project (Nuovo progetto), espandere Installed (Installato), espandere Templates (Modelli), espandere Visual C# e quindi scegliere Web.
3. Nell'elenco di modelli di progetto Web, scegliere un modello che contiene le parole `Web` e `Application` nella descrizione. Per questo esempio, scegli ASP.NET Web Forms Application.

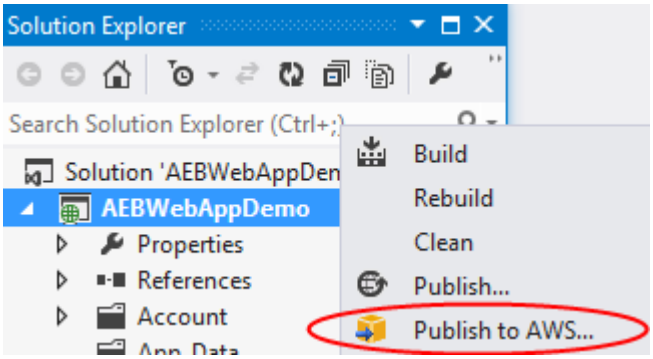


4. Nella casella Name (Nome), digitare `AEBWebAppDemo`.
5. Nella casella Posizione, digitate il percorso di una cartella di soluzione sul computer di sviluppo o scegliete Sfoglia, quindi cercate e scegliete una cartella della soluzione e scegliete Seleziona cartella.
6. Verificare che la casella Create directory for solution (Crea directory per soluzione) sia selezionata. Nell'elenco a discesa Soluzione, confermate che l'opzione Crea nuova soluzione è selezionata, quindi scegliete OK. Visual Studio creerà una soluzione e un progetto basati sul modello di progetto dell'applicazione ASP.NET Web Forms. Visual Studio mostrerà quindi Solution Explorer dove vengono visualizzati la nuova soluzione e il nuovo progetto.

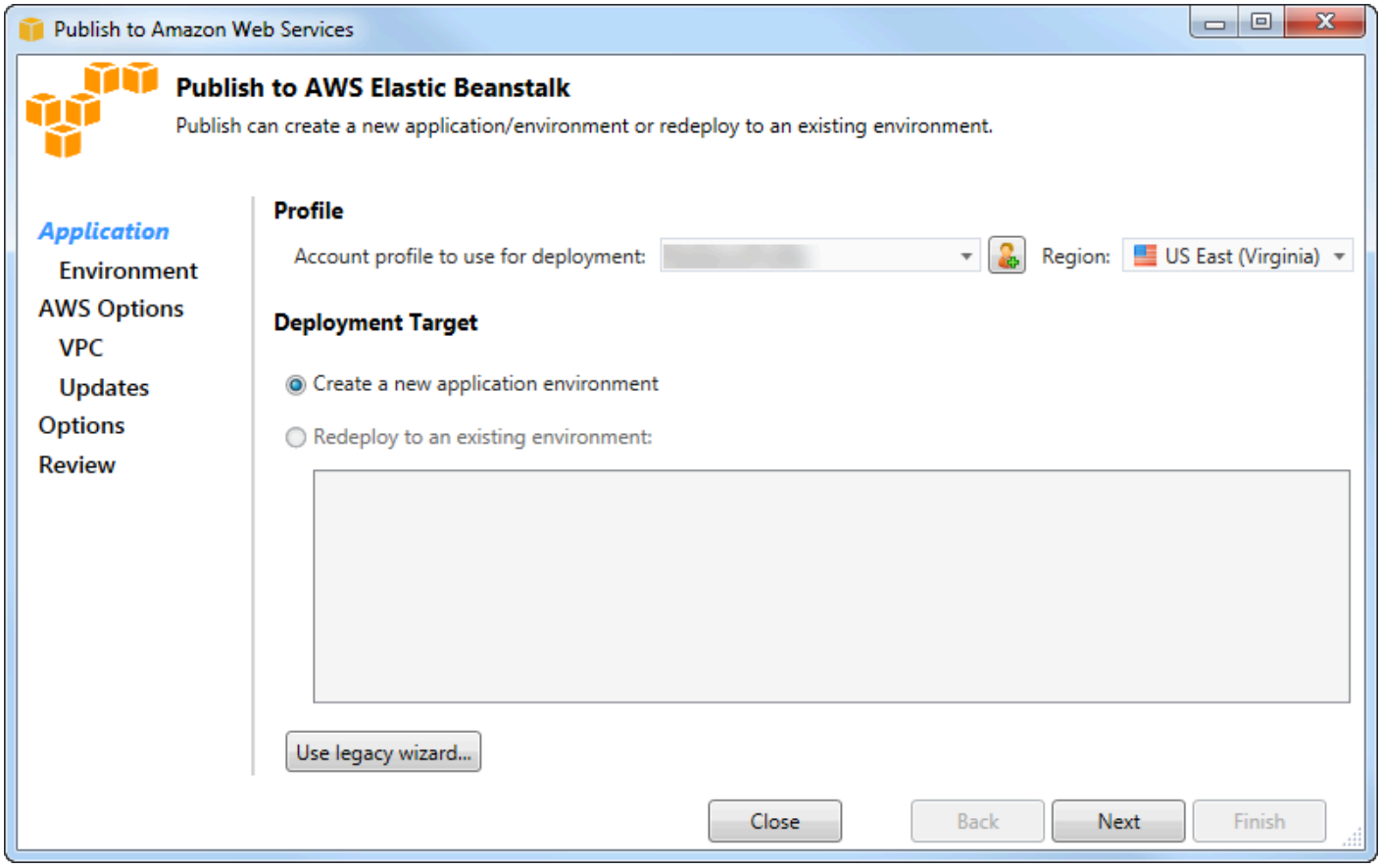


Per distribuire un'applicazione utilizzando la procedura guidata di pubblicazione su Elastic Beanstalk

1. In Solution Explorer, apri il menu contestuale (con il AEBWebAppDemopulsante destro del mouse) per la cartella di progetto per il progetto creato nella sezione precedente oppure apri il menu contestuale per la cartella di progetto per la tua applicazione e scegli Pubblica su AWS Elastic Beanstalk.



   Si apre la procedura guidata Publish to Elastic Beanstalk (Pubblica su Elastic Beanstalk).



2. In Profilo, dall'elenco a discesa Profilo dell'account da utilizzare per la distribuzione, scegli il profilo dell' AWS account che desideri utilizzare per la distribuzione.

   Facoltativamente, se desideri utilizzare un AWS account ma non ne hai ancora creato un profilo, puoi scegliere il pulsante con il simbolo più (+) per aggiungere un AWS profilo AWS account.

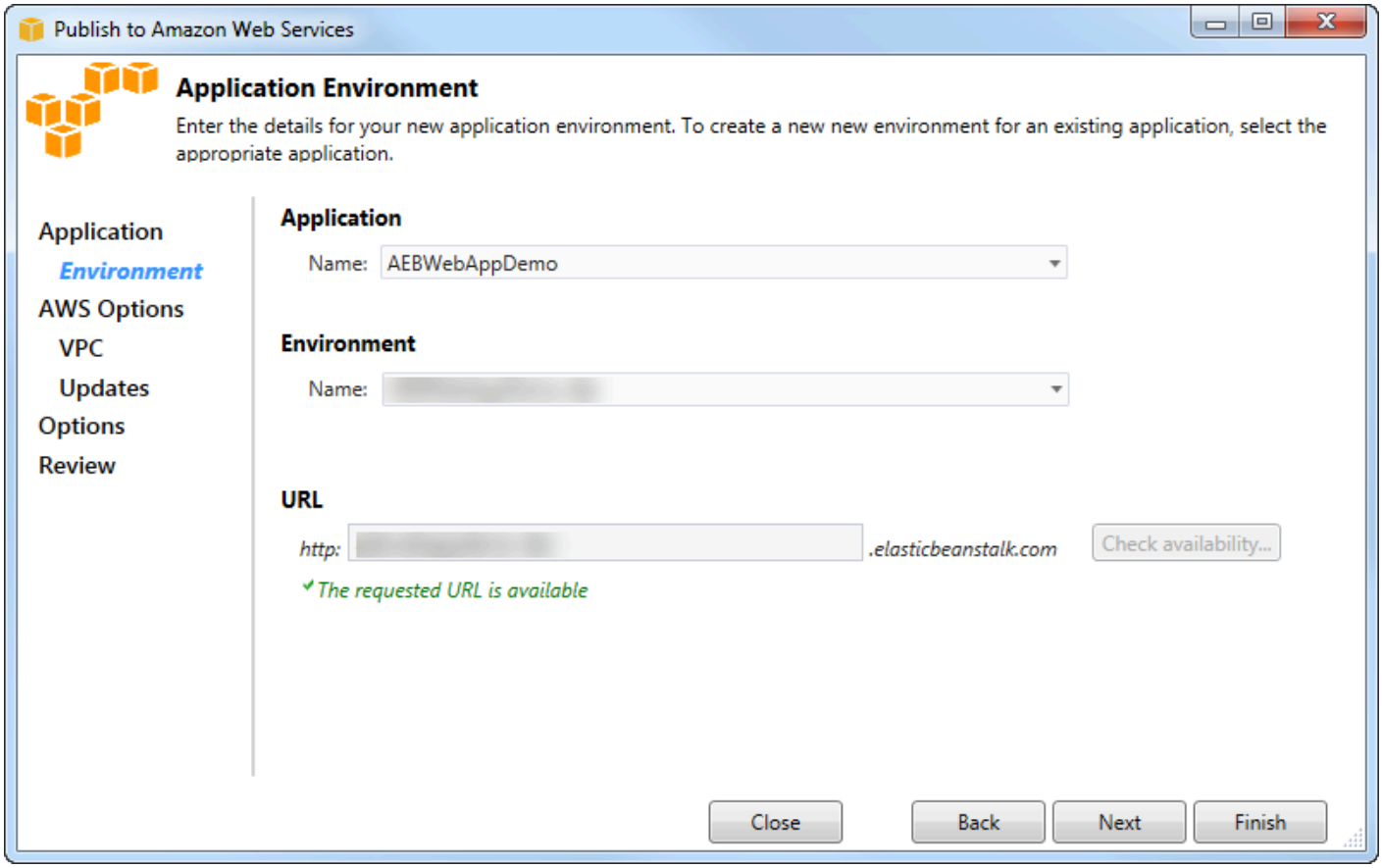
3. Dall'elenco a discesa Regione, scegli la regione in cui desideri che Elastic Beanstalk distribuisca l'applicazione.

4. In Deployment Target, puoi scegliere Crea un nuovo ambiente applicativo per eseguire una distribuzione iniziale di un'applicazione o Reimplementa in un ambiente esistente per ridistribuire un'applicazione precedentemente distribuita. (Le distribuzioni precedenti potrebbero essere state eseguite con la procedura guidata o il obsoleto Standalone Deployment Tool.) Se si sceglie Ridistribuisci in un ambiente esistente, potrebbe verificarsi un ritardo durante il recupero delle informazioni dalle distribuzioni precedenti attualmente in esecuzione.

> **Note**
>
> Se scegli Ridistribuisci in un ambiente esistente, scegli un ambiente dall'elenco e quindi scegli Avanti, la procedura guidata ti porterà direttamente alla pagina Opzioni

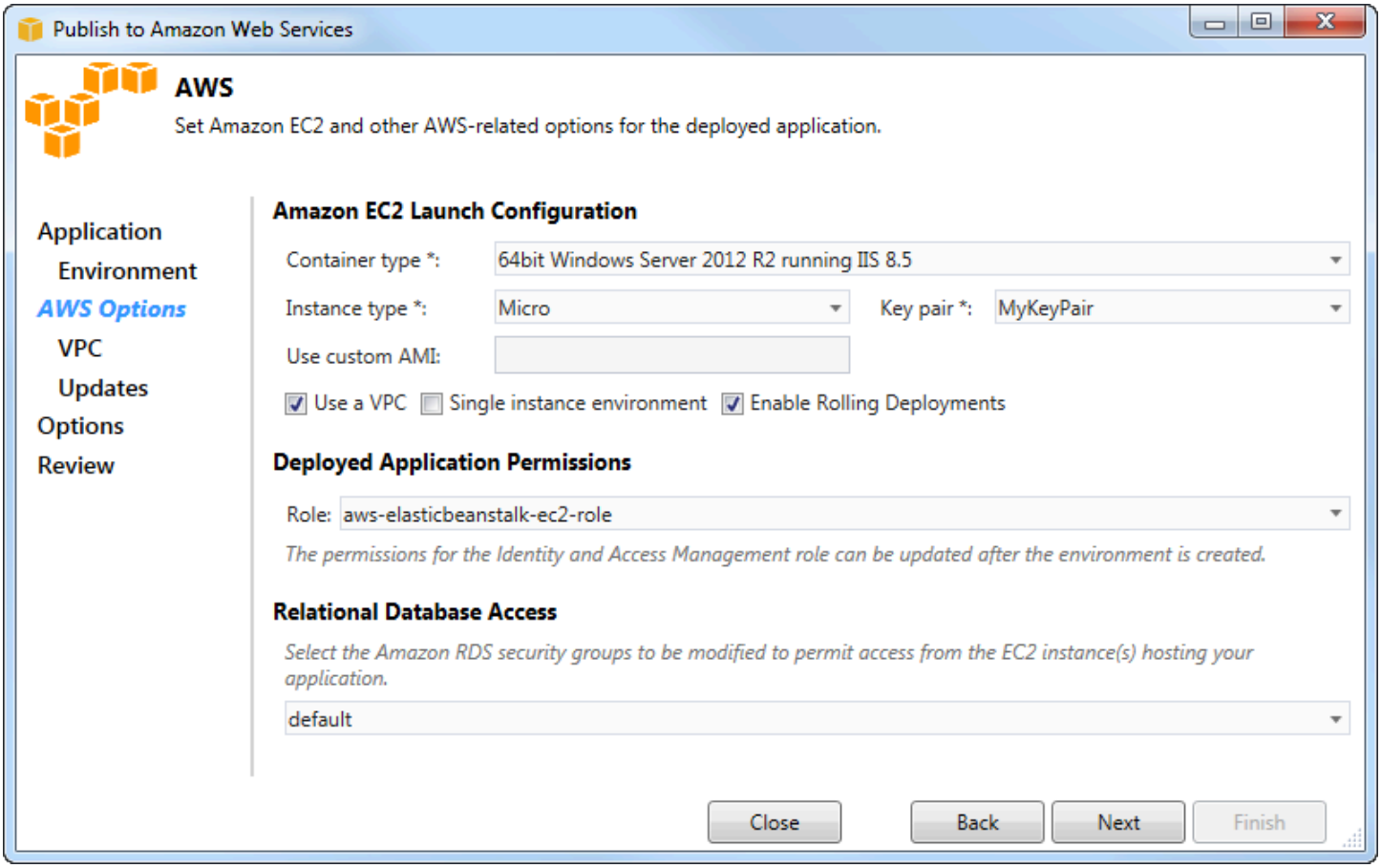
dell'applicazione. Se seguite questa strada, passate alle istruzioni riportate più avanti in questa sezione che descrivono come utilizzare la pagina Opzioni dell'applicazione.

5. Scegli Next (Successivo).



6. Nella pagina Ambiente dell'applicazione, nell'area Applicazione, l'elenco a discesa Nome propone un nome predefinito per l'applicazione. È possibile modificare il nome predefinito scegliendo un nome diverso dall'elenco a discesa.
7. Nell'area Ambiente, nell'elenco a discesa Nome, digita un nome per il tuo ambiente Elastic Beanstalk. In questo contesto, il termine ambiente si riferisce all'infrastruttura Elastic Beanstalk che fornisce l'applicazione. Un nome predefinito potrebbe già essere proposto in questo elenco a discesa. Se non è già stato proposto un nome predefinito, è possibile digitarne uno o sceglierne uno dall'elenco a discesa, se sono disponibili altri nomi. Il nome dell'ambiente non può contenere più di 23 caratteri.
8. Nell'area URL, la casella propone un sottodominio predefinito `.elasticbeanstalk.com` che sarà l'URL dell'applicazione web. È possibile modificare il sottodominio predefinito digitando un nuovo nome di sottodominio.
9. Scegli Verifica disponibilità per assicurarti che l'URL della tua applicazione web non sia già in uso.

