Leitfaden

AWS Toolkit mit Amazon Q

AWS Toolkit mit Amazon Q: Leitfaden

Table of Contents

AWS Toolkit mit Amazon Q

Dies ist das Benutzerhandbuch für das AWS Toolkit for Visual Studio mit Amazon Q. Wenn Sie nach dem AWS Toolkit for VS Code suchen, finden Sie im Benutzerhandbuch für den AWS Toolkit for Visual Studio Code.

Was ist das AWS Toolkit for Visual Studio mit Amazon Q

Das AWS Toolkit for Visual Studio mit Amazon Q ist eine Erweiterung für die Visual Studio-IDE, die es Ihnen erleichtert, .NET-Anwendungen zu entwickeln, zu debuggen und bereitzustellen, die Amazon Web Services verwenden. Das AWS Toolkit mit Amazon Q wird für Visual Studio-Versionen 2022 und höher unterstützt. Einzelheiten zum Herunterladen und Installieren des Kits finden Sie im Thema Installation und Einrichtung in diesem Benutzerhandbuch.

> **Note**
>
> Das Toolkit for Visual Studio wurde auch für die Versionen Visual Studio 2008, 2010, 2012, 2013, 2015, 2017 und 2019 veröffentlicht. Diese Versionen werden jedoch nicht mehr unterstützt. Weitere Informationen finden Sie im Thema Installation und Einrichtung in diesem Benutzerhandbuch.

Das AWS Toolkit mit Amazon Q enthält die folgenden Funktionen, um Ihre Entwicklungserfahrung zu verbessern.

AWS Entdecker

Das AWS Explorer-Toolfenster ist über das View-Menü der IDE zugänglich und ermöglicht Ihnen die Interaktion mit AWS Diensten in Visual Studio. Eine Liste der unterstützten AWS Dienste und Funktionen finden Sie im Thema Arbeiten mit AWS Diensten in diesem Benutzerhandbuch.

Amazon Q

Chatten Sie mit Amazon Q Developer in Visual Studio, um Fragen zur Softwareentwicklung zu stellen AWS und Unterstützung bei der Softwareentwicklung zu erhalten. Amazon Q kann Codierungskonzepte und Codefragmente erklären, Code- und Komponententests generieren und Code durch Debugging oder Refactoring verbessern.

Informationen zur Installation und Einrichtung von Amazon Q for the Toolkit for Visual Studio finden Sie im Thema Erste Schritte in diesem Benutzerhandbuch. Weitere Informationen zur Zusammenarbeit mit Amazon Q Developer finden Sie im IDEs Thema Amazon Q Developer im Amazon Q Developer User Guide. Detaillierte Informationen zu Plänen und Preisen für Amazon Q finden Sie im Amazon Q-Preisleitfaden.

Verwandte Informationen

Um ein Problem zu öffnen oder sich aktuell offene Probleme anzusehen, besuchen Sie https://github.com/aws/aws-toolkit-visual-studio/issues.

Weitere Informationen zu Visual Studio finden Sie unter https://visualstudio.microsoft.com/vs/.

Amazon Q

Was ist Amazon Q

Seit dem 30. April 2024 CodeWhisperer ist Amazon jetzt Teil von Amazon Q Developer. Dazu gehören Inline-Codevorschläge und Sicherheitsscans.

Weitere Informationen zur Zusammenarbeit mit Amazon Q Developer finden Sie im AWS Toolkit for Visual Studio IDEs Thema Amazon Q Developer im Amazon Q Developer User Guide. Detaillierte Informationen zu Plänen und Preisen für Amazon Q finden Sie im Amazon Q-Preisleitfaden.

Das Toolkit for Visual Studio herunterladen

Sie können das Toolkit for Visual Studio über den Visual Studio Marketplace in Ihrer IDE herunterladen, installieren und einrichten. Ausführliche Anweisungen finden Sie im Abschnitt Installation des AWS Toolkit for Visual Studio im Thema Erste Schritte dieses Benutzerhandbuchs.

Das Toolkit vom Visual Studio Marketplace herunterladen

Laden Sie die Installationsdateien für das Toolkit for Visual Studio herunter, indem Sie in Ihrem Webbrowser zur AWS Visual Studio-Downloads-Website navigieren.

Zusätzliche IDE-Toolkits von AWS

Bietet neben dem Toolkit for Visual Studio AWS auch IDE-Toolkits für VS Code und. JetBrains

AWS Toolkit for Visual Studio Code Links

- Folgen Sie diesem Link, um den AWS Toolkit for Visual Studio Code vom VS Code Marketplace herunterzuladen.
- Weitere Informationen zu AWS Toolkit for Visual Studio Code finden Sie im AWS Toolkit for Visual Studio CodeBenutzerhandbuch.

AWS Toolkit for JetBrains Links

- Folgen Sie diesem Link, um das AWS Toolkit for JetBrains vom JetBrains Marketplace herunterzuladen.
- Weitere Informationen zu AWS Toolkit for JetBrains finden Sie im AWS Toolkit for JetBrainsBenutzerhandbuch.

Erste Schritte

Das AWS Toolkit for Visual Studio stellt Ihre AWS Dienste und Ressourcen über die integrierte Entwicklungsumgebung (IDE) von Visual Studio zur Verfügung.

Um Ihnen den Einstieg zu erleichtern, beschreiben die folgenden Themen die Installation, Einrichtung und Konfiguration von AWS Toolkit for Visual Studio.

Themen

Installation und Einrichtung des AWS Toolkit for Visual Studio

In den folgenden Themen wird beschrieben, wie Sie den herunterladen, installieren, einrichten und deinstallieren AWS Toolkit for Visual Studio.

Themen

Voraussetzungen

Im Folgenden finden Sie die Voraussetzungen für die Einrichtung unterstützter Versionen von AWS Toolkit for Visual Studio.

- Visual Studio 19 oder eine neuere Version
- Windows 10 oder eine spätere Windows-Version
- Administratorzugriff auf Windows und Visual Studio
- Aktive AWS IAM-Anmeldeinformationen

> **Note**
>
> Nicht unterstützte Versionen von AWS Toolkit for Visual Studio sind für Visual Studio 2008, 2010, 2012, 2013, 2015 und 2017 verfügbar. Um eine nicht unterstützte Version herunterzuladen, navigieren Sie zur AWS Toolkit for Visual StudioLanding Page und wählen Sie die gewünschte Version aus der Liste der Download-Links aus.
> Um mehr über IAM-Anmeldeinformationen zu erfahren oder ein Konto zu eröffnen, besuchen Sie das AWS Konsolen-Gateway.

Installation des AWS Toolkit for Visual Studio

Um das zu installieren AWS Toolkit for Visual Studio, suchen Sie anhand der folgenden Verfahren nach Ihrer Version von Visual Studio und führen Sie die erforderlichen Schritte aus. Download-Links für alle Versionen von AWS Toolkit for Visual Studio finden Sie auf der AWS Toolkit for Visual StudioLandingpage.

> **Note**
>
> Wenn Sie bei der Installation von auf Probleme stoßen AWS Toolkit for Visual Studio, finden Sie weitere Informationen unter dem Thema Behebung von Installationsproblemen in diesem Handbuch.

Installation von AWS Toolkit for Visual Studio für Visual Studio 2022

Gehen Sie wie folgt vor, um AWS Toolkit for Visual Studio 2022 von Visual Studio aus zu installieren:

1. Navigieren Sie im Hauptmenü zu Erweiterungen und wählen Sie Erweiterungen verwalten.
2. Suchen Sie im Suchfeld nach AWS.
3. Wählen Sie die Download-Schaltfläche für die entsprechende Version von Visual Studio 2022 und folgen Sie den Installationsanweisungen.

   > **Note**
   >
   > Möglicherweise müssen Sie Visual Studio manuell schließen und neu starten, um den Installationsvorgang abzuschließen.

4. Wenn der Download und die Installation abgeschlossen sind, können Sie den öffnen, AWS Toolkit for Visual Studio indem Sie im Menü Ansicht den AWS Explorer wählen.

Installation von AWS Toolkit for Visual Studio für Visual Studio 2019

Gehen Sie wie folgt vor, um AWS Toolkit for Visual Studio 2019 von Visual Studio aus zu installieren:

1. Navigieren Sie im Hauptmenü zu Erweiterungen und wählen Sie Erweiterungen verwalten.
2. Suchen Sie im Suchfeld nach AWS.
3. Wählen Sie die Download-Schaltfläche für Visual Studio 2017 und 2019 und folgen Sie den Anweisungen.

> **Note**
>
> Möglicherweise müssen Sie Visual Studio manuell schließen und neu starten, um den Installationsvorgang abzuschließen.

4. Wenn der Download und die Installation abgeschlossen sind, können Sie den öffnen, AWS Toolkit for Visual Studio indem Sie im Menü Ansicht den AWS Explorer wählen.

Deinstallation des AWS Toolkit for Visual Studio

Um das zu deinstallieren AWS Toolkit for Visual Studio, suchen Sie anhand der folgenden Verfahren nach Ihrer Version von Visual Studio und führen Sie die erforderlichen Schritte aus.

Deinstallation von AWS Toolkit for Visual Studio für Visual Studio 2022

Gehen Sie wie folgt vor, um AWS Toolkit for Visual Studio 2022 aus Visual Studio zu deinstallieren:

1. Navigieren Sie im Hauptmenü zu Erweiterungen und wählen Sie Erweiterungen verwalten.
2. Erweitern Sie im Navigationsmenü „Erweiterungen verwalten“ die Überschrift „Installiert“.
3. Suchen Sie die Erweiterung AWS Toolkit for Visual Studio 2022 und klicken Sie auf die Schaltfläche Deinstallieren.

> **Note**
>
> Wenn das im Abschnitt Installiert des Navigationsmenüs AWS Toolkit for Visual Studio nicht sichtbar ist, müssen Sie Visual Studio möglicherweise neu starten.

4. Folgen Sie den Anweisungen auf dem Bildschirm, um den Deinstallationsvorgang abzuschließen.

Deinstallation von AWS Toolkit for Visual Studio für Visual Studio 2019

Gehen Sie wie folgt vor, um AWS Toolkit for Visual Studio 2019 von Visual Studio zu deinstallieren:

1. Navigieren Sie im Hauptmenü zu Tools und wählen Sie Erweiterungen verwalten.
2. Erweitern Sie im Navigationsmenü „Erweiterungen verwalten“ die Überschrift „Installiert“.
3. Suchen Sie die Erweiterung für AWS Toolkit for Visual Studio 2019 und klicken Sie auf die Schaltfläche Deinstallieren.
4. Folgen Sie den Anweisungen auf dem Bildschirm, um den Deinstallationsvorgang abzuschließen.

Deinstallation von AWS Toolkit for Visual Studio für Visual Studio 2017

Gehen Sie wie folgt vor, um AWS Toolkit for Visual Studio 2017 in Visual Studio zu deinstallieren:

1. Navigieren Sie im Hauptmenü zu Tools und wählen Sie Erweiterungen und Updates aus.
2. Erweitern Sie im Navigationsmenü Erweiterungen und Updates die Überschrift Installiert.
3. Suchen Sie die Erweiterung für AWS Toolkit for Visual Studio 2017 und klicken Sie auf die Schaltfläche Deinstallieren.
4. Folgen Sie den Anweisungen auf dem Bildschirm, um den Deinstallationsvorgang abzuschließen.

Deinstallation von AWS Toolkit for Visual Studio für Visual Studio 2013 oder 2015

Gehen Sie wie folgt vor, um AWS Toolkit for Visual Studio 2013 oder 2015 zu deinstallieren:

1. Öffnen Sie in der Windows-Systemsteuerung die Option Programme und Funktionen.

> **Note**
>
> Sie können Programme und Funktionen sofort öffnen, indem Sie sie über eine Windows-Befehlszeile oder das Windows-Dialogfeld „Ausführen“ aufrufen. `appwiz.cpl`

2. Öffnen Sie in der Liste der installierten Programme das Kontextmenü für AWS Tools für Windows (klicken Sie mit der rechten Maustaste darauf).
3. Wählen Sie Deinstallieren und folgen Sie den Anweisungen, um den Deinstallationsvorgang abzuschließen.

> **Note**
>
> Ihr Samples-Verzeichnis wird während des Deinstallationsvorgangs nicht gelöscht. Dieses Verzeichnis bleibt erhalten, falls Sie Samples geändert haben. Dieses Verzeichnis muss manuell entfernt werden.

Verbindung herstellen zu AWS

In den folgenden Abschnitten werden die ersten Schritte mit dem AWS Toolkit for Visual Studio mit Amazon Q beschrieben. Wenn Sie Visual Studio nach der Installation der Erweiterung zum ersten Mal starten, wird im Editorfenster die Meldung Getting Started angezeigt. Auf der Registerkarte Erste Schritte können Sie die folgenden Aktionen ausführen.

- Aktivieren oder deaktivieren Sie Amazon Q und das AWS Toolkit.
- Fügen Sie neue Anmeldeinformationen hinzu und authentifizieren Sie sich mit ihnen.
- Authentifizieren Sie sich mit vorhandenen Anmeldeinformationen.
- Greifen Sie auf Dokumentation und Tutorials zu, die Ihnen den Einstieg in die Arbeit mit Amazon Q und dem AWS Toolkit erleichtern.

Voraussetzungen

Um mit der Arbeit mit Amazon Q und dem AWS Toolkit zu beginnen, müssen Sie sich mit AWS Anmeldeinformationen authentifizieren. Wenn Sie zuvor ein AWS Konto eingerichtet und sich über ein anderes AWS Tool oder einen anderen Dienst (z. B. den AWS Command Line Interface) authentifiziert haben, erkennt das AWS Toolkit Ihre Anmeldeinformationen automatisch. Wenn Sie

neu bei uns sind AWS oder noch kein Konto erstellt haben, können Sie sich über das Anmeldeportal für ein AWS Konto AWS registrieren. Ausführliche Informationen zur Einrichtung eines neuen AWS Kontos finden Sie unter dem Thema „Übersicht“ im AWS Setup-Benutzerhandbuch.

Über das AWS Toolkit eine Verbindung herstellen

Um über das AWS Toolkit eine Verbindung zu Ihren AWS Konten herzustellen, können Sie jederzeit die Registerkarte Erste Schritte öffnen, indem Sie die folgenden Schritte ausführen.

Öffnen Sie die Registerkarte „Erste Schritte“ in Visual Studio

1. Erweitern Sie in Visual Studio im Hauptmenü Erweiterungen und dann das AWS Toolkit-Untermenü.
2. Wählen Sie Getting started (Erste Schritte).
3. Die Registerkarte Erste Schritte wird im Visual Studio-Editorfenster geöffnet.

Auf der Registerkarte Erste Schritte gibt es zwei Hauptbereiche:

- Funktionen: In diesem Abschnitt können Sie Funktionen wie Amazon Q und das AWS Toolkit aktivieren oder deaktivieren.
- Dokumentation und Tutorials: Eine Sammlung von Verweisen auf Ihre aktivierten Funktionen.

> **Note**
>
> Der Abschnitt Dokumentation und Tutorials ist nur sichtbar, wenn eine oder mehrere Funktionen aktiviert sind.

Amazon Q Developer

Im Bereich Amazon Q auf der Registerkarte Erste Schritte können Sie Amazon Q aktivieren oder deaktivieren, eine neue Verbindung hinzufügen oder zu einer anderen AWS Verbindung wechseln. Bevor Sie eine dieser Aktionen anzeigen oder darauf zugreifen können, muss Amazon Q aktiviert sein. Um Amazon Q zu aktivieren, klicken Sie auf die Schaltfläche Aktivieren.

Wenn Amazon Q deaktiviert ist, werden alle Features und Funktionen von Amazon Q vollständig aus Visual Studio entfernt. Durch die Aktivierung von Amazon Q wird automatisch die Setup-Authentifizierung für Amazon Q auf der Registerkarte Erste Schritte geöffnet. Um fortzufahren,

müssen Sie sich mit Ihren AWS IAM Identity Center Anmeldeinformationen für den Zugriff auf das Professional-Kontingent oder mit Ihrer AWS Builder-ID für den Zugriff auf das kostenlose Kontingent authentifizieren. Ausführliche Informationen zu den einzelnen Stufenoptionen finden Sie im Thema Grundlegendes zu den Servicestufen für Amazon Q Developer im Amazon Q Developer User Guide.

Um fortzufahren, führen Sie eines der folgenden Verfahren aus.

Professionelle Authentifizierung mit IAM Identity Center

> **Note**
>
> Die Felder Profilname, Start-URL, Profilregion oder SSO-Region, die für die Authentifizierung mit der Professional-Stufe erforderlich sind, werden in der Regel von einem Administrator in Ihrem Unternehmen oder Ihrer Organisation bereitgestellt. Ausführliche Informationen zu den IAM Identity Center-Anmeldeinformationen finden Sie unter dem Thema Was ist IAM Identity Center im AWS IAM Identity Center-Benutzerhandbuch.

1. Wählen Sie auf dem Bildschirm Getting Started: AWS Toolkit with Amazon Q die Schaltfläche Anmelden in der Amazon Q-Kachel, um zum Bildschirm Authentifizierung für Amazon Q einrichten zu gelangen.
2. Navigieren Sie auf dem Bildschirm „Authentifizierung für Amazon Q einrichten“ zum Abschnitt Stufe Professional, füllen Sie die erforderlichen Felder aus und klicken Sie auf die Schaltfläche Connect.
3. Bestätigen Sie, dass Sie das Portal für AWS Autorisierungsanfragen in Ihrem Standard-Webbrowser öffnen möchten.
4. Führen Sie die vom Portal für AWS Autorisierungsanfragen erforderlichen Schritte aus. Sie werden benachrichtigt, wenn Sie Ihren Browser sicher schließen und zu Visual Studio zurückkehren können
5. Auf der Registerkarte Erste Schritte wird Amazon Q aktualisiert und zeigt an, dass Sie mit IAM Identity Center verbunden sind, wenn der Vorgang abgeschlossen ist.

Kostenlose Authentifizierung mit AWS Builder ID

> **Note**
>
> Weitere Informationen zur AWS Builder-ID finden Sie unter dem Thema Mit AWS Builder-ID anmelden im AWS Anmelde-Benutzerhandbuch.

1. Wählen Sie auf dem Bildschirm Getting Started: AWS Toolkit with Amazon Q die Schaltfläche Anmelden in der Amazon Q-Kachel, um zum Bildschirm Authentifizierung für Amazon Q einrichten zu gelangen.
2. Navigieren Sie auf dem Bildschirm „Authentifizierung für Amazon Q einrichten“ zum Abschnitt „Kostenloses Kontingent“ und wählen Sie die Schaltfläche „Registrieren“ oder „Anmelden“.
3. Bestätigen Sie, dass Sie das Portal für AWS Autorisierungsanfragen in Ihrem Standard-Webbrowser öffnen möchten.
4. Führen Sie die vom Portal für AWS Autorisierungsanfragen erforderlichen Schritte aus. Sie werden benachrichtigt, wenn Sie Ihren Browser sicher schließen und zu Visual Studio zurückkehren können.
5. Auf der Registerkarte Erste Schritte wird Amazon Q aktualisiert und zeigt an, dass Sie mit Ihrer AWS Builder-ID verbunden sind, wenn der Vorgang abgeschlossen ist.

Nachdem Sie sich entweder mit Ihren IAM Identity Center- oder AWS Builder ID-Anmeldeinformationen authentifiziert haben, können Sie in Visual Studio auf Amazon Q zugreifen. Darüber hinaus können Sie auf der Registerkarte Erste Schritte die folgenden Aktionen ausführen:

- Abmelden: Trennt Ihre aktuelle Verbindung mit Anmeldeinformationen von allen Amazon Q-Funktionen. Amazon Q bleibt aktiviert, aber die meisten Funktionen funktionieren nicht.
- Amazon Q deaktivieren: Deaktiviert vollständig alle Amazon Q-Funktionen in Visual Studio.

AWS Toolkit

Im Abschnitt AWS Toolkit auf der Registerkarte Erste Schritte mit dem AWS Toolkit können Sie das AWS Toolkit aktivieren oder deaktivieren, eine neue Verbindung hinzufügen oder zu einer anderen Verbindung wechseln. AWS Bevor Sie eine dieser Aktionen anzeigen oder darauf zugreifen können, muss das AWS Toolkit aktiviert sein. Um das AWS Toolkit zu aktivieren, klicken Sie auf die Schaltfläche Aktivieren.

Wenn das AWS Toolkit aktiviert ist, wird die Setup-Authentifizierung für AWS Toolkit automatisch auf der Registerkarte Erste Schritte mit dem AWS Toolkit geladen. Um fortzufahren, müssen Sie sich entweder mit Ihren AWS IAM Identity CenterAnmeldeinformationen oder Ihren Anmeldeinformationen für die IAM-Benutzerrolle authentifizieren.

> **Note**
>
> Ausführliche Informationen zu den IAM Identity Center-Anmeldeinformationen finden Sie im Thema Was ist IAM Identity Center im AWS IAM Identity Center-Benutzerhandbuch. Ausführliche Informationen zu den Anmeldeinformationen für die IAM-Benutzerrolle finden Sie im Thema AWS Zugriffsschlüssel: Langfristige Anmeldeinformationen im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch.

Authentifizieren Sie sich und stellen Sie eine Verbindung mit dem IAM Identity Center her

1. Wählen Sie auf dem Bildschirm Getting Started: AWS Toolkit with Amazon Q die Schaltfläche Anmelden in der AWS Toolkit-Kachel, um zum Bildschirm Authentifizierung für AWS Toolkit einrichten zu gelangen.
2. Wählen Sie auf dem Bildschirm „Authentifizierung für AWS Toolkit einrichten“ im Drop-down-Menü „Profiltyp“ die Option IAM Identity Center (Nachfolger von Single Sign-On) aus.
3. Wählen Sie im Drop-down-Menü Aus vorhandenem Profil auswählen oder neues hinzufügen ein vorhandenes Profil aus oder wählen Sie Neues Profil hinzufügen aus, um neue Profilinformationen hinzuzufügen.

   > **Note**
   >
   > Wenn Sie ein vorhandenes Profil auswählen, fahren Sie mit Schritt 7 fort.

4. Geben Sie im Feld Profilname das mit dem IAM Identity Center **`profile name`** verknüpfte Konto ein, mit dem Sie sich authentifizieren möchten.
5. Geben Sie im Textfeld Start-URL die **`Start URL`** an Ihre IAM Identity Center-Anmeldeinformationen angehängte URL ein.
6. Wählen Sie im Drop-down-Menü Profilregion (standardmäßig us-east-1) die Profilregion aus, die durch das IAM Identity Center-Benutzerprofil definiert ist, mit dem Sie sich authentifizieren.
7. Wählen Sie im Drop-down-Menü SSO-Region (standardmäßig us-east-1) die SSO-Region aus, die durch Ihre IAM Identity Center-Anmeldeinformationen definiert ist.

8. Wählen Sie die Schaltfläche Connect, um die Website „Anfrage AWS autorisieren“ in Ihrem Standard-Webbrowser zu öffnen.
9. Folgen Sie den Anweisungen in Ihrem Standard-Webbrowser. Sie werden benachrichtigt, wenn der Autorisierungsvorgang abgeschlossen ist. Sie können Ihren Browser problemlos schließen und zu Visual Studio zurückkehren.
10. Auf der Registerkarte Erste Schritte wird der Abschnitt AWS Toolkit aktualisiert und zeigt an, dass Sie nach Abschluss des Vorgangs mit IAM Identity Center verbunden sind.

Authentifizieren Sie sich mit den Anmeldeinformationen für die IAM-Benutzerrolle und stellen Sie eine Verbindung her

1. Wählen Sie auf dem Bildschirm Getting Started: AWS Toolkit with Amazon Q die Schaltfläche Anmelden in der AWS Toolkit-Kachel, um zum Bildschirm Authentifizierung für AWS Toolkit einrichten zu gelangen.
2. Wählen Sie auf dem Bildschirm „Authentifizierung für AWS Toolkit einrichten“ im Drop-down-Menü „Profiltyp“ die Option „IAM-Benutzerrolle“ aus.
3. Wählen Sie im Drop-down-Menü Aus vorhandenem Profil auswählen oder neues hinzufügen aus. **`Add new profile`**

   > **Note**
   >
   > Wenn Sie einen vorhandenen Profilnamen aus der Liste auswählen, fahren Sie mit Schritt 8 fort.

4. Geben Sie im Textfeld Profilname einen Namen für Ihr neues Profil ein.
5. Geben Sie im Textfeld Access Key ID den **`Access Key ID`** für das Profil ein, mit dem Sie sich authentifizieren möchten.
6. Geben Sie im Textfeld Geheimer Schlüssel den Wert **`Secret Key`** für das Profil ein, mit dem Sie sich authentifizieren möchten.
7. Geben Sie im Dropdownmenü Speicherort (standardmäßig Datei mit gemeinsamen Anmeldeinformationen) an, ob Sie Ihre Anmeldeinformationen in einer Datei mit gemeinsamen Anmeldeinformationen oder mit dem.NET Encrypted Store speichern möchten.
8. Wählen Sie in den Dropdownmenüs Profilregion (standardmäßig us-east-1) die Partition und die Profilregion aus, die an das Profil angehängt sind, mit dem Sie sich authentifizieren möchten.

9. Wählen Sie die Schaltfläche Connect, um dieses Profil zu Ihrem AWS Speicherort hinzuzufügen und/oder sich damit AWS zu authentifizieren.
10. Auf der Registerkarte „Erste Schritte“ wird der Abschnitt „ AWS Toolkit“ aktualisiert und zeigt an, dass Sie mit den Anmeldeinformationen Ihrer IAM-Benutzerrolle verbunden sind, wenn der Vorgang abgeschlossen ist.

Nachdem Sie sich entweder mit Ihren Anmeldeinformationen für das IAM Identity Center oder der IAM-Benutzerrolle authentifiziert haben, können Sie im Toolkit for Visual Studio auf den AWS Explorer zugreifen. Darüber hinaus können Sie sich über den Tab Erste Schritte abmelden und das AWS Toolkit for Visual Studio mit Amazon Q deaktivieren.

Dokumentation und Tutorials

Der Bereich Dokumentation und Tutorials wird automatisch mit Dokumentationen und Tutorialvorschlägen aktualisiert, die auf Ihren AWS Service- und Funktionseinstellungen basieren. Diese Verweise sind nur sichtbar, wenn mindestens eine Funktion aktiviert wurde.

Behebung von Installationsproblemen für den AWS Toolkit for Visual Studio

Die folgenden Informationen lösen bekanntermaßen häufig auftretende Installationsprobleme bei der Einrichtung von AWS Toolkit for Visual Studio.

Wenn bei der Installation von ein Fehler auftritt AWS Toolkit for Visual Studio oder es unklar ist, ob die Installation abgeschlossen wurde, lesen Sie sich die Informationen in den folgenden Abschnitten durch.

Administratorrechte für Visual Studio

Für die AWS Toolkit for Visual Studio Erweiterung sind Administratorrechte erforderlich, um sicherzustellen, dass auf alle AWS Dienste und Funktionen zugegriffen werden kann.

Wenn Sie über lokale Administratorrechte verfügen, erstrecken sich Ihre Administratorrechte möglicherweise nicht direkt auf Ihre Visual Studio-Instanz.

Um Visual Studio lokal mit Administratorrechten zu starten:

1. Suchen Sie in Windows nach dem Visual Studio-Anwendungsstarter (Symbol).

2. Öffnen Sie das Kontextmenü für das Visual Studio-Symbol (klicken Sie mit der rechten Maustaste darauf), um das Kontextmenü zu öffnen.
3. Wählen Sie im Kontextmenü die Option Als Administrator ausführen aus.

Um Visual Studio mit Administratorrechten remote zu starten:

1. Suchen Sie in Windows den Anwendungsstarter für die Anwendung, mit der Sie eine Verbindung zu Ihrer Remoteinstanz von Visual Studio herstellen.
2. Öffnen Sie das Kontextmenü für die Anwendung (klicken Sie mit der rechten Maustaste darauf), um das Kontextmenü zu öffnen.
3. Wählen Sie im Kontextmenü die Option Als Administrator ausführen aus.

> **Note**
>
> Unabhängig davon, ob Sie das Programm lokal starten oder eine Remoteverbindung herstellen, fordert Windows Sie möglicherweise auf, Ihre Administratoranmeldedaten zu bestätigen.

Abrufen eines Installationsprotokolls

Wenn Sie die Schritte im vorherigen Abschnitt Administratorberechtigungen ausgeführt haben und bestätigt wurde, dass Sie Visual Studio mit Administratorrechten ausführen oder eine Verbindung zu Visual Studio herstellen, kann das Abrufen einer Installationsprotokolldatei bei der Diagnose anderer Probleme helfen.

Gehen Sie wie folgt vor, um das manuell AWS Toolkit for Visual Studio aus einer `.vsix` Datei zu installieren und eine Installationsprotokolldatei zu generieren.

1. Folgen Sie auf der AWS Toolkit for Visual StudioLandingpage dem Download-Link und speichern Sie die `.vsix` Datei der AWS Toolkit for Visual Studio Version, die Sie installieren möchten.
2. Erweitern Sie im Visual Studio-Hauptmenü den Tools-Header, erweitern Sie das Befehlszeilen-Untermenü und wählen Sie dann Visual Studio Developer Command Prompt.
3. Geben Sie in der Visual Studio **`vsixinstaller`** Developer-Befehlszeile den Befehl im folgenden Format ein:

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

4. `[file path to log file]`Ersetzen Sie ihn durch den Dateinamen und den vollständigen Dateipfad des Verzeichnisses, in dem das Installationsprotokoll erstellt werden soll. Ein Beispiel für den `vsixinstaller` Befehl mit dem angegebenen Dateipfad und Dateinamen sieht wie folgt aus:

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

5. `[file path to Toolkit installation file]`Ersetzen Sie durch den vollständigen Dateipfad des Verzeichnisses, in dem sich der `AWSToolkitPackage.vsix` befindet.

   Ein Beispiel für den `vsixinstaller` Befehl mit dem vollständigen Dateipfad zur Toolkit-Installationsdatei sollte wie folgt aussehen:

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

6. Vergewissern Sie sich, dass der Dateiname und die Pfade korrekt sind, und führen Sie dann den `vsixinstaller` Befehl aus.

   Ein Beispiel für einen vollständigen `vsixinstaller` Befehl sieht wie folgt aus:

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

Installation verschiedener Visual Studio-Erweiterungen

Wenn Sie eine Installationsprotokolldatei erhalten haben und immer noch nicht feststellen können, warum der Installationsvorgang fehlschlägt, überprüfen Sie, ob Sie andere Visual Studio-Erweiterungen installieren können. Die Installation verschiedener Visual Studio-Erweiterungen kann zusätzliche Einblicke in Ihre Installationsprobleme bieten. Falls Sie keine Visual Studio-Erweiterungen installieren können, müssen Sie möglicherweise Probleme stattdessen mit Visual Studio beheben AWS Toolkit for Visual Studio.

