

Guida per l'utente

AWS Toolkit per Visual Studio



AWS Toolkit per Visual Studio: Guida per l'utente

Copyright © 2024 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 delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

AWS Toolkit for Visual Studio	1
Cos'è il Toolkit for Visual Studio	1
AWS Explorer	1
Gestione delle credenziali e delle regioni	1
Amazon EC2	2
AWS Lambda	2
AWS CodeCommit	2
Amazon DynamoDB	2
Amazon S3	2
Amazon RDS	2
AWS Elastic Beanstalk	3
AWS CloudFormation	3
AWS Identity and Access Management (IAM)	3
Informazioni correlate	3
Scarica il Toolkit	4
Download del Toolkit da Visual Studio Marketplace	4
Toolkit IDE aggiuntivi da AWS	4
Guida introduttiva	5
Installazione e configurazione	5
Prerequisiti	5
Installazione del AWS Toolkit	6
Disinstallazione del Toolkit AWS	7
Connessione ad AWS	9
Prerequisiti	9
Connessione a dal Toolkit AWS	9
Autenticazione per Amazon CodeWhisperer	11
Autenticazione per Explorer AWS	1
Risoluzione dei problemi di installazione	14
Autorizzazioni di amministratore per Visual Studio	14
Ottenere un registro di installazione	15
Installazione di diverse estensioni di Visual Studio	16
Contattare il supporto	16
Profili e rilegatura delle finestre	16
Profili e associazione delle finestre per Toolkit for Visual Studio	16

Autenticazione e accesso	18
IAM Identity Center	18
Autenticazione con IAM Identity Center dal AWS Toolkit for Visual Studio	19
Credenziali IAM	20
Creazione di un utente IAM	21
Creazione di un file di credenziali	21
Modifica delle credenziali utente IAM dal toolkit	22
Modifica delle credenziali utente IAM da un editor di testo	23
Creazione di utenti IAM da () AWS Command Line InterfaceAWS CLI	23
AWS ID del costruttore	24
Registrazione di un Builder ID AWS	24
Autenticazione a più fattori (MFA)	24
Fase 1: creazione di un ruolo IAM per delegare l'accesso agli utenti IAM	25
Passaggio 2: creazione di un utente IAM che assuma le autorizzazioni del ruolo	26
Fase 3: Aggiungere una policy per consentire all'utente IAM di assumere il ruolo	26
Fase 4: Gestione di un dispositivo MFA virtuale per l'utente IAM	27
Fase 5: Creazione di profili per consentire l'autenticazione a più fattori	28
Credenziali esterne	29
Lavorare con AWS i servizi	30
Amazon CodeCatalyst	30
Che cos'è Amazon CodeCatalyst?	30
Nozioni di base su CodeCatalyst	31
Utilizzo di CodeCatalyst	32
Risoluzione dei problemi	34
Amazon CodeWhisperer	35
Che cos'è CodeWhisperer?	35
CloudWatch Integrazione di log	35
Configurazione di CloudWatch Log	35
Utilizzo di CloudWatch Log	36
Gestione delle istanze Amazon EC2	42
Le immagini di Amazon Machine e le visualizzazioni delle istanze Amazon EC2	43
Avvio di un'istanza Amazon EC2	45
Connessione a un'istanza Amazon EC2	48
Terminazione di un'istanza Amazon EC2	51
Gestione delle istanze Amazon ECS	54
Modifica delle proprietà del servizio	55

Interruzione di un'attività	55
Eliminazione di un servizio	55
Eliminazione di un cluster	56
Creazione di un repository	56
Eliminazione di un repository	56
Gestione di gruppi di sicurezza daAWSEsploratore	57
Creazione di un gruppo di sicurezza	57
Aggiunta di autorizzazioni ai gruppi di sicurezza	58
Creazione AMI un'istanza Amazon EC2	59
Impostazione delle autorizzazioni di avvio per un'Amazon Machine Image	61
Amazon Virtual Private Cloud (VPC)	63
Creazione di un VPC pubblico-privato per la distribuzione conAWS Elastic Beanstalk	64
Utilizzo dell'editor AWS CloudFormation di modelli per Visual Studio	68
Creazione di unAWS CloudFormationProgetto modello in Visual Studio	69
Distribuzione di unAWS CloudFormationModello in Visual Studio	72
Formattazione di unAWS CloudFormationModello in Visual Studio	75
Uso di Amazon S3 daAWSEsploratore	76
Creazione di un bucket Amazon S3	77
Gestione dei bucket Amazon S3 daAWSEsploratore	77
Caricamento di file e cartelle in Amazon S3	79
Operazioni sui file Amazon S3 daAWSToolkit for Visual Studio	80
Utilizzo di DynamoDBAWSEsploratore	84
Creazione di una tabella DynamoDB	85
Visualizzazione di una tabella DynamoDB come una griglia	86
Modifica e aggiunta di attributi e valori	87
Scansione di una tabella DynamoDB	89
Utilizzo diAWS CodeCommitcon Visual Studio Team Explorer	90
Tipo di credenziali perAWS CodeCommit	91
Connessione ad AWS CodeCommit	91
Creazione di un repository	93
Configurazione delle credenziali Git	94
Clonazione di un repository	96
Utilizzo dei repository	97
Utilizzo di CodeArtifact in Visual Studio	98
Aggiungi il tuo repository CodeArtifact come sorgente di pacchetti NuGet	98
Amazon RDS daAWSEsploratore	99

Seleziona Avvia un'istanza di database Amazon RDS	100
Creare un database Microsoft SQL Server in un'istanza RDS	108
Gruppi di sicurezza Amazon RDS	109
Utilizzo di Amazon SimpleDB daAWSEsploratore	113
Utilizzo di Amazon SQSAWSEsploratore	115
Creazione di una coda	115
Eliminazione di una coda	116
Gestione delle proprietà della coda	116
Invio di un messaggio a una coda	117
Identity and Access Management	118
Creazione e configurazione di un utente IAM	119
Creazione di un gruppo IAM	120
Aggiunta di un utente IAM a un gruppo IAM	121
Creazione di credenziali per un utente IAM	123
Creare un ruolo IAM	125
Creare una policy IAM	126
AWS Lambda	129
AWS Lambda Progetto base	129
AWS Lambda Progetto di base per la creazione di un'immagine Docker	136
Tutorial: crea e testa un'applicazione serverless con AWS Lambda	144
Tutorial: creazione di un'applicazione Amazon Rekognition Lambda	150
Tutorial: Utilizzo di Amazon Logging Frameworks AWS Lambda per creare log di applicazioni	158
Implementazione suAWS	161
Publish to (Pubblica in CloudWatch)AWS	161
Prerequisiti	162
Tipi di applicazioni supportati	163
Pubblicazione delle applicazioniAWSbersagli	163
AWS Lambda	165
Prerequisiti	165
Argomenti correlati	166
Elenco dei comandi Lambda disponibili tramite l'interfaccia a riga di comando di .NET Core	166
Pubblicazione di un progetto .NET Core Lambda dall'interfaccia della riga di comando .NET Core	167
Distribuzione su Elastic Beanstalk	169

Implementazione di un'app ASP.NET (tradizionale)	170
Implementazione di un'app ASP.NET (.NET Core) (Legacy)	182
SpecificaAWSCredenziali	184
Ripubblica su Elastic Beanstalk (Legacy)	185
Distribuzioni personalizzate (tradizionali)	187
Distribuzioni personalizzate (.NET Core)	189
Support per molteplici applicazioni	193
Implementazione in Amazon EC2 Container Service	196
SpecificaAWSCredenziali	197
Implementazione di un'app ASP.NET Core 2.0 (Fargate) (Legacy)	199
Distribuire un'applicazione ASP.NET Core 2.0 (EC2)	206
Risoluzione dei problemi	211
Best practice per la risoluzione dei problemi	211
Amazon CodeWhisperer Sign In e Sign Out sono disattivati	212
Sicurezza	213
Protezione dei dati	213
Identity and Access Management	214
Destinatari	215
Autenticazione con identità	215
Gestione dell'accesso con policy	219
Come Servizi AWS lavorare con IAM	222
Risoluzione dei problemi di AWS identità e accesso	222
Convalida della conformità	224
Resilienza	225
Sicurezza dell'infrastruttura	226
Analisi della configurazione e delle vulnerabilità	226
Cronologia dei documenti	228
Cronologia dei documenti	228
.....	ccxxxvi

AWS Toolkit for Visual Studio

Questa è la guida per l'utente di AWS Toolkit for Visual Studio. 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 Toolkit for Visual Studio

AWS Toolkit for Visual Studio è un plug-in per l'IDE di Visual Studio che semplifica lo sviluppo, il debug e la distribuzione di applicazioni.NET che utilizzano Amazon Web Services. Il Toolkit for Visual Studio è supportato per le versioni di Visual Studio 2019 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 e 2017. Tuttavia, tali versioni non sono più supportate. Per ulteriori informazioni, consulta l'argomento [Installazione e configurazione](#) di questa Guida per l'utente.

Il Toolkit for Visual Studio contiene le seguenti funzionalità per migliorare l'esperienza di sviluppo.

AWS Explorer

La finestra degli strumenti AWS Explorer, disponibile nel menu Visualizza dell'IDE, consente di interagire con molti AWS servizi dall'interno dell'IDE di Visual Studio. I servizi dati supportati includono Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS) e Amazon CloudFront. AWS Explorer fornisce anche l'accesso alla gestione di Amazon Elastic Compute Cloud (Amazon EC2), AWS Identity and Access Management, alla gestione di utenti e policy (IAM), alla distribuzione di applicazioni e funzioni serverless e AWS Lambda alla distribuzione di applicazioni Web su e. AWS Elastic Beanstalk AWS CloudFormation

Gestione delle credenziali e delle regioni

AWS Explorer supporta più AWS account (inclusi gli account utente IAM) e regioni e consente di modificare facilmente la visualizzazione visualizzata da un account all'altro o di visualizzare e gestire risorse e servizi in diverse regioni.

Amazon EC2

Da AWS Explorer, puoi visualizzare le Amazon Machine Images (AMI) disponibili, creare istanze Amazon EC2 da tali AMI e quindi connetterti a tali istanze utilizzando Windows Remote Desktop. AWS Explorer abilita anche funzionalità di supporto, come la capacità di creare e gestire coppie di chiavi e gruppi di sicurezza.

AWS Lambda

Puoi usare Lambda per ospitare le funzioni e le applicazioni serverless di .NET Core C#. Usa i blueprint per creare rapidamente nuovi progetti serverless e iniziare subito a sviluppare applicazioni serverless.

AWS CodeCommit

CodeCommit è integrato con Visual Studio Team Explorer. Ciò semplifica la clonazione e la creazione di repository archiviati CodeCommit e l'utilizzo delle modifiche al codice sorgente dall'interno dell'IDE.

Amazon DynamoDB

DynamoDB è un servizio di database non relazionale veloce, altamente scalabile, altamente disponibile ed economico. Il Toolkit for Visual Studio offre funzionalità per lavorare con Amazon DynamoDB in un contesto di sviluppo. Con Toolkit for Visual Studio, puoi creare e modificare gli attributi nelle tabelle DynamoDB ed eseguire operazioni di scansione sulle tabelle.

Amazon S3

Puoi caricare contenuti in modo rapido e semplice su bucket Amazon S3 trascinandoli o scaricandoli da Amazon S3. Puoi anche impostare comodamente autorizzazioni, metadati e tag sugli oggetti contenuti nei bucket.

Amazon RDS

AWS Explorer può aiutarti a creare e gestire risorse Amazon RDS in Visual Studio. Le istanze Amazon RDS che utilizzano Microsoft SQL Server possono anche essere aggiunte a Server Explorer di Visual Studio.

AWS Elastic Beanstalk

Puoi usare Elastic Beanstalk per distribuire i tuoi progetti di applicazioni web.NET su. AWS È possibile distribuire l'applicazione in un ambiente a singola istanza o in un ambiente con carico completamente bilanciato e scalato automaticamente dall'interno dell'IDE. Puoi anche distribuire nuove versioni dell'applicazione in modo rapido e comodo senza uscire da Visual Studio. Se la tua applicazione utilizza SQL Server in Amazon RDS, la procedura guidata di distribuzione può anche configurare la connettività tra l'ambiente applicativo in Elastic Beanstalk e l'istanza di database in Amazon RDS. Il Toolkit for Visual Studio include anche lo strumento di distribuzione a riga di comando autonomo. Usa lo strumento di distribuzione per rendere la distribuzione una parte automatica del processo di compilazione o per includere la distribuzione in altri scenari di script esterni a Visual Studio.

AWS CloudFormation

Puoi usare Toolkit for Visual Studio per AWS CloudFormation modificare modelli in formato JSON con supporto per IntelliSense l'editor e l'evidenziazione della sintassi. Con un AWS CloudFormation modello descrivi le risorse che desideri istanziare per ospitare la tua applicazione. Dall'interno dell'IDE, quindi distribuisce il modello in. AWS CloudFormation Le risorse descritte nel modello vengono fornite automaticamente, consentendoti di concentrarti sullo sviluppo delle funzionalità dell'applicazione.

AWS Identity and Access Management (IAM)

Da AWS Explorer, puoi creare utenti, ruoli e policy IAM e allegare policy agli utenti.

Informazioni correlate

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

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

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 [AWSdei download di Visual Studio](#) nel tuo browser web.

Toolkit IDE aggiuntivi da AWS

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

AWS Toolkit for Visual Studio Codelink

- Segui questo link per [scaricare il file AWS Toolkit for Visual Studio Code](#) dal VS Code Marketplace.
- Per saperne di piùAWS Toolkit for Visual Studio Code, consulta la Guida [AWS Toolkit for Visual Studio Code](#)per l'utente.

AWS Toolkit for JetBrainslink

- Segui questo link per [scaricarlo AWS Toolkit for JetBrains dal](#) JetBrains Marketplace.
- Per ulteriori informazioniAWS Toolkit for JetBrains, consulta la Guida per l'[AWS Toolkit for JetBrains](#)utente.

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](#)
- [Connessione ad AWS](#)
- [Risoluzione dei problemi di installazione di AWS Toolkit for Visual Studio](#)
- [Profili e rilegatura delle finestre](#)

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](#)
- [Installazione del AWS Toolkit for Visual Studio](#)
- [Disinstallazione di AWS Toolkit for Visual Studio](#)

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 Studio](#) destinazione 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 Studio](#) destinazione.

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'installazione 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 ad AWS

La maggior parte dei servizi e delle risorse Amazon Web Services (AWS) viene gestita tramite un AWS account. Non è necessario un AWS account per utilizzare il ToolkitAWS Toolkit for Visual Studio, tuttavia le funzioni del Toolkit sono limitate senza una connessione.

Se in precedenza hai configurato un AWS account e l'autenticazione tramite un altro AWS servizio (comeAWS Command Line Interface), Toolkit for Visual Studio rileva automaticamente le tue credenziali.

Prerequisiti

Se sei nuovo AWS o non hai ancora creato un account, ci sono 3 passaggi principali per connettere Toolkit for Visual Studio al AWS tuo account:

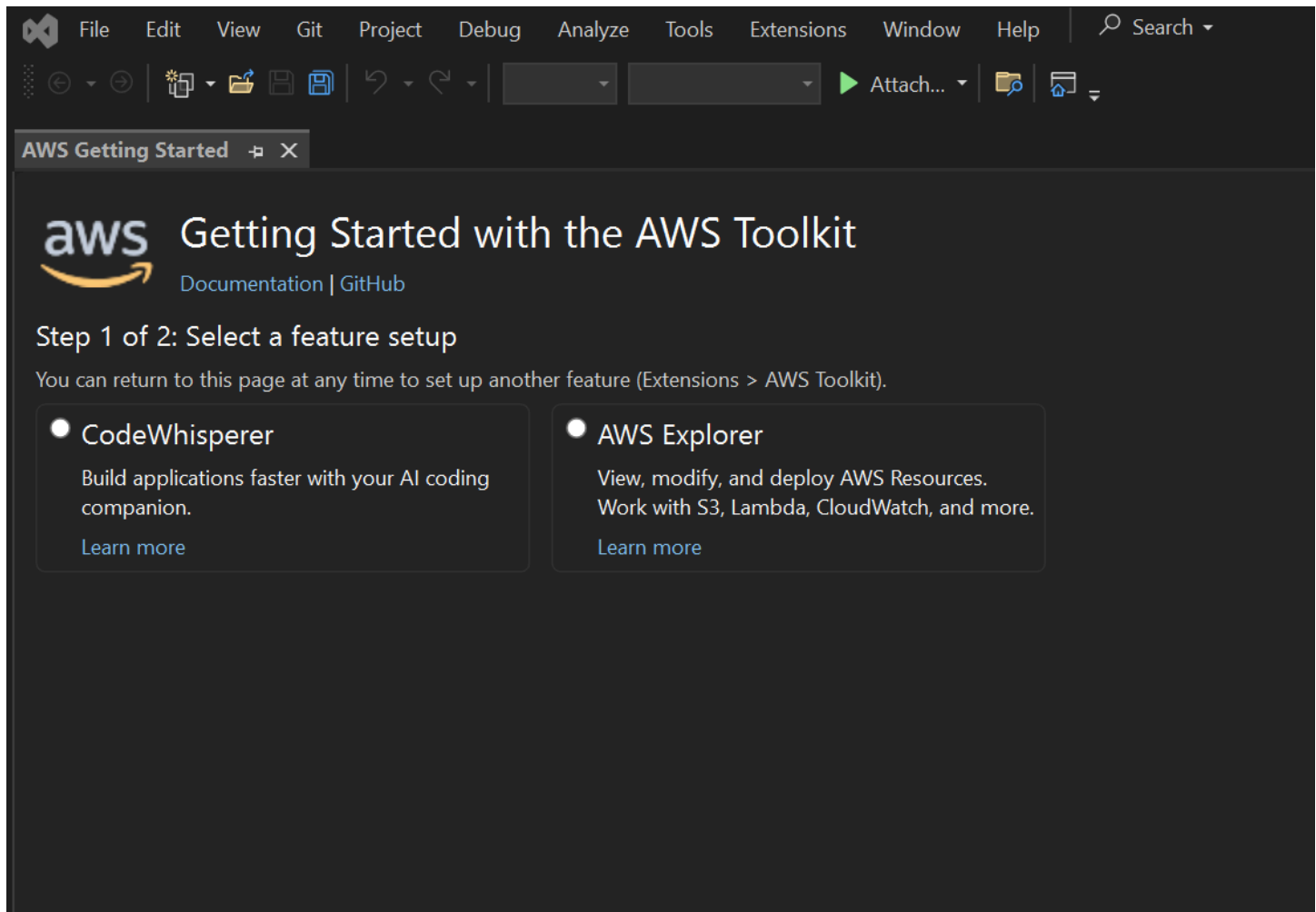
1. Creazione di un account AWS: puoi creare un account AWS dal portale [Iscriviti ad AWS](#). Per informazioni dettagliate sulla configurazione di un nuovo AWS account, consulta l'argomento [Panoramica](#) nella Guida per l'utente alla AWS configurazione.
2. Configurazione dell'autenticazione: Esistono 3 metodi principali per l'autenticazione con l'AWSaccount del Toolkit for Visual Studio. Per ulteriori informazioni su ciascuno di questi metodi, consulta l'argomento [Autenticazione e accesso](#) in questa Guida per l'utente.
3. Autenticazione AWS dal Toolkit: è possibile connettersi al AWS proprio account dal Toolkit completando le procedure descritte nelle seguenti sezioni di questa Guida per l'utente.

Connessione a dal Toolkit AWS

Per connetterti ai tuoi AWS account da Toolkit for Visual Studio, apri la Guida introduttiva AWS all'interfaccia utente Toolkit (interfaccia utente di connessione) completando la procedura seguente.

1. Dal menu principale di Visual Studio, espandi Estensioni, quindi espandi Toolkit. AWS

2. Dalle opzioni del menu AWSToolkit scegli Guida introduttiva.
3. L'interfaccia utente di connessione Getting Started with the AWS Toolkit si apre in Visual Studio.



La tabella seguente descrive quali metodi di autenticazione sono compatibili con ciascuna funzionalità. Per ulteriori informazioni su ciascuno dei 3 metodi di autenticazione AWS IAM Identity Center, AWS Identity and Access Management le credenziali e l'ID AWS Builder, consulta il sommario [Autenticazione e accesso](#) in questa Guida per l'utente.

Note

Al momento, quando lavori con CodeCatalyst Toolkit for Visual Studio, devi solo autorizzare con il tuo ID Builder quando cloni un repository di terze parti.

Amazon CodeWhisperer	AWS Explorer	Amazon CodeCatalyst
<input checked="" type="checkbox"/> ID del AWS costruttore	<input checked="" type="checkbox"/> ID del AWS costruttore	<input checked="" type="checkbox"/> ID del AWS costruttore
<input checked="" type="checkbox"/> IAM Identity Center	<input checked="" type="checkbox"/> IAM Identity Center	<input checked="" type="checkbox"/> IAM Identity Center
<input checked="" type="checkbox"/> Credenziali AWS IAM	<input checked="" type="checkbox"/> Credenziali AWS IAM	<input checked="" type="checkbox"/> Credenziali AWS IAM

Autenticazione per Amazon CodeWhisperer

Per iniziare CodeWhisperer, autenticali e connessi con le tue credenziali AWS IAM Identity Center o con il AWS Builder ID.

Le seguenti procedure descrivono come autenticare e connettere il Toolkit al tuo account. AWS

Autentica e connessi con IAM Identity Center

1. Dall'interfaccia utente di connessione Getting Started with the AWS Toolkit, seleziona il CodeWhispererradiale per espandere le CodeWhisperer opzioni di autenticazione.

Note

Se non esistono credenziali archiviate, procedi al passaggio 3 per aggiungere o aggiornare le credenziali di IAM Identity Center.

2. Dalla CodeWhisperer sezione La mia organizzazione ha abilitato, espandi il menu Scegli da un profilo esistente o aggiungi un nuovo menu a discesa da scegliere dall'elenco delle credenziali archiviate.
3. Dal menu a discesa Tipo di profilo, scegli AWS IAM Identity Center
4. Nel campo di testo Profile Name, inserisci il **Profile Name** profilo 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 (il valore predefinito 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 credenziali del tuo IAM Identity Center, quindi scegli il pulsante Connect per aprire la finestra di dialogo Accedi con IAM Identity Center. AWS
8. Dalla finestra di dialogo Accedi con AWS IAM Identity Center, scegli il pulsante Procedi al browser per aprire il sito di richiesta di autorizzazione nel tuo browser web predefinito. AWS
9. Conferma che il codice di sicurezza nel tuo IDE corrisponda al codice di conferma della richiesta di AWS autorizzazione visualizzato nel tuo browser web e scegli il pulsante Invia e continua per procedere.
10. 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.

Autentica e connettiti con un Builder ID AWS

1. Dall'interfaccia utente di connessione Getting Started with the AWS Toolkit, seleziona il CodeWhispererradiale per espandere le opzioni di autenticazione. CodeWhisperer
2. Nella sezione Sto usando per CodeWhisperer conto mio, scegli il pulsante Registrati o Accedi per aprire la finestra di dialogo Accedi con AWS Builder ID.
3. Scegli il pulsante Procedi al browser per aprire il sito di richiesta di AWS autorizzazione nel tuo browser web predefinito.
4. Conferma che il codice di sicurezza nel tuo IDE corrisponda al codice di conferma della richiesta di AWS autorizzazione visualizzato nel tuo browser web e scegli il pulsante Invia e continua per procedere.
5. 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.

Autenticazione per Explorer AWS

Per iniziare a lavorare con AWS Explorer dal Toolkit, esegui l'autenticazione e connettiti con le tue credenziali IAM Identity Center o le credenziali IAM.

Le seguenti procedure descrivono come autenticare e connettere il Toolkit al tuo account. AWS

Autentica e connettiti con IAM Identity Center

1. Dall'interfaccia utente di connessione Getting Started with the AWS Toolkit, seleziona AWSExplorer radial per espandere le CodeWhisperer opzioni di autenticazione.

2. Dal **Profile Type** menu a discesa, scegli. AWS IAM Identity Center
3. Nel campo di testo Profile Name, inserisci il **Profile Name** profilo IAM Identity Center che desideri utilizzare.
4. Nel campo di testo Start URL, inserisci le **Start URL** credenziali allegate alle tue credenziali IAM Identity Center.
5. Dal menu a discesa Profile Region (il valore predefinito è us-east-1), scegli la regione del profilo definita dal profilo utente IAM Identity Center con cui ti stai autenticando.
6. Dal menu a discesa Regione SSO (il valore predefinito è us-east-1), scegli la regione SSO definita dalle tue credenziali IAM Identity Center.
7. Scegli il pulsante Procedi al browser per aprire il sito di richiesta di autorizzazione nel AWS tuo browser web predefinito.
8. Conferma che il codice di sicurezza nel tuo IDE corrisponda al codice di conferma della richiesta di AWS autorizzazione visualizzato nel tuo browser web e scegli il pulsante Invia e continua per procedere.
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.

Autentica e connettiti con le credenziali IAM

1. Dall'interfaccia utente di connessione Getting Started with the AWS Toolkit, seleziona AWSExplorer radial per espandere le opzioni di autenticazione. CodeWhisperer
2. Dal menu a **Profile Type** discesa, scegli IAM User Role.
3. Nel campo di testo Profile Name, inserisci il **Profile Name** profilo con cui desideri autenticarti.
4. Nel campo di testo Access Key ID, inserisci **Access Key ID** il profilo con cui desideri autenticarti.
5. Nel campo di testo Secret Key, inserisci **Secret Key** il profilo con cui desideri autenticarti.
6. 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 Stored.
7. Dal menu a discesa Regione del profilo (il valore predefinito è us-east-1), scegli l'area del profilo associata al profilo con cui desideri autenticarti.

Risoluzione dei problemi di installazione di AWS Toolkit for Visual Studio

È noto che le seguenti informazioni risolvono i problemi di installazione più comuni durante l'installazione di AWS Toolkit for Visual Studio.

Se riscontri 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 in ciascuna delle sezioni seguenti.

Autorizzazioni di amministratore per Visual Studio

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

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 il programma di avvio delle applicazioni di Visual Studio (icona).
2. Apri il menu contestuale per (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 da remoto:

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

Note

Sia che tu stia avviando il programma localmente o effettuando una connessione remota, Windows potrebbe richiedere di confermare le tue credenziali amministrative.

Ottenere un registro di installazione

Se hai completato i passaggi della precedente sezione delle autorizzazioni di amministratore riportata sopra e hai confermato che stai eseguendo o ti connetti a Visual Studio con le autorizzazioni di amministratore, ottenere un file di registro dell'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 dell'installazione, completa i seguenti passaggi.

1. Dalla pagina [AWS Toolkit for Visual Studio](#) iniziale, 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 Command Line, quindi scegli Visual Studio Developer Command Prompt.
3. Dal prompt dei comandi per sviluppatori di Visual Studio, 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 del `vsixinstaller` comando con il percorso e il nome del file specificati è simile al seguente:

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

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

Un esempio del `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 dell'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 con 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 aprirne uno nuovo dal sito [AWS Toolkit for Visual StudioGithub](#) Issues.

Per aiutarti a trovare rapidamente una soluzione al tuo problema:

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

Profili e rilegatura delle finestre

Profili e associazione delle finestre per Toolkit for Visual Studio

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

- La finestra AWS Explorer è associata a un singolo profilo e regione alla volta. Le finestre sono state aperte dall'impostazione predefinita di AWS Explorer a quel profilo e regione associati.

- Dopo aver aperto una nuova finestra, puoi usare quell'istanza di AWS Explorer per passare a un profilo o un'area geografica diversi.
- Gli strumenti e le funzionalità di pubblicazione del Toolkit for Visual Studio si basano automaticamente sul profilo e sulla regione impostati in AWS Explorer.
- Se viene specificato un nuovo profilo o una nuova regione in uno strumento, una procedura guidata o una funzionalità di pubblicazione: tutte le risorse create successivamente continueranno a utilizzare le nuove impostazioni del profilo e della regione.
- Se sono aperte più istanze di Visual Studio, ciascuna istanza può essere associata a un profilo e a un'area diversi.
- L'AWS Explorer salva l'ultimo profilo e la regione 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. Tuttavia, la maggior parte AWS delle risorse viene gestita tramite un AWS account. Per accedere a tutti i servizi e le funzionalità di AWS Toolkit for Visual Studio, sono necessari almeno 2 tipi di autenticazione dell'account:

1. AWS Identity and Access Management (IAM) o AWS IAM Identity Center autenticazione 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](#)

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 (SDK) e su come AWS Toolkit for Visual Studio, consulta la sezione sull'[autenticazione di IAM Identity Center](#) della Guida di riferimento agli AWS SDK and Tools.

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 `<home-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 `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: creazione del 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 AWS SDK 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

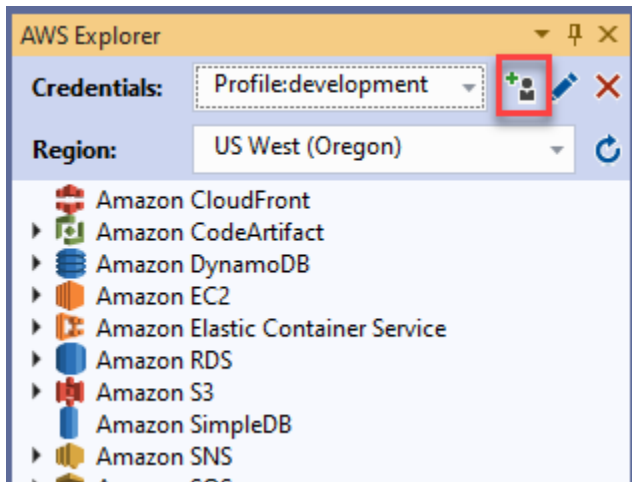
Per aggiungere o creare un utente `credentials file` da: AWS Toolkit for Visual Studio

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 di riferimento agli AWS SDK and Tools.

Creazione di utenti IAM da () AWS Command Line InterfaceAWS 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, come Amazon CodeWhisperer e Amazon CodeCatalyst.

Le sezioni seguenti descrivono come creare un AWS Builder ID e autenticarsi con il tuo AWS account da AWS Toolkit for Visual Studio

Note

Al momento, l'unica volta in cui è richiesto un AWS Builder ID per il CodeCatalyst servizio per Toolkit for Visual Studio è quando si clona un repository di terze parti.

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

Registrazione di un Builder ID AWS

Per iscriverti al tuo AWS Builder ID da Visual Studio, completa i passaggi seguenti.

1. Dall'interfaccia utente di connessione Getting Started with the AWS Toolkit, seleziona il CodeWhispererradiale per espandere le CodeWhisperer opzioni di autenticazione.
2. Nella sezione Sto usando per CodeWhisperer conto mio, scegli il pulsante Registrati o Accedi per aprire la finestra di dialogo Accedi con AWS AWS Builder ID.
3. Scegli il pulsante Apri e copia il codice per aprire il sito di richiesta di AWS autorizzazione nel tuo browser web predefinito.
4. Dal sito di richiesta di AWS autorizzazione, incolla il codice di conferma da Visual Studio e scegli il pulsante Invia e continua per procedere.
5. 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.

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 https://console.aws.amazon.com/iam](https://console.aws.amazon.com/iam).
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 opzionale.
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](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. Scegli 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 Review policy (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]` il profilo definisce in che modo 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.

Lavorare con AWS i servizi

Negli argomenti seguenti viene descritto come iniziare a utilizzare i AWS servizi del AWS Toolkit for Visual Studio.

Argomenti

- [Amazon CodeCatalyst per il AWS Toolkit per Visual Studio](#)
- [Lavorare con Amazon CodeWhisperer](#)
- [Amazon CloudWatch Integrazione di log per Visual Studio](#)
- [Gestione delle istanze Amazon EC2](#)
- [Gestione delle istanze Amazon ECS](#)
- [Gestione di gruppi di sicurezza daAWSEsploratore](#)
- [Creazione AMI un'istanza Amazon EC2](#)
- [Impostazione delle autorizzazioni di avvio per un'Amazon Machine Image](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- [Utilizzo dell'editor AWS CloudFormation di modelli per Visual Studio](#)
- [Uso di Amazon S3 daAWSEsploratore](#)
- [Utilizzo di DynamoDBAWSEsploratore](#)
- [Utilizzo diAWS CodeCommitcon Visual Studio Team Explorer](#)
- [Utilizzo di CodeArtifact in Visual Studio](#)
- [Amazon RDS daAWSEsploratore](#)
- [Utilizzo di Amazon SimpleDB daAWSEsploratore](#)
- [Utilizzo di Amazon SQSAWSEsploratore](#)
- [Identity and Access Management](#)
- [AWS Lambda](#)

Amazon CodeCatalyst per il AWS Toolkit per Visual Studio

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, puoi visualizzare e gestire CodeCatalyst le

risorse direttamente da AWS Toolkit for Visual Studio. Per ulteriori informazioni CodeCatalyst, consulta la [Amazon CodeCatalyst User Guide](#).

Gli argomenti seguenti descrivono come connettere il AWS Toolkit per Visual Studio CodeCatalyst e come utilizzarlo CodeCatalyst tramite AWS Toolkit for Visual Studio.

Argomenti

- [Guida introduttiva ad Amazon CodeCatalyst e al AWS Toolkit per Visual Studio](#)
- [Utilizzo CodeCatalyst delle risorse Amazon del AWS Toolkit per Visual Studio](#)
- [Risoluzione dei problemi](#)

Guida introduttiva ad Amazon CodeCatalyst e al AWS Toolkit per Visual Studio

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

Argomenti

- [Installazione del AWS Toolkit per Visual Studio](#)
- [Creazione di un CodeCatalyst account e di un AWS Builder ID](#)
- [Connessione di AWS Toolkit per Visual Studio con CodeCatalyst](#)

Installazione del AWS Toolkit per Visual Studio

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

Creazione di un CodeCatalyst account e di un AWS Builder ID

Oltre a installare la versione più recente di AWS Toolkit for Visual Studio, devi disporre di un ID AWS Builder e di un CodeCatalyst account attivi per connetterti a AWS Toolkit for Visual Studio. Se non disponi di un ID o di un CodeCatalyst account AWS Builder attivo, consulta la CodeCatalyst sezione [Configurazione con](#) nella Guida per l'CodeCatalystutente.

Note

Un AWS Builder ID è diverso dalle tue AWS credenziali. Per istruzioni su come registrarsi e autenticarsi con un AWS Builder ID, consulta l'argomento [Autenticazione e accesso: AWS Builder ID](#) di questa Guida per l'utente.

Per informazioni dettagliate sugli ID AWS Builder, consulta l'argomento [AWSBuilder ID](#) nella Guida per l'utente di riferimento AWS generale.

Connessione di AWS Toolkit per Visual Studio con CodeCatalyst

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

1. Dalla voce di menu Git in Visual Studio, scegli Clone Repository... .
2. Dalla sezione Browse a Repository, seleziona Amazon CodeCatalyst come provider.
3. Dalla sezione Connessione, scegli Connettiti con AWS Builder ID per aprire la CodeCatalyst console nel tuo browser web preferito.
4. Dal tuo browser, inserisci il tuo ID AWS Builder nell'apposito campo e segui le istruzioni per continuare.
5. Quando richiesto, scegli Consenti per confermare la connessione tra AWS Toolkit for Visual Studio e il tuo CodeCatalyst account. Quando il processo di connessione è completo, CodeCatalyst viene visualizzata una conferma che indica che è sicuro chiudere il browser.

Utilizzo CodeCatalyst delle risorse Amazon del AWS Toolkit per Visual Studio

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

Argomenti

- [Clonare un repository](#)

Clonare un repository

CodeCatalyst è un servizio basato su cloud che richiede la connessione al cloud per lavorare su CodeCatalyst progetti. Per lavorare su un progetto localmente, puoi clonare i CodeCatalyst repository sul tuo computer locale e sincronizzarli con il tuo CodeCatalyst progetto la prossima volta che ti connetti al cloud.

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

1. Dalla voce di menu Git in Visual Studio, scegli Clone Repository... .
2. Dalla sezione Browse a Repository, seleziona Amazon CodeCatalyst come provider.

Note

Se la sezione Connessione visualizza un Not Connected messaggio, completa i passaggi 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 clonare correttamente.

6. Seleziona Clona 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 nel repository clonato, le opzioni di Visual Studio possono essere regolate dall'impostazione Carica automaticamente la soluzione all'apertura di un repository Git, che si trova nelle Impostazioni globali di Git, del menu Controllo del codice sorgente.

Risoluzione dei problemi

Di seguito sono riportati gli argomenti relativi alla risoluzione di problemi noti quando si lavora con Amazon CodeCatalyst tramite AWS Toolkit per Visual Studio.

Argomenti

- [Credenziali](#)

Credenziali

Se incontri una finestra di dialogo che richiede le credenziali quando tenti di clonare un repository basato su git, il tuo AWSCodeCommitCredential helper potrebbe essere configurato a CodeCatalyst livello globale, causando interferenze con. CodeCatalyst Per ulteriori informazioni sull'helper delle AWS CodeCommit credenziali, consulta la sezione relativa alla [configurazione delle connessioni HTTPS ai AWS CodeCommit repository su Windows con l'aiuto delle credenziali AWS CLI della Guida per l'utente](#). AWSCodeCommit

Per limitare l'Helper AWS CodeCommit delle credenziali alla gestione solo degli CodeCommit URL, completa i seguenti passaggi.