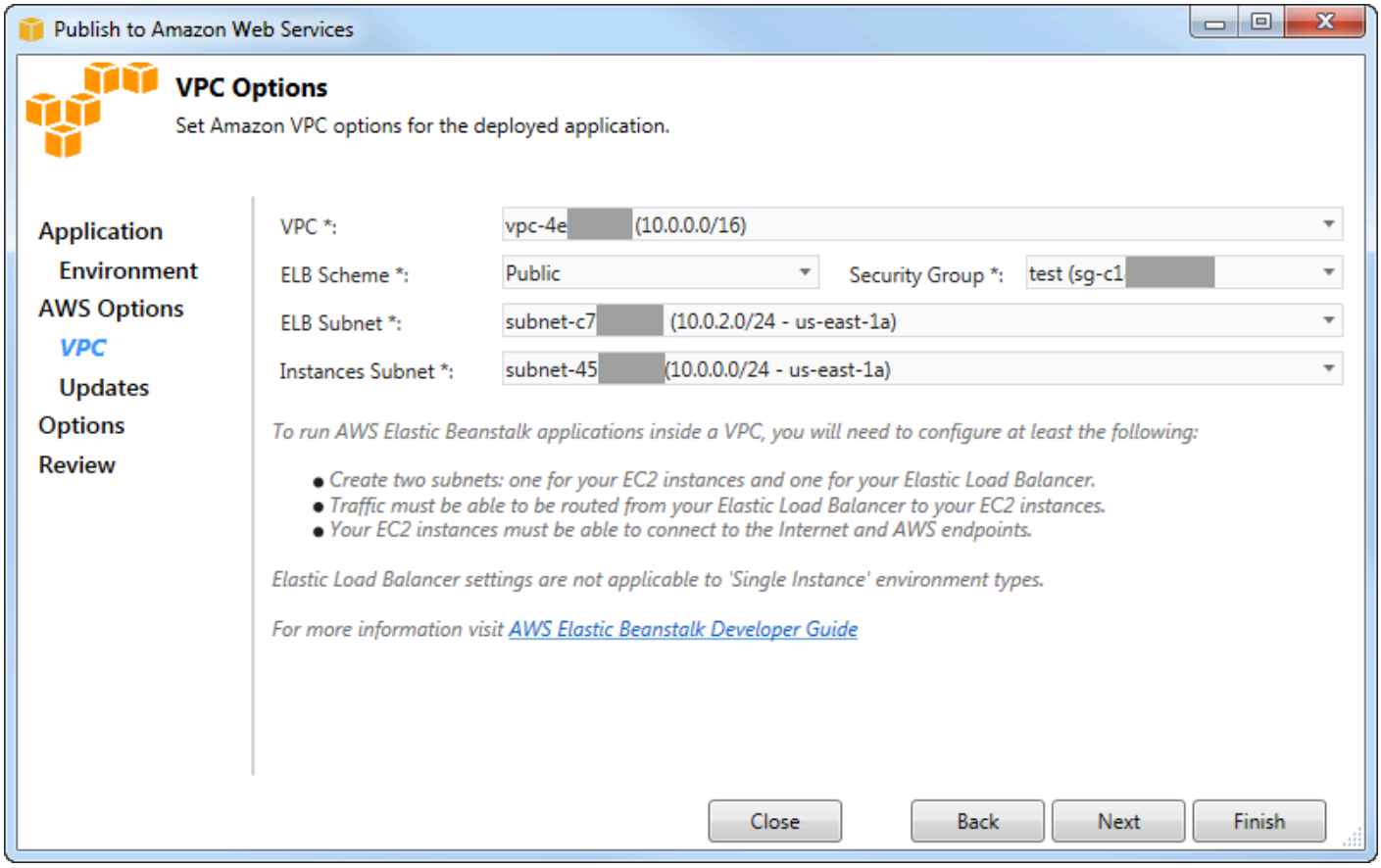
10. Se l'URL dell'applicazione Web è accettabile, scegli Avanti.



1. Nella pagina AWS Opzioni, in Amazon EC2 Launch Configuration, dall'elenco a discesa Tipo di contenitore, scegli un tipo di Amazon Machine Image (AMI) che verrà utilizzato per la tua applicazione.
2. Nell'elenco a discesa Tipo di istanza, specifica un tipo di istanza Amazon EC2 da utilizzare. Per questo esempio, ti consigliamo di utilizzare Micro. Ciò ridurrà al minimo i costi associati all'esecuzione dell'istanza. Per ulteriori informazioni sui costi di Amazon EC2, consulta la pagina dei prezzi di EC2.
3. Nell'elenco a discesa Coppia di chiavi, scegli una coppia di chiavi di istanze Amazon EC2 da utilizzare per accedere alle istanze che verranno utilizzate per la tua applicazione.
4. Facoltativamente, nella casella Usa AMI personalizzato, puoi specificare un AMI personalizzato che sostituirà l'AMI specificato nell'elenco a discesa Tipo di contenitore. Per ulteriori informazioni su come creare un'AMI personalizzata, consulta Using Custom AMIs nella AWS Elastic Beanstalk Developer Guide e Crea un'AMI da un'istanza Amazon EC2.

5. Facoltativamente, se desideri avviare le istanze in un VPC, seleziona la casella Usa un VPC.
6. Facoltativamente, se desideri avviare una singola istanza Amazon EC2 e poi distribuirvi l'applicazione, seleziona la casella Ambiente a istanza singola.

   Se selezioni questa casella, Elastic Beanstalk creerà comunque un gruppo Auto Scaling, ma non lo configurerà. Se si desidera configurare il gruppo Auto Scaling in un secondo momento, è possibile utilizzare il. Console di gestione AWS
7. Facoltativamente, se desideri controllare le condizioni in cui l'applicazione viene distribuita sulle istanze, seleziona la casella Enable Rolling Deployments. È possibile selezionare questa casella solo se non è stata selezionata la casella Ambiente a istanza singola.
8. Se la tua applicazione utilizza AWS servizi come Amazon S3 e DynamoDB, il modo migliore per fornire le credenziali è utilizzare un ruolo IAM. Nell'area Deployed Application Permissions, puoi scegliere un ruolo IAM esistente o crearne uno che la procedura guidata utilizzerà per avviare il tuo ambiente. Le applicazioni che utilizzano AWS SDK per .NET utilizzeranno automaticamente le credenziali fornite da questo ruolo IAM quando effettuano una richiesta a un servizio. AWS
9. Se la tua applicazione accede a un database Amazon RDS, nell'elenco a discesa nell'area Relational Database Access, seleziona le caselle accanto a qualsiasi gruppo di sicurezza Amazon RDS che la procedura guidata aggiornerà in modo che le tue istanze Amazon EC2 possano accedere a quel database.
10. Scegli Next (Successivo).
    - Se hai selezionato Usa un VPC, verrà visualizzata la pagina Opzioni VPC.
    - Se hai selezionato Enable Rolling Deployments, ma non hai selezionato Usa un VPC, verrà visualizzata la pagina Rolling Deployments. Passa alle istruzioni riportate più avanti in questa sezione che descrivono come utilizzare la pagina Rolling Deployments.
    - Se non hai selezionato Usa un VPC o Abilita distribuzioni in sequenza, verrà visualizzata la pagina Opzioni dell'applicazione. Passa alle istruzioni riportate più avanti in questa sezione che descrivono come utilizzare la pagina Opzioni dell'applicazione.
11. Se hai selezionato Usa un VPC, specifica le informazioni nella pagina Opzioni VPC per avviare l'applicazione in un VPC.



Il VPC deve essere già stato creato. Se hai creato il VPC nel Toolkit for Visual Studio, il Toolkit for Visual Studio popolerà questa pagina per te. Se hai creato il VPC nella console di AWS gestione, digita le informazioni sul tuo VPC in questa pagina.

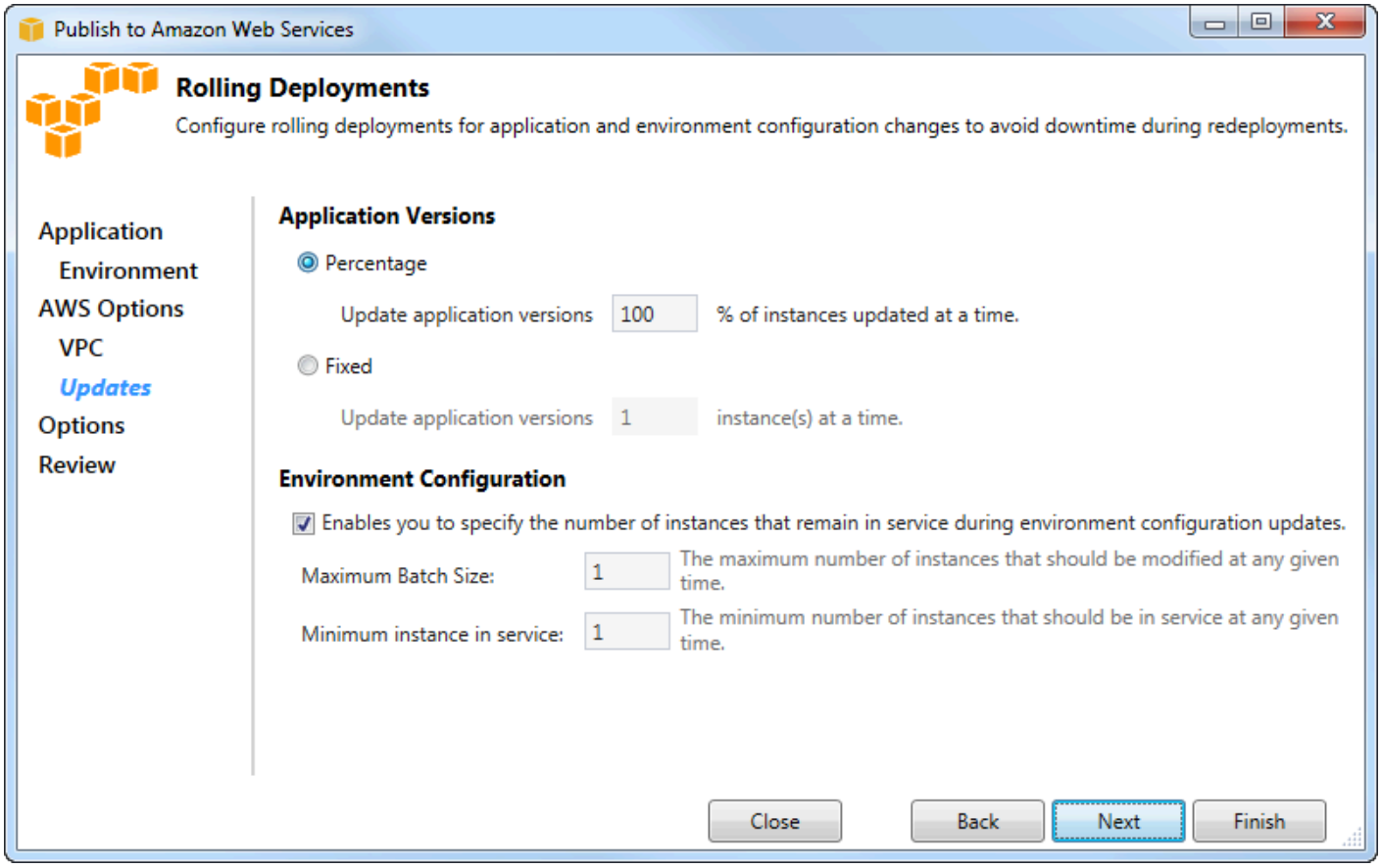
Considerazioni chiave per l'implementazione su un VPC

- Il tuo VPC necessita di almeno una sottorete pubblica e una privata.
- Nell'elenco a discesa ELB Subnet, specifica la sottorete pubblica. Il Toolkit for Visual Studio distribuisce il load balancer Elastic Load Balancing per l'applicazione nella sottorete pubblica. La sottorete pubblica è associata a una tabella di routing con una voce che punta a un gateway Internet. È possibile riconoscere un gateway Internet perché ha un ID che inizia con `igw-` (ad esempio,`igw-83cddaex`). Le sottoreti pubbliche create utilizzando Toolkit for Visual Studio hanno valori di tag che le identificano come pubbliche.
- Nell'elenco a discesa Subnet delle istanze, specifica la sottorete privata. Il Toolkit for Visual Studio distribuisce le istanze Amazon EC2 per la tua applicazione nella sottorete privata.

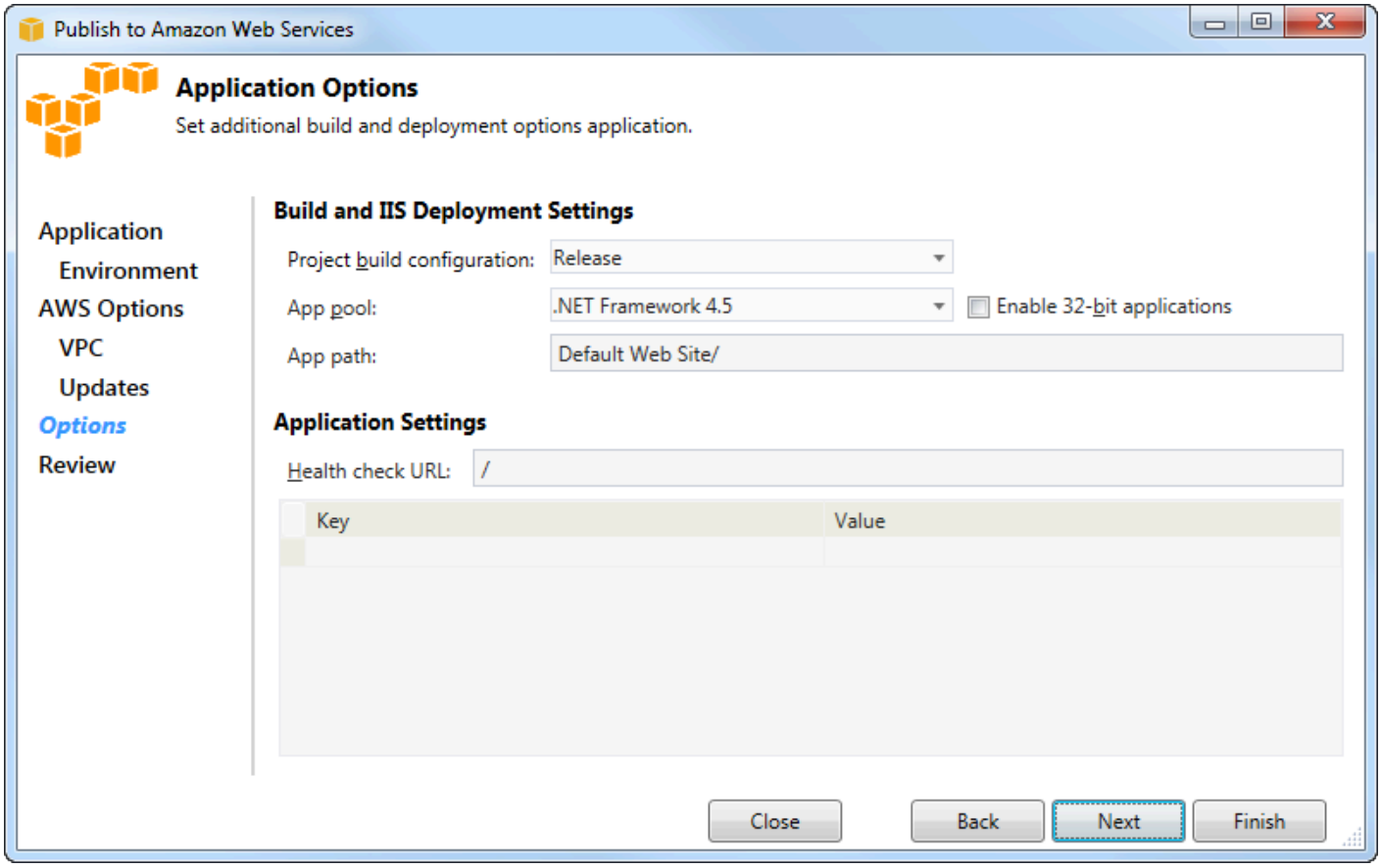
- Le istanze Amazon EC2 per la tua applicazione comunicano dalla sottorete privata a Internet tramite un'istanza Amazon EC2 nella sottorete pubblica che esegue la traduzione degli indirizzi di rete (NAT). Per abilitare questa comunicazione, è necessario un gruppo di sicurezza VPC che consenta il flusso del traffico dalla sottorete privata all'istanza NAT. Specificare questo gruppo di sicurezza VPC nell'elenco a discesa Security Group.

Per ulteriori informazioni su come distribuire un'applicazione Elastic Beanstalk su un VPC, consulta la Elastic Beanstalk Developer Guide.AWS

1. Dopo aver inserito tutte le informazioni nella pagina Opzioni VPC, scegli Avanti.
   - Se hai selezionato Enable Rolling Deployments, verrà visualizzata la pagina Rolling Deployments.
   - Se non hai selezionato Enable Rolling Deployments, verrà visualizzata la pagina Opzioni dell'applicazione. Passa alle istruzioni riportate più avanti in questa sezione che descrivono come utilizzare la pagina Opzioni dell'applicazione.
2. Se hai selezionato Enable Rolling Deployments, specifichi le informazioni nella pagina Rolling Deployments per configurare il modo in cui le nuove versioni delle applicazioni vengono distribuite alle istanze in un ambiente con bilanciamento del carico. Ad esempio, se nell'ambiente sono presenti quattro istanze e si desidera modificare il tipo di istanza, è possibile configurare l'ambiente in modo da modificare due istanze alla volta. Questo aiuta a garantire che l'applicazione sia ancora in esecuzione mentre vengono apportate le modifiche.



3. Nell'area Versioni delle applicazioni, scegli un'opzione per controllare le distribuzioni in base a una percentuale o a un numero di istanze alla volta. Specificate la percentuale o il numero desiderati.
4. Facoltativamente, nell'area Configurazione dell'ambiente, seleziona la casella se desideri specificare il numero di istanze che rimangono in servizio durante le distribuzioni. Se selezioni questa casella, specifica il numero massimo di istanze che devono essere modificate alla volta, il numero minimo di istanze che devono rimanere in servizio alla volta o entrambi.
5. Scegli Next (Successivo).
6. Nella pagina Opzioni dell'applicazione, si specificano le informazioni sulla build, su Internet Information Services (IIS) e sulle impostazioni dell'applicazione.