Den -Support kontaktieren

Wenn Sie alle Abschnitte dieses Handbuchs gelesen haben und zusätzliche Ressourcen oder Unterstützung benötigen, können Sie sich frühere Ausgaben ansehen oder eine neue Ausgabe auf der AWS Toolkit for Visual Studio Github Issues-Website öffnen.

So findest du schneller eine Lösung für dein Problem:

- Überprüfe vergangene und aktuelle Probleme, um zu sehen, ob andere auf eine ähnliche Situation gestoßen sind.
- Machen Sie sich detaillierte Notizen zu jedem Schritt, den Sie zur Behebung des Problems unternommen haben.
- Speichern Sie alle Protokolldateien, die Sie bei der Installation der AWS Toolkit for Visual Studio oder anderer Erweiterungen erhalten haben.
- Hängen Sie Ihre AWS Toolkit for Visual Studio Installationsprotokolldateien an die neue Ausgabe an.

Profile und Fensterbindung

Profile und Fensterbindung für das Toolkit for Visual Studio

Beachten Sie bei der Arbeit mit den Veröffentlichungstools, Assistenten und anderen Funktionen des Toolkit for Visual Studio Folgendes:

- Das AWS Explorer-Fenster ist jeweils an ein einzelnes Profil und eine Region gebunden. Fenster, die vom AWS Explorer aus geöffnet werden, sind standardmäßig an dieses gebundene Profil und diese Region gebunden.
- Nachdem ein neues Fenster geöffnet wurde, können Sie diese Instanz des AWS Explorers verwenden, um zu einem anderen Profil oder einer anderen Region zu wechseln.
- Die Tools und Funktionen des Toolkit for Visual Studio zur Veröffentlichung verwenden standardmäßig automatisch das im AWS Explorer festgelegte Profil und die Region.
- Wenn in einem Veröffentlichungstool, Assistenten oder Feature ein neues Profil oder eine neue Region angegeben wird, verwenden alle danach erstellten Ressourcen weiterhin die neuen Profil- und Regionseinstellungen.
- Wenn Sie mehrere Instanzen von Visual Studio geöffnet haben, kann jede Instanz an ein anderes Profil und eine andere Region gebunden werden.

- Der AWS Explorer speichert das letzte Profil und die Region, die angegeben wurden, und die Werte der allerletzten Visual Studio-Instanz, die geschlossen wurde, werden beibehalten.

Authentifizierung und Zugriff

Sie müssen sich nicht bei authentifizieren AWS , um mit dem AWS Toolkit for Visual Studio mit Amazon Q zu arbeiten. Die meisten AWS Ressourcen werden jedoch über ein Konto verwaltet. AWS Um auf das gesamte AWS Toolkit for Visual Studio mit den Diensten und Funktionen von Amazon Q zugreifen zu können, benötigen Sie mindestens zwei Arten der Kontoauthentifizierung:

1. Entweder AWS Identity and Access Management (IAM) oder AWS IAM Identity CenterAuthentifizierung für Ihre AWS Konten. Die meisten AWS Dienste und Ressourcen werden über IAM und IAM Identity Center verwaltet.
2. Eine AWS Builder-ID ist für bestimmte andere Dienste entweder optional. AWS

Die folgenden Themen enthalten zusätzliche Informationen und Anweisungen zur Einrichtung der einzelnen Anmeldeinformationstypen und Authentifizierungsmethoden.

Themen

AWS IAM Identity Center-Anmeldeinformationen in AWS Toolkit for Visual Studio

AWS IAM Identity Center ist die empfohlene bewährte Methode für die Verwaltung Ihrer AWS Kontoauthentifizierung.

Detaillierte Anweisungen zur Einrichtung von IAM Identity Center for Software Development Kits (SDKs) und dem AWS Toolkit for Visual Studio finden Sie im Abschnitt zur IAM Identity Center-Authentifizierung im Referenzhandbuch AWS SDKs zu Tools.

Authentifizierung mit IAM Identity Center von der AWS Toolkit for Visual Studio

Gehen Sie wie folgt vor, um sich bei IAM Identity Center von aus zu authentifizieren, AWS Toolkit for Visual Studio indem Sie ein IAM Identity Center-Profil zu Ihrer `credentials config` OR-Datei hinzufügen.

1. Öffnen Sie in Ihrem bevorzugten Texteditor die in der Datei gespeicherten AWS Anmeldeinformationen. `<hone-directory>\.aws\credentials`
2. Fügen Sie im `credentials file` unteren Bereich `[default]` eine Vorlage für ein benanntes IAM Identity Center-Profil hinzu. Im Folgenden finden Sie ein Beispiel für eine Vorlage:

> **Important**
>
> Verwenden Sie beim Erstellen eines Eintrags in der `credential` Datei nicht das Wort Profil, da dies zu einem Konflikt mit den `credential` Dateibenennungskonventionen führt.
> Schließen Sie das Präfixwort `profile_` nur ein, wenn Sie ein benanntes Profil in der `config` Datei konfigurieren.

```
[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`**: Die URL, die auf das IAM Identity Center-Benutzerportal Ihrer Organisation verweist.
- **`sso_region`**: Die AWS Region, in der sich Ihr IAM Identity Center-Portalhost befindet. Dies kann sich von der AWS Region unterscheiden, die später im `region` Standardparameter angegeben wurde.
- **`sso_account_id`**: Die AWS Konto-ID, die die IAM-Rolle mit der Berechtigung enthält, die Sie diesem IAM Identity Center-Benutzer gewähren möchten.

- **`sso_role_name`**: Der Name der IAM-Rolle, die die Berechtigungen des Benutzers definiert, wenn er dieses Profil verwendet, um Anmeldeinformationen über IAM Identity Center abzurufen.
- **`region`**: Die AWS Standardregion, in der sich dieser IAM Identity Center-Benutzer anmeldet.

> **Note**
>
> Sie können Ihrem auch ein für IAM Identity Center aktiviertes Profil hinzufügen, AWS CLI indem Sie den `aws configure sso` Befehl ausführen. Nachdem Sie diesen Befehl ausgeführt haben, geben Sie Werte für die IAM Identity Center-Start-URL (`sso_start_url`) und die AWS Region (`region`) an, die das IAM Identity Center-Verzeichnis hostet. Weitere Informationen finden Sie unter Konfiguration der AWS CLI für die Verwendung von AWS Single Sign-On im AWS Command Line Interface Benutzerhandbuch.

Melden Sie sich mit IAM Identity Center an

Wenn Sie sich mit einem IAM Identity Center-Profil anmelden, wird der Standardbrowser mit dem in Ihrem `sso_start_url` angegebenen Browser gestartet. `credential file` Sie müssen Ihre IAM Identity Center-Anmeldung verifizieren, bevor Sie auf Ihre AWS Ressourcen in zugreifen können. AWS Toolkit for Visual Studio Wenn Ihre Anmeldeinformationen ablaufen, müssen Sie den Verbindungsvorgang wiederholen, um neue temporäre Anmeldeinformationen zu erhalten.

AWS IAM-Anmeldeinformationen

AWS IAM-Anmeldeinformationen authentifizieren sich mit Ihrem AWS Konto über lokal gespeicherte Zugriffsschlüssel.

In den folgenden Abschnitten wird beschrieben, wie Sie IAM-Anmeldeinformationen einrichten, um sich mit Ihrem AWS Konto über den zu authentifizieren. AWS Toolkit for Visual Studio

> **Important**
>
> Bevor Sie IAM-Anmeldeinformationen für die Authentifizierung mit Ihrem AWS Konto einrichten, beachten Sie Folgendes:
>
> - Wenn Sie IAM-Anmeldeinformationen bereits über einen anderen AWS Dienst (z. B. den AWS CLI) eingerichtet haben, erkennt der diese Anmeldeinformationen AWS Toolkit for Visual Studio automatisch.

- AWS empfiehlt die Verwendung der AWS IAM Identity Center Authentifizierung. Weitere Informationen zu Best Practices für AWS IAM finden Sie im Abschnitt Bewährte Sicherheitsmethoden in IAM im AWS Identity and Access Management-Benutzerhandbuch.
- Um Sicherheitsrisiken zu vermeiden, sollten Sie IAM-Benutzer nicht zur Authentifizierung verwenden, wenn Sie speziell entwickelte Software entwickeln oder mit echten Daten arbeiten. Verwenden Sie stattdessen den Verbund mit einem Identitätsanbieter wie. AWS IAM Identity Center Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center Benutzerhandbuch.

Erstellen eines IAM-Benutzers

Bevor Sie die AWS Toolkit for Visual Studio Authentifizierung mit Ihrem AWS Konto einrichten können, müssen Sie Schritt 1: Erstellen Sie Ihren IAM-Benutzer und Schritt 2: Abrufen Ihrer Zugangsschlüssel im Thema Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch abschließen.

> **Note**
>
> Schritt 3: Die Aktualisierung der gemeinsamen Anmeldeinformationen ist optional. Wenn Sie Schritt 3 abgeschlossen haben, erkennt der AWS Toolkit for Visual Studio automatisch Ihre Anmeldeinformationen aus dem`credentials file`. Wenn Sie Schritt 3 noch nicht abgeschlossen haben, werden AWS Toolkit for Visual Studio Sie durch den Prozess der Erstellung einer geführt, `credentials file` wie im Abschnitt Erstellen einer Anmeldeinformationsdatei aus dem AWS Toolkit for Visual Studio Abschnitt unten beschrieben.

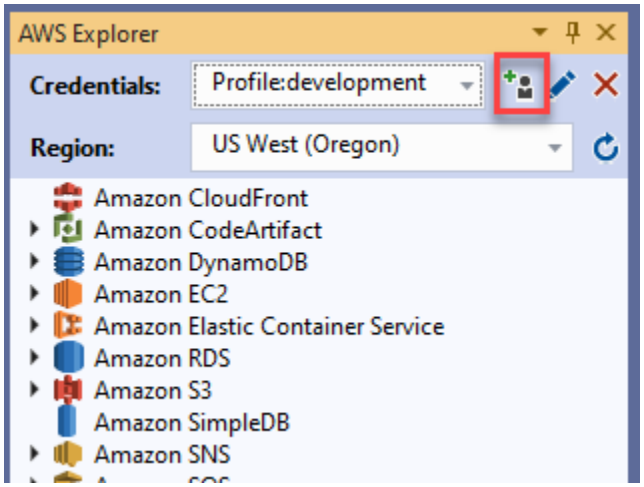
Eine Anmeldeinformationsdatei erstellen

Um einen Benutzer hinzuzufügen oder einen `credentials file` aus dem zu erstellen AWS Toolkit for Visual Studio:

> **Note**
>
> Wenn ein neues Benutzerprofil aus dem Toolkit hinzugefügt wird:

- Wenn ein `credentials file` bereits vorhanden ist, werden die neuen Benutzerinformationen der vorhandenen Datei hinzugefügt.
- Wenn eine nicht `credentials file` existiert, wird eine neue Datei erstellt.

1. Wählen Sie im AWS Explorer das Symbol „Neues Kontoprofil“, um das Dialogfeld „Neues Kontoprofil“ zu öffnen.



2. Füllen Sie die erforderlichen Felder im Dialogfeld „Neues Kontoprofil“ aus und klicken Sie auf die Schaltfläche „OK“, um den IAM-Benutzer zu erstellen.

Bearbeitung der IAM-Benutzeranmeldedaten aus dem Toolkit

Gehen Sie wie folgt vor, um die IAM-Benutzeranmeldedaten aus dem Toolkit zu bearbeiten:

1. Wählen Sie im AWS Explorer in der Dropdownliste „Anmeldeinformationen“ die IAM-Benutzeranmeldeinformationen aus, die Sie bearbeiten möchten.
2. Wählen Sie das Symbol „Profil bearbeiten“, um das Dialogfeld „Profil bearbeiten“ zu öffnen.
3. Nehmen Sie im Dialogfeld „Profil bearbeiten“ Ihre Aktualisierungen vor und klicken Sie auf OK, um Ihre Änderungen zu speichern.

Gehen Sie wie folgt vor, um die IAM-Benutzeranmeldedaten aus dem Toolkit zu löschen:

1. Wählen Sie im AWS Explorer in der Dropdownliste „Anmeldeinformationen“ die IAM-Benutzeranmeldeinformationen aus, die Sie löschen möchten.
2. Wählen Sie das Symbol „Profil löschen“, um die Aufforderung „Profil löschen“ zu öffnen.

3. Bestätigen Sie, dass Sie das Profil löschen möchten, um es aus Ihrem zu entfernen`Credentials file`.

> **Important**
>
> Profile, die erweiterte Zugriffsfunktionen wie IAM Identity Center oder Multi-Factor Authentication (MFA) im Dialogfeld „Profil bearbeiten“ unterstützen, können nicht über den bearbeitet werden. AWS Toolkit for Visual Studio Um Änderungen an diesen Profiltypen vorzunehmen, müssen Sie sie `credentials file` mit einem Texteditor bearbeiten.

Bearbeiten von IAM-Benutzeranmeldedaten in einem Texteditor

Sie können IAM-Benutzer nicht nur mit dem verwalten AWS Toolkit for Visual Studio, sondern auch in `credential files` Ihrem bevorzugten Texteditor bearbeiten. Der Standardspeicherort von `credential file` in Windows ist`C:\Users\`*`USERNAME`*`\.aws\credentials`.

Weitere Informationen zum Speicherort und zur Struktur von `credential files` finden Sie im Abschnitt Dateien mit gemeinsam genutzten Konfigurationen und Anmeldeinformationen im AWS SDKs Tools-Referenzhandbuch.

IAM-Benutzer aus dem AWS Command Line Interface ()AWS CLI erstellen

Das AWS CLI ist ein weiteres Tool, mit dem Sie mithilfe des Befehls einen IAM-Benutzer in der `credentials file` erstellen können. `aws configure`

Ausführliche Informationen zum Erstellen von IAM-Benutzern AWS CLI finden Sie im Abschnitt Konfiguration der AWS CLI Themen im AWS CLI Benutzerhandbuch.

Das Toolkit for Visual Studio unterstützt die folgenden Konfigurationseigenschaften:

```
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 Builder-ID

AWS Builder ID ist eine zusätzliche AWS Authentifizierungsmethode, die möglicherweise erforderlich ist, um bestimmte Dienste oder Funktionen zu nutzen, z. B. das Klonen eines Drittanbieter-Repositorys mit Amazon CodeCatalyst.

Ausführliche Informationen zur AWS Builder-ID-Authentifizierungsmethode finden Sie unter dem Thema Mit AWS Builder-ID anmelden im AWS Anmelde-Benutzerhandbuch.

Weitere Informationen zum Klonen eines Repositorys für CodeCatalyst AWS Toolkit for Visual Studio from finden Sie im CodeCatalyst Thema Arbeiten mit Amazon in diesem Benutzerhandbuch.

Multi-Faktor-Authentifizierung (MFA) im Toolkit for Visual Studio

Die Multi-Faktor-Authentifizierung (MFA) bietet zusätzliche Sicherheit für Ihre AWS Konten. Bei MFA müssen Benutzer beim Zugriff auf AWS Websites oder Dienste Anmeldeinformationen und eine eindeutige Authentifizierung über einen AWS unterstützten MFA-Mechanismus angeben.

AWS unterstützt eine Reihe von virtuellen Geräten und Hardwaregeräten für die MFA-Authentifizierung. Im Folgenden finden Sie ein Beispiel für ein virtuelles MFA-Gerät, das über eine Smartphone-Anwendung aktiviert wird. Weitere Informationen zu MFA-Geräteoptionen finden Sie unter Verwenden der Multi-Faktor-Authentifizierung (MFA) AWS im IAM-Benutzerhandbuch.

Schritt 1: Eine IAM-Rolle erstellen, um den Zugriff an IAM-Benutzer zu delegieren

Im folgenden Verfahren wird beschrieben, wie Sie die Rollendelegierung für die Zuweisung von Berechtigungen an einen IAM-Benutzer einrichten. Ausführliche Informationen zur Rollenverteilung finden Sie unter dem Thema Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer im Benutzerhandbuch.AWS Identity and Access Management

1. Rufen Sie die IAM-Konsole unter /iam auf. https://console.aws.amazon.com

2. Wählen Sie in der Navigationsleiste Rollen und anschließend Rolle erstellen aus.
3. Wählen Sie auf der Seite „Rolle erstellen“ die Option „Anderes AWS Konto“ aus.
4. Geben Sie Ihre erforderliche Konto-ID ein und markieren Sie das Kontrollkästchen MFA erforderlich.

> **Note**
>
> Um Ihre 12-stellige Kontonummer (ID) zu finden, rufen Sie die Navigationsleiste in der Konsole auf und wählen Sie dann Support, Support Center aus.

5. Wählen Sie Weiter: Berechtigungen aus.
6. Hängen Sie bestehende Richtlinien an Ihre Rolle an oder erstellen Sie eine neue Richtlinie dafür. Die Richtlinien, die Sie auf dieser Seite auswählen, bestimmen, auf welche AWS Dienste der IAM-Benutzer mit dem Toolkit zugreifen kann.
7. Nachdem Sie die Richtlinien angehängt haben, wählen Sie Weiter: Tags für die Option, Ihrer Rolle IAM-Tags hinzuzufügen. Wählen Sie dann Weiter: Überprüfen, um fortzufahren.
8. Geben Sie auf der Seite „Überprüfen“ den erforderlichen Rollennamen ein (z. B. die Toolkit-Rolle). Sie können auch eine optionale Rollenbeschreibung hinzufügen.
9. Wählen Sie Rolle erstellen aus.
10. Wenn die Bestätigungsmeldung angezeigt wird (z. B. „Die Rollen-Toolkit-Rolle wurde erstellt“), wählen Sie den Namen der Rolle in der Nachricht aus.
11. Wählen Sie auf der Übersichtsseite das Kopiersymbol, um den Rollen-ARN zu kopieren und in eine Datei einzufügen. (Sie benötigen diesen ARN, wenn Sie den IAM-Benutzer so konfigurieren, dass er die Rolle übernimmt.).

Schritt 2: Einen IAM-Benutzer erstellen, der die Berechtigungen der Rolle übernimmt

In diesem Schritt wird ein IAM-Benutzer ohne Berechtigungen erstellt, sodass eine Inline-Richtlinie hinzugefügt werden kann.

1. Rufen Sie die IAM-Konsole unter /iam auf. https://console.aws.amazon.com
2. Wählen Sie in der Navigationsleiste Benutzer und dann Benutzer hinzufügen aus.
3. Geben Sie auf der Seite „Benutzer hinzufügen“ den erforderlichen Benutzernamen ein (z. B. Toolkit-Benutzer) und aktivieren Sie das Kontrollkästchen Programmatischer Zugriff.

4. Wählen Sie Weiter: Berechtigungen, Weiter: Stichwörter und Weiter: Überprüfen, um zu den nächsten Seiten zu gelangen. Sie fügen zu diesem Zeitpunkt keine Berechtigungen hinzu, da der Benutzer die Berechtigungen der Rolle übernehmen wird.
5. Auf der Überprüfungsseite werden Sie darüber informiert, dass dieser Benutzer keine Berechtigungen hat. Wählen Sie Create user (Benutzer erstellen) aus.
6. Wählen Sie auf der Seite „Erfolg“ die Option „.csv herunterladen“, um die Datei herunterzuladen, die die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel enthält. (Sie benötigen beide, wenn Sie das Benutzerprofil in der Anmeldeinformationsdatei definieren.)
7. Klicken Sie auf Schließen.

Schritt 3: Hinzufügen einer Richtlinie, damit der IAM-Benutzer die Rolle übernehmen kann

Mit dem folgenden Verfahren wird eine Inline-Richtlinie erstellt, die es dem Benutzer ermöglicht, die Rolle (und die Berechtigungen dieser Rolle) zu übernehmen.

1. Wählen Sie auf der Seite Benutzer der IAM-Konsole den IAM-Benutzer aus, den Sie gerade erstellt haben (z. B. toolkit-user).
2. Wählen Sie auf der Seite „Zusammenfassung“ auf der Registerkarte „Berechtigungen“ die Option „Inline-Richtlinie hinzufügen“ aus.
3. Wählen Sie auf der Seite Richtlinie erstellen die Option Dienst auswählen aus, geben Sie STS im Feld Dienst suchen ein, und wählen Sie dann STS aus den Ergebnissen aus.
4. Beginnen Sie mit der Eingabe des Begriffs für Aktionen AssumeRole. Markieren AssumeRoleSie das Kontrollkästchen, wenn es angezeigt wird.
5. Stellen Sie sicher, dass im Abschnitt Ressource die Option Spezifisch ausgewählt ist, und klicken Sie auf ARN hinzufügen, um den Zugriff einzuschränken.
6. Fügen Sie im Dialogfeld ARN (s) hinzufügen unter ARN für Rolle angeben den ARN der Rolle hinzu, die Sie in Schritt 1 erstellt haben.

   Nachdem Sie den ARN der Rolle hinzugefügt haben, werden das vertrauenswürdige Konto und der Rollenname, die dieser Rolle zugeordnet sind, unter Konto und Rollenname mit Pfad angezeigt.
7. Wählen Sie Hinzufügen aus.

8. Zurück auf der Seite Richtlinie erstellen wählen Sie Anforderungsbedingungen angeben (optional) aus, markieren Sie das Kontrollkästchen MFA erforderlich, und wählen Sie dann zur Bestätigung Schließen aus.
9. Wählen Sie Review policy (Richtlinie überprüfen) aus.
10. Geben Sie auf der Seite Richtlinie überprüfen einen Namen für die Richtlinie ein und wählen Sie dann Richtlinie erstellen aus.

    Auf der Registerkarte „Berechtigungen“ wird die neue Inline-Richtlinie angezeigt, die direkt an den IAM-Benutzer angehängt ist.

Schritt 4: Verwaltung eines virtuellen MFA-Geräts für den IAM-Benutzer

1. Laden Sie eine virtuelle MFA-Anwendung herunter und installieren Sie sie auf Ihrem Smartphone.

   Eine Liste der unterstützten Anwendungen finden Sie auf der Ressourcenseite zur Multi-Faktor-Authentifizierung.
2. Wählen Sie in der IAM-Konsole in der Navigationsleiste Benutzer und dann den Benutzer aus, der eine Rolle annimmt (in diesem Fall Toolkit-Benutzer).
3. Wählen Sie auf der Übersichtsseite die Registerkarte Sicherheitsanmeldedaten und wählen Sie für Zugewiesenes MFA-Gerät die Option Verwalten aus.
4. Wählen Sie im Bereich MFA-Gerät verwalten die Option Virtuelles MFA-Gerät und dann Weiter aus.
5. Wählen Sie im Bereich Virtuelles MFA-Gerät einrichten die Option QR-Code anzeigen aus und scannen Sie dann den Code mit der virtuellen MFA-Anwendung, die Sie auf Ihrem Smartphone installiert haben.
6. Nachdem Sie den QR-Code gescannt haben, generiert die virtuelle MFA-Anwendung einmalige MFA-Codes. Geben Sie zwei aufeinanderfolgende MFA-Codes in MFA-Code 1 und MFA-Code 2 ein.
7. Klicken Sie auf Assign MFA (MFA zuordnen).
8. Kopieren Sie auf der Registerkarte Sicherheitsanmeldeinformationen für den Benutzer den ARN des neuen zugewiesenen MFA-Geräts.

Die ARN enthält Ihre 12-stellige Konto-ID und das Format ähnelt dem folgenden:`arn:aws:iam::123456789012:mfa/toolkit-user`. Sie benötigen diesen ARN, wenn Sie im nächsten Schritt das MFA-Profil definieren.

Schritt 5: Profile erstellen, um MFA zuzulassen

Mit dem folgenden Verfahren werden die Profile erstellt, die MFA beim Zugriff auf AWS Dienste aus dem Toolkit for Visual Studio zulassen.

Die von Ihnen erstellten Profile enthalten drei Informationen, die Sie in den vorherigen Schritten kopiert und gespeichert haben:

- Zugriffsschlüssel (Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel) für den IAM-Benutzer
- ARN der Rolle, die Berechtigungen an den IAM-Benutzer delegiert
- ARN des virtuellen MFA-Geräts, das dem IAM-Benutzer zugewiesen ist

Fügen Sie in der Datei AWS mit den gemeinsam genutzten Anmeldeinformationen oder dem SDK-Speicher, der Ihre AWS Anmeldeinformationen enthält, die folgenden Einträge hinzu:

```
[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
```

In dem angegebenen Beispiel sind zwei Profile definiert:

- `[toolkit-user]`Das Profil enthält den Zugriffsschlüssel und den geheimen Zugriffsschlüssel, die generiert und gespeichert wurden, als Sie den IAM-Benutzer in Schritt 2 erstellt haben.
- `[mfa]`Das Profil definiert, wie die Multi-Faktor-Authentifizierung unterstützt wird. Es gibt drei Einträge:

  ◦`source_profile`: Gibt das Profil an, dessen Anmeldeinformationen verwendet werden, um die in dieser `role_arn` Einstellung angegebene Rolle in diesem Profil anzunehmen. In diesem Fall ist es das `toolkit-user` Profil.

- `role_arn`: Gibt den Amazon-Ressourcennamen (ARN) der IAM-Rolle an, die Sie verwenden möchten, um mit diesem Profil angeforderte Operationen auszuführen. In diesem Fall ist es der ARN für die Rolle, die Sie in Schritt 1 erstellt haben.

- `mfa_serial`: Gibt die Identifikations- oder Seriennummer des MFA-Geräts an, die der Benutzer verwenden muss, wenn er eine Rolle annimmt. In diesem Fall ist es der ARN des virtuellen Geräts, das Sie in Schritt 3 eingerichtet haben.

Externe Anmeldeinformationen einrichten

Wenn Sie über eine Methode zum Generieren oder Nachschlagen von Anmeldeinformationen verfügen, die nicht direkt von unterstützt wird AWS, können Sie der Datei mit den gemeinsamen Anmeldeinformationen ein Profil hinzufügen, das die `credential_process` Einstellung enthält. Diese Einstellung gibt einen externen Befehl an, der ausgeführt wird, um zu verwendende Authentifizierungsanmeldeinformationen zu generieren oder abzurufen. Sie könnten beispielsweise einen Eintrag, der dem folgenden ähnelt, in die `config` Datei aufnehmen:

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

Weitere Informationen zur Verwendung externer Anmeldeinformationen und den damit verbundenen Sicherheitsrisiken finden Sie unter Beschaffung von Anmeldeinformationen mit einem externen Prozess im AWS Command Line Interface Benutzerhandbuch.

Aktualisierung von Firewalls und Gateways, um den Zugriff zu ermöglichen

Wenn Sie den Zugriff auf bestimmte AWS Domains oder URL-Endpunkte mithilfe einer Lösung zur Filterung von Webinhalten filtern, müssen die folgenden Endpunkte in der Liste „Zulassen“ aufgeführt sein, um auf alle Dienste und Funktionen zugreifen zu können, die AWS Toolkit for Visual Studio über Amazon Q verfügbar sind. Detaillierte Schritte zur Fehlerbehebung bei Firewall- und Proxyeinstellungen für das AWS Toolkit mit Amazon Q finden Sie im Abschnitt Firewall- und Proxyeinstellungen im Thema Fehlerbehebung in diesem Benutzerhandbuch. Ausführliche Informationen zur Konfiguration eines Unternehmens-Proxys für Amazon Q finden Sie im Thema Konfiguration eines Unternehmens-Proxys in Amazon Q im Amazon Q Developer User Guide.

AWS Toolkit for Visual Studio Endpunkte

Im Folgenden finden Sie Listen mit AWS Toolkit for Visual Studio bestimmten Endpunkten und Referenzen, die zugelassen werden müssen.

Endpunkte

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

Endpunkte des Amazon Q-Plug-ins

Im Folgenden finden Sie eine Liste der Amazon Q-Plug-in-spezifischen Endpunkte und Referenzen, die zugelassen werden müssen.

```
https://idetoolkits-hostedfiles.amazonaws.com/*    (Plugin for configs)
https://idetoolkits.amazonwebservices.com/*   (Plugin for endpoints)
https://aws-toolkit-language-servers.amazonaws.com/*  (Language Server Process)
https://client-telemetry.us-east-1.amazonaws.com/ (Telemetry)
https://cognito-identity.us-east-1.amazonaws.com    (Telemetry)
https://aws-language-servers.us-east-1.amazonaws.com (Language Server Process)
```

Amazon Q Developer-Endpunkte

Im Folgenden finden Sie eine Liste der Amazon Q Developer-spezifischen Endpunkte und Referenzen, die zugelassen werden müssen.

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

Endpunkte für die Transformation von Amazon Q Code

Im Folgenden finden Sie eine Liste der spezifischen Endpunkte und Referenzen für Amazon Q Code Transform, die zugelassen werden müssen.

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

Endpunkte für die Authentifizierung

Im Folgenden finden Sie eine Liste der Authentifizierungsendpunkte und Referenzen, die zugelassen werden müssen.

```
[Directory ID or alias].awsapps.com
* oidc.[Region].amazonaws.com
*.sso.[Region].amazonaws.com
*.sso-portal.[Region].amazonaws.com
*.aws.dev
*.awsstatic.com
*.console.aws.a2z.com
*.sso.amazonaws.com
```

Identitätsendpunkte

Die folgenden Listen enthalten identitätsspezifische Endpunkte, wie z. B. die AWS IAM Identity Center AWS Builder-ID.

AWS IAM Identity Center

Einzelheiten zu den erforderlichen Endpunkten für IAM Identity Center finden Sie unter dem Thema „IAM Identity Center aktivieren“ im Benutzerhandbuch. AWS IAM Identity Center

Enterprise IAM Identity Center

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

AWS Builder-ID

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

Telemetrie

Im Folgenden ist ein telemetriespezifischer Endpunkt aufgeführt, der zugelassen werden muss.

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

Referenzen

Im Folgenden finden Sie eine Liste von Endpunktreferenzen.

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

```
assets.sso-portal.eu-west-1.amazonaws.com
oidc.eu-west-1.amazonaws.com
aws-toolkit-language-servers.amazonaws.com
aws-language-servers.us-east-1.amazonaws.com
idetoolkits.amazonwebservices.com
```

Mit AWS Diensten arbeiten

In den folgenden Themen werden die ersten Schritte zur Arbeit mit AWS Diensten aus dem AWS Toolkit for Visual Studio mit Amazon Q beschrieben.