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

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

3. Cambia quella sezione nel modo seguente:

```
[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.

Lavorare con Amazon CodeWhisperer

Che cos'è CodeWhisperer?

Amazon CodeWhisperer è un generatore di machine-learning-powered codice generico che ti fornisce consigli sul codice in tempo reale. Durante la scrittura del codice, genera CodeWhisperer automaticamente suggerimenti in base al codice e ai commenti esistenti. I consigli personalizzati possono variare in termini di dimensioni e portata, da un commento a riga singola a funzioni complete.

Per ulteriori informazioni, consulta la [Amazon CodeWhisperer User Guide](#).

Per istruzioni su come autenticarsi e connettersi CodeWhisperer dal Toolkit, consulta la CodeWhisperer sezione [Authentication for Amazon](#) nell'argomento Getting Started di questa Guida per l'utente.

Amazon CloudWatch Integrazione di log per Visual Studio

Amazon CloudWatch Integrazione di log daAWSToolkit for Visual Studio ti dà la possibilità di monitorare, archiviare e accedere CloudWatch Registra le risorse, senza dover lasciare il tuo IDE. Per ulteriori informazioni su come impostare CloudWatch servizio e come utilizzare CloudWatch Funzionalità dei log, scegli tra i seguenti argomenti.

Argomenti

- [Configurazione di CloudWatch Integrazione di log per Visual Studio](#)
- [Utilizzo di CloudWatch Accesso di Visual Studio](#)

Configurazione di CloudWatch Integrazione di log per Visual Studio

Prima di poter utilizzare Amazon CloudWatch Integrazione di log con Toolkit for Visual Studio, è necessarioAWSconto. Puoi creare un nuovoAWSaccount dal[AWSaccesso](#)sito. La maggior parte delle CloudWatch Le funzionalità dei registri disponibili nel Toolkit for Visual Studio sono accessibili con activeAWSCredenziali . Se una particolare funzione richiede una configurazione aggiuntiva, i requisiti sono inclusi nelle sezioni pertinenti del[Utilizzo di CloudWatch Log](#)guide.

Per ulteriori informazioni e opzioni sulla configurazione CloudWatch Log, vedere la[Configurazione delle impostazioni](#)sezione dell'Amazzonia CloudWatch Guida ai registri.

Utilizzo di CloudWatch Accesso di Visual Studio

Amazon CloudWatch L'integrazione dei log di consente di monitorare, archiviare e accedere CloudWatch I log di eventi diAWSToolkit for Visual Studio Avere accesso a CloudWatch Le funzionalità di log, senza la necessità di uscire dal proprio IDE, migliorano l'efficienza semplificando il CloudWatch Registra il processo di sviluppo e riduce le interruzioni del flusso di lavoro. Negli argomenti seguenti viene descritto come usare le caratteristiche e le funzioni di base CloudWatch Integrazione dei log.

Argomenti

- [CloudWatch Gruppi di log di](#)
- [CloudWatch Flussi di log](#)
- [CloudWatch Eventi di log](#)
- [Accesso aggiuntivo a CloudWatchLog](#)

CloudWatch Gruppi di log di

UNlog groupè un gruppo di log streamsche condividono 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

LaView Log Groupsmostra un elenco di CloudWatchEsplora

Per accedere alla funzione Visualizza gruppi di log e aprire il CloudWatch Flussi di log

1. DaAWSExplorer, espandiAmazon CloudWatch.
2. Fare clicGruppi di log dioppure aprire il menu contestuale (tasto destro del mouse) e selezionareVisualizzazioneper aprireCloudWatch Esplora.

Note

La CloudWatch Log Groups Explorer si aprirà nella stessa posizione della finestra di Solutions Explorer.

Filtraggio

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

1. Da CloudWatch Esplora, imposta 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 Esplora viene aggiornato automaticamente per mostrare i risultati corrispondenti ai termini di ricerca specificati nel passaggio precedente.

Eliminazione di eventi di log

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

1. Da CloudWatch Esplora, fare clic con il pulsante destro del mouse sul Gruppo di log
2. Confermare che si desidera eliminare il Gruppo di log
3. Scegliere `Elimina` il gruppo di log selezionato, quindi aggiorna il CloudWatch Esplora.

Gruppi di log

Per aggiornare l'elenco corrente dei gruppi di log visualizzati nella CloudWatch Esplora, scegliere il `Refresh` pulsante situato nella barra degli strumenti.

Copia ARN gruppo log

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

1. Da CloudWatch Esplora, fare clic con il pulsante destro del mouse sul gruppo di log da cui si desidera copiare un
2. Seleziona `Copia ARN` opzione dal menu.
3. L'ARN è ora copiato negli appunti locali e pronto per essere incollato.

CloudWatch Flussi di log

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

Note

Durante la visualizzazione dei flussi di log, tenere presenti 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, attivando l'opzione **accento circonflesso** che si trova nelle intestazioni delle colonne.
- Le voci filtrate possono essere ordinate solo per **Nome flusso di log**.

Visualizzazione di log

1. Da **CloudWatch Esplora** fare doppio clic su **Streaming di log** dal menu contestuale.
2. Si aprirà una nuova scheda nella **documentofinestra**, che contiene un elenco di flussi di log associati al gruppo di log.

Filtraggio di log

1. Da **Flussi di log** scheda, nella **documentofinestra**, imposta il cursore nella barra di ricerca.
2. Inizia a digitare un prefisso relativo al flusso di log che stai cercando.
3. Durante la digitazione, il display corrente si aggiorna automaticamente per filtrare i Log Stream in base all'input.

Flussi di log

Per aggiornare l'elenco corrente dei flussi di log visualizzati nella **documentofinestra** scegliere l'icona di **aggiornamento** pulsante, che si trova nella **barra degli strumenti** accanto alla **barra di ricerca**.

Copia di ARN

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

1. Da **Flussi di log** scheda, nella **documentofinestra** fare clic con il pulsante destro del mouse sul flusso di log da cui si desidera copiare un ARN
2. Seleziona **Copia ARN** opzione dal menu.

3. L'ARN è ora copiato negli appunti locali e pronto per essere incollato.

Download di log

LaFlusso di log scarica e memorizza localmente il flusso di log selezionato, dove è possibile accedervi da strumenti e software personalizzati per un'ulteriore elaborazione.

1. DaFlussi di log scheda, nelladocumento, fare clic con il pulsante destro del mouse sul flusso di log da scaricare.
2. ScegliereFlusso di log per aprireEsportazione in un file di testofinestra di dialogo.
3. Scegli la posizione in cui desideri archiviare il file localmente e specifica un nome nel campo di testo fornito.
4. Conferma il download selezionandoOK. Lo stato del download viene visualizzato nellaCentro stato attività di Visual Studio

CloudWatch Eventi di log

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

Azioni di eventi di eventi

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

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

- Modalità testo a capo: È possibile attivare o disattivare il testo a capo facendo clic su un evento.
- Pulsante a capo automatico: situato nelladocument window **toolbar**, questo pulsante attiva e disattiva il testo a capo, 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 scegliCopy (Copia)(scelta rapida)Ctrl + C).

Visualizzazione dei eventi di log

1. Dadocumento, scegliere una scheda che contenga un elenco di flussi di log.

2. Fare doppio clic su un flusso di log o fare clic con il pulsante destro del mouse Streaming di log dal menu.
3. Un nuovo evento di log scheda si aprirà nella document window, che contiene una tabella di eventi di log associati al flusso di log scelto.

Filtraggio

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, iniziare filtrando i messaggi in base al contenuto o all'intervallo di tempo, quindi filtrare i risultati con l'altro metodo.

Per filtrare gli eventi del registro in base al contenuto:

1. Da eventi di log scheda, nella document window, imposta il cursore nella barra di ricerca, situata nella parte superiore della finestra.
2. Inizia a digitare un termine o una frase relativi agli eventi di registro che stai cercando.
3. Durante la digitazione, il display 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 [Sintassi di filtri e modelli](#) argomento in Amazonia CloudWatch guida.

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

1. Da eventi di log scheda, nella document window scegliere l'icona del calendario pulsante, che si trova nella barra degli strumenti.
2. Utilizzando i campi forniti, specificare l'intervallo di tempo che si desidera cercare.
3. I risultati filtrati si aggiornano automaticamente quando si specificano i vincoli di data e ora.

Note

La Clear Filter l'opzione cancella tutto il tuo attuale date-and-time selezioni di filtri.

Eventi di aggiornamento dei log

Per aggiornare l'elenco corrente degli eventi di registro visualizzati nella sezione di log scegliere il cono di aggiornamento pulsante, che si trova nella barra degli strumenti.

Accesso aggiuntivo a CloudWatch Log

Puoi accedere a CloudWatch Logs associated with other 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 CloudWatchTronchi. Lambda CloudWatch Log, vedere la <https://docs.aws.amazon.com/lambda/latest/dg/monitoring-cloudwatchlogs.html#monitoring-cloudwatchlogs-prereqs>

1. Da AWS Toolkit Explorer, espandi Lambda.
2. fare clic con il pulsante destro del mouse sulla funzione da visualizzare, poi scegliere Visualizzare i log per aprire i flussi di log associati nella finestra di documento.

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

1. Da AWS Toolkit Explorer, espandi Lambda.
2. fare clic con il pulsante destro del mouse sulla funzione da visualizzare, poi scegliere Funzione Viewer per aprire la visualizzazione delle funzioni nella finestra di documento.
3. Da function view passare alla Log, vengono visualizzati i flussi di log associati alla funzione Lambda scelta.

ECS

Per visualizzare le risorse di log associate a un contenitore di attività ECS, completare la procedura seguente.

Note

Affinché il servizio Amazon ECS possa inviare i log a CloudWatch, ogni contenitore per una determinata attività Amazon ECS deve soddisfare la configurazione richiesta. Per ulteriori informazioni sulla configurazione e le configurazioni richieste, consultare la guida [Utilizzo di AWS Driver di log](#).

1. Da **AWSToolkit Explorer**, espandi **Amazon ECS**.
2. Scegli il cluster Amazon ECS da visualizzare in **Cluster ECS scheda**, nell'adocumento finestra.
3. Dal menu di navigazione, situato sul lato sinistro **Cluster ECS** scegliere **Attività** per elencare tutte le attività associate al cluster.
4. Da **Attività** visualizzare, selezionare un'attività e scegliere **Visualizzare i log link**, che si trova nell'angolo in basso a sinistra.

Note

Questa visualizzazione elenca tutte le attività contenute nel cluster, **View Logs** è visibile solo per ogni attività che soddisfa la configurazione dei registri richiesta.

- Se un'attività è associata solo a un singolo contenitore, **Visualizzare i log link** apre il flusso di log di quel contenitore.
- Se un'attività è associata a più contenitori, **Visualizzare i log link** apre la visualizzazione **CloudWatch I log di attività di evento** finestra di dialogo, usa il **Container:** menu a discesa per scegliere il contenitore per cui si desidera visualizzare i registri, quindi scegliere **OK**.

5. Si apre una nuova scheda nell'adocumento finestra che mostra i flussi di log associati alla selezione del contenitore.

Gestione delle istanze Amazon EC2

AWSExplorer fornisce viste dettagliate delle istanze Amazon Machine Image (AMI) e Amazon Elastic Compute Cloud (Amazon EC2). Da queste visualizzazioni, è possibile avviare un'istanza Amazon EC2 da un'AMI, connettersi a tale istanza e interrompere o terminare l'istanza, il tutto dall'ambiente

di sviluppo di Visual Studio. È possibile utilizzare la vista istanze per creare AMI dalle istanze. Per ulteriori informazioni, consulta [Creazione di un'AMI da un'istanza Amazon EC2](#).

Le immagini di Amazon Machine e le visualizzazioni delle istanze Amazon EC2

Da AWS Explorer, puoi visualizzare le visualizzazioni delle istanze Amazon Machine Image (AMI) e Amazon EC2. Nello stato AWS Explorer, espandi Amazon EC2 nodo.

Per visualizzare la vista AMI, sul primo sottonodo, AMI, aprire il menu contestuale (pulsante destro del mouse) e quindi selezionare Visualizzazione.

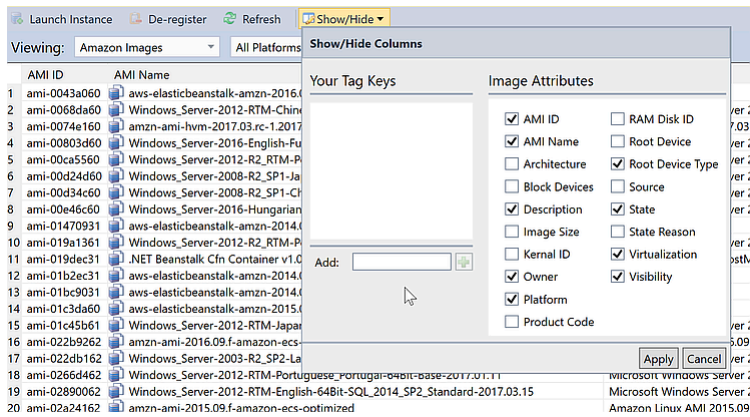
Per visualizzare la vista delle istanze Amazon EC2, sull'istanzenodo, aprire il menu contestuale (pulsante destro del mouse) e quindi selezionare Visualizzazione.

È inoltre possibile visualizzare entrambe le viste facendo doppio clic sul nodo appropriato.

- Le viste vengono assegnate alla regione specificata in AWS Explorer (ad esempio, la regione Stati Uniti occidentali (California settentrionale)).
- È possibile riorganizzare le colonne facendo clic e trascinando. Per ordinare i valori in una colonna, fare clic sull'intestazione della colonna.
- È possibile utilizzare gli elenchi a discesa e la casella di filtro in Visualizzazione per configurare le viste. La vista iniziale visualizza AMI di qualsiasi tipo di piattaforma (Windows o Linux) di proprietà dell'account specificato in AWS Explorer.

Show/Hide colonne

È possibile anche scegliere l'opzione Show/Hide menu a discesa nella parte superiore della vista per configurare quali colonne vengono visualizzate. La scelta delle colonne persisterà se chiudi la vista e la riapri.



Show/Hide colonne Interfaccia utente per viste AMI e istanze

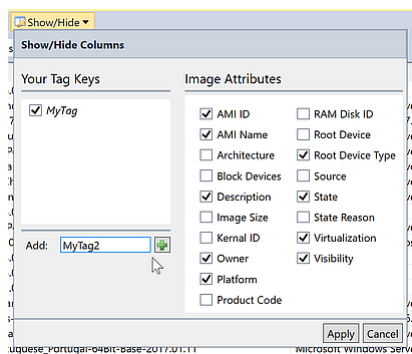
Tagging di AMI, istanze e volumi

È possibile utilizzare anche l'opzione Show/Hide elenco a discesa per aggiungere tag per AMI, istanze Amazon EC2 o volumi di tua proprietà. I tag sono coppie nome-valore che ti consentono di collegare metadati alle AMI, istanze e volumi. I nomi dei tag sono assegnati sia al tuo account sia separatamente alle AMI e alle istanze. Ad esempio, non ci sarebbero conflitti se utilizzassi lo stesso nome di tag per le AMI e le istanze. I nomi dei tag non distinguono tra maiuscole e min

Per ulteriori informazioni sui tag, vai a [Uso dei tag](#) nella Guida per l'utente di Amazon EC2 User Guide per le istanze Linux.

Per aggiungere un tag

1. Nella casella di input, digita un nome per l'etichetta. Scegli il pulsante verde con il segno più (+), quindi scegli **Applica**.



Aggiungere un tag a un'istanza AMI o Amazon EC2

Il nuovo tag viene visualizzato in corsivo, il che indica che non sono ancora stati associati valori a quel tag.

Nella vista elenco, il nome del tag viene visualizzato come una nuova colonna. Quando è stato associato almeno un valore al tag, il tag sarà visibile nella [AWS Management Console](#).

2. Per aggiungere un valore per il tag, fare doppio clic su una cella nella colonna del tag e digitare un valore. Per eliminare il valore del tag, fare doppio clic sulla cella ed eliminare il testo.

Se si cancella il tag nel Show/Hide elenco a discesa, la colonna corrispondente scompare dalla vista. Il tag viene conservato insieme a tutti i valori di tag associati a AMI, istanze o volumi.

Note

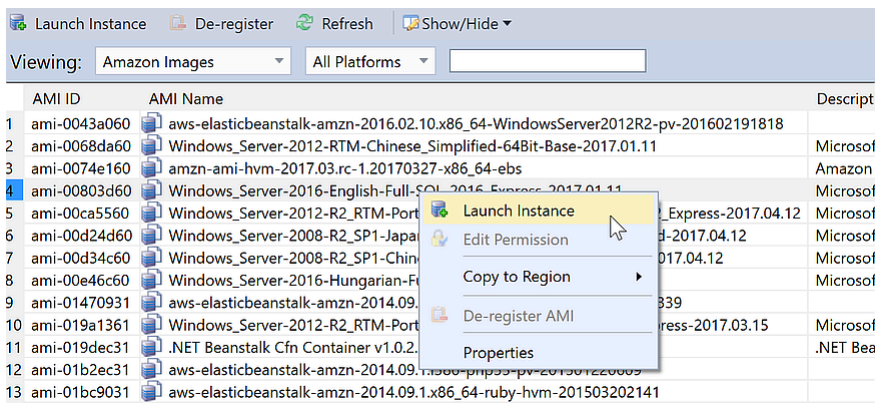
Se si cancella un tag nel Show/Hide elenco a discesa che non ha valori associati, AWSToolkit eliminerà completamente il tag. Non verrà più visualizzato nella visualizzazione elenco o nella Show/Hide (Provenienza chiamata). Per utilizzare di nuovo quel tag, usa il Show/Hide finestra di dialogo per ricrearla.

Avvio di un'istanza Amazon EC2

AWSExplorer 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 di Windows Server

1. Nella parte superiore della vista AMI, nell'elenco a discesa a sinistra, scegli Amazon Image. Nell'elenco a discesa a destra, seleziona finestre. Nella casella del filtro, digita ebs per la conservazione di blocchi elastici. Potrebbero trascorrere alcuni minuti prima che la vista venga rinfrescata.
2. Scegli un'AMI nell'elenco, apri il menu contestuale (pulsante destro del mouse) e quindi scegli Avvia istanza. .



Elenco AMI

- Nella Avvio della nuova istanza di Amazon EC2 finestra di dialogo, configura l'AMI per la tua applicazione.

Tipi di istanza

Scegliere 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 essere più lungo di 256 caratteri.

Coppia di chiavi

Una key pair viene utilizzata per ottenere la password Windows utilizzata per effettuare l'accesso all'istanza EC2 utilizzando Remote Desktop Protocol (RDP). Scegli una key pair per la quale hai accesso alla chiave privata o scegli l'opzione per creare una key pair. Se crei la key pair nel Toolkit, il Toolkit può memorizzare la chiave privata per te.

Le coppie di chiavi memorizzate nel Toolkit sono crittografate. Puoi trovarle all'indirizzo `%LOCALAPPDATA%\AWSToolkit\keypairs` (tipicamente: `C:\Users\\AppData\Local\AWSToolkit\keypairs`). È possibile esportare la key pair crittografate in un .pemfile.

- In Visual Studio, selezionare Visualizzazione e clicca su AWS Esploratore.
- Fare clic su Amazon EC2 e selezionare Coppie di chiavi.
- Le coppie di chiavi saranno elencate e quelle create o gestite dal Toolkit contrassegnate come Archiviato in AWS Toolkit.

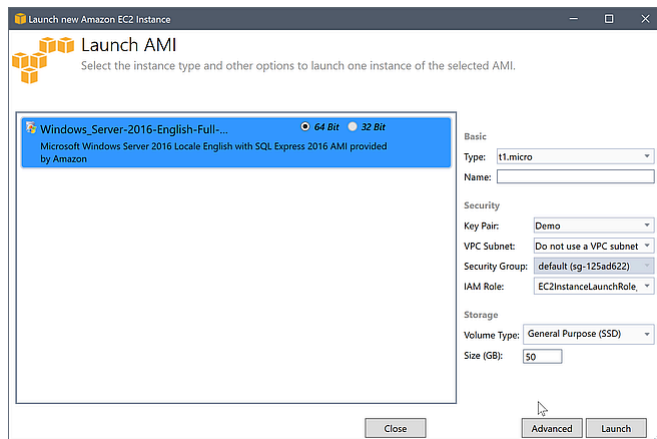
- d. Fai clic con il pulsante destro del mouse sulla key pair creata e seleziona **Esportazione di chiave privata**. La chiave privata non verrà crittografata e memorizzata nella posizione specificata.

Gruppo di sicurezza

Il gruppo di sicurezza controlla il tipo di traffico di rete che l'istanza EC2 accetterà. Scegliere un gruppo di sicurezza che consentirà il traffico in entrata sulla porta 3389, la porta utilizzata da RDP, in modo da connettersi all'istanza EC2. Per informazioni su come utilizzare il Toolkit per creare gruppi di sicurezza, consultare [Gestione dei gruppi di sicurezza da AWS Explorer](#).

Profilo dell'istanza

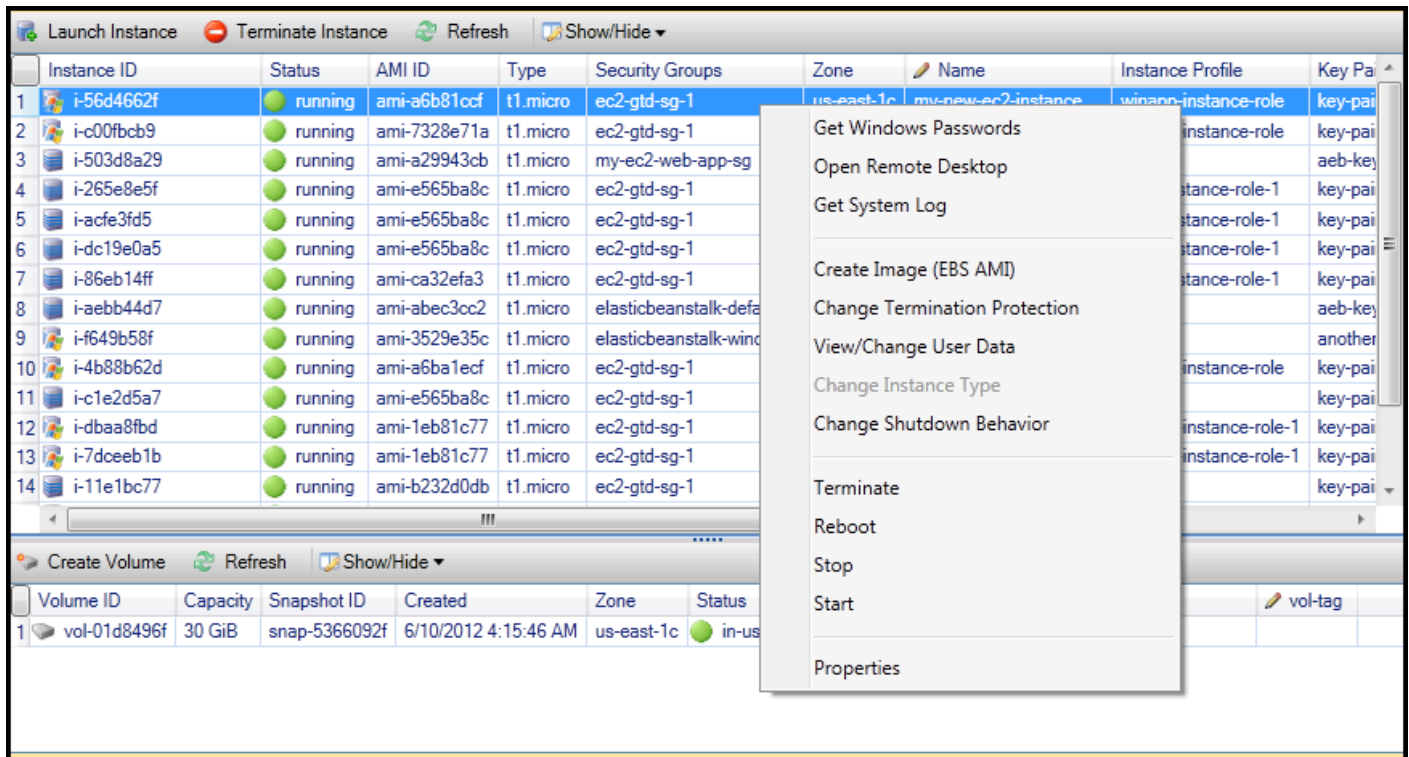
Il profilo dell'istanza è un container logico per un ruolo IAM. Quando selezioni un profilo dell'istanza, associ il ruolo IAM corrispondente all'istanza EC2. I ruoli IAM sono configurati con policy che specificano l'accesso ad Amazon Web Services e alle risorse dell'account. Quando un'istanza EC2 è associata a un ruolo IAM, il software dell'applicazione eseguito sull'istanza viene eseguito con le autorizzazioni specificate dal ruolo IAM. In questo modo il software dell'applicazione viene eseguito senza dover specificare nessuna AWS credenziali proprie, il che lo rende più sicuro. Per ulteriori informazioni sui ruoli IAM, vai a [IAM User Guide](#).



EC2 Avvia AMI finestra di dialogo

4. Scegliere Launch (Avvia).

Nello stato **AWS Explorer**, sull'istanza **sotto** nodo di **Amazon EC2**, aprire il menu contestuale (pulsante destro del mouse) e quindi selezionare **Visualizzazione**. La **AWS Toolkit** visualizza l'elenco delle istanze Amazon EC2 associate all'account attivo. Potrebbe essere necessario scegliere **Aggiorna** per visualizzare la nuova istanza. Quando viene visualizzata per la prima volta l'istanza, potrebbe essere in sospeso, ma dopo alcuni istanti passa a uno stato di esecuzione.



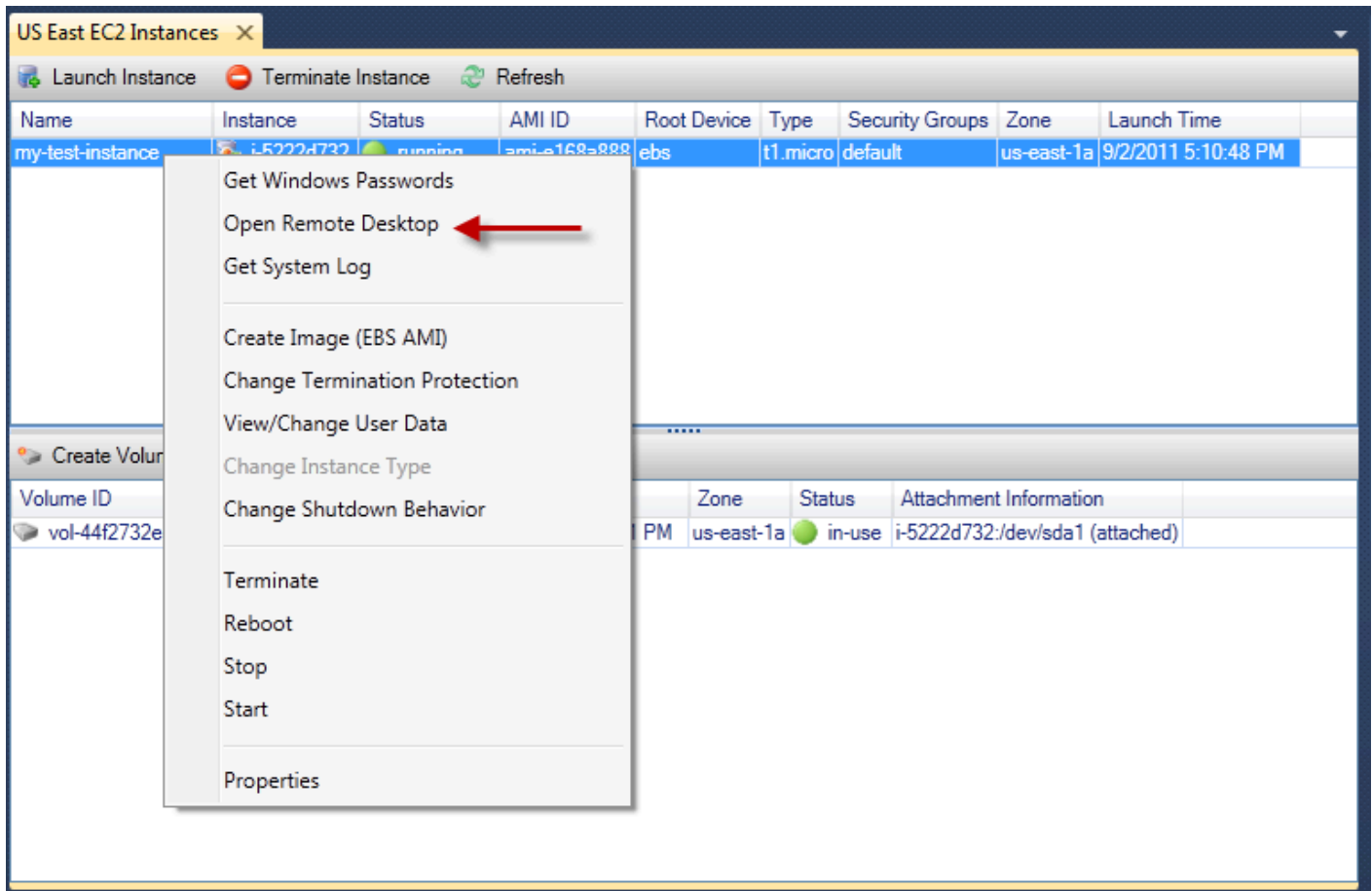
Connessione a un'istanza Amazon EC2

È possibile utilizzare Windows Remote Desktop per connettersi a un'istanza Windows Server. Per l'autenticazione, ilAWSToolkit consente di recuperare la password di amministratore per l'istanza oppure è possibile utilizzare semplicemente la key pair memorizzate associata all'istanza. Nella procedura seguente, useremo la key pair memorizzate.

Per connettersi a un'istanza Windows Server tramite Desktop remoto Windows

1. Nell'elenco delle istanze EC2 fare clic con il pulsante destro del mouse sull'istanza Windows Server alla quale si desidera connettersi. Nel menu contestuale, selezionareApri Desktop remoto.

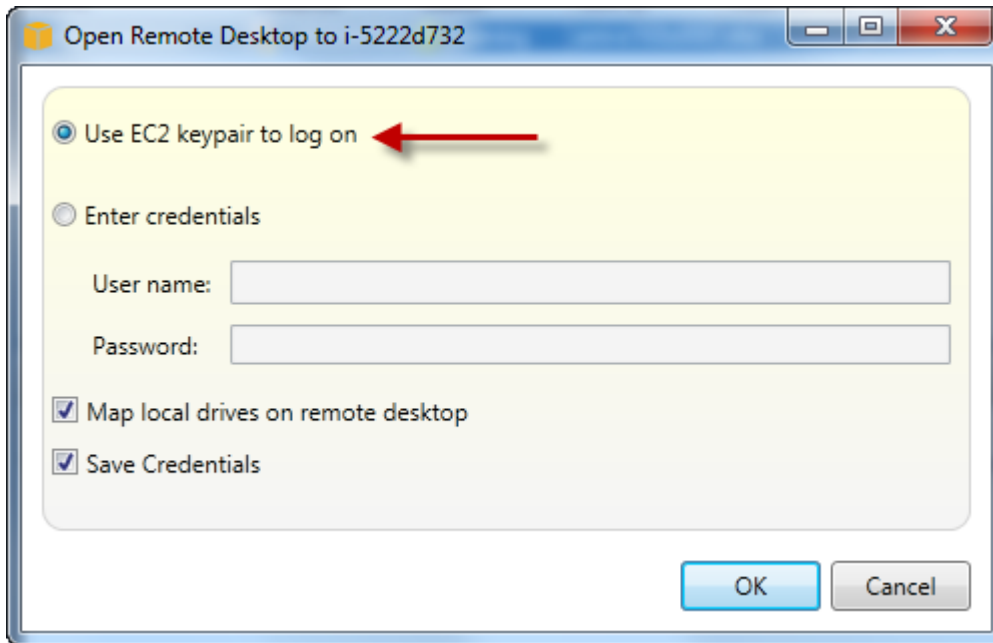
Se si desidera autenticare utilizzando la password dell'amministratore, scegliereOttieni password Windows.



Menu contestuale istanza EC2

2. Nella finestra di dialogo Desktop remoto, selezionare la coppia di chiavi EC2 per accedere quindi scegliere OK.

Se non hai memorizzato una key pair con AWS Toolkit, specificare il file PEM contenente la chiave privata.

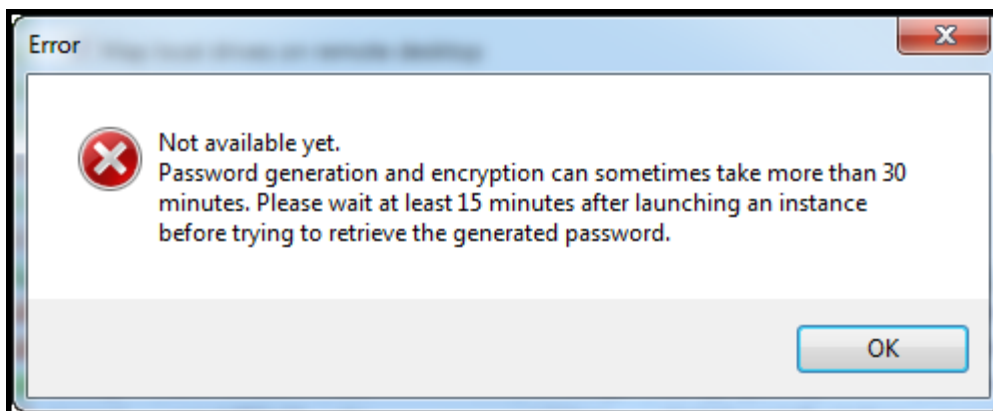


Apri Desktop remotofinestra di dialogo

3. LaRemote Desktop (Desktop remoto)si aprirà la finestra. Non è necessario accedere perché si è verificata l'autenticazione con la key pair. È possibile eseguire come amministratore sull'istanza Amazon EC2.

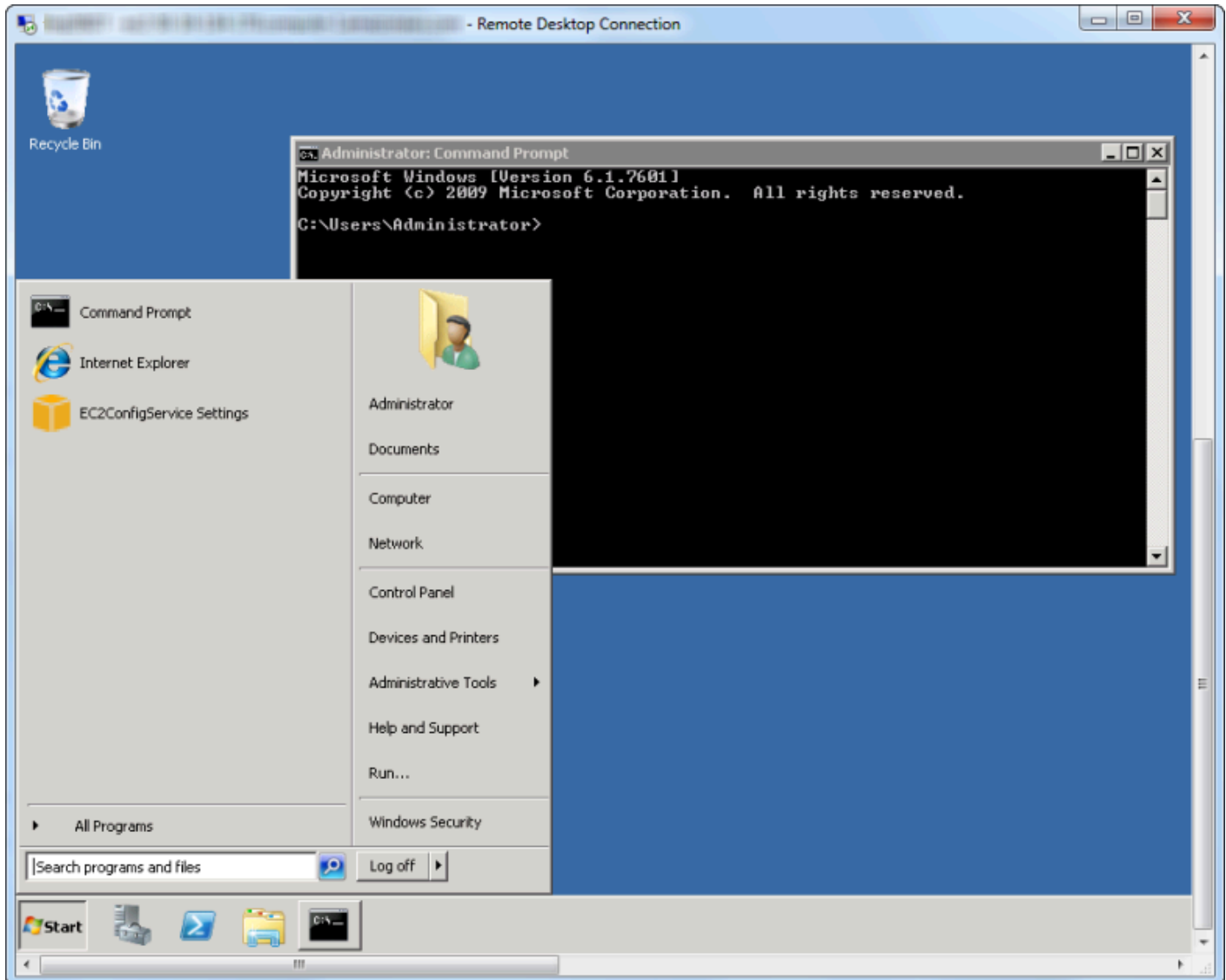
Se l'istanza EC2 è stata avviata solo di recente, potrebbe non essere possibile connettersi per due possibili motivi:

- Il servizio Desktop remoto 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

Lo screenshot seguente mostra un utente connesso come amministratore tramite Desktop remoto.



Remote Desktop (Desktop remoto)

Terminazione di un'istanza Amazon EC2

Utilizzo di AWSToolkit, puoi arrestare o terminare un'istanza Amazon EC2 in esecuzione da Visual Studio. Per arrestare 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.

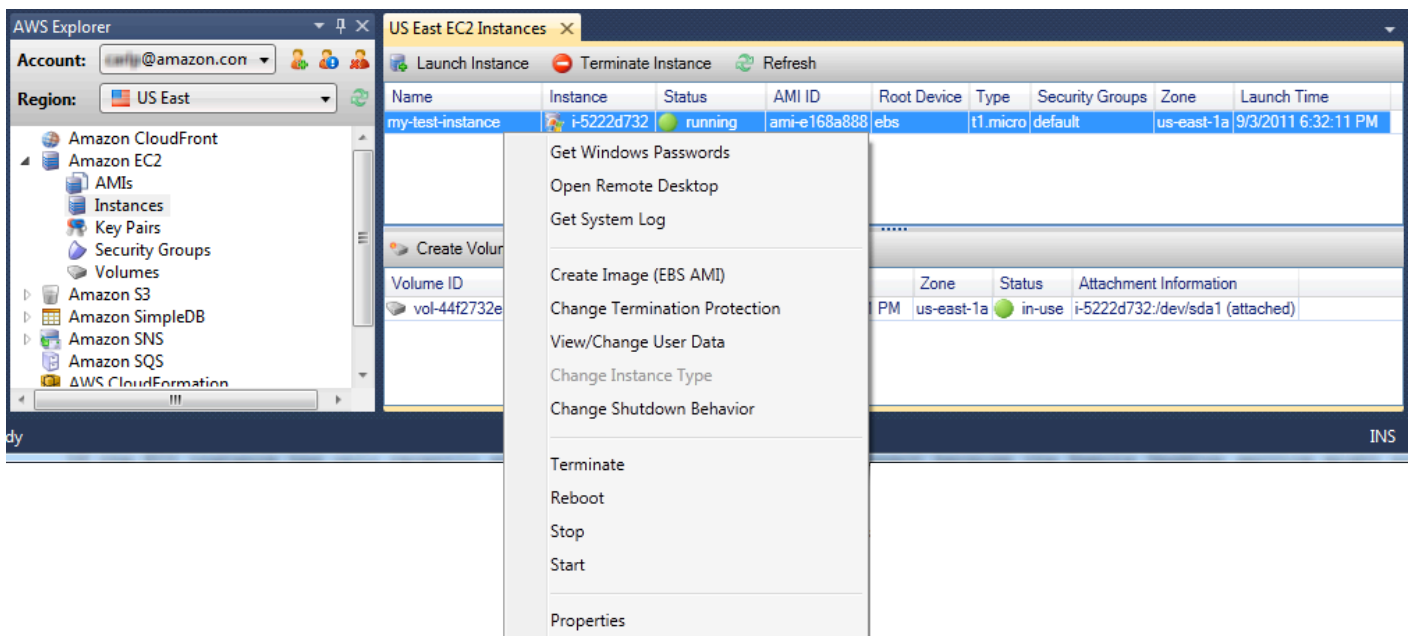
Se si arresta l'istanza, i dati memorizzati sul volume EBS vengono conservati. Se si interrompe l'istanza, tutti i dati memorizzati sul dispositivo di archiviazione locale dell'istanza andranno persi. In

entrambi i casi, interrompi o interrompi, non verrà addebitato l'addebito per l'istanza EC2. Tuttavia, se si interrompe un'istanza, continuerai a essere addebitato per lo storage EBS che persiste dopo l'arresto dell'istanza.

Un altro modo possibile per terminare un'istanza è utilizzare Desktop remoto per connettersi all'istanza e quindi da Windows Avvio del menu, utilizzare Arresto. È possibile configurare l'istanza in modo che venga interrotta o terminata in questo scenario.

Per arrestare un'istanza Amazon EC2

1. Nello stato AWSExplorer, espandi Amazon EC2 Nodo, aprire il menu di scelta rapida (destra del mouse) per l'istanza quindi scegliere Visualizzazione. Nella l'istanza elista, fai clic con il pulsante destro del mouse sull'istanza che desideri interrompere e scegli Arresto del menu contestuale. Scegli Res per confermare che si desidera interrompere l'istanza.



2. Nella parte superiore della barra degli strumenti l'istanza elista, scegli Aggiorna per visualizzare la modifica dello stato dell'istanza Amazon EC2. Poiché abbiamo interrotto anziché terminare l'istanza, il volume EBS associato all'istanza è ancora attivo.

The screenshot shows the 'US East EC2 Instances' window. At the top, there are buttons for 'Launch Instance', 'Terminate Instance', and 'Refresh'. The 'Refresh' button is circled in red. Below the buttons is a table of EC2 instances:

Name	Instance	Status	AMI ID	Root Device	Type	Security Groups	Zone	Launch Time
my-test-instance	i-5222d732	stopped	ami-e168a888	ebs	t1.micro	default	us-east-1a	9/3/2011 6:32:11 PM

Below the instances table, there is a 'Create Volume' button and another 'Refresh' button. Below that is a table of volumes:

Volume ID	Name	Capacity	Snapshot	Created	Zone	Status	Attachment Information