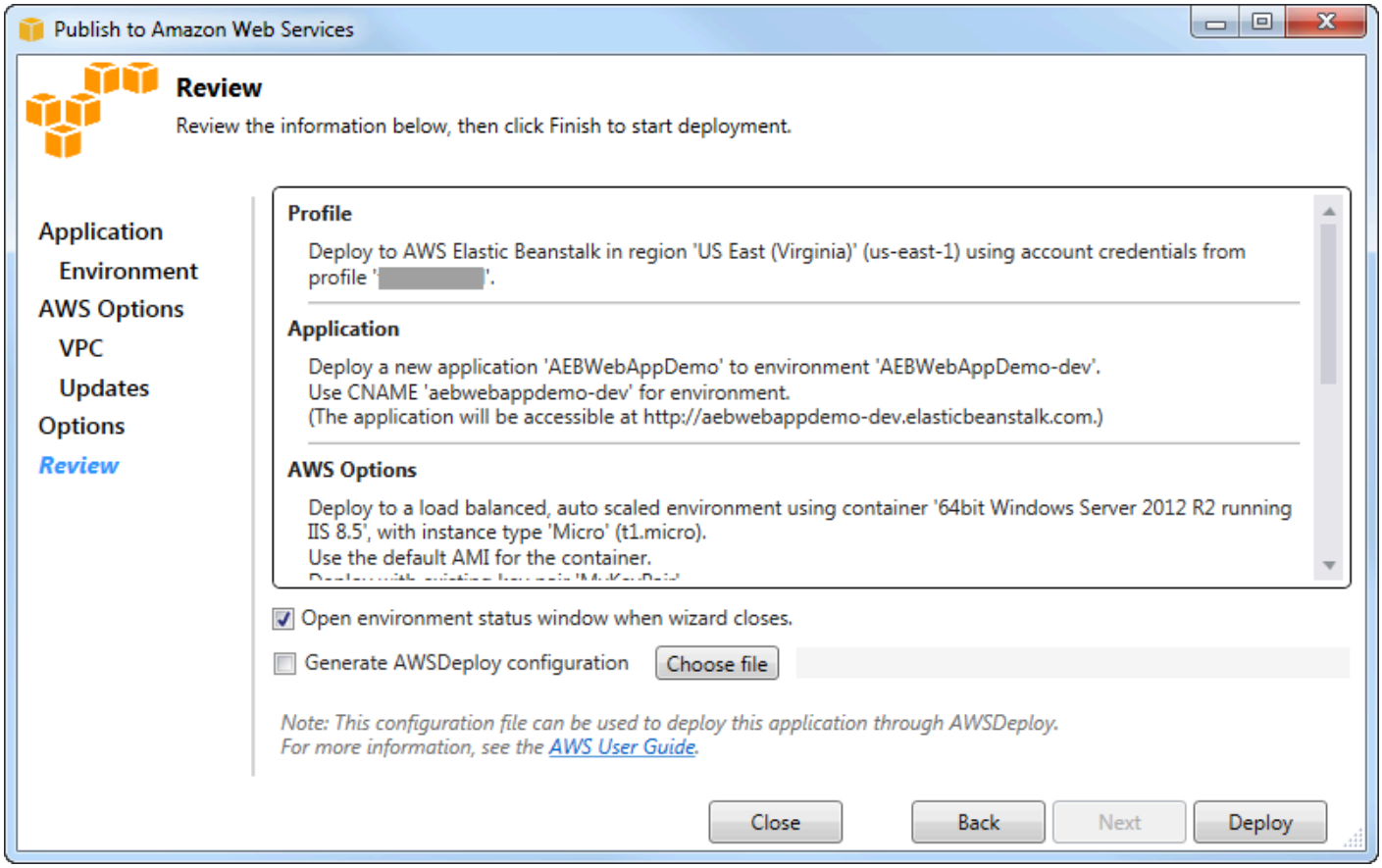


7. Nell'area Build and IIS Deployment Settings, nell'elenco a discesa Configurazione della build del progetto, scegli la configurazione della build di destinazione. Se la procedura guidata riesce a trovarla, viene visualizzato Release; in caso contrario, la configurazione attiva viene visualizzata in questa casella.
8. Nell'elenco a discesa App pool, scegli la versione di.NET Framework richiesta dall'applicazione. La versione corretta di .NET Framework dovrebbe già essere visualizzata.
9. Se l'applicazione è a 32 bit, seleziona la casella Abilita applicazioni a 32 bit.
10. Nella casella Percorso dell'app, specifica il percorso che IIS utilizzerà per distribuire l'applicazione. Per impostazione predefinita, viene specificato Default Web Site/, che in genere si traduce nel percorso. `c:\inetpub\wwwroot` Se si specifica un percorso diverso da Sito Web predefinito/, la procedura guidata inserirà un reindirizzamento nel percorso Sito Web predefinito/ che punta al percorso specificato.
11. Nell'area Impostazioni dell'applicazione, nella casella Health check URL, digita un URL per Elastic Beanstalk da verificare per determinare se l'applicazione Web è ancora reattiva. Questo URL è relativo all'URL del server principale. L'URL del server principale è specificato per impostazione predefinita. Ad esempio, se l'URL completo è`example.com/site-is-up.html`, devi digitare`/site-is-up.html`.

12 Nell'area Chiave e Valore, è possibile specificare tutte le coppie di chiavi e valori che si desidera aggiungere al `Web.config` file dell'applicazione.

> **Note**
>
> Sebbene non sia consigliabile, è possibile utilizzare l'area Chiave e Valore per specificare AWS le credenziali con cui eseguire l'applicazione. L'approccio preferito consiste nello specificare un ruolo IAM nell'elenco a discesa Identity and Access Management Role nella pagina AWS Opzioni. Tuttavia, se è necessario utilizzare AWS le credenziali anziché un ruolo IAM per eseguire l'applicazione, nella riga Chiave, scegli Chiave. AWSAccess Nella riga Valore, digita la chiave di accesso. Ripeti questi passaggi per AWSSecretKey.

13 Scegli Next (Successivo).



14 Nella pagina Revisione, esamina le opzioni configurate e seleziona la casella Apri la finestra di stato dell'ambiente alla chiusura della procedura guidata.

15 Se tutto è corretto, scegliere Deploy (Distribuisci).

> **Note**
>
> Quando si distribuisce l'applicazione, all'account attivo verranno addebitati costi per le AWS risorse utilizzate dall'applicazione.

Le informazioni sulla distribuzione verranno visualizzate nella barra di stato di Visual Studio e nella finestra Output. L'operazione potrebbe richiedere alcuni minuti. Una volta completata la distribuzione, nella finestra Output verrà visualizzato un messaggio di conferma.

16. Per eliminare la distribuzione, in AWS Explorer, espandi il nodo Elastic Beanstalk, apri il menu contestuale (fai clic con il pulsante destro del mouse) per il sottonodo per la distribuzione, quindi scegli Elimina. Il processo di eliminazione potrebbe richiedere alcuni minuti.

Distribuzione di un'applicazione ASP.NET Core su Elastic Beanstalk (Legacy)

> **Important**
>
> Questa documentazione si riferisce ai servizi e alle funzionalità legacy. Per guide e contenuti aggiornati, consulta la guida agli strumenti di AWS distribuzione.NET e il sommario Deploying to AWS aggiornato.

AWS Elastic Beanstalk è un servizio che semplifica il processo di approvvigionamento delle AWS risorse per l'applicazione. AWS Elastic Beanstalk fornisce tutta l' AWS infrastruttura necessaria per distribuire l'applicazione.

Il Toolkit for Visual Studio supporta la distribuzione di applicazioni ASP.NET Core con AWS Elastic Beanstalk. ASP.NET Core è la riprogettazione di ASP.NET con un'architettura modulare che riduce al minimo il sovraccarico di dipendenza e semplifica l'esecuzione dell'applicazione nel cloud.

AWS Elastic Beanstalk semplifica la distribuzione di applicazioni in una varietà di lingue diverse su. AWS Elastic Beanstalk supporta sia le applicazioni ASP.NET tradizionali che le applicazioni ASP.NET Core. Questo argomento descrive la distribuzione di applicazioni ASP.NET Core.

Utilizzo della procedura guidata di distribuzione

Il modo più semplice per distribuire le applicazioni ASP.NET Core su Elastic Beanstalk è con Toolkit for Visual Studio.

Se hai già utilizzato il toolkit per distribuire ASP tradizionale. Applicazioni NET, scoprirai che l'esperienza con ASP.NET Core è molto simile. Nei passaggi seguenti, illustreremo l'esperienza di implementazione.

Se non hai mai usato il toolkit prima, la prima cosa che devi fare dopo averlo installato è registrare le tue AWS credenziali nel toolkit. Vedi la documentazione Come specificare le credenziali AWS di sicurezza per l'applicazione per Visual Studio per i dettagli su come eseguire questa operazione.

Per distribuire un'applicazione Web ASP.NET Core, fai clic con il pulsante destro del mouse sul progetto in Solution Explorer e seleziona Pubblica su... AWS

Nella prima pagina della procedura guidata di pubblicazione su AWS Elastic Beanstalk distribuzione, scegli di creare una nuova applicazione Elastic Beanstalk. Un'applicazione Elastic Beanstalk è una raccolta logica di componenti di Elastic Beanstalk, tra cui gli ambienti, le versioni e le configurazioni degli ambienti. La procedura guidata di distribuzione genera un'applicazione che a sua volta contiene una raccolta di versioni e ambienti dell'applicazione. Gli ambienti contengono le AWS risorse effettive che eseguono una versione dell'applicazione. Ogni volta che si distribuisce un'applicazione, viene creata una nuova versione dell'applicazione e la procedura guidata indirizza l'ambiente a quella versione. Puoi saperne di più su questi concetti in Elastic Beanstalk Components. .

Quindi, imposta i nomi per l'applicazione e il suo primo ambiente. A ogni ambiente è associato un CNAME univoco che è possibile utilizzare per accedere all'applicazione una volta completata la distribuzione.

La pagina successiva, AWS Opzioni, consente di configurare il tipo di AWS risorse da utilizzare. Per questo esempio, lascia i valori predefiniti, ad eccezione della sezione Coppia di chiavi. Le coppie di chiavi consentono di recuperare la password dell'amministratore di Windows in modo da poter accedere al computer. Se non hai ancora creato una coppia di chiavi, potresti voler selezionare Crea nuova coppia di chiavi.

Permissions

La pagina Autorizzazioni viene utilizzata per assegnare AWS credenziali alle istanze EC2 che eseguono l'applicazione. Questo è importante se l'applicazione la utilizza per accedere ad altri servizi.

AWS SDK per .NET AWS Se non utilizzi altri servizi dell'applicazione, puoi lasciare questa pagina con le impostazioni predefinite.

Opzioni dell'applicazione

I dettagli nella pagina Opzioni dell'applicazione sono diversi da quelli specificati durante la distribuzione di applicazioni ASP.NET tradizionali. Qui, si specifica la configurazione di build e il framework utilizzati per impacchettare l'applicazione e si specifica anche il percorso delle risorse IIS per l'applicazione.

Dopo aver completato la pagina Opzioni dell'applicazione, fai clic su Avanti per rivedere le impostazioni, quindi fai clic su Distribuisci per iniziare il processo di distribuzione.

Verifica dello stato dell'ambiente

Dopo aver impacchettato e caricato l'applicazione AWS, puoi controllare lo stato dell'ambiente Elastic Beanstalk aprendo la visualizzazione AWS dello stato dell'ambiente da Explorer in Visual Studio.

Gli eventi vengono visualizzati nella barra di stato man mano che l'ambiente è online. Una volta completato tutto, lo stato dell'ambiente passerà allo stato integro. È possibile fare clic sull'URL per visualizzare il sito. Da qui, puoi anche estrarre i log dall'ambiente o dal desktop remoto nelle istanze Amazon EC2 che fanno parte del tuo ambiente Elastic Beanstalk.

La prima implementazione di qualsiasi applicazione richiederà un po' più tempo rispetto alle successive ridistribuzioni, in quanto crea nuove risorse. AWS Mentre esegui un'iterazione sull'applicazione durante lo sviluppo, puoi ridistribuirla rapidamente tornando indietro alla procedura guidata o selezionando l'opzione Ripubblica quando fai clic con il pulsante destro del mouse sul progetto.

Ripubblica i pacchetti dell'applicazione utilizzando le impostazioni dell'esecuzione precedente tramite la procedura guidata di distribuzione e carica il bundle dell'applicazione nell'ambiente Elastic Beanstalk esistente.

Come specificare le credenziali AWS di sicurezza per l'applicazione

L' AWS account specificato nella procedura guidata di pubblicazione su Elastic Beanstalk AWS è l'account che la procedura guidata utilizzerà per la distribuzione su Elastic Beanstalk.

Sebbene non sia consigliato, potrebbe essere necessario specificare anche le credenziali AWS dell'account che l'applicazione utilizzerà per accedere ai servizi dopo la distribuzione. AWS

L'approccio preferito consiste nello specificare un ruolo IAM. Nella procedura guidata di pubblicazione su Elastic Beanstalk, questa operazione viene eseguita tramite l'elenco a discesa Identity and Access Management Role nella pagina Opzioni.AWS Nella precedente procedura guidata di pubblicazione su Amazon Web Services, questa operazione viene eseguita tramite l'elenco a discesa IAM Role nella pagina Opzioni.AWS

Se devi utilizzare le credenziali dell' AWS account anziché un ruolo IAM, puoi specificare le credenziali dell' AWS account per la tua applicazione in uno dei seguenti modi:

- Fai riferimento a un profilo corrispondente alle credenziali dell' AWS account nell'`appSettings`elemento del file del progetto. `Web.config` (Per creare un profilo, consulta Configurazione delle AWS credenziali.) L'esempio seguente specifica le credenziali il cui nome di profilo è. `myProfile`

  ```
  <appSettings>
    <!-- AWS CREDENTIALS -->
    <add key="AWSProfileName" value="myProfile"/>
  </appSettings>
  ```

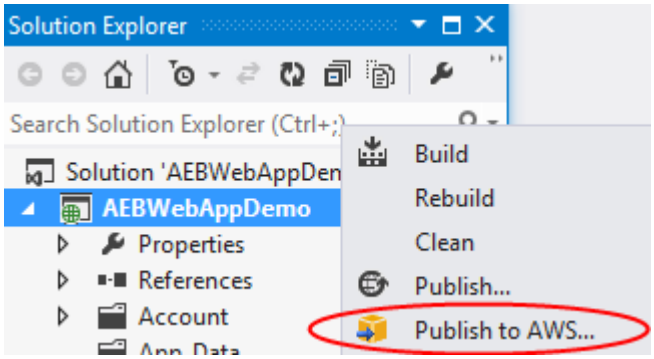
- Se utilizzi la procedura guidata di pubblicazione su Elastic Beanstalk, nella pagina Opzioni dell'applicazione, nella riga Chiave dell'area Chiave e valore, scegli. AWS AccessKey Nella riga Valore, digita la chiave di accesso. Ripeti questi passaggi per AWS SecretKey.
- Se utilizzi la procedura guidata precedente di pubblicazione su Amazon Web Services, nella pagina Opzioni dell'applicazione, nell'area Credenziali dell'applicazione, scegli Usa queste credenziali, quindi digita la chiave di accesso e la chiave di accesso segreta nelle caselle Chiave di accesso e Chiave segreta.

Come ripubblicare l'applicazione in un ambiente Elastic Beanstalk (Legacy)

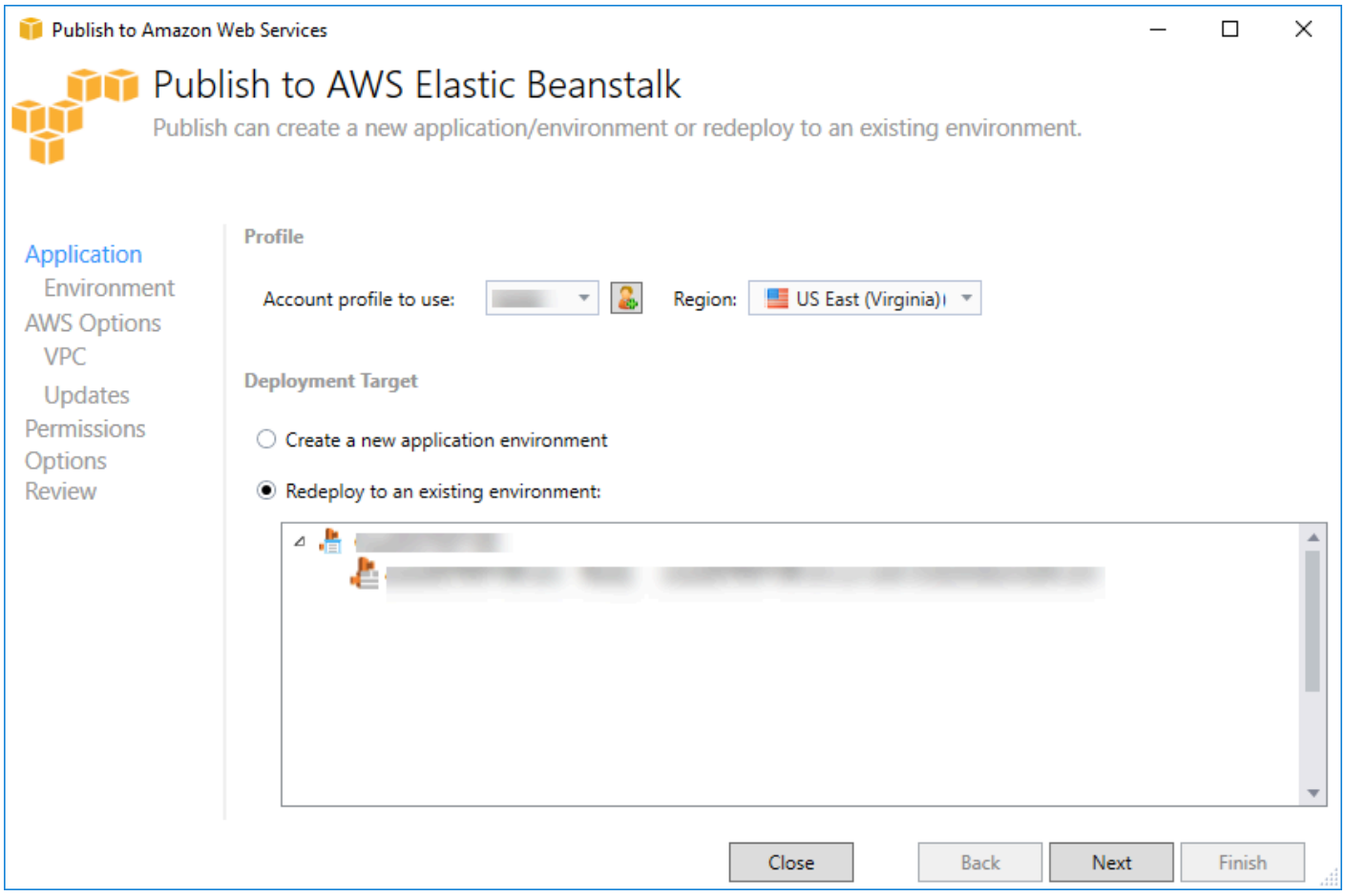
> **Important**
>
> Questa documentazione si riferisce ai servizi e alle funzionalità legacy. Per guide e contenuti aggiornati, consulta la guida agli strumenti di AWS distribuzione.NET.