Themen

Amazon CodeCatalyst für das AWS Toolkit for Visual Studio mit Amazon Q

Was ist Amazon CodeCatalyst?

Amazon CodeCatalyst ist ein cloudbasierter Kollaborationsraum für Softwareentwicklungsteams. Wenn Sie das AWS Toolkit for Visual Studio mit Amazon Q verwenden, können Sie CodeCatalyst

Ressourcen direkt vom AWS Toolkit for Visual Studio mit Amazon Q aus anzeigen und verwalten. Weitere Informationen CodeCatalyst dazu finden Sie im CodeCatalystAmazon-Benutzerhandbuch.

In den folgenden Themen wird beschrieben, wie Sie das AWS Toolkit for Visual Studio mit Amazon Q verbinden CodeCatalyst und wie Sie mit dem CodeCatalyst AWS Toolkit for Visual Studio mit Amazon Q arbeiten.

Themen

Erste Schritte mit Amazon CodeCatalyst und dem AWS Toolkit for Visual Studio mit Amazon Q

Gehen Sie wie folgt vor, um mit der Arbeit mit Amazon CodeCatalyst aus dem AWS Toolkit for Visual Studio mit Amazon Q zu beginnen.

Themen

Installation des AWS Toolkit for Visual Studio mit Amazon Q

Bevor Sie das AWS Toolkit for Visual Studio mit Amazon Q in Ihre CodeCatalyst Konten integrieren, stellen Sie sicher, dass Sie eine aktuelle Version von AWS Toolkit for Visual Studio mit Amazon Q verwenden. Einzelheiten zur Installation und Einrichtung der neuesten Version von AWS Toolkit for Visual Studio mit Amazon Q finden Sie im Abschnitt Einrichtung des AWS Toolkit for Visual Studio mit Amazon Q dieses Benutzerhandbuchs.

Ein Konto und eine Builder-ID erstellen CodeCatalyst AWS

Zusätzlich zur Installation der neuesten Version des AWS Toolkit for Visual Studio mit Amazon Q benötigen Sie eine aktive AWS Builder-ID und ein CodeCatalyst Konto, um eine Verbindung mit AWS

Toolkit for Visual Studio mit Amazon Q herzustellen. Wenn Sie keine aktive AWS Builder-ID oder kein aktives CodeCatalyst Builder-Konto haben, lesen Sie den CodeCatalyst Abschnitt Einrichtung mit im Benutzerhandbuch. CodeCatalyst

> **Note**
>
> Eine AWS Builder-ID unterscheidet sich von Ihren Anmeldeinformationen. AWS Anweisungen zur Registrierung und Authentifizierung mit einer AWS Builder-ID finden Sie im Thema Authentifizierung und Zugriff: AWS Builder-ID in diesem Benutzerhandbuch.
> Ausführliche Informationen zu AWS Builder IDs finden Sie unter dem Thema AWS Builder ID im AWS Allgemeinen Referenzbenutzerhandbuch.

AWS Toolkit for Visual Studio mit Amazon Q verbinden mit CodeCatalyst

Gehen Sie wie folgt vor, um AWS Toolkit for Visual Studio mit Amazon Q mit Ihrem CodeCatalyst Konto zu verbinden.

1. Wählen Sie im Git-Menüelement in Visual Studio die Option Clone Repository... .
2. Wählen Sie im Abschnitt „Ein Repository durchsuchen“ Amazon CodeCatalyst als Anbieter aus.
3. Wählen Sie im Abschnitt Verbindung die Option Connect with AWS Builder ID aus, um die CodeCatalyst Konsole in Ihrem bevorzugten Webbrowser zu öffnen.
4. Geben Sie in Ihrem Browser Ihre AWS Builder-ID in das dafür vorgesehene Feld ein und folgen Sie den Anweisungen, um fortzufahren.
5. Wenn Sie dazu aufgefordert werden, wählen Sie Zulassen, um die Verbindung zwischen AWS Toolkit for Visual Studio with Amazon Q und Ihrem CodeCatalyst Konto zu bestätigen. Wenn der Verbindungsvorgang abgeschlossen ist, CodeCatalyst wird eine Bestätigung angezeigt, dass Sie Ihren Browser sicher schließen können.

Arbeiten mit CodeCatalyst Amazon-Ressourcen aus dem AWS Toolkit for Visual Studio mit Amazon Q

Die folgenden Abschnitte bieten einen Überblick über die Amazon CodeCatalyst Amazon-Ressourcenverwaltungsfunktionen, die für das AWS Toolkit for Visual Studio mit Amazon Q verfügbar sind.

Themen

Klonen Sie ein Repository

CodeCatalyst ist ein cloudbasierter Dienst, bei dem Sie mit der Cloud verbunden sein müssen, um an CodeCatalyst Projekten arbeiten zu können. Um lokal an einem Projekt zu arbeiten, können Sie CodeCatalyst Repositorys auf Ihrem lokalen Computer klonen und mit Ihrem CodeCatalyst Projekt synchronisieren, wenn Sie das nächste Mal eine Verbindung zur Cloud herstellen.

Gehen Sie wie folgt vor, um ein Repository auf Ihren lokalen Computer zu klonen.

1. Wählen Sie im Git-Menüelement in Visual Studio die Option Clone Repository... .
2. Wählen Sie im Abschnitt „Ein Repository durchsuchen“ Amazon CodeCatalyst als Anbieter aus.

> **Note**
>
> Wenn im Abschnitt Verbindung eine `Not Connected` Meldung angezeigt wird, führen Sie die Schritte im Abschnitt Authentifizierung und Zugriff: AWS Builder-ID dieses Benutzerhandbuchs durch, bevor Sie fortfahren.

3. Wählen Sie den Bereich und das Projekt aus, aus dem Sie ein Repository klonen möchten.
4. Wählen Sie im Bereich Repositorys das Repository aus, das Sie klonen möchten.
5. Wählen Sie im Abschnitt Pfad den Ordner aus, in den Sie Ihr Repository klonen möchten.

> **Note**
>
> Dieser Ordner muss zunächst leer sein, um erfolgreich klonen zu können.

6. Wählen Sie Clone, um mit dem Klonen des Repositorys zu beginnen.
7. Nachdem das Repository geklont wurde, lädt Visual Studio Ihre geklonte Lösung

> **Note**
>
> Wenn Visual Studio die Lösung nicht im geklonten Repository öffnet, können Ihre Visual Studio-Optionen über die Einstellung Automatisch beim Öffnen eines Git-Repositorys laden in den globalen Git-Einstellungen des Quellcodeverwaltungsmenüs angepasst werden.

Fehlerbehebung

Im Folgenden finden Sie Themen zur Fehlerbehebung zur Behebung bekannter Probleme bei der Arbeit mit Amazon CodeCatalyst aus dem AWS Toolkit for Visual Studio mit Amazon Q.

Themen

Anmeldeinformationen

Wenn Sie beim Versuch, ein Git-basiertes Repository von zu klonen, auf ein Dialogfeld stoßen, in dem Sie nach Anmeldeinformationen gefragt werden CodeCatalyst, ist Ihr AWS CodeCommit Credential-Helper möglicherweise global konfiguriert, was zu Interferenzen mit führt. CodeCatalyst Weitere Informationen zum AWS CodeCommit Credential Helper finden Sie im Abschnitt Einrichten von Schritten für HTTPS-Verbindungen zu AWS CodeCommit Repositorys unter Windows mit dem AWS CLI Credential Helper im AWS CodeCommitBenutzerhandbuch.

Gehen Sie wie folgt vor, um den AWS CodeCommit Credential-Helper auf die Verarbeitung zu beschränken. CodeCommit URLs

1. öffne die globale Git-Konfigurationsdatei in: `%userprofile%\.gitconfig`
2. Suchen Sie den folgenden Abschnitt in Ihrer Datei:

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

3. Ändern Sie diesen Abschnitt wie folgt:

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

4. Speichern Sie Ihre Änderungen und führen Sie dann die Schritte zum Klonen Ihres Repositorys aus.

Amazon CloudWatch Logs-Integration für Visual Studio

Die Amazon CloudWatch Logs-Integration aus dem AWS Toolkit for Visual Studio mit Amazon Q gibt Ihnen die Möglichkeit, CloudWatch Logs-Ressourcen zu überwachen, zu speichern und darauf zuzugreifen, ohne Ihre IDE verlassen zu müssen. Um mehr über die Einrichtung des CloudWatch Service und die Arbeit mit den CloudWatch Logs-Funktionen zu erfahren, wählen Sie eines der folgenden Themen aus.

Themen

CloudWatch Log-Integration für Visual Studio einrichten

Bevor Sie die Amazon CloudWatch Logs-Integration mit dem AWS Toolkit mit Amazon Q verwenden können, benötigen Sie ein AWS Konto. Sie können auf der AWS Anmeldeseite ein neues AWS Konto erstellen. Auf die meisten CloudWatch Logs-Funktionen, die im AWS Toolkit mit Amazon Q verfügbar sind, kann mit aktiven AWS Anmeldeinformationen zugegriffen werden. Wenn für eine bestimmte Funktion eine zusätzliche Konfiguration erforderlich ist, sind die Anforderungen in den entsprechenden Abschnitten des Handbuchs Arbeiten mit CloudWatch Protokollen aufgeführt.

Weitere Informationen und Optionen zur Einrichtung von CloudWatch Logs finden Sie im Abschnitt Getting setup des Amazon CloudWatch Logs-Handbuchs.

Arbeiten mit CloudWatch Protokollen in Visual Studio

Die Amazon CloudWatch Logs-Integration ermöglicht es Ihnen, CloudWatch Logs aus dem AWS Toolkit for Visual Studio mit Amazon Q zu überwachen, zu speichern und darauf zuzugreifen. Der Zugriff auf CloudWatch Logs-Funktionen — ohne Ihre IDE verlassen zu müssen — verbessert die Effizienz, indem der CloudWatch Logs-Entwicklungsprozess vereinfacht und Unterbrechungen in Ihrem Arbeitsablauf reduziert werden. In den folgenden Themen wird beschrieben, wie Sie mit den grundlegenden Merkmalen und Funktionen der Logs-Integration arbeiten. CloudWatch

Themen

- Zusätzlicher Zugriff auf CloudWatch Protokolle

CloudWatch Protokollgruppen

A `log group` ist eine Gruppe von Gruppen`log streams`, die dieselben Einstellungen für Aufbewahrung, Überwachung und Zugriffskontrolle verwenden. Es gibt keine Begrenzung dazu, wie viele Protokollstreams zu einer Protokollgruppe gehören können.

Protokollgruppen anzeigen

Die `View Log Groups` Funktion zeigt eine Liste von Protokollgruppen im CloudWatch Protokollgruppen-Explorer an.

Gehen Sie wie folgt vor, um auf die Funktion „ CloudWatch Protokollgruppen anzeigen“ zuzugreifen und den Protokollgruppen-Explorer zu öffnen.

1. Erweitern Sie Amazon im AWS Explorer CloudWatch.
2. Doppelklicken Sie auf Protokollgruppen oder öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Ansicht, um den CloudWatch Protokollgruppen-Explorer zu öffnen.

> **Note**
>
> Der CloudWatch Log Groups Explorer wird an derselben Fensterposition wie der Solutions Explorer geöffnet.

Protokollgruppen filtern

Ihr individuelles Konto kann Tausende verschiedener Protokollgruppen enthalten. Verwenden Sie die unten beschriebene `filtering` Funktion, um Ihre Suche nach bestimmten Gruppen zu vereinfachen.

1. Platzieren CloudWatch Sie im Log Groups Explorer den Cursor in der Suchleiste oben im Fenster.
2. Geben Sie zunächst ein Präfix ein, das sich auf die Log-Gruppen bezieht, nach denen Sie suchen.
3. CloudWatch Der Log Groups Explorer wird automatisch aktualisiert und zeigt Ergebnisse an, die den Suchbegriffen entsprechen, die Sie im vorherigen Schritt angegeben haben.

Protokollgruppen löschen

Gehen Sie wie folgt vor, um eine bestimmte Protokollgruppe zu löschen.

1. Klicken CloudWatch Sie im Protokollgruppen-Explorer mit der rechten Maustaste auf die Protokollgruppe, die Sie löschen möchten.
2. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass Sie die aktuell ausgewählte Protokollgruppe löschen möchten.
3. Wenn Sie auf Ja klicken, wird die ausgewählte Protokollgruppe gelöscht und anschließend der CloudWatch Protokollgruppen-Explorer aktualisiert.

Protokollgruppen aktualisieren

Um die aktuelle Liste der im Protokollgruppen-Explorer angezeigten Protokollgruppen zu aktualisieren, klicken Sie in der CloudWatch Werkzeugleiste auf die Symbolschaltfläche „Aktualisieren“.

Protokollgruppen-ARN kopieren

Um den ARN einer bestimmten Protokollgruppe zu kopieren, führen Sie die unten beschriebenen Schritte aus.

1. Klicken CloudWatch Sie im Log Groups Explorer mit der rechten Maustaste auf die Protokollgruppe, aus der Sie einen ARN kopieren möchten.
2. Wählen Sie im Menü die Option ARN kopieren.
3. Der ARN wird jetzt in Ihre lokale Zwischenablage kopiert und kann eingefügt werden.

CloudWatch Streams protokollieren

Ein Protokollstream ist eine Abfolge von Protokollereignissen, die dieselbe Quelle nutzen.

> **Note**
>
> Beachten Sie beim Anzeigen von Log-Streams die folgenden Eigenschaften:
>
> - Standardmäßig sind die Protokollstreams nach dem Zeitstempel des letzten Ereignisses sortiert.

- Mit einem Log-Stream verknüpfte Spalten können entweder in aufsteigender oder absteigender Reihenfolge sortiert werden, indem das Einfügezeichen in den Spaltenüberschriften umgeschaltet wird.
- Gefilterte Einträge können nur nach dem Namen des Protokolldatenstroms sortiert werden.

Log-Streams anzeigen

1. Doppelklicken Sie im CloudWatch Protokollgruppen-Explorer auf eine Protokollgruppe, oder klicken Sie mit der rechten Maustaste auf eine Protokollgruppe und wählen Sie im Kontextmenü die Option Protokollstream anzeigen aus.
2. Im Dokumentfenster wird eine neue Registerkarte geöffnet, die eine Liste der Logstreams enthält, die Ihrer Protokollgruppe zugeordnet sind.

Log-Streams filtern

1. Platzieren Sie auf der Registerkarte „Log-Streams“ im Dokumentfenster den Cursor in der Suchleiste.
2. Beginnen Sie mit der Eingabe eines Präfixes, das sich auf den Log-Stream bezieht, nach dem Sie suchen.
3. Während der Eingabe wird die aktuelle Anzeige automatisch aktualisiert, um Ihre Log-Streams nach Ihren Eingaben zu filtern.

Log-Streams aktualisieren

Um die aktuelle Liste der im Dokumentfenster angezeigten Protokollstreams zu aktualisieren, klicken Sie in der Werkzeugleiste neben der Suchleiste auf die Symbolschaltfläche „Aktualisieren“.

ARN für Protokollstreams kopieren

Um den ARN eines bestimmten Log-Streams zu kopieren, führen Sie die unten beschriebenen Schritte aus.

1. Klicken Sie auf der Registerkarte Log Streams im Dokumentfenster mit der rechten Maustaste auf den Logstream, aus dem Sie einen ARN kopieren möchten.
2. Wählen Sie im Menü die Option ARN kopieren.

3. Der ARN wird jetzt in Ihre lokale Zwischenablage kopiert und kann eingefügt werden.

Laden Sie Log-Streams herunter

Mit der Funktion Protokollstream exportieren wird der ausgewählte Protokollstream heruntergeladen und lokal gespeichert, sodass benutzerdefinierte Tools und Software zur weiteren Verarbeitung darauf zugreifen können.

1. Klicken Sie im Dokumentfenster auf der Registerkarte Protokolldatenströme mit der rechten Maustaste auf den Protokollstream, den Sie herunterladen möchten.
2. Wählen Sie Protokollstream exportieren, um das Dialogfeld In eine Textdatei exportieren zu öffnen.
3. Wählen Sie den Speicherort, an dem Sie die Datei lokal speichern möchten, und geben Sie einen Namen in das dafür vorgesehene Textfeld ein.
4. Bestätigen Sie den Download, indem Sie OK wählen. Der Status des Downloads wird im Visual Studio Task Status Center angezeigt

CloudWatch Ereignisse protokollieren

Protokollereignisse sind Aufzeichnungen von Aktivitäten, die von der Anwendung oder Ressource aufgezeichnet wurden, von der bzw. die überwacht wird CloudWatch.

Aktionen von Ereignissen protokollieren

Protokollereignisse werden als Tabelle angezeigt. Standardmäßig werden die Ereignisse vom ältesten bis zum neuesten Ereignis sortiert.

Die folgenden Aktionen sind mit Protokollereignissen in Visual Studio verknüpft:

- Modus für umbrochenen Text: Sie können den umbrochenen Text umschalten, indem Sie auf ein Ereignis klicken.
- Schaltfläche für Textumbruch: Diese Schaltfläche befindet sich in der und schaltet den Zeilenumbruch für `document window` **`toolbar`** alle Einträge ein und aus.
- Nachrichten in die Zwischenablage kopieren: Wählen Sie die Nachrichten aus, die Sie kopieren möchten, klicken Sie dann mit der rechten Maustaste auf die Auswahl und wählen Sie Kopieren (Tastenkombination). `Ctrl + C`

Protokollereignisse anzeigen

1. Wählen Sie im Dokumentfenster eine Registerkarte aus, die eine Liste von Protokolldatenströmen enthält.
2. Doppelklicken Sie auf einen Log-Stream oder klicken Sie mit der rechten Maustaste auf einen Log-Stream und wählen Sie im Menü Log-Stream anzeigen aus.
3. Im Dokumentfenster wird eine neue Registerkarte mit Protokollereignissen geöffnet, die eine Tabelle mit Protokollereignissen enthält, die mit dem ausgewählten Protokollstream verknüpft sind.

Filterung von Protokollereignissen

Es gibt drei Möglichkeiten, Protokollereignisse zu filtern: nach Inhalt, Zeitraum oder beidem. Um Ihre Protokollereignisse sowohl nach Inhalt als auch nach Zeitraum zu filtern, filtern Sie Ihre Nachrichten zunächst nach Inhalt oder Zeitraum und filtern Sie diese Ergebnisse dann mit der anderen Methode.

So filtern Sie Ihre Protokollereignisse nach Inhalt:

1. Platzieren Sie auf der Registerkarte „Protokollereignisse“ im Dokumentfenster den Cursor in der Suchleiste, die sich oben im Fenster befindet.
2. Beginnen Sie mit der Eingabe eines Begriffs oder einer Wortgruppe, die sich auf die Protokollereignisse bezieht, nach denen Sie suchen.
3. Während der Eingabe beginnt die aktuelle Anzeige automatisch, Ihre Protokollereignisse zu filtern.

> **Note**
>
> Filtermuster beachten die Groß-/Kleinschreibung. Sie können die Suchergebnisse verbessern, indem Sie exakte Begriffe und Wortgruppen mit nicht-alphanumerischen Zeichen in doppelte Anführungszeichen (*""*) setzen. Ausführlichere Informationen zu Filtermustern finden Sie unter dem Thema Filter- und Mustersyntax im CloudWatch Amazon-Leitfaden.

So zeigen Sie Protokollereignisse an, die in einem bestimmten Zeitraum generiert wurden:

1. Wählen Sie auf der Registerkarte „Ereignisse protokollieren“ im Dokumentfenster die Symbolschaltfläche „Kalender“ in der Werkzeugleiste aus.

2. Geben Sie mithilfe der bereitgestellten Felder den Zeitraum an, in dem Sie suchen möchten.
3. Die gefilterten Ergebnisse werden automatisch aktualisiert, wenn Sie die Datums- und Uhrzeitbeschränkungen angeben.

> **Note**
>
> Die Option Filter löschen löscht alle Ihre aktuellen date-and-time Filterauswahlen.

Protokollereignisse aktualisieren

Um die aktuelle Liste der Protokollereignisse, die auf der Registerkarte „Protokollereignisse“ angezeigt wird, zu aktualisieren, wählen Sie in der Werkzeugleiste die Symbolschaltfläche „Aktualisieren“.

Zusätzlicher Zugriff auf CloudWatch Protokolle

Sie können direkt über das AWS Toolkit in Visual Studio auf CloudWatch Protokolle zugreifen, die mit anderen AWS Diensten und Ressourcen verknüpft sind.

Lambda

So zeigen Sie Log-Streams an, die mit einer Lambda-Funktion verknüpft sind:

> **Note**
>
> Ihre Lambda-Ausführungsrolle muss über die entsprechenden Berechtigungen verfügen, um Protokolle an Logs zu CloudWatch senden. Weitere Informationen zu den für CloudWatch Logs erforderlichen Lambda-Berechtigungen finden Sie in der https://docs.aws.amazon.com/lambda/latest/dg/monitoring-cloudwatchlogs.html#monitoring-cloudwatchlogs-prereqs

1. Erweitern Sie Lambda im AWS Toolkit Explorer.
2. Klicken Sie mit der rechten Maustaste auf die Funktion, die Sie anzeigen möchten, und wählen Sie dann Protokolle anzeigen, um die zugehörigen Log-Streams im Dokumentfenster zu öffnen.

So zeigen Sie Log-Streams mit der Lambda-Integration `function view` an:

1. Erweitern Sie Lambda im AWS Toolkit Explorer.

2. Klicken Sie mit der rechten Maustaste auf die Funktion, die Sie anzeigen möchten, und wählen Sie dann Funktion anzeigen, um die Funktionsansicht im Dokumentfenster zu öffnen.
3. Wechseln Sie von der `function view` Registerkarte Logs zur Registerkarte Logs. Dort werden die Log-Streams angezeigt, die der ausgewählten Lambda-Funktion zugeordnet sind.

ECS

Gehen Sie wie folgt vor, um Protokollressourcen anzuzeigen, die einem ECS-Task-Container zugeordnet sind.

> **Note**
>
> Damit der Amazon ECS-Service Protokolle senden kann CloudWatch, muss jeder Container für eine bestimmte Amazon ECS-Task die erforderliche Konfiguration erfüllen. Weitere Informationen zur erforderlichen Einrichtung und Konfiguration finden Sie in der Anleitung Using the AWS Logs Log Driver.

1. Erweitern Sie Amazon ECS im AWS Toolkit Explorer.
2. Wählen Sie den Amazon ECS-Cluster aus, den Sie anzeigen möchten, um im Dokumentfenster eine neue Registerkarte für den ECS-Cluster zu öffnen.
3. Wählen Sie im Navigationsmenü auf der linken Seite der Registerkarte ECS-Cluster die Option Aufgaben aus, um alle mit dem Cluster verknüpften Aufgaben aufzulisten.
4. Wählen Sie in der Aufgabenanzeige eine Aufgabe aus und klicken Sie auf den Link Protokolle anzeigen, der sich in der unteren linken Ecke befindet.

> **Note**
>
> In dieser Anzeige werden alle im Cluster enthaltenen Aufgaben aufgeführt. Der `View Logs` Link ist nur für jede Aufgabe sichtbar, die der erforderlichen Protokollkonfiguration entspricht.
>
> - Wenn eine Aufgabe nur einem einzelnen Container zugeordnet ist, öffnet der Link „Protokolle anzeigen“ den Log-Stream dieses Containers.
> - Wenn eine Aufgabe mehreren Containern zugeordnet ist, öffnet der Link „Logs anzeigen“ das Dialogfeld „ CloudWatch Logs für ECS-Task anzeigen“. Wählen Sie im

Drop-down-Menü Container: den Container aus, für den Sie Logs anzeigen möchten, und wählen Sie dann OK.

5. Im Dokumentfenster wird eine neue Registerkarte geöffnet, auf der die Log-Streams angezeigt werden, die mit Ihrer Container-Auswahl verknüpft sind.

Verwaltung von EC2 Amazon-Instances

AWS Der Explorer bietet detaillierte Ansichten der Amazon Machine Images (AMI) - und Amazon Elastic Compute Cloud (Amazon EC2) -Instances. In diesen Ansichten können Sie eine EC2 Amazon-Instance von einem AMI aus starten, eine Verbindung zu dieser Instance herstellen und die Instance entweder beenden oder beenden, und das alles innerhalb der Visual Studio-Entwicklungsumgebung. Sie können die Instanzenansicht verwenden, um AMIs aus Ihren Instances etwas zu erstellen. Weitere Informationen finden Sie unter Erstellen eines AMI aus einer EC2 Amazon-Instance.

Die Ansichten von Amazon Machine Images und Amazon EC2 Instances

Im AWS Explorer können Sie Ansichten von Amazon Machine Images (AMIs) und EC2 Amazon-Instances anzeigen. Erweitern Sie im AWS Explorer den EC2Amazon-Knoten.

Um die AMIs Ansicht anzuzeigen, öffnen Sie auf dem ersten Unterknoten das Kontextmenü (Rechtsklick) und wählen Sie dann Ansicht. AMIs

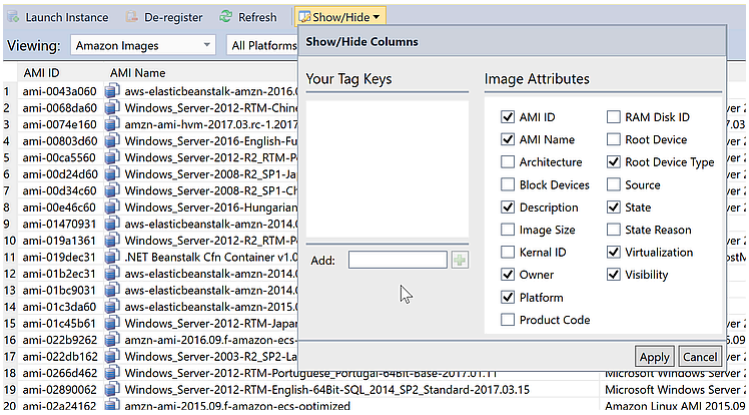
Um die EC2 Amazon-Instanzen-Ansicht anzuzeigen, öffnen Sie im Knoten Instances das Kontextmenü (Rechtsklick) und wählen Sie dann Ansicht aus.

Sie können die jeweilige Ansicht auch durch Doppelklicken auf den jeweiligen Knoten anzeigen.

- Die Ansichten beziehen sich auf die im AWS Explorer angegebene Region (z. B. die Region USA West (Nordkalifornien)).
- Sie können die Reihenfolge der Spalten durch Klicken und Ziehen ändern. Klicken Sie auf die Spaltenüberschrift, um die Werte in einer Spalte zu sortieren.
- Anhand der Dropdown-Listen und des Filterfelds in Viewing (Anzeigen) können Sie Ansichten konfigurieren. In der ersten Ansicht werden alle Plattformtypen (Windows oder Linux) angezeigt AMIs , die dem im Explorer angegebenen Konto gehören. AWS

Spalten ein-/ausblenden

Sie können auch über die Dropdown-Liste Show/Hide (Einblenden/Ausblenden) oben in der Ansicht festlegen, welche Spalten angezeigt werden. Ihre Spaltenauswahl bleibt bestehen, wenn Sie die Ansicht schließen und erneut öffnen.



BenutzeroberflächeShow/Hide Columns (Spalten einblenden/ausblenden) für AMI- und Instances-Ansichten

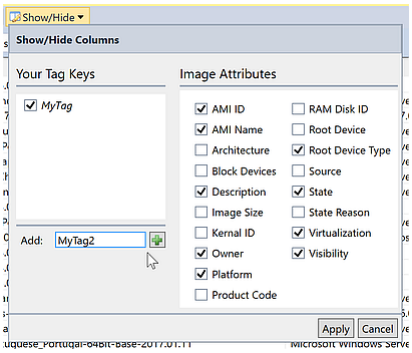
Tagging AMIs, Instanzen und Volumes

Sie können auch die Drop-down-Liste Ein-/Ausblenden verwenden AMIs, um Tags für EC2 Amazon-Instances oder Volumes hinzuzufügen, die Sie besitzen. Bei Tags handelt es sich um Name-Wert-Paare, mit denen Sie Metadaten an Ihre AMIs Instances und Volumes anhängen können. Tagnamen beziehen sich sowohl auf Ihr Konto als auch separat auf Ihre Instanzen und Instanzen. AMIs Es gäbe beispielsweise keinen Konflikt, wenn Sie denselben Tag-Namen für Ihre Instances AMIs und Ihre Instances verwenden würden. Bei den Tagnamen muss die Groß- und Kleinschreibung nicht berücksichtigt werden.

Weitere Informationen zu Tags finden Sie unter Using Tags im EC2 Amazon-Benutzerhandbuch für Linux-Instances.

So fügen Sie ein Tag hinzu

1. Geben Sie in das Feld Add (Hinzufügen) einen Namen für das Tag ein. Wählen Sie die grüne Schaltfläche mit dem Pluszeichen (+), und dann Apply (Anwenden).



Hinzufügen eines Tags zu einer AMI- oder EC2 Amazon-Instance

Das neue Tag wird in Kursivschrift angezeigt. Das bedeutet, dass noch keine Werte mit diesem Tag verknüpft wurden.

Der Tagname erscheint in der Listenansicht als neue Spalte. Wenn dem Tag mindestens ein Wert zugeordnet wurde, ist das Tag in der sichtbar AWS Management Console.

2. Wenn Sie einem Tag einen Wert hinzufügen möchten, doppelklicken Sie in die Spalte für dieses Tag und geben einen Wert ein. Um den Tagwert zu löschen, doppelklicken Sie auf die Zelle und löschen den Text.

   Wenn Sie das Tag aus der Dropdown-Liste Show/Hide (Einblenden/Ausblenden) entfernen, verschwindet die entsprechende Spalte aus der Ansicht. Das Tag bleibt erhalten, ebenso wie alle Tag-Werte AMIs, die mit Instances oder Volumes verknüpft sind.

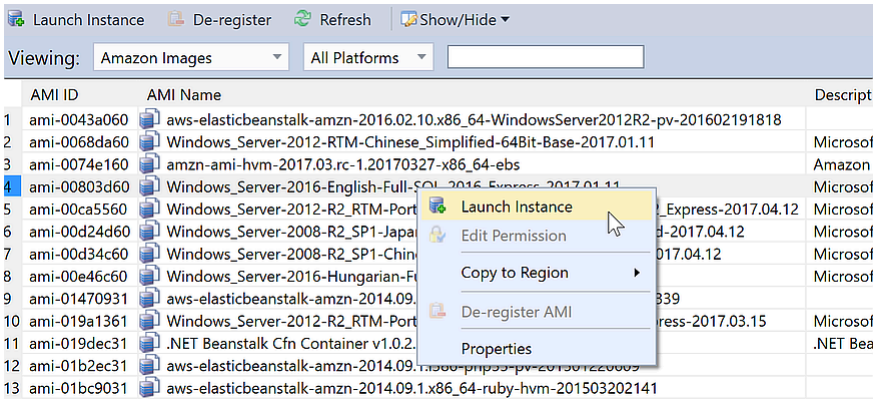
> **Note**
>
> Wenn Sie ein Tag in der Dropdownliste Ein-/Ausblenden löschen, dem keine Werte zugeordnet sind, löscht das AWS Toolkit das Tag vollständig. Es wird dann nicht mehr in der Listenansicht und auch nicht mehr in der Dropdown-Liste Show/Hide (Einblenden/Ausblenden) angezeigt. Wenn Sie dieses Tag erneut nutzen möchten, verwenden Sie das Dialogfeld Show/Hide (Einblenden/Ausblenden), um es wieder zu erstellen.