vol-44f2732e		35 GiB	snap-76109e16	9/2/2011 5:10:51 PM	us-east-1a	in-use	i-5222d732:/dev/sda1 (attached)

Le istanze terminate rimangono visibili

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

The screenshot shows the 'US East EC2 Instances' window. At the top, there are buttons for 'Launch Instance', 'Terminate Instance', and 'Refresh'. The 'Refresh' button is circled in green. Below the buttons is a table of EC2 instances:

Name	Instance	Status	AMI ID	Root Device	Type	Security Groups	Zone	Launch Time
my-other-win-instance	i-9bbea2fa	terminated	ami-0a8a7863	ebs	t1.micro	default	us-east-1a	8/29/2011 4:56:58 PM
my-test-instance	i-5222d732	running	ami-e168a888	ebs	t1.micro	default	us-east-1a	9/2/2011 5:10:48 PM

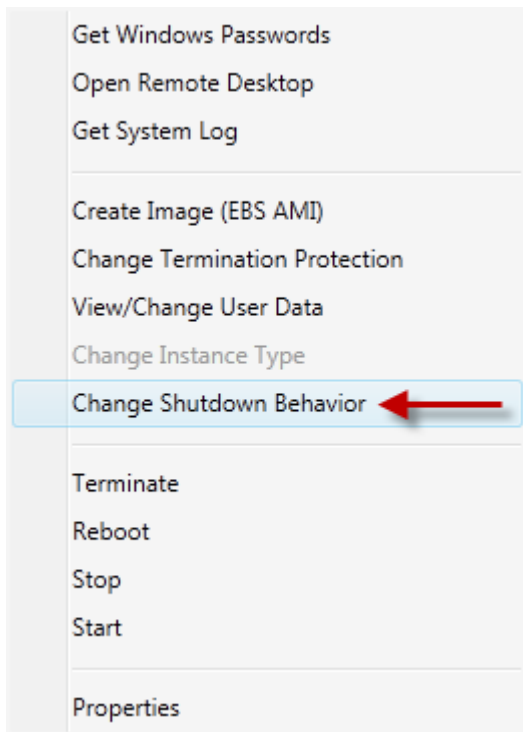
Below the instances table, there is a 'Create Volume' button and another 'Refresh' button. Below that is a table of volumes:

Volume ID	Name	Capacity	Snapshot	Created	Zone	Status	Attachment Information
vol-44f2732e		35 GiB	snap-76109e16	9/2/2011 5:10:51 PM	us-east-1a	in-use	i-5222d732:/dev/sda1 (attached)

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

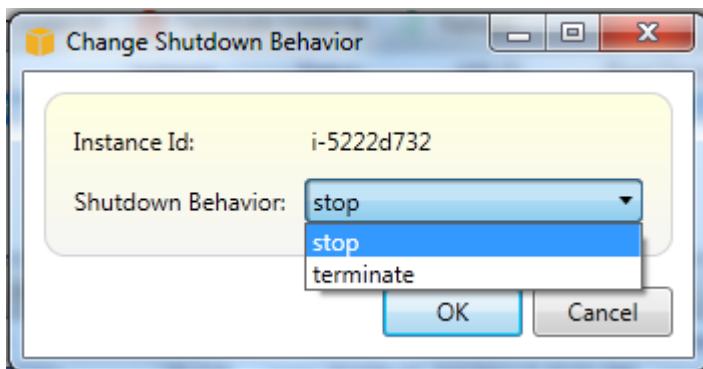
La AWS Toolkit ti consente di specificare se un'istanza Amazon EC2 verrà interrotta o terminata se l'arresto è selezionato dal menu di avvio.

1. Nella **istanze** elencare, fare clic con il pulsante destro del mouse su un'istanza Amazon EC2 e **Modifica del comportamento di arresto**.



Modifica del comportamento di arresto voce di menu

2. Nella **Modifica del comportamento di arresto** finestra di dialogo, dal **Comportamento di arresto** (Proseguenza chiamata) **Arresto delle** **Interruzione**.



Gestione delle istanze Amazon ECS

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

Modifica delle proprietà del servizio

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

1. Nello stato **AWSExplorer (Explorer)**, aprire il menu contestuale (pulsante destro del mouse) per la gestione del cluster, quindi scegliere **Visualizzazione**.
2. Nella vista **Cluster ECS**, fare clic su **Servizi** sinistra, quindi fare clic su **Dettagli scheda** nella vista dei dettagli. È possibile fare clic su **Eventi** per vedere i messaggi degli eventi e **Distribuzione** allo stato della distribuzione.
3. Fare clic su **Edit (Modifica)**. È possibile modificare il conteggio delle attività desiderato e la percentuale minima e massima di integrità.
4. Fare clic su **Save (Salva)** per accettare modifiche o **Annulla** per tornare ai valori esistenti.

Interruzione di un'attività

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

Per interrompere un'attività

1. Nello stato **AWSExplorer (Esplora)**, aprire il menu contestuale (pulsante destro del mouse) per il cluster con attività che si desidera interrompere, quindi scegliere **Visualizzazione**.
2. Nella vista **Cluster ECS**, fare clic su **Attività** sinistra.
3. Assicurarsi che **Stato** dell'attività desiderata è impostato su **.Running**. Scegli le singole attività da interrompere e fai clic su **Arresto delle** oppure fai clic su **Arrestare tutto** per selezionare e interrompere tutte le attività in esecuzione.
4. Nella **Interrompi attività** finestra di dialogo, selezionare **sì**.

Eliminazione di un servizio

È possibile eliminare i servizi da un cluster dalla vista cluster.

Per eliminare un servizio cluster

1. Nello stato **AWSExplorer (Explorer)**, aprire il menu contestuale (pulsante destro del mouse) per il cluster con un servizio che si desidera eliminare, quindi scegliere **Visualizzazione**.

2. Nella vista Cluster ECS, fare clic su **Servizi** sinistra, quindi fare clic su **Elimina**.
3. Nella **Per eliminare cluster** finestra di dialogo, se nel cluster sono presenti un bilanciamento del carico e un gruppo di destinazione, è possibile scegliere di eliminarli con il cluster. Non verranno utilizzati quando il servizio viene eliminato.
4. Nella **Per eliminare cluster** finestra di dialogo, selezionare **OK**. Quando il cluster viene eliminato, verrà rimosso dal **AWSExplorer**.

Eliminazione di un cluster

Puoi eliminare un cluster Amazon Elastic Container Service **AWSExplorer**.

Per eliminare un cluster

1. Nello stato **AWSExplorer (Explorer)**, aprire il menu contestuale (pulsante destro del mouse) per il cluster che si desidera eliminare sotto **Cluster** nodo di **Amazon ECS** e quindi scegliere **Elimina**.
2. Nella **Per eliminare cluster** finestra di dialogo, selezionare **OK**. Quando il cluster viene eliminato, verrà rimosso dal **AWSExplorer**.

Creazione di un repository

È possibile creare un repository Amazon Elastic Container Registry da **AWSExplorer**.

Per creare un repository

1. Nello stato **AWSExplorer (Explorer)**, aprire il menu contestuale (pulsante destro del mouse) della **Repositories** nodo sotto **Amazon ECS** e quindi scegliere **Crea repository**.
2. Nella **Crea repository** finestra di dialogo, fornire un nome del repository e quindi scegliere **OK**.

Eliminazione di un repository

Puoi eliminare un repository Amazon Elastic Container Registry da **AWSExplorer**.

Per eliminare un repository

1. Nello stato **AWSExplorer (Explorer)**, aprire il menu contestuale (pulsante destro del mouse) della **Repositories** nodo sotto **Amazon ECS** e quindi scegliere **Eliminazione del repository**.

2. Nella Eliminazione del repository finestra di dialogo, è possibile scegliere di eliminare il repository anche se contiene immagini. In caso contrario, verrà eliminato solo se è vuoto. Fare clic su Sì.

Gestione di gruppi di sicurezza da AWSEsploratore

Toolkit for Visual Studio consente di creare e configurare gruppi di sicurezza da utilizzare con le istanze Amazon Elastic Compute Cloud (Amazon EC2) e AWS CloudFormation. Quando si avviano le istanze Amazon EC2 o si distribuisce un'applicazione su AWS CloudFormation, si specifica un gruppo di sicurezza da associare alle istanze Amazon EC2. (Distribuzione su AWS CloudFormation crea istanze Amazon EC2.)

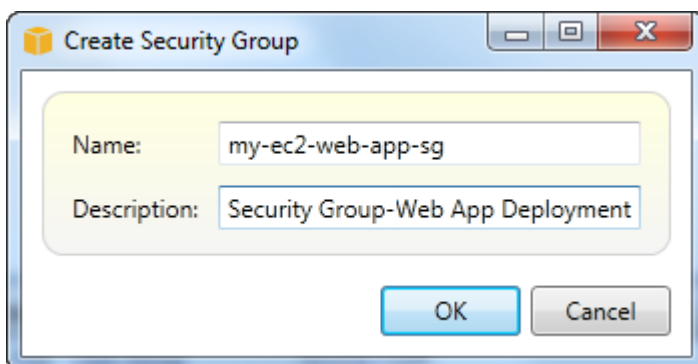
Un gruppo di sicurezza agisce come un firewall sul traffico di rete in entrata. Il gruppo di sicurezza specifica quali tipi di traffico di rete sono consentiti su un'istanza Amazon EC2. È inoltre possibile specificare che il traffico in entrata venga accettato solo da determinati indirizzi IP o solo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

Creazione di un gruppo di sicurezza

In questa sezione, verrà creato un gruppo di sicurezza. Una volta creato, il gruppo di sicurezza non dispone di autorizzazioni configurate. La configurazione delle autorizzazioni viene gestita attraverso un'ulteriore operazione.

Per creare un gruppo di sicurezza

1. Nello stato AWSExplorer, sotto il Amazon EC2, aprire il menu contestuale (pulsante destro del mouse) nella Security Groups (Gruppi di sicurezza) nodo, quindi scegliere Visualizzazione.
2. Sul Gruppo di sicurezza EC2 tab, scegli Creazione di gruppi di sicurezza.
3. Nella Creazione di gruppi di sicurezza, digitare un nome e una descrizione per il gruppo di sicurezza, quindi scegliere OK.

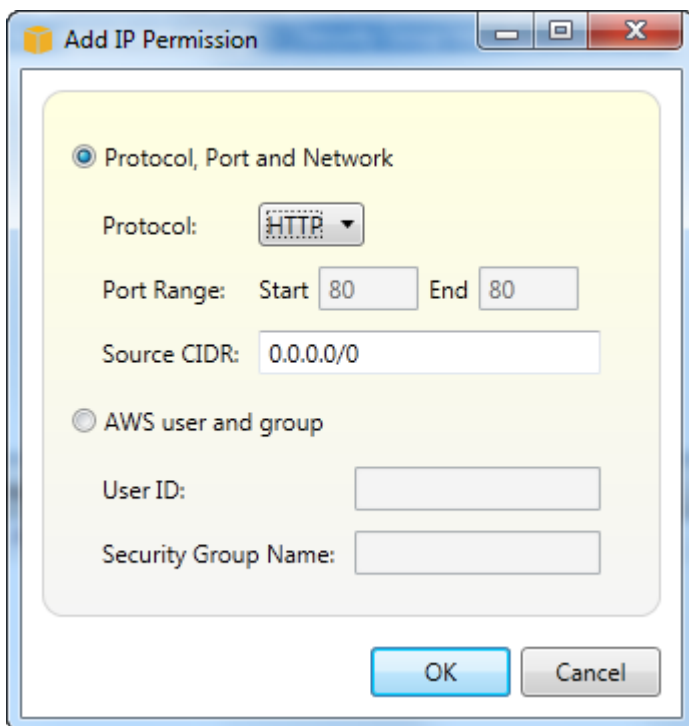


Aggiunta di autorizzazioni ai gruppi di sicurezza

In questa sezione, verranno aggiunte le autorizzazioni per il gruppo di sicurezza per consentire il traffico Web tramite i protocolli HTTP e HTTPS. Consentiranno inoltre ad altri computer di connettersi utilizzando Windows Remote Desktop Protocol (RDP).

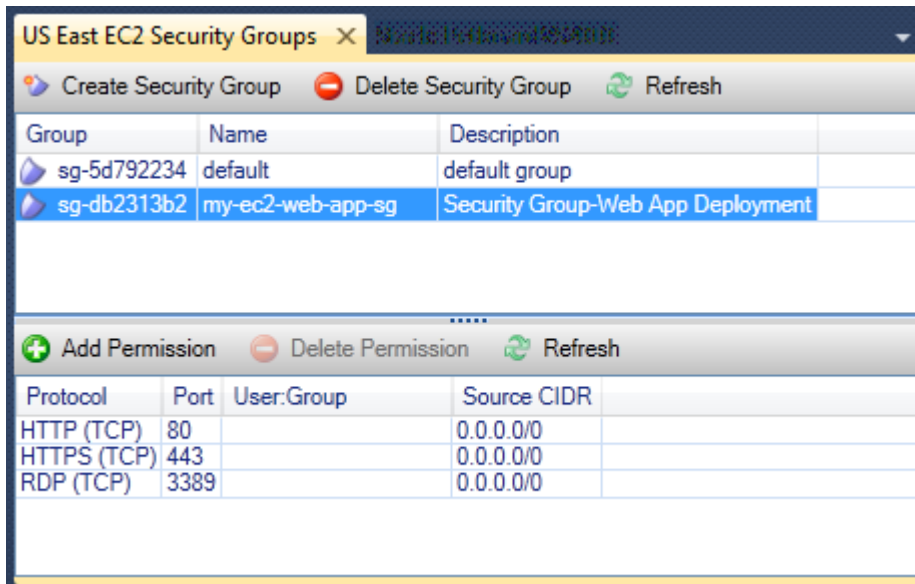
Per aggiungere un'autorizzazione a un gruppo di sicurezza

1. Sul Gruppo di sicurezza EC2, scegli un gruppo di sicurezza e scegli ilaggiungi autorizzazioneepulsante.
2. Nellaaggiungi autorizzazione IPfinestra di dialogo, scegli ilProtocollo, porta e retepulsante di opzione e quindi dalProtocollo(Provenienza chiamata)HTTP. L'intervallo di porte si adatta automaticamente alla porta 80, la porta predefinita per HTTP. LaCIDR di fontell campo viene impostato su 0.0.0.0/0, ovvero viene specificato che il traffico di rete HTTP verrà accettato da qualsiasi indirizzo IP esterno. Scegli OK.



Porta aperta 80 (HTTP) per questo gruppo di sicurezza

3. Ripetere questo processo per HTTPS e RDP. Le autorizzazioni per i gruppi di sicurezza saranno ora simili alle seguenti.



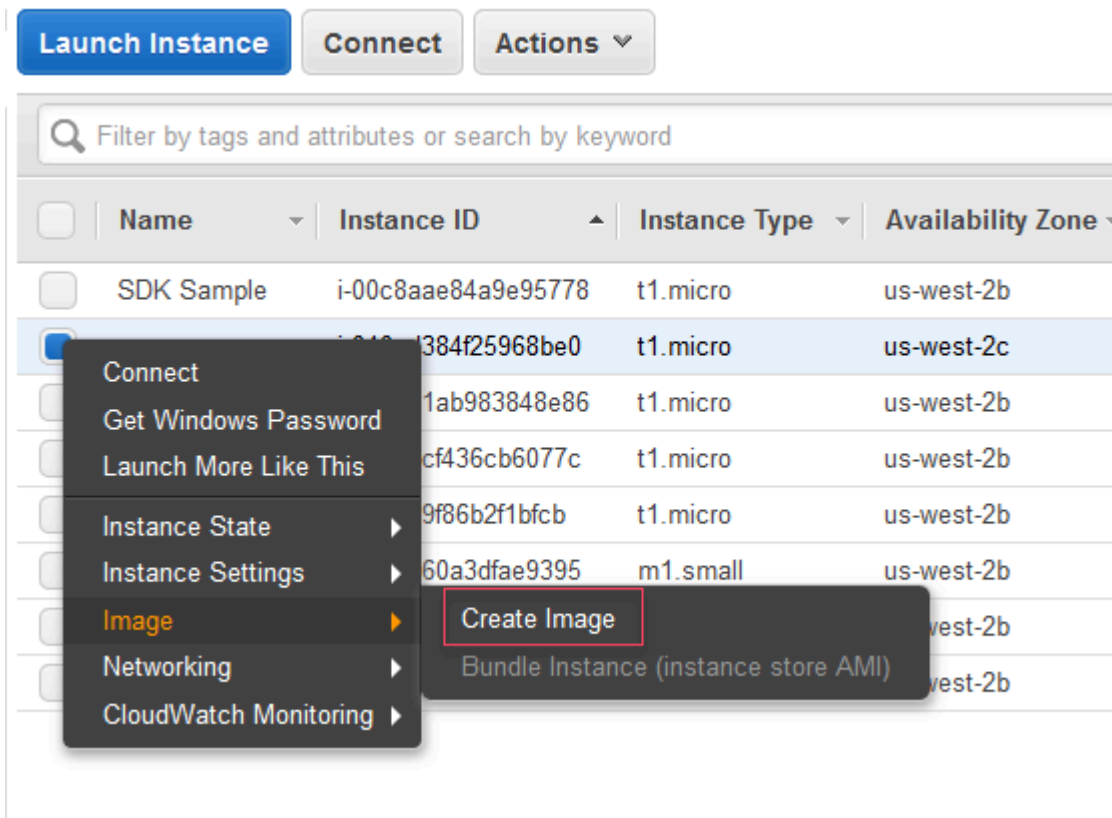
È inoltre possibile impostare le autorizzazioni nel gruppo di sicurezza specificando un ID utente e un nome del gruppo di sicurezza. In questo caso, le istanze Amazon EC2 in questo gruppo di sicurezza accetteranno tutto il traffico di rete in entrata dalle istanze Amazon EC2 nel gruppo di sicurezza specificato. È inoltre necessario specificare l'ID utente come un modo per disambiguare il nome del gruppo di sicurezza; i nomi dei gruppi di sicurezza non devono essere univoci in tutti iAWS. Per ulteriori informazioni sui gruppi di sicurezza, consulta la [Documentazione EC2](#).

Creazione AMI un'istanza Amazon EC2

Dalla vista delle istanze di Amazon EC2, puoi creare Amazon Machine Images (AMI) da istanze in esecuzione o interrotte. Per informazioni più dettagliate sulle istanze Windows, consulta l'argomento [Accettatore Grafica elastica \(AMI\)](#) nella Guida per l'utente di Amazon Elastic Compute Cloud per le istanze Windows.

Creazione AMI un'istanza

1. Fate clic con il pulsante destro del mouse sull'istanza che desiderate utilizzare come base per l'AMI e scegliete Crea immagine dal menu contestuale.



Menu contestuale Crea immagine

2. Nella finestra di dialogo Crea immagine, digitate un nome e una descrizione univoci, quindi scegliete Crea immagine. Per impostazione predefinita, Amazon EC2 arresta l'istanza, acquisisce delle snapshot dei volumi collegati, crea e registra l'AMI e riavvia l'istanza. Scegli Nessun riavvio se non desideri che l'istanza venga chiusa.

Warning

Se si sceglie l'opzione No reboot (Non riavviare), non possiamo garantire l'integrità del file system dell'immagine creata.

Create Image
✕

Instance ID ⓘ i-008549029f860b9b0

Image name ⓘ

Image description ⓘ

No reboot ⓘ

Instance Volumes

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encrypted ⓘ
Root	/dev/xvda	snap-066b5016ee2261563	8	General Purpose SSD (GP2) ▾	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Total size of EBS Volumes: 8 GiB
When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.

Finestra di dialogo Crea immagine

Potrebbero essere necessari alcuni minuti per creare l'AMI. Una volta creato, verrà visualizzato nella vista AMI in AWS Explorer. Per visualizzare questa vista, fai doppio clic sul nodo Amazon EC2 | AMI in AWS Explorer. Per visualizzare le tue AMI, dall'elenco a discesa Visualizzazione, scegli Posseduta da me. Potrebbe essere necessario scegliere Aggiorna per visualizzare l'AMI. Quando l'AMI appare per la prima volta, può essere in sospeso, ma dopo alcuni istanti passa a uno stato disponibile.

Owned by me ▾							
Filter by tags and attributes or search by keyword							
Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date
<input checked="" type="checkbox"/>	atw-linux-2	ami-d18412b1			Private	available	April 4, 2017 at 9:39:06 AM ...

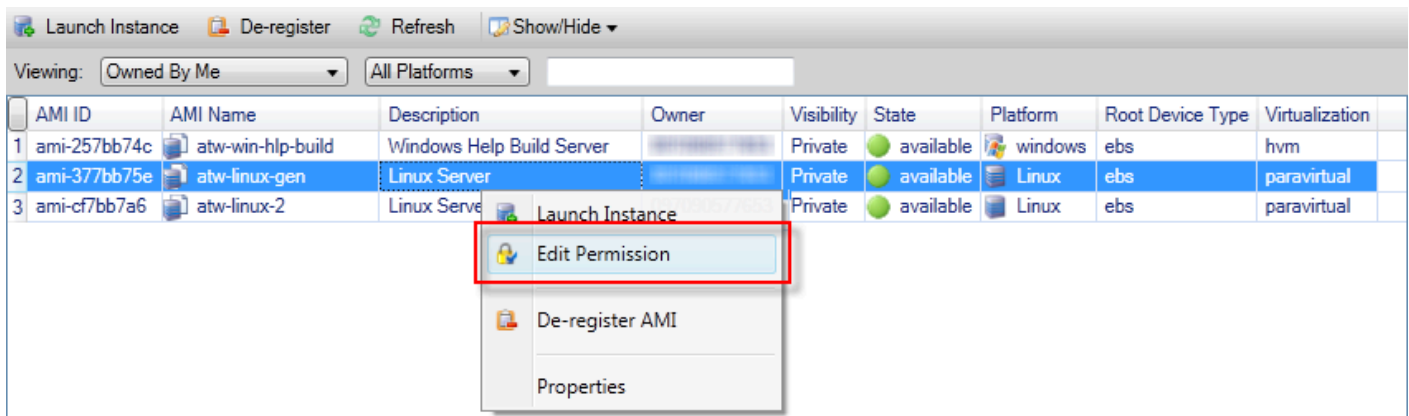
Elenco delle AMI create

Impostazione delle autorizzazioni di avvio per un'Amazon Machine Image

Puoi impostare le autorizzazioni di avvio per le Amazon Machine Images (AMI) dalla visualizzazione in AWS Explorer. Puoi utilizzare il plugin Impostazione delle autorizzazioni AMI finestra di dialogo per copiare le autorizzazioni dalle AMI.

Per impostare le autorizzazioni per un'AMI

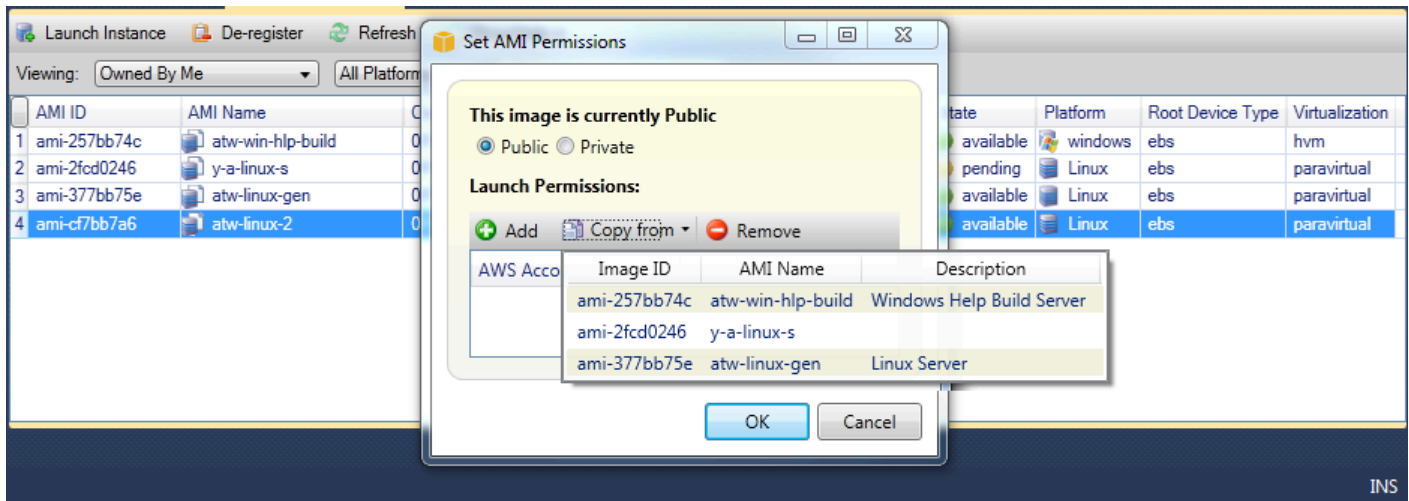
1. Nella AMI visualizzazione in AWSExplorer, aprire il menu contestuale (clic con il pulsante destro del mouse) in un'AMI (AMI), quindi scegliere Modifica delle autorizzazioni.



2. Sono disponibili tre opzioni nell'impostazione delle autorizzazioni AMI finestra di dialogo:

- Per dare il permesso di lancio, scegli Inserisci e digita il numero di conto per il AWS utente a cui stai dando il permesso di lancio.
- Per rimuovere l'autorizzazione di avvio, scegli il numero di account per il AWS utente da cui si sta rimuovendo l'autorizzazione di avvio e scegli Remove.
- Per copiare le autorizzazioni da un'AMI a un'altra, scegli un'AMI dall'elenco e scegli COPY da. Gli utenti che dispongono delle autorizzazioni di lancio sull'AMI che hai scelto riceveranno le autorizzazioni di lancio sull'AMI corrente. È possibile ripetere questo processo con altre AMI nell'elenco per copiare le autorizzazioni da più AMI nell'AMI di destinazione.

La COPY da elenco contiene solo le AMI di proprietà dell'account che era attivo quando l'AMI vista è stata visualizzata da AWSExplorer. Di conseguenza, il COPY da elenco potrebbe non visualizzare alcuna AMI se nessun'altra AMI è di proprietà dell'account attivo.



COPY delle autorizzazioni AMI finestra di dialogo

Amazon Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (Amazon VPC) consente di avviare risorse di Amazon Web Services in una rete virtuale personalizzata. Questa rete virtuale è simile a una normale 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 [AWS Management Console](#) ma dall'ambiente di sviluppo di Visual Studio. La Amazon VPC nodo di AWSExplorer include i sottonodi per le seguenti aree.

- [VPC](#)
- [Sottoreti](#)
- [IP elastici](#)
- [Internet Gateway](#)
- [liste di controllo accessi di rete](#)
- [Tabelle di routing](#)
- [Gruppi di sicurezza](#)

Creazione di un VPC pubblico-privato per la distribuzione con AWS Elastic Beanstalk

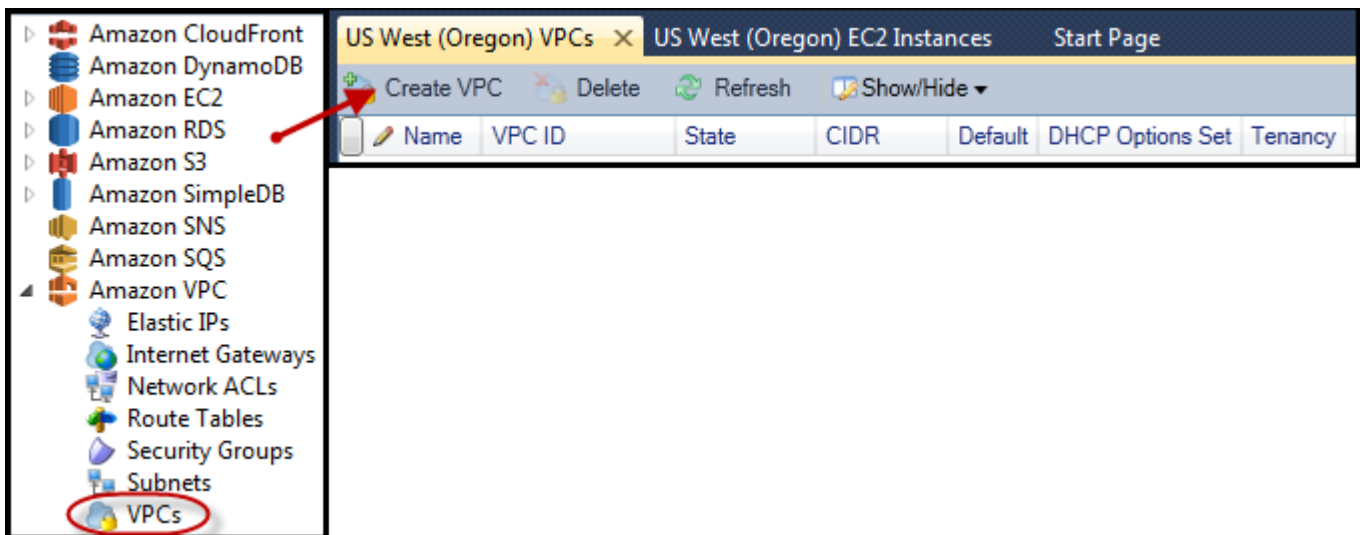
Questa sezione descrive come creare un Amazon VPC contenente sottoreti pubbliche e private. La sottorete pubblica contiene un'istanza Amazon EC2 che esegue NAT (Network Address Translation) per consentire alle istanze nella sottorete privata di comunicare con Internet pubblica. Le due sottoreti devono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

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

Per ulteriori informazioni sulla Network Address Translation (NAT), consulta [Istanze NAT](#) nella Amazon Virtual Private Cloud Guida per l'utente. Per un esempio su come configurare la distribuzione per l'utilizzo di un VPC, consulta [Distribuzione su Elastic Beanstalk](#).

Per creare un VPC di subnet pubblico-privato

1. Nella Amazon VPC Node in AWS Explorer, apri il VPC subnode, quindi scegli Crea VPC.



2. Configurare il VPC come segue:

- Digita un nome per il VPC.
- Seleziona il Con sottorete pubblica e la Con sottorete privata (Sentinella pigra?).
- Dalla Availability zone (Zona di disponibilità) casella di riepilogo a discesa per ogni sottorete, scegliere una zona di disponibilità. Assicurati di utilizzare lo stesso AZ per entrambe le subnet.

- Per la sottorete privata, inNome coppia di chiaviFornisci una key pair. Questa key pair viene utilizzata per l'istanza Amazon EC2 che esegue la traduzione degli indirizzi di rete dalla sottorete privata a Internet pubblico.
- Seleziona ilConfigurare un gruppo di sicurezza predefinito per consentire il traffico verso NAT.

Digita un nome per il VPC. Seleziona ilCon sottorete pubblicae laCon sottorete privata(Sentinella pigra?). DallaAvailability zone (Zona di disponibilità)casella di riepilogo a discesa per ogni sottorete, scegliere una zona di disponibilità. Assicurati di utilizzare lo stesso AZ per entrambe le subnet. Per la sottorete privata, inNome coppia di chiaviFornisci una key pair. Questa key pair viene utilizzata per l'istanza Amazon EC2 che esegue la traduzione degli indirizzi di rete dalla sottorete privata a Internet pubblico. Seleziona ilConfigurare un gruppo di sicurezza predefinito per consentire il traffico verso NAT.

Scegli OK.

Create VPC

Name: myDeploymentVPC

CIDR Block*: 10.0.0.0/16

Tenancy: default

With Public Subnet

Public Subnet: 10.0.0.0/24 Availability Zone: us-west-2b

A subnet will be added to the VPC with an internet gateway associated to it. This will allow instances in this subnet access to the internet.

With Private Subnet

Private Subnet: 10.0.1.0/24 Availability Zone: us-west-2b

NAT Instance Type: Small NAT Key Pair Name: key-pair-vs-1ip

Configure default security group to allow traffic to NAT

Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation. (Hourly charges for NAT instances apply)

Creation of public or private subnets will be performed in the background. To check the status view the output window.

OK Cancel

È possibile visualizzare il nuovo VPC nella VPC tab in AWSExplorer.

	Name	VPC ID	State	CIDR	Default	DHCP Options Set	Tenancy
1	myDeploymentVPC	vpc-da0013b3	available	10.0.0.0/16	False	dopt-80cddae9	default

L'istanza NAT potrebbe richiedere alcuni minuti. Quando è disponibile, è possibile visualizzarlo espandendo il Amazon EC2 Nodo in AWSExplorer e quindi aprendo il sottonodo.

Un record AWS Elastic Beanstalk (Amazon EBS) viene creato automaticamente per l'istanza NAT. Per ulteriori informazioni su Elastic Beanstalk, consulta [AWS Elastic Beanstalk \(EBS\)](#) nella Guida per l'utente di Amazon EC2 User Guide per le istanze Linux.

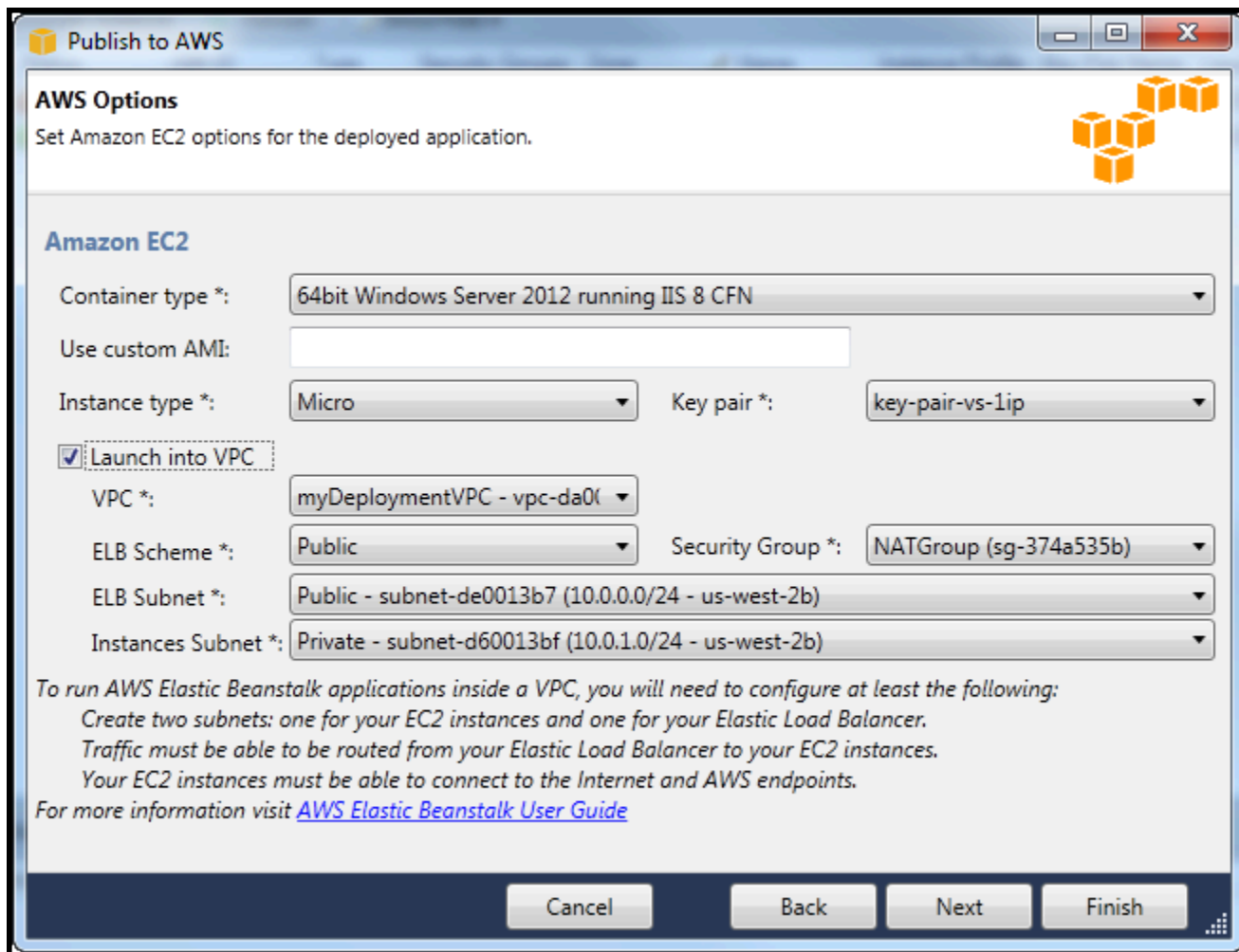
Instance ID	Status	AMI ID	Type	Security Groups	Zone	Name	Instance Profile	Key Pair Name	Launch Time	Public DNS
i-709d9342	running	ami-52ff7262	m1.small	default	us-west-2b	NAT		key-pair-vs-1ip	4/5/2013 9:26:57 AM	

Volume ID	Capacity	Snapshot ID	Created	Zone	Status	Attachment Information	vol-tag
vol-da5a91e2	8 GiB	snap-4301d52b	4/5/2013 9:27:00 AM	us-west-2b	in-use	i-709d9342:/dev/sda1 (attached)	

Se [tu distribuire un'applicazione su un AWS Elastic Beanstalk ambiente](#) e scegli di lanciare l'ambiente in un VPC, il Toolkit popolerà il Publish to (Pubblica in CloudWatch) Amazon Web Services finestra di dialogo con le informazioni di configurazione per il VPC.

Il Toolkit popola la finestra di dialogo con le informazioni solo dai VPC creati nel Toolkit e non da VPC creati utilizzando il AWS Management Console. Questo perché quando il Toolkit crea un VPC, tagga i componenti del VPC in modo che possa accedere alle loro informazioni.

Lo screenshot seguente della procedura guidata di distribuzione mostra un esempio di finestra di dialogo popolata con i valori di un VPC creato nel Toolkit.



Per eliminare un VPC

Per eliminare il VPC, devi prima terminare qualsiasi istanza Amazon EC2 nel VPC.

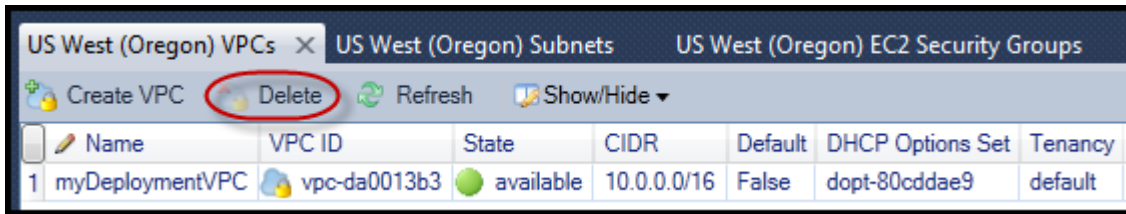
1. Se è stata distribuita un'applicazione su unAWS Elastic BeanstalkAmbiente nel VPC, eliminare l'ambiente. Ciò terminerà tutte le istanze Amazon EC2 che ospitano la tua applicazione insieme al bilanciamento del carico Elastic Load Balancing.

Se si tenta di terminare 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 sviluppatori di Auto Scaling](#).

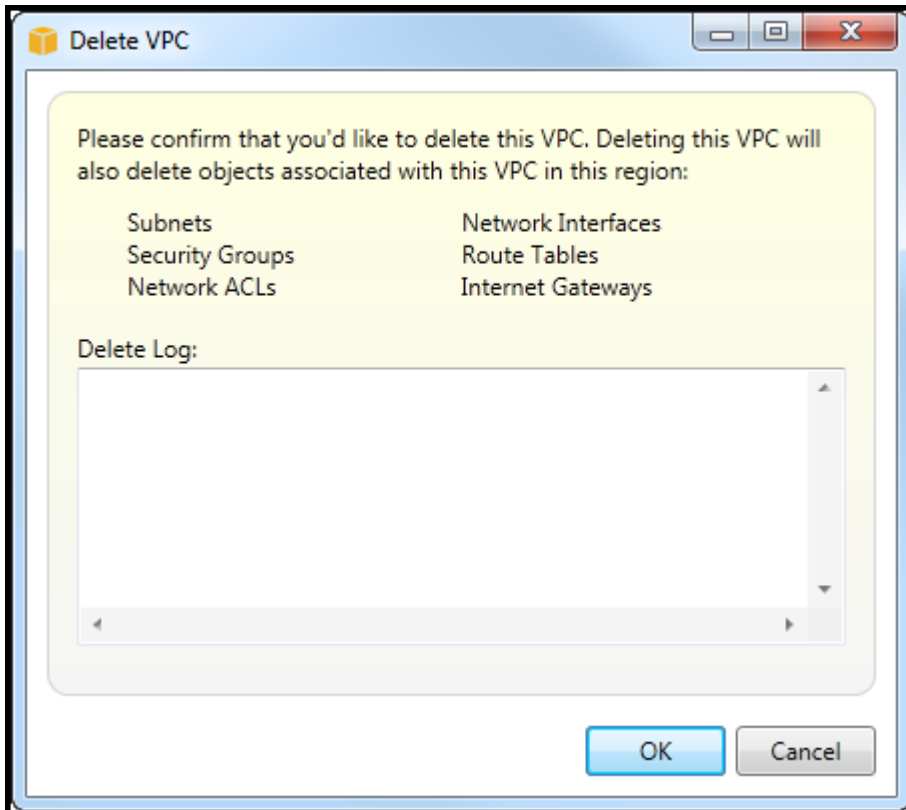
2. Eliminare l'istanza NAT per il VPC.

Non è necessario eliminare il volume Amazon EBS associato all'istanza NAT per eliminare il VPC. Tuttavia, se non si elimina il volume, continuerà ad essere addebitato anche se si elimina l'istanza NAT e il VPC.

3. Su **VPCTab**, scegli **il link per eliminare il VPC**.



4. Nella **finestra di dialogo per eliminare il VPC**, scegli **OK**.



Utilizzo dell'editor AWS CloudFormation di modelli per Visual Studio

Il Toolkit for Visual Studio include AWS CloudFormation un editor di modelli AWS 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 AWS 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

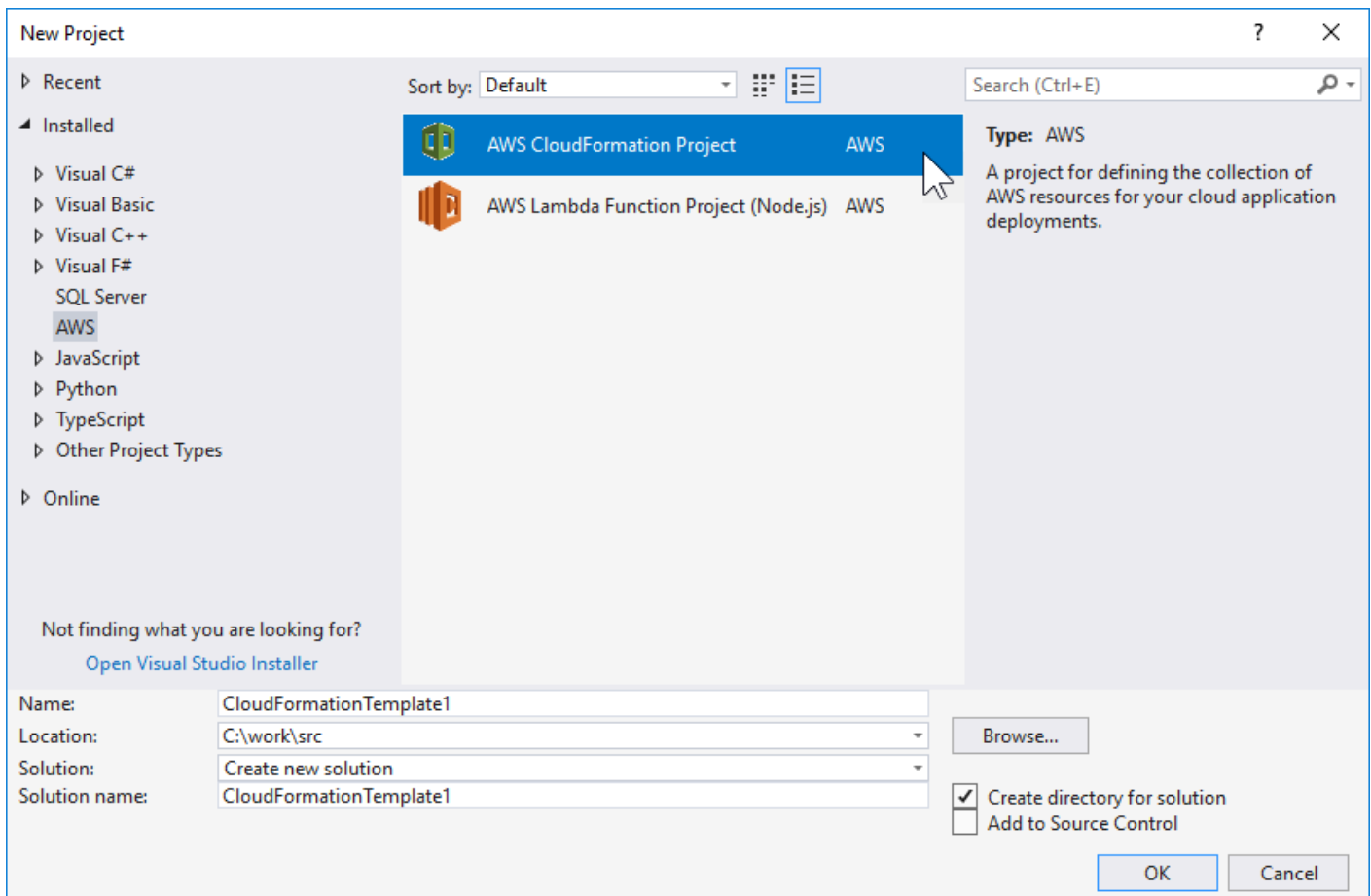
- [Creazione di unAWS CloudFormationProgetto modello in Visual Studio](#)
- [Distribuzione di unAWS CloudFormationModello in Visual Studio](#)
- [Formattazione di unAWS CloudFormationModello in Visual Studio](#)

Creazione di unAWS CloudFormationProgetto modello in Visual Studio

Per creare un progetto modello

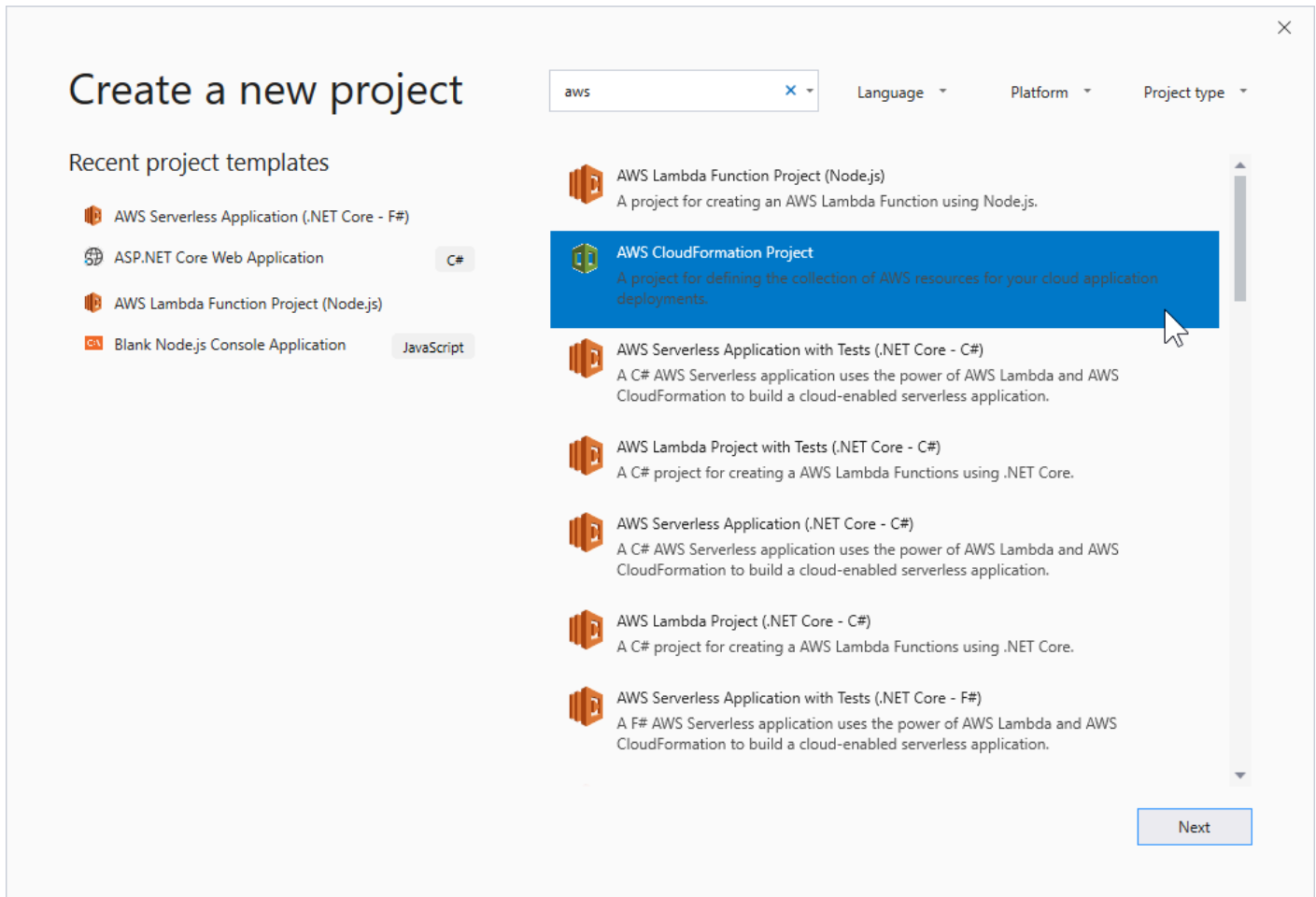
1. In Visual Studio, scegliereFile, scegliNovitàe quindiProgetto.
2. Per Visual Studio 2017:

NellaNuovo progettofinestra di dialogo, espansioneInstallatoe selezionareAWS.



Per Visual Studio 2019:

Nella Nuova finestra di dialogo, assicurarsi che il Linguaggio, Piattaforma, e Tipo di progetto caselle a discesa sono impostate su «Tutto...» e digitare aws nella Cerca.



3. Seleziona ilAWSProgetto CloudFormationmodello.

4. Per Visual Studio 2017:

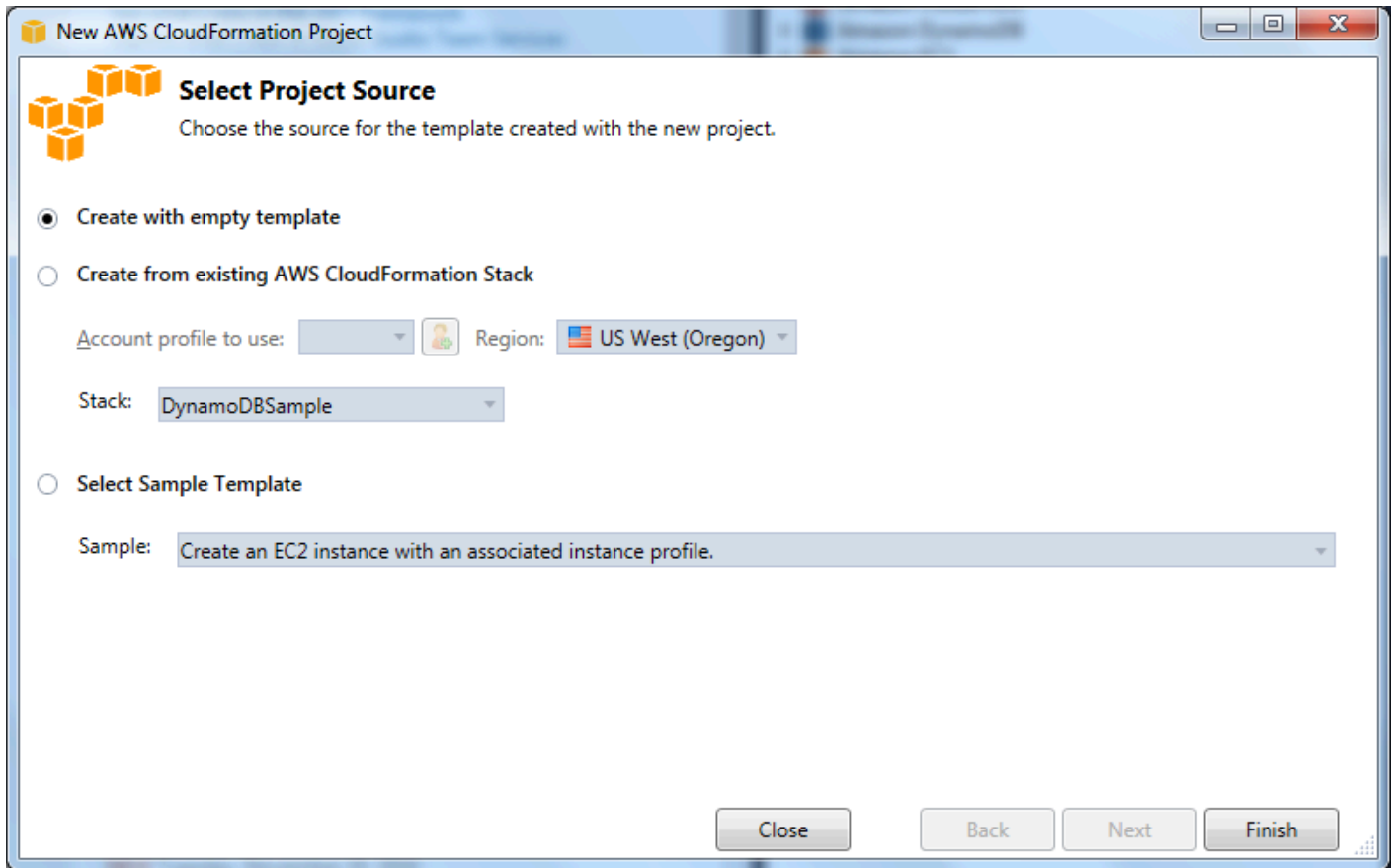
Immetti il desideratoNome,Posizione, ecc., per il tuo progetto modello, quindi fai clic suOK.

Per Visual Studio 2019:

Fai clic su Next (Successivo). Nella finestra di dialogo successiva, immettere il desideratoNome,Posizione, ecc., per il tuo progetto modello, quindi fai clic suCreate.

5. SulSELECT PROJECT, scegliere l'origine del modello da creare:

- Crea con modello vuotogenera un nuovo vuotoAWS CloudFormationmodello.
- Creazione da esistenteAWS|CFN| stackgenera un modello da uno stack esistente nel tuoAWSconto. (Lo stack non ha bisogno di avere uno stato diCREATE_COMPLETE.)
- Seleziona modello di esempiogenera un modello da uno deiAWS CloudFormationModelli di esempio.

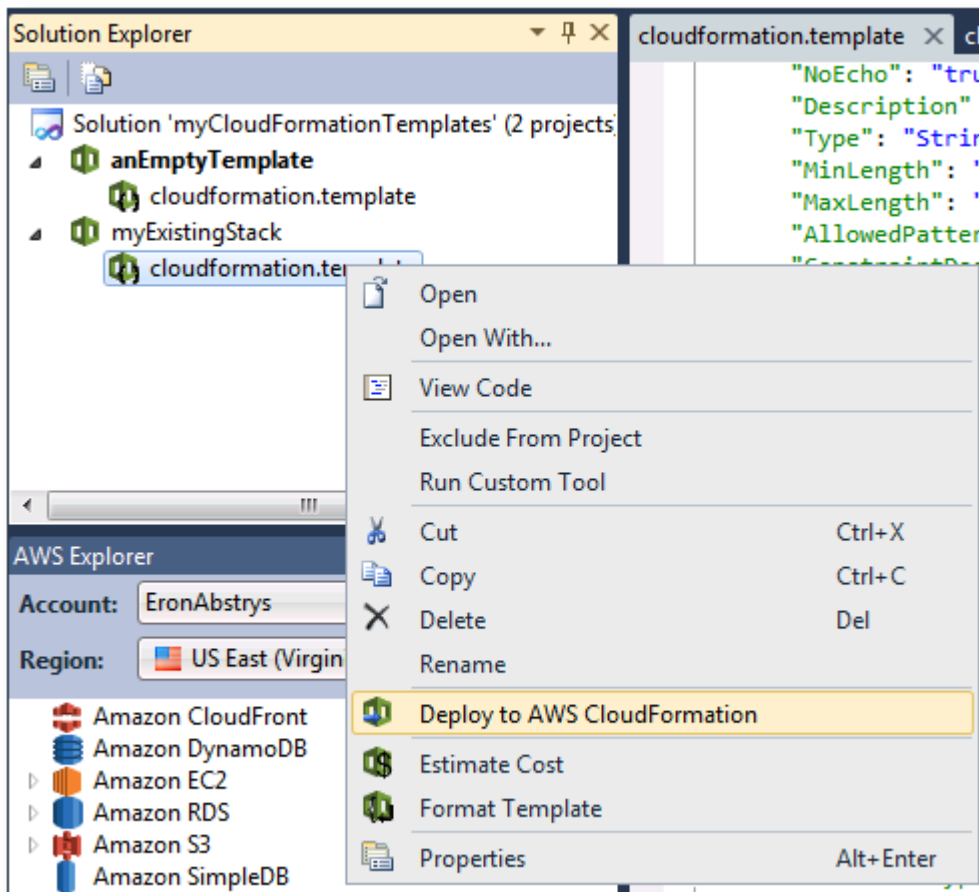


6. Per completare la creazione del tuo AWS CloudFormation progetto modello, scegli **Termina**.

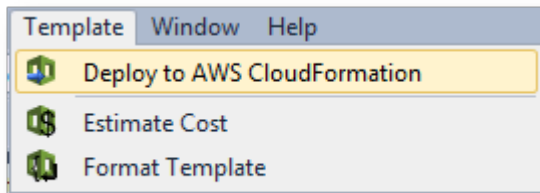
Distribuzione di un AWS CloudFormation Modello in Visual Studio

Per distribuire un modello CFN

1. In **Esplora soluzioni** aprire il menu contestuale (pulsante destro del mouse) per il modello che vuoi distribuire e scegliere **Distribuzione su AWS CloudFormation**.



In alternativa, per distribuire il modello che stai attualmente modificando, dal **Templatemenu**, scegli **Distribuzione suAWS CloudFormation**.



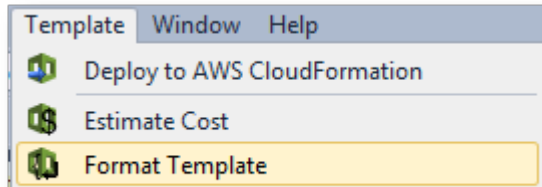
2. Sul **Modello di distribuzione** pagina, scegli il **Account AWS** da utilizzare per lanciare lo stack e la regione in cui verrà lanciato.

3. Scegliere Creare nuovo stack e digita un nome per lo stack.
4. Seleziona una (o nessuna) delle seguenti opzioni:
 - Per ricevere notifiche sullo stato di avanzamento dello stack, dall'argomento SNS Seleziona a discesa, scegliere un argomento SNS. È inoltre possibile creare un argomento SNS scegliendo Creare nuovo argomento e digitando un indirizzo e-mail nella casella.
 - Utilizza Creation Timeout per specificare per quanto tempo AWS CloudFormation dovrebbe concedere alla creazione dello stack prima che venga dichiarata non riuscita (ed eseguito il rollback, a meno che il Rollback on failure (Rollback in caso di errore) opzione è cancellata).
 - Utilizza Rollback on failure (Rollback in caso di errore) se vuoi che venga eseguito il rollback dello stack (ovvero, elimina se stesso) al fallimento. Lasciala deselezionata se vuoi che lo stack rimanga attivo per il debug, anche se l'avvio non è stato completato correttamente.
5. Scegliere Termina per avviare lo stack.

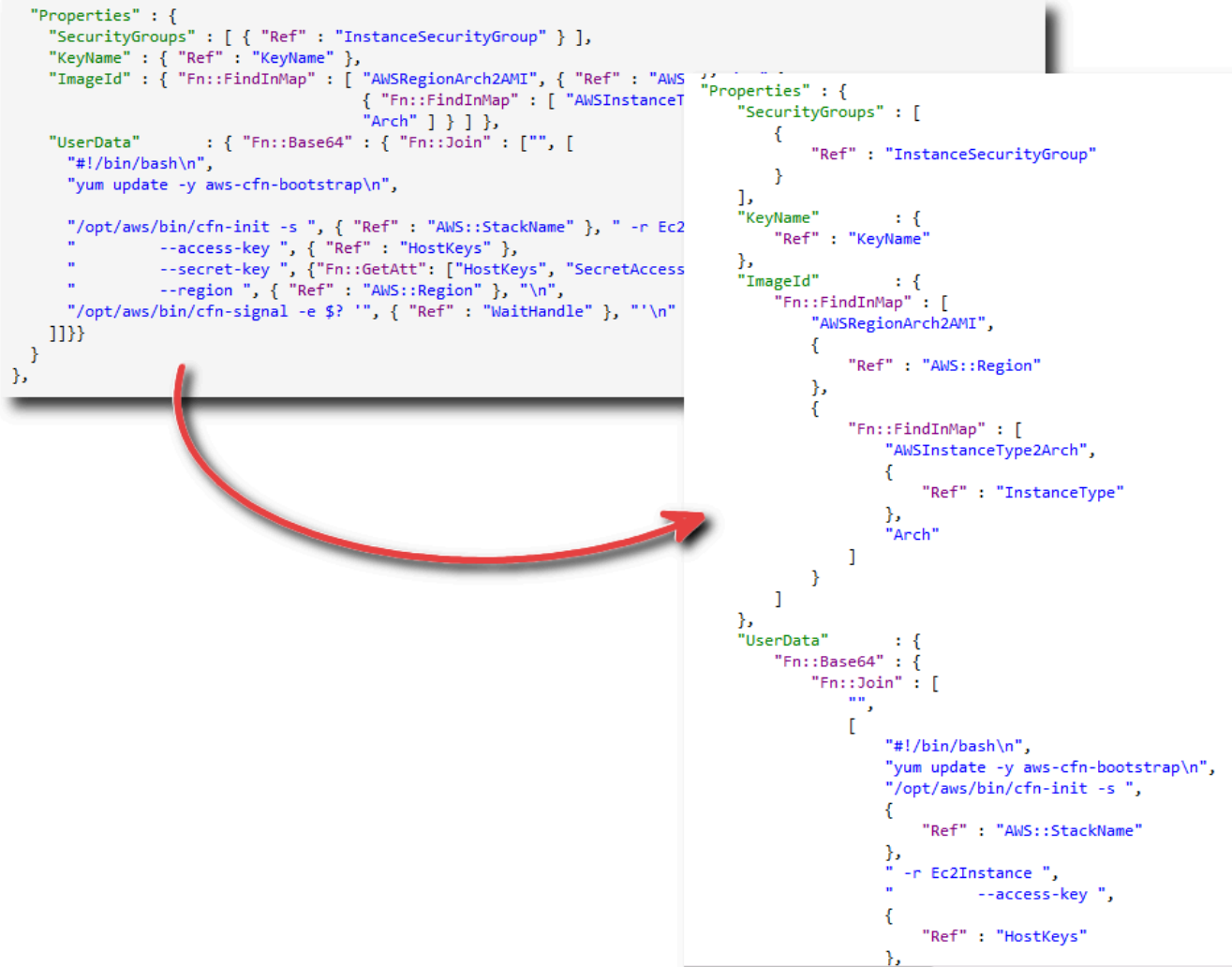
Formattazione di unAWS CloudFormationModello in Visual Studio

- In Solution Explorer (Esplora soluzioni), apri il menu contestuale del modello facendo clic con il pulsante destro del mouseFormat template.

In alternativa, per formattare il modello che stai modificando, dalTemplatemenu, scegliFormat template.



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