Puoi iterare sulla tua applicazione apportando modifiche discrete e quindi ripubblicando una nuova versione nell'ambiente Elastic Beanstalk già avviato.

1. In Solution Explorer, apri il menu contestuale (fai clic con il pulsante destro del AEBWebAppDemomouse) per la cartella del progetto che hai pubblicato nella sezione precedente e scegli Pubblica su. AWS Elastic Beanstalk

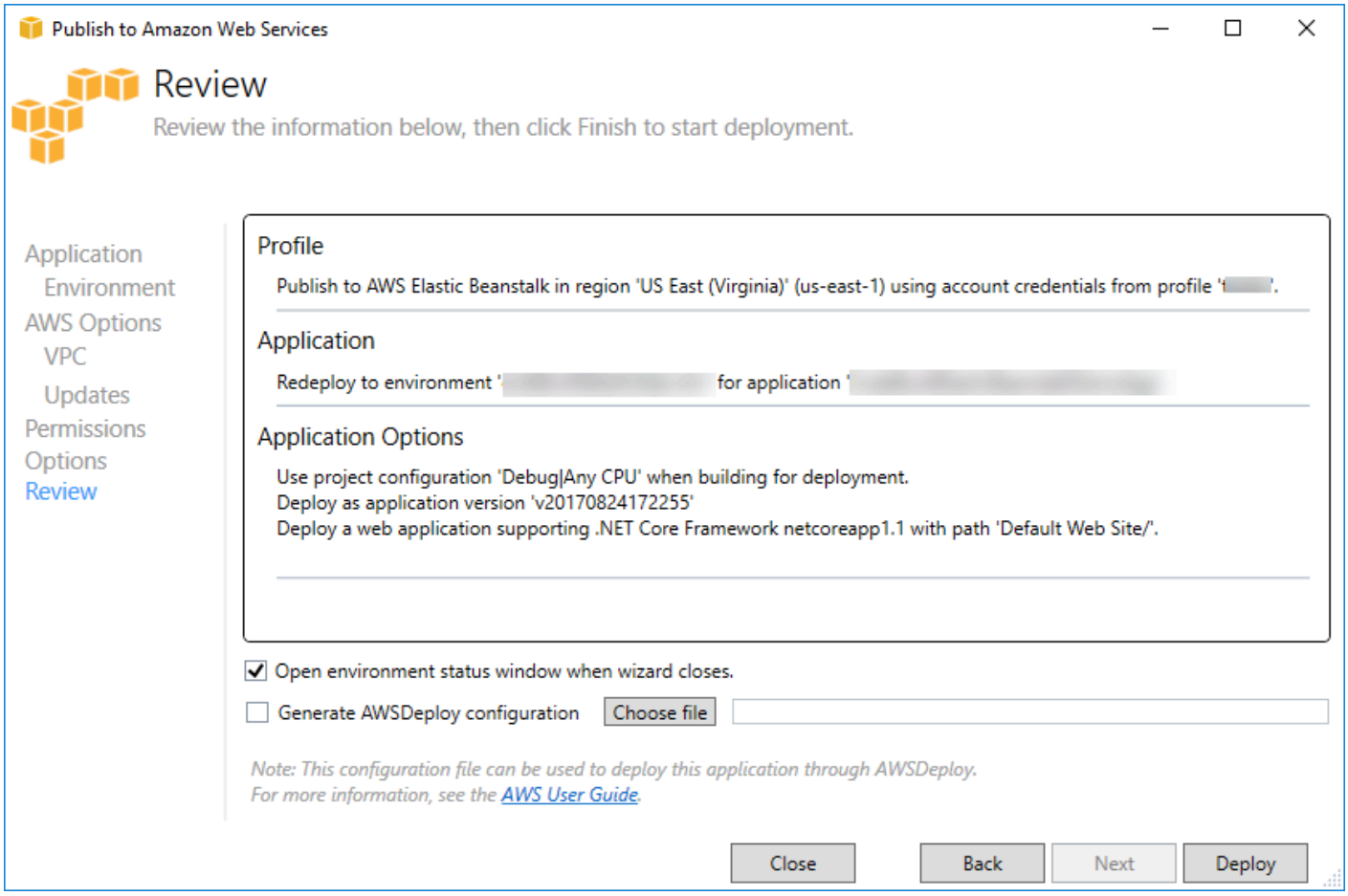


Si apre la procedura guidata Publish to Elastic Beanstalk (Pubblica su Elastic Beanstalk).



2. Seleziona Ridistribuisci in un ambiente esistente e scegli l'ambiente in cui hai pubblicato in precedenza. Fare clic su Avanti.

   Viene visualizzata la procedura guidata di revisione.



3. Fai clic su Distribuisci. L'applicazione verrà ridistribuita nello stesso ambiente.

Non è possibile ripubblicare se l'applicazione è in fase di avvio o chiusura.

Implementazioni di applicazioni Elastic Beanstalk personalizzate

Questo argomento descrive in che modo il manifesto di distribuzione per il contenitore Microsoft Windows di Elastic Beanstalk supporta le distribuzioni di applicazioni personalizzate.

Le implementazioni di applicazioni personalizzate sono una funzionalità potente per gli utenti avanzati che desiderano sfruttare la potenza di Elastic Beanstalk per creare e gestire le proprie AWS risorse, ma desiderano il controllo completo su come viene distribuita la propria applicazione. Per una distribuzione di applicazioni personalizzata, crei PowerShell script di Windows per le tre diverse azioni eseguite da Elastic Beanstalk. L'azione di installazione viene utilizzata quando viene avviata una distribuzione, il riavvio viene utilizzato quando l'`RestartAppServer`API viene richiamata dal toolkit o dalla console Web e la disinstallazione viene richiamata in qualsiasi distribuzione precedente ogni volta che si verifica una nuova distribuzione.

Ad esempio, potresti avere un'applicazione ASP.NET che desideri distribuire mentre il team di documentazione ha scritto un sito Web statico da includere nella distribuzione. Puoi farlo scrivendo il manifesto di distribuzione in questo modo:

```
{
  "manifestVersion": 1,
  "deployments": {

    "msDeploy": [
      {
        "name": "app",
        "parameters": {
          "appBundle": "CoolApp.zip",
          "iisPath": "/"
        }
      }
    ],
    "custom": [
      {
        "name": "PowerShellDocs",
        "scripts": {
          "install": {
            "file": "install.ps1"
          },
          "restart": {
            "file": "restart.ps1"
          },
          "uninstall": {
            "file": "uninstall.ps1"
          }
        }
      }
    ]
  }
}
```

Gli script elencati per ogni azione devono trovarsi nel bundle dell'applicazione relativo al file manifesto di distribuzione. Per questo esempio, il bundle dell'applicazione conterrà anche un file documentation.zip che contiene un sito Web statico creato dal team di documentazione.

Lo `install.ps1` script estrae il file zip e configura il percorso IIS.

```
Add-Type -assembly "system.io.compression.filesystem"
[io.compression.zipfile]::ExtractToDirectory('./documentation.zip', 'c:\inetpub\wwwroot
\documentation')

powershell.exe -Command {New-WebApplication -Name documentation -PhysicalPath  c:
\inetpub\wwwroot\documentation -Force}
```

Poiché l'applicazione è in esecuzione in IIS, l'azione di riavvio richiamerà un ripristino di IIS.

```
iisreset /timeout:1
```

Per gli script di disinstallazione, è importante ripulire tutte le impostazioni e i file utilizzati durante la fase di installazione. In questo modo, durante la fase di installazione della nuova versione, è possibile evitare qualsiasi collisione con le distribuzioni precedenti. Per questo esempio, è necessario rimuovere l'applicazione IIS per il sito Web statico e rimuovere i file del sito Web.

```
powershell.exe -Command {Remove-WebApplication -Name documentation}
Remove-Item -Recurse -Force 'c:\inetpub\wwwroot\documentation'
```

Con questi file di script e il file documentation.zip inclusi nel bundle dell'applicazione, la distribuzione crea l'applicazione ASP.NET e quindi distribuisce il sito di documentazione.

Per questo esempio, scegliamo un esempio semplice che distribuisce un semplice sito Web statico, ma con la distribuzione personalizzata delle applicazioni puoi distribuire qualsiasi tipo di applicazione e lasciare che Elastic Beanstalk gestisca le relative risorse. AWS

Distribuzioni personalizzate di ASP.NET Core Elastic Beanstalk

Questo argomento descrive come funziona la distribuzione e cosa è possibile fare per personalizzare le distribuzioni durante la creazione di applicazioni ASP.NET Core con Elastic Beanstalk e Toolkit for Visual Studio.

Dopo aver completato la procedura guidata di distribuzione in Toolkit for Visual Studio, il toolkit raggruppa l'applicazione e la invia a Elastic Beanstalk. Il primo passaggio nella creazione del pacchetto di applicazioni consiste nell'utilizzare la nuova CLI dotnet per preparare l'applicazione per la pubblicazione utilizzando il comando publish. Il framework e la configurazione vengono trasmessi dalle impostazioni della procedura guidata al comando publish. Quindi, se hai selezionato Release for `configuration` e netcoreapp1.0 per`framework`, il toolkit eseguirà il seguente comando:

```
dotnet publish --configuration Release --framework netcoreapp1.0
```

Al termine del comando publish, il toolkit scrive il nuovo manifesto di distribuzione nella cartella di pubblicazione. Il manifesto di distribuzione è un file JSON denominato aws-windows-deployment-manifest.json, che il contenitore Windows Elastic Beanstalk (versione 1.2 o successiva) legge per determinare come distribuire l'applicazione. Ad esempio, per un'applicazione ASP.NET Core che desideri distribuire nella radice di IIS, il toolkit genera un file manifest simile al seguente:

```
{
  "manifestVersion": 1,
  "deployments": {

    "aspNetCoreWeb": [
      {
        "name": "app",
        "parameters": {
          "appBundle": ".",
          "iisPath": "/",
          "iisWebSite": "Default Web Site"
        }
      }
    ]
  }
}
```

La `appBundle` proprietà indica dove si trovano i bit dell'applicazione rispetto al file manifest. Questa proprietà può puntare a una directory o a un archivio ZIP. Le `iisWebSite` proprietà `iisPath` and indicano dove in IIS ospitare l'applicazione.

Personalizzazione del manifesto

Il toolkit scrive il file manifesto solo se non ne esiste già uno nella cartella di pubblicazione. Se il file esiste, il toolkit aggiorna le `appBundle` `iisWebSite` proprietà `iisPath` e nella prima applicazione elencata nella `aspNetCoreWeb` sezione del manifesto. Ciò consente di aggiungere il aws-windows-deployment-manifestfile.json al progetto e personalizzare il manifest. A tale scopo, per un'applicazione Web ASP.NET Core in Visual Studio, aggiungi un nuovo file JSON alla radice del progetto e chiamalo .json. aws-windows-deployment-manifest

Il manifesto deve essere denominato aws-windows-deployment-manifest.json e deve trovarsi alla radice del progetto. Il contenitore Elastic Beanstalk cerca il manifest nella radice e, se lo trova, invoca

gli strumenti di distribuzione. Se il file non esiste, il contenitore Elastic Beanstalk ricorre ai vecchi strumenti di distribuzione, che presuppongono che l'archivio sia un archivio msdeploy.

Per garantire che il comando `publish` CLI dotnet includa il manifesto, aggiorna `project.json` il file in modo che includa il file manifest nella sezione `include` include sotto in. `publishOptions`

```
{
   "publishOptions": {
     "include": [
       "wwwroot",
       "Views",
       "Areas/**/Views",
       "appsettings.json",
       "web.config",
       "aws-windows-deployment-manifest.json"
     ]
   }
 }
```

Ora che hai dichiarato il manifesto in modo che sia incluso nel pacchetto dell'app, puoi configurare ulteriormente il modo in cui desideri distribuire l'applicazione. È possibile personalizzare la distribuzione oltre a quanto supportato dalla procedura guidata di distribuzione. AWS ha definito uno schema JSON per il aws-windows-deployment-manifestfile.json e quando hai installato Toolkit for Visual Studio, l'installazione ha registrato l'URL per lo schema.

Quando lo apri`windows-deployment-manifest.json`, vedrai l'URL dello schema selezionato nella casella a discesa Schema. Puoi accedere all'URL per ottenere una descrizione completa di ciò che può essere impostato nel manifesto. Con lo schema selezionato, Visual Studio lo fornirà IntelliSense durante la modifica del manifesto.

Una personalizzazione che puoi eseguire è configurare il pool di applicazioni IIS in cui verrà eseguita l'applicazione. L'esempio seguente mostra come definire un pool di applicazioni IIS («CustomPool») che ricicla il processo ogni 60 minuti e lo assegna all'applicazione che lo utilizza. `"appPool": "customPool"`

```
{
  "manifestVersion": 1,
  "iisConfig": {
    "appPools": [
      {
```

```
        "name": "customPool",
        "recycling": {
          "regularTimeInterval": 60
        }
      }
    ]
  },
  "deployments": {
    "aspNetCoreWeb": [
      {
        "name": "app",
        "parameters": {
          "appPool": "customPool"
        }
      }
    ]
  }
}
```

Inoltre, il manifesto può dichiarare PowerShell gli script di Windows da eseguire prima e dopo le azioni di installazione, riavvio e disinstallazione. Ad esempio, il seguente manifesto esegue lo PowerShell script di Windows `PostInstallSetup.ps1` per eseguire ulteriori operazioni di configurazione dopo la distribuzione dell'applicazione ASP.NET Core su IIS. Quando aggiungi script come questo, assicurati che vengano aggiunti alla sezione include in PublishOptions nel `project.json` file, proprio come hai fatto con il file. `aws-windows-deployment-manifest.json` In caso contrario, gli script non verranno inclusi come parte del comando di pubblicazione della CLI dotnet.

```
{
  "manifestVersion": 1,
  "deployments": {
    "aspNetCoreWeb": [
      {
        "name": "app",
        "scripts": {
          "postInstall": {
            "file": "SetupScripts/PostInstallSetup.ps1"
          }
        }
      }
    ]
  }
```

```
}
```

Che dire delle estensioni.ebextensions?

I file di configurazione Elastic Beanstalk .ebextensions sono supportati come tutti gli altri contenitori Elastic Beanstalk. Per includere .ebextensions in un'applicazione ASP.NET Core, aggiungi la directory alla sezione sottostante del file. `.ebextensions` `include` `publishOptions` `project.json` Per ulteriori informazioni su.ebextensions, consulta la Elastic Beanstalk Developer Guide.

Supporto di più applicazioni per.NET ed Elastic Beanstalk

Utilizzando il manifesto di distribuzione, hai la possibilità di distribuire più applicazioni nello stesso ambiente Elastic Beanstalk.

Il manifesto di distribuzione supporta le applicazioni Web ASP.NET Core e gli archivi msdeploy per le applicazioni ASP.NET tradizionali. Immagina uno scenario in cui hai scritto una nuova fantastica applicazione utilizzando ASP.NET Core per il frontend e un progetto di API Web per un'API di estensioni. Hai anche un'app di amministrazione che hai scritto usando il tradizionale ASP.NET.

La procedura guidata di distribuzione del toolkit si concentra sulla distribuzione di un singolo progetto. Per sfruttare i vantaggi della distribuzione di più applicazioni, è necessario creare manualmente il pacchetto di applicazioni. Per iniziare, scrivi il manifesto. Per questo esempio, scriverai il manifesto alla radice della tua soluzione.

La sezione di distribuzione nel manifesto ha due elementi secondari: un array di applicazioni Web ASP.NET Core da distribuire e un array di archivi msdeploy da distribuire. Per ogni applicazione, si imposta il percorso IIS e la posizione dei bit dell'applicazione relativi al manifesto.

```
{
  "manifestVersion": 1,
  "deployments": {

    "aspNetCoreWeb": [
      {
        "name": "frontend",
        "parameters": {
          "appBundle": "./frontend",
          "iisPath": "/frontend"
        }
```

```
      },
      {
        "name": "ext-api",
        "parameters": {
          "appBundle": "./ext-api",
          "iisPath": "/ext-api"
        }
      }
    ],
    "msDeploy": [
      {
        "name": "admin",
        "parameters": {
          "appBundle": "AmazingAdmin.zip",
          "iisPath": "/admin"
        }
      }
    ]
  }
}
```

Una volta scritto il manifesto, utilizzerai Windows PowerShell per creare il pacchetto di applicazioni e aggiornare un ambiente Elastic Beanstalk esistente per eseguirlo. Lo script è scritto presupponendo che venga eseguito dalla cartella contenente la soluzione Visual Studio.