Starten einer EC2 Amazon-Instance

AWS Der Explorer bietet alle Funktionen, die zum Starten einer EC2 Amazon-Instance erforderlich sind. In diesem Abschnitt wählen wir ein Amazon Machine Image (AMI) aus, konfigurieren es und starten es dann als EC2 Amazon-Instance.

So starten Sie eine Windows EC2 Server-Amazon-Instance

1. Wählen Sie oben in der AMIs Ansicht in der Drop-down-Liste auf der linken Seite Amazon Images aus. Wählen Sie in der Dropdown-Liste rechts Windows aus. Geben Sie in das Filterfeld `ebs` für Elastic Block Storage ein. Es kann einen Moment dauern, bis die Ansicht aktualisiert ist.
2. Wählen Sie ein AMI aus der Liste aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Launch Instance (Instance starten) aus.



AMI-Liste

3. Konfigurieren Sie im Dialogfeld Neue EC2 Amazon-Instance starten das AMI für Ihre Anwendung.

   Instance-Typ

   Wählen Sie den Typ der EC2 Instance aus, die gestartet werden soll. Eine Liste der Instance-Typen und Preisinformationen finden Sie auf der EC2 Preisseite.

   Name

   Geben Sie einen Namen für die Instance ein. Dieser Name darf nicht mehr als 256 Zeichen enthalten.

   Schlüsselpaar

   Ein key pair wird verwendet, um das Windows-Passwort abzurufen, mit dem Sie sich mithilfe des Remote Desktop Protocol (RDP) bei der EC2 Instanz anmelden. Wählen Sie ein Schlüsselpaar aus, für das Sie Zugriff auf den privaten Schlüssel haben oder wählen Sie die Option für die Erstellung eines Schlüsselpaars. Wenn Sie das Schlüsselpaar im Toolkit erstellen, kann dieses den privaten Schlüssel für Sie speichern.

   Die im Toolkit enthaltenen Schlüsselpaare sind verschlüsselt. Sie können sie unter `%LOCALAPPDATA%\AWSToolkit\keypairs` finden (normalerweise `C:\Users\<user>`

`\AppData\Local\AWSToolkit\keypairs`). Sie können das verschlüsselte Schlüsselpaar in eine `.pem`-Datei exportieren.

a. Wählen Sie in Visual Studio Ansicht aus und klicken Sie auf AWS Explorer.

b. Klicken Sie auf Amazon EC2 und wählen Sie Schlüsselpaare aus.

c. Die Schlüsselpaare werden aufgelistet, und die vom Toolkit erstellten/verwalteten Schlüsselpaare werden als Gespeichert in markiert. AWSToolkit

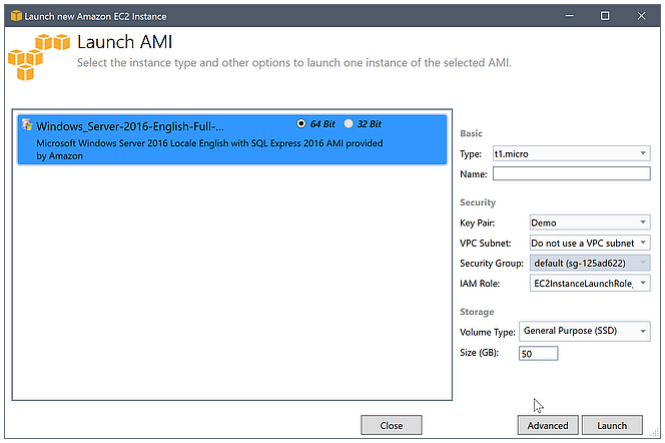
d. Klicken Sie mit der rechten Maustaste auf das Schlüsselpaar, das Sie erstellt haben, und wählen Sie Export Private Key (Privaten Schüssel exportieren) aus. Der private Schlüssel bleibt unverschlüsselt und wird am angegebenen Speicherort gespeichert.

Sicherheitsgruppe

Die Sicherheitsgruppe steuert die Art des Netzwerkverkehrs, den die EC2 Instance akzeptiert. Wählen Sie eine Sicherheitsgruppe, die eingehenden Datenverkehr auf Port 3389, dem von RDP verwendeten Port, zulässt, sodass Sie eine Verbindung mit der EC2 Instance herstellen können. Informationen zur Verwendung des Toolkits zum Erstellen von Sicherheitsgruppen finden Sie unter Sicherheitsgruppen im Explorer verwalten. AWS

Instance-Profil

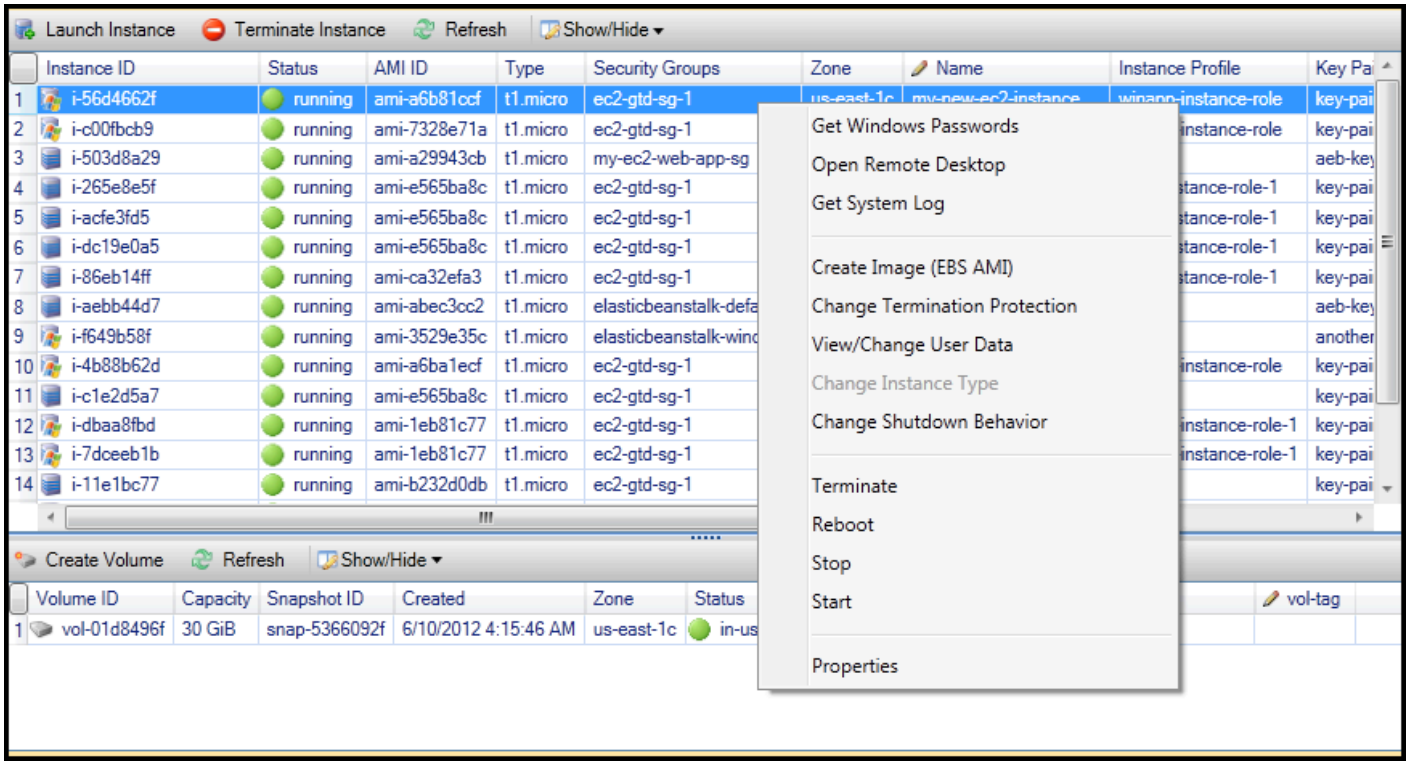
Das Instance-Profil ist ein logischer Container für eine IAM-Rolle. Wenn Sie ein Instanzprofil auswählen, ordnen Sie der Instanz die entsprechende IAM-Rolle zu. EC2 IAM-Rollen sind mit Richtlinien konfiguriert, die den Zugriff auf Amazon Web Services und Kontoressourcen spezifizieren. Wenn eine EC2 Instance einer IAM-Rolle zugeordnet ist, wird die Anwendungssoftware, die auf der Instance ausgeführt wird, mit den in der IAM-Rolle angegebenen Berechtigungen ausgeführt. Dadurch kann die Anwendungssoftware ausgeführt werden, ohne dass eigene AWS Anmeldeinformationen angegeben werden müssen, wodurch die Software sicherer wird. Weitere Informationen über IAM-Rollen finden Sie im IAM User Guide.



EC2 Dialogfeld „AMI starten“

4. Wählen Sie Launch (Starten) aus.

Öffnen Sie im AWS Explorer im Unterknoten Instances von Amazon EC2 das Kontextmenü (Rechtsklick) und wählen Sie dann Ansicht aus. Das AWS Toolkit zeigt die Liste der EC2 Amazon-Instances an, die mit dem aktiven Konto verknüpft sind. Möglicherweise müssen Sie die Schaltfläche Refresh (Aktualisieren) wählen, damit die neue Instance angezeigt wird. Wenn die Instance zum ersten Mal angezeigt wird, kann sie sich noch wenige Minuten im ausstehenden Modus befinden. Nach ein paar Minuten wechselt sie jedoch in einen Ausführungsmodus.



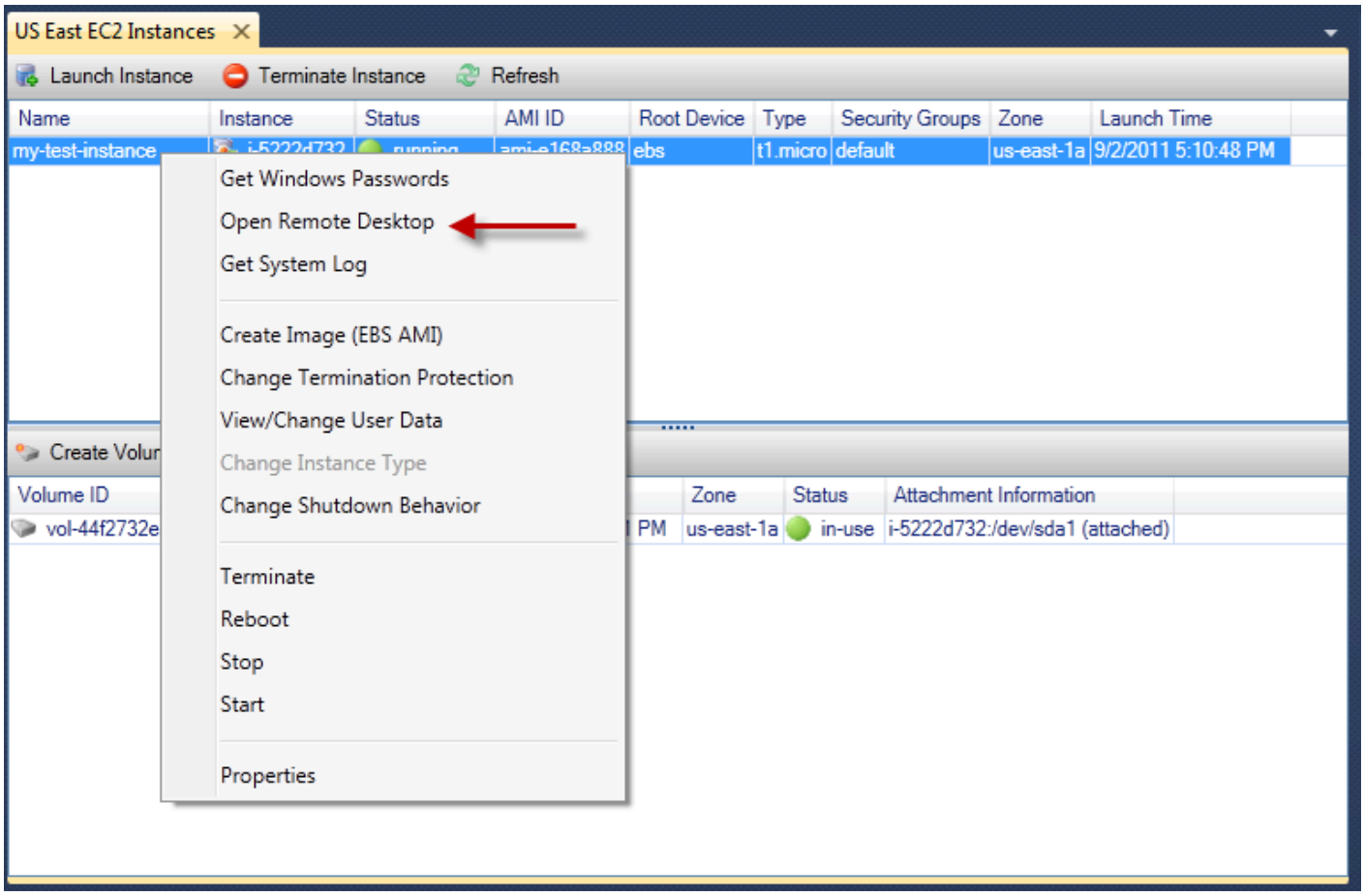
Verbindung zu einer EC2 Amazon-Instance herstellen

Sie können Windows Remote Desktop verwenden, um eine Verbindung mit einer Windows Server-Instance herzustellen. Für die Authentifizierung können Sie mit dem AWS Toolkit das Administratorkennwort für die Instanz abrufen, oder Sie können einfach das gespeicherte key pair verwenden, das der Instanz zugeordnet ist. Im folgenden Verfahren wird das gespeicherte Schlüsselpaar verwendet.

So stellen Sie eine Verbindung zur Windows Server-Instance unter Verwendung von Windows Remote Desktop her

1. Klicken Sie in der EC2 Instanzliste mit der rechten Maustaste auf die Windows Server-Instanz, zu der Sie eine Verbindung herstellen möchten. Wählen Sie aus dem Kontextmenü Open Remote Desktop (Remote Desktop öffnen).

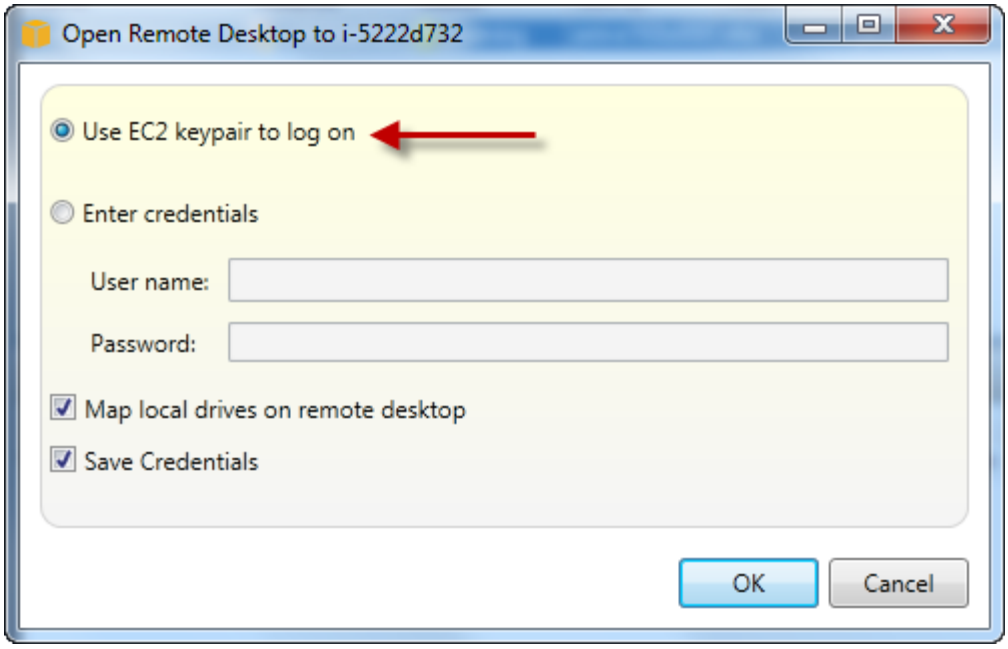
   Wenn Sie sich mit dem Administratorpasswort authentifizieren möchten, müssen Sie hierfür Get Windows Passwords (Windows-Passwörter abrufen) wählen.



   EC2 Kontextmenü der Instanz

2. Wählen Sie im Dialogfeld „Remotedesktop öffnen“ die Option „Anmeldung EC2 mit Schlüsselpaar verwenden“ und anschließend „OK“.

   Wenn Sie kein key pair mit dem AWS Toolkit gespeichert haben, geben Sie die PEM-Datei an, die den privaten Schlüssel enthält.

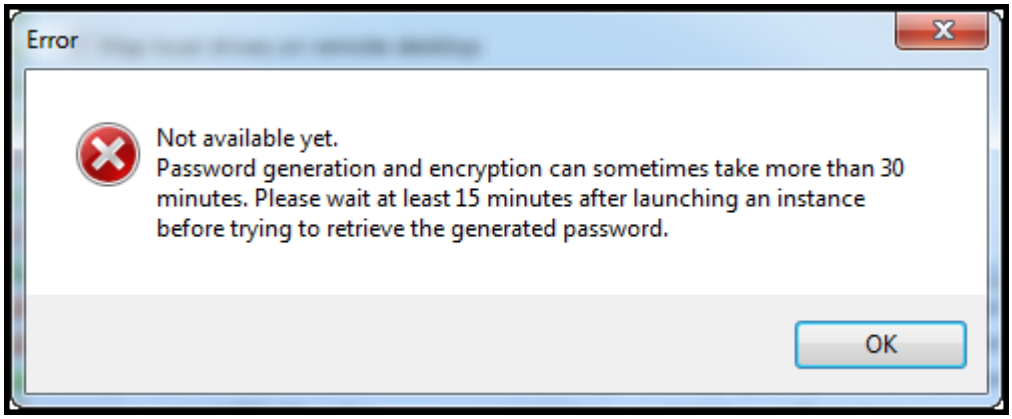


   Dialogfeld "Open Remote Desktop (Remotedesktop öffnen)"

3. Das Fenster Remote Desktop öffnet sich. Sie müssen sich nicht anmelden, da die Authentifizierung mit dem Schlüsselpaar erfolgt ist. Sie werden als Administrator auf der EC2 Amazon-Instance laufen.

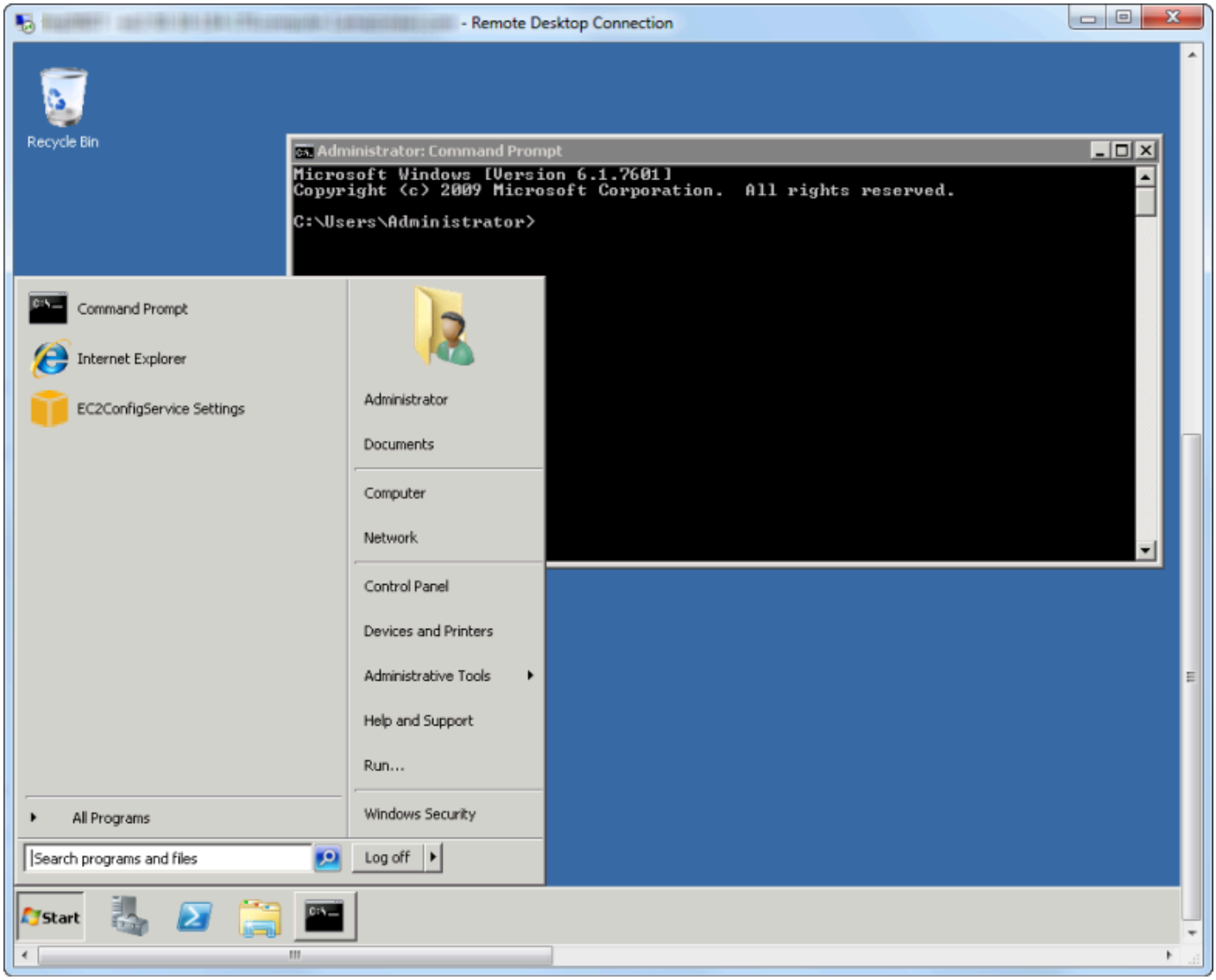
   Wenn die EC2 Instance erst kürzlich gestartet wurde, können Sie aus zwei möglichen Gründen möglicherweise keine Verbindung herstellen:

   - Der Remote Desktop Service ist noch nicht in Betrieb. Warten Sie einige Minuten und versuchen Sie es dann erneut.
   - Die Passwortinformationen wurden noch nicht in die Instance übertragen. In diesem Fall wird eine Meldung ähnlich der Folgenden wird angezeigt.



Passwort noch nicht verfügbar

In der folgenden Abbildung ist ein Benutzer zu sehen, der über Remote Desktop als Administrator verbunden ist.



Remotedesktop

Beenden einer EC2 Amazon-Instance

Mit dem AWS Toolkit können Sie eine laufende EC2 Amazon-Instance von Visual Studio aus beenden oder beenden. Um die Instance zu beenden, muss die EC2 Instance ein Amazon EBS-Volume verwenden. Wenn die EC2 Instance kein Amazon EBS-Volume verwendet, besteht Ihre einzige Möglichkeit darin, die Instance zu beenden.

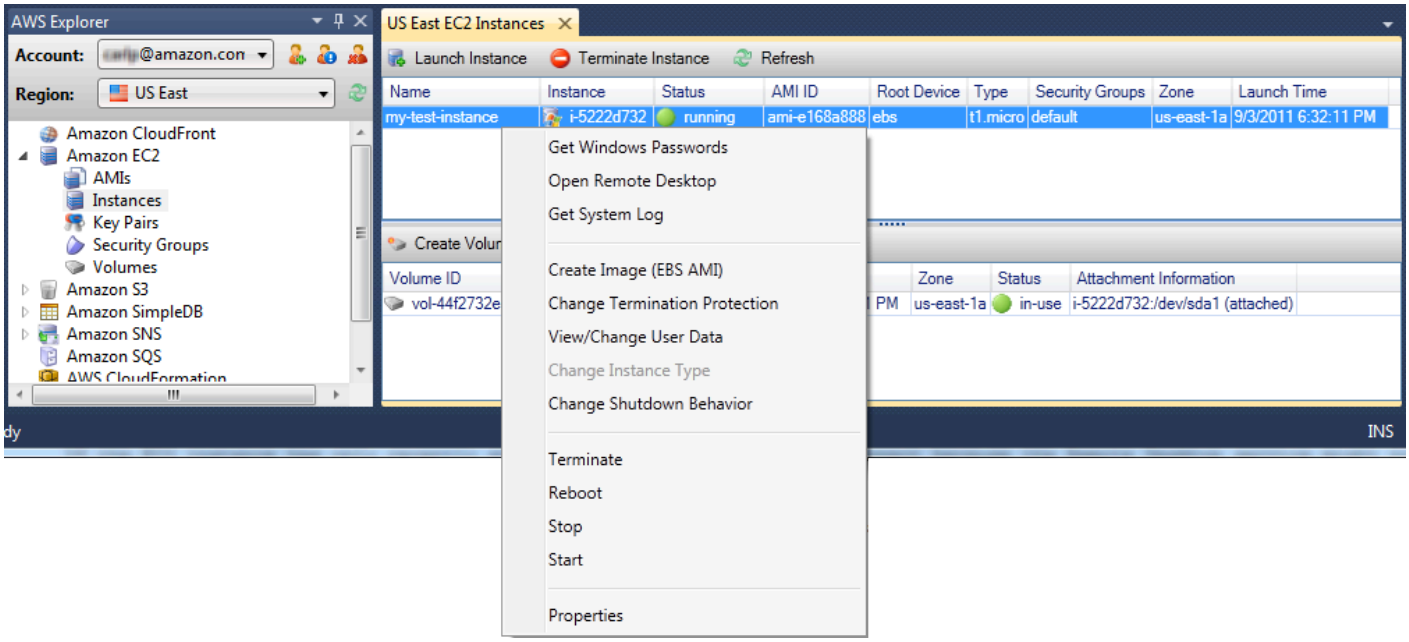
Wenn Sie die Instance stoppen, werden auf dem EBS-Volume gespeicherte Daten beibehalten. Wenn Sie die Instance beenden, gehen alle Daten auf dem lokalen Speichergerät der Instance verloren. In beiden Fällen, ob Sie die Instance beenden oder beenden, wird Ihnen die EC2 Instance

nicht weiter in Rechnung gestellt. Wenn Sie eine Instance stoppen, wird Ihnen jedoch weiterhin der EBS-Speicher in Rechnung gestellt, der nach dem Stoppen der Instance bestehen bleibt.

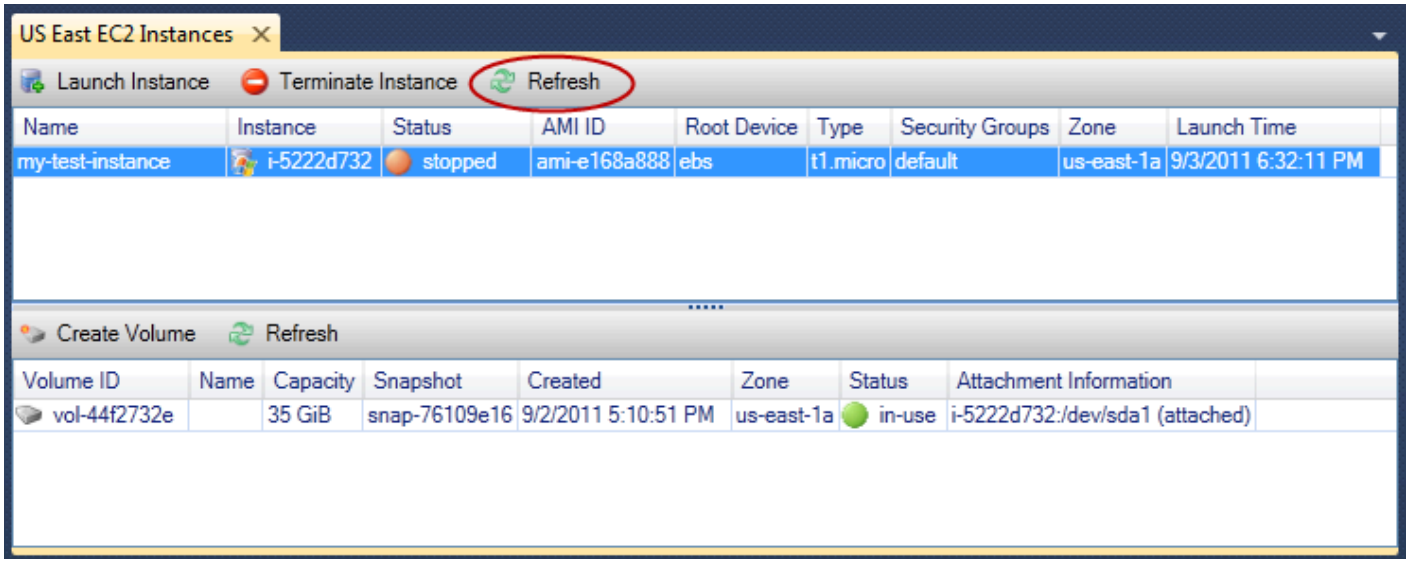
Eine weitere Möglichkeit zum Beenden einer Instanz besteht darin, mit Remote Desktop eine Verbindung mit der Instance herzustellen und dann aus dem Windows Start-Menü den Befehl Shutdown (Herunterfahren) zu verwenden. Sie können die Instance so konfigurieren, dass sie bei diesem Szenario entweder gestoppt oder beendet wird.

Um eine EC2 Amazon-Instance zu stoppen

1. Erweitern Sie im AWS Explorer den EC2Amazon-Knoten, öffnen Sie das Kontextmenü (mit der rechten Maustaste) für Instances und wählen Sie dann Ansicht aus. Klicken Sie in der Liste Instances mit der rechten Maustaste auf die Instanz, die Sie stoppen möchten, und wählen Sie aus dem Kontextmenü Stop (Anhalten) aus. Wählen Sie Yes (Ja) aus, um zu bestätigen, dass Sie die Instance stoppen möchten.