```

"Properties" : {
  "SecurityGroups" : [ { "Ref" : "InstanceSecurityGroup" } ],
  "KeyName" : { "Ref" : "KeyName" },
  "ImageId" : { "Fn::FindInMap" : [ "AWSRegionArch2AMI", { "Ref" : "AWSInstanceType2Arch",
    { "Fn::FindInMap" : [ "AWSInstanceType2Arch",
      { "Ref" : "InstanceType",
        "Arch" ] } ] } ] ] },
  "UserData" : { "Fn::Base64" : { "Fn::Join" : [ "", [
    "#!/bin/bash\n",
    "yum update -y aws-cfn-bootstrap\n",
    "\n",
    "/opt/aws/bin/cfn-init -s ", { "Ref" : "AWS::StackName" }, " -r Ec2Instance ",
    "--access-key ", { "Ref" : "HostKeys" },
    "--secret-key ", { "Fn::GetAtt" : [ "HostKeys", "SecretAccessKey" ] },
    "--region ", { "Ref" : "AWS::Region" }, "\n",
    "/opt/aws/bin/cfn-signal -e $? ", { "Ref" : "WaitHandle" }, "\n" ] ] ] } }
}
}

```

```

"Properties" : {
  "SecurityGroups" : [
    {
      "Ref" : "InstanceSecurityGroup"
    }
  ],
  "KeyName" : {
    "Ref" : "KeyName"
  },
  "ImageId" : {
    "Fn::FindInMap" : [
      "AWSRegionArch2AMI",
      {
        "Ref" : "AWS::Region"
      }
    ],
    "Fn::FindInMap" : [
      "AWSInstanceType2Arch",
      {
        "Ref" : "InstanceType",
        "Arch"
      }
    ]
  }
},
"UserData" : {
  "Fn::Base64" : {
    "Fn::Join" : [
      "",
      [
        "#!/bin/bash\n",
        "yum update -y aws-cfn-bootstrap\n",
        "/opt/aws/bin/cfn-init -s ",
        {
          "Ref" : "AWS::StackName"
        },
        " -r Ec2Instance ",
        "--access-key ",
        {
          "Ref" : "HostKeys"
        }
      ]
    ]
  }
}

```

Uso di Amazon S3 da AWSEsploratore

Amazon 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, è possibile accedere solo da te. Il Toolkit for Visual Studio consente di archiviare i dati su Amazon S3 e di visualizzare, gestire, recuperare e distribuire tali dati.

Amazon S3 utilizza il concetto di bucket, che puoi pensare come simile ai file system o alle unità logiche. I bucket possono contenere cartelle simili a directory e oggetti simili ai file. In questa sezione, useremo questi concetti mentre esploriamo la funzionalità Amazon S3 esposta dal Toolkit for Visual Studio.

Note

Per utilizzare questo strumento, la policy di IAM deve concedere le autorizzazioni per `ils3:GetBucketAcl`, `s3:GetBucket`, `es3:ListBucket` azioni. Per ulteriori informazioni, consulta [Panoramica di AWS Policy IAM](#).

Creazione di un bucket Amazon S3

Il bucket è l'unità di archiviazione fondamentale in Amazon S3.

Per creare un bucket S3

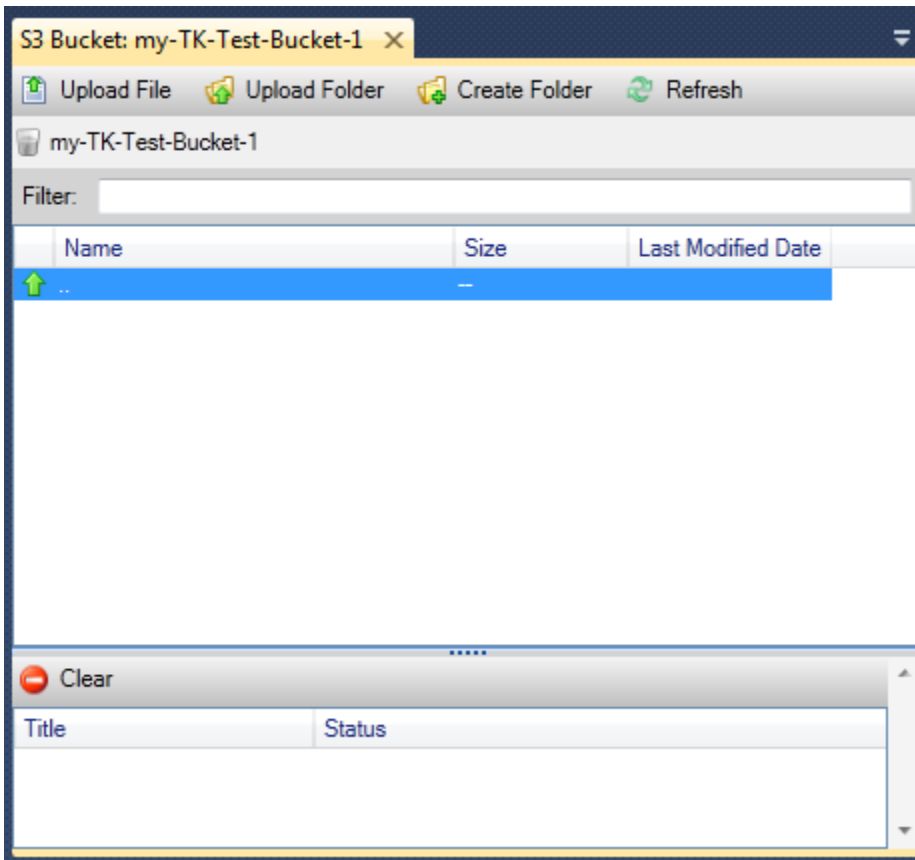
1. Nello stato `AWSExplorer`, aprire il menu di scelta rapida (destro del mouse) per il `Amazon S3` nodo, quindi scegliere `Per creare bucket`.
2. Nella `Per creare bucket`, digitare un nome per il bucket. I nomi dei bucket devono essere univoci `AWS`. Per informazioni su altri vincoli, consulta la [Documentazione Amazon S3](#).
3. Scegli `OK`.

Gestione dei bucket Amazon S3 da `AWSEsploratore`

Nello stato `AWSExplorer`, le seguenti operazioni sono disponibili quando si apre un menu contestuale (pulsante destro del mouse) per un bucket Amazon S3.

Sfoggia

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 visualizza i messaggi di stato relativi al processo di caricamento. Per cancellare questi messaggi, scegli `Annulla`. È inoltre possibile accedere a questa vista del bucket facendo doppio clic sul nome del bucket in `AWSExplorer`.



Proprietà

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

- Impostazione delle autorizzazioni Amazon S3 che mirano a:
 - tu come proprietario del secchio.
 - tutti gli utenti che sono stati autenticati suAWS.
 - tutti con accesso a Internet.
- Attiva la registrazione per il secchio.
- Configurare 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 [Domande frequenti su S3](#).
- Creazione di un sito Web statico utilizzando i dati nel bucket.

Policy

Consente di configurare AWS Identity and Access Management (IAM) policy per il tuo bucket. Per ulteriori informazioni, consulta la [Documentazione di IAM](#) e i casi d'uso per [IAM e S3](#).

Creazione di URL prefirmato

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

Visualizzazione di caricamenti multi-parte

Consente di visualizzare i caricamenti multiparte. Amazon S3 supporta la rottura di carichi di oggetti di grandi dimensioni in parti per rendere il processo di caricamento più efficiente. Per ulteriori informazioni, consulta la discussione di [caricamenti multiparte nella documentazione di S3](#).

Elimina

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

Caricamento di file e cartelle in Amazon S3

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

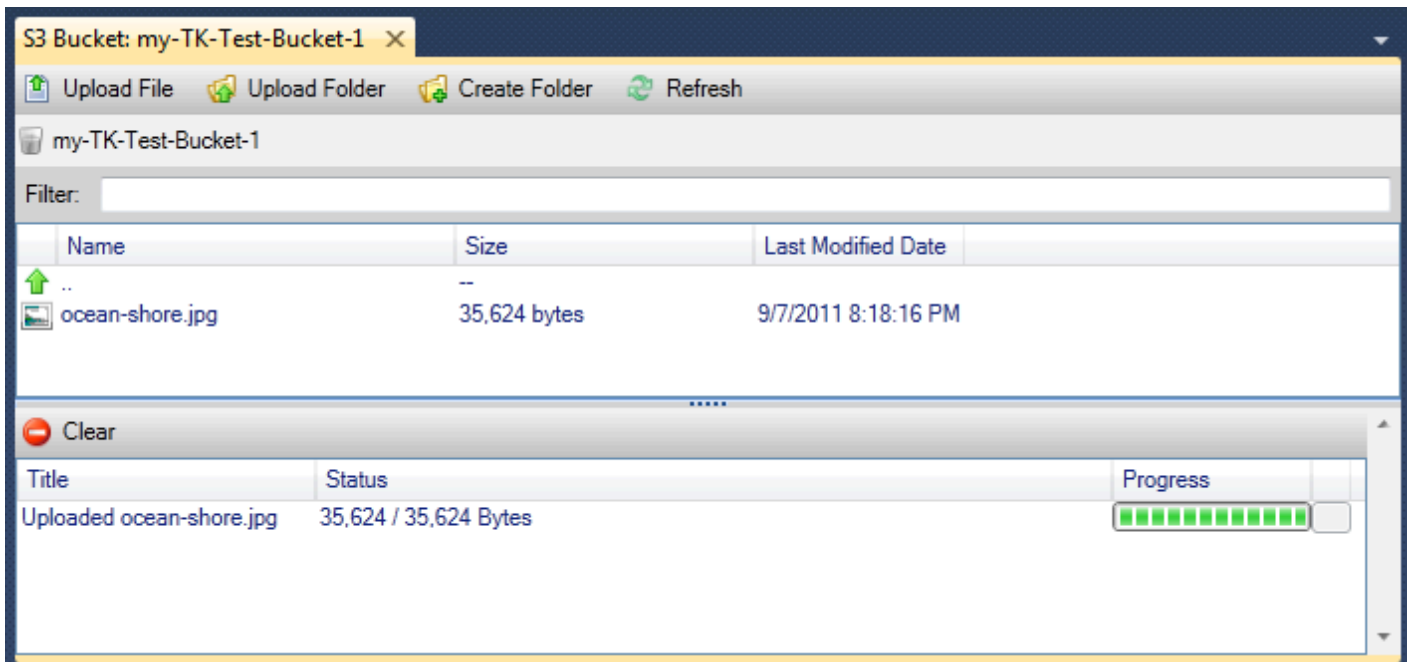
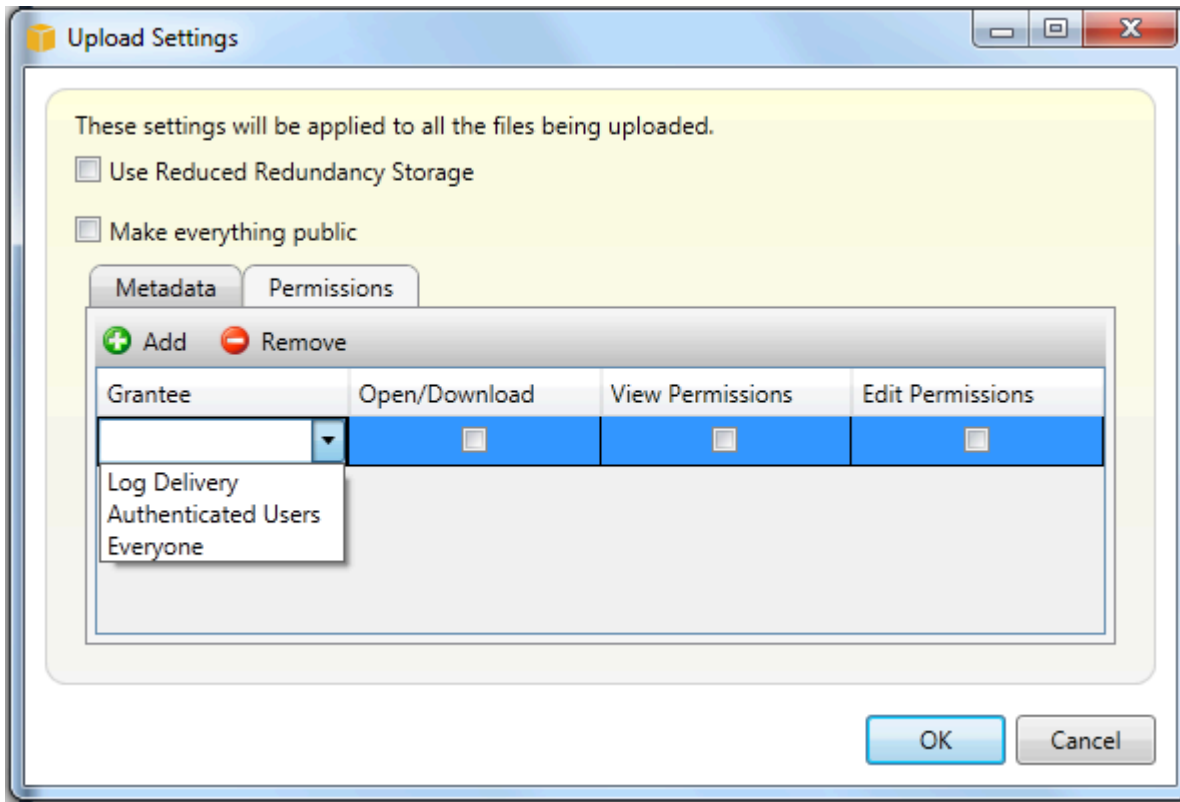
Note

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

Per caricare un file in S3

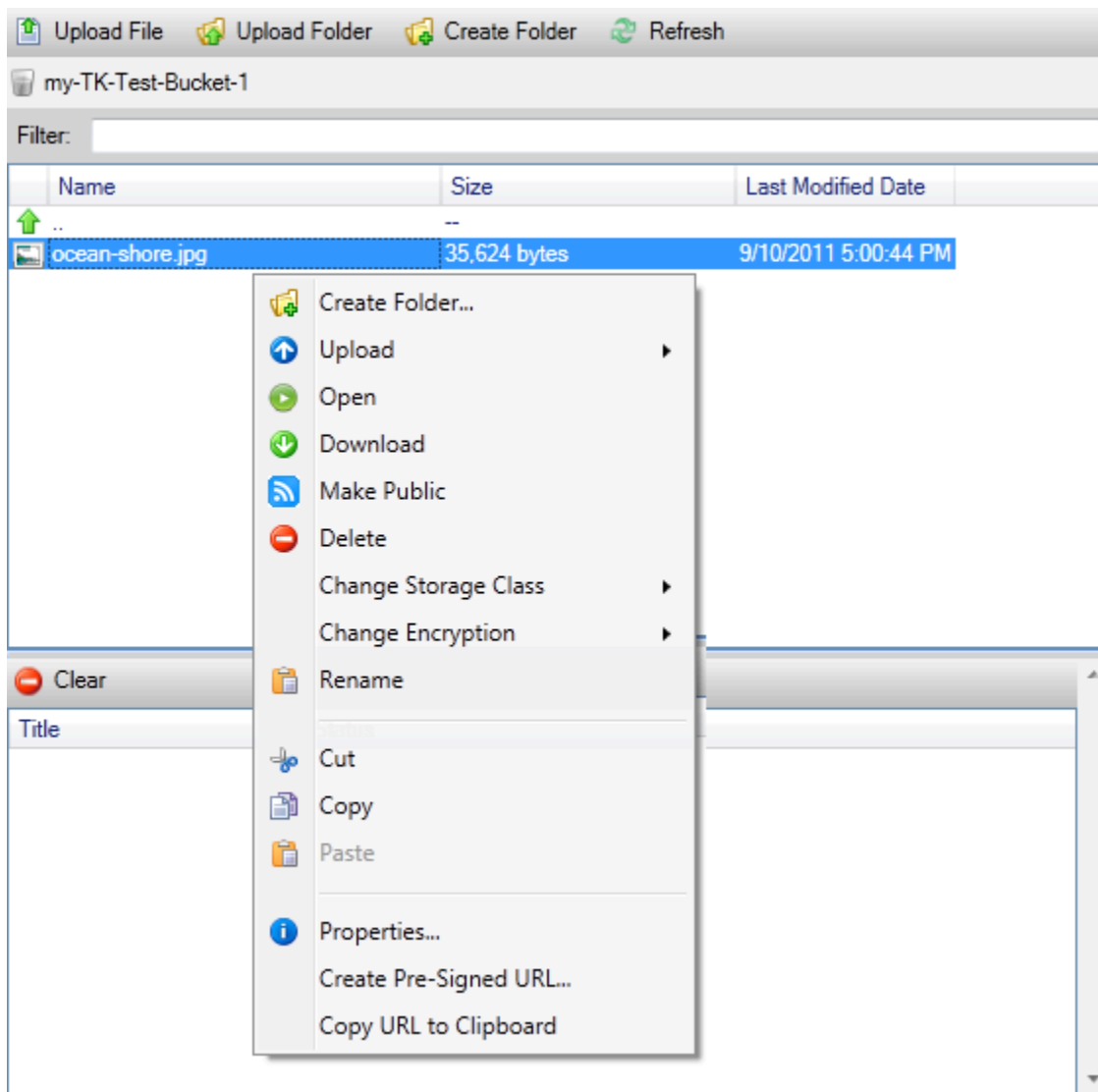
1. Nello stato AWS Explorer, espandi Amazon S3 e fare doppio clic su un bucket o aprire il menu contestuale (pulsante destro del mouse) per il bucket e scegliere Sfoglia.
2. Nella Sfogliavista del tuo secchio, scegli Carica file o Carica cartella.
3. Nella Apri file finestra di dialogo, passare ai file da caricare, selezionarli e scegliere Open (Apertura). Se stai caricando una cartella, accedi e scegli quella cartella, quindi scegli Open (Apertura).

La Caricamento delle impostazioni finestra di dialogo consente di impostare metadati e autorizzazioni per i file o la cartella che si sta caricando. Selezione della Rendere pubblico tutta la casella di controllo equivale all'impostazione Apertura/scarica autorizzazioni per Tutti. È possibile selezionare l'opzione da utilizzare [Ridondanza ridotta](#) per i file caricati.



Operazioni sui file Amazon S3 daAWSToolkit for Visual Studio

Se scegli un file nella visualizzazione Amazon S3 e apri il menu contestuale (pulsante destro del mouse), puoi eseguire varie operazioni sul file.



Create Folder

Consente di creare una cartella nel bucket corrente. (Equivalente alla scelta del [Create Folder](#) (link)).

Caricamento

Consente di caricare file o cartelle. (Equivalente alla scelta del [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 predefinite del browser, il file potrebbe non essere visualizzato. Potrebbe essere semplicemente scaricato dal browser.

Scarica

Apri un albero di cartelle in una finestra di dialogo per consentire di scaricare il file selezionato.

Rendi pubblico

Imposta le autorizzazioni per il file selezionato. (Equivalente alla selezione dell'opzione di rendere pubblico nella finestra di dialogo di controllo sulla configurazione delle impostazioni.)

Elimina

Elimina i file o le cartelle selezionati. È inoltre possibile eliminare file o cartelle scegliendoli e premendo **Delete**.

Modifica classe di storage

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

Modifica della crittografia

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

Assegnazione di un nuovo nome

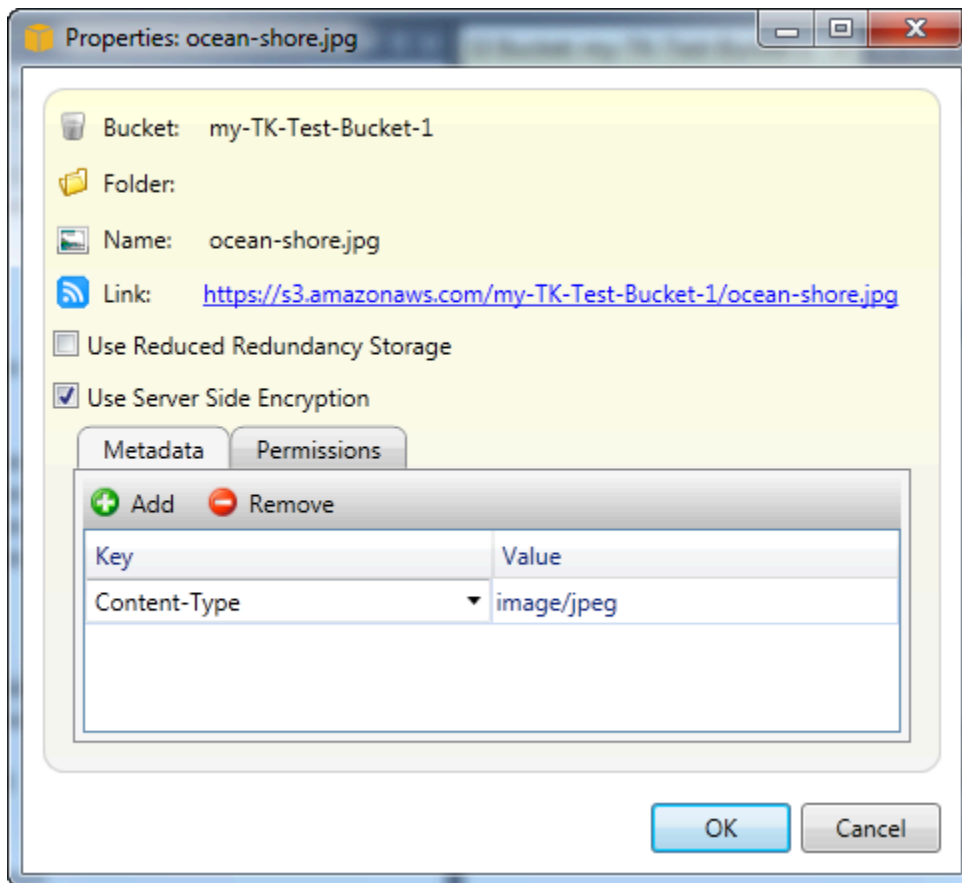
Consente di rinominare un file. Non è possibile rinominare una cartella.

Taglia | Copia | Incolla

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

Proprietà

Visualizza una finestra di dialogo che consente di impostare metadati e autorizzazioni per il file, nonché di attivare l'opzione di archiviazione per il 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 si sceglie questo collegamento, il Toolkit for Visual Studio apre il file nel browser predefinito. Se si dispone di autorizzazioni per il file impostate su **Apertura/scarica tutti**, altre persone saranno in grado di accedere al file tramite questo link. Invece di distribuire questo link, ti consigliamo di creare e distribuire URL pre-firmati.



Creazione di URL prefirmato

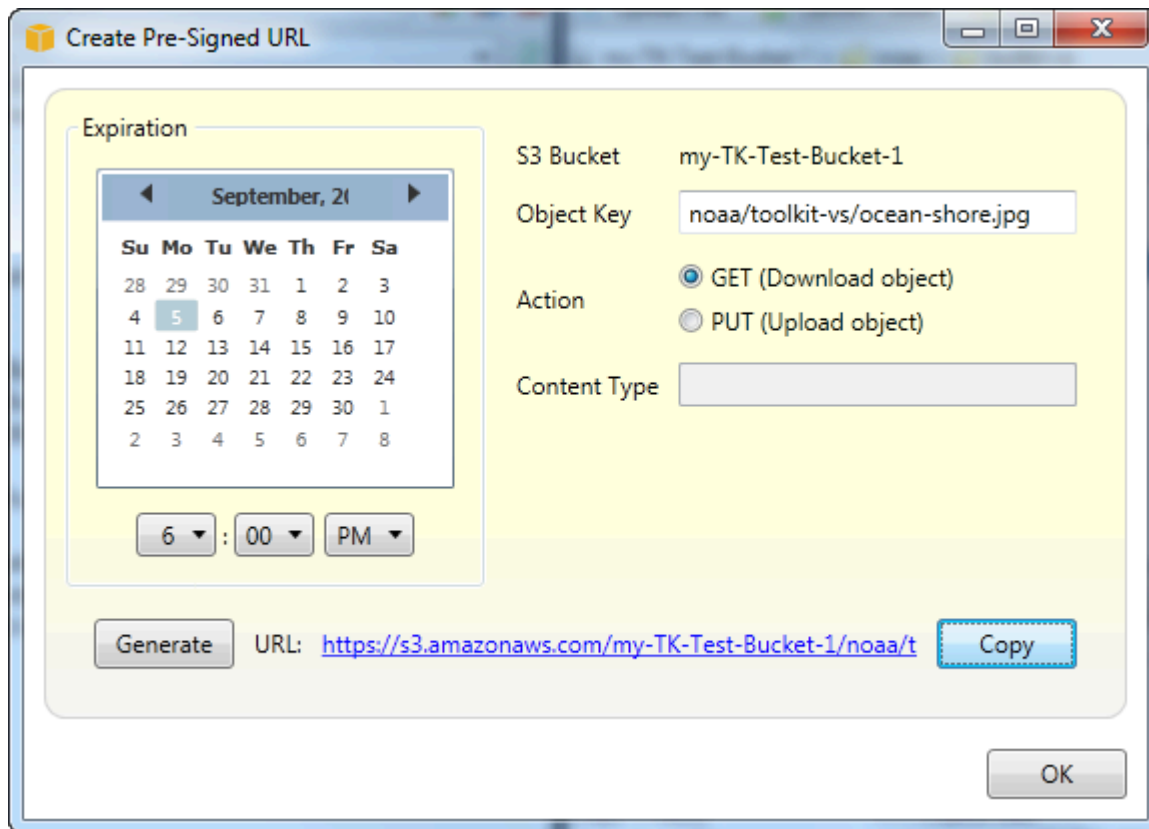
Consente di creare un URL prefirmato a tempo limitato che puoi distribuire per consentire ad altre persone di accedere ai contenuti che hai archiviato su Amazon S3.

Come creare un URL prefirmato

È possibile creare un URL prefirmato per un bucket o 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 quando si crea l'URL.

Per creare un URL prefirmato

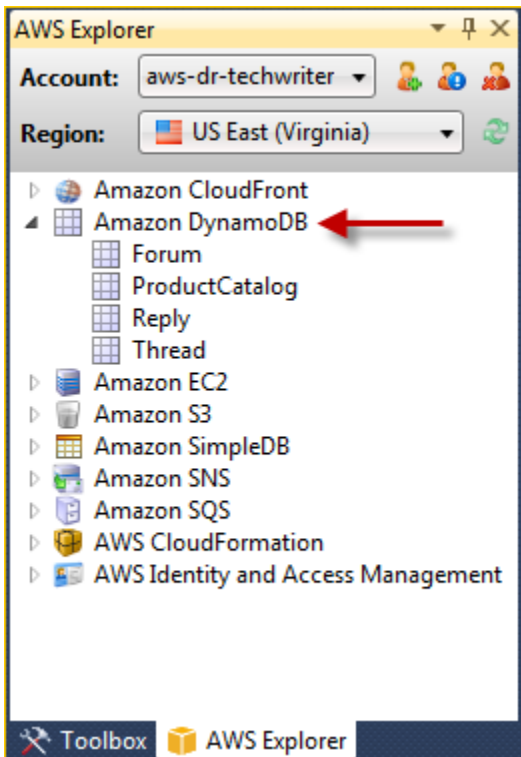
1. Nella Creazione di URL prefirmato, impostare la data e l'ora di scadenza per l'URL. L'impostazione predefinita è un'ora dall'ora corrente.
2. Seleziona Genera pulsante.
3. Per copiare l'URL negli appunti, scegliere Copia (Copia).



Utilizzo di DynamoDBAWSEsploratore

Amazon DynamoDB è un servizio di database non relazionale, conveniente, veloce e altamente scalabile e disponibile. DynamoDB rimuove le tradizionali limitazioni di scalabilità dello storage dei dati, mantenendo una bassa latenza e prestazioni prevedibili. Toolkit for Visual Studio fornisce la funzionalità per l'utilizzo con DynamoDB in un contesto di sviluppo. Per ulteriori informazioni su DynamoDB, consulta [DynamoDB](#) sul sito Web Amazon Web Services.

Nel Toolkit for Visual Studio, AWSExplorer visualizza tutte le tabelle DynamoDB associate alla Account AWS.



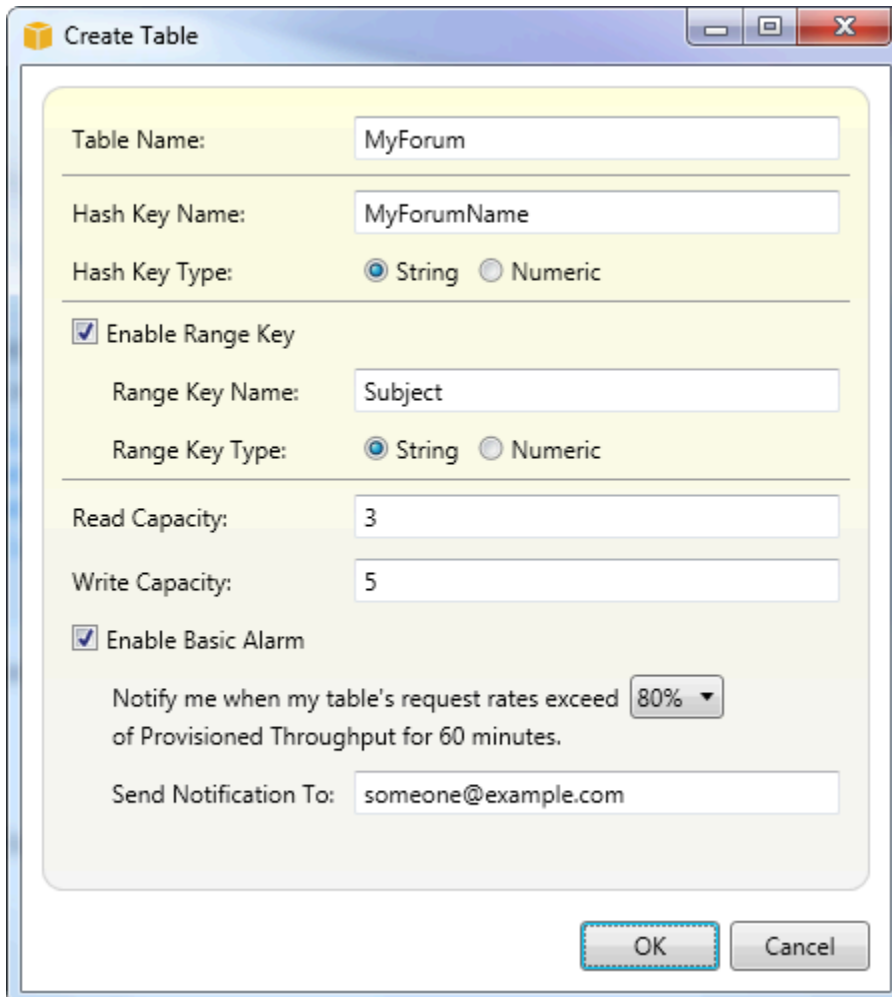
Creazione di una tabella DynamoDB

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

Per creare una tabella inAWSEsploratore

1. Nello statoAWSEsplora risorse, aprire il menu contestuale (pulsante destro del mouse) perAmazon DynamoDBe quindiCREATE TABLE.
2. NellaCREATE TABLE, inNome tabella, digitare un nome per la tabella.
3. NellaNome chiave hashcampo, digitare un attributo chiave hash primario e dalTipo di chiave hash, scegliere il tipo di chiave hash. DynamoDB crea un indice hash non ordinato utilizzando l'attributo della chiave primaria e un indice di intervallo ordinato opzionale che utilizza l'attributo della chiave primaria di intervallo. Per ulteriori informazioni sull'attributo chiave hash principale, consulta la[Chiave primaria](#)nellaGuida per gli sviluppatori di Amazon DynamoDB.
4. (Opzionale) SelezionaAttivare la chiave. NellaNome chiavecampo, digitare un attributo chiave intervallo e quindi dalTipo di chiave, scegliere un tipo di chiave di intervallo.
5. NellaCapacità di lettura, digitare il numero di unità di capacità di lettura. NellaCapacità di scrittura, digitare il numero di unità di capacità di scrittura. È necessario specificare un minimo di tre unità di capacità in lettura e di cinque unità di capacità in scrittura. Per ulteriori informazioni sulle unità di capacità in lettura e scrittura, consulta[Throughput assegnato in DynamoDB](#).

- (Opzionale) Seleziona **Attivare l'allarme** per avvisarti quando i tassi di richiesta del tuo tavolo sono troppo alti. Scegliere la percentuale di throughput fornito per 60 minuti che deve essere superato prima dell'invio dell'avviso. In **Invia notifiche a**, digitare un indirizzo e-mail.
- Fare clic su **OK** per creare la tabella.



The screenshot shows the 'Create Table' dialog box with the following configuration:

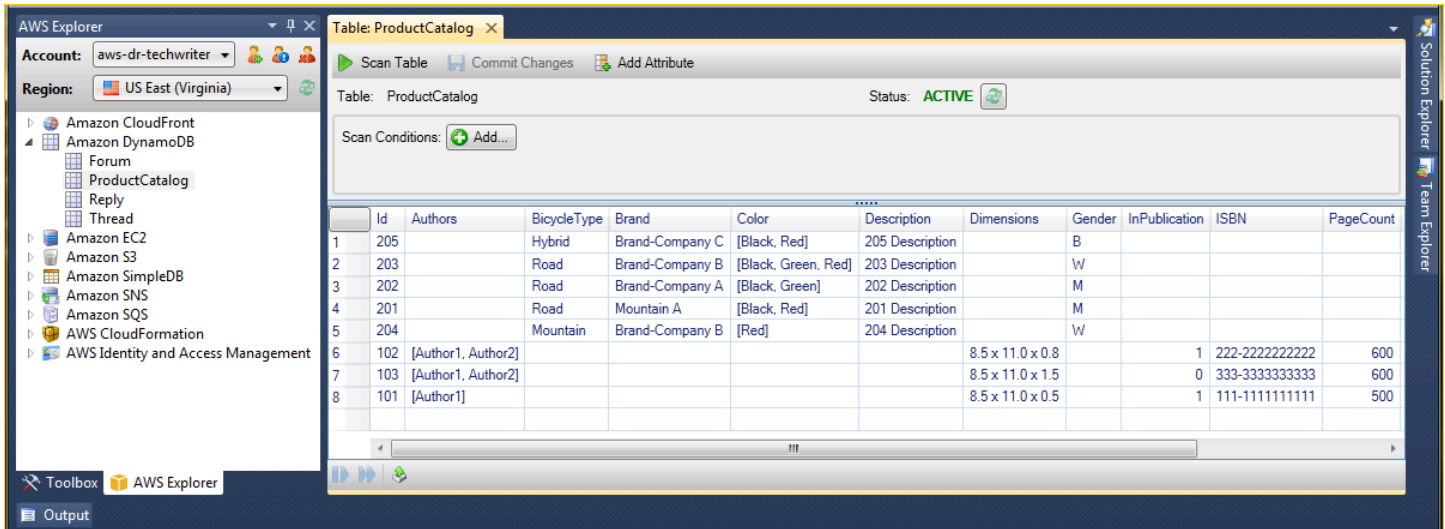
- Table Name: MyForum
- Hash Key Name: MyForumName
- Hash Key Type: String (selected)
- Enable Range Key:
- Range Key Name: Subject
- Range Key Type: String (selected)
- Read Capacity: 3
- Write Capacity: 5
- Enable Basic Alarm:
- Notify me when my table's request rates exceed: 80% (dropdown)
- of Provisioned Throughput for 60 minutes.
- Send Notification To: someone@example.com

Per ulteriori informazioni sulle tabelle DynamoDB, consulta [Concetti dei modelli di dati: tabelle, elementi e attributi](#).

Visualizzazione di una tabella DynamoDB come una griglia

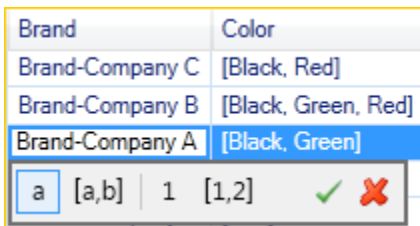
Per aprire una visualizzazione a griglia di una tabella DynamoDB, in AWS Fare doppio clic sul sottonodo corrispondente alla tabella. Dalla visualizzazione griglia, è possibile visualizzare le voci, gli attributi e i valori memorizzati nella tabella. Ogni riga corrisponde a una voce nella tabella. Le 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.

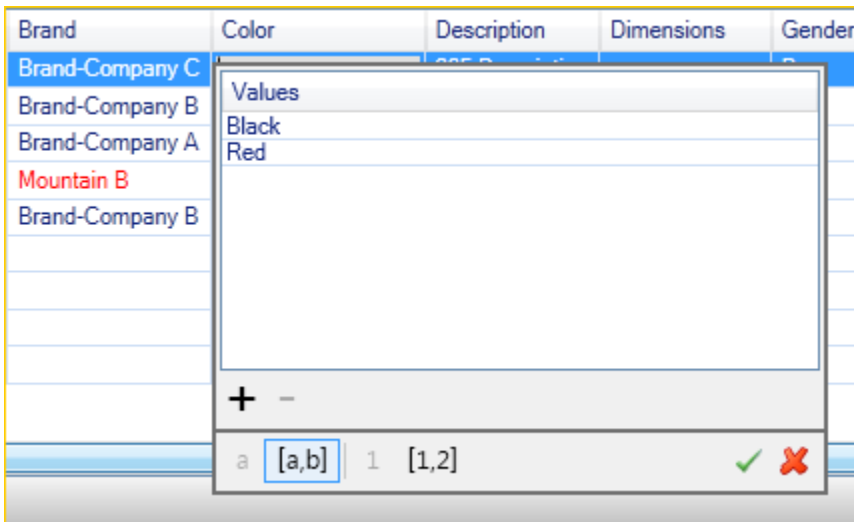


Modifica e aggiunta di attributi e valori

Facendo doppio clic su una cella, è possibile modificare i valori dell'attributo corrispondente della voce. 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, è anche possibile, con alcune limitazioni, 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 set di valori. 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.

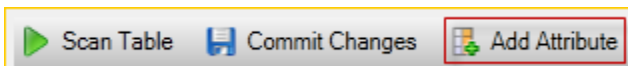


Dopo la modifica del valore dell'attributo, scegli il segno di spunta verde per confermare le modifiche. Se vuoi ignorare le modifiche, scegli la X.

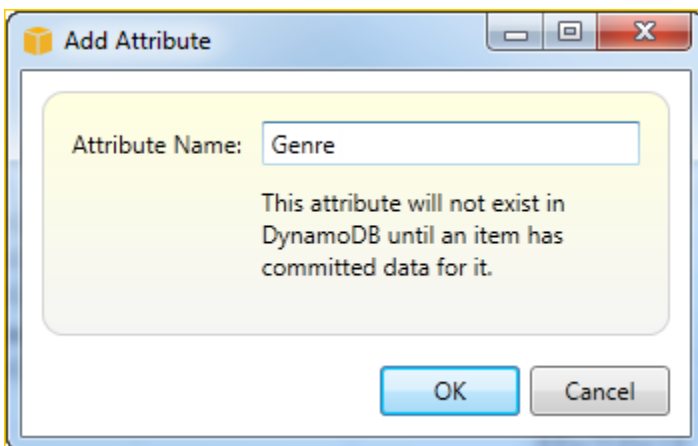
Dopo aver confermato le modifiche, il valore dell'attributo verrà visualizzato in rosso. Questo indica che l'attributo è stato aggiornato, ma che il nuovo valore non è stato riscritto nel database di DynamoDB. Per riscrivere le modifiche su DynamoDB, scegli **Commit modifiche**. Per ignorare le modifiche, scegli **Scansione della tabella** e quando il Toolkit chiede se si desidera eseguire il commit delle modifiche prima della scansione, scegli **No**.

Aggiunta di un attributo

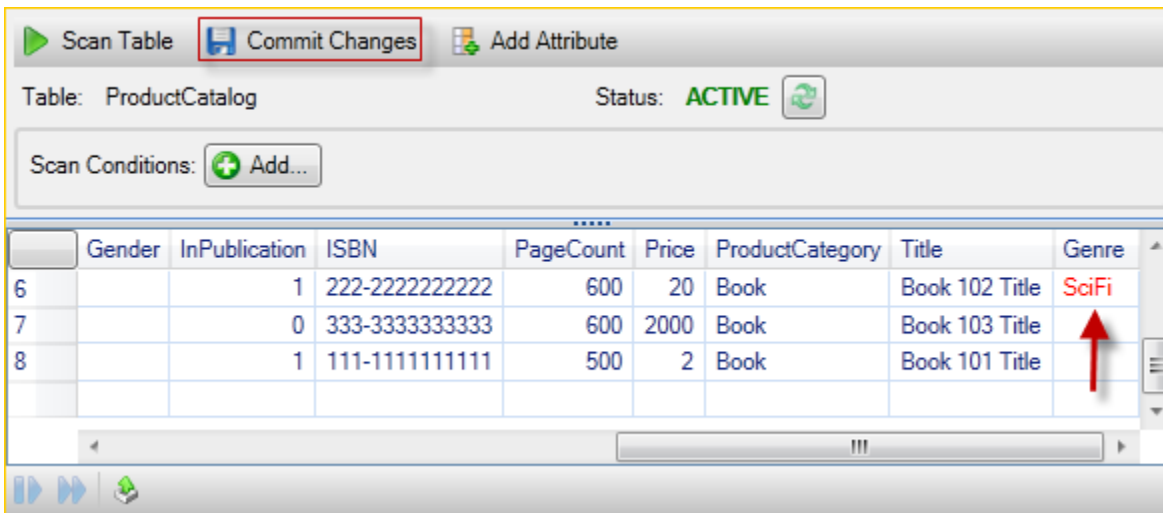
Dalla visualizzazione griglia, puoi anche aggiungere attributi alla tabella. Per aggiungere un nuovo attributo, scegli **Aggiungi attributo**.



Nella **Aggiungi attributo**, digitare un nome per l'attributo e quindi scegliere **OK**.



Per far sì che il nuovo attributo diventi parte della tabella, è necessario aggiungervi un valore per almeno un elemento e quindi scegliere il Commit modifiche. Per eliminare il nuovo attributo, basta chiudere la vista griglia della tabella senza scegliere Commit modifiche.



Scansione di una tabella DynamoDB

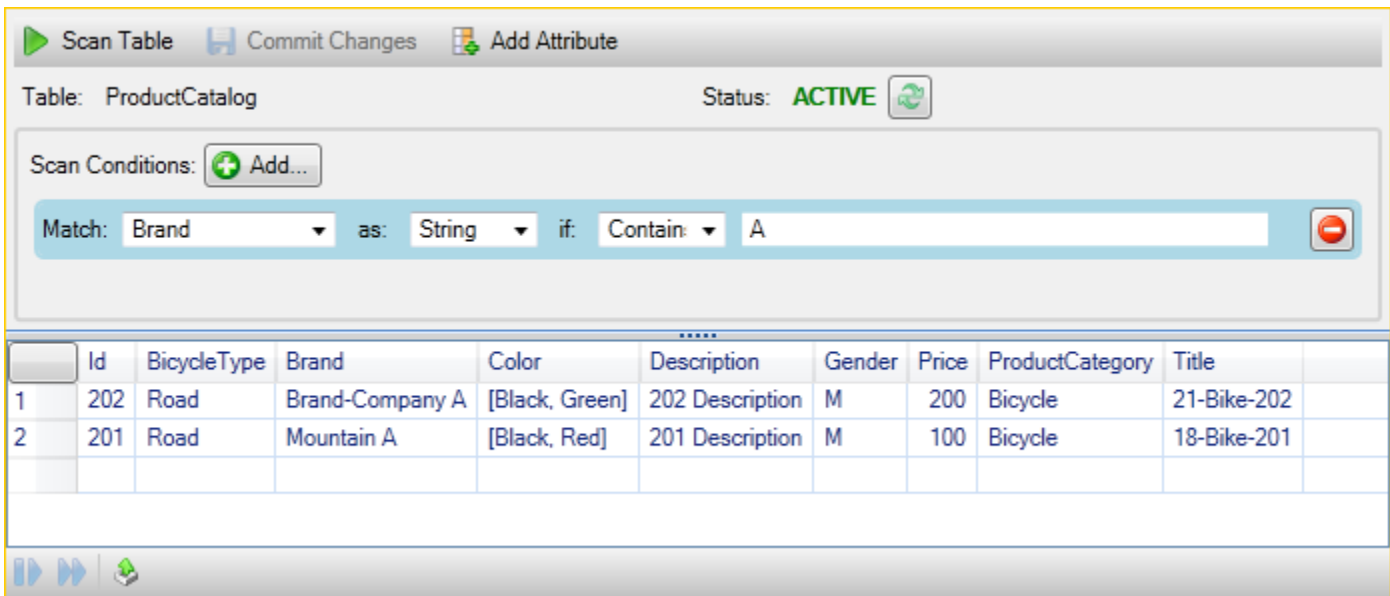


È possibile eseguire la scansione delle tabelle DynamoDB dal Toolkit. In una scansione si definisce un set di criteri e la scansione restituisce tutte le voci della tabella che soddisfano i criteri specificati. Le scansioni sono operazioni onerose e devono essere utilizzate con attenzione per evitare di compromettere il traffico di produzione con priorità elevata sul tavolo. Per ulteriori informazioni sull'utilizzo dell'operazione di scansione, consulta la Guida per gli sviluppatori di Amazon DynamoDB.

Per eseguire una scansione in una tabella DynamoDB da AWSEsploratore

1. Nella visualizzazione griglia, scegliere condizioni di scansione: aggiungi.
2. Nell'editor della clausola di scansione, selezionare l'attributo su cui eseguire il confronto, 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. Aggiunta di altre clausole di scansione, se necessario, per la ricerca. La scansione restituirà solo le voci che soddisfano i criteri di tutte le clausole di scansione. Scansione eseguirà un confronto con distinzione tra lettere maiuscole e minuscole durante il confronto con i valori
4. Nella barra dei pulsanti nella parte superiore della visualizzazione griglia, selezionare Scansione della tabella.

Per rimuovere una clausola di scansione, selezionare il pulsante rosso con la riga bianca a destra di ciascuna clausola.



Per tornare alla visualizzazione della tabella che include tutte le voci, rimuovi tutte le clausole di scansione e scegli Scansione della tabella di nuovo.

Paginazione dei risultati della scansione

Nella parte inferiore della visualizzazione ci sono tre pulsanti.



I primi due pulsanti blu forniscono la paginazione dei risultati della scansione. Il primo pulsante mostrerà una pagina aggiuntiva dei risultati. Il secondo pulsante mostrerà altre dieci pagine di risultati. In questo contesto, una pagina è uguale a 1 MB di contenuto.

Esporta risultati di scansione in CSV

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

Utilizzo di AWS CodeCommit con Visual Studio Team Explorer

È possibile utilizzare AWS Identity and Access Management (IAM) account utente per creare credenziali Git e utilizzarle per creare e clonare repository da Team Explorer.

Tipo di credenziali perAWS CodeCommit

La maggior parteAWS Toolkit for Visual Studiogli utenti sono a conoscenza della configurazioneAWSprofili credenziali che contengono il loro accesso e chiavi segrete. Questi profili credenziali vengono utilizzati nel Toolkit for Visual Studio per abilitare le chiamate alle API di servizio, ad esempio per l'elenco dei bucket Amazon S3AWSExplorer o per avviare un'istanza Amazon EC2. Integrazione diAWS CodeCommitcon Team Explorer utilizza anche questi profili credenziali. Tuttavia, per lavorare con Git stesso hai bisogno di credenziali aggiuntive, in particolare credenziali Git per le connessioni HTTPS. Puoi leggere queste credenziali (un nome utente e una password) all'indirizzo [Configurazione degli utenti HTTPS con le credenziali Git](#) nellaAWS CodeCommitGuida per l'utente di.

È possibile creare le credenziali Git perAWS CodeCommit solo per account utente IAM. Non è possibile crearli 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 inattivi, i set inattivi continuano a contare sul limite di due set. Si noti che puoi eliminare e ricreare le credenziali in qualsiasi momento. Quando utilizziAWS CodeCommitda Visual Studio, il tuo tradizionaleAWSle credenziali vengono utilizzate per lavorare con il servizio stesso, ad esempio durante la creazione e l'elenco dei repository. Quando si lavora con i repository Git effettivi ospitati inAWS CodeCommit, si utilizzano le credenziali Git.

Come parte del supporto diAWS CodeCommit, il Toolkit for Visual Studio crea e gestisce automaticamente queste credenziali Git per te e le associa al tuoAWSprofilo delle credenziali. Non è necessario preoccuparsi 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 tuoAWSprofilo credenziale, le credenziali Git associate vengono utilizzate automaticamente ogni volta che si lavora con un telecomando Git.

Connessione ad AWS CodeCommit

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



AWS CodeCommit is a fully-managed source control service that makes it easy for companies to host secure and highly scalable private Git repositories.

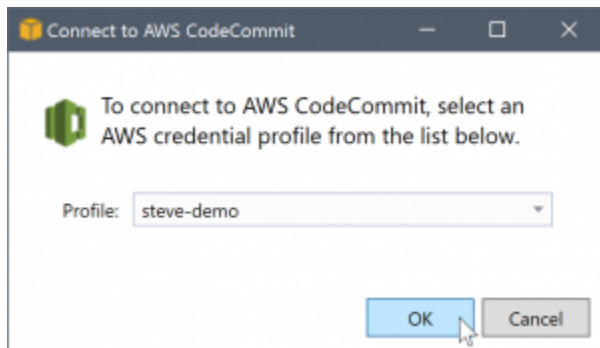
[Connect...](#)

[Sign up](#)

SceltaRegistrazioneapre la home page di Amazon Web Services in una finestra del browser. Cosa succede se si sceglieCollegarsidipende dal fatto che Toolkit for Visual Studio sia in grado di trovare un profilo delle credenziali conAWSchiavi di accesso e segrete per abilitarlo a effettuare chiamateAWSa nome tuo. È possibile che sia stato impostato un profilo di credenziali utilizzando la nuova pagina Guida introduttiva che viene visualizzata nell'IDE quando il Toolkit for Visual Studio non riesce a trovare credenziali memorizzate localmente. Oppure potresti aver utilizzato Toolkit for Visual Studio,AWS Tools for Windows PowerShell, o ilAWS CLIe giàAWSdisponibili per Toolkit for Visual Studio.

Quando si sceglieCollegarsi, il Toolkit for Visual Studio avvia il processo per trovare un profilo credenziale da utilizzare nella connessione. Se il Toolkit for Visual Studio non riesce a trovare un profilo credenziale, apre una finestra di dialogo che invita a immettere le chiavi di accesso e segrete per il tuoAccount AWS. Si consiglia di utilizzare un account utente IAM e non le credenziali di root. Inoltre, come notato in precedenza, le credenziali Git necessarie 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 eAWS CodeCommitè pronto per l'uso.

Se Toolkit for Visual Studio ne trova più di unoAWSprofilo credenziali, ti viene richiesto di selezionare l'account che desideri utilizzare all'interno di Team Explorer.



Se si dispone di un solo profilo credenziale, il Toolkit for Visual Studio ignora la finestra di dialogo di selezione del profilo e si è connessi immediatamente:

Quando viene stabilita una connessione tra Team Explorer eAWS CodeCommittramite i profili credenziali, la finestra di dialogo dell'invito si chiude e viene visualizzato il pannello di connessione.



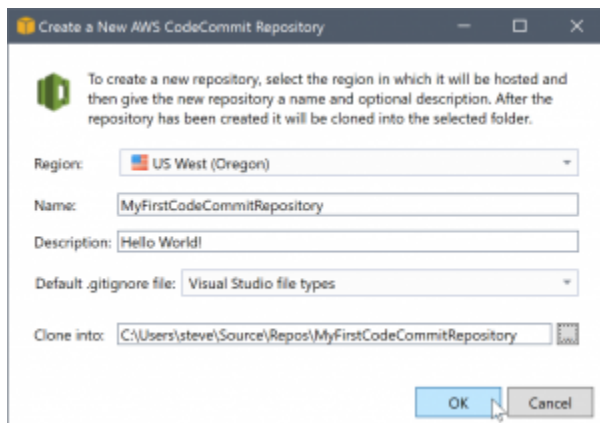
Poiché non si dispone di repository clonati localmente, il pannello mostra solo le operazioni che è possibile eseguire: Clona,Create, eDisconnessione. Come altri fornitori,AWS CodeCommitin

Team Explorer può essere associato a un solo AWS in un dato profilo delle credenziali. Per cambiare account, utilizza **Disconnessione** per rimuovere la connessione in modo da poter avviare una nuova connessione utilizzando un altro account.

Dopo aver stabilito una connessione, puoi creare un repository facendo clic su **Crea** link.

Creazione di un repository

Quando si fa clic sul pulsante **Crea** link, il link **Creazione di una nuova AWS CodeCommit Repository** Si apre una finestra di dialogo.



AWS CodeCommit 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 (richiesto) e la descrizione (facoltativo) per il nostro nuovo repository.

Il comportamento predefinito della finestra di dialogo consiste nel suffisso del percorso della cartella per il nuovo repository con il nome del repository (quando si immette il nome, viene aggiornata anche la posizione della cartella). Per utilizzare un nome di cartella diverso, modificare il **Clona in** percorso della cartella dopo aver terminato l'immissione del nome del repository.

Puoi anche scegliere di creare automaticamente un'iniziale `.gitignore` file per il repository. La AWS Toolkit for Visual Studio fornisce un valore predefinito predefinito per i tipi di file di Visual Studio. È inoltre possibile scegliere di non avere alcun file o di utilizzare un file esistente personalizzato che si desidera riutilizzare nei repository. Basta selezionare **Utilizzare custom** nell'elenco e vai al file personalizzato da usare.

Una volta che hai il nome e la posizione del repository, sei pronto a fare clic **OK** e inizia 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 si utilizza uno. È a

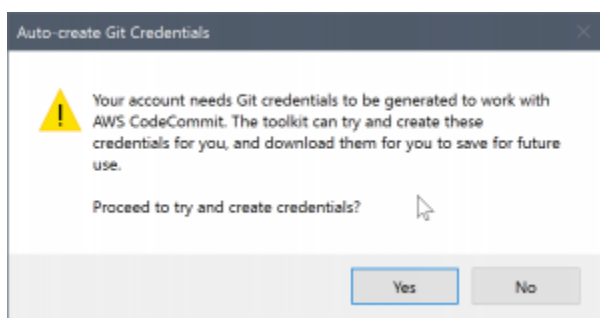
questo punto che inizi a lavorare con il telecomando Git, quindi il Toolkit for Visual Studio ora ha bisogno di accedere alle credenziali Git descritte in precedenza.

Configurazione delle credenziali Git

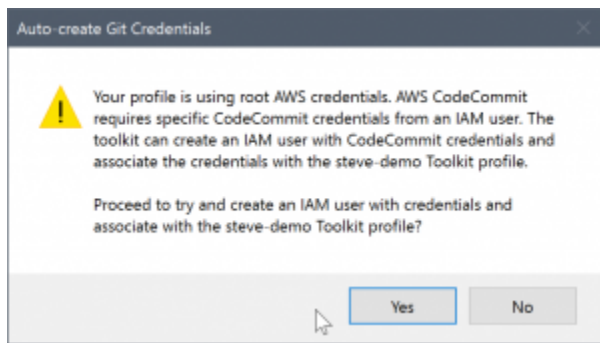
A questo punto hai usato AWS Chiavi di accesso e segrete per richiedere che il servizio crei il tuo repository. Ora devi lavorare con Git stesso per eseguire l'operazione di clone reale e Git non capisce AWS accesso e chiavi segrete. Invece, è necessario fornire le credenziali di nome utente e password a Git da utilizzare su una connessione HTTPS con il telecomando.

Come notato in [Impostazione di credenziali Git](#), le credenziali Git che intendi utilizzare devono essere associate a un utente IAM. Non è possibile generarli per le credenziali root. Dovresti sempre impostare la AWS profili credenziali per contenere l'accesso utente IAM e le chiavi segrete e non le chiavi root. Toolkit for Visual Studio può tentare di impostare le credenziali Git per AWS CodeCommit per te, e associarli a AWS profilo credenziale utilizzato per connetterti in Team Explorer in precedenza.

Quando si sceglie OK nella Creazione di una nuova AWS CodeCommit Repository finestra di dialogo e creare correttamente il repository, il Toolkit for Visual Studio controlla il AWS profilo credenziale connesso in Team Explorer per determinare se le credenziali Git AWS CodeCommit esistono e sono associati localmente al profilo. In tal caso, il Toolkit for Visual Studio indica a Team Explorer di iniziare l'operazione di clone sul nuovo repository. Se le credenziali Git non sono disponibili localmente, il Toolkit for Visual Studio verifica il tipo di credenziali dell'account utilizzate nella connessione in Team Explorer. Se le credenziali sono per un utente IAM, come consigliamo, viene visualizzato il seguente messaggio.

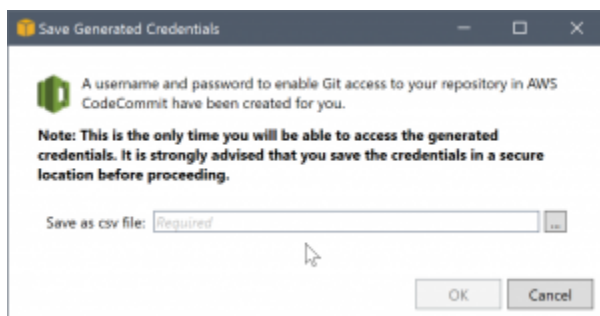


Se le credenziali sono credenziali root, viene visualizzato il seguente messaggio.



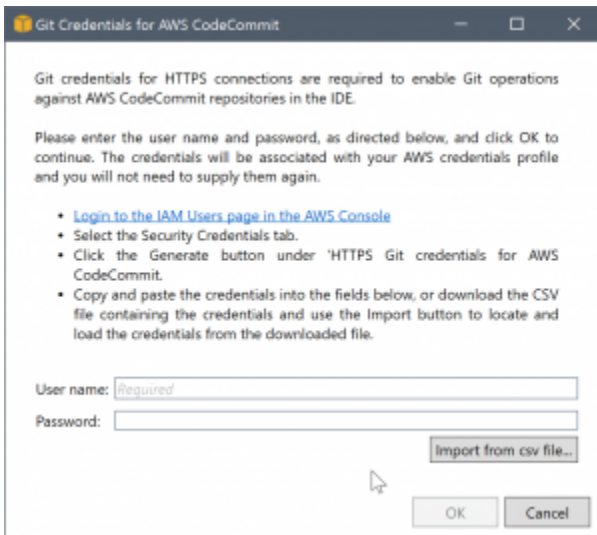
In entrambi i casi, il Toolkit for Visual Studio offre di tentare di eseguire il lavoro per creare le credenziali Git necessarie per te. Nel primo scenario, tutto ciò che deve essere creato è un set di credenziali Git per l'utente IAM. Quando è in uso un account root, Toolkit for Visual Studio tenta prima di creare un utente IAM e quindi procede alla creazione di credenziali Git per quel nuovo utente. Se il Toolkit for Visual Studio deve creare un nuovo utente, applica ilAWS CodeCommitIl criterio di Power User ha gestito il nuovo account utente. Questa politica consente l'accesso solo aAWS CodeCommite consente di eseguire tutte le operazioni conAWS CodeCommittranne che per l'eliminazione del repository.

Quando crei credenziali, puoi visualizzarle una sola volta. Pertanto, il Toolkit for Visual Studio richiede di salvare le credenziali appena create come .csvfile prima di continuare.



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

Potrebbero verificarsi casi in cui Toolkit for Visual Studio non è in grado di creare automaticamente credenziali. Ad esempio potresti aver già creato il numero massimo di set di credenziali Git perAWS CodeCommit(due), oppure potresti non disporre di diritti programmatici sufficienti per il Toolkit for Visual Studio per eseguire il lavoro per te (se hai effettuato l'accesso come utente IAM). In questi casi, è possibile effettuare l'accesso aAWS Management Consoleper gestire le credenziali o ottenerle dall'amministratore. Puoi inserirli inCredenziali Git perAWS CodeCommitfinestra di dialogo visualizzata dal Toolkit for Visual Studio.

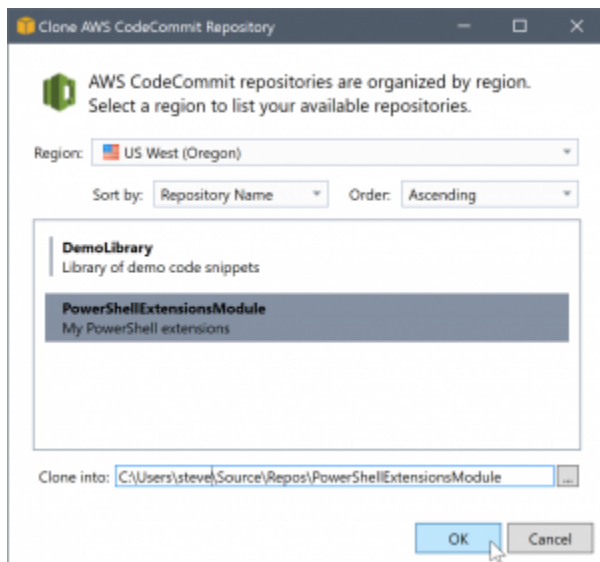


Ora che le credenziali per Git sono disponibili, l'operazione di clone per il nuovo repository procede (vedere l'indicazione dello stato di avanzamento dell'operazione all'interno di Team Explorer). Se hai scelto di avere un valore predefinito `.gitignorefile` applicato, è impegnato nel repository con un commento di 'Initial Commit'.

Questo è tutto ciò che serve per configurare le credenziali e creare un repository all'interno di Team Explorer. Una volta che le credenziali richieste sono state posizionate, tutto ciò che si vede quando si creano nuovi repository in futuro è Creazione di una nuova AWS CodeCommit Repository finestra di dialogo stessa.

Clonazione di un repository

Per clonare un repository esistente, torna al pannello di connessione per AWS CodeCommit in Team Explorer. Fai clic sull'icona della barra degli strumenti Clonalink per aprire il Clona AWS CodeCommit Repository finestra di dialogo, quindi selezionare il repository da clonare e la posizione sul disco in cui si desidera posizionarlo.



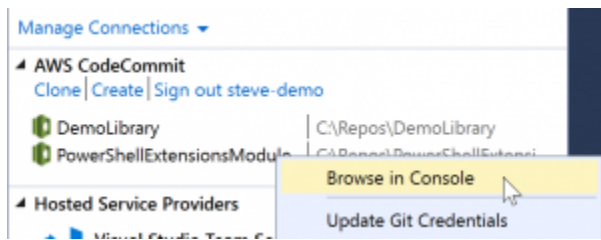
Una volta scelta l'area, il Toolkit for Visual Studio interroga il servizio per individuare i repository disponibili in tale area e li visualizza nella parte dell'elenco centrale della finestra di dialogo. Vengono inoltre visualizzati il nome e la descrizione facoltativa di ciascun repository. È possibile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

Una volta selezionato il repository, puoi scegliere la posizione in cui clonare. Questa impostazione predefinita è la stessa posizione del repository utilizzata in altri plugin di Team Explorer, ma è possibile navigare o immettere qualsiasi altra posizione. Per impostazione predefinita, il nome del repository è suffisso sul percorso selezionato. Tuttavia, se si desidera un percorso specifico, è sufficiente modificare la casella di testo dopo aver selezionato la cartella. Qualunque testo sia presente nella casella quando si fa clic OK sarà la cartella in cui troverai il repository clonato.

Dopo aver selezionato il repository e la posizione della cartella, fare clic su OK per procedere con l'operazione di clone. Proprio come per la creazione di un repository, è possibile visualizzare lo stato di avanzamento dell'operazione di clone riportato in Team Explorer.

Utilizzo dei repository

Quando clonate o create repository, notate che i repository locali per la connessione sono elencati nel pannello di connessione in Team Explorer sotto i collegamenti operativi. Queste voci offrono un modo conveniente per accedere al repository per sfogliare i contenuti. Basta fare clic con il pulsante destro del mouse sul repository Naviga in Console.



È possibile utilizzare anche **Aggiorna le credenziali Git** per aggiornare le credenziali Git memorizzate associate al profilo delle credenziali. Ciò è utile se hai ruotato le credenziali. Il comando apre il **Credenziali Git per AWS CodeCommit** finestra di dialogo in cui è possibile immettere o importare le nuove credenziali.

Le operazioni Git sui repository funzionano come ci si aspetterebbe. Puoi effettuare commit locali e, quando sei pronto per condividere, utilizza l'opzione **Sync (Sincronizza)** in **Team Explorer**. Perché le credenziali Git sono già memorizzate localmente e associate alla nostra connessione **AWS** profilo credenziale, non ci verrà richiesto di fornirli di nuovo per le operazioni contro il **AWS CodeCommit** remoto.

Utilizzo di CodeArtifact in Visual Studio

AWS CodeArtifact è un servizio di repository di artifact completamente gestito che semplifica alle organizzazioni l'archiviazione e la condivisione di pacchetti software utilizzati per lo sviluppo di applicazioni in modo sicuro. È possibile utilizzare **CodeArtifact** con i più diffusi strumenti di compilazione e gestori di pacchetti come **NuGet** e **CLI Core .NET** e **Visual Studio**. È inoltre possibile configurare **CodeArtifact** per estrarre pacchetti da un repository pubblico esterno, come [Nuget.org](https://www.nuget.org).

In **CodeArtifact**, i pacchetti vengono memorizzati in repository che vengono poi memorizzati all'interno di un dominio. La **AWS Toolkit for Visual Studio** semplifica la configurazione di **Visual Studio** con i repository **CodeArtifact**, semplificando il consumo di pacchetti in **Visual Studio** sia da **CodeArtifact** direttamente che da **Nuget.org**.

Aggiungi il tuo repository CodeArtifact come sorgente di pacchetti NuGet

Per consumare i pacchetti dal tuo **CodeArtifact**, dovrai aggiungere il tuo repository come sorgente di pacchetti nel **Programma di gestione dei pacchetti NuGet** in **Visual Studio**

Per aggiungere il repository come origine del pacchetto

1. Nello stato **AWS** Esplora risorse, accedi al repository nel **AWS CodeArtifact** nodo.

2. Apri il menu contestuale (tasto destro del mouse) per il repository che desideri aggiungere, quindi scegli Endpoint di origine NuGet.