La prima cosa da fare nello script è configurare una cartella dell'area di lavoro in cui creare il pacchetto dell'applicazione.

```
$publishFolder = "c:\temp\publish"

$publishWorkspace = [System.IO.Path]::Combine($publishFolder, "workspace")
$appBundle = [System.IO.Path]::Combine($publishFolder, "app-bundle.zip")

If (Test-Path $publishWorkspace){
  Remove-Item $publishWorkspace -Confirm:$false -Force
}
If (Test-Path $appBundle){
  Remove-Item $appBundle -Confirm:$false -Force
}
```

Dopo aver creato la cartella, è il momento di preparare il frontend. Come per la procedura guidata di distribuzione, utilizza la CLI dotnet per pubblicare l'applicazione.

```
Write-Host 'Publish the ASP.NET Core frontend'
$publishFrontendFolder = [System.IO.Path]::Combine($publishWorkspace, "frontend")
dotnet publish .\src\AmazingFrontend\project.json -o $publishFrontendFolder -c Release
 -f netcoreapp1.0
```

Si noti che la sottocartella «frontend» è stata utilizzata per la cartella di output, corrispondente alla cartella impostata nel manifesto. Ora devi fare lo stesso per il progetto Web API.

```
Write-Host 'Publish the ASP.NET Core extensibility API'
$publishExtAPIFolder = [System.IO.Path]::Combine($publishWorkspace, "ext-api")
dotnet publish .\src\AmazingExtensibleAPI\project.json -o $publishExtAPIFolder -c
 Release -f netcoreapp1.0
```

Il sito di amministrazione è un'applicazione ASP.NET tradizionale, quindi non è possibile utilizzare la CLI dotnet. Per l'applicazione di amministrazione, è necessario utilizzare msbuild, passando il pacchetto build target per creare l'archivio msdeploy. Per impostazione predefinita, la destinazione del pacchetto crea l'archivio msdeploy nella `obj\Release\Package` cartella, quindi sarà necessario copiare l'archivio nell'area di lavoro di pubblicazione.

```
Write-Host 'Create msdeploy archive for admin site'
msbuild .\src\AmazingAdmin\AmazingAdmin.csproj /t:package /p:Configuration=Release
Copy-Item .\src\AmazingAdmin\obj\Release\Package\AmazingAdmin.zip $publishWorkspace
```

Per indicare all'ambiente Elastic Beanstalk cosa fare con tutte queste applicazioni, copia il manifesto dalla soluzione nell'area di lavoro di pubblicazione, quindi comprimi la cartella.

```
Write-Host 'Copy deployment manifest'
Copy-Item .\aws-windows-deployment-manifest.json $publishWorkspace

Write-Host 'Zipping up publish workspace to create app bundle'
Add-Type -assembly "system.io.compression.filesystem"
[io.compression.zipfile]::CreateFromDirectory( $publishWorkspace, $appBundle)
```

Ora che hai il pacchetto di applicazioni, puoi andare alla console web e caricare l'archivio in un ambiente Elastic Beanstalk. In alternativa, puoi continuare a utilizzare i AWS PowerShell cmdlet per aggiornare l'ambiente Elastic Beanstalk con il bundle dell'applicazione. Assicurati di aver impostato il profilo e la regione correnti sul profilo e sull'area che contiene l'ambiente Elastic Beanstalk utilizzando i cmdlet and. `Set-AWSCredentials` `Set-DefaultAWSRegion`

```
Write-Host 'Write application bundle to S3'
# Determine S3 bucket to store application bundle
$s3Bucket = New-EBStorageLocation
Write-S3Object -BucketName $s3Bucket -File $appBundle


$applicationName = "ASPNETCoreOnAWS"
$environmentName = "ASPNETCoreOnAWS-dev"
$versionLabel = [System.DateTime]::Now.Ticks.ToString()

Write-Host 'Update Beanstalk environment for new application bundle'
New-EBApplicationVersion -ApplicationName $applicationName -VersionLabel $versionLabel
 -SourceBundle_S3Bucket $s3Bucket -SourceBundle_S3Key app-bundle.zip
Update-EBEnvironment -ApplicationName $applicationName -EnvironmentName
 $environmentName -VersionLabel $versionLabel
```

Ora, controlla lo stato dell'aggiornamento utilizzando la pagina di stato dell'ambiente Elastic Beanstalk nel toolkit o nella console web. Una volta completato, sarai in grado di accedere a ciascuna delle applicazioni distribuite nel percorso IIS impostato nel manifesto di distribuzione.

Distribuzione su Amazon EC2 Container Service

> **Important**
>
> La nuova AWS funzionalità Publish to è progettata per semplificare la modalità di pubblicazione delle applicazioni.NET su AWS. È possibile che ti venga chiesto se desideri passare a questa esperienza di pubblicazione dopo aver scelto Publish Container in AWS. Per ulteriori informazioni, consulta Utilizzo di Publish to AWS in Visual Studio.

Amazon Elastic Container Service è un servizio di gestione dei container altamente scalabile e ad alte prestazioni che supporta i contenitori Docker e consente di eseguire facilmente applicazioni su un cluster gestito di istanze Amazon EC2 .

Per distribuire applicazioni su Amazon Elastic Container Service, i componenti dell'applicazione devono essere sviluppati per essere eseguiti in un contenitore Docker. Un container Docker è un'unità di sviluppo software standardizzata che contiene tutto ciò che l'applicazione software deve eseguire: codice, runtime, strumenti e librerie di sistema e così via.

Il Toolkit for Visual Studio fornisce una procedura guidata che semplifica la pubblicazione di applicazioni tramite Amazon ECS. Questa procedura guidata è descritta nelle seguenti sezioni.

Per ulteriori informazioni su Amazon ECS, consulta la documentazione di Elastic Container Service. Include una panoramica delle nozioni di base di Docker e della creazione di un cluster.

Argomenti

Specificare AWS le credenziali per l'applicazione ASP.NET Core 2

Esistono due tipi di credenziali in gioco quando si distribuisce l'applicazione in un contenitore Docker: credenziali di distribuzione e credenziali di istanza.

Le credenziali di distribuzione vengono utilizzate dalla AWS procedura guidata Publish Container to per creare l'ambiente in Amazon ECS. Ciò include attività, servizi, ruoli IAM, un repository di contenitori Docker e, se lo desideri, un sistema di bilanciamento del carico.

Le credenziali dell'istanza vengono utilizzate dall'istanza (inclusa l'applicazione) per accedere a diversi servizi. AWS Ad esempio, se un'applicazione ASP.NET Core 2.0 legge e scrive su oggetti Amazon S3, avrà bisogno delle autorizzazioni appropriate. Puoi fornire credenziali diverse utilizzando metodi diversi in base all'ambiente. Ad esempio, l'applicazione ASP.NET Core 2 potrebbe essere destinata ad ambienti di sviluppo e produzione. È possibile utilizzare un'istanza Docker locale e credenziali per lo sviluppo e un ruolo definito nella produzione.

Specificare le credenziali di distribuzione

L' AWS account specificato nella AWS procedura guidata Publish Container to è l' AWS account che la procedura guidata utilizzerà per la distribuzione su Amazon ECS. Il profilo dell'account deve disporre delle autorizzazioni per Amazon Elastic Compute Cloud, Amazon Elastic Container Service e. AWS Identity and Access Management

Se noti che mancano delle opzioni negli elenchi a discesa, è possibile che non disponi delle autorizzazioni. Ad esempio, se hai creato un cluster per la tua applicazione ma non lo vedi nella pagina Publish Container to AWS wizard Cluster. In tal caso, aggiungi le autorizzazioni mancanti e riprova con la procedura guidata.

Specificazione delle credenziali dell'istanza di sviluppo

Per gli ambienti non di produzione, puoi configurare le tue credenziali nelle impostazioni dell'app. <environment>file.json. Ad esempio, per configurare le credenziali nel file AppSettings.Development.json in Visual Studio 2017:

1. Aggiungi AWSSDK le .Extensions. NETCore NuGet Pacchetto.Setup al tuo progetto.
2. Aggiungi AWS impostazioni a AppSettings.Development.json. La configurazione seguente imposta e. `Profile` `Region`

```
{
    "AWS": {
        "Profile": "local-test-profile",
        "Region": "us-west-2"
    }
}
```

Specificazione delle credenziali dell'istanza di produzione

Per le istanze di produzione, ti consigliamo di utilizzare un ruolo IAM per controllare a cosa può accedere l'applicazione (e il servizio). Ad esempio, per configurare un ruolo IAM con Amazon ECS come principale del servizio con autorizzazioni per Amazon Simple Storage Service e Amazon DynamoDB da: Console di gestione AWS

1. Accedi a Console di gestione AWS e apri la console IAM all'indirizzo. https://console.aws.amazon.com/iam/
2. Nel pannello di navigazione della console IAM, scegli Ruoli e poi Crea ruolo.
3. Scegli il tipo AWS di ruolo Service, quindi scegli EC2 Container Service.
4. Scegli il caso d'uso EC2 Container Service Task. I casi d'uso sono definiti dal servizio per includere la politica di fiducia richiesta dal servizio. Quindi scegliere Next: Permissions (Successivo: Autorizzazioni).
5. Scegli le politiche di autorizzazione di AmazonS3 FullAccess e AmazonDynamoDBFullAccess. Seleziona la casella accanto a ciascuna politica, quindi scegli Avanti: revisione,
6. Per Nome ruolo, digita un nome di ruolo o un suffisso per identificare lo scopo di questo ruolo. I nomi dei ruoli devono essere univoci all'interno dell'account AWS . Non vengono distinti per caso. Ad esempio, non è possibile creare ruoli denominati sia `PRODROLE` che `prodrole`. Poiché varie

entità possono fare riferimento al ruolo, non è possibile modificare il nome del ruolo dopo averlo creato.

7. (Facoltativo) In Role description (Descrizione ruolo), immettere una descrizione per il nuovo ruolo.
8. Rivedere il ruolo e scegliere Crea ruolo.

È possibile utilizzare questo ruolo come ruolo di attività nella pagina ECS Task Definition della AWS procedura guidata Publish Container to.

Per ulteriori informazioni, vedere Utilizzo dei ruoli basati sui servizi.

Distribuzione di un'app ASP.NET Core 2.0 su Amazon ECS (Fargate) (Legacy)

> **Important**
>
> Questa documentazione si riferisce ai servizi e alle funzionalità precedenti. Per guide e contenuti aggiornati, consulta la guida agli strumenti di AWS distribuzione.NET e il sommario Deploying to AWS aggiornato.

Questa sezione descrive come utilizzare la AWS procedura guidata Publish Container to, fornita come parte del Toolkit for Visual Studio, per distribuire un'applicazione ASP.NET Core 2.0 containerizzata destinata a Linux tramite Amazon ECS utilizzando il tipo di avvio Fargate. Poiché un'applicazione Web è concepita per essere eseguita in maniera continua, verrà distribuita come un servizio.

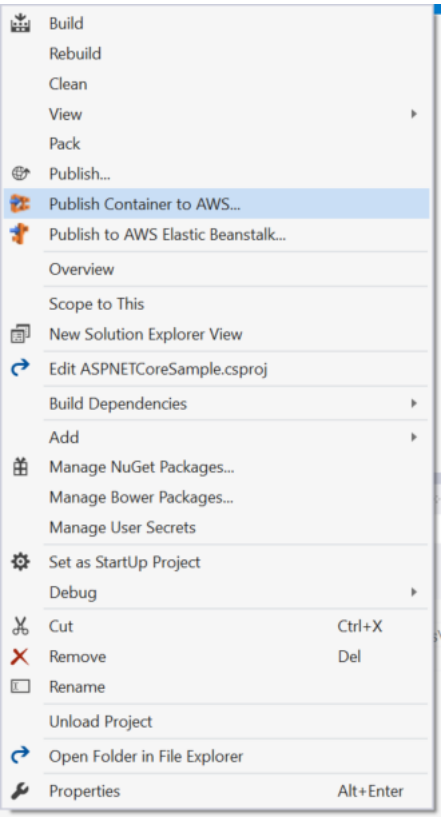
Prima di pubblicare il contenitore

Prima di utilizzare la AWS procedura guidata Publish Container to per distribuire l'applicazione ASP.NET Core 2.0:

- Specificate AWS le vostre credenziali e iniziate la configurazione con Amazon ECS.
- Installa Docker. Sono disponibili diverse opzioni di installazione, tra cui Docker per Windows.
- In Visual Studio, crea (o apri) un progetto per un'app containerizzata ASP.NET Core 2.0 destinata a Linux.

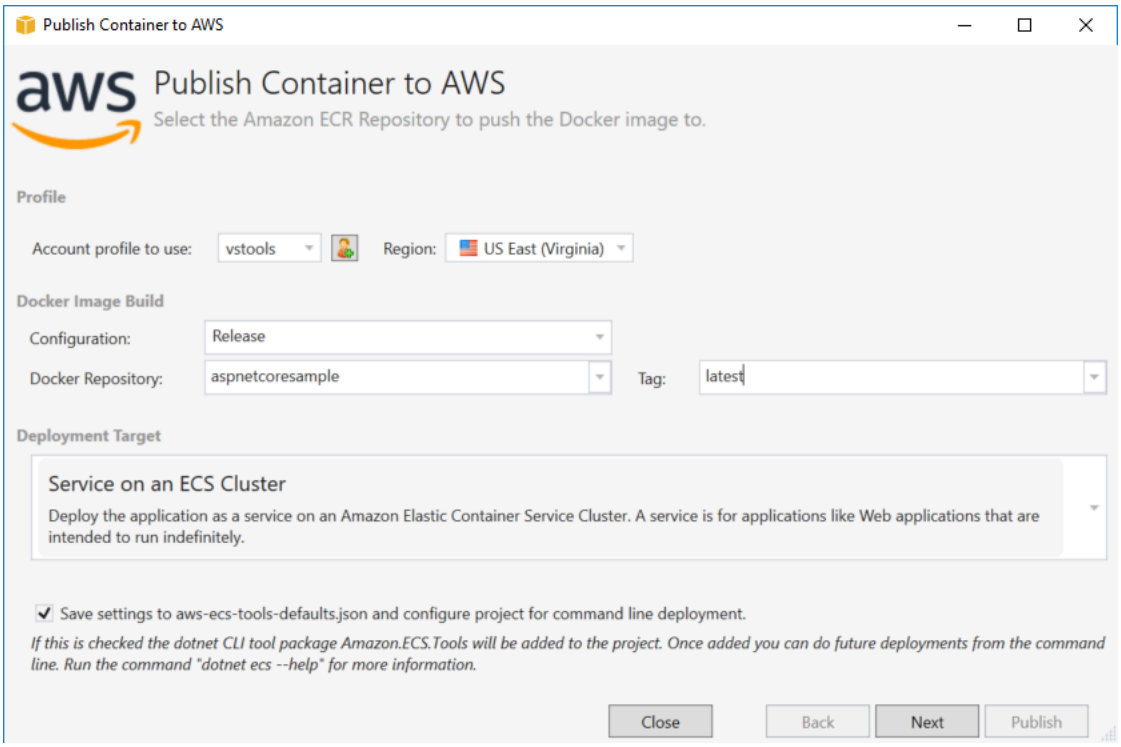
Accesso al Publish Container alla procedura guidata AWS

Per distribuire un'applicazione containerizzata ASP.NET Core 2.0 destinata a Linux, fai clic con il pulsante destro del mouse sul progetto in Solution Explorer e seleziona Publish Container to. AWS



Puoi anche selezionare Publish Container nel AWS menu Build di Visual Studio.

Pubblica contenitore su AWS Wizard



Profilo account da utilizzare: seleziona un profilo account da utilizzare.

Regione: scegli la regione di distribuzione. Il profilo e la regione vengono utilizzati per configurare le risorse dell'ambiente di distribuzione e per selezionare il registro Docker predefinito.

Configurazione: seleziona la configurazione di build dell'immagine Docker.