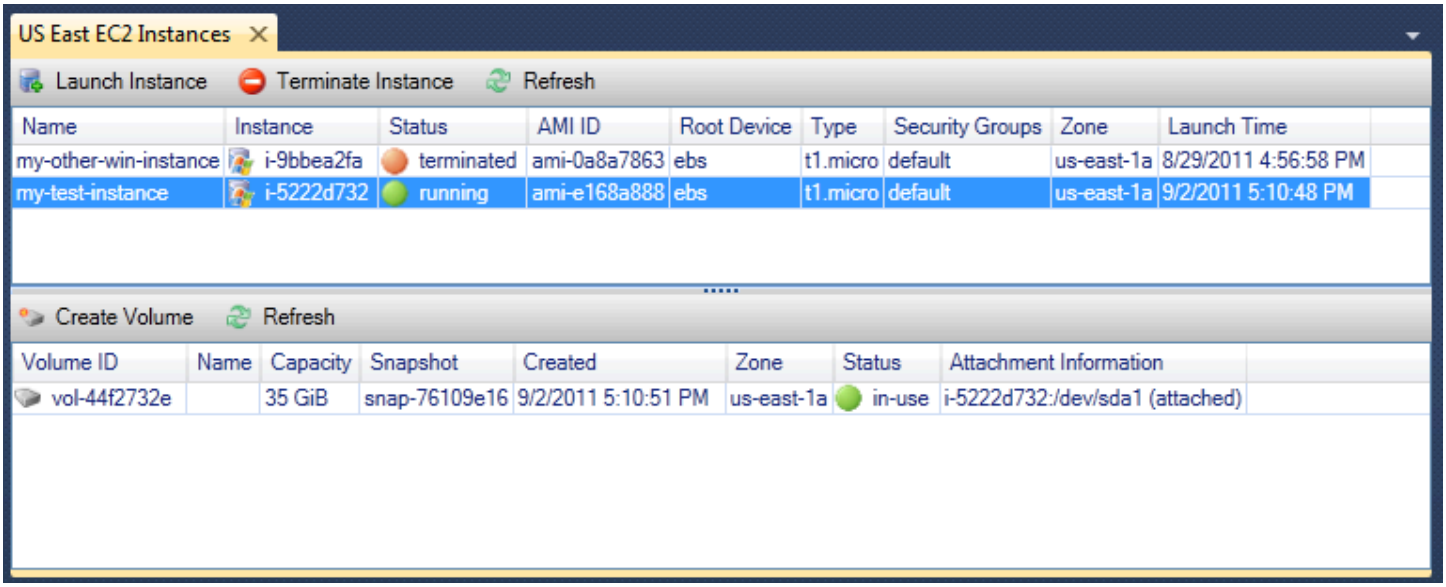


2. Wählen Sie oben in der Instanzenliste die Option Aktualisieren aus, um die Statusänderung der EC2 Amazon-Instance zu sehen. Da die Instance eher gestoppt als beendet wurde, ist das mit der Instance verknüpfte EBS-Volume noch aktiv.



Beendete Instances bleiben sichtbar

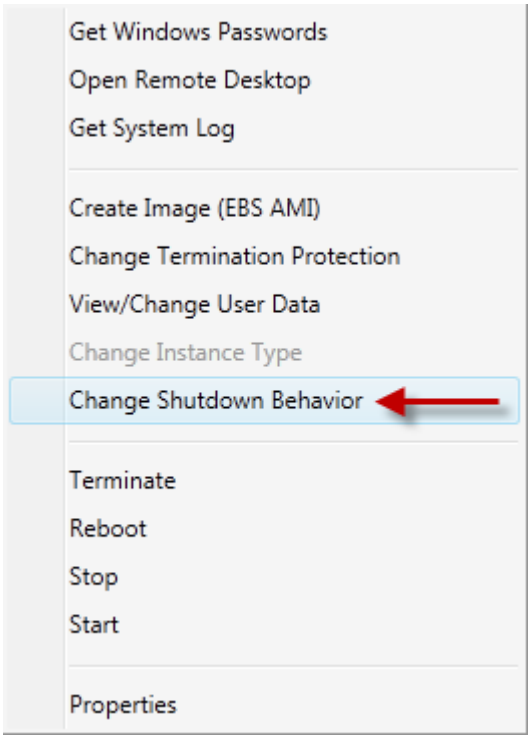
Wenn Sie eine Instance beenden, bleibt diese weiterhin in der Instance-Liste neben den laufenden oder gestoppten Instances sichtbar. Fordert diese Instances schließlich AWS zurück und sie verschwinden aus der Liste. Beendete Instances werden Ihnen nicht in Rechnung gestellt.



Um das Verhalten einer EC2 Instanz beim Herunterfahren festzulegen

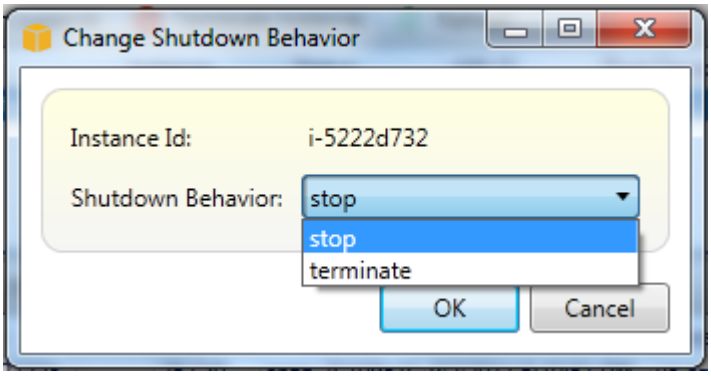
Mit dem AWS Toolkit können Sie angeben, ob eine EC2 Amazon-Instance gestoppt oder beendet werden soll, wenn Shutdown im Startmenü ausgewählt ist.

1. Klicken Sie in der Instance-Liste mit der rechten Maustaste auf eine EC2 Amazon-Instance und wählen Sie dann Shutdown-Verhalten ändern aus.



Menüelement Change Shutdown Behavior (Verhalten beim Herunterfahren ändern)

2. Wählen Sie im Dialogfeld Change Shutdown Behavior (Verhalten beim Herunterfahren ändern) in der Dropdown-Liste Shutdown Behavior (Verhalten beim Herunterfahren) die Option Stop (Anhalten) oder Terminate (Beenden) aus.



Verwalten von Amazon ECS Instances

AWS Der Explorer bietet detaillierte Ansichten der Amazon Elastic Container Service (Amazon ECS) -Cluster und Container-Repositorys. Sie können Cluster- und Container-Details über die Visual Studio-Entwicklungsumgebung erstellen, löschen und verwalten.

Ändern von Service-Eigenschaften

Sie können Service-Details, Service-Ereignisse und Service-Eigenschaften in der Cluster-Ansicht anzeigen.

1. Öffnen Sie im AWS Explorer das Kontextmenü (mit der rechten Maustaste) für den zu verwaltenden Cluster und wählen Sie dann Ansicht aus.
2. Klicken Sie in der ECS-Cluster-Ansicht auf Services auf der linken Seite, und klicken Sie dann auf der Registerkarte Details in der Details-Ansicht. Sie können auf Events (Ereignisse) klicken, um Ereignismeldungen anzuzeigen, und auf Deployments (Bereitstellungen), um den Bereitstellungsstatus anzuzeigen.
3. Klicken Sie auf Bearbeiten. Sie können die gewünschte Aufgabenanzahl und den minimalen und maximalen Prozentsatz fehlerfreier Aufgaben ändern.
4. Klicken Sie auf Save (Speichern), um die Änderungen zu übernehmen oder Cancel (Abbrechen), um zu vorhandenen Werten zurückzukehren.

Beenden einer Aufgabe

In der Cluster-Ansicht können Sie den aktuellen Status von Aufgaben anzeigen und eine oder mehrere Aufgaben beenden.

So beenden Sie eine Aufgabe

1. Öffnen Sie im AWS Explorer das Kontextmenü (Rechtsklick) für den Cluster mit den Aufgaben, die Sie beenden möchten, und wählen Sie dann Ansicht aus.
2. Klicken Sie in der ECS-Cluster-Ansicht auf Tasks (Aufgaben) auf der linken Seite.
3. Stellen Sie sicher, dass Desired Task Status (Gewünschter Aufgabenstatus) auf `Running` gesetzt ist. Wählen Sie die einzelnen Aufgaben aus, die beendet werden sollen, und klicken Sie dann auf Stop (Beenden) oder klicken Sie auf Stop All (Alle beenden), um alle ausgeführten Aufgaben auszuwählen und zu beenden.
4. Klicken Sie im Dialogfeld Stop Tasks (Aufgaben anhalten) auf Yes (Ja).

Löschen eines Service

Über die Cluster-Ansicht können Sie Services aus einem Cluster löschen.

So löschen Sie einen Cluster-Service

1. Öffnen Sie im AWS Explorer das Kontextmenü (mit der rechten Maustaste) für den Cluster mit einem Dienst, den Sie löschen möchten, und wählen Sie dann Ansicht aus.
2. Klicken Sie in der ECS-Cluster-Ansicht auf Services auf der linken Seite, und klicken Sie dann auf Delete (Löschen).
3. Wenn es einen Load Balancer und eine Zielgruppe in Ihrem Cluster gibt, können Sie diese im Dialogfeld Delete Cluster (Cluster löschen) löschen. Sie werden nicht verwendet, wenn der Service gelöscht wird.
4. Wählen Sie im Dialogfeld Delete Cluster (Cluster löschen) die Option OK aus. Wenn der Cluster gelöscht wird, wird er aus dem AWS Explorer entfernt.

Löschen eines Clusters

Sie können einen Amazon Elastic Container Service-Cluster aus dem AWS Explorer löschen.

Löschen eines Clusters

1. Öffnen Sie im AWS Explorer unter dem Knoten Clusters von Amazon ECS das Kontextmenü (Rechtsklick) für den Cluster, den Sie löschen möchten, und wählen Sie dann Löschen.
2. Wählen Sie im Dialogfeld Delete Cluster (Cluster löschen) die Option OK aus. Wenn der Cluster gelöscht wird, wird er aus dem AWS Explorer entfernt.

Erstellen eines Repositorys

Sie können im AWS Explorer ein Amazon Elastic Container Registry-Repository erstellen.

So erstellen Sie ein Repository

1. Öffnen Sie im AWS Explorer das Kontextmenü (Rechtsklick) des Knotens Repositorys unter Amazon ECS und wählen Sie dann Create Repository.
2. Geben Sie im Dialogfeld Create Repository (Repository erstellen) einen Namen für ein Repository ein und wählen Sie dann OK aus.

Löschen eines Repositorys

Sie können ein Amazon Elastic Container Registry-Repository aus dem AWS Explorer löschen.

So löschen Sie ein Repository

1. Öffnen Sie im AWS Explorer das Kontextmenü (Rechtsklick) des Knotens Repositorys unter Amazon ECS und wählen Sie dann Repository löschen.
2. Im Dialogfeld Delete Repository (Repository löschen) können Sie das Repository auch dann löschen, wenn es Images enthält. Andernfalls wird es nur gelöscht werden, wenn es leer ist. Klicken Sie auf Yes (Ja).

Sicherheitsgruppen vom AWS Explorer aus verwalten

Das Toolkit for Visual Studio ermöglicht es Ihnen, Sicherheitsgruppen für die Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances und zu erstellen und AWS CloudFormation zu konfigurieren. Wenn Sie EC2 Amazon-Instances starten oder eine Anwendung bereitstellen AWS CloudFormation, geben Sie eine Sicherheitsgruppe an, die den EC2 Amazon-Instances zugeordnet werden soll. (Bereitstellung zur Erstellung von AWS CloudFormation EC2 Amazon-Instances.)

Eine Sicherheitsgruppe ist wie eine Firewall für eingehenden Netzwerkverkehr. Die Sicherheitsgruppe gibt an, welche Arten von Netzwerkverkehr auf einer EC2 Amazon-Instance zulässig sind. Sie können auch festlegen, dass nur eingehender Datenverkehr von bestimmten IP-Adressen oder nur von angegebenen Benutzern oder anderen Sicherheitsgruppen akzeptiert wird.

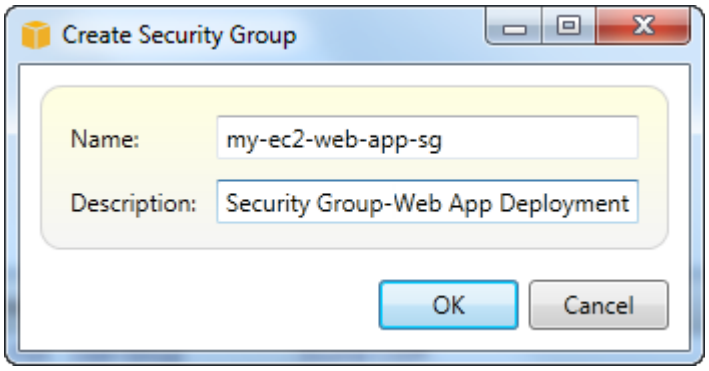
Erstellen einer Sicherheitsgruppe

In diesem Abschnitt erstellen Sie eine Sicherheitsgruppe. Für die Sicherheitsgruppe sind nach ihrer Erstellung noch keine Berechtigungen konfiguriert. Das Konfigurieren von Berechtigungen erfolgt über einen zusätzlichen Arbeitsschritt.

So erstellen Sie eine Sicherheitsgruppe

1. Öffnen Sie im AWS Explorer unter dem EC2Amazon-Knoten das Kontextmenü (Rechtsklick) auf dem Knoten Sicherheitsgruppen und wählen Sie dann Ansicht aus.
2. Wählen Sie auf der Registerkarte EC2 Sicherheitsgruppen die Option Sicherheitsgruppe erstellen aus.

3. Geben Sie im Dialogfeld Create Security Group (Sicherheitsgruppe erstellen) einen Namen und eine Beschreibung für die Sicherheitsgruppe ein und wählen Sie dann OK aus.

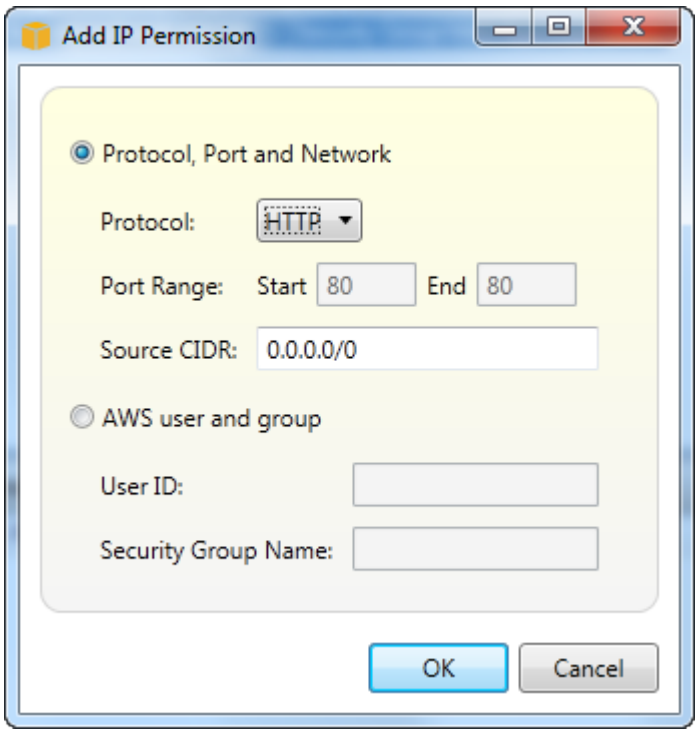


Hinzufügen von Berechtigungen zu einer Sicherheitsgruppe

In diesem Abschnitt werden Berechtigungen für die Sicherheitsgruppe hinzugefügt, um Web-Datenverkehr über HTTP- und HTTPS-Protokolle zuzulassen. Sie können auch anderen Computern erlauben, sich mithilfe des Windows Remote Desktop Protocol (RDP) zu verbinden.

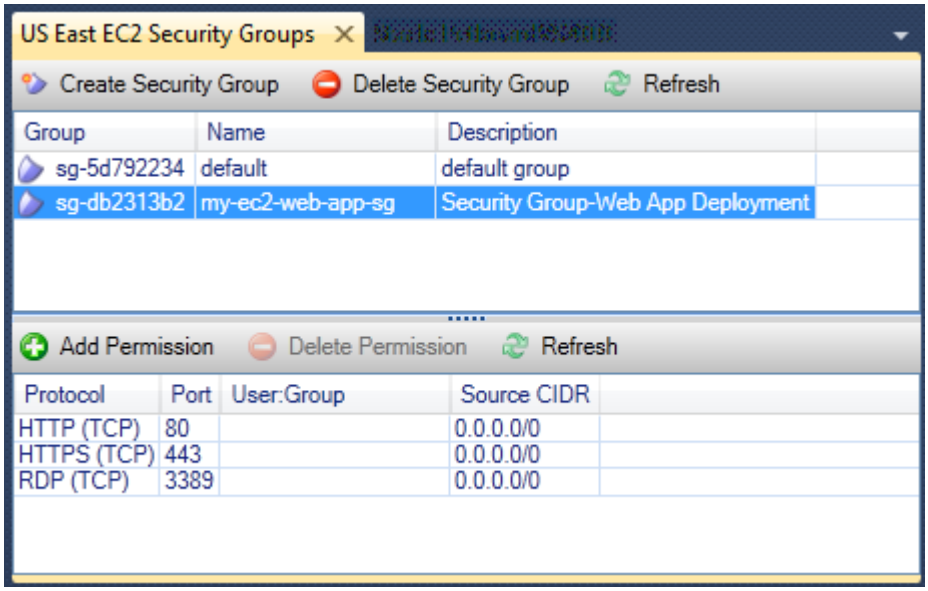
So fügen Sie einer Sicherheitsgruppe Berechtigungen hinzu

1. Wählen Sie auf der Registerkarte EC2 Sicherheitsgruppen eine Sicherheitsgruppe aus und klicken Sie dann auf die Schaltfläche „Berechtigung hinzufügen“.
2. Wählen Sie im Dialogfeld Add IP Permission (IP-Berechtigung hinzufügen) das Optionsfeld Protocol, Port and Network (Protokoll, Port und Netzwerk) und dann aus der Dropdown-Liste Protocol (Protokoll) die Option HTTP. Der Portbereich stellt sich automatisch auf Port 80 ein (Standard-Port für HTTP). Das Feld Source CIDR hat die Standardeinstellung 0.0.0.0/0, womit festgelegt wird, dass HTTP-Netzwerkverkehr von allen externen IP-Adressen akzeptiert wird. Wählen Sie OK aus.



Öffnen Sie Port 80 (HTTP) für diese Sicherheitsgruppe

3. Wiederholen Sie diesen Vorgang für HTTPS und RDP. Ihre Sicherheitsgruppen-Berechtigungen sollten jetzt wie folgt aussehen:



Sie können auch Berechtigungen in der Sicherheitsgruppe konfigurieren, indem Sie eine Benutzer-ID und einen Sicherheitsgruppennamen angeben. In diesem Fall akzeptieren EC2 Amazon-Instances in dieser Sicherheitsgruppe den gesamten eingehenden Netzwerkverkehr von EC2 Amazon-Instances

in der angegebenen Sicherheitsgruppe. Sie müssen auch die Benutzer-ID angeben, um den Namen der Sicherheitsgruppe eindeutig zu identifizieren. Sicherheitsgruppennamen müssen nicht für alle eindeutig sein. AWSWeitere Informationen zu Sicherheitsgruppen finden Sie in der Dokumentation. EC2

Ein AMI aus einer EC2 Amazon-Instance erstellen

Sie können ein Amazon Machine Image (AMI) mit dem erstellen AWS Toolkit for Visual Studio. Ausführlichere Informationen AMIs dazu finden Sie im Thema Amazon Machine Images (AMI) im Amazon Elastic Compute Cloud for Windows Instances User Guide.

Gehen Sie wie folgt vor, um ein AMI aus einer bestehenden EC2 Amazon-Instance zu erstellen.

Erstellen eines AMI aus einer vorhandenen EC2 Amazon-Instance

1. Erweitern Sie im AWS Toolkit Explorer Amazon EC2 und wählen Sie Instances aus, um eine Liste Ihrer vorhandenen Instances anzuzeigen.
2. Klicken Sie mit der rechten Maustaste auf die Instance, die Sie als Grundlage für Ihr AMI verwenden möchten, und wählen Sie Create Image (ABS AMI), um das Dialogfenster Create Image zu öffnen.
3. Geben Sie im Dialogfenster Create Image einen Namen und eine Beschreibung für Ihr Image in die dafür vorgesehenen Felder ein und klicken Sie dann auf OK, um fortzufahren.
4. Das Bestätigungsfenster „Bild erstellt“ wird in Visual Studio geöffnet, wenn das Bild erstellt wurde. Wählen Sie die Schaltfläche OK, um fortzufahren.

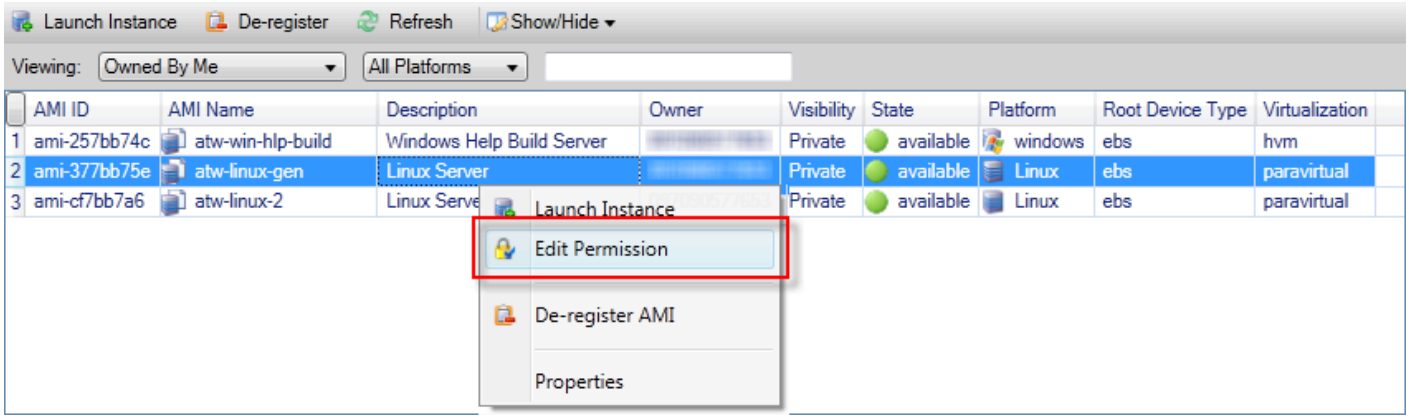
Um Ihr neues AMI mit dem AWS Toolkit anzuzeigen, erweitern Sie Amazon EC2 und doppelklicken Sie, AMIsum ein Fenster im Visual Studio Editor Payne zu öffnen, in dem eine Liste Ihrer vorhandenen angezeigt wird. AMIs Wenn Sie Ihr neues AMI nicht in der Liste sehen, wählen Sie die Schaltfläche Aktualisieren oben im AMI-Fenster.

Einrichten von Startberechtigungen für ein Amazon Machine Image

Sie können Startberechtigungen für Ihre Amazon Machine Images (AMIs) in der AMIsAnsicht im AWS Explorer festlegen. Sie können das Dialogfeld „AMI-Berechtigungen festlegen“ verwenden, um Berechtigungen von zu kopieren AMIs.

So richten Sie Berechtigungen für ein AMI ein:

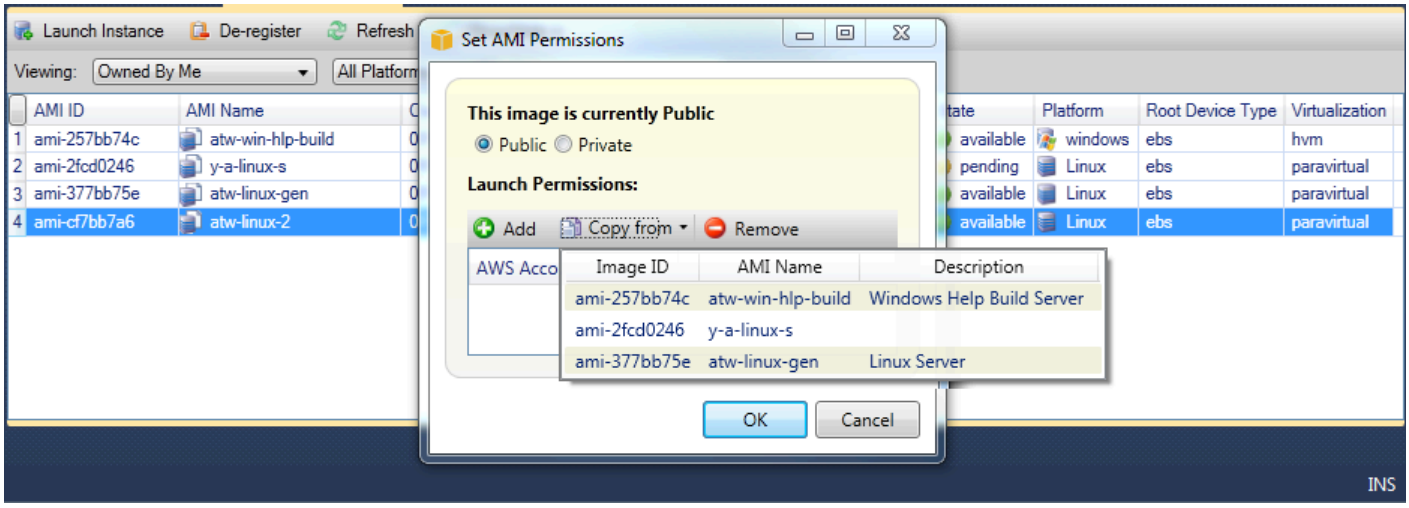
1. Öffnen AMIsSie in der Ansicht im AWS Explorer das Kontextmenü (Rechtsklick) auf einem AMI und wählen Sie dann „Berechtigung bearbeiten“.



2. Im Dialogfeld Set AMI Permissions (AMI-Berechtigungen festlegen) sind drei Optionen verfügbar:

   - Um die Startberechtigung zu erteilen, wählen Sie Hinzufügen und geben Sie die Kontonummer des AWS Benutzers ein, dem Sie die Startberechtigung erteilen.
   - Um die Startberechtigung zu entfernen, wählen Sie die Kontonummer des AWS Benutzers aus, dem Sie die Startberechtigung entziehen, und wählen Sie Entfernen aus.
   - Wenn Sie Berechtigungen von einem AMI auf ein anderes kopieren möchten, wählen Sie ein AMI aus der Liste aus und klicken dann auf Copy from (Kopieren von). Die Benutzer, die über Berechtigungen für ausgewählte AMI verfügen, erhalten Startberechtigungen für das aktuelle AMI. Sie können diesen Vorgang mit anderen AMIs in der Copy-From -Liste wiederholen, um Berechtigungen von mehreren AMIs in das Ziel-AMI zu kopieren.

     Die Copy-Fon-Liste enthält nur diejenigen, die dem Konto AMIs gehören, das aktiv war, als die AMIsAnsicht im Explorer angezeigt wurde. AWS Aus diesem Grund werden in der Liste „Von kopieren“ möglicherweise keine Dateien angezeigt, AMIs wenn dem aktiven Konto keine anderen AMIs gehören.



Dialogfeld Copy AMI permissions (AMI-Berechtigungen kopieren)

Amazon Virtual Private Cloud (VPC)

Mit Amazon Virtual Private Cloud (Amazon VPC) können Sie Amazon Web Services Services-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen. Weitere Informationen finden Sie im Amazon VPC-Benutzerhandbuch.

Das Toolkit for Visual Studio ermöglicht es Entwicklern, auf VPC-Funktionen zuzugreifen, die denen ähneln, die in der Visual Studio-Entwicklungsumgebung bereitgestellt werden, AWS Management Consoleaber von der Visual Studio-Entwicklungsumgebung aus verfügbar gemacht werden. Der Amazon VPC-Knoten von AWS Explorer umfasst Unterknoten für die folgenden Bereiche.

- VPCs
- Subnets
- Elastic IPs
- Internet-Gateways
- Netzwerk ACLs
- Routing-Tabellen
- Sicherheitsgruppen

Erstellen einer öffentlich-privaten VPC für die Bereitstellung mit AWS Elastic Beanstalk

In diesem Abschnitt wird beschrieben, wie Sie eine Amazon-VPC erstellen, die sowohl öffentliche als auch private Subnetze enthält. Das öffentliche Subnetz enthält eine EC2 Amazon-Instance, die Network Address Translation (NAT) durchführt, damit Instances im privaten Subnetz mit dem öffentlichen Internet kommunizieren können. Die zwei Subnetze müssen sich in derselben Availability Zone (AZ) befinden.

Dies ist die minimale VPC-Konfiguration, die für die Bereitstellung einer AWS Elastic Beanstalk Umgebung in einer VPC erforderlich ist. In diesem Szenario befinden sich die EC2 Amazon-Instances, die Ihre Anwendung hosten, im privaten Subnetz. Der Elastic Load Balancing Load Balancer, der eingehenden Traffic an Ihre Anwendung weiterleitet, befindet sich im öffentlichen Subnetz.

Weitere Informationen zur Network Address Translation (NAT) finden Sie unter NAT-Instances im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch. Ein Beispiel für die Konfiguration der Bereitstellung für die Verwendung einer VPC finden Sie unter Deploying to Elastic Beanstalk.