3. Accedere a Origini pacchetti sotto il Programma di gestione dei pacchetti NuGet Nodo nel Strumenti > Opzioni menu.
4. Nello stato Origini pacchetto, seleziona il segno più (+), modificare il nome e incollare l'URL dell'endpoint di origine NuGet copiato in precedenza Crea.
5. Seleziona la casella di controllo accanto all'origine del pacchetto appena aggiunta per abilitarla.

Note

Si consiglia di aggiungere una connessione esterna a Nuget.org al tuo CodeArtifact e disabilitando il nuget.org sorgente dei pacchetti in Visual Studio. Quando si utilizza una connessione esterna, tutte le dipendenze sono state estratte da Nuget.org e sono memorizzati in CodeArtifact. Se Nuget.org si spegne per qualsiasi motivo, i pacchetti di cui hai bisogno saranno ancora disponibili. Per ulteriori informazioni sulle connessioni esterne, consulta [Aggiunta di una connessione esterna](#) nella AWS CodeArtifact Guida per l'utente di.

6. Scegliere OK per chiudere il menu.

Per ulteriori informazioni sull'utilizzo di CodeArtifact con Visual Studio, consulta [Utilizzo di CodeArtifact con Visual Studio](#) nella AWS CodeArtifact Guida per l'utente di.

Amazon RDS da AWSEsploratore

Amazon Relational Database Service (Amazon RDS) è un servizio che consente di eseguire il provisioning e gestione dei sistemi di database relazionali SQL nel cloud. Amazon RDS supporta tre tipi di sistemi di database:

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

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

Molte delle funzionalità discusse qui sono disponibili anche attraverso il [AWS Console di gestione](#) per Amazon RDS.

Argomenti

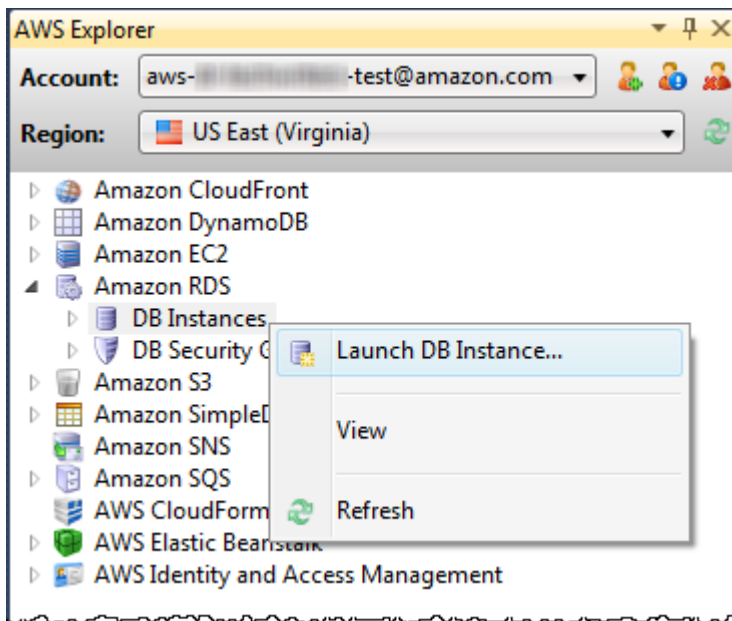
- [Selezione Avvia un'istanza di database Amazon RDS](#)
- [Creare un database Microsoft SQL Server in un'istanza RDS](#)
- [Gruppi di sicurezza Amazon RDS](#)

Selezione Avvia un'istanza di database Amazon RDS

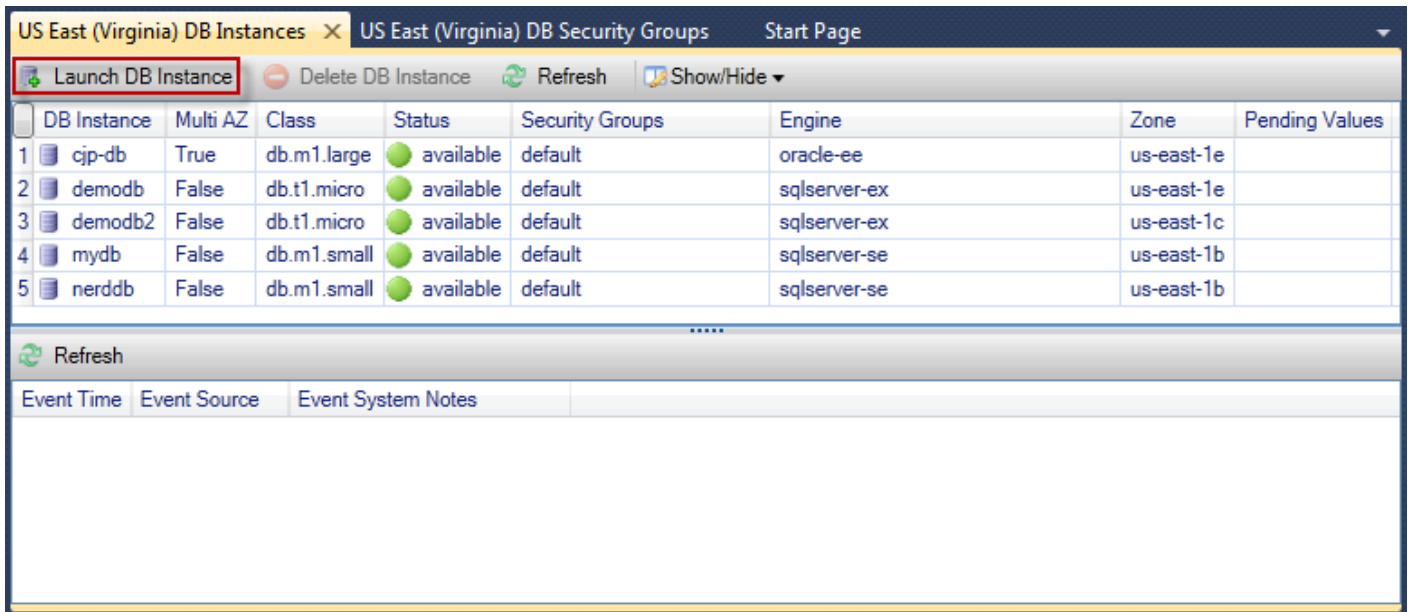
con AWS Explorer, puoi avviare un'istanza di uno dei motori di database supportati da Amazon RDS. La seguente procedura dettagliata mostra l'esperienza utente per l'avvio di un'istanza di Microsoft SQL Server Standard Edition, ma l'esperienza utente è simile per tutti i motori supportati.

Per avviare un'istanza Amazon RDS

1. Nello stato AWS Explorer, aprire il menu contestuale (tasto destro del mouse) per Amazon RDS nodo e scegli Selezione Avvia istanza database.



In alternativa, sull'istanza database tab, scegli Selezione Avvia istanza database.



US East (Virginia) DB Instances x US East (Virginia) DB Security Groups Start Page

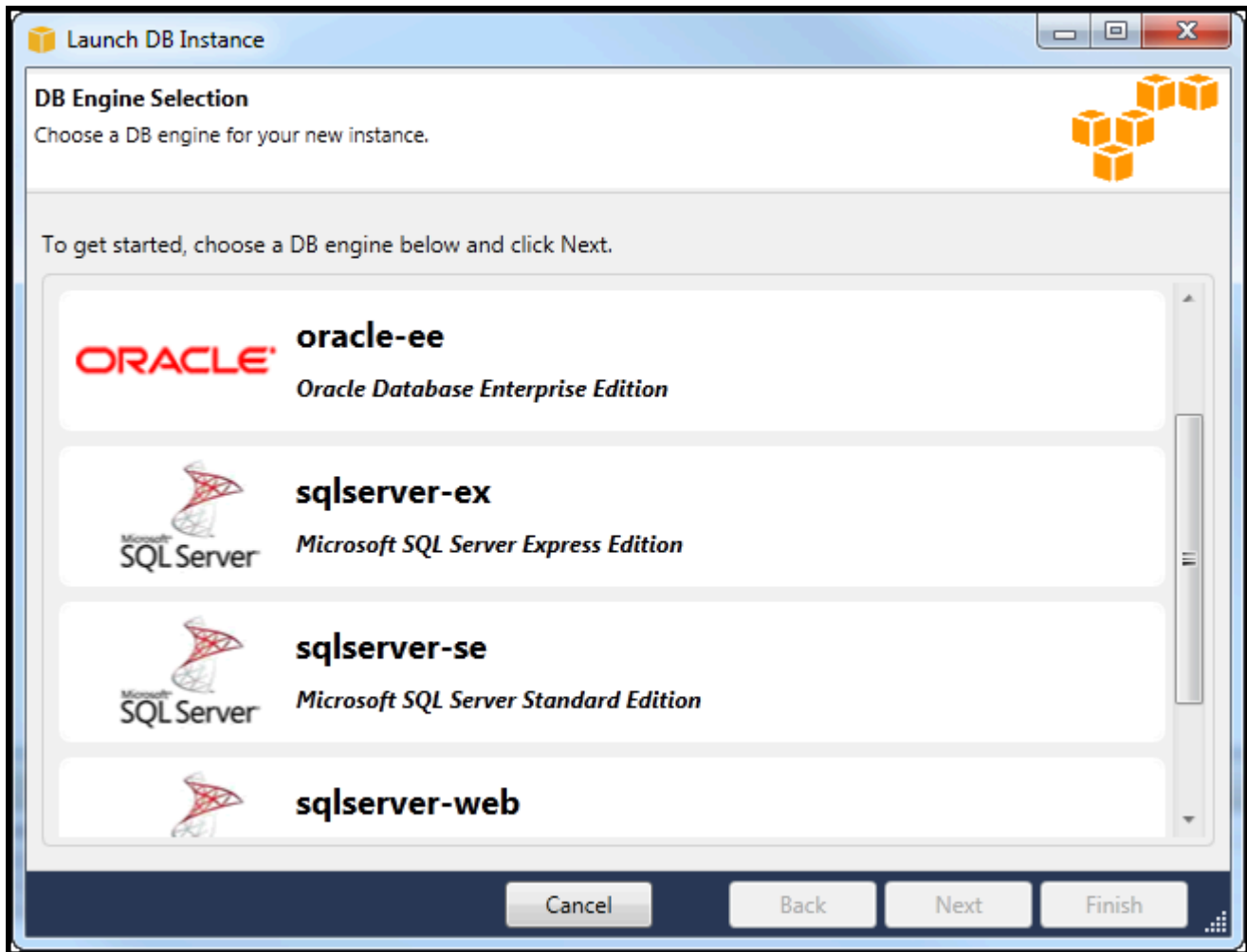
Launch DB Instance Delete DB Instance Refresh Show/Hide

	DB Instance	Multi AZ	Class	Status	Security Groups	Engine	Zone	Pending Values
1	cjp-db	True	db.m1.large	available	default	oracle-ee	us-east-1e	
2	demodb	False	db.t1.micro	available	default	sqlserver-ex	us-east-1e	
3	demodb2	False	db.t1.micro	available	default	sqlserver-ex	us-east-1c	
4	mydb	False	db.m1.small	available	default	sqlserver-se	us-east-1b	
5	nerddb	False	db.m1.small	available	default	sqlserver-se	us-east-1b	

Refresh

Event Time Event Source Event System Notes

2. Nella Selezione motore DB finestra di dialogo, selezionare il tipo di motore di database da avviare. Per questa procedura dettagliata, scegliere Microsoft SQL Server Standard Edition (sqlserver-se), quindi scegliere Successivo.



3. Nella Opzioni di istanza database Engine finestra di dialogo, selezionare opzioni di configurazione.

Nella Opzioni e classe dell'istanza di DB Engine (sezione), è possibile specificare le seguenti impostazioni.

License Model (Modello di licenza)

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

Il modello di licenza varia a seconda del tipo di motore di database. Licenza del tipo di motore Licenza Microsoft SQL Server inclusa nella licenza generale pubblica di MySQL Server Oracle bring-your-own-license

Versione dell'istanza DB

Scegliere la versione del motore di database che desideri utilizzare. Se è supportata una sola versione, questa viene selezionata per te.

Classe di istanza database

Scegliere la classe di istanza per il motore di database. I prezzi, ad esempio, le classi variano. Per ulteriori informazioni, consulta [Prezzi di Amazon RDS](#).

Esegui una distribuzione multi-AZ

Selezionare questa opzione per creare una distribuzione Multi-AZ per migliorare la durata e la disponibilità dei dati. Amazon RDS effettua il provisioning 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 per le distribuzioni Multi-AZ, consulta la sezione relativa ai prezzi della [Amazon RDS](#) pagina dei dettagli. Questa opzione non è supportata per Microsoft SQL Server.

Aggiorna automaticamente le versioni secondarie

Seleziona questa opzione per avere AWS eseguire automaticamente aggiornamenti di versione secondaria sulle istanze RDS per te.

Nella istanza di database RDS (sezione), è possibile specificare le seguenti impostazioni.

Allocated Storage (Storage allocato)

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

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

I minimi e i 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

DB Instance Identifier (Identificatore istanza database)

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

Master User Name (Nome utente master)

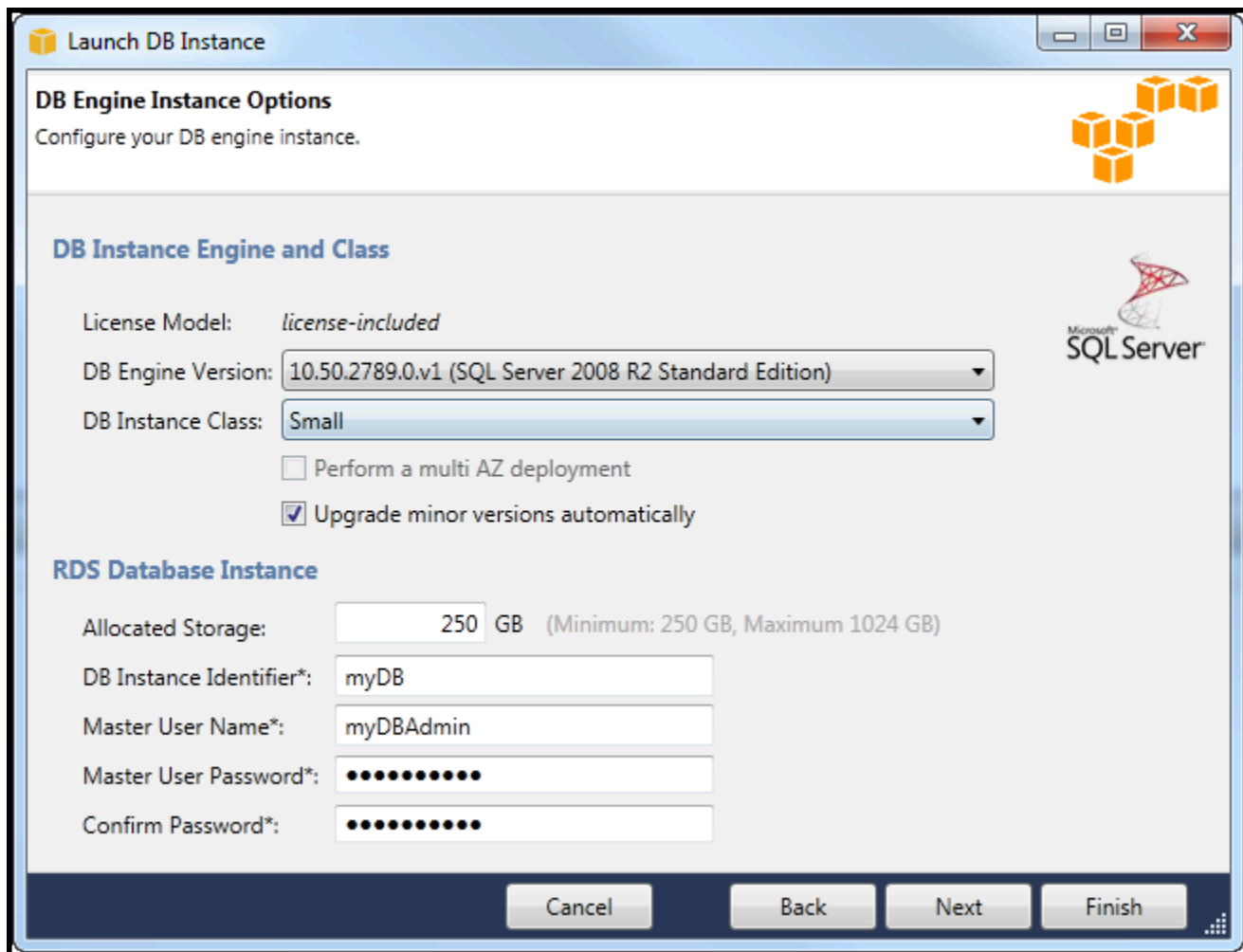
Digitare un nome per l'amministratore dell'istanza database.

Password utente master

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

Conferma la password

Digitare nuovamente la password per verificare che sia corretta.



1. Nella Opzioni aggiuntive finestra di dialogo, 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, impostare questo valore su una porta attraverso la quale il firewall consente il traffico.

Zona di disponibilità

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

Gruppo di sicurezza RDS

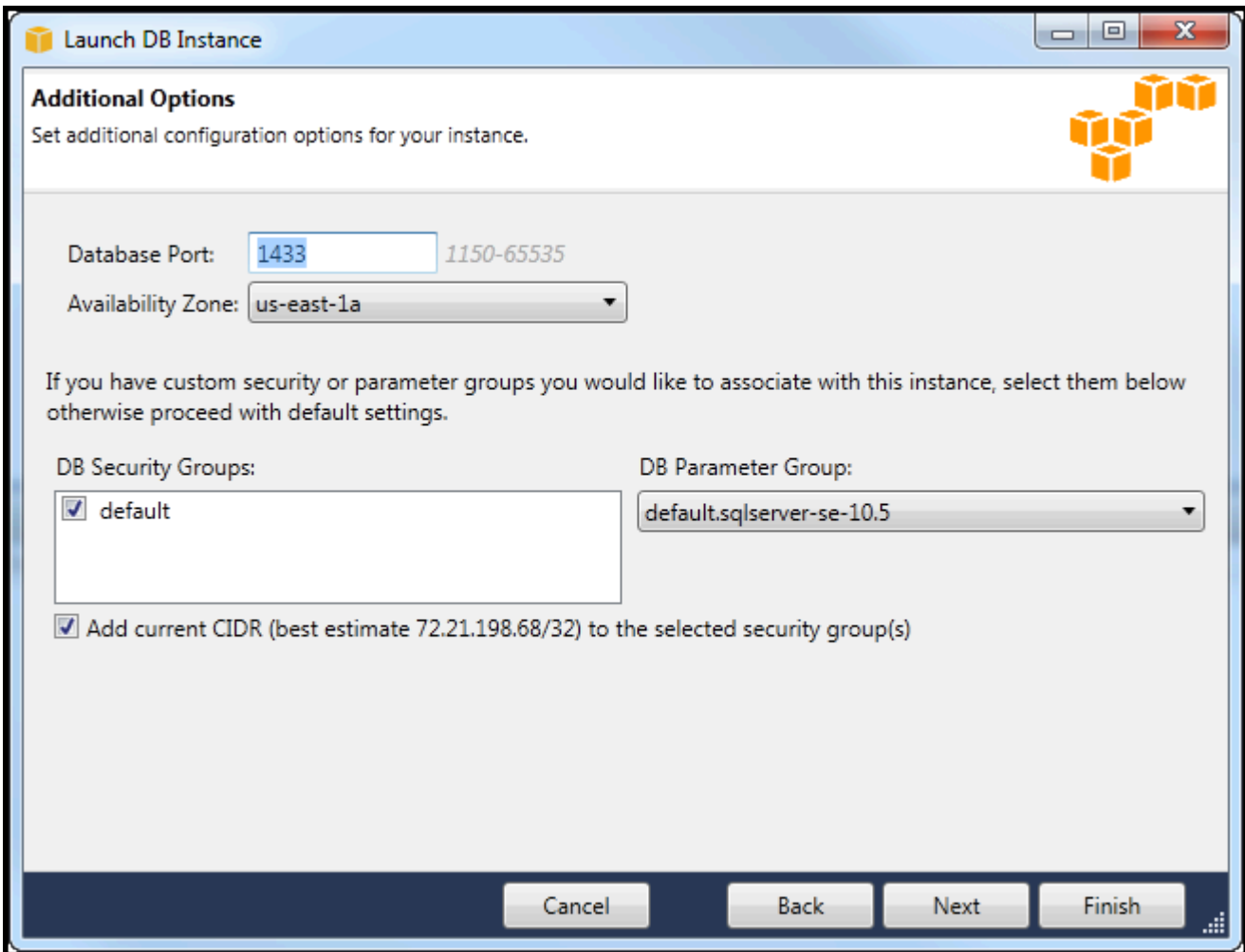
Seleziona un gruppo di sicurezza RDS o gruppi di sicurezza da associare all'istanza. I gruppi di sicurezza RDS specificano l'indirizzo IP, le istanze Amazon EC2 e Account AWS che è

consentito accedere alla tua istanza. Per ulteriori informazioni sui gruppi di sicurezza RDS, consulta [Gruppi di sicurezza Amazon RDS](#). Il Toolkit for Visual Studio tenta di determinare l'indirizzo IP corrente e fornisce 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 accurato. Per determinare quale indirizzo IP utilizzare, consultare l'amministratore di sistema.

DB Parameter Group (Gruppo di parametri database)

(Facoltativo) Da questo elenco a discesa, scegliere 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 [Guida per l'utente di Amazon Relational Database Service](#) e [questo articolo](#).

Quando sono state specificate le impostazioni in questa finestra di dialogo, scegliere **Successivo**.



Launch DB Instance

Additional Options
Set additional configuration options for your instance.

Database Port: 1150-65535

Availability Zone:

If you have custom security or parameter groups you would like to associate with this instance, select them below otherwise proceed with default settings.

DB Security Groups:

- default

DB Parameter Group:

Add current CIDR (best estimate 72.21.198.68/32) to the selected security group(s)

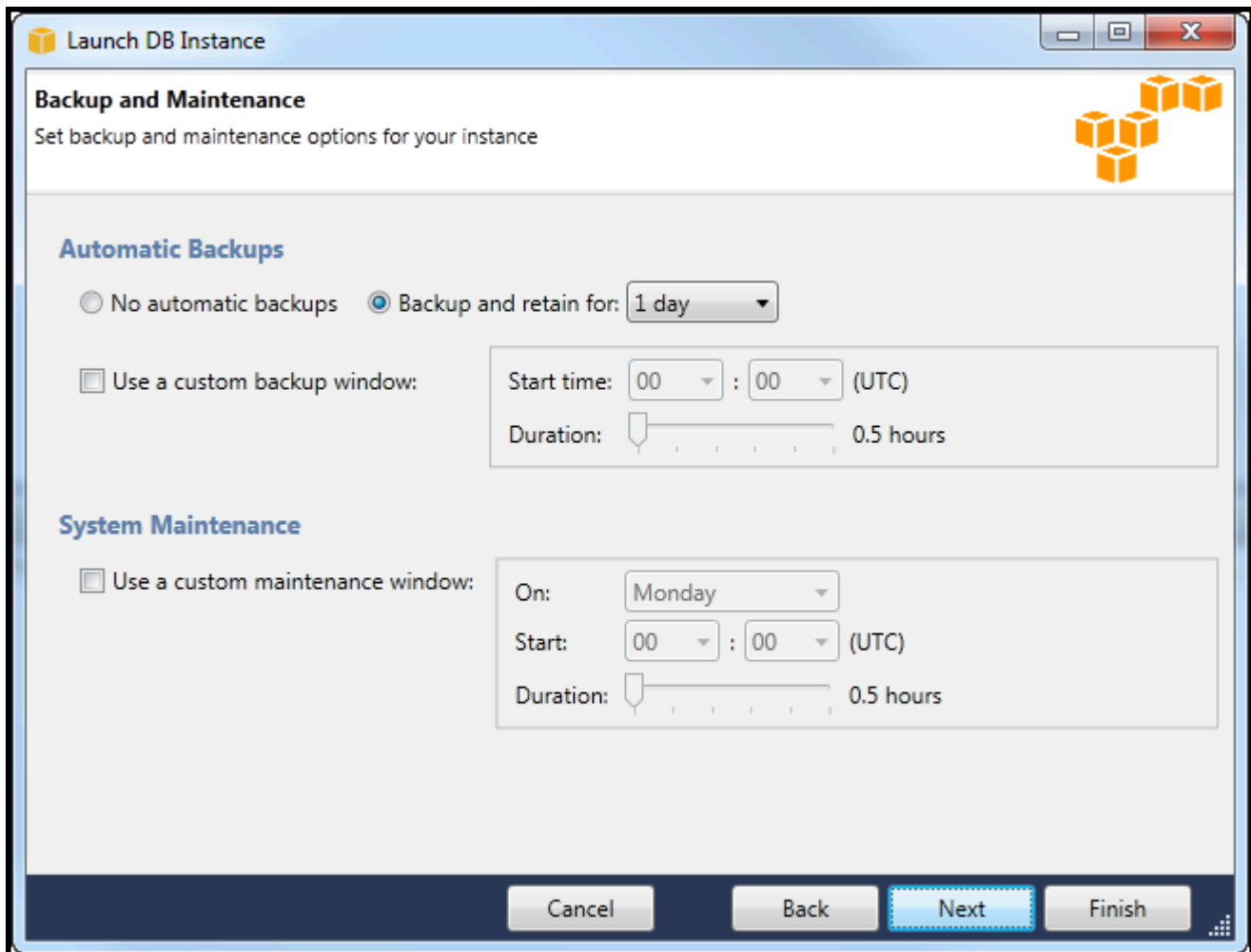
Cancel Back Next Finish

2. LaBackup e manutenzione la finestra di dialogo consente di specificare se Amazon RDS deve eseguire il backup dell'istanza e, in tal caso, per quanto tempo deve essere mantenuto il backup. È inoltre possibile specificare una finestra temporale durante la quale devono essere eseguiti i backup.

Questa finestra di dialogo consente inoltre di specificare se si desidera che Amazon RDS esegua la manutenzione del sistema sull'istanza. La manutenzione include patch di routine e aggiornamenti di versione secondaria.

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

Seleziona Next (Successivo).



3. La finestra di dialogo finale della procedura guidata consente di rivedere le impostazioni dell'istanza. Se devi modificare le impostazioni, usa l'Indietro pulsante. Se tutte le impostazioni sono corrette, scegli Avvio di.

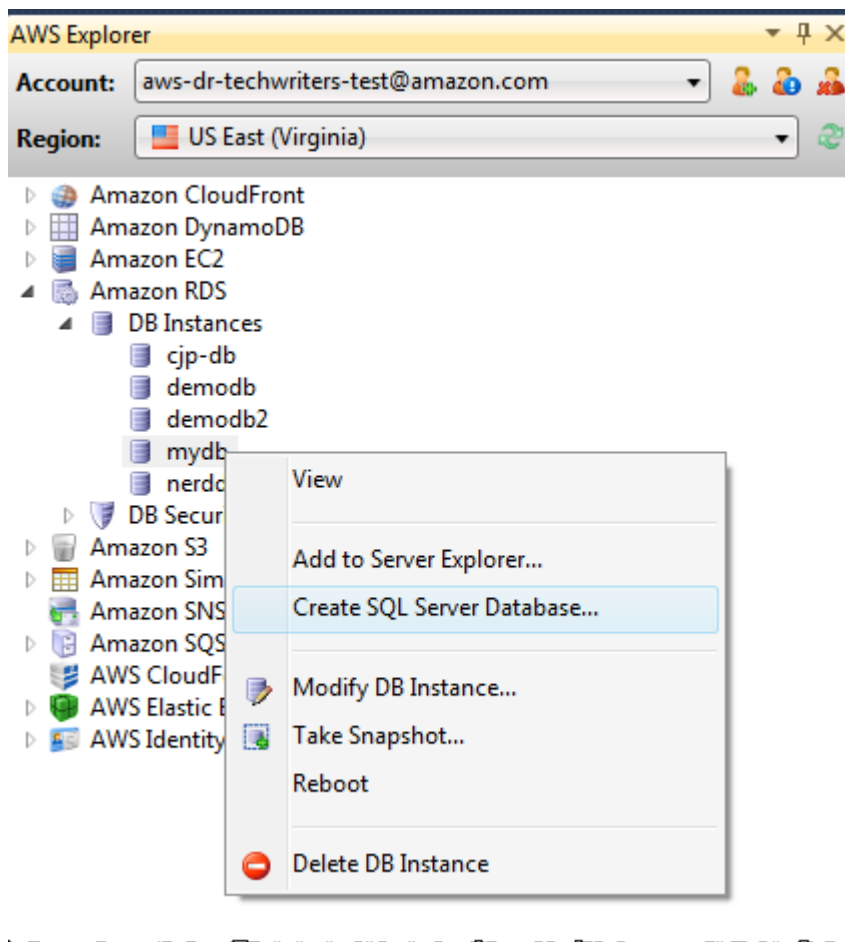
Creare un database Microsoft SQL Server in un'istanza RDS

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

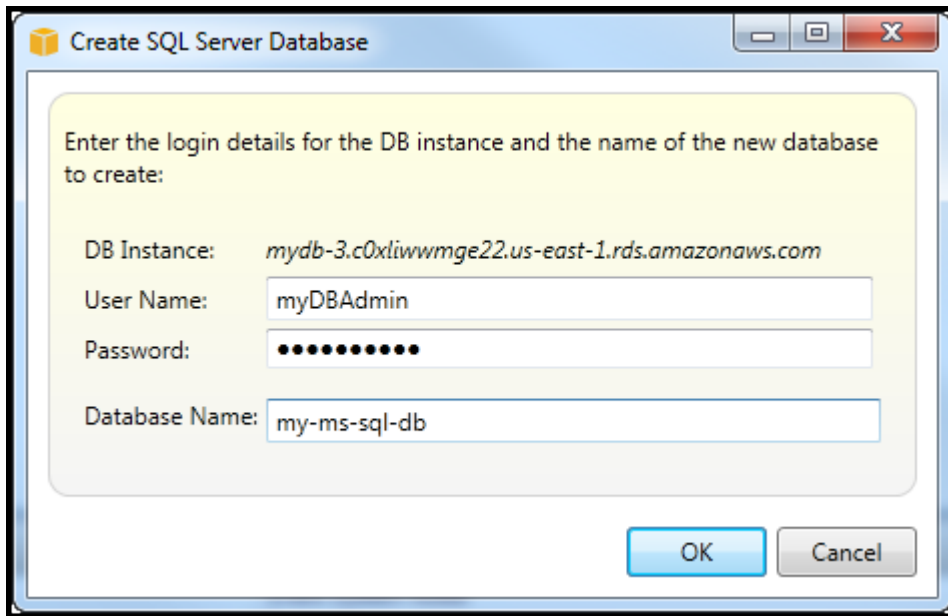
Per informazioni su come creare un'istanza Amazon RDS, consulta [Avvia un'istanza di database Amazon RDS](#).

Per la creazione di un database Microsoft SQL Server

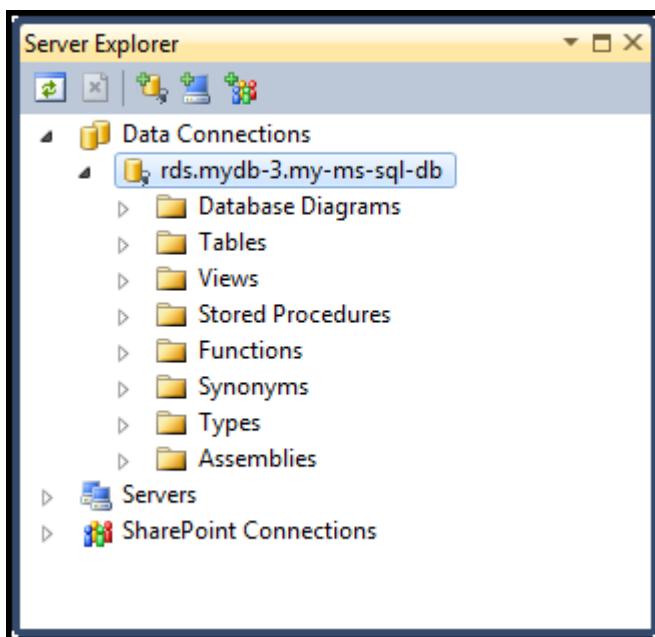
1. Nello stato AWSEsplora risorse, apri il menu contestuale (clic con il pulsante destro del mouse) per il nodo corrispondente all'istanza RDS per Microsoft SQL Server e scegliere **Creare database SQL Server**.



2. Nella **Creare database SQL Server** finestra di dialogo, digitare la password specificata al momento della creazione dell'istanza RDS, digitare un nome per il database di Microsoft SQL Server, quindi scegliere **OK**.



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



Gruppi di sicurezza Amazon RDS

I gruppi di sicurezza Amazon RDS ti consentono di gestire l'accesso alla 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 membri del gruppo di sicurezza EC2 sono quindi in grado di accedere alle istanze RDS membri del gruppo di sicurezza RDS.

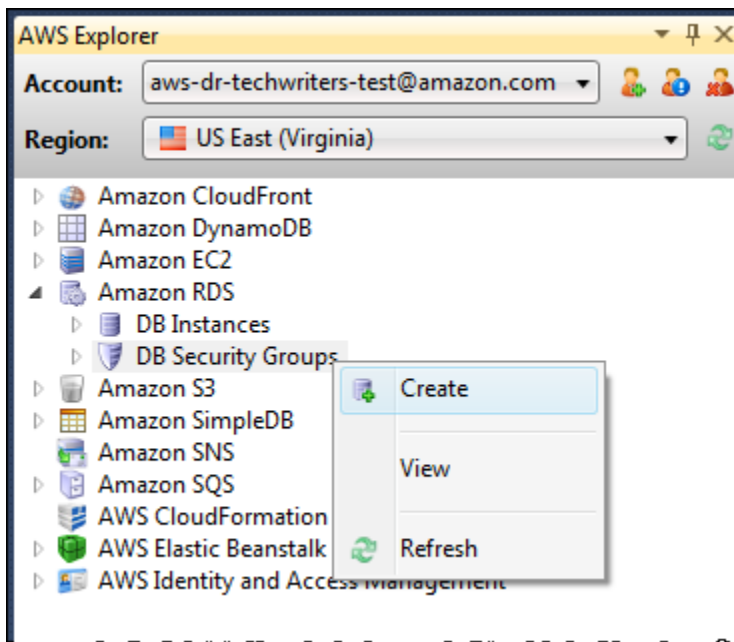
Per ulteriori informazioni sui gruppi di sicurezza Amazon RDS, consulta [Gruppi di sicurezza RDS](#). Per ulteriori informazioni sui gruppi di sicurezza Amazon EC2, consulta il sito [Guida per l'utente EC2](#).

Creazione di un gruppo di sicurezza Amazon RDS

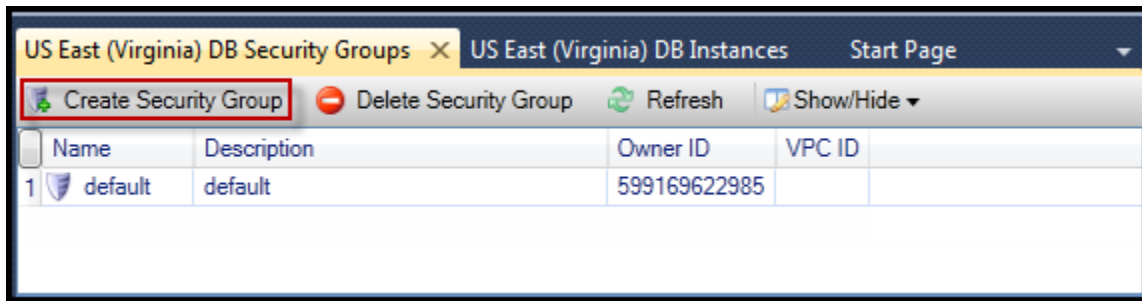
È possibile utilizzare Toolkit for Visual Studio per creare un gruppo di sicurezza RDS. Se utilizzi il plugin AWSToolkit per avviare un'istanza RDS, la procedura guidata consente di specificare un gruppo di sicurezza RDS da utilizzare con l'istanza. È possibile utilizzare la procedura seguente per creare un gruppo di sicurezza prima di avviare la procedura guidata.

Per creare un gruppo di sicurezza Amazon RDS

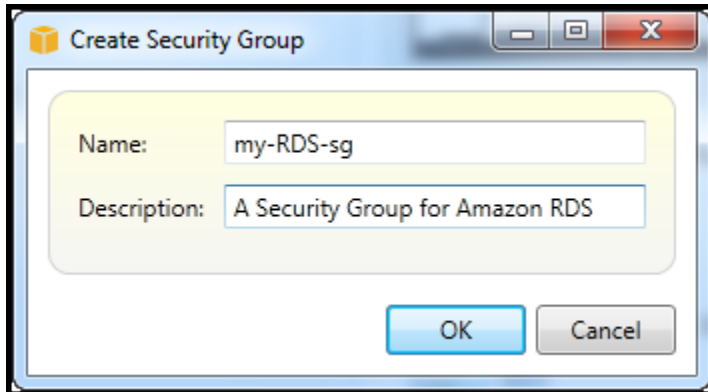
1. Nello stato AWSExplorer, espandi Amazon RDS nodo, aprire il menu contestuale (pulsante destro del mouse) per il Gruppi di sicurezza DB subnode e scegli Create.



In alternativa, sul Security Groups (Gruppi di sicurezza) scheda, scegli Creazione di gruppo di sicurezza. Se questa scheda non viene visualizzata, aprire il menu contestuale (pulsante destro del mouse) per la finestra di scelta rapida Gruppi di sicurezza DB subnode e scegli Visualizzazione.



2. Nella Creazione di gruppo di sicurezza finestra di dialogo, digitare un nome e una descrizione per il gruppo di sicurezza, quindi scegliere OK.



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

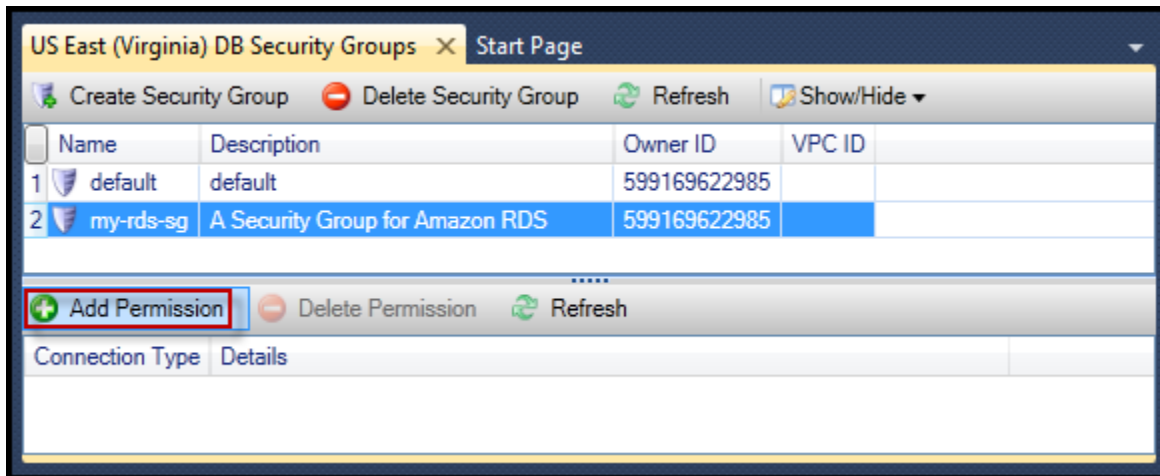
Per impostazione predefinita, un nuovo gruppo di sicurezza Amazon RDS non fornisce accesso alla rete. Per abilitare l'accesso alle istanze Amazon RDS che utilizzano il gruppo di sicurezza, utilizzare la procedura seguente per impostare le autorizzazioni di accesso.

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

1. Sul Security Groups (Gruppi di sicurezza) scheda, scegli il gruppo di sicurezza dalla vista elenco. Se il gruppo di sicurezza non viene visualizzato nell'elenco, scegli Aggiorna. Se il gruppo di sicurezza non viene ancora visualizzato nell'elenco, verificare di aver visualizzato l'elenco per il corretto AWS regione. Gruppo di sicurezza schede nel AWSI toolkit sono specifiche per regione.

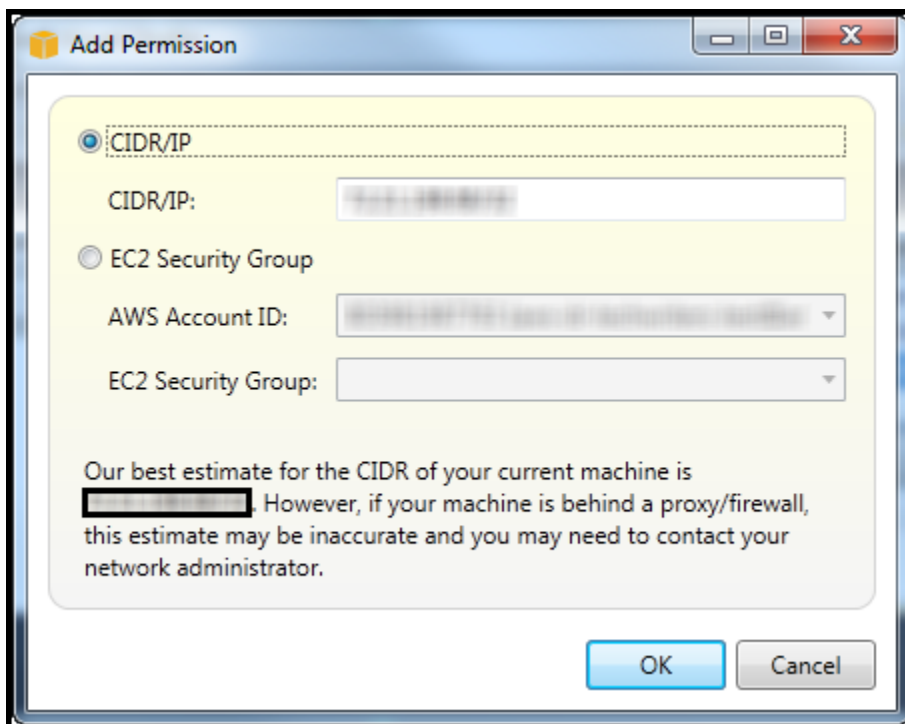
Se no Gruppo di sicurezza appaiono schede, in AWSExplorer, aprire il menu contestuale (pulsante destro del mouse) per il menu contestuale Gruppi di sicurezza DB subnode e scegli Visualizzazione.

2. Scegli Add Permission (Aggiungi autorizzazioni).



Aggiungi autorizzazione pulsante sul pulsante Security Groups (Gruppi di sicurezza) linguetta

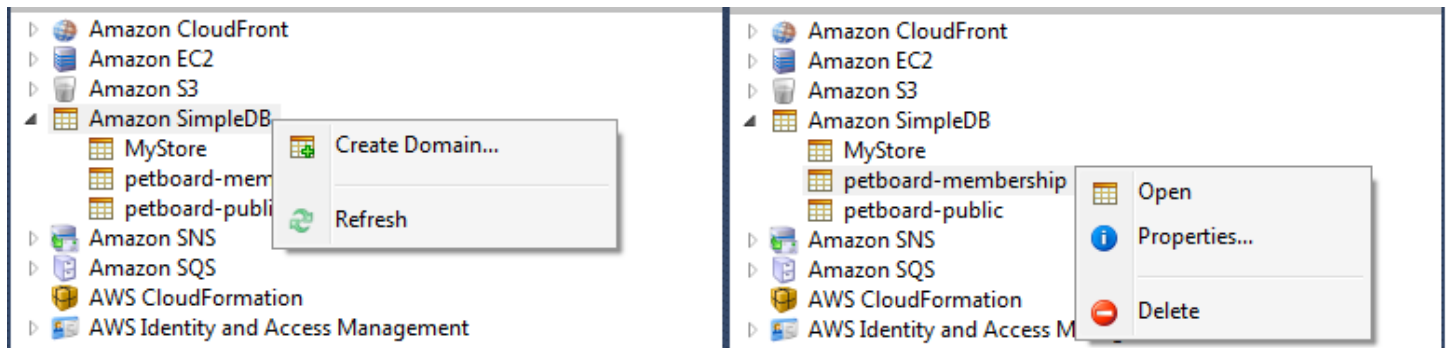
3. Nella Aggiungi autorizzazione finestra di dialogo, è possibile utilizzare la notazione CIDR per specificare quali indirizzi IP possono accedere all'istanza RDS oppure specificare quali gruppi di sicurezza EC2 possono accedere all'istanza RDS. Quando si sceglie Gruppo di sicurezza EC2, è possibile specificare l'accesso per tutte le istanze EC2 associate a un Account AWS avere accesso oppure è possibile scegliere un gruppo di sicurezza EC2 dall'elenco a discesa.



La AWS Toolkit tenta di determinare l'indirizzo IP e di compilare automaticamente la finestra di dialogo con la specifica CIDR appropriata. Tuttavia, se il computer accede a Internet tramite un firewall, il CIDR determinato dal Toolkit potrebbe non essere accurato.

Utilizzo di Amazon SimpleDB da AWSEsploratore

AWSEplorer visualizza tutti i domini Amazon SimpleDB associati all'attivo AWS conto. Da AWSEplorer, puoi creare o eliminare domini Amazon SimpleDB.



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

Esecuzione di query e modifica dei risultati

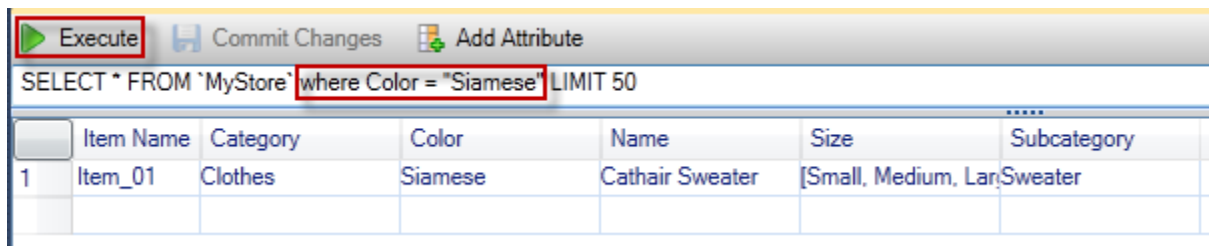
AWSEplorer può anche visualizzare una visualizzazione a griglia di un dominio Amazon SimpleDB da cui è possibile visualizzare gli elementi, gli attributi e i valori in quel dominio. Puoi eseguire query in modo che venga visualizzato solo un sottoinsieme di elementi del dominio. Facendo doppio clic su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

Il dominio visualizzato qui proviene dall'esempio Amazon SimpleDB incluso con il AWS SDK for .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 una query, modificare la query nella casella di testo nella parte superiore della vista griglia, quindi scegliere Execute. La vista viene filtrata per mostrare solo gli elementi che corrispondono alla query.

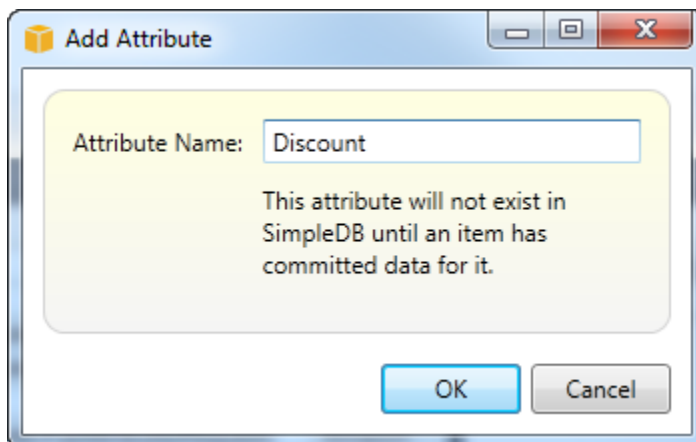


Execute query from AWS Explorer

Per modificare i valori associati a un attributo, fare doppio clic sulla cella corrispondente, modificare i valori e quindi scegliere Commit modifiche.

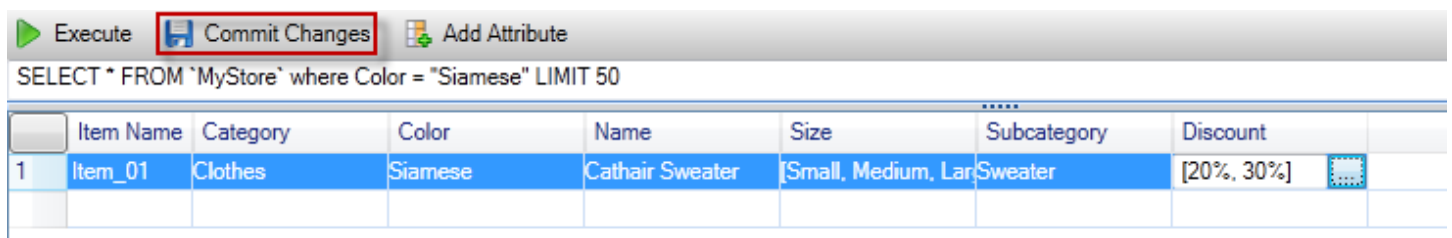
Aggiunta di un attributo

Per aggiungere un attributo, nella parte superiore della visualizzazione, scegli Add Attribute.



Add Attribute dialog box

Per rendere l'attributo parte del dominio, è necessario aggiungerlo ad almeno un elemento e quindi scegliere Commit modifiche.



Commit changes for a new attribute

Paginazione dei risultati della query

Nella parte inferiore della visualizzazione sono presenti tre pulsanti.



Paginate and export buttons

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

Esportazione in CSV

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

Utilizzo di Amazon SQSAWSEsploratore

Amazon Simple Queue Service (Amazon SQS) è un servizio di code flessibile che consente di passare messaggi tra diversi processi di esecuzione in un'applicazione software. Le code di Amazon SQS si trovano nellaAWSinfrastruttura, ma i processi che passano messaggi possono essere localizzati in locale, su istanze Amazon EC2 o su alcune combinazioni di questi. Amazon SQS è ideale per coordinare la distribuzione del lavoro su più computer.

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

Per maggiori informazioni su Amazon SQS, consulta la sezione [Introduzione a SQS](#) nellaAWSdocumentazione.

Creazione di una coda

Puoi creare una coda Amazon SQS daAWSExplorer. L'ARN e l'URL per la coda saranno basati sul numero di conto dell'account attivo e sul nome della coda specificato al momento della creazione.

Per creare una coda

1. Nello statoAWSExplorer, aprire il menu contestuale (pulsante destro del mouse) perAmazon SQSnodo, quindi scegliCREATE QUEUE.
2. NellaCREATE QUEUEfinestra di dialogo, specificare il nome della coda, il timeout di visibilità predefinito e il ritardo di consegna predefinito. Il timeout di visibilità predefinito e il ritardo di

consegna predefinito sono specificati in pochi 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 ha acquisito il messaggio. Il ritardo di recapito predefinito è la quantità di tempo dal momento in cui il messaggio viene inviato al momento in cui diventa visibile ai potenziali processi di ricezione.

3. Scegli OK. La nuova coda apparirà come sottonodo sotto ilAmazon SQSnodo.

Eliminazione di una coda

È possibile eliminare le code esistenti daAWSExplorer. Se si elimina una coda, i messaggi associati alla coda non sono più disponibili.

Per eliminare una coda

1. Nello statoAWSEsplora risorse, aprire i menu contestuali (pulsante destro del mouse) per la coda da eliminare e scegliereElimina.

Gestione delle proprietà della coda

È possibile visualizzare e modificare le proprietà di una qualsiasi delle code visualizzate inAWSExplorer. Puoi anche inviare messaggi alla coda da questa vista delle proprietà.

Per gestire le proprietà della coda

- Nello statoAWSExplorer, aprire il menu contestuale (pulsante destro del mouse) per la coda di cui si desidera gestire le proprietà e scegliereVisualizzare la coda.

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

Save Send Refresh

Visibility timeout (Seconds): Created timestamp: 10/20/2011 1:34:49 PM

Maximum message size (Bytes): Last modified timestamp: 10/20/2011 1:34:49 PM

Message retention period (Seconds): Number of messages: 0


Default Delivery Delay (Seconds): Number of messages not visible: 0

Queue ARN: arn:aws:sqs:us-east-1: :my-tk-queue

Queue URL: https://queue.amazonaws.com/ /my-tk-queue

Message Sampling

Message Id	Message Body	Sender Id	Sent

 Changes can take up to 60 seconds to propagate throughout the SQS system.

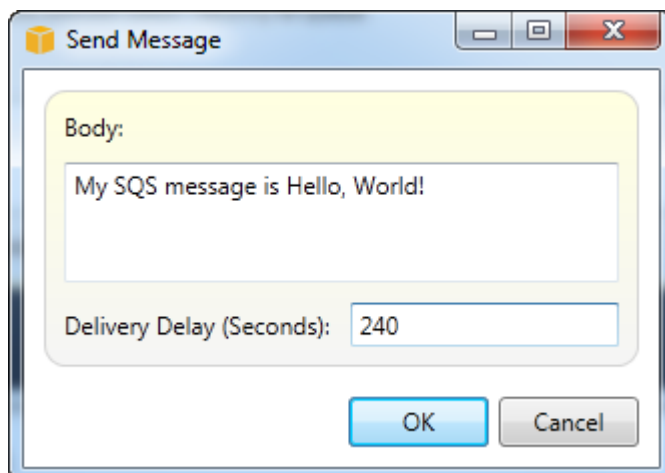
SQS queue properties view

Invio di un messaggio a una coda

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

Per inviare un messaggio

1. Nella parte superiore della vista delle proprietà della coda, scegliere **Invia**.
2. Digita il messaggio. (Facoltativo) Inserire un ritardo di consegna che sostituirà il ritardo di consegna predefinito per la coda. Nell'esempio seguente, abbiamo sovrascritto il ritardo con un valore di 240 secondi. Scegli **OK**.



Inviare messaggio dialog box

3. Attendere circa 240 secondi (quattro minuti). Il messaggio apparirà nella **Campionamento dei messaggi** della vista delle proprietà della coda.

Save Send Refresh

Visibility timeout (Seconds): Created timestamp: 10/20/2011 1:34:49 PM

Maximum message size (Bytes): Last modified timestamp: 10/20/2011 1:34:49 PM

Message retention period (Seconds): Number of messages: 1

Default Delivery Delay (Seconds): Number of messages not visible: 0

Queue ARN: `arn:aws:sqs:us-east-1:XXXXXXXXXX:my-tk-queue`

Queue URL: `https://queue.amazonaws.com/XXXXXXXXXX/my-tk-queue`

Message Sampling

Message Id	Message Body	Sender Id	Sent
d58475df-2f92-49ec-a400-957bafcc5daf	My SQS message is Hello, World!	XXXXXXXXXX	10/20/2011 2:33:02 PM

⚠ Changes can take up to 60 seconds to propagate throughout the SQS system.

SQS properties view with sent message

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

Identity and Access Management

AWS Identity and Access Management(IAM) consente di gestire in modo più sicuro l'accesso al tuo Account AWS e risorse. Con IAM, puoi creare più utenti nel tuo primario (radice) Account AWS. Questi utenti possono avere le proprie credenziali: password, ID chiave di accesso e chiave segreta, ma tutti gli utenti IAM condividono un singolo numero di account.

È possibile gestire il livello di accesso alle risorse di ciascun utente IAM collegando le policy IAM all'utente. Ad esempio, puoi allegare una policy a un utente IAM che dà all'utente l'accesso al servizio Amazon S3 e alle risorse correlate nel tuo account, ma che non fornisce accesso a nessun altro servizio o risorsa.

Per una gestione degli accessi più efficiente, puoi creare gruppi IAM, ovvero raccolte di utenti. Quando allegati un criterio al gruppo, ciò influirà su tutti gli utenti membri 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, è possibile associare criteri ai ruoli IAM. Quindi, puoi associare il ruolo IAM a un'istanza Amazon EC2. Le applicazioni che vengono 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 [Creare un ruolo IAM](#). Per ulteriori informazioni su IAM, consulta [IAM User Guide](#).

Creazione e configurazione di un utente IAM

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

Come best practice, tutti gli utenti che accedono a Account AWS dovrebbe farlo come utenti IAM, anche il proprietario dell'account. In questo modo, se le credenziali per uno degli utenti IAM sono compromesse, è possibile disattivare solo queste credenziali. Non è necessario disattivare o modificare le credenziali root per l'account.

Dal Toolkit for Visual Studio, è possibile assegnare le autorizzazioni a un utente IAM collegando una policy IAM all'utente o assegna l'utente a un gruppo. Gli utenti IAM assegnati a un gruppo ricavano le proprie autorizzazioni dalle policy collegate 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 generare anche AWS Le credenziali (ID chiave di accesso e chiave segreta) per l'utente IAM. Per ulteriori informazioni, consulta [Creazione di credenziali per un utente IAM](#)

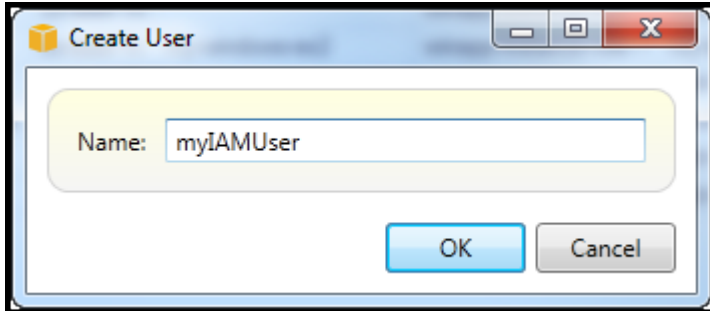


Toolkit for Visual Studio supporta la specifica delle credenziali utente IAM per l'accesso ai servizi tramite AWS Explorer. Poiché gli utenti IAM in genere non hanno accesso completo a tutti i Amazon Web Services, alcune funzionalità in AWS Explorer potrebbe non essere disponibile. Se utilizzi AWS Explorer per modificare le risorse mentre l'account attivo è un utente IAM e quindi passare l'account attivo all'account root, le modifiche potrebbero non essere visibili fino a quando non si aggiorna la vista in AWS Explorer. Per aggiornare la vista, scegliere il pulsante refresh () ().

Per informazioni su come configurare gli utenti IAM dalla AWS Management Console, vai a [Utilizzo di utenti e gruppi](#) nella Guida per l'utente di IAM.

Per creare un utente IAM

1. Nello statoAWS Explorer, espandi ilAWS Identity and Access Managementnodo, aprire il menu contestuale (tasto destro del mouse) perUtentiQuindi scegliCreazione dell'utente.
2. NellaCreazione dell'utentefinestra di dialogo, digitare un nome per l'utente IAM e scegliereOK. Questo è l'IAM[nome amichevole](#). Per informazioni sui vincoli sui nomi per gli utenti IAM, consulta laIAM [User Guide](#).



Create an IAM user

Il nuovo utente verrà visualizzato come un nodo secondario inUtentisottoAWS Identity and Access Managementnodo.

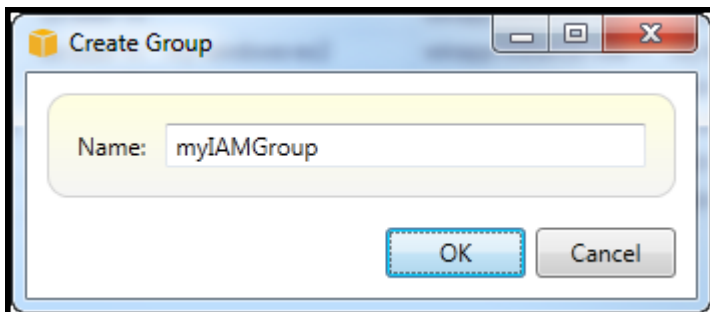
Per informazioni su come creare una policy e collegarla all'utente, consulta[Creare una policy IAM](#).

Creazione di un gruppo IAM

I gruppi forniscono un modo per applicare i criteri IAM a una raccolta di utenti. Per informazioni su come gestire gli utenti e i gruppi IAM, consulta[Utilizzo di utenti e gruppi](#) nella Guida per l'utente di IAM.

Per creare un gruppo IAM

1. Nello statoAWS Explorer, inIdentity and Access Management, aprire il menu contestuale (tasto destro del mouse) perGruppie scegliere crea gruppo.
2. Nellacrea grupppfinestra di dialogo, digitare un nome per il gruppo IAM e scegliereOK.



Create IAM group

Il nuovo gruppo IAM apparirà sotto il Gruppisottonodo di Identity and Access Management.

Per informazioni su come creare una policy e collegarla al gruppo IAM, consulta [Creare una policy IAM](#).

Aggiunta di un utente IAM a un gruppo IAM

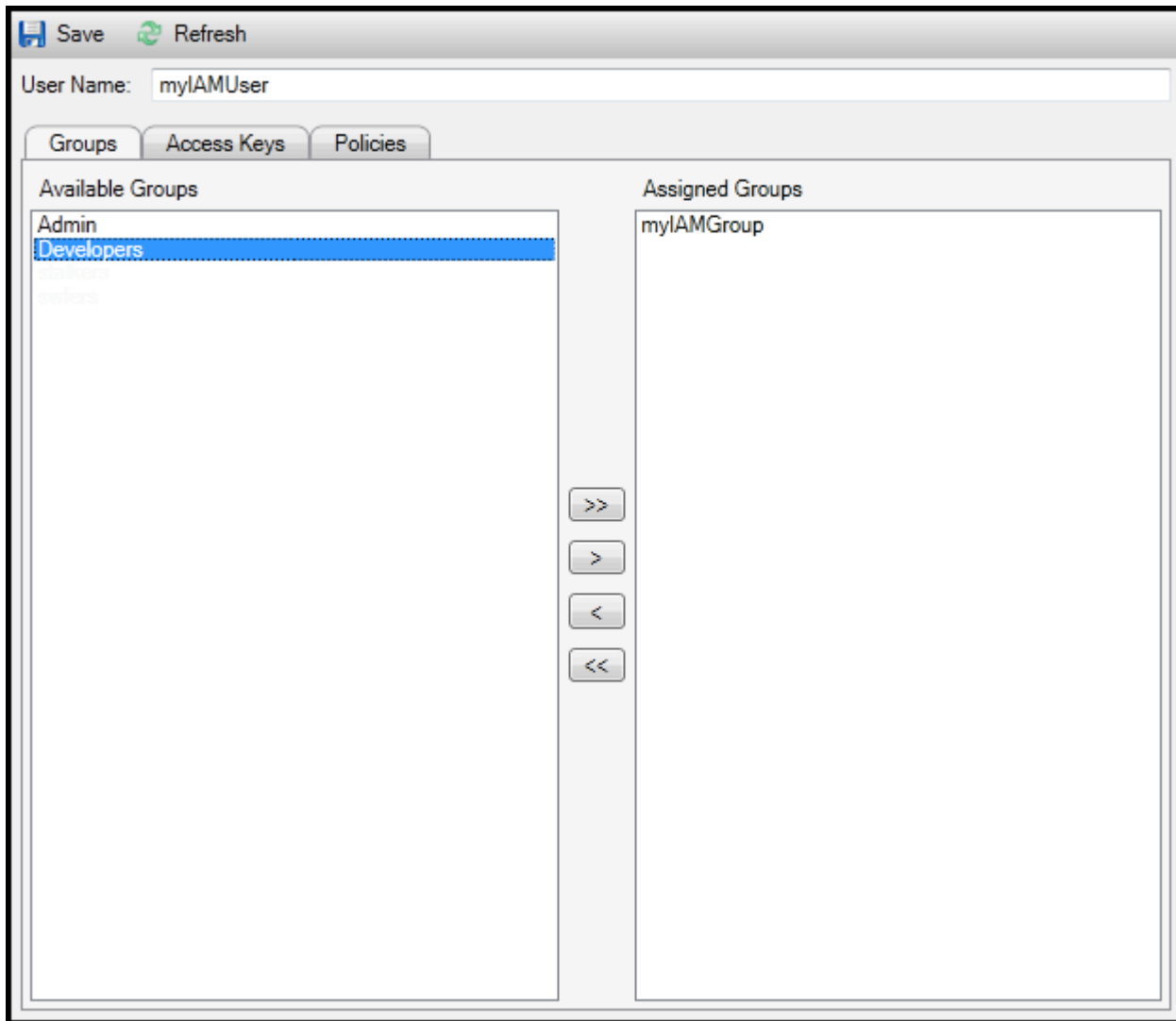
Gli utenti IAM membri di un gruppo IAM ricavano le autorizzazioni di accesso dalle policy collegate al gruppo. Lo scopo di un gruppo IAM è semplificare la gestione delle autorizzazioni per una raccolta di utenti IAM.

Per informazioni su come le policy associate a un gruppo IAM interagiscono con le policy associate agli utenti IAM membri di quel gruppo IAM, visitare [Gestione di policy IAM nella Guida per l'utente di IAM](#).

Nello stato AWSExplorer, puoi aggiungere gli utenti IAM ai gruppi IAM dalla Utentisubnode, non il Gruppisottonodo.

Per aggiungere un utente IAM a un gruppo IAM

1. Nello stato AWSExplorer, in Identity and Access Management, aprire il menu contestuale (tasto destro del mouse) per l'utente e scegliere Modificare.



Assign an IAM user to a IAM group

- Il riquadro di sinistra della Gruppischeda visualizza i gruppi IAM disponibili. Nel riquadro destro vengono visualizzati 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 e scegli il >.

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

Per aggiungere l'utente IAM a tutti i gruppi IAM, scegliere il >>. Analogamente, per rimuovere l'utente IAM da tutti i gruppi, scegliere il <<.

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

- Al termine dell'assegnazione dell'utente IAM ai gruppi IAM, scegliere Save (Salva).

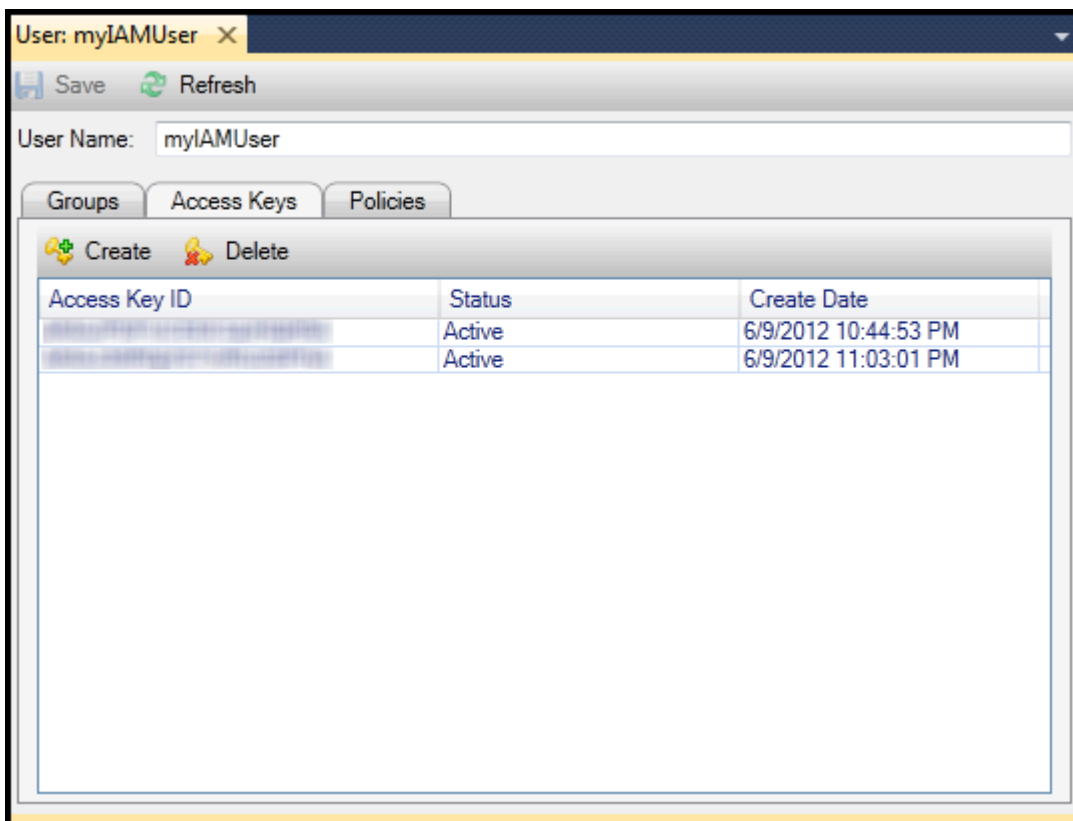
Creazione di credenziali per un utente IAM

Con Toolkit for Visual Studio, è possibile generare l'ID chiave di accesso e la chiave segreta utilizzata per effettuare chiamate API a AWS. Queste chiavi possono anche essere specificate per accedere ad Amazon Web Services tramite il Toolkit. Per ulteriori informazioni su come specificare le credenziali per l'uso con il Toolkit, consulta [creds \(creds\)](#). Per ulteriori informazioni su come gestire in modo sicuro le credenziali, consulta [Best practice per la gestione AWS Chiavi di accesso](#).

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

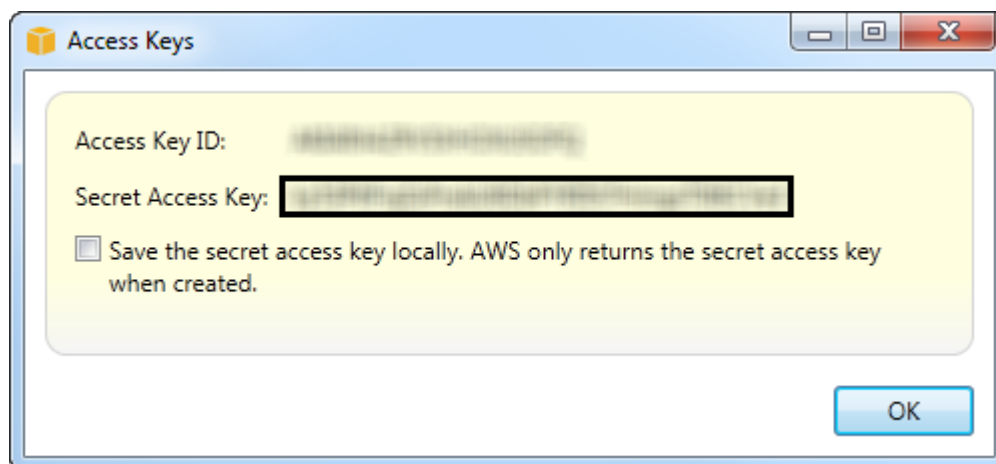
Per generare credenziali per un utente IAM

1. Nello stato **AWSEsplora risorse**, aprire il menu contestuale (clic con il pulsante destro del mouse) per un utente IAM e scegliere **Modificare**.



2. Per generare credenziali, sul **Chiavi di accesso** tab, scegli **Create**.

Puoi generare solo due set di credenziali per ogni utente IAM. Se hai già due set di credenziali e devi creare un set aggiuntivo, dovrai eliminare uno dei set esistenti.

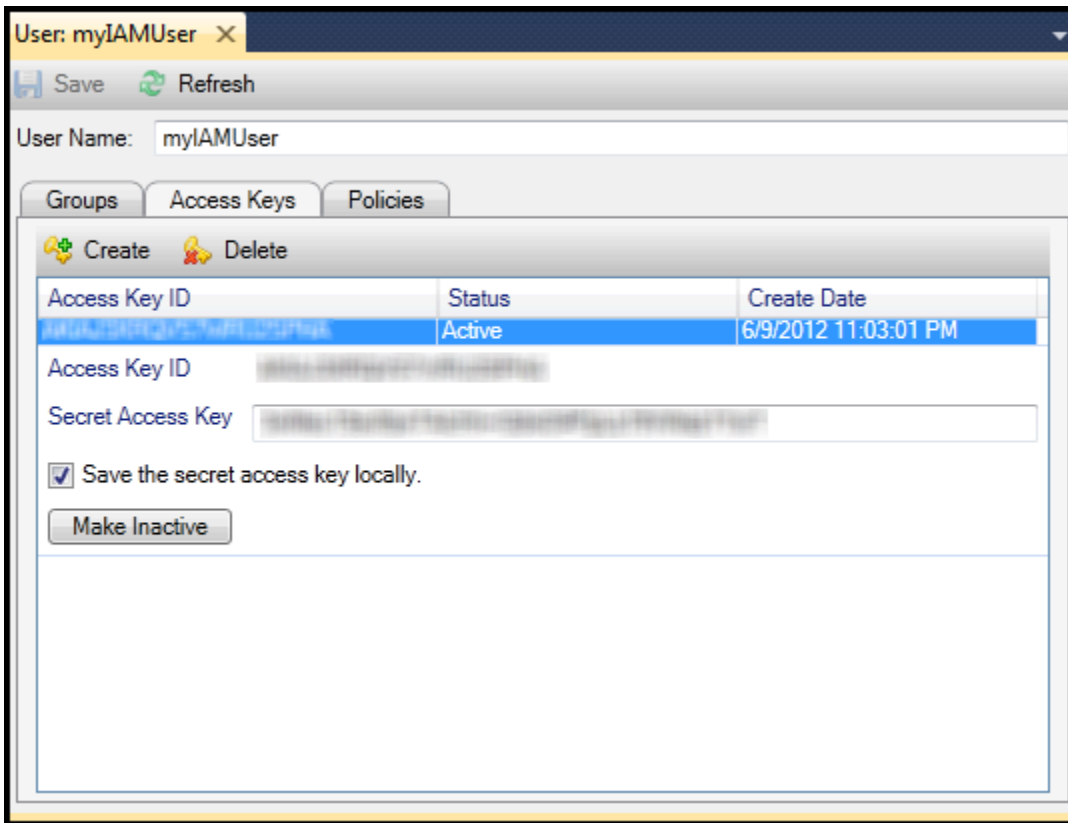


reate credentials for IAM user

Se vuoi che il Toolkit salvi una copia crittografata della chiave di accesso segreta nell'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 avere generato le credenziali, puoi visualizzarle dalla **Chiavi di accesso** scheda. 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 anche il Toolkit la salvasse, nel Secret Access Key (Chiave di accesso segreta) box, digita la chiave di accesso segreta, quindi seleziona Salva la chiave di accesso segreta localmente.

Per disattivare le credenziali, scegli Make Inactive (Rendi inattiva). (Potresti farlo se sospetti che le credenziali siano state compromesse. Puoi riattivare le credenziali se ricevi una garanzia che siano protette.)

Creare un ruolo IAM

Toolkit for Visual Studio supporta la creazione e la configurazione dei ruoli IAM. Proprio come per utenti e gruppi, è possibile associare criteri ai ruoli IAM. Quindi, puoi associare il ruolo IAM a un'istanza Amazon EC2. L'associazione con l'istanza EC2 viene gestita tramite un profilo dell'istanza, un contenitore logico per il ruolo. Le applicazioni eseguite sull'istanza EC2 ricevono automaticamente il livello di accesso specificato dal criterio associato al ruolo IAM. Ciò è vero anche quando l'applicazione non ne ha specificato altre AWS credenziali.

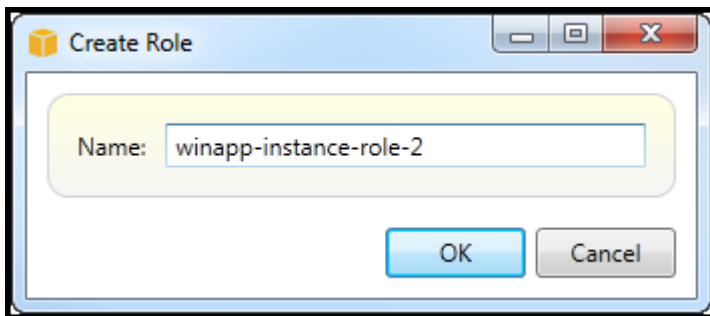
Ad esempio, puoi creare un ruolo e collegare una policy a tale ruolo per limitare l'accesso solo ad Amazon S3. Dopo aver associato questo ruolo a un'istanza EC2, è possibile eseguire un'applicazione

su tale 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 credenziali sull'istanza EC2.

Per ulteriori informazioni sui ruoli IAM, consulta [Gestione di ruoli IAM nella Guida per l'utente di IAM](#). Per esempi di programmi che accedono a AWS utilizzando il ruolo IAM associato a un'istanza Amazon EC2, vai alla [AWS Guide per gli sviluppatori](#) [Java](#), [.NET](#), [PHP](#), e Ruby ([Impostazione delle credenziali utilizzando IAM](#), [Creazione di un ruolo IAM](#), e [Lavorare con le policy IAM](#)).

Per creare un ruolo IAM

1. Nello stato **AWSExplorer**, in **Identity and Access Management**, aprire il menu contestuale (tasto destro del mouse) per **Ruoli**. Quindi scegliere **Creazione di ruoli**.
2. Nella **crea ruolo** finestra di dialogo, digitare un nome per il ruolo IAM e scegliere **OK**.



Create IAM role

Il nuovo ruolo IAM apparirà sotto **Ruoli** in **Identity and Access Management**.

Per informazioni su come creare una policy e collegarla al ruolo, consulta [Creare una policy IAM](#).

Creare una policy IAM

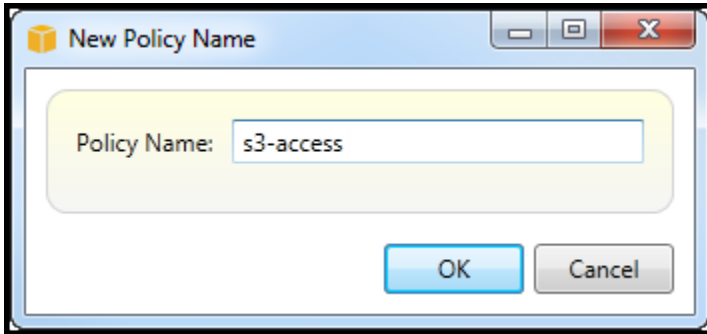
Le politiche sono fondamentali per IAM. Le policy possono essere associate a **entità** come utenti, gruppi o ruoli. Le policy specificano il livello di accesso abilitato per un utente, un gruppo o un ruolo.

Per creare una policy IAM

Nello stato **AWSExplorer**, espandi il **AWS Identity and Access Management** nodo, quindi espandere il nodo per il tipo di entità (**Gruppi**, **Ruoli**, oppure **Utenti**) a cui allegherai la politica. Ad esempio, apri un menu contestuale per un ruolo IAM e scegli **Modificare**.

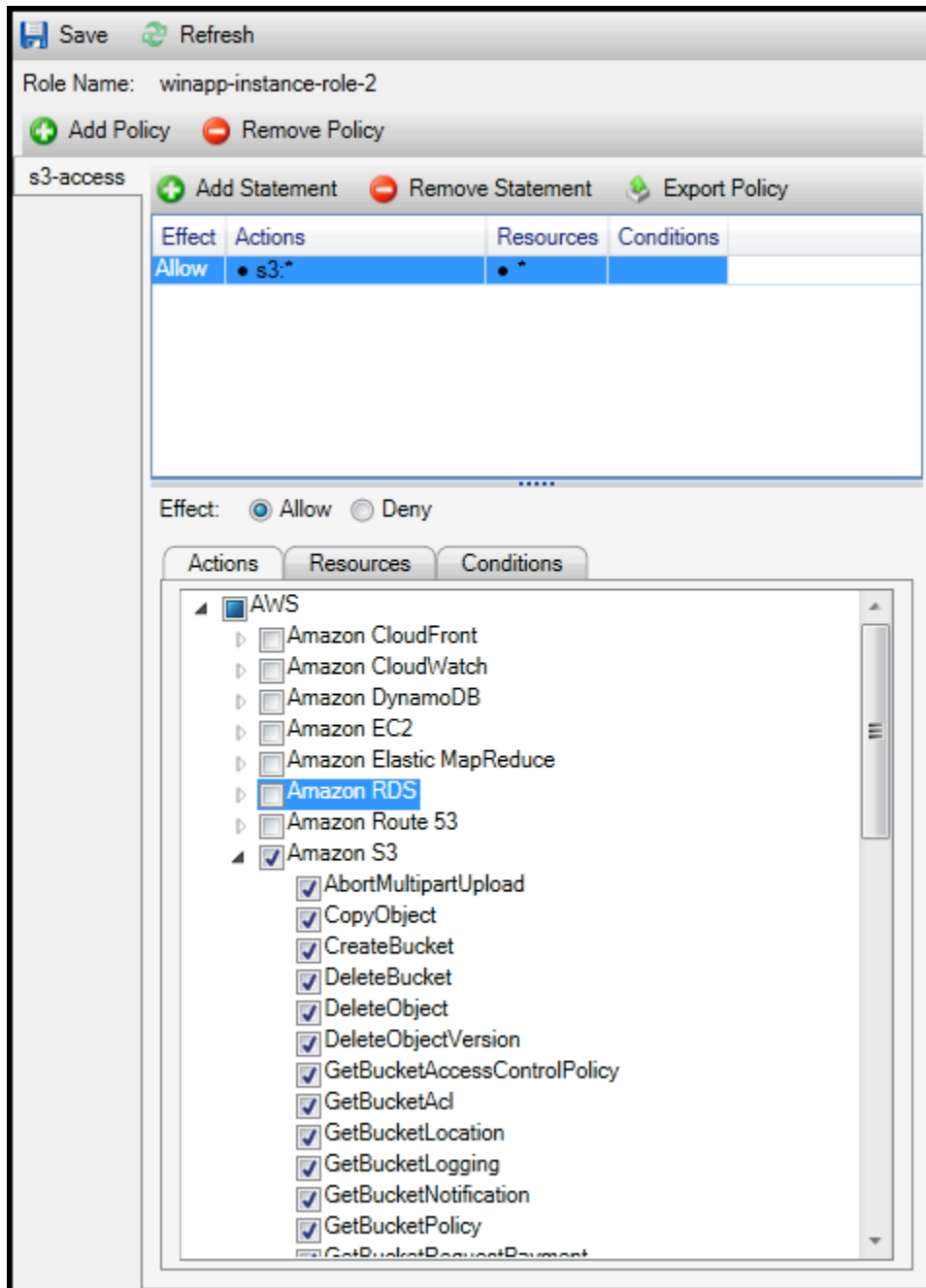
Una scheda associata al ruolo apparirà nel **AWSExplorer**. Seleziona **aggiungi policy link**.

Nella Nuova policy digitare un nome per la policy (ad esempio s3-access).



New Policy Name dialog box

Nell'editor dei criteri, aggiungere istruzioni per specificare il livello di accesso da fornire al ruolo (in questo esempio, winapp-instance-role-2 associato al criterio. 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 dei criteri per consentire o impedire le azioni associate ad Amazon Web Services.

Dopo aver modificato il criterio, scegli il **Save (Salva)** link.

AWS Lambda

Sviluppa e distribuisce 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](#)
- [AWS Lambda Progetto di base per la creazione di un'immagine Docker](#)
- [Tutorial: crea e testa un'applicazione serverless con AWS Lambda](#)
- [Tutorial: creazione di un'applicazione Amazon Rekognition Lambda](#)
- [Tutorial: Utilizzo di Amazon Logging Frameworks AWS Lambda per creare log di applicazioni](#)

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'insieme, 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.",
```