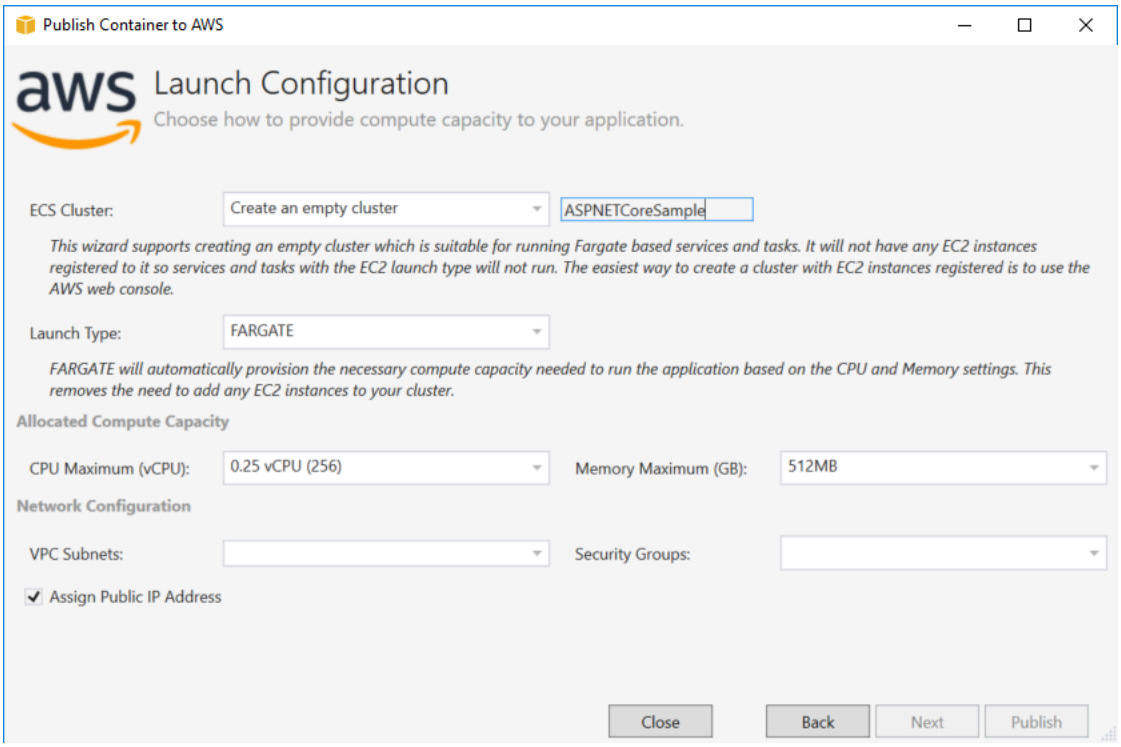
Docker Repository: scegli un repository Docker esistente o digita il nome di un nuovo repository e verrà creato. Questo è il repository in cui viene inviato il contenitore di build.

Tag: seleziona un tag esistente o digita il nome di un nuovo tag. I tag possono tenere traccia di dettagli importanti come versione, opzioni o altri elementi di configurazione unici del contenitore Docker.

Obiettivo di distribuzione: seleziona il servizio su un cluster ECS. Utilizza questa opzione di distribuzione quando l'applicazione è destinata a durare a lungo (come un'applicazione Web ASP.NET).

Salva le impostazioni **`aws-docker-tools-defaults.json`** e configura il progetto per la distribuzione da riga di comando: seleziona questa opzione se desideri la flessibilità della distribuzione dalla riga di comando. `dotnet ecs deploy`Utilizzala dalla directory del progetto per la distribuzione e `dotnet ecs publish` il contenitore.

Avvia la pagina di configurazione



Cluster ECS: scegli il cluster che eseguirà la tua immagine Docker. Se scegli di creare un cluster vuoto, fornisci un nome per il nuovo cluster.

Tipo di avvio: scegli FARGATE.

CPU Maximum (vCPU): scegli la quantità massima di capacità di elaborazione necessaria per la tua applicazione. Per visualizzare gli intervalli consentiti di valori di CPU e memoria, consulta la dimensione dell'attività.

Memoria massima (GB): seleziona la quantità massima di memoria disponibile per l'applicazione.

Sottoreti VPC: scegli una o più sottoreti sotto un singolo VPC. Se scegli più di una sottorete, le tue attività verranno distribuite su di esse. Ciò può migliorare la disponibilità. Per ulteriori informazioni, consulta VPC predefinito e sottoreti predefinite.

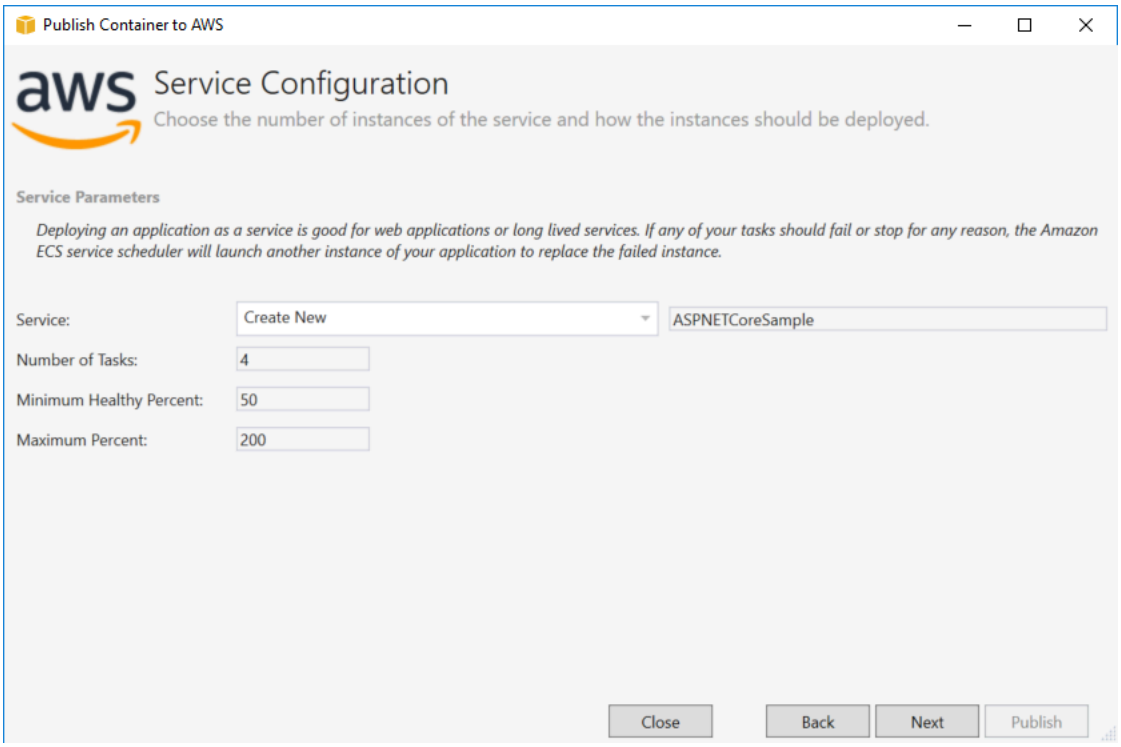
Gruppi di sicurezza: scegli un gruppo di sicurezza.

Un gruppo di sicurezza funge da firewall per le istanze Amazon EC2 associate, controllando il traffico in entrata e in uscita a livello di istanza.

I gruppi di sicurezza predefiniti sono configurati per consentire il traffico in entrata dalle istanze assegnate allo stesso gruppo di sicurezza e tutto il traffico in uscita. IPv4 È necessario consentire l'uscita in uscita in modo che il servizio possa raggiungere l'archivio del contenitore.

Assegna indirizzo IP pubblico: seleziona questa opzione per rendere l'attività accessibile da Internet.

Pagina di configurazione del servizio



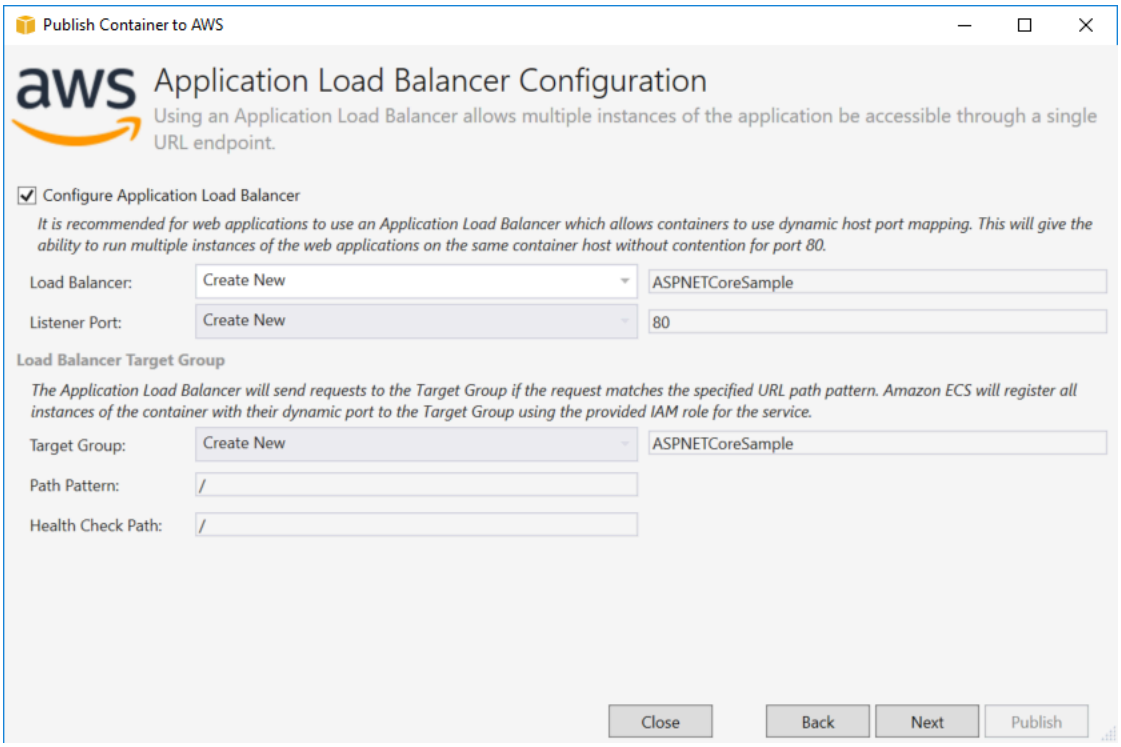
Servizio: seleziona uno dei servizi nel menu a discesa per distribuire il contenitore in un servizio esistente. Oppure scegli Crea nuovo per creare un nuovo servizio. I nomi dei servizi devono essere univoci all'interno di un cluster, ma puoi avere servizi dai nomi simili in più cluster all'interno di una regione o in più regioni.

Numero di attività: il numero di attività da distribuire e mantenere in esecuzione sul cluster. Ogni attività è un'istanza del contenitore.

Percentuale minima di integrità: la percentuale di attività che devono rimanere invariate durante una distribuzione arrotondata al numero intero più vicino. `RUNNING`

Percentuale massima: la percentuale di attività consentite `PENDING` nello stato `RUNNING` o durante una distribuzione arrotondata per difetto al numero intero più vicino.

Pagina Application Load Balancer



Configura Application Load Balancer: seleziona questa opzione per configurare un Application Load Balancer.

Load Balancer: seleziona un load balancer esistente o scegli Crea nuovo e digita il nome del nuovo load balancer.

Porta listener: seleziona una porta listener esistente o scegli Crea nuova e digita un numero di porta. L'impostazione predefinita, la porta`80`, è appropriata per la maggior parte delle applicazioni Web.

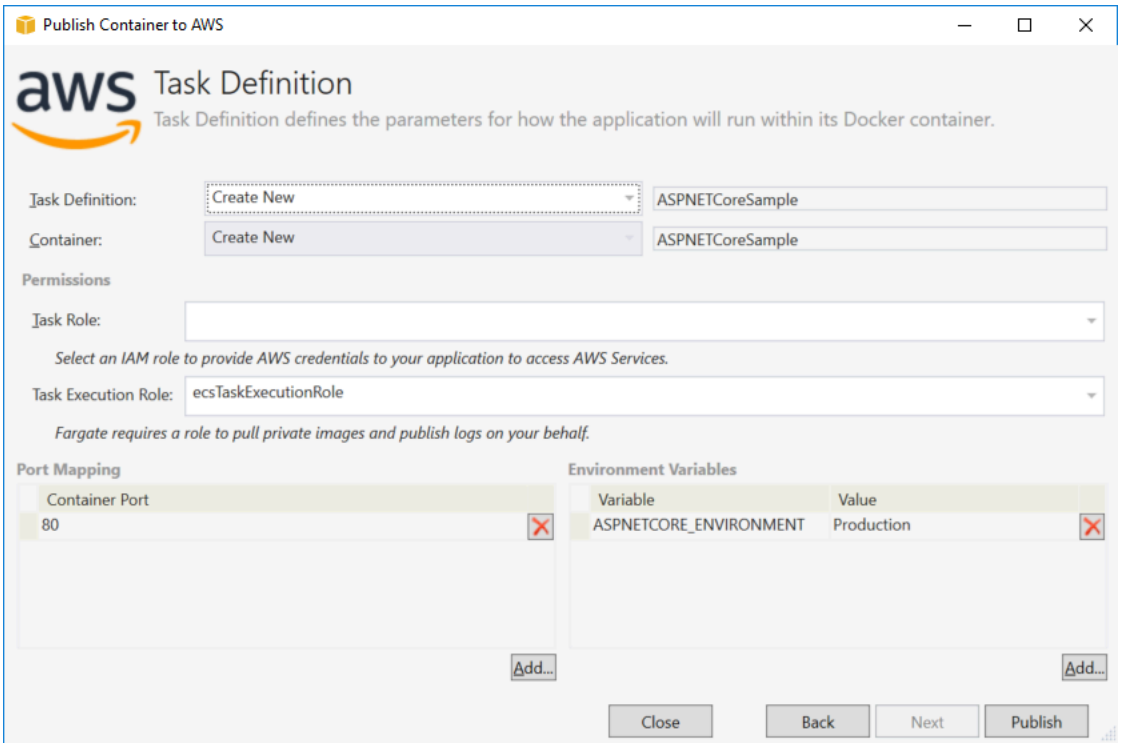
Gruppo target: seleziona il gruppo target in cui Amazon ECS registrerà le attività nel servizio.

Path Pattern: il load balancer utilizzerà il routing basato sul percorso. Accetta l'impostazione predefinita `/` o fornisci uno schema diverso. Il modello di percorso fa distinzione tra maiuscole e minuscole, può contenere fino a 128 caratteri e contiene un set selezionato di caratteri.

Health Check Path: il percorso ping che rappresenta la destinazione degli obiettivi per i controlli sanitari. Per impostazione predefinita, tale valore è `/`. Se necessario, inserisci un percorso diverso. Se il percorso inserito non è valido, il controllo dello stato di salute avrà esito negativo e verrà considerato non integro.

Se distribuisci più servizi e ogni servizio verrà distribuito in un percorso o in una posizione diversa, avrai bisogno di percorsi di controllo personalizzati.

Pagina di definizione delle attività



Definizione dell'attività: seleziona una definizione di attività esistente o scegli Crea nuova attività e digita il nome della nuova definizione dell'attività.

Contenitore: seleziona un contenitore esistente o scegli Crea nuovo e digita il nome del nuovo contenitore.

Task Role: seleziona un ruolo IAM con le credenziali di cui la tua app ha bisogno per accedere ai AWS Servizi. Ecco come vengono passate le credenziali all'applicazione. Scopri come specificare le credenziali AWS di sicurezza per la tua applicazione.

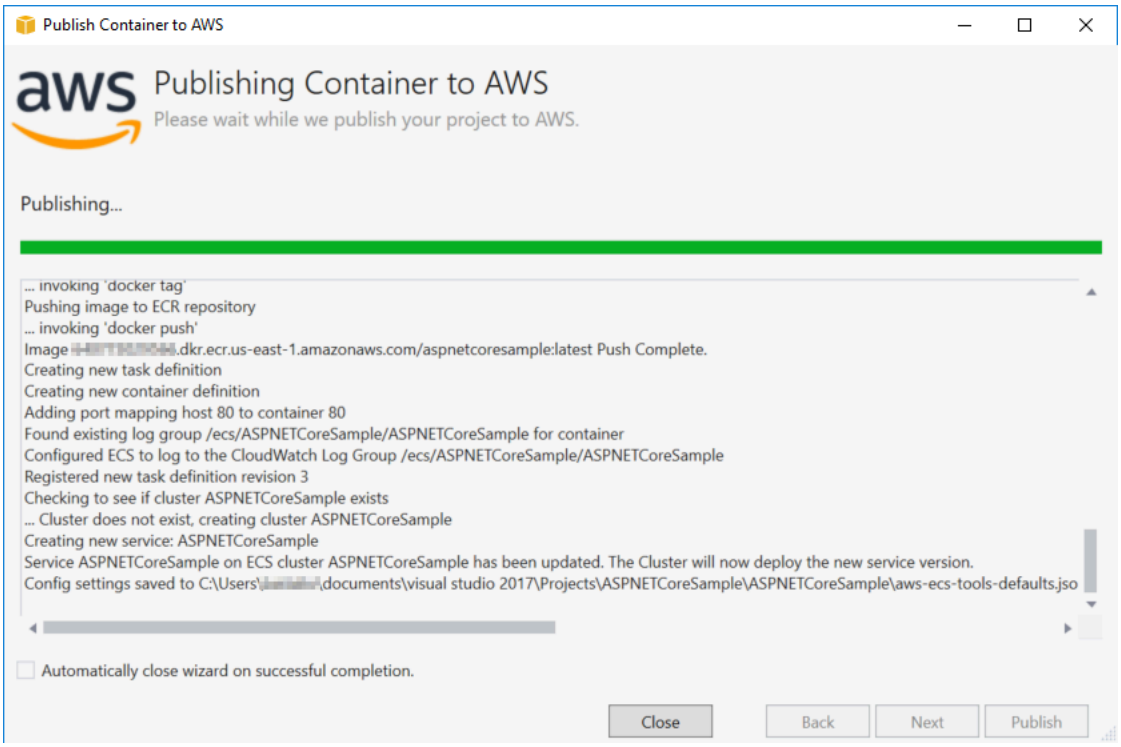
Ruolo di esecuzione dell'attività: seleziona un ruolo con le autorizzazioni per estrarre immagini private e pubblicare registri. AWS Fargate lo userà per vostro conto.

Mappatura delle porte: scegli il numero di porta sul container associato alla porta host assegnata automaticamente.

Variabili di ambiente: aggiungi, modifica o elimina le variabili di ambiente per il contenitore. Puoi modificarlo in base alla tua implementazione.