So erstellen Sie eine öffentliche/private VPC

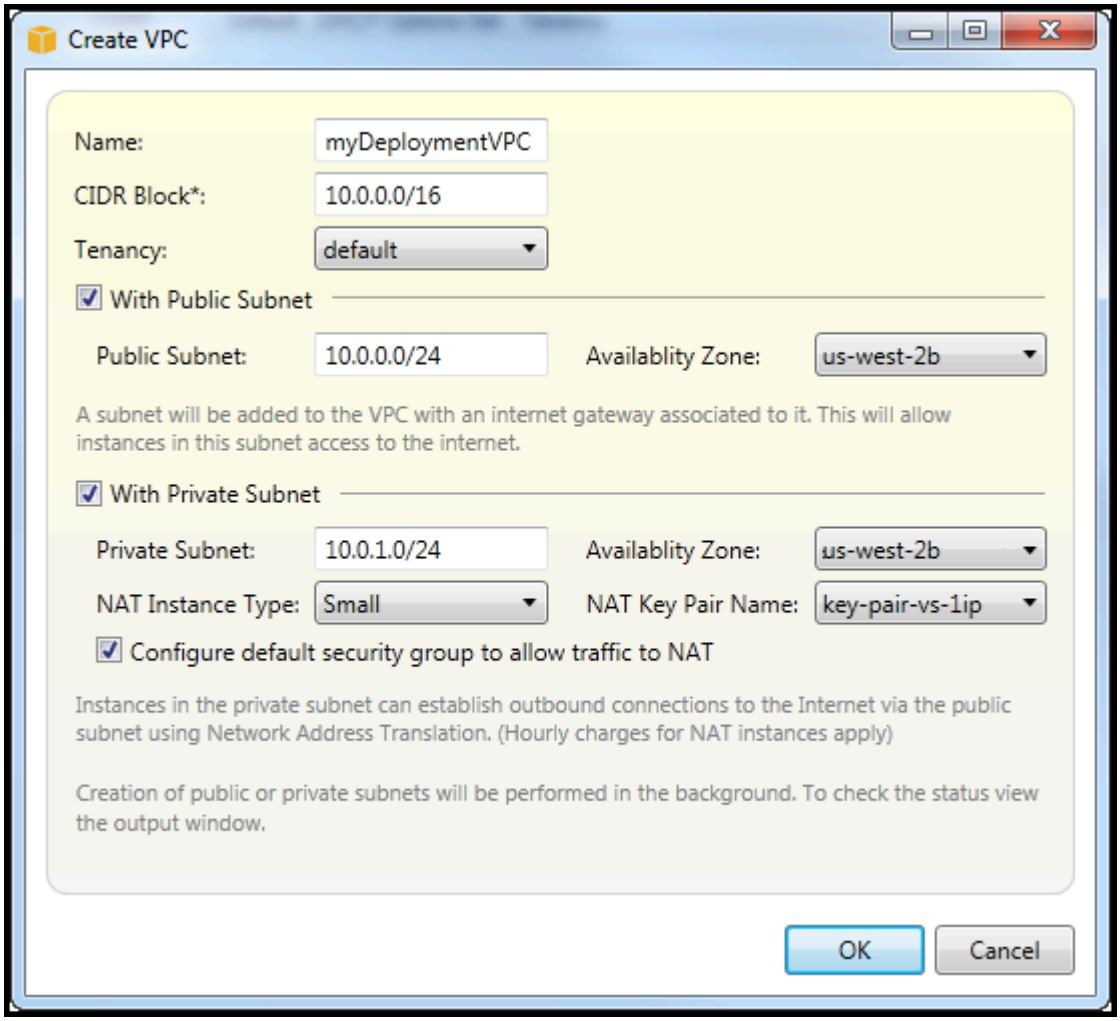
1. Öffnen Sie im Amazon VPC-Knoten im AWS Explorer den VPCsUnterknoten und wählen Sie dann Create VPC aus.

2. Konfigurieren Sie die VPC wie folgt:
   - Geben Sie einen Namen für Ihre VPC ein.

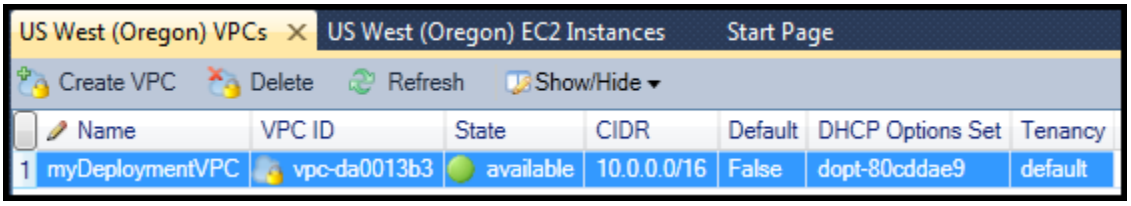
- Aktivieren Sie die Kontrollkästchen With Public Subnet (Mit öffentlichem Subnetz) und With Private Subnet (Mit privatem Subnetz).
- Wählen Sie in der Dropdown-Liste Availability Zone für jedes Subnetz eine Availability Zone aus. Verwenden Sie unbedingt dieselbe AZ für beide Subnetze.
- Geben Sie für das private Subnetz in NAT Key Pair Name (NAT-Schlüsselpaarname) ein Schlüsselpaar an. Dieses key pair wird für die EC2 Amazon-Instance verwendet, die die Netzwerkadressübersetzung vom privaten Subnetz in das öffentliche Internet durchführt.
- Aktivieren Sie das Kontrollkästchen Configure default security group to allow traffic to NAT (Datenverkehrt zum NAT für Standardsicherheitsgruppe zulassen).

Geben Sie einen Namen für Ihre VPC ein. Aktivieren Sie die Kontrollkästchen With Public Subnet (Mit öffentlichem Subnetz) und With Private Subnet (Mit privatem Subnetz). Wählen Sie in der Dropdown-Liste Availability Zone für jedes Subnetz eine Availability Zone aus. Verwenden Sie unbedingt dieselbe AZ für beide Subnetze. Geben Sie für das private Subnetz in NAT Key Pair Name (NAT-Schlüsselpaarname) ein Schlüsselpaar an. Dieses key pair wird für die EC2 Amazon-Instance verwendet, die die Netzwerkadressübersetzung vom privaten Subnetz in das öffentliche Internet durchführt. Aktivieren Sie das Kontrollkästchen Configure default security group to allow traffic to NAT (Datenverkehrt zum NAT für Standardsicherheitsgruppe zulassen).

Wählen Sie OK aus.

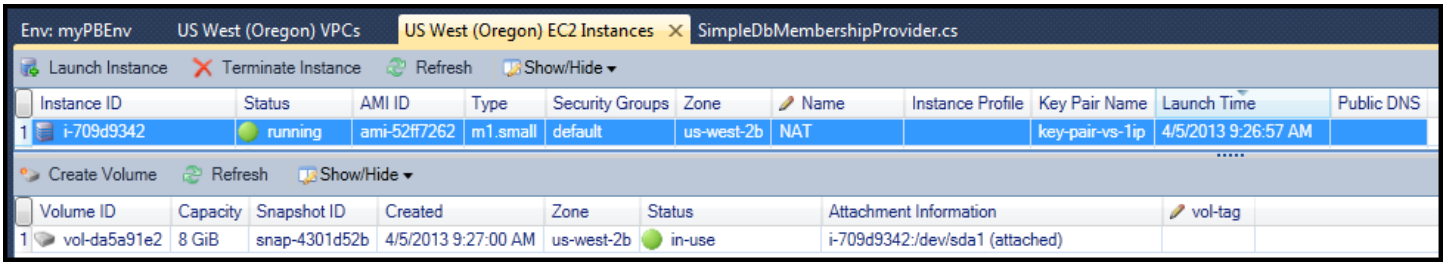


Sie können die neue VPC auf der VPCsRegisterkarte im AWS Explorer anzeigen.



Es dauert einen Moment, bis die NAT-Instance gestartet wird. Wenn er verfügbar ist, können Sie ihn anzeigen, indem Sie den EC2Amazon-Knoten im AWS Explorer erweitern und dann den Unterknoten Instances öffnen.

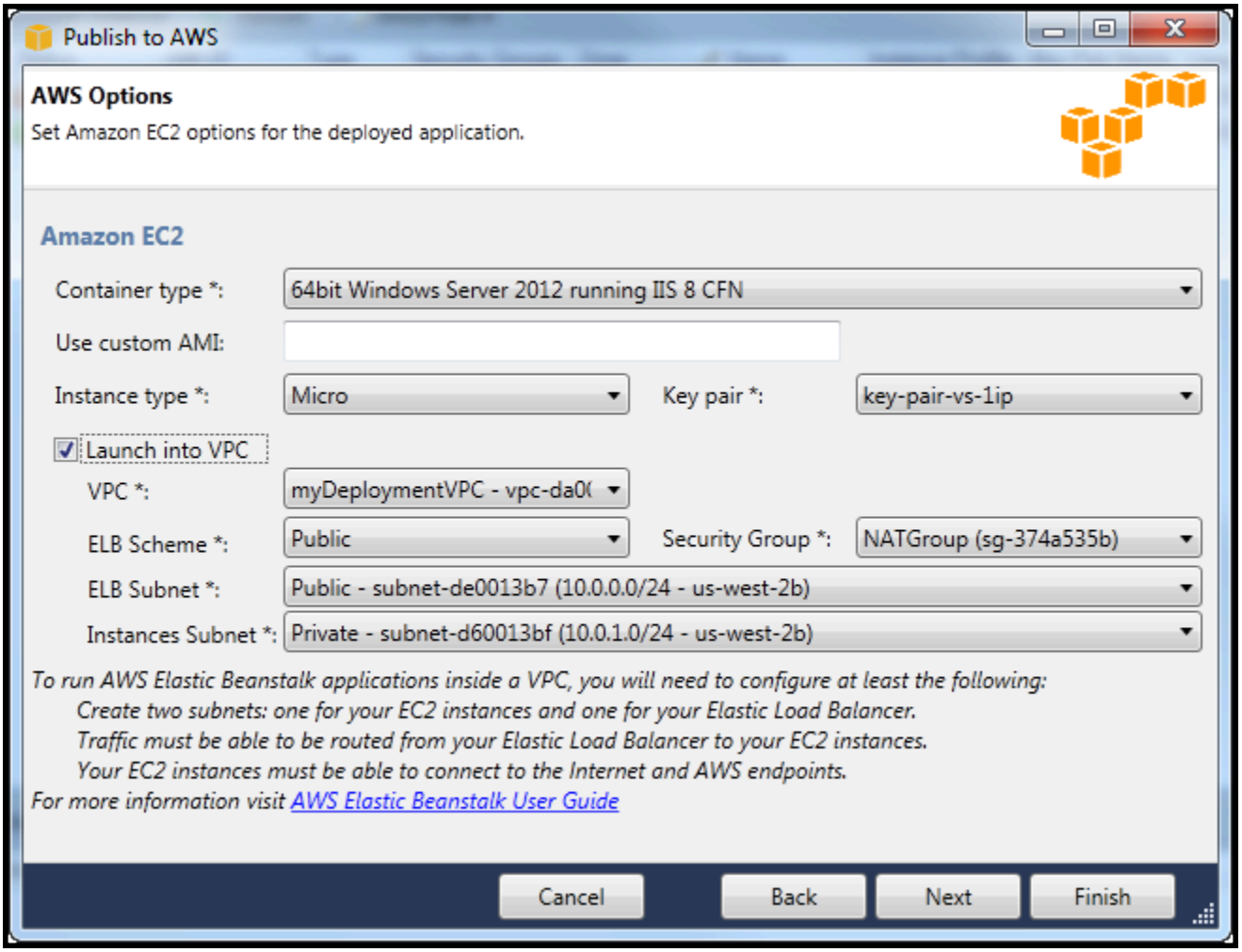
Ein Amazon Elastic Block Store (Amazon EBS) -Volume wird automatisch für die NAT-Instance erstellt. Weitere Informationen zu Amazon EBS finden Sie im Thema Amazon Elastic Block Store (EBS) im EC2 Amazon-Benutzerhandbuch für Linux-Instances.



Wenn Sie eine Anwendung in einer AWS Elastic Beanstalk Umgebung bereitstellen und sich dafür entscheiden, die Umgebung in einer VPC zu starten, füllt das Toolkit das Amazon Web Services Dialogfeld „Veröffentlichen in“ mit den Konfigurationsinformationen für Ihre VPC aus.

Das Toolkit füllt das Dialogfeld nur mit Informationen aus, die im Toolkit erstellt wurden VPCs , nicht mit Daten, die mit dem erstellt wurden. VPCs AWS Management Console Der Grund hierfür ist, dass das Toolkit beim Erstellen einer VPC die Komponenten der VPC mit Tags versieht, um auf ihre Daten zugreifen zu können.

Der folgende Screenshot vom Bereitstellungs-Assistenten zeigt ein Beispiel für ein Dialogfeld mit Werten von einer im Toolkit erstellten VPC.



So löschen Sie eine VPC

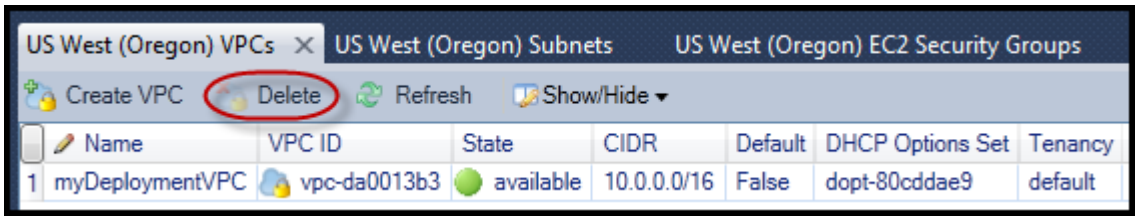
Um die VPC zu löschen, müssen Sie zunächst alle EC2 Amazon-Instances in der VPC beenden.

1. Wenn Sie eine Anwendung in einer AWS Elastic Beanstalk Umgebung in der VPC bereitgestellt haben, löschen Sie die Umgebung. Dadurch werden alle EC2 Amazon-Instances beendet, die Ihre Anwendung zusammen mit dem Elastic Load Balancing Load Balancer hosten.

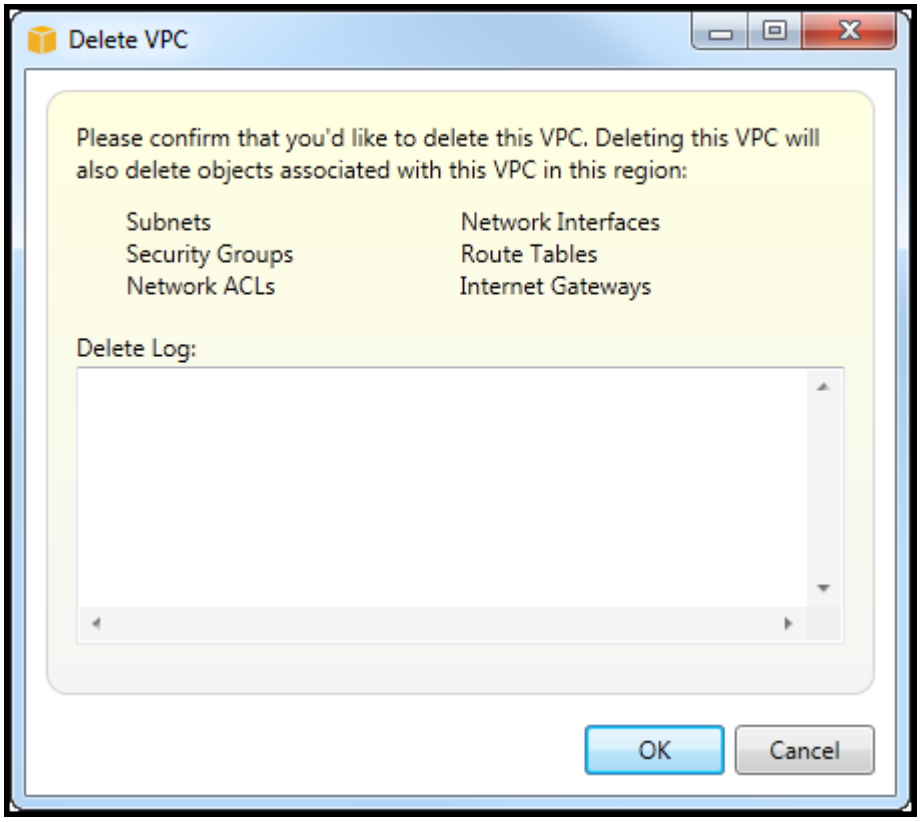
   Wenn Sie versuchen, die Instances, die Ihre Anwendung hosten, direkt zu beenden, ohne die Umgebung zu löschen, erstellt der Auto Scaling Scaling-Dienst automatisch neue Instances, um die gelöschten zu ersetzen. Weitere Informationen finden Sie im Auto Scaling Developer Guide.
2. Löschen Sie die NAT-Instance für die VPC.

   Sie müssen das Amazon EBS-Volume, das der NAT-Instance zugeordnet ist, nicht löschen, um die VPC zu löschen. Wenn Sie das Volume jedoch nicht löschen, wird es weiterhin in Rechnung gestellt, auch wenn Sie die NAT-Instance und die VPC gelöscht haben.

3. Wählen Sie auf der Registerkarte VPC den Link Delete (Löschen) aus, um die VPC zu löschen.



4. Wählen Sie im Dialogfeld Delete VPC (VPC löschen) die Option OK aus.



Verwenden des AWS CloudFormation Vorlageneditors für Visual Studio

Das Toolkit for Visual Studio umfasst einen AWS CloudFormation Vorlageneditor und AWS CloudFormation Vorlagenprojekte für Visual Studio. Zu den unterstützten Funktionen gehören.:

- Erstellen neuer Vorlagen (entweder leer oder aus einem vorhandenen Stapel oder einer Beispielvorlage kopiert) unter Verwendung des mitgelieferten AWS CloudFormation Vorlagenprojekttyps.

- Bearbeiten von Vorlagen mit automatischer JSON-Validierung, automatischer Vervollständigung, Code-Folding und Syntax-Hervorhebung.
- Automatisches Vorschlagen von intrinsischen Funktionen und Ressourcen-Referenzparametern für die Feldwerte in Ihrer Vorlage.
- Menüelemente zum Ausführen häufiger Aktionen für Ihre Vorlage in Visual Studio.

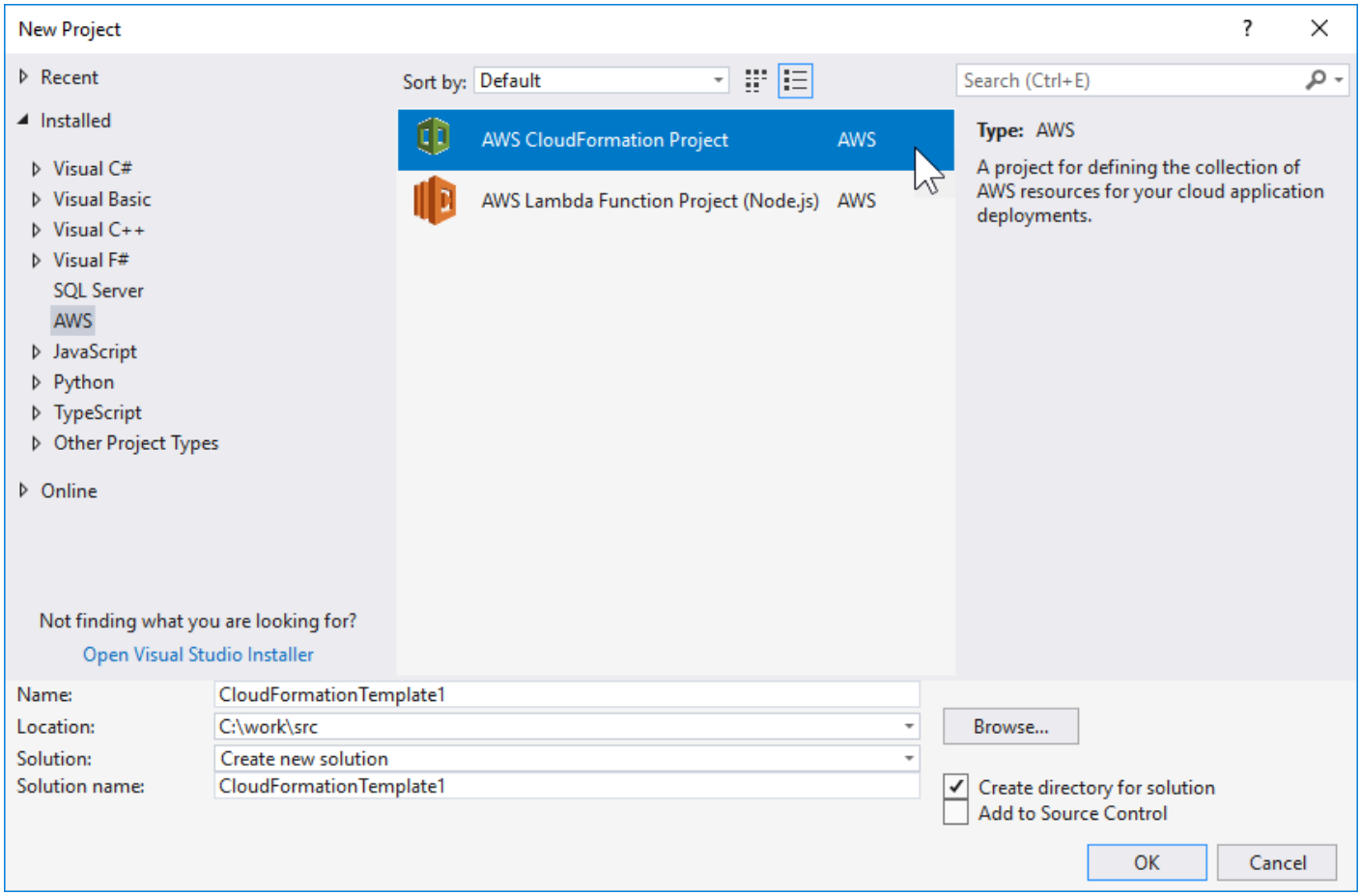
Themen

Erstellen eines AWS CloudFormation Vorlagenprojekts in Visual Studio

So erstellen Sie ein Vorlageprojekt:

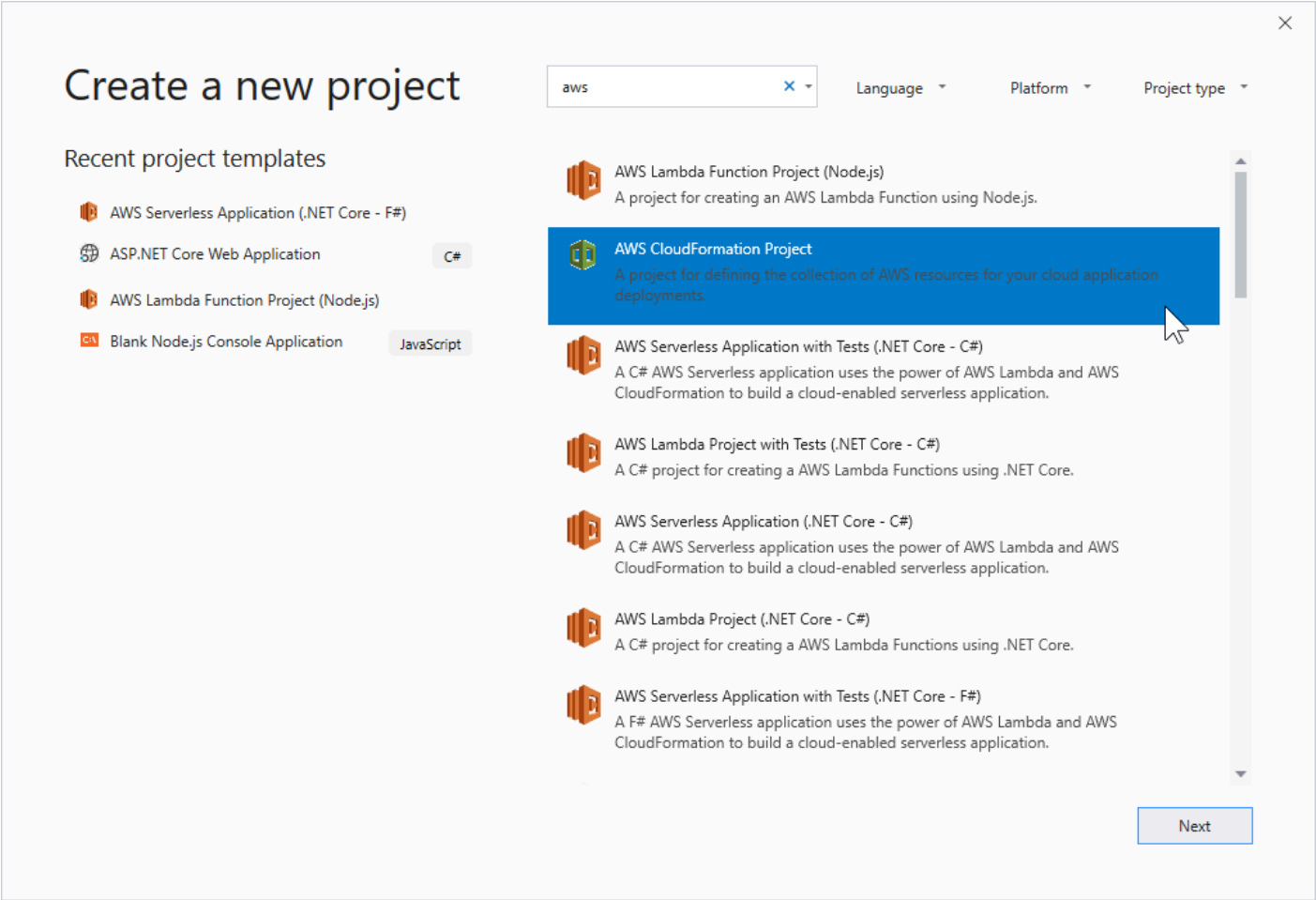
1. Wählen Sie in Visual Studio File (Datei), New (Neu) und dann Project (Projekt) aus.
2. Für Visual Studio 2017:

   Erweitern Sie im Dialogfeld Neues Projekt die Option Installiert und wählen Sie. AWS



Für Visual Studio 2019:

Stellen Sie im Dialogfeld New Project (Neues Projekt) sicher, dass die Dropdownfelder Language (Sprache), Platform (Plattform) und Project type (Projekttyp) auf „Alle...“ eingestellt sind, und geben Sie aws in das Feld Search (Suche) ein.



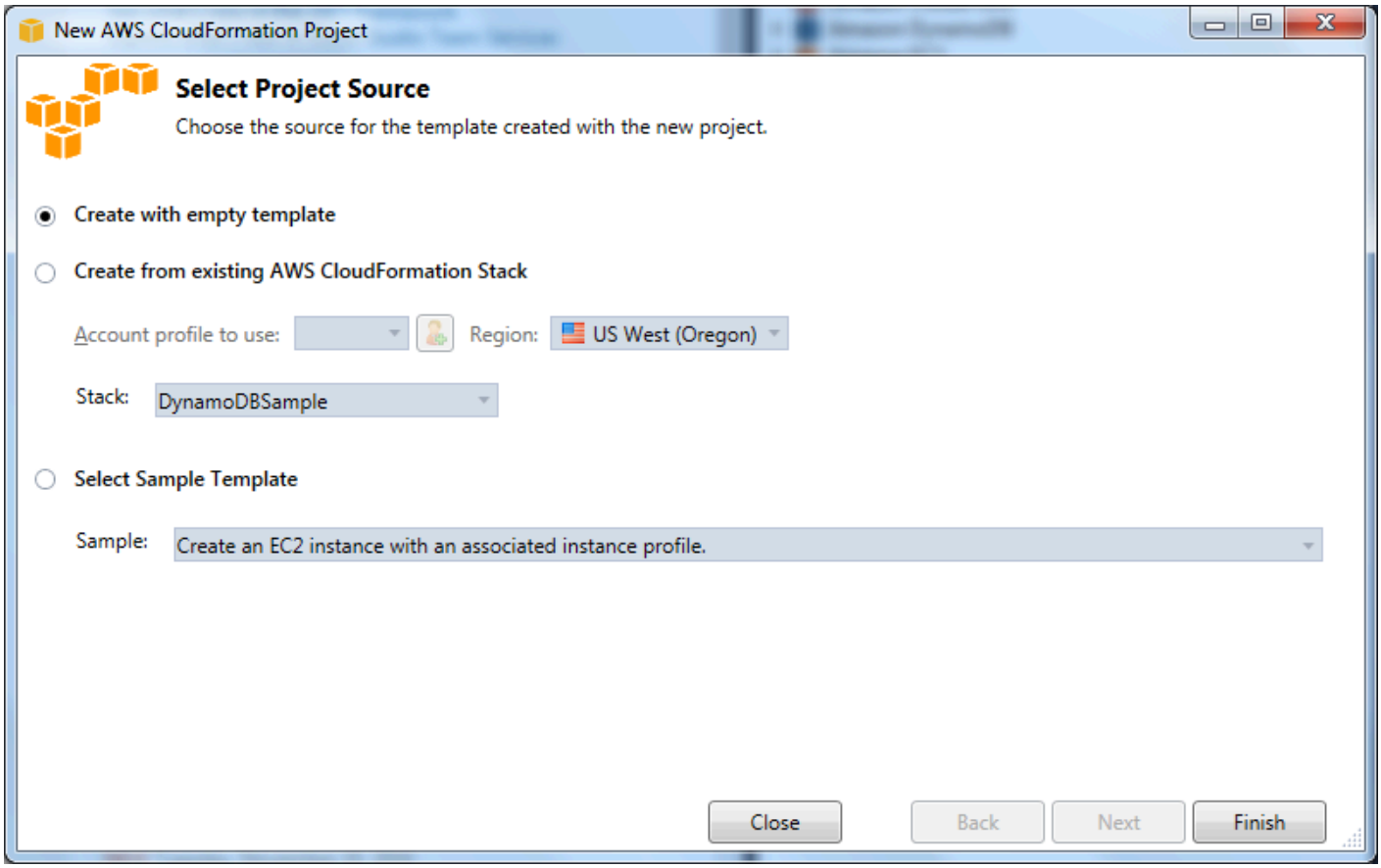
3. Wählen Sie die AWS CloudFormation Projektvorlage aus.
4. Für Visual Studio 2017:

   Geben Sie für Ihr Vorlagenprojekt Name, Location (Speicherort) usw. ein und klicken Sie dann auf OK.

   Für Visual Studio 2019:

   Klicken Sie auf Weiter. Geben Sie für Ihr Vorlagenprojekt im nächsten Dialogfeld Name, Location (Speicherort) usw. ein und klicken Sie dann auf Create (Erstellen).
5. Wählen Sie auf der Seite Select Project Source (Projektquelle auswählen) die Quelle für die zu erstellende Vorlage aus:
   - Mit Create with empty template (Mit leerer Vorlage erstellen) wird eine neue, leere AWS CloudFormation -Vorlage erzeugt.
   - Aus vorhandenem AWS |CFN|-Stack erstellen generiert eine Vorlage aus einem vorhandenen Stack in Ihrem Konto. AWS (Der Stack muss nicht den Status `CREATE_COMPLETE` aufweisen.)

- MitSelect sample template (Beispielvorlage auswählen) wird anhand einer der AWS CloudFormation -Beispielvorlagen eine Vorlage erzeugt.