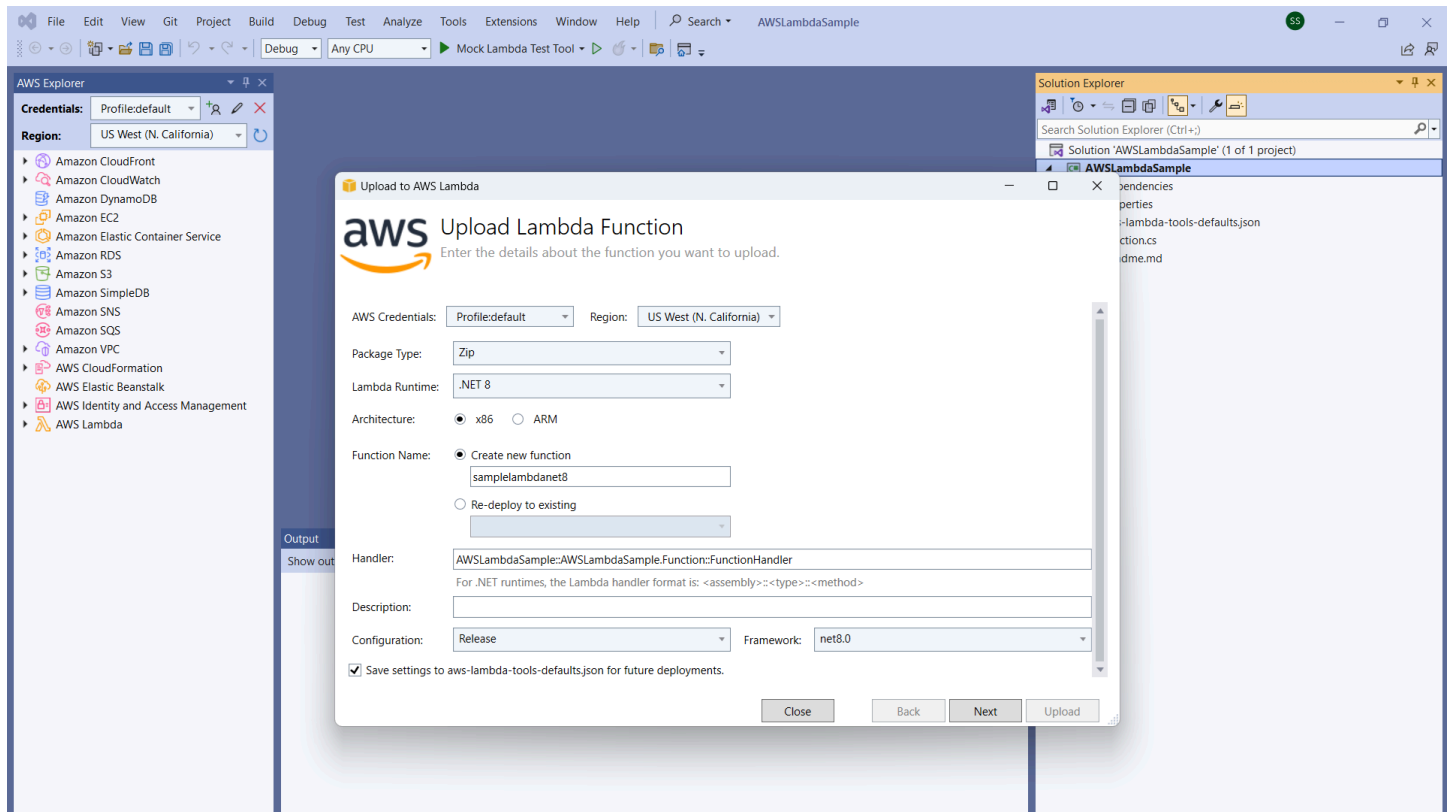
```
"dotnet lambda help",
  "All the command line options for the Lambda command can be specified in this
file."
],
"profile": "default",
"region": "us-west-2",
"configuration": "Release",
"function-architecture": "x86_64",
"function-runtime": "dotnet8",
"function-memory-size": 512,
"function-timeout":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



Publicazione 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 il display **AWS Management Console**.

- 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 AWS Management Console
 - 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

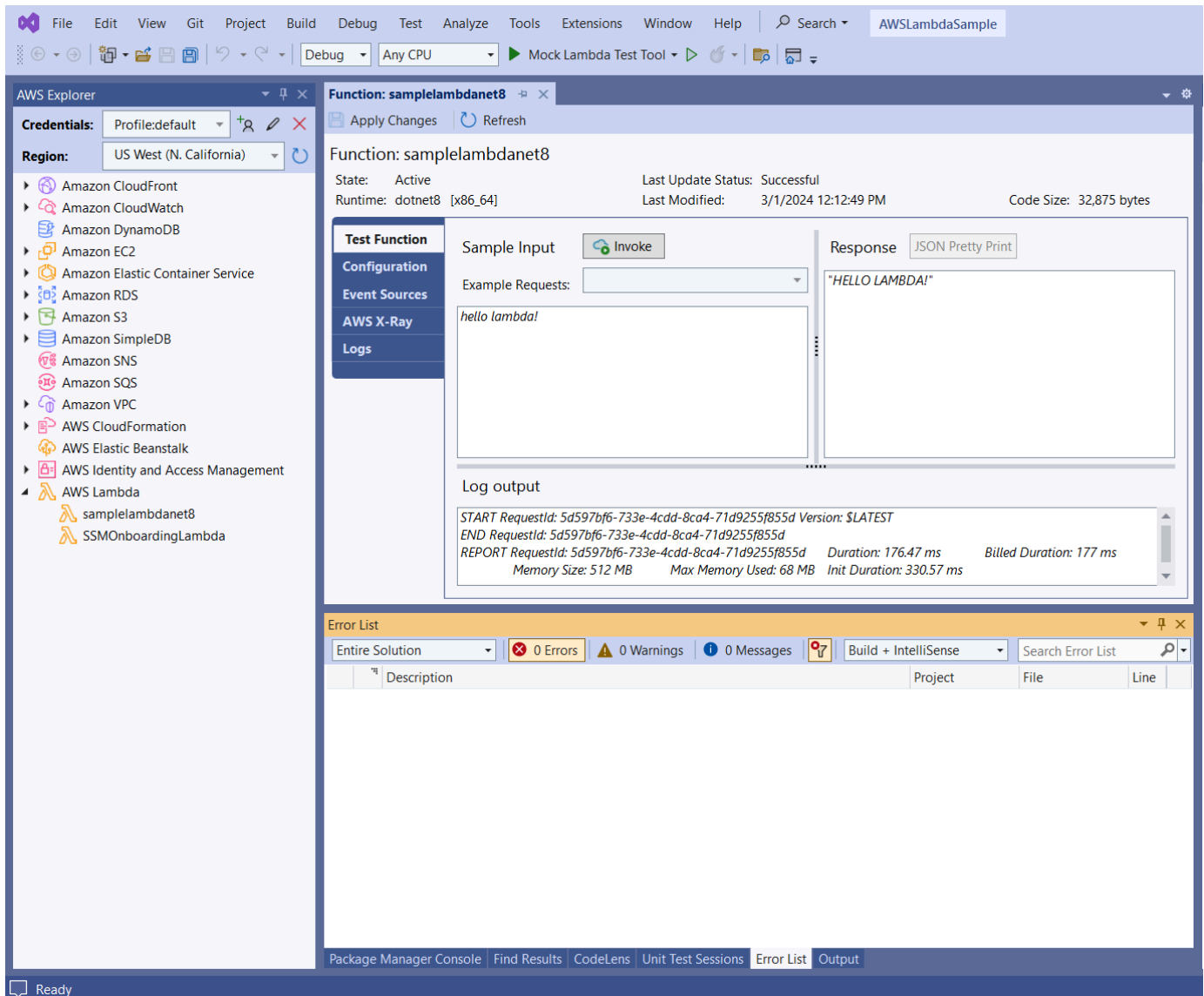
La pagina Funzione di caricamento viene visualizzata durante il caricamento della funzione su. AWS Per mantenere aperta la procedura guidata dopo il caricamento in modo da poter visualizzare il rapporto, deseleziona Chiudi automaticamente la procedura guidata in caso di completamento con successo nella 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 AWS Management Console 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'argomento [CloudWatch](#) [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 Lambda nodo.
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 Studio](#) argomento 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:

The screenshot shows the 'Upload to AWS Lambda' dialog box. The title bar reads 'Upload to AWS Lambda'. The main header features the AWS logo and the text 'Upload Lambda Function' with the subtitle 'Enter the details about the function you want to upload.' Below this, there are several configuration sections: 'AWS Credentials' with a dropdown for 'Profile: Default' and 'Region' set to 'US West (Oregon)'; 'Package Type' set to 'Image'; 'Lambda Runtime' set to 'Not Applicable to Image based Functions'; 'Architecture' with radio buttons for 'x86' (selected) and 'ARM'; 'Function Name' with radio buttons for 'Create new function' (selected) and 'Re-deploy to existing', with a text input field containing 'LambdafunctionDocker'; 'Description' with an empty text area; 'Image Command' with the text 'AWSLambdaDocker::AWSLambdaDocker.Function::FunctionHandler'; 'Image Repo' set to 'awslambdadocker' and 'Image Tag' set to 'latest'. At the bottom right, there are four buttons: 'Close', 'Back', 'Next', and 'Upload'.


- 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 AWS Management Console
- c. Per Descrizione, inserisci il testo da visualizzare con l'istanza in AWS Management Console.
- 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. Seleziona 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.

The screenshot displays the AWS Lambda console interface for a function named "LambdafunctionDocker". The function is in an "Active" state with a "Successful" last update status. The image URI is partially redacted, and the last modified date is 3/19/2024 3:25:47 PM. The code size is "Not Applicable".

The "Test Function" section is active, showing a "Sample Input" field with the text "hello image based lambda" and an "Invoke" button. The "Response" field displays the following JSON output:

```
{
  "Lower": "hello image based lambda",
  "Upper": "HELLO IMAGE BASED LAMBDA"
}
```

The "Log output" section shows the following log entries:

```
START RequestId: a8aff2c0-b473-4fdc-b3bf-3703f60f49d7 Version: $LATEST
END RequestId: a8aff2c0-b473-4fdc-b3bf-3703f60f49d7
REPORT RequestId: a8aff2c0-b473-4fdc-b3bf-3703f60f49d7    Duration: 221.17 ms    Billed Duration: 870 ms
Memory Size: 512 MB    Max Memory Used: 68 MB    Init Duration: 648.61 ms
```

The "Output" section at the bottom shows the output from the "Package Manager".

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 AWS CloudFormation modello serverless. AWS 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": ""
}
```

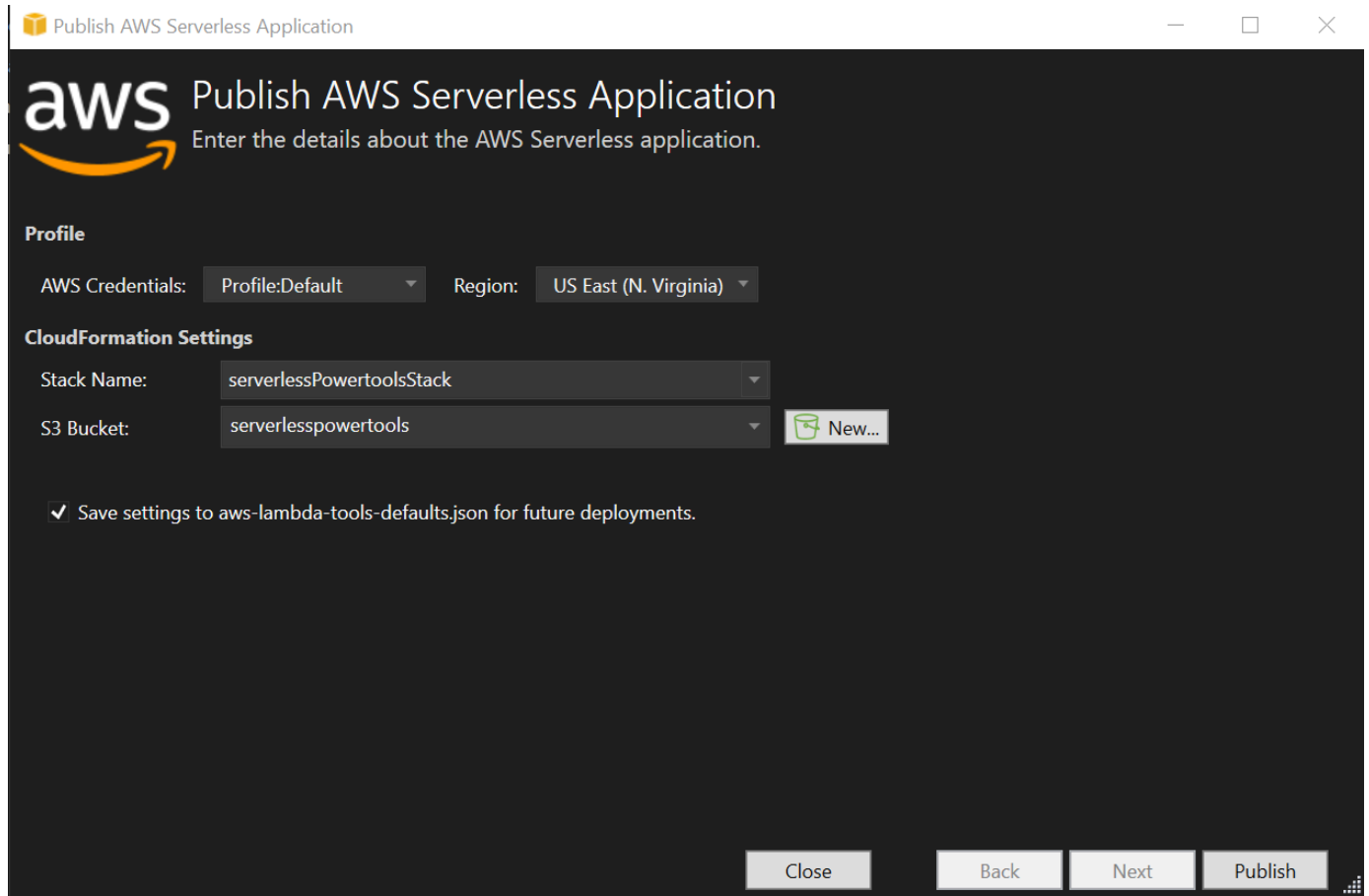
Distribuzione dell'applicazione serverless

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 AWS 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

AWS 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`

Stack: **serverlessPowertoolsStack** | aws-lambda-to...-defaults.json | Functions.cs | serverless.template | Readme.md | serverlessPowertools

Connect to Instance | Delete Stack | Cancel Update | Refresh

Stack Name: serverlessPowertoolsStack | Created: 3/29/2024 12:44:49 PM

Status: **CREATE COMPLETE** | Create Timeout: None

Status (Reason): | Rollback on Failure

Stack ID: arn:aws:cloudformation:us-east-1:150845879014:stack/serverlessPowertoolsStack/

SNS Topic:

Description: An AWS Serverless Application.

AWS Serverless URL: <https://us-east-1.console.aws.amazon.com/Prod> Copy

Events | Filter:

Resources	Time	Type	Logical ID	Physical ID	Status	Reason
Monitoring	3/29/2024 12:45:26 PM	AWS::CloudFormation::Stack	serverlessPowertoolsStack	arn:aws:cloudformation:us-east-1:150845879014:stack/serverlessPowertoolsStack/	CREATE_COMPLETE	
Template	3/29/2024 12:45:25 PM	AWS::ApiGateway::Stage	ServerlessRestApiProdStage	Prod	CREATE_COMPLETE	
Parameters	3/29/2024 12:45:25 PM	AWS::ApiGateway::Stage	ServerlessRestApiProdStage	Prod	CREATE_IN_PROGRESS	Resource not available for this event.
Outputs	3/29/2024 12:45:24 PM	AWS::ApiGateway::Stage	ServerlessRestApiProdStage		CREATE_IN_PROGRESS	
	3/29/2024 12:45:23 PM	AWS::Lambda::Function	Get	serverlessPowertoolsStack-Get-Lgaks	CREATE_COMPLETE	
	3/29/2024 12:45:23 PM	AWS::ApiGateway::Deployment	ServerlessRestApiDeployment9d78fb6c57	qpdntli	CREATE_COMPLETE	
	3/29/2024 12:45:23 PM	AWS::ApiGateway::Deployment	ServerlessRestApiDeployment9d78fb6c57	qpdntli	CREATE_IN_PROGRESS	Resource not available for this event.
	3/29/2024 12:45:22 PM	AWS::Lambda::Permission	GetRootGetPermissionProd	serverlessPowertoolsStack-GetRootGetPermissionProd	CREATE_COMPLETE	
	3/29/2024 12:45:22 PM	AWS::Lambda::Permission	GetRootGetPermissionProd	serverlessPowertoolsStack-GetRootGetPermissionProd	CREATE_IN_PROGRESS	Resource not available for this event.
	3/29/2024 12:45:21 PM	AWS::ApiGateway::Deployment	ServerlessRestApiDeployment9d78fb6c57		CREATE_IN_PROGRESS	
	3/29/2024 12:45:21 PM	AWS::Lambda::Permission	GetRootGetPermissionProd		CREATE_IN_PROGRESS	
	3/29/2024 12:45:21 PM	AWS::ApiGateway::RestApi	ServerlessRestApi	bhntmpmjoj	CREATE_COMPLETE	
	3/29/2024 12:45:20 PM	AWS::ApiGateway::RestApi	ServerlessRestApi	bhntmpmjoj	CREATE_IN_PROGRESS	Resource not available for this event.
	3/29/2024 12:45:19 PM	AWS::ApiGateway::RestApi	ServerlessRestApi		CREATE_IN_PROGRESS	
	3/29/2024 12:45:18 PM	AWS::Lambda::Function	Get	serverlessPowertoolsStack-Get-Lgaks	CREATE_IN_PROGRESS	Event not found.
	3/29/2024 12:45:17 PM	AWS::Lambda::Function	Get	serverlessPowertoolsStack-Get-Lgaks	CREATE_IN_PROGRESS	Resource not available for this event.
	3/29/2024 12:45:16 PM	AWS::Lambda::Function	Get		CREATE_IN_PROGRESS	
	3/29/2024 12:45:15 PM	AWS::IAM::Role	GetRole	serverlessPowertoolsStack-GetRole-D	CREATE_COMPLETE	
	3/29/2024 12:44:59 PM	AWS::IAM::Role	GetRole	serverlessPowertoolsStack-GetRole-D	CREATE_IN_PROGRESS	Resource not available for this event.
	3/29/2024 12:44:58 PM	AWS::IAM::Role	GetRole		CREATE_IN_PROGRESS	
	3/29/2024 12:44:55 PM	AWS::CloudFormation::Stack	serverlessPowertoolsStack	arn:aws:cloudformation:us-east-1:150845879014:stack/serverlessPowertoolsStack/	CREATE_IN_PROGRESS	User initiated.
	3/29/2024 12:44:49 PM	AWS::CloudFormation::Stack	serverlessPowertoolsStack	arn:aws:cloudformation:us-east-1:150845879014:stack/serverlessPowertoolsStack/	REVIEW_IN_PROGRESS	User initiated.

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.IsNullOrEmpty(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 `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 reindirizzate ad Amazon CloudWatch Logs.

2. `aws-lambda-tools-defaults.json`

Il file `aws-lambda-tools-defaults.json` 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 delle 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**.

Upload to AWS Lambda

aws Upload Lambda Function
Enter the details about the function you want to upload.

Package Type: Zip

Lambda Runtime: .NET 8

Architecture: x86 ARM

Function Name: Create new function
ImageRekognition
 Re-deploy to existing

Handler: AWSLambdaRek::AWSLambdaRek.Function::FunctionHandler
For .NET runtimes, the Lambda handler format is: <assembly>::<type>::<method>

Description:

Configuration: Release Framework: net8.0

Save settings to aws-lambda-tools-defaults.json for future deployments.

Close Back Next Upload

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`

- 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**.