Quando sei soddisfatto della configurazione, fai clic su Pubblica per iniziare il processo di distribuzione.

Contenitore di pubblicazione su AWS



Gli eventi vengono visualizzati durante la distribuzione. La procedura guidata viene chiusa automaticamente al completamento. È possibile sostituire questo deselezionando la casella nella parte inferiore della pagina.

Puoi trovare l'URL delle tue nuove istanze in Explorer. AWS Espandi Amazon ECS e Clusters, quindi fai clic sul tuo cluster.

Distribuzione di un'app ASP.NET Core 2.0 su Amazon ECS (EC2)

Questa sezione descrive come utilizzare la AWS procedura guidata Publish Container to, fornita come parte del Toolkit for Visual Studio, per distribuire un'applicazione ASP.NET Core 2.0 containerizzata destinata a Linux tramite Amazon ECS utilizzando il tipo di avvio EC2. Poiché un'applicazione Web è pensata per essere eseguita continuamente, verrà distribuita come servizio.

Prima di pubblicare il contenitore

Prima di utilizzare Publish Container AWS per distribuire l'applicazione ASP.NET Core 2.0:

- Specificate AWS le vostre credenziali e iniziate la configurazione con Amazon ECS.
- Installa Docker. Sono disponibili diverse opzioni di installazione, tra cui Docker per Windows.

- Crea un cluster Amazon ECS in base alle esigenze della tua applicazione web. Bastano pochi passaggi.
- In Visual Studio, crea (o apri) un progetto per un'app containerizzata ASP.NET Core 2.0 destinata a Linux.

Accesso al Publish Container alla procedura guidata AWS

Per distribuire un'applicazione containerizzata ASP.NET Core 2.0 destinata a Linux, fai clic con il pulsante destro del mouse sul progetto in Solution Explorer e seleziona Publish Container to. AWS

Puoi anche selezionare Publish Container to nel menu Build di AWS Visual Studio.

Pubblica contenitore su AWS Wizard

Profilo dell'account da utilizzare: seleziona un profilo account da utilizzare.

Regione: scegli una regione di distribuzione. Il profilo e la regione vengono utilizzati per configurare le risorse dell'ambiente di distribuzione e selezionare il registro Docker predefinito.

Configurazione: seleziona la configurazione di build dell'immagine Docker.

Docker Repository: scegli un repository Docker esistente o digita il nome di un nuovo repository e verrà creato. Questo è il repository in cui viene inviata l'immagine del contenitore creato.

Tag: seleziona un tag esistente o digita il nome di un nuovo tag. I tag possono tenere traccia di dettagli importanti come versione, opzioni o altri elementi di configurazione unici del contenitore Docker.

Distribuzione: seleziona il servizio su un cluster ECS. Utilizza questa opzione di distribuzione quando l'applicazione è destinata a durare a lungo (come un'applicazione Web ASP.NET Core 2.0).

Salva le impostazioni **`aws-docker-tools-defaults.json`** e configura il progetto per la distribuzione da riga di comando: seleziona questa opzione se desideri la flessibilità della distribuzione dalla riga di comando. `dotnet ecs deploy`Utilizzala dalla directory del progetto per la distribuzione e `dotnet ecs publish` il contenitore.

Avvia la pagina di configurazione

Cluster ECS: scegli il cluster che eseguirà la tua immagine Docker. Puoi creare un cluster ECS utilizzando la Console di gestione. AWS

Tipo di avvio: scegli EC2. Per utilizzare il tipo di avvio Fargate, consulta Distribuzione di un'applicazione ASP.NET Core 2.0 su Amazon ECS (Fargate).

Pagina di configurazione del servizio

Servizio: seleziona uno dei servizi nel menu a discesa per distribuire il contenitore in un servizio esistente. Oppure scegli Crea nuovo per creare un nuovo servizio. I nomi dei servizi devono essere univoci all'interno di un cluster, ma puoi avere servizi dai nomi simili in più cluster all'interno di una regione o in più regioni.

Numero di attività: il numero di attività da distribuire e mantenere in esecuzione sul cluster. Ogni attività è un'istanza del contenitore.

Percentuale minima di integrità: la percentuale di attività che devono rimanere invariate durante una distribuzione arrotondata al numero intero più vicino. `RUNNING`

Percentuale massima: la percentuale di attività consentite `PENDING` nello stato `RUNNING` o durante una distribuzione arrotondata per difetto al numero intero più vicino.

Modelli di posizionamento: seleziona un modello di posizionamento delle attività.

Quando avvii un'attività in un cluster, Amazon ECS deve determinare dove collocarla in base ai requisiti specificati nella definizione dell'attività, come CPU e memoria. Analogamente, quando riduci orizzontalmente il conteggio di processi, Amazon ECS deve determinare quali processi terminare.

Il modello di posizionamento controlla il modo in cui le attività vengono avviate in un cluster:

- AZ Balanced Spread (Distribuzione bilanciata tra zone di disponibilità): consente di distribuire le attività tra zone di disponibilità e istanze di container nella zona di disponibilità.
- AZ Balanced BinPack : distribuisci le attività tra le zone di disponibilità e tra le istanze di container con la minima memoria disponibile.
- BinPack - distribuisci le attività in base alla quantità minima disponibile di CPU o memoria.
- One Task Per Host (Un'attività per host): consente di posizionare al massimo un'attività dal servizio in ogni istanza di container.

Per ulteriori informazioni, consulta Amazon ECS Task Placement.

Pagina Application Load Balancer

Configura Application Load Balancer: seleziona questa opzione per configurare un Application Load Balancer.

Seleziona il ruolo IAM per il servizio: seleziona un ruolo esistente o scegli Crea nuovo e verrà creato un nuovo ruolo.

Load Balancer: seleziona un load balancer esistente o scegli Crea nuovo e digita il nome del nuovo load balancer.

Porta listener: seleziona una porta listener esistente o scegli Crea nuova e digita un numero di porta. L'impostazione predefinita, la porta`80`, è appropriata per la maggior parte delle applicazioni Web.

Gruppo di destinazione: per impostazione predefinita, il sistema di bilanciamento del carico invia le richieste alle destinazioni registrate utilizzando la porta e il protocollo specificati per il gruppo di destinazione. È possibile sostituire questa porta al momento della registrazione di ogni target con il gruppo target.

Path Pattern: il load balancer utilizzerà il routing basato sul percorso. Accetta l'impostazione predefinita `/` o fornisci uno schema diverso. Il modello di percorso fa distinzione tra maiuscole e minuscole, può contenere fino a 128 caratteri e contiene un set selezionato di caratteri.

Health Check Path: il percorso ping che rappresenta la destinazione degli obiettivi per i controlli sanitari. Per impostazione predefinita, è `/` ed è appropriato per le applicazioni Web. Se necessario, immettete un percorso diverso. Se il percorso inserito non è valido, il controllo dello stato di salute avrà esito negativo e verrà considerato non integro.

Se distribuisci più servizi e ogni servizio verrà distribuito in un percorso o in una posizione diversa, potresti aver bisogno di percorsi di controllo personalizzati.

Pagina ECS Task Definition

Definizione dell'attività: seleziona una definizione di attività esistente o scegli Crea nuova e digita il nome della nuova definizione dell'attività.

Contenitore: seleziona un contenitore esistente o scegli Crea nuovo e digita il nome del nuovo contenitore.

Memoria (MiB): fornisce i valori per Soft Limit o Hard Limit o entrambi.

Il limite morbido (in MiB) di memoria da riservare per il contenitore. Docker tenta di mantenere la memoria del contenitore al di sotto del limite consentito. Il contenitore può consumare più memoria, fino al limite rigido specificato con il parametro memory (se applicabile) o tutta la memoria disponibile sull'istanza del contenitore, a seconda dell'evento che si verifica per primo.

Il limite rigido (in MiB) di memoria da presentare al contenitore. Se il container tenta di superare la memoria specificata qui, viene terminato.

Ruolo attività: seleziona un ruolo di attività per un ruolo IAM che consenta al contenitore l' AWS APIs autorizzazione a chiamare per tuo conto i dati specificati nelle politiche associate. Ecco come vengono passate le credenziali all'applicazione. Scopri come specificare le credenziali AWS di sicurezza per la tua applicazione.

Mappatura delle porte: aggiungi, modifica o elimina le mappature delle porte per il contenitore. Se è attivo un sistema di bilanciamento del carico, la porta host verrà impostata di default su 0 e l'assegnazione delle porte sarà dinamica.

Variabili di ambiente: aggiungi, modifica o elimina le variabili di ambiente per il contenitore.

Quando sei soddisfatto della configurazione, fai clic su Pubblica per iniziare il processo di distribuzione.

Contenitore di pubblicazione su AWS

Gli eventi vengono visualizzati durante la distribuzione. La procedura guidata viene chiusa automaticamente al completamento. È possibile sostituire questo deselezionando la casella nella parte inferiore della pagina.

Puoi trovare l'URL delle tue nuove istanze in AWS Explorer. Espandi Amazon ECS e Clusters, quindi fai clic sul tuo cluster.

Risoluzione dei problemi relativi al AWS Toolkit for Visual Studio

Le sezioni seguenti contengono informazioni generali sulla risoluzione dei problemi relativi ai servizi del AWS Toolkit for Visual Studio toolkit e all'utilizzo AWS dei servizi.

> **Note**
>
> Le informazioni sull'installazione e la set-up-specific risoluzione dei problemi sono disponibili nell'argomento Risoluzione dei problemi di installazione, disponibile in questa Guida per l'utente.

Argomenti

Best practice per la risoluzione dei problemi

Di seguito sono riportate le best practice consigliate per la risoluzione dei AWS Toolkit for Visual Studio problemi.

- Ripristina Visual Studio e riavvia il sistema
- Prova a ricreare il problema o l'errore prima di inviare una segnalazione.
- Prendi nota dettagliata di ogni passaggio, impostazione e messaggio di errore durante il processo di ricreazione.
- Raccogli i AWS log del Toolkit. Per una descrizione dettagliata di come individuare i log del AWS Toolkit, consulta la procedura Come localizzare AWS i log, disponibile in questo argomento della guida.
- Controlla le richieste aperte, le soluzioni note o segnala il problema irrisolto nella sezione AWS Toolkit for Visual Studio Problemi del repository. AWS Toolkit for Visual Studio GitHub

Ripara Visual Studio e riavvia il sistema

1. Chiudi tutte le istanze in esecuzione di Visual Studio.
2. Dal menu di avvio di Windows, avvia Visual Studio Installer.
3. Esegui Repair sulle installazioni interessate di Visual Studio. Ciò consente a Visual Studio di ricostruire l'indice delle estensioni installate.
4. Riavvia Windows prima di riavviare Visual Studio.

Come individuare i log del Toolkit AWS

1. Dal menu principale di Visual Studio, espandi Estensioni.
2. Scegli il AWS Toolkit per espandere il menu AWS Toolkit, quindi scegli Visualizza i registri del Toolkit.
3. Quando la cartella AWS Toolkit logs si apre nel tuo sistema operativo, ordina i file per data e individua qualsiasi file di registro che contenga informazioni pertinenti al problema corrente.

Visualizzazione e filtraggio delle scansioni di sicurezza di Amazon Q

Per visualizzare le scansioni di sicurezza di Amazon Q in Visual Studio, apri l'elenco degli errori di Visual Studio espandendo l'intestazione Visualizza nel menu principale di Visual Studio e selezionando Elenco errori.

Per impostazione predefinita, l'Elenco degli errori di Visual Studio mostra tutti gli avvisi e gli errori relativi alla codebase. Per filtrare i risultati delle scansioni di sicurezza di Amazon Q dall'elenco degli errori di Visual Studio, crea un filtro completando la seguente procedura.

> **Note**
>
> I risultati della scansione di sicurezza di Amazon Q sono visibili solo dopo l'esecuzione della scansione di sicurezza e il rilevamento di problemi.
> I risultati delle scansioni di sicurezza di Amazon Q vengono visualizzati come avvisi in Visual Studio. Per visualizzare i risultati delle scansioni di sicurezza di Amazon Q dall'elenco degli errori, è necessario selezionare l'opzione Avvertenze nell'intestazione Elenco errori.

1. Dal menu principale di Visual Studio, espandi l'intestazione Visualizza e scegli Elenco errori per aprire il riquadro Elenco errori.
2. Dal riquadro Elenco errori, fai clic con il pulsante destro del mouse sulla riga di intestazione per aprire il menu contestuale.
3. Dal menu contestuale, espandi Mostra colonne, quindi seleziona Strumento nel menu espanso.
4. La colonna Strumento viene aggiunta all'Elenco errori.
5. Dall'intestazione della colonna Tool, seleziona l'icona Filtro e scegli Amazon Q per filtrare i risultati delle scansioni di sicurezza di Amazon Q.

Il AWS Toolkit non è installato correttamente

Problema:

Entro un minuto dall'avvio di Visual Studio, AWS Toolkit for Visual Studio i seguenti messaggi vengono visualizzati rispettivamente nel riquadro di output e nella barra delle informazioni:

```
Some Toolkit components could not be initialized. Some functionality may
not work during this IDE session.
```

```
The AWS Toolkit is not properly installed.
```

Soluzione::

È possibile che l'aggiornamento o l'installazione di un'estensione abbiano causato la perdita di alcuni file della cache interna di Visual Studio out-of-sync. La procedura seguente descrive come far ricostruire questi file al successivo avvio di Visual Studio.

> **Note**
>
> È possibile che questa soluzione influisca sulle personalizzazioni di Visual Studio. Dopo aver completato questa procedura, l'estensione AWS Toolkit dovrebbe essere elencata come installata e non riportare più alcun messaggio di errore. Se continui a riscontrare questo problema dopo aver completato i seguenti passaggi, consulta il numero #452 nell' AWS Toolkit for Visual Studio GitHub archivio per ulteriori informazioni.

1. Installa l'ultima versione di Visual Studio 2022.

> **Note**
>
> La versione minima richiesta è 17.11.5.

2. Chiudi tutte le istanze in esecuzione di Visual Studio.
3. Da Windows, apri il Developer Command Prompt come amministratore.
4. Dal prompt dei comandi dello sviluppatore, esegui il seguente comando:`devenv /updateconfiguration /resetExtensions`, quindi attendi il completamento del comando.
5. Al termine del comando, riavvia Visual Studio.
6. In Visual Studio l' AWS estensione è ora elencata come installata e non riporta più i messaggi di errore elencati all'inizio di questo problema.

Impostazioni del firewall e del proxy

Risoluzione dei problemi relativi alle impostazioni del firewall e del proxy

Il software di scansione di sicurezza può interferire con la capacità di scaricare file dai server di linguaggio AWS Toolkit rimuovendo i file dai download o impedendo del tutto i download.

Per verificare le impostazioni del firewall e del proxy, accedi a https://aws-toolkit-language-servers.amazonaws.com/codewhisperer/0/manifest.json da un browser Internet installato sullo stesso sistema dell'istanza di Visual Studio in uso. Se riscontri un errore o la pagina non riesce a caricarsi, è possibile che sia presente un firewall o un filtro proxy che ti impedisce di raggiungerla. `aws-toolkit-language-servers.amazonaws.com`

Certificati personalizzati

AWS Toolkit for Visual Studio utilizza un server di lingua che viene eseguito sul runtime Node.js. Per informazioni dettagliate su come verificare se la rete utilizza un certificato personalizzato, consultate l'impostazione del file di configurazione e delle credenziali nell' AWS CLI argomento della Guida per l'AWS Command Line Interfaceutente della versione 1.

Per configurare le impostazioni del proxy e definire un certificato, è necessario configurare la variabile `HTTPS_PROXY` env e creare variabili di ambiente Windows per le chiavi `NODE_OPTIONS` and`NODE_EXTRA_CA_CERTS`.

Per configurare la variabile HTTPS_PROXY env, completa i seguenti passaggi.

1. Dal menu principale di Visual Studio, scegli Strumenti, quindi scegli Opzioni.
2. Dal menu Opzioni, espandi AWS Toolkit, quindi scegli Proxy.
3. Dal menu Proxy, definisci Host e Porta.

> **Note**
>
> Per informazioni sulla configurazione del modulo HTTPS_PROXY AWS CLI, consultate Utilizzo di un proxy HTTP AWS CLI relativo all'argomento della Guida per l'AWS Command Line Interfaceutente.

Create variabili di ambiente Windows per le seguenti chiavi.

- `NODE_OPTIONS = --use-openssl-ca`
- `NODE_EXTRA_CA_CERTS = Path/To/Corporate/Certs`

> **Note**
>
> Per ulteriori informazioni sull'estrazione dei certificati root aziendali, consulta l'articolo Esportare un certificato con la relativa chiave privata all'indirizzo learn.microsoft.com. Per informazioni dettagliate sulle chiavi delle variabili di ambiente di Windows, consulta la documentazione di Node.js v23.3.0 all'indirizzo nodejs.org.