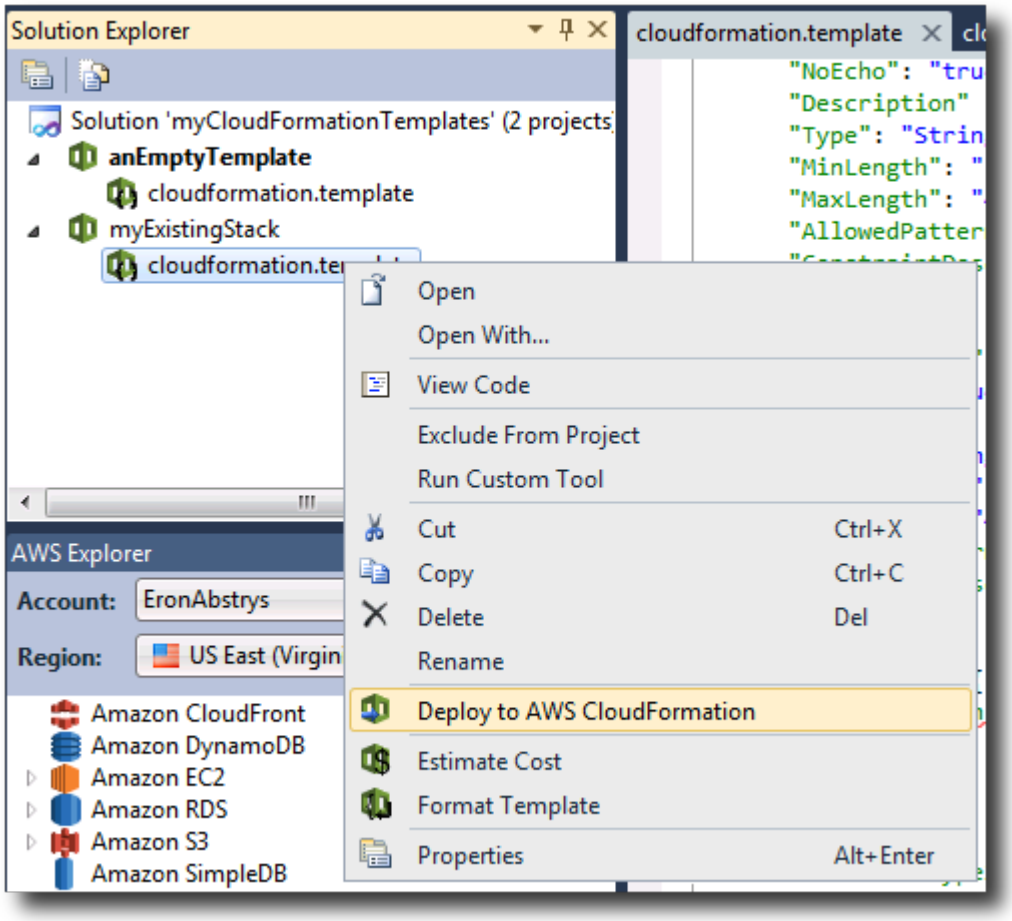


6. Um die Erstellung Ihres AWS CloudFormation Vorlagenprojekts abzuschließen, wählen Sie Fertig stellen.

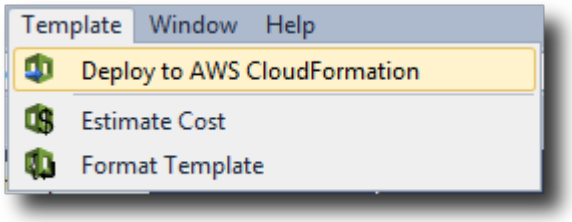
Bereitstellen einer AWS CloudFormation Vorlage in Visual Studio

So stellen Sie eine CFN-Vorlage bereit

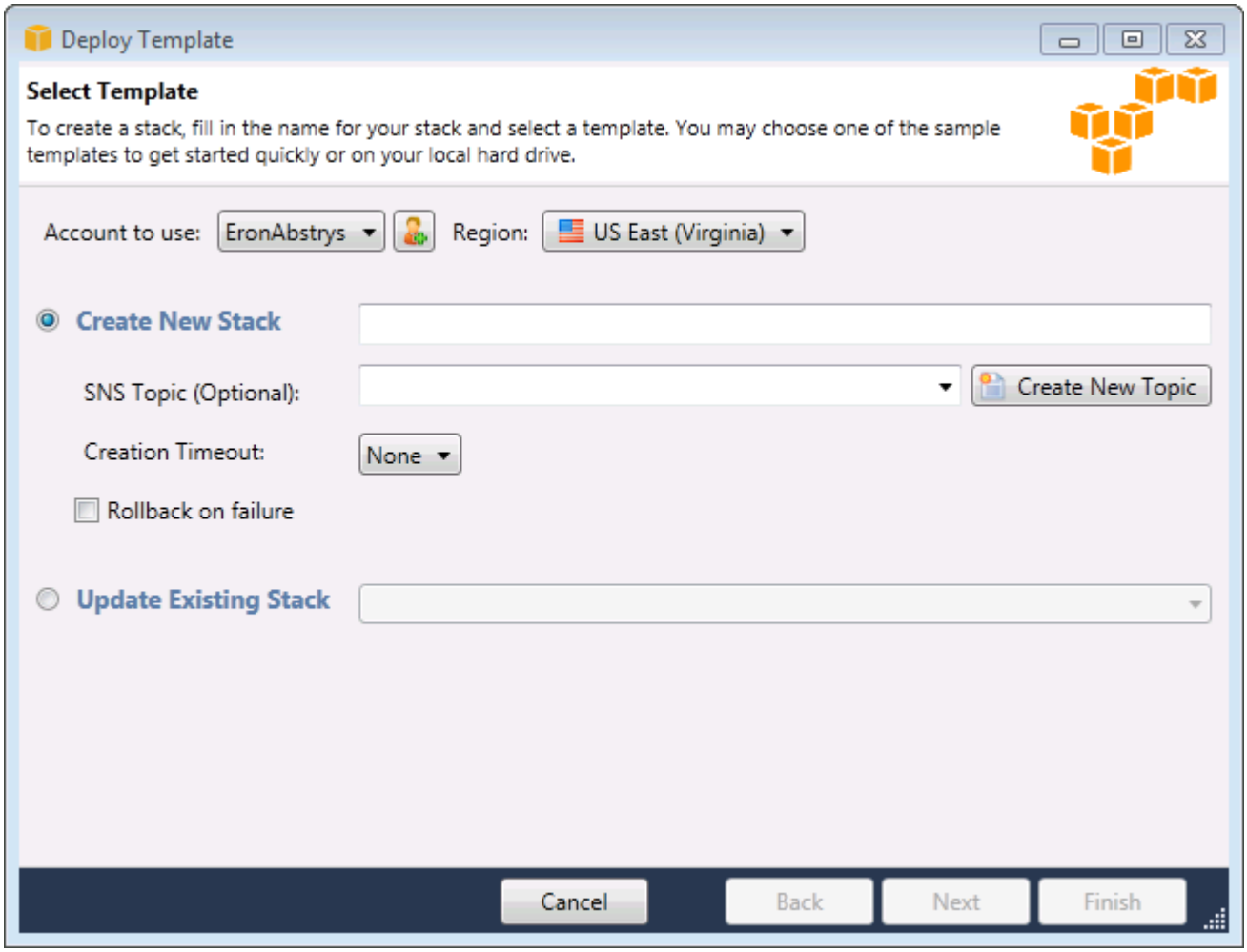
1. Öffnen Sie im Solution Explorer das Kontextmenü (mit der rechten Maustaste) für die Vorlage, die Sie bereitstellen möchten, und wählen Sie Bereitstellen für aus. AWS CloudFormation



Sie können die Vorlage, die Sie gerade bearbeiten, auch bereitstellen, indem Sie im Menü Vorlage die Option Bereitstellen für auswählen AWS CloudFormation.



2. Wählen Sie auf der Seite „Vorlage bereitstellen“ die AWS-Konto Option aus, mit der der Stack gestartet werden soll, und die Region, in der er gestartet werden soll.



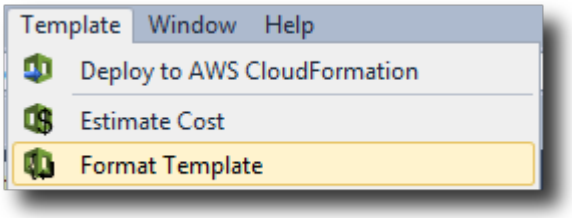
3. Wählen Sie Create New Stack (Neuen Stack erstellen) aus und geben Sie einen Namen für den Stack ein.
4. Wählen Sie beliebige der folgenden Optionen (oder keine) aus:
   - Um Benachrichtigungen über den Fortschritt des Stacks zu erhalten, wählen Sie in der Dropdown-Liste SNS Topic (SNS-Thema) ein SNS-Thema aus. Sie können auch ein SNS-Thema erstellen, indem Sie Create New Topic (Neues Thema erstellen) auswählen und im Feld eine E-Mail-Adresse eingeben.
   - Verwenden Sie Creation Timeout, um anzugeben, wie lange es dauern AWS CloudFormation soll, bis der Stack erstellt werden soll, bevor er für ausgefallen erklärt (und zurückgesetzt wird, sofern die Option Rollback bei Fehler nicht deaktiviert ist).
   - Verwenden Sie Rollback on failure (Rollback bei Fehler), wenn Sie möchten, dass der Stack bei fehlgeschlagener Erstellung rückgängig gemacht werden soll (Selbstlöschung). Lassen Sie diese Option deaktiviert, wenn der Stack für Debugging-Zwecke aktiv bleiben soll, auch wenn er nicht vollständig gestartet wurde.

5. Wählen Sie Finish (Abschließen) aus, um den Stack zu starten.

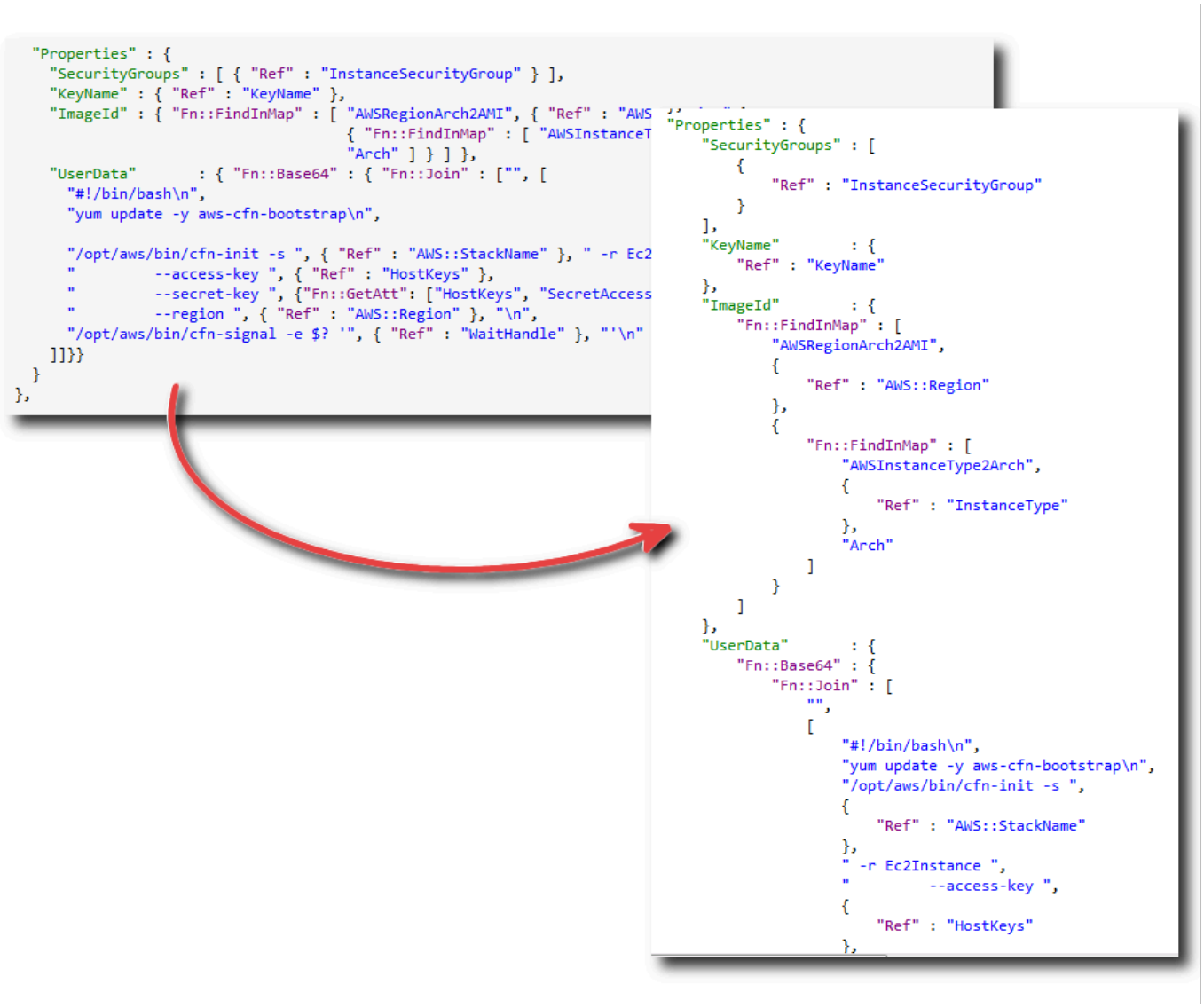
Formatieren einer AWS CloudFormation Vorlage in Visual Studio

- Öffnen Sie im Solution Explorer das Kontextmenü (rechte Maustaste) für die Vorlage und wählen Sie Format Template (Formatvorlage) aus.

  Alternativ können Sie die derzeit bearbeitete Vorlage formatieren, indem Sie im Menü Template (Vorlage) die Option Format Template (Formatvorlage) auswählen.



  Ihr JSON-Code wird formatiert, sodass die Struktur deutlich dargestellt wird.



Amazon S3 vom AWS Explorer aus verwenden

Mit Amazon Simple Storage Service (Amazon S3) können Sie Daten von jeder Verbindung zum Internet speichern und abrufen. Alle Daten, die Sie auf Amazon S3 speichern, sind mit Ihrem Konto verknüpft und können standardmäßig nur von Ihnen abgerufen werden. Das Toolkit for Visual Studio ermöglicht es Ihnen, Daten auf Amazon S3 zu speichern und diese Daten anzuzeigen, zu verwalten, abzurufen und zu verteilen.

Amazon S3 verwendet das Konzept von Buckets, das Sie sich ähnlich wie Dateisysteme oder logische Laufwerke vorstellen können. Buckets können Ordner enthalten, ähnlich Verzeichnissen, und Objekte, ähnlich Dateien. In diesem Abschnitt verwenden wir diese Konzepte, während wir uns die Amazon S3 S3-Funktionalität ansehen, die durch das Toolkit for Visual Studio bereitgestellt wird.

> **Note**
>
> Um dieses Tool verwenden zu können, muss Ihre IAM-Richtlinie Berechtigungen für die Aktionen `s3:GetBucketAcls3:GetBucket`, und `s3:ListBucket` gewähren. Weitere Informationen finden Sie unter Überblick über die AWS IAM-Richtlinien.

Erstellen eines Amazon-S3-Buckets

Der Bucket ist die grundlegendste Speichereinheit in Amazon S3.

So erstellen Sie einen S3-Bucket

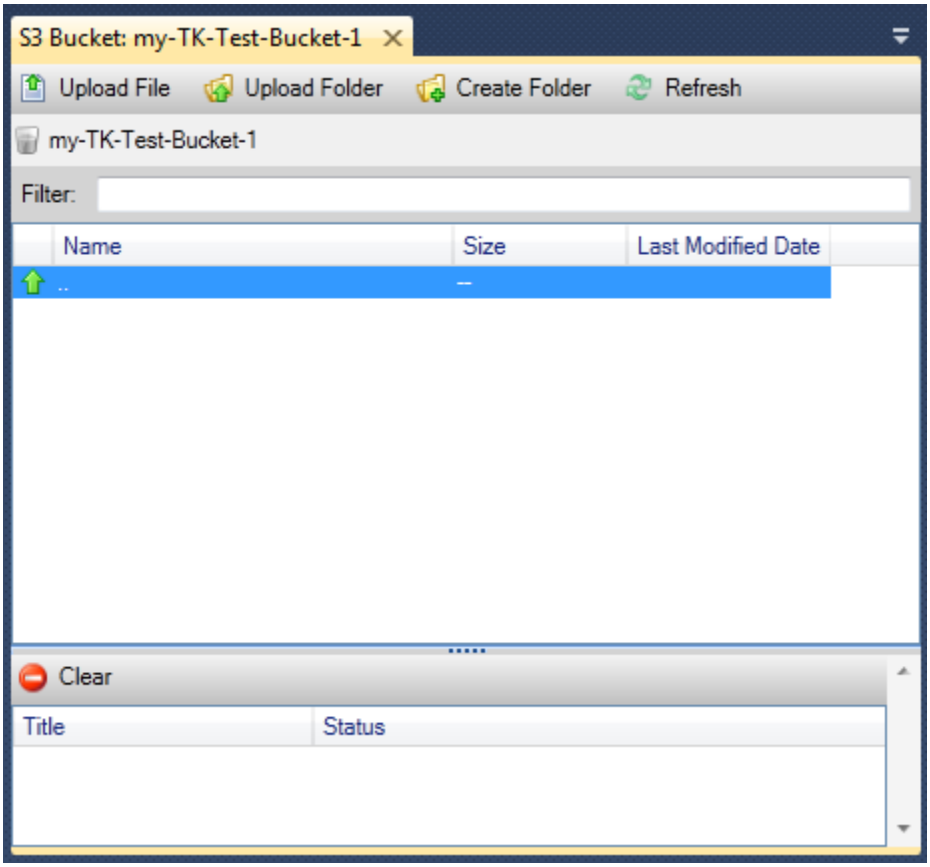
1. Öffnen Sie im AWS Explorer das Kontextmenü (Rechtsklick) für den Amazon S3 S3-Node und wählen Sie dann Create Bucket aus.
2. Geben Sie im Dialogfeld Create Bucket (Bucket erstellen) einen Namen für den Bucket ein. Bucket-Namen müssen überall eindeutig sein AWS. Informationen zu weiteren Einschränkungen finden Sie in der Amazon S3-Dokumentation.
3. Wählen Sie OK aus.

Amazon S3 S3-Buckets vom Explorer aus AWS verwalten

Im AWS Explorer sind die folgenden Operationen verfügbar, wenn Sie ein Kontextmenü (Rechtsklick) für einen Amazon S3 S3-Bucket öffnen.

Durchsuchen

Zeigt die Objekte im Bucket an. Hier können Sie Ordner erstellen oder Dateien bzw. gesamte Verzeichnisse und Ordner von Ihrem lokalen Computer hochladen. Im unteren Bereich werden Statusmeldungen zum Upload-Vorgang angezeigt. Um diese Nachrichten zu löschen, wählen Sie das Symbol Clear (Löschen) aus. Sie können auf diese Ansicht des Buckets auch zugreifen, indem Sie im AWS Explorer auf den Bucket-Namen doppelklicken.



Eigenschaften

Zeigt ein Dialogfeld an, in dem Sie die folgende Möglichkeiten haben:

- Legen Sie Amazon S3 S3-Berechtigungen mit folgendem Gültigkeitsbereich fest:
  - Sie als Bucket-Eigentümer
  - alle Benutzer, die authentifiziert wurden. AWS
  - Alle Benutzer mit Zugriff auf das Internet
- Aktivieren der Protokollierung für den Bucket
- Richten Sie mithilfe des Amazon Simple Notification Service (Amazon SNS) eine Benachrichtigung ein, sodass Sie, wenn Sie Reduced Redundancy Storage (RRS) verwenden, bei Datenverlust benachrichtigt werden. RRS ist eine Amazon S3 S3-Speicheroption, die weniger Haltbarkeit als Standardspeicher bietet, jedoch zu geringeren Kosten. Weitere Informationen finden Sie unter S3 FAQs.
- Erstellen einer statischen Webseite mithilfe von Daten im Bucket

Richtlinie

Ermöglicht das Einrichten von AWS Identity and Access Management (IAM-) Richtlinien für Ihren Bucket. Weitere Informationen finden Sie in der IAM-Dokumentation und den Anwendungsfällen für IAM und S3.

Vorsignierte URL erstellen

Ermöglicht das Generieren einer zeitlich begrenzten URL, über die Sie den Zugriff auf den Inhalt des Buckets gewähren können. Weitere Informationen finden Sie unter How to Create a Pre-Signed URL.

View Multi-Part Uploads

Ermöglicht es Ihnen, mehrteilige Uploads anzuzeigen. Amazon S3 unterstützt die Aufteilung großer Objekt-Uploads in Teile, um den Upload-Prozess effizienter zu gestalten. Weitere Informationen finden Sie in der Erläuterung von mehrteiligen Uploads in der S3-Dokumentation.

Löschen

Ermöglicht das Löschen des Buckets. Sie können nur leere Buckets löschen.

Dateien und Ordner auf Amazon S3 hochladen

Sie können den AWS Explorer verwenden, um Dateien oder ganze Ordner von Ihrem lokalen Computer in einen Ihrer Buckets zu übertragen.

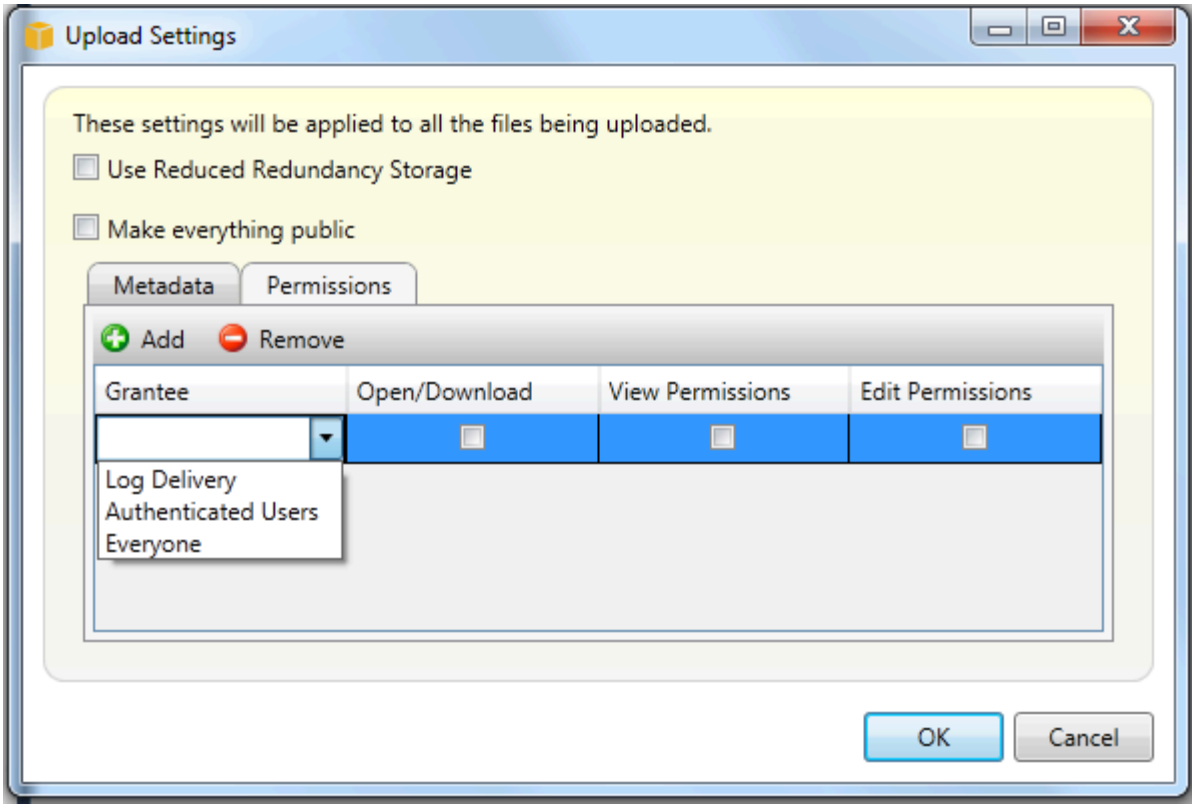
> **Note**
>
> Wenn Sie Dateien oder Ordner hochladen, die denselben Namen haben wie Dateien oder Ordner, die bereits im Amazon S3 S3-Bucket existieren, überschreiben Ihre hochgeladenen Dateien die vorhandenen Dateien ohne Warnung.

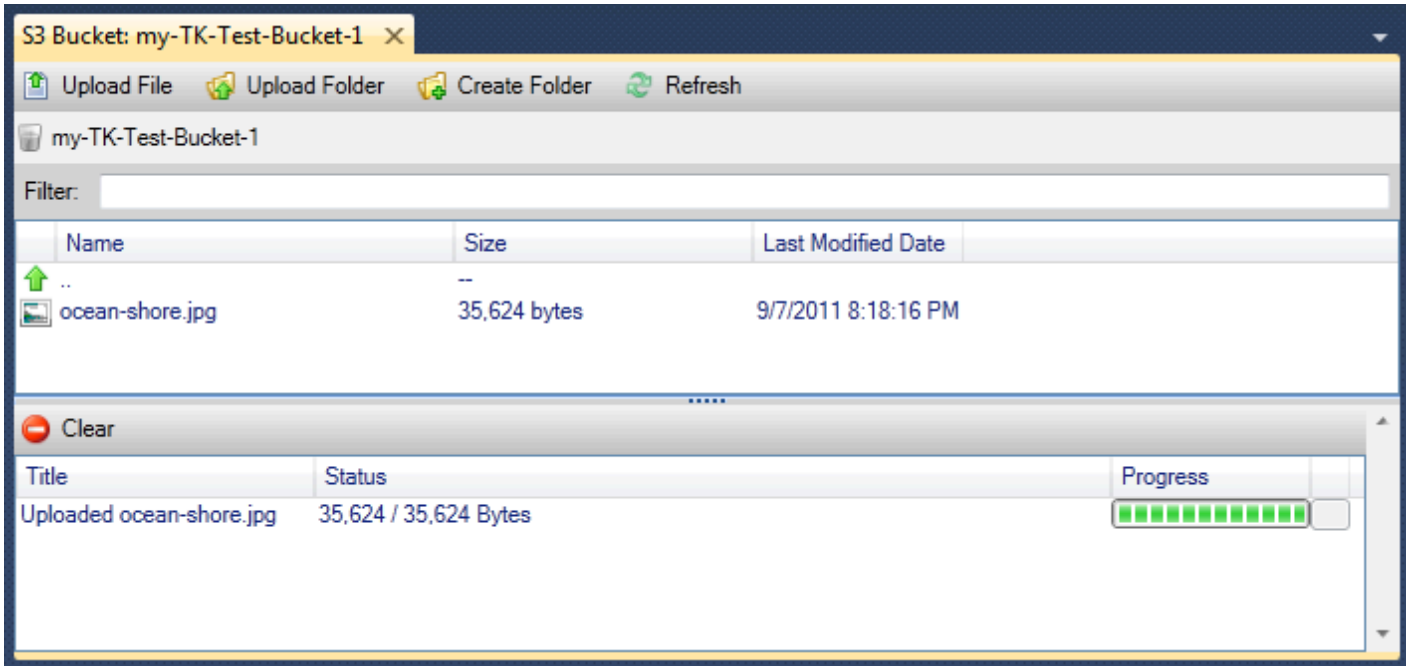
Laden Sie wie folgt eine Datei nach S3 hoch:

1. Erweitern Sie im AWS Explorer den Amazon S3 S3-Knoten und doppelklicken Sie auf einen Bucket oder öffnen Sie das Kontextmenü (Rechtsklick) für den Bucket und wählen Sie Durchsuchen.
2. Wählen Sie in der Browse (Duchsuchen)-Ansicht Ihres Buckets Upload File (Datei hochladen) oder Upload Folder (Ordner hochladen) aus.

3. Navigieren Sie im Dialogfeld File-Open (Dateiöffenen)) zu den Dateien, die Sie hochladen möchten, und wählen Sie dann Open (Öffnen)) aus. Wenn Sie einen Ordner hochladen möchten, navigieren Sie zu ihm und wählen ihn aus und klicken Sie dann auf Open (Öffnen).

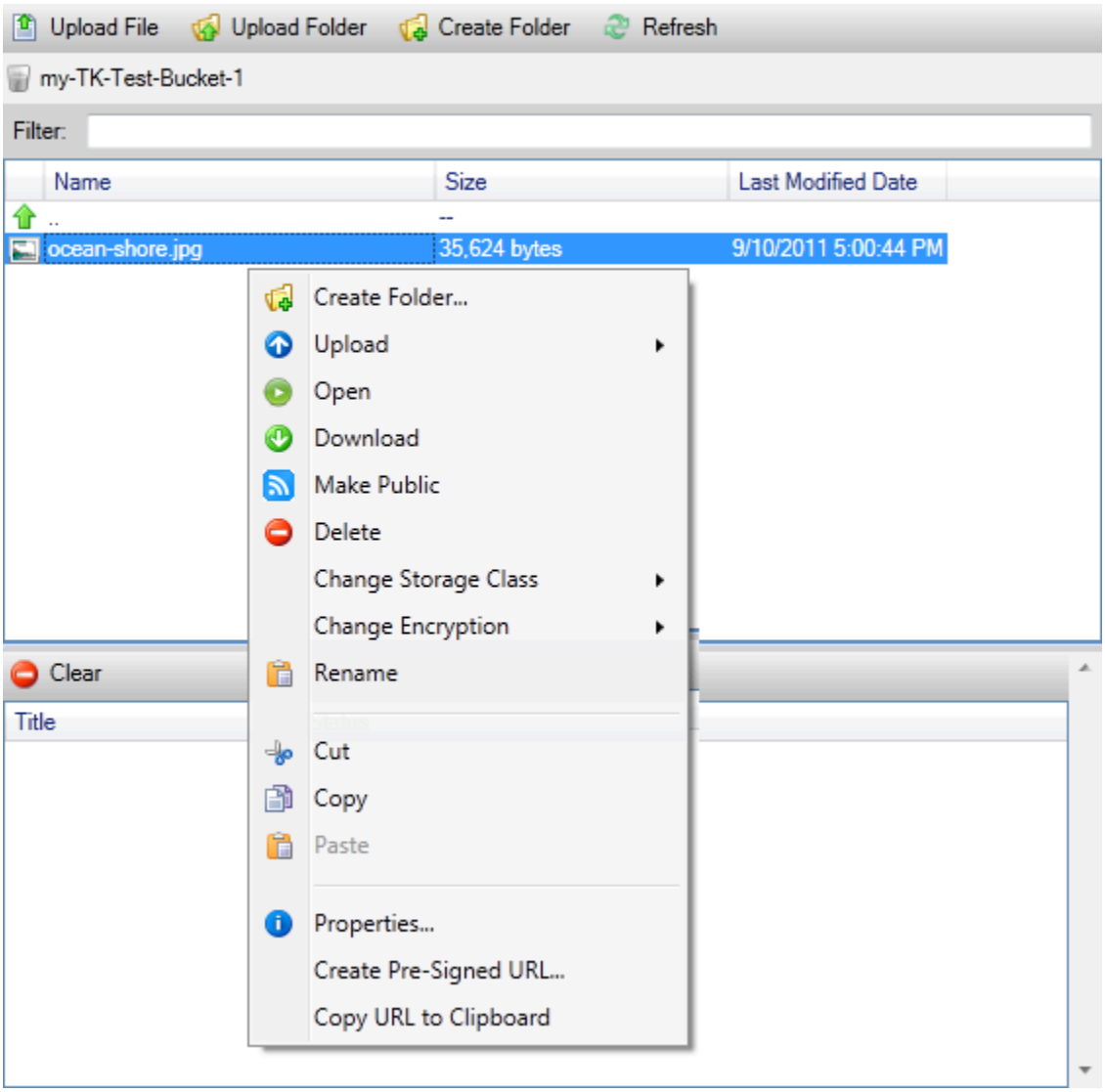
   Im Dialogfeld Upload Settings (Upload-Einstellungen) können Sie Metadaten und Berechtigungen für die Dateien oder Ordner, die Sie hochladen, festlegen. Das Aktivieren des Kontrollkästchens Make everything public (Alles als öffentlich festlegen) entspricht dem festlegen der Berechtigungen Open/Download (Öffnen/Herunterladen) auf Everyone (Jeder). Sie können die Option aktivieren, um Reduced Redundancy Storage für die hochgeladenen Dateien zu nutzen.