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

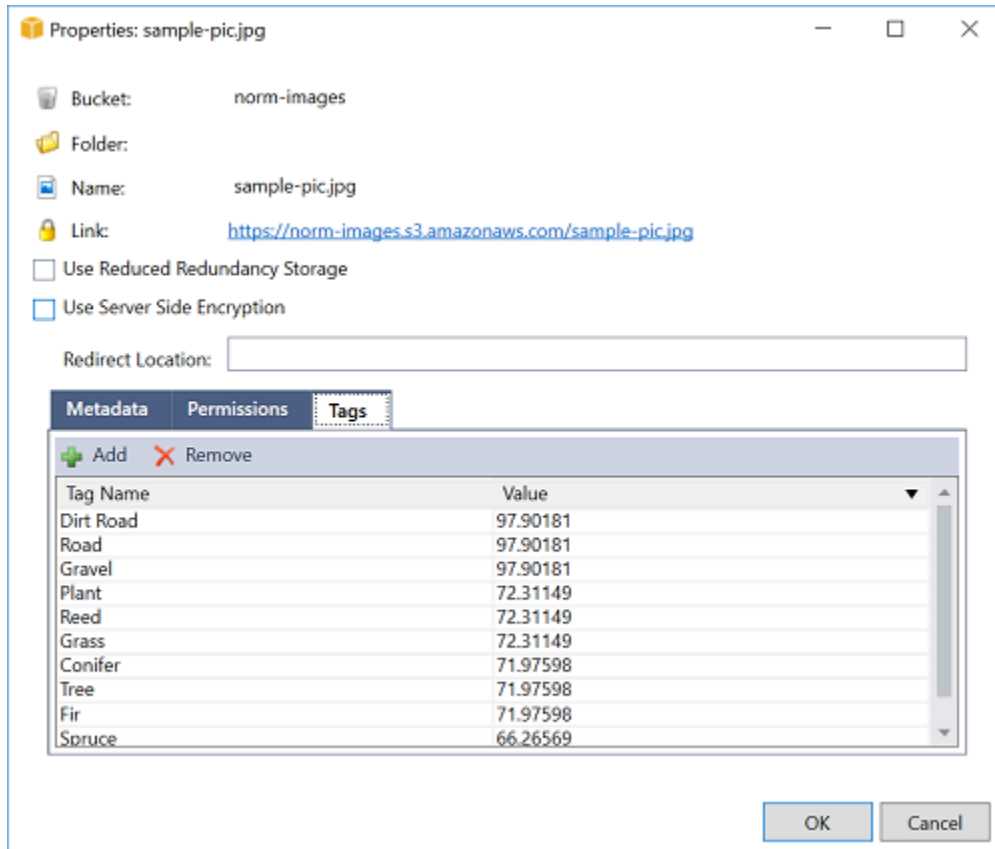
Note

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 che sono stati 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 visualizzare, vedere 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 for .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](#)

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

Implementazione suAWS

Il Toolkit for Visual Studio supporta la distribuzione delle applicazioni inAWS Elastic Beanstalk contenitori oAWS CloudFormation stack.

Note

Se si utilizza Visual Studio Express Edition:

- Puoi utilizzare l'interfaccia a riga di [comando Docker](#) per distribuire applicazioni su contenitori Amazon ECS.
- È possibile utilizzare la [console diAWS gestione](#) per distribuire applicazioni in contenitori Elastic Beanstalk.

Per le distribuzioni di Elastic Beanstalk, è necessario prima creare un pacchetto di distribuzione Web. Per ulteriori informazioni, consulta [Come creare un Package 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 for Docker](#).

Argomenti

- [Utilizzo di Pubblica in CloudWatchAWSin Visual Studio](#)
- [Distribuzione di unAWS LambdaProgetto con la CLI Core .NET Core](#)
- [Distribuzione su Elastic Beanstalk](#)
- [Implementazione in Amazon EC2 Container Service](#)

Utilizzo di Pubblica in CloudWatchAWSin Visual Studio

Publish to (Pubblica in CloudWatch)AWSè un'esperienza di distribuzione interattiva che ti aiuta a pubblicare le tue applicazioni.NET inAWSdestinazioni di distribuzione, supporto di applicazioni destinate a .NET Core 3.1 e versioni successive. Utilizzo di Pubblica in CloudWatchAWSmantiene il flusso di lavoro all'interno di Visual Studio rendendo disponibili queste funzionalità di distribuzione, direttamente dal tuo IDE:

- La possibilità di distribuire la tua applicazione con un solo clic.

- Consigli per la distribuzione basati sulla tua applicazione.
- Creazione automatica di Dockerfile, come pertinente e richiesto dall'ambiente della destinazione di distribuzione (target di distribuzione).
- Impostazioni ottimizzate per la creazione e il packaging delle applicazioni, come richiesto dal target di distribuzione.

Note

Per ulteriori informazioni sulla pubblicazione di applicazioni .NET Framework, vedere la guida [Creazione e distribuzione di applicazioni .NET su Elastic Beanstalk](#)

È inoltre possibile accedere a `Publish to AWS` dall'interfaccia a riga di comando `.NET`. Per ulteriori informazioni, consulta la [.NET AWS guide](#).

Argomenti

- [Prerequisiti](#)
- [Tipi di applicazioni supportati](#)
- [Pubblicazione delle applicazioni AWS bersagli](#)

Prerequisiti

Per pubblicare correttamente 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 informazioni sul download, visitare il [Sito di download Microsoft](#).
- Node.js 14.x o versione successiva: Node.js è richiesto per l'esecuzione AWS Cloud Development Kit (AWS CDK). Per scaricare o ottenere ulteriori informazioni su Node.js, visitare il [Node.js sito di download](#).

Note

`Publish to AWS` utilizza AWS CDK per distribuire la tua applicazione e tutta la sua infrastruttura di distribuzione come un unico progetto. Per ulteriori informazioni su AWS CDK consulta [Cloud Development Kit guide](#).

- (Facoltativo) Docker viene utilizzato durante la distribuzione su un servizio basato su container come Amazon ECS. Per ulteriori informazioni e per scaricare Docker, consulta [Docker](#) sito.

Tipi di applicazioni supportati

Prima di pubblicare su una destinazione nuova o in uscita, inizia creando o aprendo uno dei seguenti tipi di progetto in Visual Studio:

- Applicazione ASP.NET Core
- Applicazione .NET
- Blazer WebAssembly candidatura

Pubblicazione delle applicazioni AWS bersagli

Quando si pubblica su una nuova destinazione, Pubblica su AWS guiderà l'utente attraverso il processo fornendo consigli e utilizzando impostazioni comuni. Se hai bisogno di pubblicare su una destinazione che è stata impostata in precedenza, le tue preferenze vengono memorizzate e possono essere modificate, oppure sono immediatamente disponibili per la distribuzione con un clic.

Pubblica su un nuovo target

La seguente sezione descrive come configurare Publish to (Pubblica) AWS preferenze di distribuzione, quando pubblici su un nuovo target.


1. Da AWS Esploratore, espansione del Credenziali menu a discesa, quindi seleziona AWS profilo che corrisponde alla regione e AWS servizi necessari per la distribuzione.
2. Espandere Region menu a discesa, quindi seleziona AWS regione che contiene AWS servizi necessari per la distribuzione.
3. Da Visual Studio Soluzioni, apri il menu contestuale per (pulsante destro del mouse) il nome del progetto e seleziona Publish to (Pubblica in CloudWatch) AWS. Questo si aprirà Publish to (Pubblica in CloudWatch) AWS.
4. Da Publish to (Pubblica in CloudWatch) AWS, scegli Pubblica su un nuovo target per configurare una nuova distribuzione.

 Note

Per modificare le credenziali di distribuzione predefinite, scegliere o fare clic sul pulsante **Modificare link** situato accanto al **Credenziale** sezione, in **Publish to (Pubblica in CloudWatch) AWS**.

Per bypassare il processo di configurazione di destinazione, scegliere **Pubblica** su una destinazione esistente, quindi scegli la tua configurazione preferita dall'elenco dei tuoi obiettivi di distribuzione precedenti.

5. Da **Pubblicazione delle destinazioni** riquadro, scegli un **AWS servizio** per gestire la distribuzione delle applicazioni.
6. Al termine, fai clic **Pubblica** per avviare il processo di distribuzione.

 Note

Dopo aver avviato una distribuzione, **Publish to (Pubblica in CloudWatch) AWS** visualizza i seguenti aggiornamenti di stato:

- Durante il processo di distribuzione, **Publish to (Pubblica in CloudWatch) AWS** visualizza informazioni sullo stato di avanzamento della distribuzione.
- Dopo il processo di distribuzione, **Publish to (Pubblica in CloudWatch) AWS** indica se la distribuzione è riuscita o non è riuscita.
- Dopo una distribuzione riuscita, il **Risorse** pannello offre informazioni aggiuntive sulla risorsa che è stata creata. Queste informazioni variano 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 un'applicazione esistente **AWS** destinazione.

1. Da **AWS Esploratore**, espansione del **Credenziale** menu a discesa, quindi seleziona **AWS profilo** che corrisponde alla regione e **AWS servizi** necessari per la distribuzione.
2. Espandere **Region** menu a discesa, quindi seleziona **AWS regione** che contiene **AWS servizi** necessari per la distribuzione.

3. Da Visual Studio Soluzionifare clic con il pulsante destro del mouse sul nome del progetto e Publish to (Pubblica in CloudWatch) AWS per aprire Publish to (Pubblica in CloudWatch) AWS.
4. Da Publish to (Pubblica in CloudWatch) AWS, scegli Pubblica su una destinazione esistente per selezionare l'ambiente di distribuzione da un elenco di destinazioni esistenti.

Note

Se di recente hai pubblicato delle candidature su AWS Cloud, queste applicazioni vengono visualizzate in Pubblica su AWS.

5. Seleziona la destinazione di pubblicazione in cui vuoi distribuire l'applicazione, quindi fai clic Pubblica per avviare il processo di distribuzione.

Distribuzione di un AWS Lambda Progetto con la CLI Core .NET Core

La AWS Toolkit for Visual Studio include AWS Lambda Modelli di progetto di .NET Core per Visual Studio. È possibile distribuire funzioni Lambda integrate in Visual Studio utilizzando l'interfaccia a riga di comando (CLI) .NET Core.

Argomenti

- [Prerequisiti](#)
- [Argomenti correlati](#)
- [Elenco dei comandi Lambda disponibili tramite l'interfaccia a riga di comando di .NET Core](#)
- [Pubblicazione di un progetto .NET Core Lambda dall'interfaccia della riga di comando .NET Core](#)

Prerequisiti

Prima di utilizzare l'interfaccia a riga di comando di .NET Core per distribuire funzioni Lambda, è necessario soddisfare i seguenti prerequisiti:

- Verificare che Visual Studio 2015 Update 3 sia installato.
- Installa [.NET Core per Windows](#).

- Configurare la CLI Core .NET Core per l'interfaccia a riga di comando di Lambda. Per ulteriori informazioni, consulta [Interfaccia a riga di comando di .NET Core](#) nella AWS Lambda Guida per gli sviluppatori.
- Installare Toolkit for Visual Studio. Per ulteriori informazioni, consulta la pagina [Installazione del AWS Toolkit for Visual Studio](#).

Argomenti correlati

I seguenti argomenti correlati possono risultare utili durante l'utilizzo dell'interfaccia a riga di comando di .NET Core per distribuire funzioni Lambda:

- Per ulteriori informazioni sulle funzioni Lambda, consulta [Che cos'è AWS Lambda?](#) nella AWS Lambda Guida per gli sviluppatori.
- Per informazioni sulla creazione di funzioni Lambda in Visual Studio, vedere [AWS Lambda](#).
- Per ulteriori informazioni su Microsoft .NET Core, consulta [.NET Core](#) nella documentazione online di Microsoft.

Elenco dei comandi Lambda disponibili tramite l'interfaccia a riga di comando di .NET Core

Per elencare i comandi Lambda disponibili tramite l'interfaccia CLI .NET Core, effettuare le seguenti operazioni.

1. Aprire la finestra del prompt dei comandi e accedere alla cartella contenente un progetto Lambda Core di Visual Studio.
2. Specificare (sì 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 dall'interfaccia della riga di comando .NET Core

Le seguenti istruzioni presuppongono che tu abbia creato unAWS Lambdafunzione.NET Core in Visual Studio.

1. Apri la finestra del prompt dei comandi e accedi alla cartella contenente il progetto Lambda Core di Visual Studio.
2. Specificare (sì `dotnet lambda deploy-function`).
3. Quando richiesto, immettere il nome della funzione da distribuire. Può usare un nuovo nome o il nome di una funzione esistente.
4. Quando richiesto, immettere ilAWSRegione (la regione in cui verrà implementata la tua funzione Lambda).
5. Quando richiesto, seleziona o crea il ruolo IAM che Lambda assumerà durante l'esecuzione della funzione.

Al completamento, ilCreazione di una nuova funzione Lambda(Salvare).

```
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\AWSLambda1\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 ilAWSRegione .

```
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
```

```
Ziping publish folder C:\Lambda\AWSLambda1\AWSLambda1\bin\Release
\netcoreapp1.0\publish to C:\Lambda\AWSLambda1\AWSLambda1\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
```

Dopo che la funzione Lambda è stata implementata, è pronta per l'uso. Per ulteriori informazioni, consulta [Esempi su come utilizzare AWS Lambda](#).

Lambda monitora automaticamente le funzioni Lambda per te e segnala i parametri tramite Amazon CloudWatch. Per monitorare e risolvere problemi relativi alla funzione Lambda, consulta [Risoluzione dei problemi e monitoraggio AWS Funzioni Lambda con Amazon CloudWatch](#).

Distribuzione su Elastic Beanstalk

AWS Elastic Beanstalk è un servizio che semplifica il processo di provisioning AWS risorse per la tua applicazione. Elastic Beanstalk fornisce tutta l'AWS infrastruttura necessaria per distribuire l'applicazione. Questa infrastruttura include:

- Istanze Amazon EC2 che ospitano gli eseguibili e i contenuti per la tua applicazione.
- Un gruppo Auto Scaling per gestire il numero appropriato di istanze Amazon EC2 a supporto dell'applicazione.
- Un sistema di bilanciamento del carico Elastic Load Balancing che instrada il traffico in ingresso all'istanza Amazon EC2 con la maggiore larghezza di banda.

Toolkit for Visual Studio fornisce una procedura guidata che semplifica la pubblicazione di applicazioni tramite Elastic Beanstalk. Questa procedura guidata è descritta nelle sezioni seguenti.

Per ulteriori informazioni su Elastic Beanstalk, vai alla [Documentazione su Elastic Beanstalk](#).

Argomenti

- [Implementazione di un'applicazione ASP.NET tradizionale su Elastic Beanstalk](#)
- [distribuzione di un'applicazione ASP.NET Core su Elastic Beanstalk \(Legacy\)](#)
- [Come specificare la AWS Credenziali di sicurezza per la tua applicazione](#)

- [Come ripubblicare la tua applicazione in un ambiente Elastic Beanstalk \(Legacy\)](#)
- [Distribuzioni di applicazioni di Elastic Beanstalk](#)
- [Distribuzioni personalizzate di ASP.NET Core Elastic Beanstalk](#)
- [Support di più applicazioni per .NET e Elastic Beanstalk](#)

Implementazione di un'applicazione ASP.NET tradizionale su Elastic Beanstalk

Questa sezione descrive come utilizzare la procedura guidata Publish to 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 applicazioni Web integrato in Visual Studio oppure puoi usare il tuo progetto.

Note

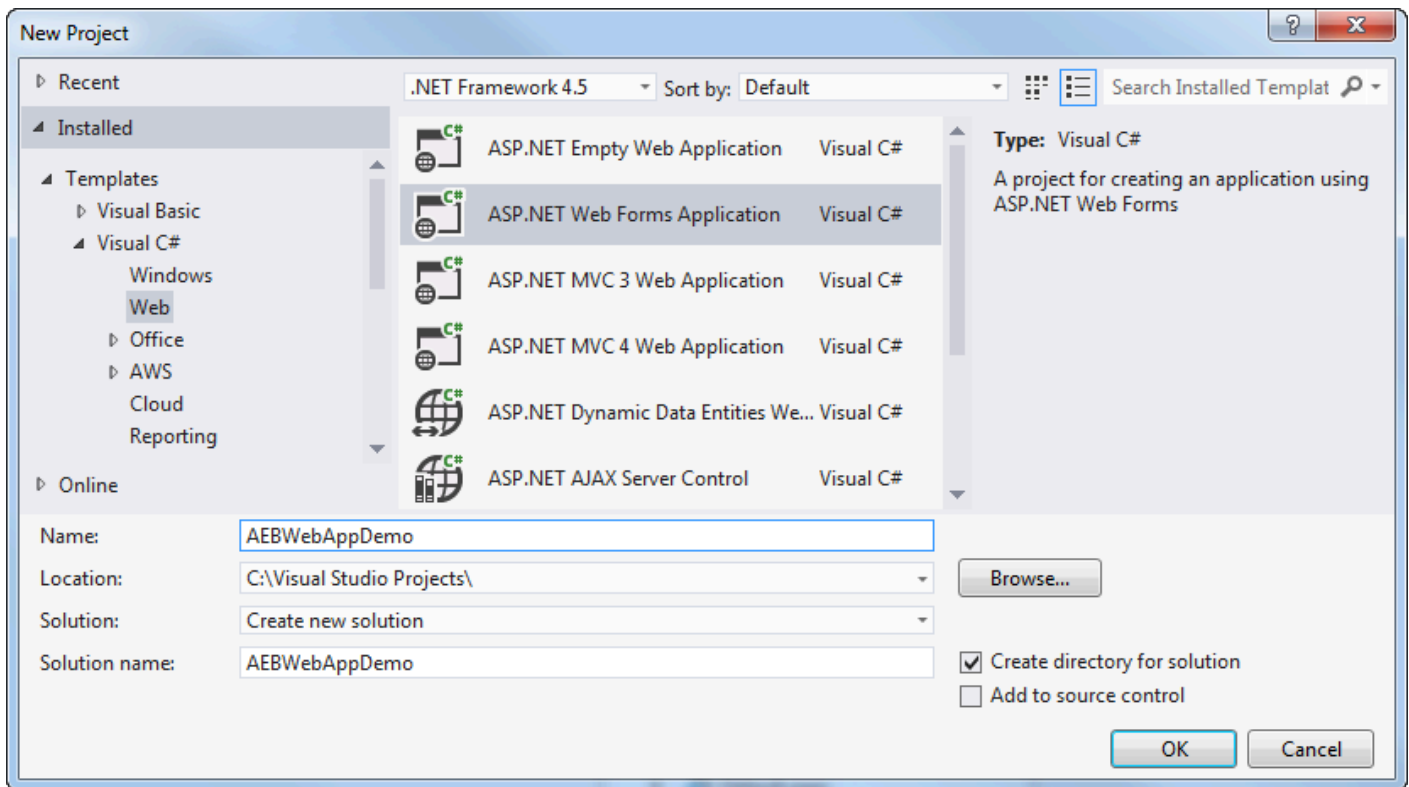
La procedura guidata supporta anche la distribuzione di applicazioni ASP.NET Core. Per informazioni su ASP.NET Core, vedere la guida agli [strumenti di distribuzione AWS .NET](#) e il sommario aggiornato di [Deploying to AWS](#).

Note

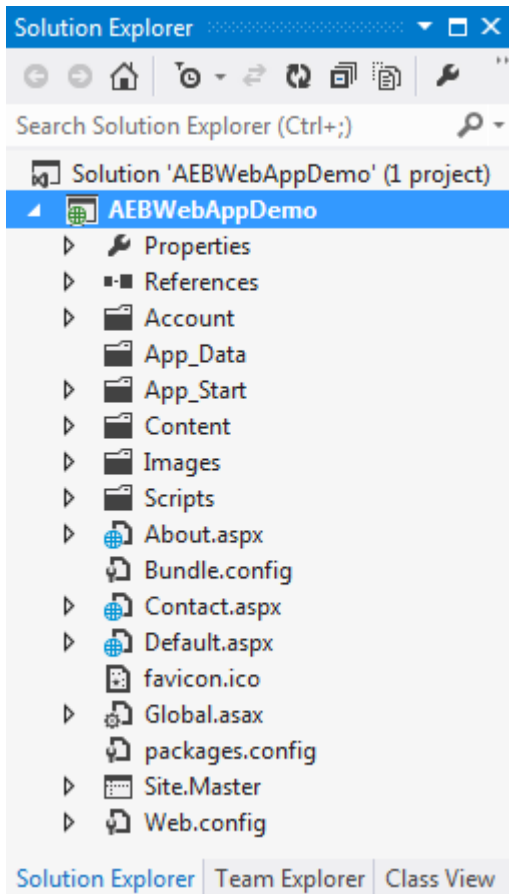
Prima di poter utilizzare la procedura guidata Publish to Elastic Beanstalk, è necessario scaricare e installare [Web Deploy](#). La procedura guidata si basa su Web Deploy per distribuire applicazioni Web e siti Web sui server Web di Internet Information Services (IIS).

Per creare un esempio di progetto iniziale per 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. In questo esempio, scegliere l'applicazione ASP.NET Web Forms.

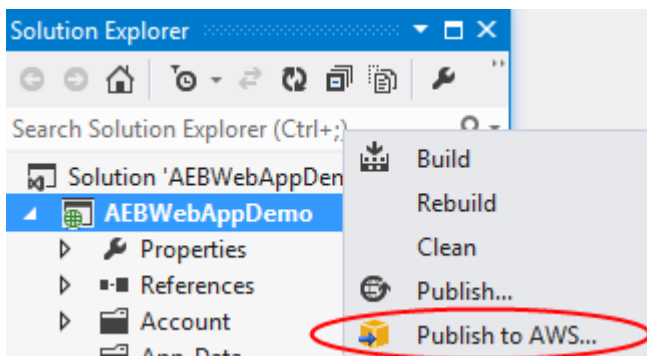


4. Nella casella Name (Nome), digitare AEBWebAppDemo.
5. Nella casella Posizione, digita il percorso di una cartella di soluzioni sul tuo computer di sviluppo o scegli Sfoglia, quindi cerca e scegli una cartella di soluzioni e scegli Seleziona cartella.
6. Verificare che la casella Create directory for solution (Crea directory per soluzione) sia selezionata. Nell'elenco a discesa Soluzione, conferma che l'opzione Crea nuova soluzione sia selezionata, quindi scegli OK. Visual Studio creerà una soluzione e un progetto basati sul modello di progetto ASP.NET Web Forms Application. Visual Studio visualizzerà quindi Solution Explorer dove vengono visualizzati la nuova soluzione e il nuovo progetto.

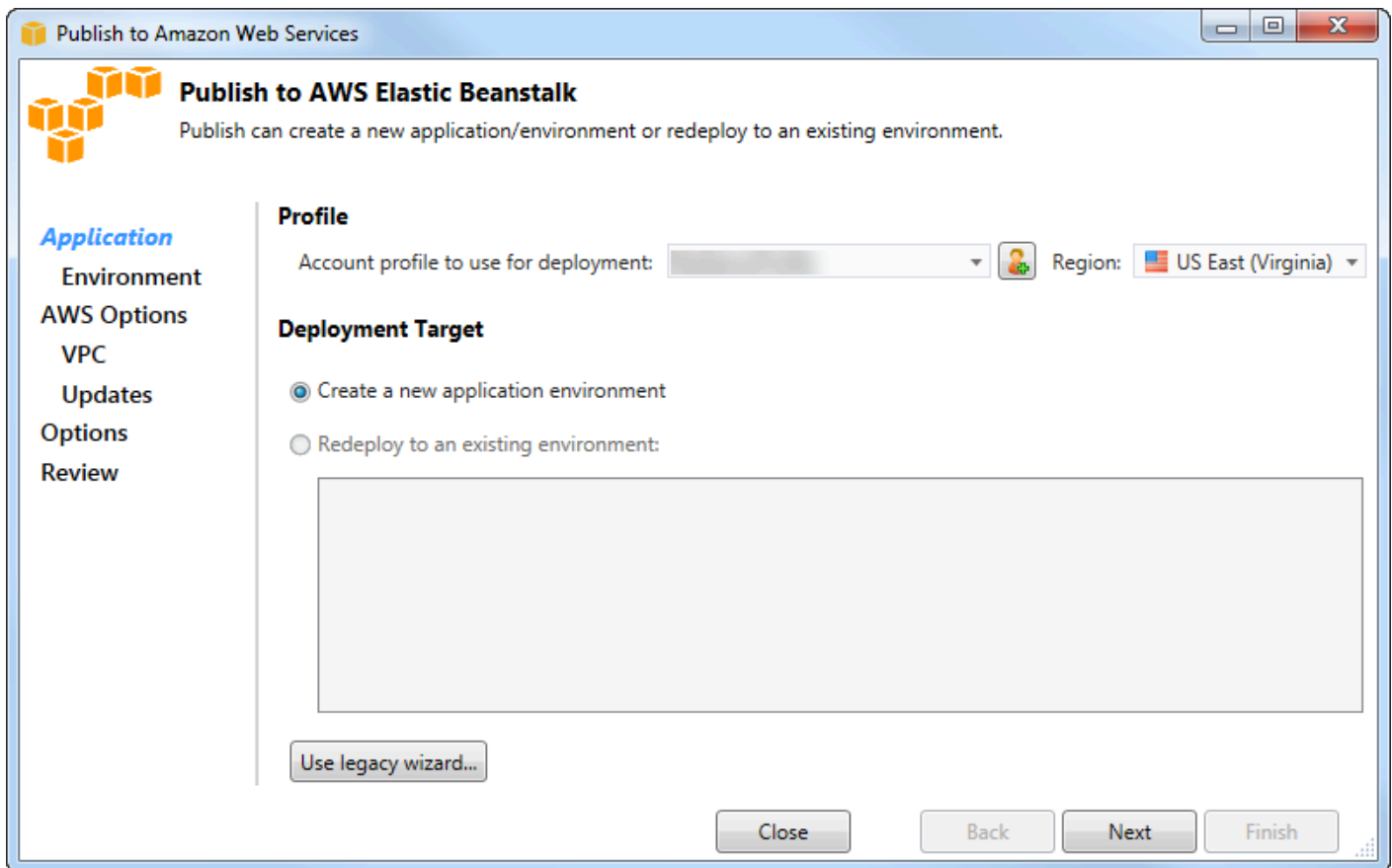


Per distribuire un'applicazione utilizzando la procedura guidata Publish to Elastic Beanstalk

1. In Solution Explorer, apri il menu contestuale (clic con il pulsante destro del mouse) per la cartella del progetto AEBWebAppDemo per il progetto che hai creato nella sezione precedente, oppure apri il menu contestuale per la cartella del progetto per la tua applicazione e scegli Pubblica suAWS 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 profiloAWS dell'account che desideri utilizzare per la distribuzione.

Facoltativamente, se hai unAWS account che desideri utilizzare, ma non hai ancora creato un profilo diAWS account, puoi scegliere il pulsante con il simbolo più (+) per aggiungere un profiloAWS dell'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 tra Creare un nuovo ambiente applicativo per eseguire una distribuzione iniziale di un'applicazione o Redistribuire in un ambiente esistente per ridistribuire un'applicazione precedentemente distribuita. (Le distribuzioni precedenti potrebbero essere state eseguite con la procedura guidata o con lo strumento di distribuzione standalone obsoleto.) Se scegli Ridistribuisce in un ambiente esistente, potrebbe esserci un ritardo nel recupero delle informazioni dalle distribuzioni precedenti attualmente in esecuzione da parte della procedura guidata.

Note

Se scegli **Redistribuisce** in un ambiente esistente, scegli un ambiente nell'elenco e quindi scegli **Avanti**, la procedura guidata ti porterà direttamente alla pagina delle opzioni dell'applicazione. Se segui questa strada, passa alle istruzioni riportate più avanti in questa sezione che descrivono come utilizzare la pagina delle opzioni dell'applicazione.

5. Seleziona Successivo.

The screenshot shows the 'Publish to Amazon Web Services' wizard window. The title bar reads 'Publish to Amazon Web Services'. The main content area is titled 'Application Environment' and contains the instruction: 'Enter the details for your new application environment. To create a new new environment for an existing application, select the appropriate application.' On the left, there is a navigation pane with the following items: 'Application', 'Environment' (highlighted in blue), 'AWS Options', 'VPC', 'Updates', 'Options', and 'Review'. The main area is divided into three sections: 'Application' with a 'Name' dropdown menu set to 'AEBWebAppDemo'; 'Environment' with a 'Name' dropdown menu; and 'URL' with a text input field containing 'http: [redacted].elasticbeanstalk.com' and a 'Check availability...' button. Below the URL field, a green checkmark and the text 'The requested URL is available' are displayed. At the bottom of the window, there are four buttons: 'Close', 'Back', 'Next', and 'Finish'.

- 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.
- 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 fornita da Elastic Beanstalk per l'applicazione. Un nome predefinito potrebbe già essere proposto in questo elenco a discesa. Se non è già stato proposto un nome predefinito, puoi digitarne uno o sceglierne uno dall'elenco a discesa, se sono disponibili altri nomi. Il nome dell'ambiente non può essere più lungo di 23 caratteri.

- Nell'area URL, la casella propone un sottodominio predefinito `elasticbeanstalk.com` che sarà l'URL della tua applicazione web. È possibile modificare il sottodominio predefinito digitando un nuovo nome di sottodominio.
- Scegli Verifica disponibilità per assicurarti che l'URL della tua applicazione web non sia già in uso.
- Se è possibile utilizzare l'URL della tua applicazione Web, scegli Avanti.

Publish to Amazon Web Services

AWS
Set Amazon EC2 and other AWS-related options for the deployed application.

Application
Environment
AWS Options
VPC
Updates
Options
Review

Amazon EC2 Launch Configuration

Container type *: 64bit Windows Server 2012 R2 running IIS 8.5

Instance type *: Micro Key pair *: MyKeyPair

Use custom AMI:

Use a VPC Single instance environment Enable Rolling Deployments

Deployed Application Permissions

Role: aws-elasticbeanstalk-ec2-role

The permissions for the Identity and Access Management role can be updated after the environment is created.

Relational Database Access

Select the Amazon RDS security groups to be modified to permit access from the EC2 instance(s) hosting your application.

default

Close Back Next Finish

- Nella pagina AWSOpzioni, in Amazon EC2 Launch Configuration, dall'elenco a discesa del tipo di contenitore, scegli un tipo di Amazon Machine Image (AMI) da utilizzare per la tua applicazione.
- Nell'elenco a discesa del tipo di istanza, specifica un tipo di istanza Amazon EC2 da utilizzare. Per questo esempio, ti consigliamo di utilizzare Micro. Questo ridurrà al minimo il costo associato all'esecuzione dell'istanza. Per ulteriori informazioni sui costi di Amazon EC2, consulta la pagina [dei prezzi di EC2](#).
- Nell'elenco a discesa Coppia di chiavi, scegli una key pair di istanza Amazon EC2 da utilizzare per accedere alle istanze che verranno utilizzate per la tua applicazione.

4. Facoltativamente, nella casella Usa AMI personalizzata, è possibile specificare un'AMI personalizzata che sostituirà l'AMI specificato nell'elenco a discesa Tipo di contenitore. Per ulteriori informazioni su come creare un'AMI personalizzata, vai a [Utilizzo di AMI personalizzate](#) nella [AWSElastic Beanstalk Developer Guide](#) e [Crea un'AMI da un'istanza Amazon EC2](#).
5. In alternativa, se si desidera avviare le istanze in un VPC, selezionare la casella Usa un VPC.
6. Facoltativamente, se desideri avviare una singola istanza Amazon EC2 e quindi distribuire la tua applicazione su di essa, seleziona la casella Ambiente a istanza singola.

Se si seleziona questa casella, Elastic Beanstalk creerà comunque un gruppo Auto Scaling, ma non lo configurerà. Se desideri configurare il gruppo Auto Scaling in un secondo momento, puoi usare ilAWS Management Console.

7. Facoltativamente, se desideri controllare le condizioni in cui l'applicazione viene distribuita nelle istanze, seleziona la casella Abilita distribuzioni in sequenza. È possibile selezionare questa casella solo se non è stata selezionata la casella Ambiente a istanza singola.
8. Se la tua applicazione utilizzaAWS servizi come Amazon S3 e DynamoDB, il modo migliore per fornire credenziali è utilizzare un ruolo IAM. Nell'area Autorizzazioni delle applicazioni distribuite, puoi scegliere un ruolo IAM esistente o crearne uno che il wizard utilizzerà per avviare il tuo ambiente. Le applicazioni che utilizzano laAWS SDK for .NET utilizzeranno automaticamente le credenziali fornite da questo ruolo IAM quando effettuano una richiesta a unAWS servizio.
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. Seleziona 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 multiple, verrà visualizzata la pagina delle opzioni dell'applicazione. Passa alle istruzioni riportate più avanti in questa sezione che descrivono come utilizzare la pagina delle opzioni dell'applicazione.

11. Se hai selezionato Usa un VPC, specifica le informazioni nella pagina Opzioni VPC per avviare l'applicazione in un VPC.

Publish to Amazon Web Services

VPC Options
Set Amazon VPC options for the deployed application.

Application
Environment
AWS Options
VPC
Updates
Options
Review

VPC *: vpc-4e (10.0.0.0/16)

ELB Scheme *: Public Security Group *: test (sg-c1)

ELB Subnet *: subnet-c7 (10.0.2.0/24 - us-east-1a)

Instances Subnet *: subnet-45 (10.0.0.0/24 - us-east-1a)

To run AWS Elastic Beanstalk applications inside a VPC, you will need to configure at least the following:

- Create two subnets: one for your EC2 instances and one for your Elastic Load Balancer.
- Traffic must be able to be routed from your Elastic Load Balancer to your EC2 instances.
- Your EC2 instances must be able to connect to the Internet and AWS endpoints.

Elastic Load Balancer settings are not applicable to 'Single Instance' environment types.

For more information visit [AWS Elastic Beanstalk Developer Guide](#)

Close Back Next Finish

Il VPC deve essere già stato creato. Se hai creato il VPC nel Toolkit for Visual Studio, il Toolkit for Visual Studio compilerà questa pagina per te. Se hai creato il VPC nella [Console di AWS gestione](#), digita le informazioni sul tuo VPC in questa pagina.

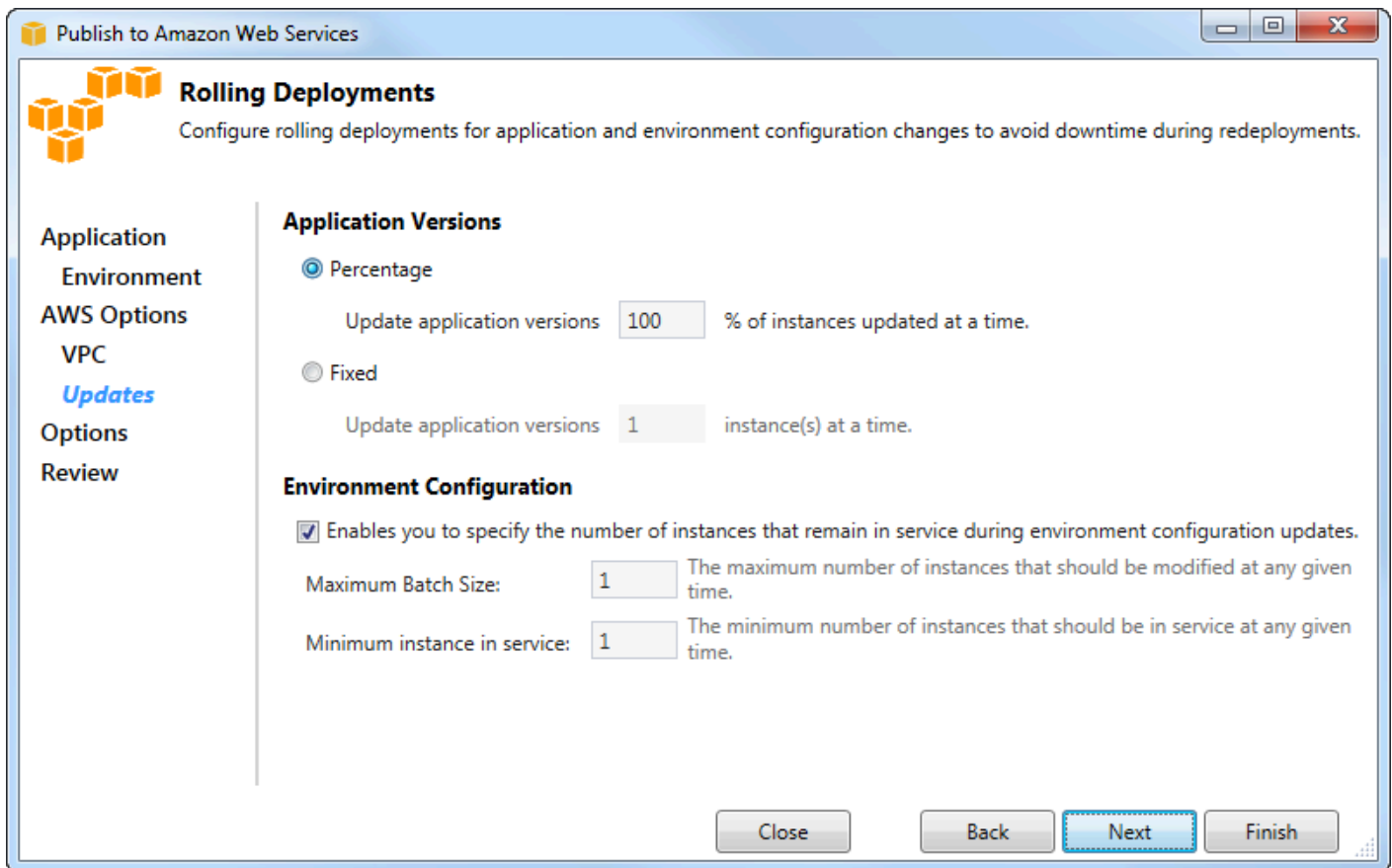
Considerazioni chiave per l'implementazione in un VPC

- Il VPC ha bisogno di almeno una sottorete pubblica e una sottorete privata.
- Nell'elenco a discesa ELB Subnet, specificare 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 a un Internet Gateway. 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 Istanze, specificare la sottorete privata. Il Toolkit for Visual Studio distribuisce le istanze Amazon EC2 per la tua applicazione nella sottorete privata.

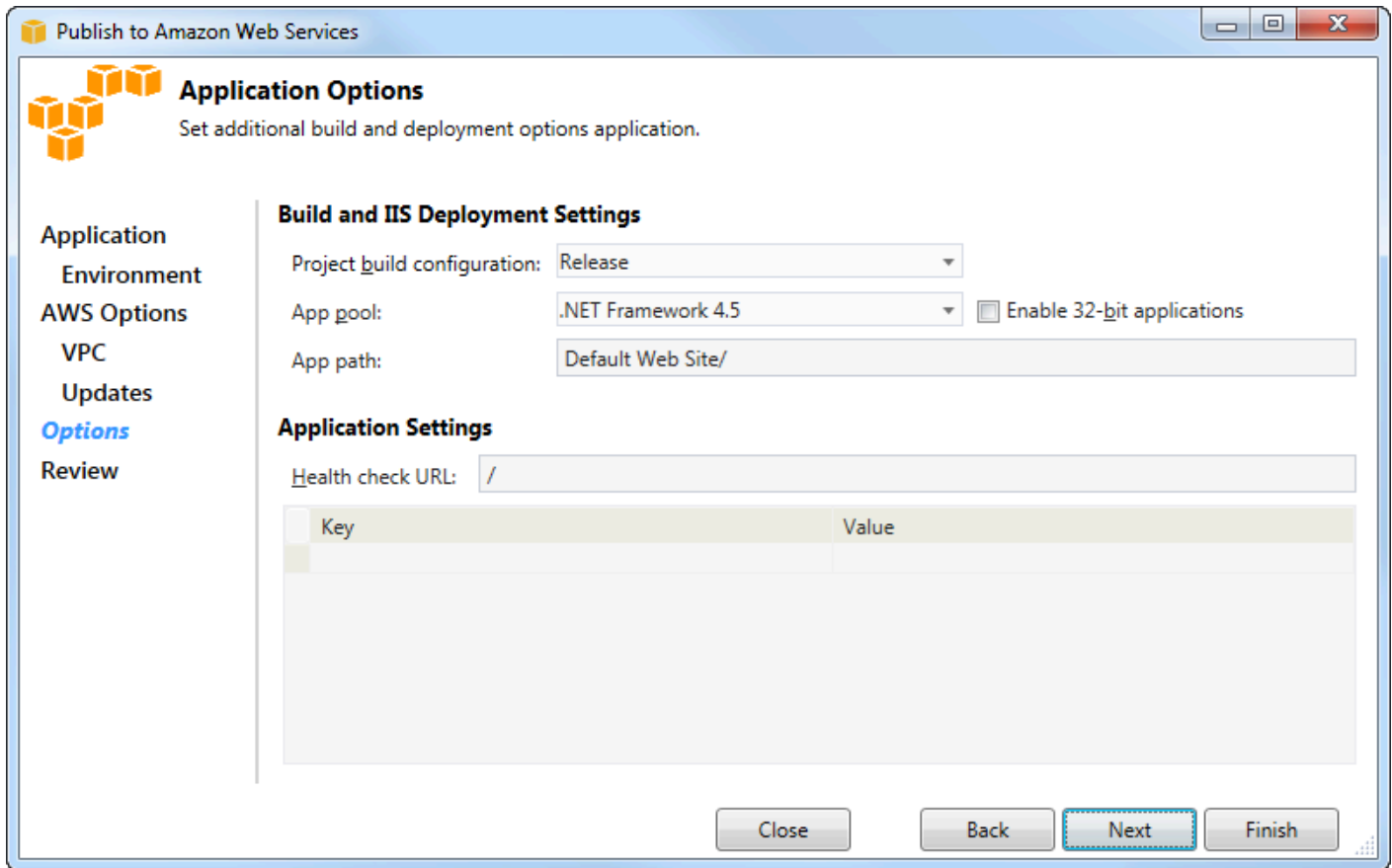
- Le istanze Amazon EC2 per la tua applicazione comunicano dalla sottorete privata a Internet tramite un'istanza Amazon EC2 nella sottorete pubblica che esegue la traduzione degli indirizzi di rete (NAT). Per abilitare questa comunicazione, è necessario un [gruppo di sicurezza VPC](#) che consenta al traffico di fluire dalla sottorete privata all'istanza NAT. Specifica 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 [AWSElastic Beanstalk Developer Guide](#).

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 delle 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 tue applicazioni vengono distribuite nelle istanze in un ambiente con bilanciamento del carico. Ad esempio, se nel proprio ambiente sono presenti quattro istanze e si desidera modificare il tipo di istanza, è possibile configurare l'ambiente per modificare due istanze alla volta. Questo aiuta a garantire che l'applicazione sia ancora in esecuzione mentre vengono apportate modifiche.



3. Nell'area Versioni dell'applicazione, scegli un'opzione per controllare le distribuzioni su una percentuale o su un numero di istanze alla volta. Specifica la percentuale o il numero desiderato.
4. Facoltativamente, nell'area Configurazione dell'ambiente, selezionare la casella se si desidera specificare il numero di istanze che rimangono in servizio durante le distribuzioni. Se si seleziona questa casella, specifica il numero massimo di istanze che devono essere modificate contemporaneamente, il numero minimo di istanze che devono rimanere in servizio contemporaneamente o entrambe.
5. Seleziona Successivo.
6. Nella pagina Opzioni dell'applicazione, si specificano le informazioni sulla build, su Internet Information Services (IIS) e sulle impostazioni dell'applicazione.



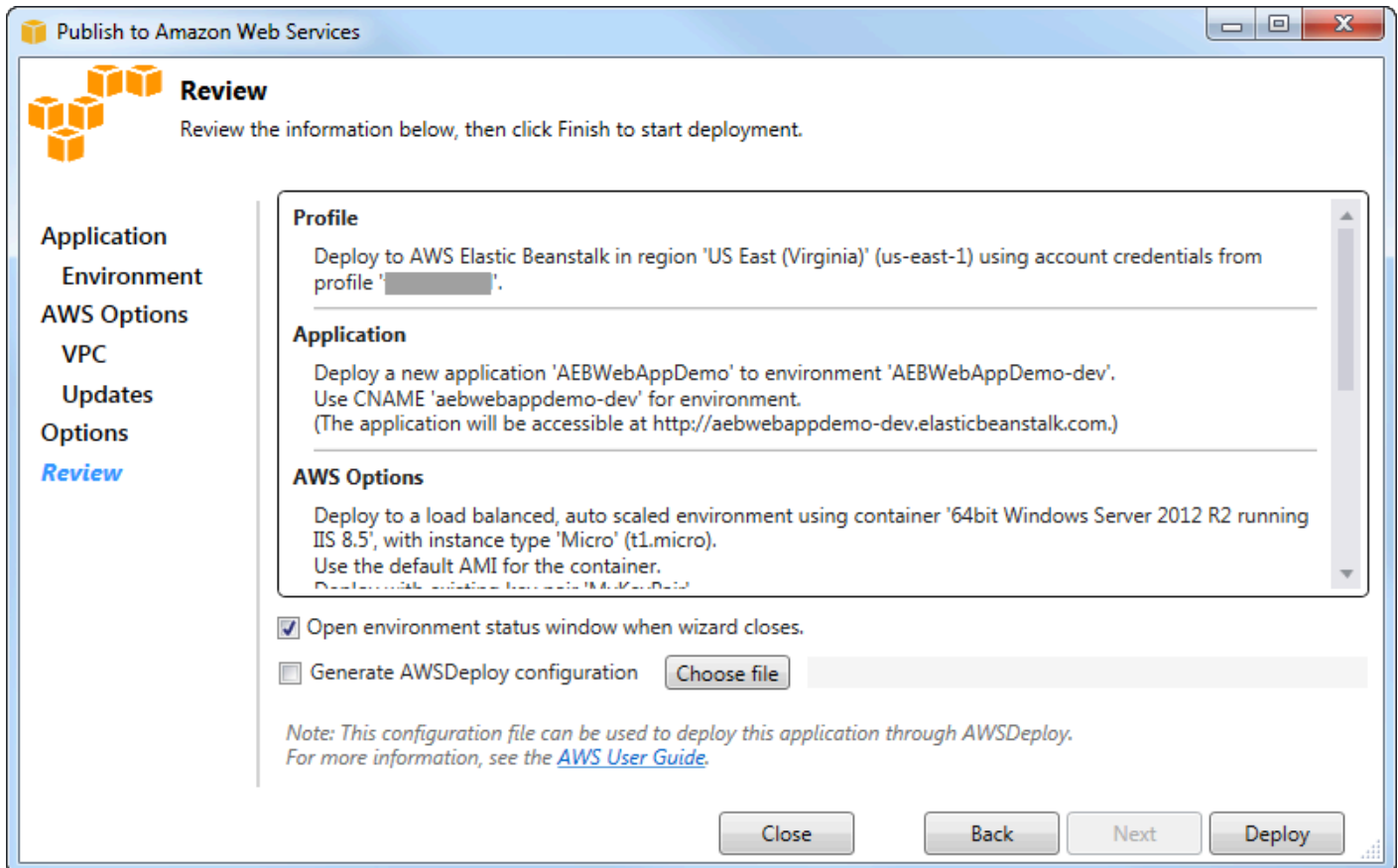
7. Nell'area Impostazioni build e IIS Deployment, nell'elenco a discesa della configurazione della build del progetto, scegli la configurazione della build di destinazione. Se il wizard riesce a trovarlo, Release appare altrimenti, la configurazione attiva viene visualizzata in questa casella.
8. Nell'elenco a discesa del pool di app, scegli la versione di .NET Framework richiesta dalla tua applicazione. La versione corretta di .NET Framework dovrebbe essere già 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 il sito Web predefinito/, 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/sito Web predefinito che rimanda al percorso specificato.
- 11 Nell'area Impostazioni dell'applicazione, nella casella URL di controllo Health, digita un URL per Elastic Beanstalk da controllare 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, puoi specificare qualsiasi coppia di chiavi e valori che desideri aggiungere al `Web.config` file della tua applicazione.

Note


Sebbene non sia consigliato, è possibile utilizzare l'area Chiave e Valore per specificare AWS le credenziali con cui deve essere eseguita l'applicazione. L'approccio preferito consiste nello specificare un ruolo IAM nell'elenco a discesa del ruolo di Identity and Access Management nella pagina AWS Opzioni. Tuttavia, se devi utilizzare AWS le credenziali anziché un ruolo IAM per eseguire l'applicazione, nella riga Chiave, scegli `AWSAccessKey`. Nella riga Valore, digitare la chiave di accesso. Ripeti questi passaggi per `AWSecretKey`.

13. Seleziona Successivo.



14. Nella pagina Revisione, rivedi le opzioni configurate e seleziona la finestra Apri lo stato dell'ambiente alla chiusura del wizard.

15. Se tutto è corretto, scegliere Deploy (Distribuisci).


 Note

Quando si distribuisce l'applicazione, l'account attivo comporterà costi per leAWS 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. Al termine della distribuzione, verrà visualizzato un messaggio di conferma nella finestra Output.

16 Per eliminare la distribuzione, inAWS Explorer, espandere il nodo Elastic Beanstalk, aprire il menu contestuale (fare clic con il pulsante destro del mouse) per il sottonodo per la distribuzione, quindi scegliere Elimina. Il processo di eliminazione potrebbe richiedere alcuni minuti.

distribuzione di un'applicazione ASP.NET Core su Elastic Beanstalk (Legacy)

 Important

Questa documentazione fa riferimento a servizi e funzionalità precedenti. Per guide e contenuti aggiornati, consulta la guida agli [strumenti di distribuzioneAWS .NET](#) e il sommario aggiornato di [Deploying toAWS](#).

AWS Elastic Beanstalkè un servizio che semplifica il processo di approvvigionamentoAWS delle risorse per l'applicazione. AWS Elastic Beanstalkfornisce tutta l'AWSinfrastruttura necessaria per distribuire l'applicazione.

Il Toolkit for Visual Studio supporta la distribuzione di applicazioni ASP.NET Core perAWS l'utilizzo di 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 Beanstalksemplifica la distribuzione di applicazioni in una varietà di lingue diverse inAWS. Elastic Beanstalk supporta sia le applicazioni ASP.NET tradizionali che le applicazioni ASP.NET Core. Questo argomento descrive la distribuzione delle 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 implementare l'ASP tradizionale. Applicazioni NET, troverai che l'esperienza per ASP.NET Core è molto simile. Nei passaggi seguenti, esamineremo l'esperienza di distribuzione.

Se non hai mai usato il kit di strumenti prima d'ora, la prima cosa che dovrai fare dopo averlo installato è registrare AWS le tue credenziali con il kit di strumenti. Vedi [Come specificare le credenziali AWS di sicurezza per la tua applicazione](#) per la documentazione di Visual Studio per i dettagli su come eseguire questa operazione.

Per distribuire un'applicazione web ASP.NET Core, fare clic con il pulsante destro del mouse sul progetto in Solution Explorer e selezionare Pubblica su AWS....

Nella prima pagina della procedura guidata Publish to AWS Elastic Beanstalk deployment, 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 delle applicazioni. Gli ambienti contengono le AWS risorse effettive che eseguono una versione dell'applicazione. Ogni volta che distribuisce un'applicazione, una nuova versione dell'applicazione viene creata 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 Key pair. Le coppie di chiavi consentono di recuperare la password dell'amministratore di Windows in modo da poter accedere al computer. Se non hai già creato una key pair, potresti voler selezionare Crea nuova key pair.

Autorizzazioni

La pagina Autorizzazioni viene utilizzata per assegnare AWS credenziali alle istanze EC2 che eseguono l'applicazione. Questo è importante se l'applicazione utilizza il AWS SDK for .NET per

accedere ad altri AWS servizi. Se non utilizzi altri servizi della tua applicazione, puoi lasciare questa pagina come predefinita.

Opzioni dell'applicazione

I dettagli nella pagina Opzioni dell'applicazione sono diversi da quelli specificati durante la distribuzione delle applicazioni ASP.NET tradizionali. Qui, si specificano 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 delle opzioni dell'applicazione, fai clic su Avanti per esaminare 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, è possibile verificare lo stato dell'ambiente Elastic Beanstalk aprendo la vista dello stato dell'ambiente da AWS Explorer in Visual Studio.

Gli eventi vengono visualizzati nella barra di stato man mano che l'ambiente diventa online. Una volta completato tutto, lo stato dell'ambiente passerà allo stato sano. Puoi 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 distribuzione di qualsiasi applicazione richiederà un po' più tempo rispetto alle ridistribuzioni successive, poiché crea nuove AWS risorse. Mentre esegui iterazioni sull'applicazione durante lo sviluppo, puoi ridistribuirla rapidamente tornando indietro attraverso la 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 pacchetto di applicazioni nell'ambiente Elastic Beanstalk esistente.

Come specificare le AWS Credenziali di sicurezza per la tua applicazione

L'AWS Account specificato nella Pubblica su Elastic Beanstalk wizard è l'AWS Account che la procedura guidata utilizzerà per la distribuzione su Elastic Beanstalk.

Sebbene non sia consigliato, potrebbe essere necessario specificare le AWS credenziali dell'account che l'applicazione utilizzerà per accedere ai servizi AWS dopo che è stato distribuito. L'approccio preferito è quello di specificare un ruolo IAM. Nella Pubblica su Elastic Beanstalk procedura guidata,

È possibile eseguire questa operazione tramite Ruolo Identity and Access Management (elenco a discesa) della AWS Opzioni (Certificato creato). Nell'eredità Pubblicazione su Amazon Web Services procedura guidata, è possibile eseguire questa operazione tramite Ruolo IAM (elenco a discesa) della AWS Opzioni (Certificato creato).

Se è necessario utilizzare le credenziali dell'account invece di un ruolo IAM, è possibile specificare le credenziali dell'account per la candidatura in uno dei seguenti modi:

- Fare riferimento a un profilo corrispondente alle credenziali dell'account nella appSettings elemento del progetto `Web.config`. (Per creare un profilo, consulta [Configurazione di 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 usi la Pubblicazione su Elastic Beanstalk wizard, sulle Opzioni dell'applicazione (Tag) della Chiave di accesso (Chiave) Chiave e Valore area, scegli `AWSAccessKey`. Nella Valore row (Chiave di accesso). Ripetere queste fasi per `AWSecretKey`.
- Se usi l'eredità Pubblicazione su Amazon Web Services wizard, sulle Opzioni dell'applicazione (Tag) della Credenziali dell'applicazione area, scegli `Use` queste credenziali e quindi digitare la chiave di accesso e la chiave di accesso segreta nella Chiave di accesso e Chiave segreta (Creare copie?)

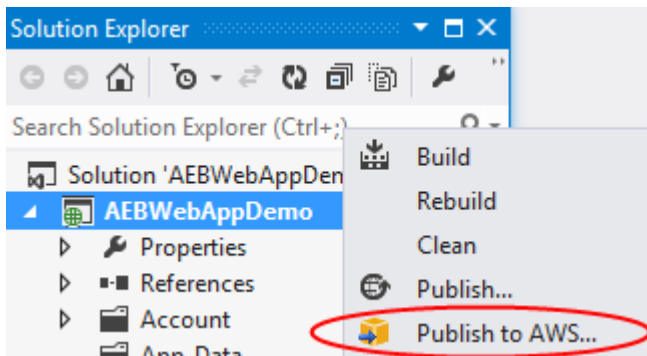
Come ripubblicare la tua applicazione in un ambiente Elastic Beanstalk (Legacy)

Important

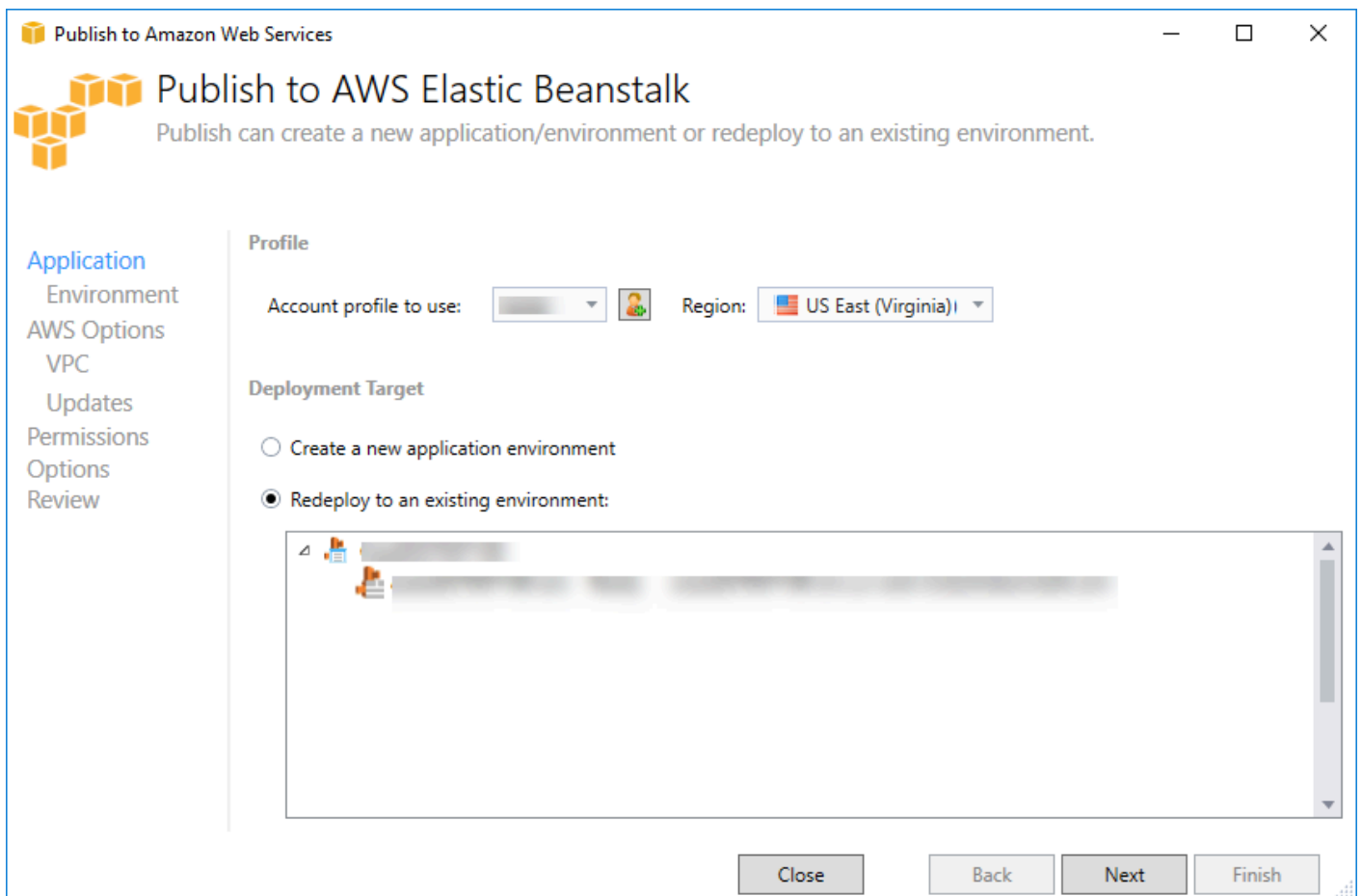
Questa documentazione fa riferimento a servizi e funzionalità precedenti. Per guide e contenuti aggiornati, consulta la guida agli [strumenti di distribuzione AWS .NET](#) e il sommario aggiornato di [Deploying to AWS](#).

Puoi iterare sulla tua applicazione apportando modifiche discrete e quindi ripubblicando una nuova versione nel tuo ambiente Elastic Beanstalk già avviato.

1. In Solution Explorer (Esplora soluzioni), apri il menu contestuale (fai clic con il pulsante destroWebAppDemo del mouse) per la cartella del progetto AEB per il progetto pubblicato nella sezione precedente e scegli Pubblica suAWS Elastic Beanstalk.

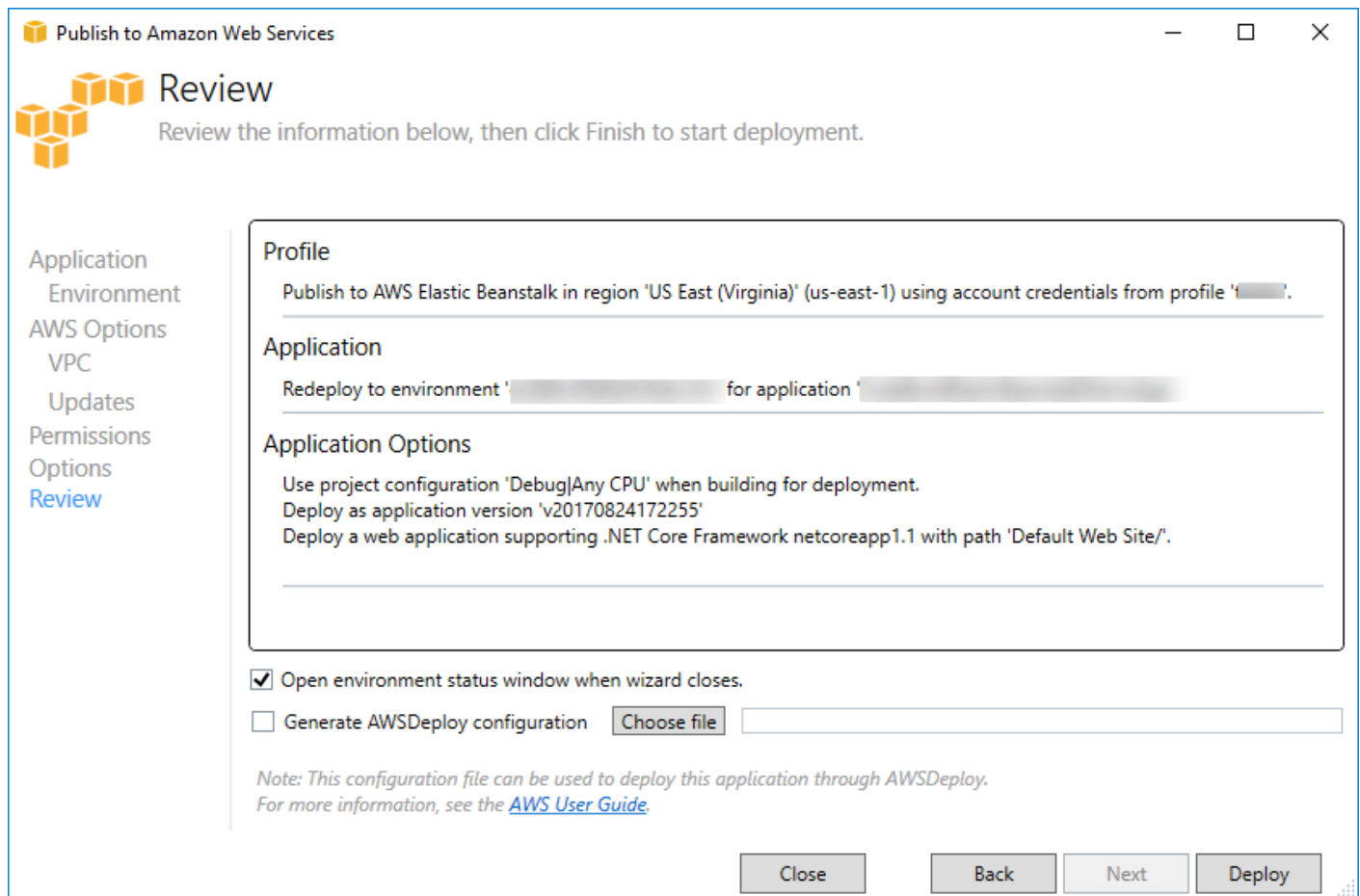


Si apre la procedura guidata Publish to Elastic Beanstalk (Pubblica su Elastic Beanstalk).



2. Seleziona Redistribuisce in un ambiente esistente e scegli l'ambiente in cui hai pubblicato in precedenza. Fai clic su Next (Successivo).

Viene visualizzata la procedura guidata di revisione.



3. Fai clic su Distribuisci. L'applicazione verrà ridistribuita nello stesso ambiente.

Non puoi ripubblicare se la tua applicazione è in fase di avvio o chiusura.

Distribuzioni di applicazioni di Elastic Beanstalk

In questo argomento viene descritto come il manifesto di distribuzione per il contenitore Microsoft Windows di Elastic Beanstalk supporta le distribuzioni di applicazioni personalizzate.

Le distribuzioni di applicazioni personalizzate sono una potente funzionalità per gli utenti avanzati che desiderano sfruttare la potenza di Elastic Beanstalk per creare e gestire il loro AWS risorse, ma vogliono un controllo completo su come viene distribuita la loro applicazione. Per una distribuzione personalizzata di applicazioni, è possibile creare script di Windows PowerShell 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 `RestartAppServer` L'API viene richiamata dal toolkit o dalla console Web e la disinstallazione che viene richiamata su qualsiasi distribuzione precedente ogni volta che si verifica una nuova distribuzione.

Ad esempio, è possibile che si disponga di un'applicazione ASP.NET che si desidera distribuire mentre il team di documentazione ha scritto un sito Web statico che desidera includere nella distribuzione. Puoi farlo scrivendo il manifest 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 rispetto al file manifest di distribuzione. Per questo esempio, il pacchetto di applicazioni conterrà anche un file `documentation.zip` che contiene un sito Web statico creato dal team di documentazione.

`Install.ps1` script estrae il file zip e imposta 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 richiederà un ripristino di IIS.