Consenti l'elenco e i passaggi aggiuntivi

Oltre a interferire con i server linguistici AWS Toolkit, le impostazioni del firewall possono impedire ad Amazon Q di caricare su Amazon S3 e richiamare l'API del servizio. Per ridurre al minimo il potenziale di questi errori, consigliamo di consentire l'accesso a Internet in uscita sulla porta 443 (HTTPS) per i seguenti endpoint:

- `https://codewhisperer.us-east-1.amazonaws.com/`
- `https://amazonq-code-transformation-us-east-1-c6160f047e0.s3.amazonaws.com/`

- `https://aws-toolkit-language-servers.amazonaws.com/`
- `https://q.us-east-1.amazonaws.com`
- `https://client-telemetry.us-east-1.amazonaws.com`
- `https://cognito-identity.us-east-1.amazonaws.com`
- `https://oidc.us-east-1.amazonaws.com`

Per un elenco dettagliato degli endpoint, consultate l'argomento Aggiornamento dei firewall e dei gateway per consentire l'accesso in questa Guida per l'utente. Per informazioni dettagliate sulla configurazione di un proxy aziendale per Amazon Q, consulta l'argomento Configurazione di un proxy aziendale in Amazon Q nella Amazon Q Developer User Guide. Se continui a riscontrare problemi con firewall e proxy, raccogli i log del AWS Toolkit e contatta il AWS Toolkit for Visual Studio team tramite la sezione AWS Toolkit for Visual Studio dei problemi del repository. AWS Toolkit for Visual Studio GitHub Per i dettagli sulla raccolta dei log del AWS Toolkit, consulta le informazioni nella sezione sulle migliori pratiche per la risoluzione dei problemi di questo argomento della Guida per l'utente.

Sicurezza per AWS Toolkit for Visual Studio

La sicurezza cloud di Amazon Web Services (AWS) è la priorità più alta. In qualità di 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 te. AWS Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud.

Security of the Cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce tutti i servizi offerti nel AWS Cloud e della fornitura di servizi che è possibile utilizzare in modo sicuro. La nostra responsabilità in AWS materia di sicurezza è la massima priorità e l'efficacia della nostra sicurezza viene regolarmente testata e verificata da revisori di terze parti nell'ambito dei Programmi di AWS conformità.

Sicurezza nel cloud: la responsabilità dell'utente è determinata dal AWS servizio utilizzato e da altri fattori, tra cui la sensibilità dei dati, i requisiti dell'organizzazione e le leggi e i regolamenti applicabili.

Questo AWS prodotto o servizio segue il modello di responsabilità condivisa attraverso i servizi specifici di Amazon Web Services (AWS) che supporta. Per informazioni sulla sicurezza dei AWS servizi, consulta la pagina della documentazione sulla sicurezza del AWS servizio e AWS i servizi che rientrano nell'ambito delle iniziative di AWS conformità previste dal programma di conformità.

Argomenti

Protezione dei dati in AWS Toolkit for Visual Studio

Il modello di responsabilità AWS condivisa di si applica alla protezione dei dati in AWS Toolkit for Visual Studio con Amazon Q. Come descritto in questo modello AWS , è responsabile della protezione dell'infrastruttura globale che esegue tutto il. Cloud AWS L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della

configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per maggiori informazioni sulla privacy dei dati, consulta le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al AWS Modello di responsabilità condivisa e GDPR nel AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con AWS Toolkit con Amazon Q o altro Servizi AWS utilizzando la console, l'API o AWS SDKs. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Identity and Access Management

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori

IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che AWS svolgi.

Utente del servizio: se lo utilizzi Servizi AWS per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS, consulta Risoluzione dei problemi di AWS identità e accesso o consulta la guida per l'utente della funzionalità Servizio AWS che stai utilizzando.

Amministratore del servizio: se sei responsabile delle AWS risorse della tua azienda, probabilmente hai pieno accesso a AWS. È tuo compito determinare a quali AWS funzionalità e risorse devono accedere gli utenti del servizio. Devi quindi inviare le richieste all'amministratore IAM per modificare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS, consulta la guida per l'utente del Servizio AWS software 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 AWS basate sull'identità che puoi utilizzare in IAM, consulta la guida per l'utente di quella Servizio AWS che stai utilizzando.

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la

federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come

creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .

- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come Servizi AWS lavorare con IAM

Per avere una visione di alto livello di come Servizi AWS funziona la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Per scoprire 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 AWS identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con un AWS IAM.

Argomenti

- Non sono autorizzato a eseguire alcuna azione in AWS
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS risorse

Non sono autorizzato a eseguire alcuna azione 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`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona 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 quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

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 trasmettere il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo.

Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS supporta queste funzionalità, consulta. Come Servizi AWS lavorare con IAM
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente di IAM.

Convalida della conformità per questo AWS prodotto o servizio

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta la Documentazione AWS sulla sicurezza.

Questo AWS prodotto o servizio segue il modello di responsabilità condivisa attraverso i servizi specifici di Amazon Web Services (AWS) che supporta. Per informazioni sulla sicurezza dei AWS servizi, consulta la pagina della documentazione sulla sicurezza del AWS servizio e AWS i servizi che rientrano nell'ambito delle iniziative di AWS conformità previste dal programma di conformità.

Resilienza per questo AWS prodotto o servizio

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS di disponibilità.

Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti.

Con le zone di disponibilità è possibile progettare e gestire applicazioni e database che eseguono automaticamente il failover 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 tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, vedere Global Infrastructure.AWS

Questo AWS prodotto o servizio segue il modello di responsabilità condivisa attraverso i servizi specifici di Amazon Web Services (AWS) che supporta. Per informazioni sulla sicurezza dei AWS servizi, consulta la pagina della documentazione sulla sicurezza del AWS servizio e AWS i servizi che rientrano nell'ambito delle iniziative di AWS conformità previste dal programma di conformità.

Sicurezza dell'infrastruttura per questo AWS prodotto o servizio

Questo AWS prodotto o servizio utilizza servizi gestiti ed è pertanto protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere a questo AWS Prodotto o Servizio attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa è possibile utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Questo AWS prodotto o servizio segue il modello di responsabilità condivisa attraverso i servizi specifici di Amazon Web Services (AWS) che supporta. Per informazioni sulla sicurezza dei AWS servizi, consulta la pagina della documentazione sulla sicurezza del AWS servizio e AWS i servizi che rientrano nell'ambito delle iniziative di AWS conformità previste dal programma di conformità.

Analisi della configurazione e delle vulnerabilità in AWS Toolkit for Visual Studio

Il Toolkit for Visual Studio viene rilasciato in Visual Studio Marketplace man mano che vengono sviluppate nuove funzionalità o correzioni. Questi aggiornamenti a volte includono aggiornamenti di sicurezza, quindi è importante mantenere aggiornato AWS Toolkit with Amazon Q

Per verificare che gli aggiornamenti automatici delle estensioni siano abilitati

1. Apri il gestore delle estensioni scegliendo Strumenti, estensioni e aggiornamenti (Visual Studio 2017) o Estensioni, gestisci estensioni (Visual Studio 2019).
2. Scegli Modifica le impostazioni delle estensioni e degli aggiornamenti (Visual Studio 2017) o Modifica le impostazioni per le estensioni (Visual Studio 2019).
3. Regolare le impostazioni per l'ambiente.

Se scegli di disabilitare gli aggiornamenti automatici per le estensioni, assicurati di verificare la presenza di aggiornamenti a AWS Toolkit with Amazon Q a intervalli appropriati per il tuo ambiente.

Cronologia dei documenti della Guida AWS Toolkit for Visual Studio per l'utente

Cronologia dei documenti

La tabella seguente descrive le importanti modifiche recenti della Guida per l' AWS Toolkit for Visual Studio utente. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile sottoscrivere un feed RSS.

Modifica	Descrizione	Data
Aggiornamenti ai contenuti introduttivi	Aggiornamenti apportati a Guida introduttiva e Connessione ai AWS contenuti per riflettere le modifiche apportate all'interfaccia utente.	24 aprile 2025
Aggiornamento di firewall e gateway per consentire l'accesso	Elenchi di endpoint e risorse che devono essere consentiti per accedere a tutti i servizi e le funzionalità AWS Toolkit for Visual Studio di Amazon Q for extensions.	20 marzo 2025
Risoluzione dei problemi relativi alle impostazioni del firewall e del proxy	È stato aggiunto un nuovo argomento di risoluzione dei problemi relativo alle impostazioni del firewall AWS Toolkit for Visual Studio e del proxy per Amazon Q.	15 dicembre 2024
Risoluzione dei problemi di installazione e aggiornamento	Aggiornamento del contenuto del problema di installazione per tenere conto di un aggiornamento di Microsoft.	20 novembre 2024

Aggiornamenti al contenuto introduttivo	Aggiornamenti apportati a Guida introduttiva e Connessione ai AWS contenuti per riflettere le modifiche apportate all'interfaccia utente.	24 ottobre 2024
Aggiornamenti alla connessione a AWS	Aggiornamenti apportati a Connecting to AWS content.	26 settembre 2024
Aggiornamenti ai contenuti di Amazon EC2 AMI	Sono stati apportati aggiornamenti dei contenuti per documentare le modifiche al processo e alle procedure di Amazon EC2 AMI.	13 settembre 2024
AWS I componenti del Toolkit non possono essere inizializzati	È stato aggiunto un argomento di risoluzione dei problemi relativi alla mancata AWS Toolkit for Visual Studio inizializzazione dei componenti.	13 settembre 2024
Visualizzazione e filtraggio delle scansioni di sicurezza di Amazon Q	È stato aggiunto un argomento di risoluzione dei problemi per facilitare la visualizzazione e il filtraggio delle scansioni di sicurezza di Amazon Q.	31 luglio 2024
Amazon Q per AWS Toolkit for Visual Studio	Amazon Q è ora disponibile per AWS Toolkit for Visual Studio.	30 giugno 2024
Aggiornamenti e manutenzione dei contenuti	Aggiornamento dei contenuti per modifiche all'interfaccia utente e alle linee guida di AWS stile.	6 marzo 2024

Aggiornamenti e manutenzione dei contenuti	Aggiornamento dei contenuti per modifiche all'interfaccia utente e alle linee guida di AWS stile.	6 marzo 2024
Aggiornamenti e manutenzione dei contenuti	Aggiornamento dei contenuti per modifiche all'interfaccia utente e alle linee guida di AWS stile.	6 marzo 2024
Aggiornamenti e manutenzione dei contenuti	Aggiornamento dei contenuti per modifiche all'interfaccia utente e alle linee guida di AWS stile.	6 marzo 2024
Aggiornamenti e manutenzione dei contenuti	Aggiornamento dei contenuti per modifiche all'interfaccia utente e alle linee guida di AWS stile.	6 marzo 2024
Aggiornamenti alla configurazione e all'autenticazione	Gli argomenti relativi alla configurazione e all'autenticazione sono stati aggiornati per migliorare la sicurezza e l'esperienza di onboarding del toolkit. Per visualizzare le modifiche, consulta l'argomento TOCs Guida introduttiva e Autenticazione e accesso.	22 giugno 2023
Autenticazione e accesso	Fornire AWS le credenziali è ora Autenticazione e accesso. Rifattorizzazione del TOC e dei sottoargomenti per soddisfare i requisiti AWS di stile e sicurezza.	4 maggio 2023

Aggiornamenti alle sezioni e agli argomenti relativi alla configurazione	La sezione Configurazione delle AWS Toolkit for Visual Studio sezioni e degli argomenti di questa Guida per l'utente è stata aggiornat a per migliorare l'esperienza di imbarco di. AWS Toolkit for Visual Studio	30 gennaio 2023
Aggiornamenti alle sezioni e agli argomenti relativi alla configurazione	La sezione Configurazione delle AWS Toolkit for Visual Studio sezioni e degli argomenti di questa Guida per l'utente è stata aggiornat a per migliorare l'esperienza di imbarco di. AWS Toolkit for Visual Studio	30 gennaio 2023
Sono state aggiunte informazioni sul 2022 AWS Toolkit for Visual Studio	Il supporto per Visual Studio 2022 è stato aggiunto a AWS Toolkit for Visual Studio.	20 dicembre 2022
Aggiornamenti alla AWS guida Publish to	Aggiornamenti della documentazione per rifletter e le modifiche apportate al servizio per il lancio di GA.	6 luglio 2022
Aggiornamenti e trasferimento del titolo	Sono state apportate modifiche minori al titolo per riflettere meglio i contenuti. La guida si trova ora nella AWS guida Publishing to.	6 luglio 2022

Distribuzione su AWS: aggiornamenti di titoli e contenuti	La sezione della guida, formalmente intitolata: Deployment Using the AWS Toolkit, contiene un sommario (TOC) aggiornato ed è ora intitolata: Deploying to. AWS Le seguenti guide hanno completato la deprecazione e non sono più accessibili: Deploying to Elastic Beanstalk (Legacy) e Deploying to (Legacy). AWS CloudForm ation I contenuti aggiornati relativi alla distribuzione su Elastic Beanstalk e Cloudform ation sono disponibili nel sommario aggiornato di questa guida.	6 luglio 2022
La distribuzione di un'app ASP.NET Core 2.0 (Fargate) è ora una guida legacy	Questa documentazione si riferisce ai servizi e alle funzionalità legacy. Per guide e contenuti aggiornati, vedere la guida allo strumento di distribuzione AWS di.NET e il sommario aggiornato Deploying to AWS.	6 luglio 2022
Deploy an ASP.NET App è ora una guida legacy	Questa documentazione si riferisce ai servizi e alle funzionalità legacy. Per guide e contenuti aggiornati, consulta la guida agli strumenti di AWS distribuzione.NET e il sommario Deploying to AWS aggiornato.	6 luglio 2022

Deploy an ASP.NET App è ora una guida legacy	Questa documentazione si riferisce ai servizi e alle funzionalità legacy. Per guide e contenuti aggiornati, consulta la guida agli strumenti di AWS distribuzione.NET e il sommario Deploying to AWS aggiornato.	6 luglio 2022
Nuovo argomento della guida: Utilizzo dei CloudWatch registri in Visual Studio	È stato creato un nuovo argomento di panoramica per la guida all'integrazione di Amazon CloudWatch Logs in Visual Studio.	29 giugno 2022
Nuovo argomento della guida: Configurazione dell'integrazione CloudWatch dei log per Visual Studio	Creata una nuova sezione di configurazione per la guida all'integrazione di Amazon CloudWatch Logs in Visual Studio.	29 giugno 2022
CloudWatch Integrazione dei log per Visual Studio	È stata creata una nuova guida per l'integrazione di Amazon CloudWatch Logs in Visual Studio, che include gli argomenti della guida: Configurazione CloudWatch dei log per Visual Studio e Utilizzo dei CloudWatch log in Visual Studio.	29 giugno 2022
Pubblica su AWS	Pubblica su non AWS è più disponibile in anteprima. Aggiornamenti per riflettere le modifiche all'interfaccia utente e i miglioramenti ai suggerimenti di pubblicazione.	1 giugno 2022

Nuova pubblicazione AWS disponibile per l'anteprima	Esperienza di implement azione migliorata che fornisce indicazioni sul AWS servizio più adatto alla tua applicazi one.	21 ottobre 2021
Supporto SSO e MFA per le credenziali AWS	Aggiornato per documentare il nuovo supporto per AWS Single Sign-On (IAM Identity Center) e l'autenticazione a più fattori nelle credenziali. AWS	21 aprile 2021
Progetto di base AWS Lambda : creazione di un'immagine Docker	È stato aggiunto il supporto per le immagini dei container Lambda.	1 dicembre 2020
Contenuto di sicurezza	Aggiunti contenuti di sicurezza .	6 febbraio 2020
Fornitura di AWS credenziali	Aggiornato con informazioni sulla creazione di profili di credenziali nel file di AWS credenziali condiviso.	20 giugno 2019
Utilizzo del progetto AWS Lambda nel AWS Toolkit for Visual Studio	Il supporto per Visual Studio 2019 è stato aggiunto al AWS Toolkit for Visual Studio.	28 marzo 2019
Tutorial: creazione di un'applic azione Amazon Rekognition Lambda	Il supporto per Visual Studio 2019 è stato aggiunto al AWS Toolkit for Visual Studio.	28 marzo 2019
Tutorial: crea e testa un'applic azione serverless con AWS Lambda	Il supporto per Visual Studio 2019 è stato aggiunto al AWS Toolkit for Visual Studio.	28 marzo 2019

Configurazione del AWS Toolkit for Visual Studio	Il supporto per Visual Studio 2019 è stato aggiunto a AWS Toolkit for Visual Studio.	28 marzo 2019
Distribuzione di un'app ASP.NET Core 2.0 (Fargate)	Il supporto per Visual Studio 2019 è stato aggiunto al AWS Toolkit for Visual Studio.	28 marzo 2019
Distribuzione di un'app ASP.NET Core 2.0 () EC2	Il supporto per Visual Studio 2019 è stato aggiunto al AWS Toolkit for Visual Studio.	28 marzo 2019
Creazione di un progetto AWS CloudFormation modello in Visual Studio	Il supporto per Visual Studio 2019 è stato aggiunto al AWS Toolkit for Visual Studio.	28 marzo 2019
Visualizzazioni dettagliate di Container Service	Sono state aggiunte informazioni sulle visualizzazioni dettagliate dei cluster e dei repository di container di Amazon Elastic Container Service fornite da AWS Explorer.	16 febbraio 2018
Distribuzione su Amazon EC2 Container Service	Sono state aggiunte informazioni sulla distribuzione su Amazon EC2 Container Service.	16 febbraio 2018
Implementazione di Container Service con Fargate	Sono state aggiunte informazioni su come distribuire un'applicazione ASP.NET Core 2.0 containerizzata destinata a Linux tramite Amazon ECS utilizzando il tipo di avvio Fargate.	16 febbraio 2018

Distribuzione di Container Service utilizzando EC2	Sono state aggiunte informazioni su come distribuire un'applicazione ASP.NET Core 2.0 containerizzata destinata a Linux tramite Amazon ECS utilizzando il tipo di avvio. EC2	16 febbraio 2018
Credenziali per la distribuzione su Amazon Container Service EC2	Sono state aggiunte informazioni su come specificare le credenziali durante la distribuzione su Amazon EC2 Container Service.	16 febbraio 2018

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.