```
iisreset /timeout:1
```

Per la disinstallazione degli script, è importante pulire 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 pacchetto dell'applicazione, la distribuzione crea l'applicazione ASP.NET e quindi distribuisce il sito della documentazione.

Per questo esempio, scegliamo un semplice esempio che distribuisce un semplice sito Web statico, ma con la distribuzione di applicazioni personalizzate è possibile distribuire qualsiasi tipo di applicazione e consentire a Elastic Beanstalk di gestire il AWS risorse per questo.

Distribuzioni personalizzate di ASP.NET Core Elastic Beanstalk

In questo argomento viene descritto come funziona la distribuzione e cosa è possibile 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 nel Toolkit for Visual Studio, il toolkit raggruppa l'applicazione e la invia a Elastic Beanstalk. Il primo passo nella creazione del bundle di applicazioni consiste nell'utilizzare la nuova CLI `dotnet` per preparare l'applicazione per la pubblicazione utilizzando il `dotnet publish` comando. Il framework e la configurazione vengono trasmessi dalle impostazioni della procedura guidata al `dotnet publish` comando. Quindi se hai selezionato `Rilascio per configurazione netcore app 1.0 per framework`, il toolkit eseguirà il seguente comando:

```
dotnet publish --configuration Release --framework netcoreapp1.0
```

Quando il comando termina, 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 si desidera 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 proprietà `appBundle` indica dove i bit dell'applicazione sono in relazione al file manifesto. Questa proprietà può puntare a una directory o a un archivio ZIP. Le proprietà `iisPath` e `iisWebSite` indicano dove in IIS ospitare l'applicazione.

Personalizzazione del Manifest

Il toolkit scrive il file manifest solo se non esiste già nella cartella di pubblicazione. Se il file esiste, il toolkit aggiorna le proprietà `appBundle`, `iisPath` e `iisWebSite` nella prima applicazione elencata sotto la sezione `aspNetCoreWeb` del manifest. In questo modo è possibile aggiungere `aws-windows-deployment-manifest.json` al tuo progetto e personalizza il manifesto. A tale scopo, per un'applicazione Web ASP.NET Core in Visual Studio, aggiungere un nuovo file JSON alla radice del progetto e denominarlo `aws-windows-deployment-manifest.json`.

Il manifesto deve essere denominato `aws-windows-deployment-manifest.json` e deve essere alla radice del progetto. Il contenitore Elastic Beanstalk cerca il manifesto nella radice e, se viene rilevato,

richiamerà lo strumento di distribuzione. Se il file non esiste, il contenitore Elastic Beanstalk torna al vecchio strumento di distribuzione, il che presuppone che l'archivio sia unmsdeployarchivio.

Per garantire la CLI `dotnetpublish` comando include il manifest, aggiorna il `project.json` file per includere il file manifest nella sezione `Includi sottoinclude nel publishOptions`.

```
{
  "publishOptions": {
    "include": [
      "wwwroot",
      "Views",
      "Areas/**/Views",
      "appsettings.json",
      "web.config",
      "aws-windows-deployment-manifest.json"
    ]
  }
}
```

Ora che hai dichiarato il manifest in modo che sia incluso nel bundle dell'app, puoi configurare ulteriormente il modo in cui vuoi distribuire l'applicazione. È possibile personalizzare la distribuzione oltre a quanto supportato dalla procedura guidata di distribuzione. AWS ha definito uno schema JSON per `aws-windows-deployment-manifest.json` quando è stato installato il Toolkit for Visual Studio, l'impostazione ha registrato l'URL per lo schema.

Quando apri `windows-deployment-manifest.json`, vedrai l'URL dello schema selezionato nella casella a discesa `Schema`. È possibile passare all'URL per ottenere una descrizione completa di ciò che è possibile impostare nel manifesto. Con lo schema selezionato, Visual Studio fornirà IntelliSense durante la modifica del manifesto.

Una personalizzazione che puoi fare è configurare il pool di applicazioni IIS in cui verrà eseguita l'applicazione. Nell'esempio seguente viene illustrato come definire un pool di applicazioni IIS («CustomPool») che ricicla il processo ogni 60 minuti e lo assegna all'applicazione utilizzando `"appPool": "customPool"`.

```
{
  "manifestVersion": 1,
  "iisConfig": {
    "appPools": [
      {
```

```
        "name": "customPool",
        "recycling": {
            "regularTimeInterval": 60
        }
    }
],
},
"deployments": {
    "aspNetCoreWeb": [
        {
            "name": "app",
            "parameters": {
                "appPool": "customPool"
            }
        }
    ]
}
}
```

Inoltre, il manifest può dichiarare l'esecuzione degli script di Windows PowerShell prima e dopo l'installazione, il riavvio e la disinstallazione delle azioni. Ad esempio, il manifest seguente esegue lo script di Windows PowerShell `PostInstallSetup.ps1` per eseguire ulteriori operazioni di configurazione dopo che l'applicazione ASP.NET Core è stata distribuita in IIS. Quando aggiungete script come questo, assicuratevi che gli script vengano aggiunti alla sezione `Includi` sotto `publishOptions` nel `project.json` file, proprio come hai fatto con `ilaws-windows-deployment-manifest.json` file. In caso contrario, gli script non verranno inclusi come parte della CLI di `dotnetpublicocomando`.

```
{
  "manifestVersion": 1,
  "deployments": {
    "aspNetCoreWeb": [
      {
        "name": "app",
        "scripts": {
          "postInstall": {
            "file": "SetupScripts/PostInstallSetup.ps1"
          }
        }
      }
    ]
  }
}
```

```
}
```

Che ne dici delle estensioni .eb?

Beanstalk Elastic Beanstalk.ebextensions file di configurazione sono supportati come con tutti gli altri contenitori Elastic Beanstalk. Per includere .ebextensions in un'applicazione ASP.NET Core, aggiungere il .ebextensionsdirectory dellainclude sezione sottopublishOptionsnellaproject.jsonfile. Per ulteriori informazioni su .ebextensions, consulta [ilGuida per sviluppatori Elastic Beanstalk](#).

Support di più applicazioni per .NET e Elastic Beanstalk

Utilizzando il manifest di distribuzione, è possibile distribuire più applicazioni nello stesso ambiente Elastic Beanstalk.

Il manifest di distribuzione supporta [ASP.NET Core](#) applicazioni web e archivi msdeploy per le applicazioni ASP.NET tradizionali. Immagina uno scenario in cui hai scritto una nuova straordinaria applicazione utilizzando ASP.NET Core per il frontend e un progetto API Web per un'API di estensioni. Hai anche un'app di amministrazione che hai scritto utilizzando ASP.NET tradizionale.

La procedura guidata di distribuzione del toolkit si concentra sulla distribuzione di un singolo progetto. Per trarre vantaggio dalla 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 soluzione.

La sezione di distribuzione nel manifest ha due figli: un array di applicazioni Web ASP.NET Core da distribuire e un array di archivi msdeploy da distribuire. Per ogni applicazione, è possibile impostare il percorso IIS e la posizione dei bit dell'applicazione rispetto al manifest.

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

Con il manifest scritto, utilizzerai Windows PowerShell per creare il bundle di applicazioni e aggiornare un ambiente Elastic Beanstalk esistente per eseguirlo. Lo script viene scritto supponendo che venga eseguito dalla cartella contenente la soluzione Visual Studio.

La prima cosa da fare nello script è impostare una cartella del workspace in cui creare il bundle 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
}
```

Una volta creata la cartella, è ora di preparare il frontend. Come per la procedura guidata di distribuzione, utilizzare l'interfaccia a riga di comando di 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
```

Notate che la sottocartella «frontend» è stata utilizzata per la cartella di output, corrispondente alla cartella impostata nel manifest. Ora è necessaria la stessa operazione per il progetto dell'API Web.

```
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 l'interfaccia a riga di comando dotnet. Per l'applicazione admin, dovresti usare msbuild, passando il pacchetto target di build per creare l'archivio msdeploy. Per impostazione predefinita, la destinazione del pacchetto crea l'archivio msdeploy sottoobj\Release\Packagecartella, 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, copiare il manifest dalla soluzione nell'area di lavoro di pubblicazione e quindi comprimere 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 sulla console Web e caricare l'archivio in un ambiente Elastic Beanstalk. In alternativa, è possibile continuare a utilizzare ilAWSCmdlet PowerShell per aggiornare l'ambiente Elastic Beanstalk con il bundle dell'applicazione. Assicurati di aver impostato il profilo e la regione correnti sul profilo e sulla regione che contiene l'ambiente Elastic Beanstalk utilizzandoSet-AWSCredentialiseSet-DefaultAWSRegionCmdlet .

```
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, sarà possibile passare a ciascuna delle applicazioni distribuite nel percorso IIS impostato nel manifest di distribuzione.

Implementazione in Amazon EC2 Container Service

Important

Il nuovo Publish to (Pubblica in CloudWatch)AWS è progettata per semplificare il modo in cui si pubblicano le applicazioni.NETAWS. Potrebbe esserti chiesto se vuoi passare a questa esperienza di pubblicazione dopo aver scelto Pubblica Container inAWS. Per ulteriori informazioni, consultare [Utilizzo di Pubblica in CloudWatchAWS in Visual Studio](#).

Amazon Elastic Container Service è un servizio di gestione dei contenitori ad alte prestazioni altamente scalabile, che supporta contenitori Docker e consente di eseguire con facilità le applicazioni in un cluster gestito di istanze Amazon EC2.

Perché le applicazioni possano essere distribuite su Amazon Elastic Container Service, i relativi componenti devono essere sviluppati per l'esecuzione 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 sezioni seguenti.

Per ulteriori informazioni su Amazon ECS, vai alla [Documentazione Elastic Container](#). Include una panoramica di [Nozioni di base su Docker](#) e [creazione di un cluster](#).

Argomenti

- [Specifica AWS Credenziali per la tua applicazione ASP.NET Core 2](#)
- [Distribuzione di un'app ASP.NET Core 2.0 su Amazon ECS \(Fargate\) \(Legacy\)](#)
- [Distribuzione di un'applicazione ASP.NET Core 2.0 su Amazon ECS \(EC2\)](#)

Specifica AWS Credenziali per la tua applicazione ASP.NET Core 2

Quando si distribuisce l'applicazione in un contenitore Docker sono disponibili due tipi di credenziali: credenziali di distribuzione e credenziali di istanza.

Le credenziali di distribuzione vengono utilizzate dal contenitore Pubblica su AWS procedura guidata per creare l'ambiente in Amazon ECS. Ciò include attività, servizi, ruoli IAM, un repository contenitore Docker e, se lo si sceglie, un bilanciamento del carico.

Le credenziali di istanza vengono utilizzate dall'istanza (inclusa l'applicazione) per accedere a diversi AWS Servizi. Ad esempio, se un'applicazione ASP.NET Core 2.0 legge e scrive su oggetti Amazon S3, è necessario disporre delle autorizzazioni appropriate. È possibile fornire credenziali diverse utilizzando metodi diversi in base all'ambiente. Ad esempio, l'applicazione ASP.NET Core 2 potrebbe essere destinata a Sviluppo e Produzione ambienti. È possibile utilizzare un'istanza Docker locale e credenziali per lo sviluppo e un ruolo definito nella produzione.

Specifica delle credenziali di distribuzione

La AWS account specificato nel Pubblica container su AWS la procedura guidata è la 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 si notano opzioni mancanti negli elenchi a discesa, è possibile che non vi siano autorizzazioni. Ad esempio, se hai creato un cluster per la tua applicazione ma non lo vedi sul Pubblica container su AWS pagina cluster wizard. Se ciò accade, aggiungi le autorizzazioni mancanti e riprova la procedura guidata.

Specifica delle credenziali dell'istanza di sviluppo

Per gli ambienti non di produzione, puoi configurare le credenziali nelle impostazioni delle app. <environment>.json. Ad esempio, per configurare le credenziali nel file AppSettings.development.json in Visual Studio 2017:

1. Aggiungi il pacchetto AWSSDK.Extensions.NETCore.Setup NuGet al progetto.
2. InserisciAWSimpostazioni per AppSettings.Development.json. La configurazione sottostante impostaProfileeRegion.

```
{
  "AWS": {
    "Profile": "local-test-profile",
    "Region": "us-west-2"
  }
}
```

Specifica delle credenziali dell'istanza di produzione

Per le istanze di produzione, si consiglia di utilizzare un ruolo IAM per controllare l'accesso dell'applicazione (e del servizio). Ad esempio, per configurare un ruolo IAM con Amazon ECS come entità del servizio con le autorizzazioni per Amazon Simple Storage Service e Amazon DynamoDB dalAWS Management Console:

1. Accedi alla AWS Management Console e apri la console di IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione della console IAM, scegliere Ruoli e quindi Crea ruolo.
3. SelezionaAWSService (Servizio)tipo di ruolo, quindi scegliEC2 Container Service.
4. SelezionaAttività EC2 Container Servicecaso d'uso. I casi d'uso sono definiti dal servizio in modo da includere la policy di attendibilità richiesta dal servizio. Quindi scegli Next (Successivo): Autorizzazioni.
5. SelezionaAmazonS3FullAccessAmazonDynamoDBFullAccesspolicy di autorizzazione. Selezionare la casella accanto a ciascun criterio, quindi scegliereSuccessivo: Review (Revisione),
6. PerRole Name (Nome ruolo), digitare un nome del ruolo o un suffisso del nome del ruolo per facilitare l'identificazione dello scopo del ruolo. I nomi dei ruoli devono essere univoci all'interno dell'account AWS. Non fanno distinzione tra maiuscole e minuscole. Ad esempio, non è possibile

creare ruoli denominati sia `PRODR0LE` che `prod0r0le`. 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 attività sulla Definizione attività ECS pagina della Pubblica container su AWS mago.

Per ulteriori informazioni, consulta [Utilizzo di 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 distribuzione AWS .NET](#) e il sommario aggiornato di [Deploying to AWS](#).

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.

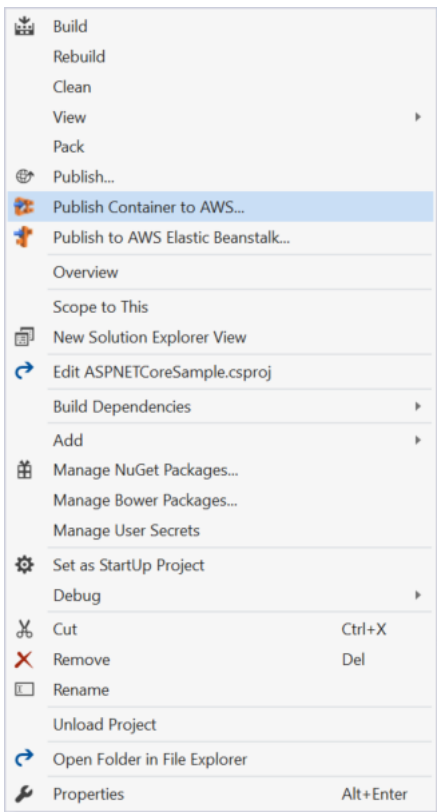
Prima di pubblicare il contenitore

Prima di utilizzare la AWS procedura guidata Publish Container to per distribuire l'applicazione ASP.NET Core 2.0:

- [Specifica AWS le tue credenziali](#) e [esegui 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 allaAWS procedura guidata Publish Container to

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 Pubblica contenitore suAWS.



È inoltre possibile selezionare Pubblica contenitoreAWS su nel menu Build di Visual Studio.

Pubblica contenitore suAWS Wizard

Publish Container to AWS

Select the Amazon ECR Repository to push the Docker image to.

Profile

Account profile to use: vstools Region: US East (Virginia)

Docker Image Build

Configuration: Release

Docker Repository: aspnetcoresample Tag: latest

Deployment Target

Service on an ECS Cluster

Deploy the application as a service on an Amazon Elastic Container Service Cluster. A service is for applications like Web applications that are intended to run indefinitely.

Save settings to aws-ecs-tools-defaults.json and configure project for command line deployment.

If this is checked the dotnet CLI tool package Amazon.ECS.Tools will be added to the project. Once added you can do future deployments from the command line. Run the command "dotnet ecs --help" for more information.

Close Back Next Publish

Profilo dell'account da utilizzare: seleziona un profilo dell'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 della 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 compilazione.

Etichetta: seleziona un tag esistente o digita il nome di un nuovo tag. I tag possono tenere traccia di dettagli importanti come la versione, le opzioni o altri elementi di configurazione unici del contenitore Docker.

Obiettivo di distribuzione: selezionare il servizio su un cluster ECS. Utilizzate 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` Utilizzatelo dalla directory del progetto per distribuire ed `dotnet ecs publish` dal contenitore.

Avvio della pagina di configurazione

Publish Container to AWS

aws Launch Configuration
Choose how to provide compute capacity to your application.

ECS Cluster:

This wizard supports creating an empty cluster which is suitable for running Fargate based services and tasks. It will not have any EC2 instances registered to it so services and tasks with the EC2 launch type will not run. The easiest way to create a cluster with EC2 instances registered is to use the AWS web console.

Launch Type:

FARGATE will automatically provision the necessary compute capacity needed to run the application based on the CPU and Memory settings. This removes the need to add any EC2 instances to your cluster.

Allocated Compute Capacity

CPU Maximum (vCPU): Memory Maximum (GB):

Network Configuration

VPC Subnets: Security Groups:

Assign Public IP Address

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 lancio: 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, vedi [dimensione dell'attività](#).

Memoria massima (GB): seleziona la quantità massima di memoria disponibile per l'applicazione.

Sottoreti VPC: scegli una o più sottoreti in un singolo VPC. Se scegli più di una sottorete, le tue attività verranno distribuite tra 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 sia il traffico in entrata che in uscita a livello di istanza.

I [gruppi di sicurezza predefiniti](#) sono configurati per consentire il traffico in entrata da istanze assegnate allo stesso gruppo di sicurezza e tutto il traffico IPv4 in uscita. È necessario consentire l'uscita in modo che il servizio possa raggiungere il repository dei container.

Assegna un indirizzo IP pubblico: seleziona questa opzione per rendere la tua attività accessibile da Internet.

Pagina di configurazione del servizio

Publish Container to AWS

aws Service Configuration
Choose the number of instances of the service and how the instances should be deployed.

Service Parameters

Deploying an application as a service is good for web applications or long lived services. If any of your tasks should fail or stop for any reason, the Amazon ECS service scheduler will launch another instance of your application to replace the failed instance.

Service:

Number of Tasks:

Minimum Healthy Percent:

Maximum Percent:

Servizio: seleziona uno dei servizi nel menu a discesa per distribuire il container 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 nel cluster. Ogni attività è un'istanza del tuo contenitore.

Percentuale minima di integrità: percentuale di attività che devono rimanere in RUNNING stato durante una distribuzione arrotondata al numero intero più vicino.

Percentuale massima: la percentuale di attività consentite PENDING nello stato RUNNING o durante una distribuzione arrotondata al numero intero più vicino.

Pagina Application Load Balancer

aws Application Load Balancer Configuration

Using an Application Load Balancer allows multiple instances of the application be accessible through a single URL endpoint.

Configure Application Load Balancer

It is recommended for web applications to use an Application Load Balancer which allows containers to use dynamic host port mapping. This will give the ability to run multiple instances of the web applications on the same container host without contention for port 80.

Load Balancer:

Listener Port:

Load Balancer Target Group

The Application Load Balancer will send requests to the Target Group if the request matches the specified URL path pattern. Amazon ECS will register all instances of the container with their dynamic port to the Target Group using the provided IAM role for the service.

Target Group:

Path Pattern:

Health Check Path:

Close Back Next Publish

Configura Application Load Balancer: seleziona per configurare un sistema di bilanciamento del carico delle applicazioni.

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 porta80, è appropriata per la maggior parte delle applicazioni Web.

Gruppo target: seleziona il gruppo target a cui Amazon ECS registrerà le attività nel servizio.

Path Pattern: il load balancer utilizzerà un routing basato su percorsi. Accetta il valore predefinito/ o fornisci uno schema diverso. Il modello di percorso non distingue tra maiuscole e minuscole, può avere una lunghezza massima di 128 caratteri e contenere un [set di caratteri selezionato](#).

Percorso di controllo dello stato di Health: il percorso di ping che è 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 sanitario fallirà e sarà considerato malsano.

Se distribuisce 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 di attività

aws Task Definition
Task Definition defines the parameters for how the application will run within its Docker container.

Task Definition:

Container:

Permissions

Task Role:

Select an IAM role to provide AWS credentials to your application to access AWS Services.

Task Execution Role:

Fargate requires a role to pull private images and publish logs on your behalf.

Port Mapping		Environment Variables	
Container Port		Variable	Value
80	<input type="checkbox"/>	ASPNETCORE_ENVIRONMENT	Production <input type="checkbox"/>

Definizione attività: seleziona una definizione di attività esistente o scegli Crea nuovo e digita il nome della nuova definizione dell'attività.

Contenitore: seleziona un contenitore esistente o scegli Crea nuovo e digita il nuovo nome del contenitore.

Ruolo dell'attività: seleziona un ruolo IAM con le credenziali necessarie alla tua app per accedere ai AWS Servizi. Ecco come vengono passate le credenziali alla tua applicazione. Scopri [come specificare le credenziali AWS di sicurezza per la tua applicazione](#).

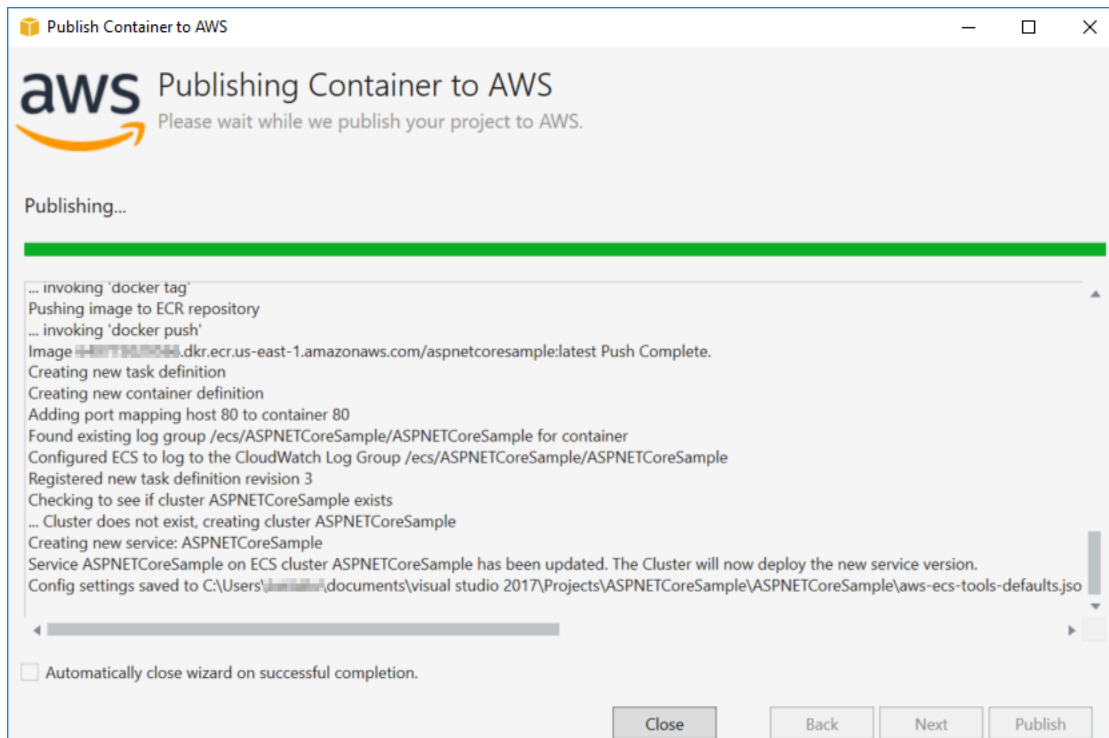
Ruolo di esecuzione delle attività: seleziona un ruolo con le autorizzazioni per estrarre immagini private e pubblicare registri. AWS Fargate utilizzerà l'operazione per tuo conto.

Mappatura delle porte: scegli il numero di porta nel container associato alla porta dell'host assegnato automaticamente.

Variabili d'ambiente: aggiungi, modifica o elimina le variabili di ambiente per il contenitore. Puoi modificarlo per adattarlo alla tua distribuzione.

Quando sei soddisfatto della configurazione, fai clic su **Pubblica** per iniziare il processo di distribuzione.

Contenitore di pubblicazione suAWS



Gli eventi vengono visualizzati durante la distribuzione. La procedura guidata viene chiusa automaticamente al completamento. È possibile sostituire questo deselegionando la casella nella parte inferiore della pagina.

Puoi trovare l'URL delle tue nuove istanze inAWS Explorer. Espandi Amazon ECS e Clusters, quindi fai clic sul tuo cluster.

Distribuzione di un'applicazione ASP.NET Core 2.0 su Amazon ECS (EC2)

In questa sezione viene descritto come utilizzare ilPubblica container suAWS, fornita come parte del Toolkit for Visual Studio, per distribuire un'applicazione ASP.NET Core 2.0 containerizzata indirizzata a Linux tramite Amazon ECS utilizzando il tipo di lancio EC2. Poiché un'applicazione Web si intende eseguire in maniera continua, verrà distribuita come un servizio.

Prima di pubblicare il contenitore

Prima di utilizzare ilPubblica container suAWSper distribuire l'applicazione ASP.NET Core 2.0:

- [Specificare il tuoAWScredenziale](#)e[Configurazione con Amazon ECS](#).
- [Installazione di Docker](#). È possibile utilizzare diverse opzioni di installazione tra cui[Docker per Windows](#).

- [Creazione di un cluster Amazon ECS](#) in base alle esigenze della tua applicazione web. Bastano pochi passi.
- In Visual Studio, crea (o apri) un progetto per un'app containerizzata ASP.NET Core 2.0 destinata a Linux.

Accesso al contenitore Pubblica suAWS

Per distribuire un'applicazione ASP.NET Core 2.0 containerizzata indirizzata a Linux, fare clic con il tasto destro del mouse sul progetto in Solution Explorer (Esplora soluzioni) e selezionare **Pubblica container suAWS**.

È anche possibile selezionare **Pubblica container suAWS** nel menu **Build (Build)** di Visual Studio.

Pubblica container suAWS Wizard

Profilo dell'account da utilizzare- Scegliere un profilo account da utilizzare.

Region- Scegli una regione di distribuzione. Profilo e regione vengono utilizzati per configurare le risorse dell'ambiente di distribuzione e selezionare il registro Docker predefinito.

Configurazione- Selezionare la configurazione della creazione di immagini Docker.

Repository Docker- Scegliere un repository Docker esistente o digitare il nome di un nuovo repository e verrà creato. Questo è il repository a cui viene trasferita l'immagine del contenitore incorporata.

Tagging di- Selezionare un tag esistente o digitare 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 **Servizio** su un cluster ECS. Utilizzare questa opzione di distribuzione quando l'applicazione è pensata per essere in esecuzione prolungata (come un'applicazione Web ASP.NET Core 2.0).

Salvataggio delle impostazioni in `aws-docker-tools-defaults.json` configura il progetto per la distribuzione da riga di comando- Selezionare questa opzione se si desidera la flessibilità di distribuzione dalla riga di comando. Utilizzare `dotnet ecs deploy` dalla directory del progetto per distribuire e `dotnet ecs publish` il container.

Pagina di avvio della configurazione

Cluster ECS- Scegli il cluster che eseguirà l'immagine Docker. È possibile [Creazione di un cluster ECS](#) utilizzando il [AWS Console](#) di gestione.

Tipo di lancio- Scegliere EC2. Per utilizzare il tipo di lancio Fargate, vedi [Distribuzione di un'applicazione ASP.NET Core 2.0 su Amazon ECS \(Fargate\)](#).

Pagina di configurazione del servizio

Service (Servizio)- Selezionare uno dei servizi nel menu a discesa per distribuire il contenitore in un servizio esistente. Oppure scegli [Creazione di nuovi](#) per creare un servizio nuovo. 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 nel cluster. Ogni attività è un'istanza del container.

Percentuale di salute minima- La percentuale di attività che devono rimanere `RUNNING` durante una distribuzione arrotondata per eccesso al valore intero più vicino.

Percentuale massimo- La percentuale di attività consentite nel `RUNNING` o `PENDING` durante una distribuzione arrotondata per difetto al valore intero più vicino.

Modelli di collocamento- Selezionare un modello di posizionamento delle attività.

Quando lanci un'attività in un cluster, Amazon ECS deve determinare dove posizionare l'attività in base ai requisiti specificati nella definizione dell'attività, ad esempio memoria e CPU. 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** (BinPack bilanciato tra zone di disponibilità): consente di distribuire le attività tra zone di disponibilità e istanze di container con la quantità minima di memoria disponibile.
- **BinPack**: consente di distribuire le attività in base alla quantità minima di memoria o CPU disponibile.

- **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 [Posizionamento delle attività di Amazon ECS](#).

Pagina di Application Load Balancer

Configurare Application Load Balancer- Controllare se configurare un Application Load Balancer.

Seleziona il ruolo IAM per il servizio- Seleziona un ruolo esistente o scegli Creazione di nuove verrà creato un nuovo ruolo.

Sistema di bilanciamento del carico- Selezionare un bilanciatore del carico esistente o scegliere Creazione di nuove digitare il nome del nuovo bilanciamento del carico.

Porta del listener- Seleziona una porta listener esistente o scegli Creazione di nuove digitare un numero di porta. La porta predefinita 80, è adatto per la maggior parte delle applicazioni web.

Gruppo di destinazione- Per impostazione predefinita, il bilanciatore del carico invia le richieste alle destinazioni registrate utilizzando la porta e il protocollo specificati per il gruppo target. È possibile sostituire questa porta al momento della registrazione di ogni target con il gruppo target.

Path Pattern (Modello di percorso)- Il bilanciatore del carico utilizzerà l'instradamento basato sul percorso. Accettare il valore predefinito/o fornire un modello diverso. Il modello di percorso non distingue tra maiuscole e minuscole, può avere una lunghezza massima di 128 caratteri e contenere [unselezione set di caratteri](#).

Percorso di controllo Health- Il percorso ping, ovvero il percorso per i controlli dello stato dei target. Per impostazione predefinita, è/ed è adatto per le applicazioni web. Se necessario, inserisci un percorso diverso. Se il percorso immesso non è valido, il controllo dello stato fallirà e sarà considerato malsano.

Se si distribuiscono più servizi e ogni servizio verrà distribuito in un percorso o una posizione diversi, è possibile che siano necessari percorsi di controllo personalizzati.

Pagina Definizione attività ECS

Definizione delle attività- Selezionare una definizione dell'attività esistente o scegliere Creazione di nuove digitare il nome della nuova definizione dell'attività.

Container- Seleziona un contenitore esistente o scegli la creazione di un nuovo contenitore.

Memoria (MiB)- Fornire valori per il limite flessibile e il limite rigido o entrambi.

La **soft limit** (in MiB) della memoria da prenotare per il container. Docker tenta di mantenere la memoria del container sotto il limite flessibile. A seconda di quale evento si verifica prima, il container può consumare più memoria, fino al limite rigido specificato con il parametro della memoria (se applicabile) o tutta la memoria disponibile sull'istanza di container, a seconda di quale evento si verifica prima.

La **limit rigido** (in MiB) della memoria da presentare al container. Se il container tenta di superare la memoria specificata qui, viene terminato.

Ruolo attività- Selezionare un ruolo di attività per un ruolo IAM che consente al contenitore di chiamare le API AWS specificate nelle policy associate per conto dell'utente. Ecco come vengono passate le credenziali alla tua applicazione. Consulta [come specificare le credenziali di sicurezza per la tua applicazione](#).

Mappatura porte- Aggiungere, modificare o eliminare i mappature delle porte per il container. Se un bilanciamento del carico è attivo, la porta host sarà predefinita su 0 e l'assegnazione della porta sarà dinamica.

Variabili di ambiente- Aggiungere, modificare o eliminare le variabili d'ambiente per il container.

Quando si è soddisfatti della configurazione, fare clic su **Pubblica** per iniziare il processo di distribuzione.

Pubblicazione in container 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 nuove istanze nel **AWS Explorer**. Espandere **Amazon ECS e Clusters** (Cluster), quindi fare clic sul cluster.

Risoluzione dei problemi relativi al AWS Toolkit for Visual Studio

Le sezioni seguenti contengono informazioni generali sulla risoluzione dei problemi relativi ai AWS servizi del toolkit AWS Toolkit for Visual Studio e all'utilizzo 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](#)
- [Amazon CodeWhisperer Sign In e Sign Out sono disattivati](#)

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.

- 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 registri 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

Come localizzare i log del AWS Toolkit

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.

Amazon CodeWhisperer Sign In e Sign Out sono disattivati

Se riscontri un problema con il CodeWhisperer servizio in cui entrambe le voci del menu Accedi e Esci sono disattivate, risolvi il problema completando i seguenti passaggi.

1. Da Windows File Explorer, vai alla cartella cache AWS Toolkit che si trova in: %LOCALAPPDATA%\aws\toolkits/language-servers/CodeWhisperer
2. Cancella il contenuto della cartella cache.
3. Chiudi e riapri la soluzione corrente.

Sicurezza per AWS Toolkit for Visual Studio

La sicurezza cloud di Amazon Web Services (AWS) è la priorità più alta. In quanto cliente AWS, è possibile trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza. La sicurezza è una responsabilità condivisa tra te e 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](#)
- [Identity and Access Management](#)
- [Convalida della conformità per questo AWS prodotto o servizio](#)
- [Resilienza per questo AWS prodotto o servizio](#)
- [Sicurezza dell'infrastruttura per questo AWS prodotto o servizio](#)
- [Analisi della configurazione e delle vulnerabilità in AWS Toolkit for Visual Studio](#)

Protezione dei dati in AWS Toolkit for Visual Studio

Il modello di [responsabilità AWS condivisa modello](#) di di si applica alla protezione dei dati in AWS Toolkit for Visual Studio. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Questi contenuti includono la configurazione della

protezione e le attività di gestione per i servizi Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [Modello di responsabilità condivisa AWS e GDPR](#) nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-2](#).

Ti consigliamo vivamente di non inserire mai informazioni 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 Toolkit for Visual Studio o Servizi AWS altro utilizzando la console, l'API AWS o gli AWS CLI SDK. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

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](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come Servizi AWS lavorare con IAM](#)
- [Risoluzione dei problemi di AWS identità e accesso](#)

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 ti 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 inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS, 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 essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi [Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente](#).

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta [Signing AWS API request](#) nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta [Autenticazione a più fattori](#) nella Guida per l'utente di AWS IAM Identity Center e [Utilizzo dell'autenticazione a più fattori \(MFA\) in AWS](#) nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta [Cos'è Centro identità IAM?](#) nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un [utente IAM](#) è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina [Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente di IAM.

Un [gruppo IAM](#) è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta [Quando creare un utente IAM \(invece di un ruolo\)](#) nella Guida per l'utente di IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console [cambiando ruolo](#). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per

ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta [Utilizzo di ruoli IAM](#) nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta [Creazione di un ruolo per un provider di identità di terza parte](#) nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .
- **Autorizzazioni utente IAM temporanee:** un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso multi-account:** è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.
- **Accesso a più servizi:** alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
- **Sessioni di accesso diretto (FAS):** quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina [Forward access sessions](#).

- **Ruolo di servizio:** un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS](#) nella Guida per l'utente di IAM.
- **Ruolo collegato al servizio:** un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- **Applicazioni in esecuzione su Amazon EC2:** puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Cloud è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta [Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2](#) nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta [Quando creare un ruolo IAM \(invece di un utente\)](#) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM

può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'azione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruoli IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scelta fra policy gestite e policy inline](#) nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta [Panoramica delle liste di controllo degli accessi \(ACL\)](#) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- **Limiti delle autorizzazioni:** un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- **Politiche di controllo dei servizi (SCP):** le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .
- **Policy di sessione:** le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [Policy di sessione](#) nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire 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 `aws:GetWidget` fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
aws: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 `aws: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 passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne 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 servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per 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 di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente 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. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Guide introduttive su sicurezza e conformità](#): queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- [Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services](#): questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

Note

Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione [Riferimenti sui servizi conformi ai requisiti HIPAA](#).

- [AWS Risorse per la conformità](#): questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.

- [AWS Guide alla conformità dei clienti](#): comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- [Valutazione delle risorse con regole](#) nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- [AWS Security Hub](#)— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina [Documentazione di riferimento sui controlli della Centrale di sicurezza](#).
- [AWS Audit Manager](#)— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione dei rischi e la conformità alle normative e agli standard di settore.

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, puoi 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. O puoi 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 Toolkit for Visual Studio.

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 controllare gli aggiornamenti di Toolkit for Visual Studio a intervalli appropriati per il tuo ambiente.

Cronologia dei documenti della Guida AWS Toolkit for Visual Studio per l'utente

Ultimo aggiornamento della documentazione: 21 aprile 2021

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, puoi sottoscrivere un [feed RSS](#).

Modifica	Descrizione	Data
Aggiornamenti e manutenzioni dei contenuti	Aggiornamento dei contenuti per modifiche all'interfaccia utente e alle linee guida di AWS stile.	6 marzo 2024
Aggiornamenti e manutenzioni dei contenuti	Aggiornamento dei contenuti per modifiche all'interfaccia utente e alle linee guida di AWS stile.	6 marzo 2024
Aggiornamenti e manutenzioni dei contenuti	Aggiornamento dei contenuti per modifiche all'interfaccia utente e alle linee guida di AWS stile.	6 marzo 2024
Aggiornamenti e manutenzioni dei contenuti	Aggiornamento dei contenuti per modifiche all'interfaccia utente e alle linee guida di AWS stile.	6 marzo 2024
Aggiornamenti e manutenzioni 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 gli argomenti [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

[Nuovo argomento generale sulla risoluzione dei problemi](#)

L'argomento [Risoluzione dei problemi](#) contiene informazioni generali sulla risoluzione dei problemi per i servizi associati. AWS Toolkit for Visual Studio

30 aprile 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 aggiornata 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 aggiornata 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 riflettere 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 CloudFormation I contenuti aggiornati relativi alla distribuzione su Elastic Beanstalk e Cloudformation 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 implementazione migliorata che fornisce indicazioni sul AWS servizio più adatto alla tua applicazione.	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
Fornire 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'applicazione 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'applicazione serverless con AWS Lambda	Il supporto per Visual Studio 2019 è stato aggiunto al AWS Toolkit for Visual Studio.	28 marzo 2019

<u>Configurazione di AWS Toolkit for Visual Studio</u>	Il supporto per Visual Studio 2019 è stato aggiunto a AWS Toolkit for Visual Studio.	28 marzo 2019
<u>Distribuzione di un'app ASP.NET Core 2.0 (Fargate)</u>	Il supporto per Visual Studio 2019 è stato aggiunto al AWS Toolkit for Visual Studio.	28 marzo 2019
<u>Distribuzione di un'app ASP.NET Core 2.0 (EC2)</u>	Il supporto per Visual Studio 2019 è stato aggiunto al AWS Toolkit for Visual Studio.	28 marzo 2019
<u>Creazione di un progetto AWS CloudFormation modello in Visual Studio</u>	Il supporto per Visual Studio 2019 è stato aggiunto al AWS Toolkit for Visual Studio.	28 marzo 2019
<u>Visualizzazioni dettagliate di Container Service</u>	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
<u>Distribuzione su Amazon EC2 Container Service</u>	Sono state aggiunte informazioni sulla distribuzione nel servizio container Amazon EC2.	16 febbraio 2018
<u>Implementazione di Container Service con Fargate</u>	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

<u>Distribuzione di Container Service utilizzando EC2</u>	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
<u>Credenziali per la distribuzione su Amazon EC2 Container Service</u>	Sono state aggiunte informazioni su come specificare le credenziali durante la distribuzione al servizio container Amazon EC2.	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.