Amazon S3 S3-Dateioperationen aus dem AWS Toolkit for Visual Studio

Wenn Sie eine Datei in der Amazon S3 S3-Ansicht auswählen und das Kontextmenü (Rechtsklick) öffnen, können Sie verschiedene Operationen an der Datei ausführen.



Ordner erstellen

Ermöglicht das Erstellen eines Ordners im aktuellen Bucket. (Entspricht dem Auswählen des Links Create Folder (Ordner erstellen).)

Hochladen

Ermöglicht das Hochladen von Dateien oder Ordnern. (Entspricht dem Auswählen der Links Upload File (Datei hochladen) bzw. Upload Folder (Ordner hochladen).)

Öffnen

Versucht, die ausgewählte Datei in Ihrem Standard-Browser zu öffnen. Abhängig vom Dateityp und den Funktionen Ihres Standard-Browsers kann die Datei möglicherweise nicht angezeigt werden. In diesem Fall wird sie einfach von Ihrem Browser heruntergeladen.

Download

Öffnet ein Folder-Tree (Ordnerstruktur)-Dialogfeld zum Herunterladen der ausgewählten Datei.

Veröffentlichen

Legt Berechtigungen für die ausgewählte Datei auf Open/Download (Öffnen/Herunterladen) und Everyone (Jeder) fest. (Entspricht dem Aktivieren des Kontrollkästchens Make everything public (Alles als öffentlich festlegen) im Dialogfeld Upload Settings (Upload-Einstellungen).)

Löschen

Löscht die ausgewählten Dateien oder Ordner. Sie können Dateien oder Ordner auch löschen, indem Sie sie auswählen und `Delete` drücken.

Speicherklasse ändern

Legt die Speicherklasse auf Standard oder Reduced Redundancy Storage (RRS) fest. Um die aktuelle Einstellung für die Speicherklasse anzuzeigen, wählen Sie Properties (Eigenschaften) aus.

Verschlüsselung ändern

Ermöglicht das Festlegen der serverseitigen Verschlüsselung für die Datei. Um die aktuelle Einstellung für Verschlüsselung anzuzeigen, wählen Sie Properties (Eigenschaften) aus.

Umbenennen

Ermöglicht das Umbenennen einer Datei. Ordner können nicht umbenannt werden.

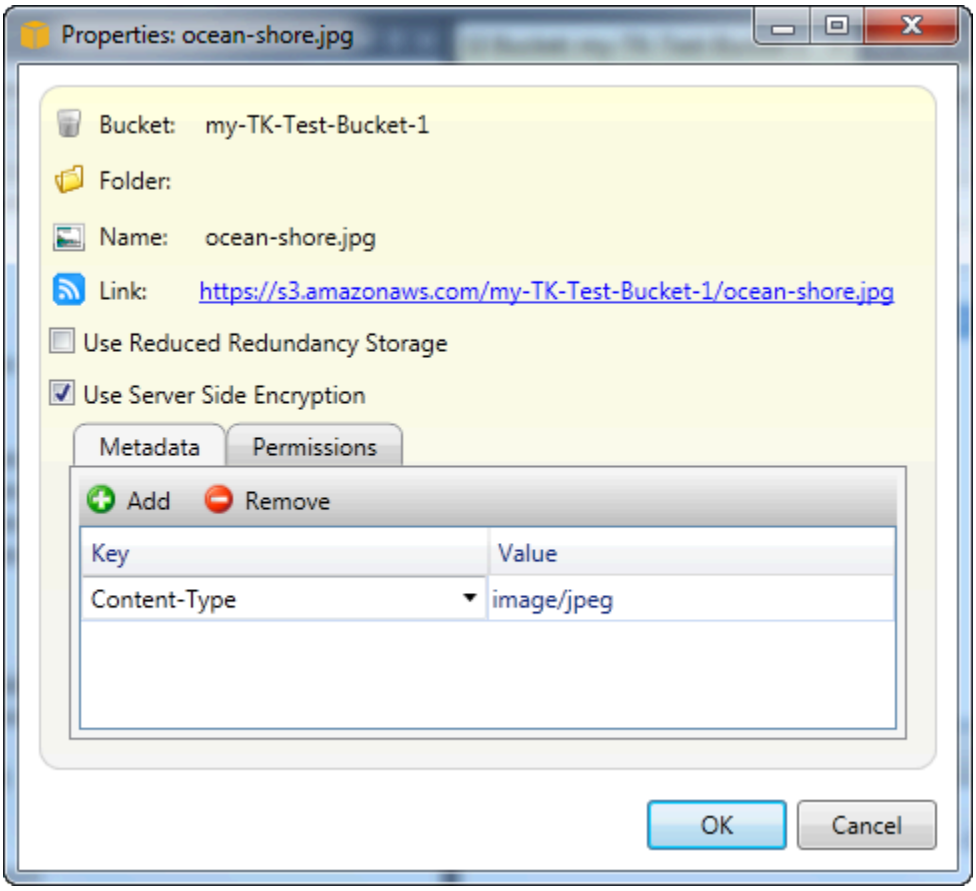
Ausschneiden | Kopieren | Einfügen

Ermöglicht das Ausschneiden, Kopieren und Einfügen von Dateien oder Ordnern zwischen Ordnern oder Buckets.

Eigenschaften

Zeigt ein Dialogfeld an, in dem Sie Metadaten und Berechtigungen für die Datei festlegen und den Speicher für die Datei zwischen Reduced Redundancy Storage (RRS) und Standard umschalten können. Außerdem können Sie serverseitige Verschlüsselung für die Datei festlegen. In diesem Dialogfeld wird außerdem ein HTTPS-Link zu der Datei angezeigt. Wenn Sie diesen Link wählen,

öffnet das Toolkit for Visual Studio die Datei in Ihrem Standardbrowser. Wenn die Berechtigungen Open/Download und Everyone (Jeder) für die Datei festgelegt wurden, können andere Benutzer über diesen Link auf die Datei zugreifen. Anstatt diesen Link zu verteilen, empfehlen wir Ihnen, URLs vorsignierte Links zu erstellen und zu verteilen.



Vorsignierte URL erstellen

Ermöglicht es Ihnen, eine zeitlich begrenzte, vorsignierte URL zu erstellen, die Sie verteilen können, damit andere Personen auf die Inhalte zugreifen können, die Sie auf Amazon S3 gespeichert haben.

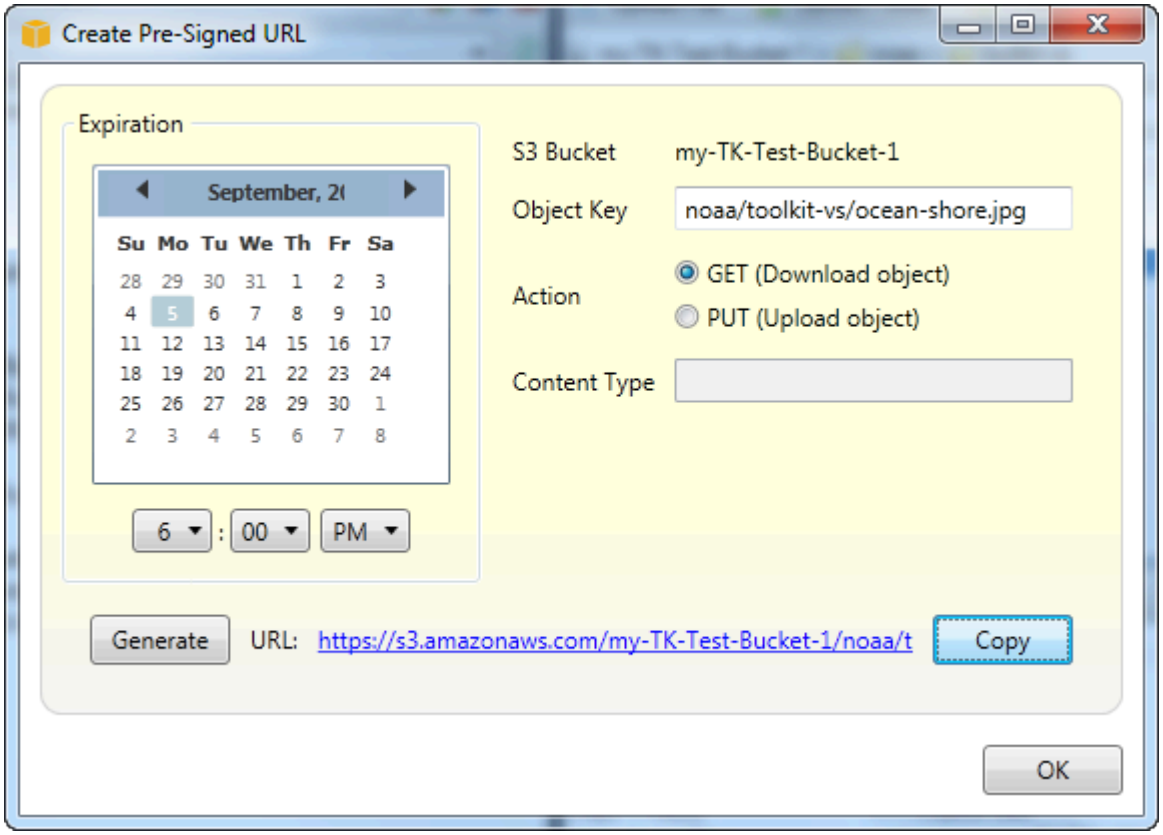
Erstellen einer vorsignierten URL

Sie können eine vorsignierte URL für einen Bucket oder Dateien in einem Bucket erstellen. Andere Personen können diese URL dann verwenden, um auf den Bucket oder die Datei zuzugreifen. Die URL läuft nach einem bestimmten Zeitraum ab, den Sie beim Erstellen der URL angeben.

So erstellen Sie eine vorsignierte URL

1. Legen Sie im Dialogfeld Create Pre-Signed URL (Vorsignierte URL erstellen) Ablaufdatum und -uhrzeit für die URL fest. Die Standardeinstellung ist eine Stunde nach dem aktuellen Zeitpunkt.

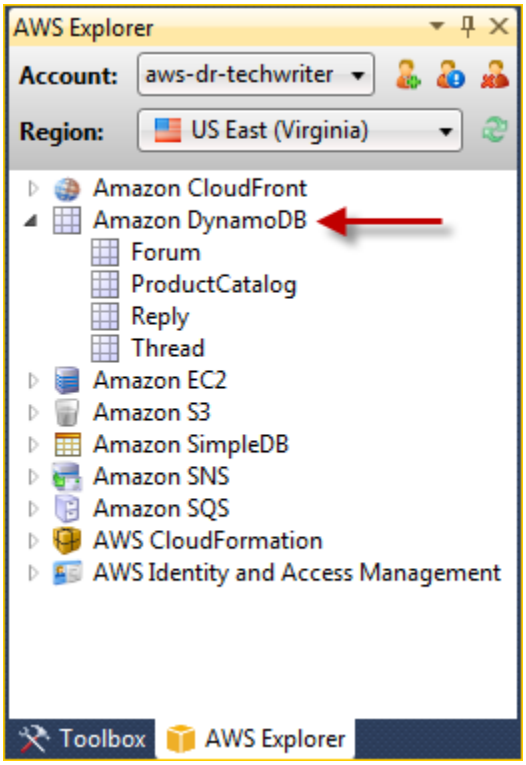
2. Wählen Sie die Schaltfläche Generate (Generieren) aus.
3. Wählen Sie zum Kopieren der URL in die Zwischenablage Copy (Kopieren) aus.



DynamoDB vom Explorer aus verwenden AWS

Amazon DynamoDB ist ein schneller, hochskalierbarer, hochverfügbarer, wirtschaftlicher, nicht relationaler Datenbank-Service. Mit DynamoDB werden Einschränkungen der Skalierbarkeit des Datenspeichers eliminiert, die Latenz wird niedrig gehalten und die Leistung ist vorhersehbar. Das Toolkit for Visual Studio bietet Funktionen für die Arbeit mit DynamoDB in einem Entwicklungskontext. Weitere Informationen zu DynamoDB finden Sie unter DynamoDB auf der Amazon Web Services Services-Website.

Im Toolkit for Visual Studio zeigt AWS Explorer alle DynamoDB-Tabellen an, die mit den aktiven Tabellen verknüpft sind. AWS-Konto



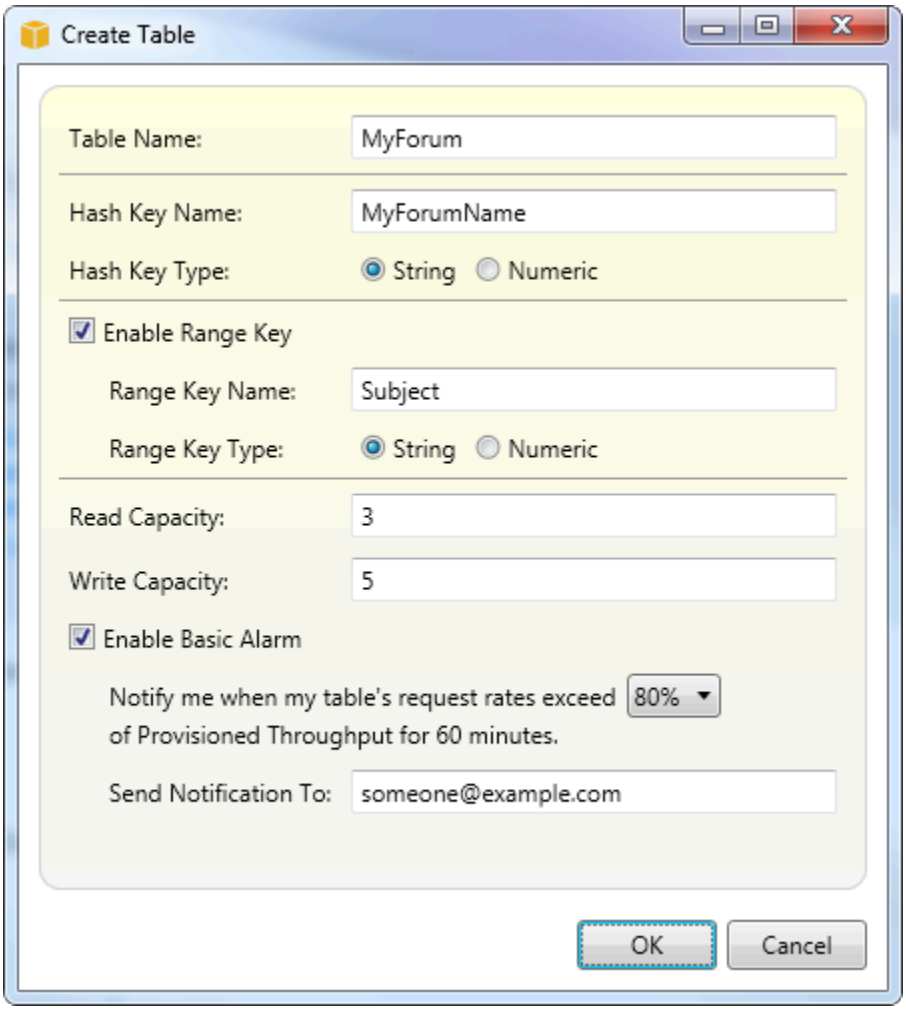
Eine DynamoDB-Tabelle erstellen

Sie können das Toolkit for Visual Studio verwenden, um eine DynamoDB-Tabelle zu erstellen.

Um eine Tabelle im Explorer zu erstellen AWS

1. Öffnen Sie im AWS Explorer das Kontextmenü (Rechtsklick) für Amazon DynamoDB und wählen Sie dann Tabelle erstellen.
2. Geben Sie im Create Table (Tabelle erstellen)-Assistenten unter Table Name (Tabellenname)einen Namen für die Tabelle ein.
3. Geben Sie im Feld Hash-Schlüsselname ein primäres Hash-Schlüsselattribut ein und wählen Sie über die Schaltflächen Hash-Schlüsseltyp den Hash-Schlüsseltyp aus. DynamoDB erstellt einen ungeordneten Hash-Index unter Verwendung des Primärschlüsselattributs und einen optionalen sortierten Bereichsindex unter Verwendung des Bereichs-Primärschlüsselattributs. Weitere Informationen zum primären Hash-Schlüsselattribut finden Sie im Abschnitt Primärschlüssel im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.
4. (Optional) Wählen Sie Enable Range Key (Bereichsschlüssel aktivieren) aus. Geben Sie im Feld Range Key Name (Bereichsschlüsselname) ein Bereichsschlüsselattribut ein und wählen Sie aus den Range Key Type (Bereichsschlüsseltyp)-Schaltflächen einen Bereichsschlüsseltyp aus.

5. Geben Sie im Feld Read Capacity (Lesekapazität) die Anzahl an Lesekapazitätseinheiten ein. Geben Sie im Feld Write Capacity (Schreibkapazität) die Anzahl an Schreibkapazitätseinheiten ein. Sie müssen mindestens 3 Lesekapazitätseinheiten und 5 Schreibkapazitätseinheiten angeben. Weiter Informationen über Lese- und Schreibkapazitätseinheiten finden Sie unter Provisioned Throughput in DynamoDB (In DynamoDB bereitgestellter Durchsatz).
6. (Optional) Wählen Sie Enable Basic Alarm (Basisalarm aktivieren) aus, um benachrichtigt zu werden, sobald die Anforderungsraten der Tabelle zu hoch werden. Wählen Sie den Prozentsatz des bereitgestellten Durchsatzes pro 60 Minuten aus, der überschritten werden muss, bevor die Warnung gesendet wird. Geben Sie in Send Notifications To (Benachrichtungen senden an) eine E-Mail-Adresse ein.
7. Klicken Sie auf OK, um die Tabelle zu erstellen.

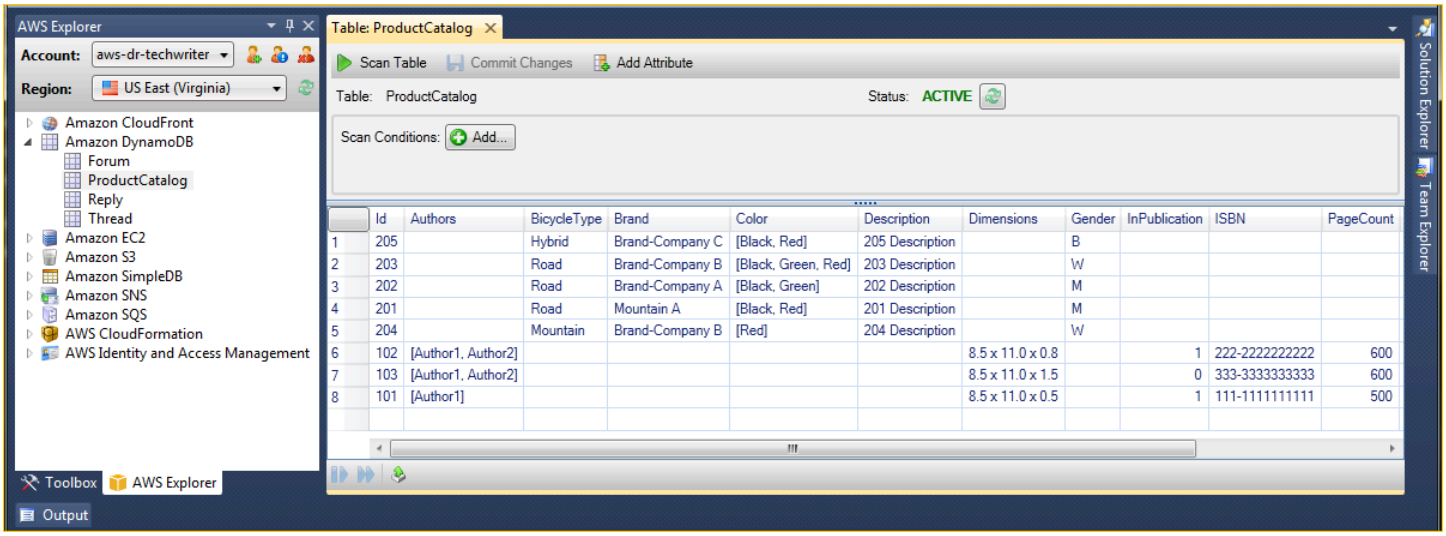


Weitere Informationen zu DynamoDB-Tabellen finden Sie unter Datenmodellkonzepte — Tabellen, Elemente und Attribute.

DynamoDB-Tabelle als Grid anzeigen

Um eine Grid-Ansicht einer Ihrer DynamoDB-Tabellen zu öffnen, doppelklicken Sie im AWS Explorer auf den Unterknoten, der der Tabelle entspricht. In der Rasteransicht können Sie die in der Tabelle gespeicherten Elemente, Attribute und Werte sehen. Jede Zeile entspricht einem Element in der Tabelle. Die Tabellenspalten entsprechen Attributen. Jede Zelle der Tabelle enthält die mit diesem Elementattribut verknüpften Werte.

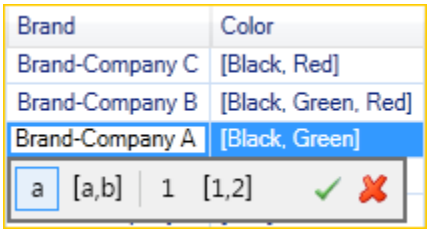
Der Wert eines Attributs kann eine Zeichenfolge oder eine Zahl sein. Manche Attribute verfügen über einen Wert, der aus einem Satz von Zeichenfolgen oder Zahlen besteht. Satzwerte werden als eine durch Komma getrennte Liste in eckigen Klammern angezeigt.



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

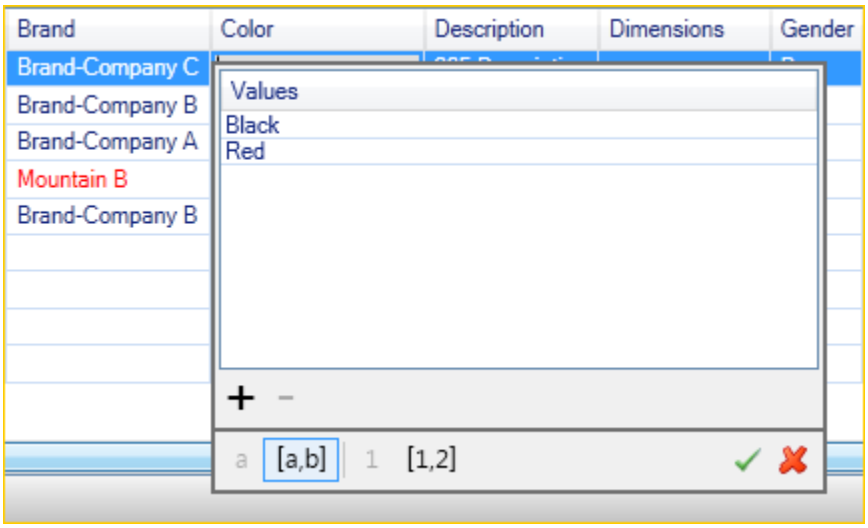
Bearbeiten und Hinzufügen von Attributen und Werten

Sie können die Werte für das entsprechende Attribut eines Elements bearbeiten, indem Sie auf eine Zelle doppelklicken. Bei Satzwertattributen können Sie auch einzelne Werte des Satzes hinzufügen oder löschen.



Sie haben nicht nur die Möglichkeit, den Wert eines Attributs zu ändern, sondern—mit einigen Einschränkungen—auch das Format des Attributwerts. Beispielsweise kann ein beliebiger Zahlenwert in eine Zeichenfolge umgewandelt werden. Bei einem Zeichenfolgenwert, dessen Inhalt eine Zahl

ist, z. B. 125, haben Sie mit der Zelleneditor die Möglichkeit, das Format des Werts von Zeichen in Zahlen umzuwandeln. Sie können auch einen Einzelwert in einen Satzwert konvertieren. In der Regel können Sie jedoch keine Umwandlungen von einem Satzwert in eine Einzelwert vornehmen, ausgenommen, der Satzwert besteht aus nur einem Element.

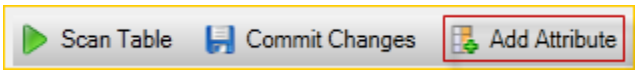


Wählen Sie nach dem Bearbeiten des Attributwerts das grüne Häkchen, um Ihre Änderungen zu bestätigen. Wenn Sie die Änderungen verwerfen möchten, wählen Sie das rote X.

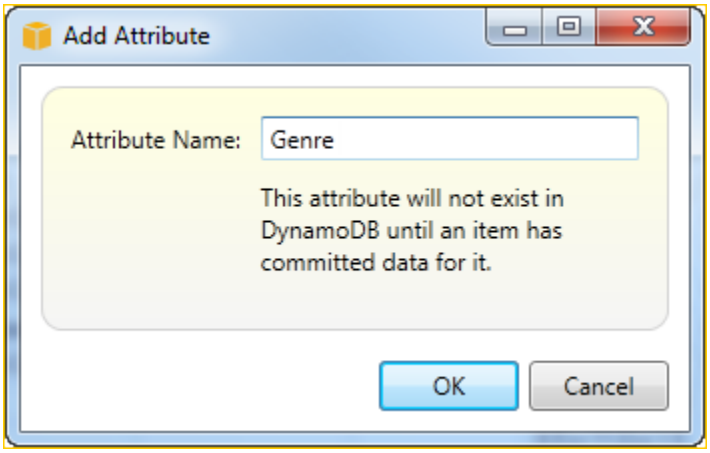
Nachdem Sie Ihre Änderungen bestätigt haben, wird der Attributwert rot angezeigt. Dies bedeutet, dass das Attribut aktualisiert wurde, der neue Wert jedoch nicht in die DynamoDB-Datenbank zurückgeschrieben wurde. Um Ihre Änderungen zurück in DynamoDB zu schreiben, wählen Sie Commit Changes. Um Ihre Änderungen zu verwerfen, wählen Sie Scan Table (Tabelle scannen) und wenn Sie vom Toolkit gefragt werden, ob Sie die Änderungen vor dem Scannen speichern möchten, wählen Sie No (Nein).

Hinzufügen eines Attributs

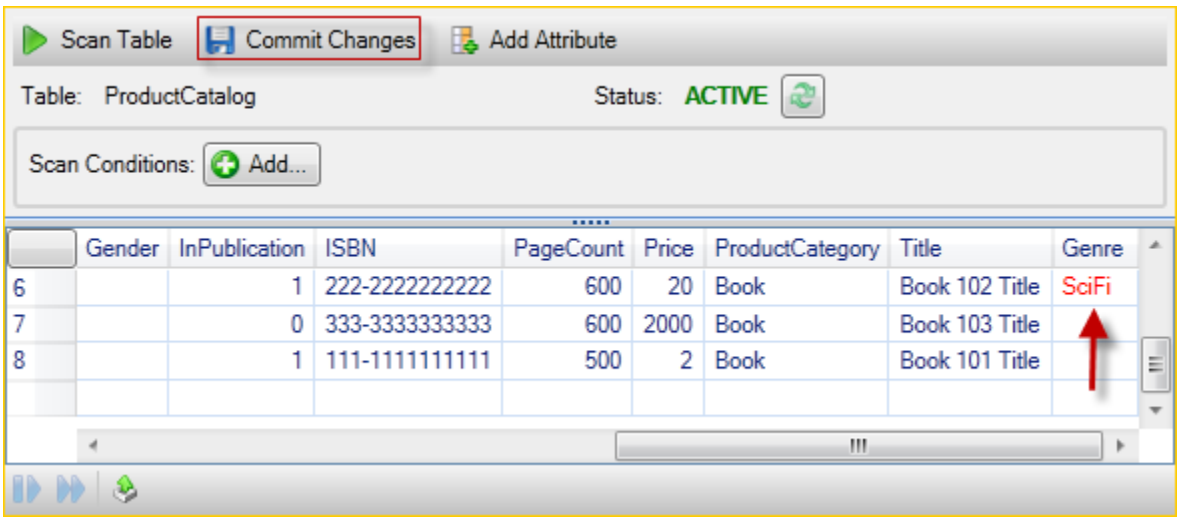
In der Rasteransicht können Sie der Tabelle auch Attribute hinzufügen. Wählen Sie Add Attribute (Attribut hinzuzufügen), um ein neues Attribut hinzuzufügen.



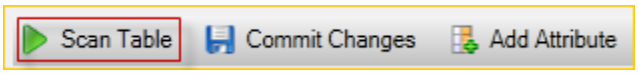
Geben Sie im Dialogfeld Add Attribut (Attribut hinzuzufügen) einen Namen für das Attribut ein und wählen Sie dann OK aus.



Um das neue Attribut in die Tabelle aufzunehmen, müssen Sie mindestens für ein Element einen Wert zum Attribut hinzufügen. Dann wählen Sie die Schaltfläche Commit Changes (Änderungen commiten). Wenn Sie das neue Attribut verwerfen möchten, schließen Sie einfach die Rasteransicht der Tabelle, ohne Commit Changes (Änderungen commiten) zu wählen.



Scannen einer DynamoDB-Tabelle

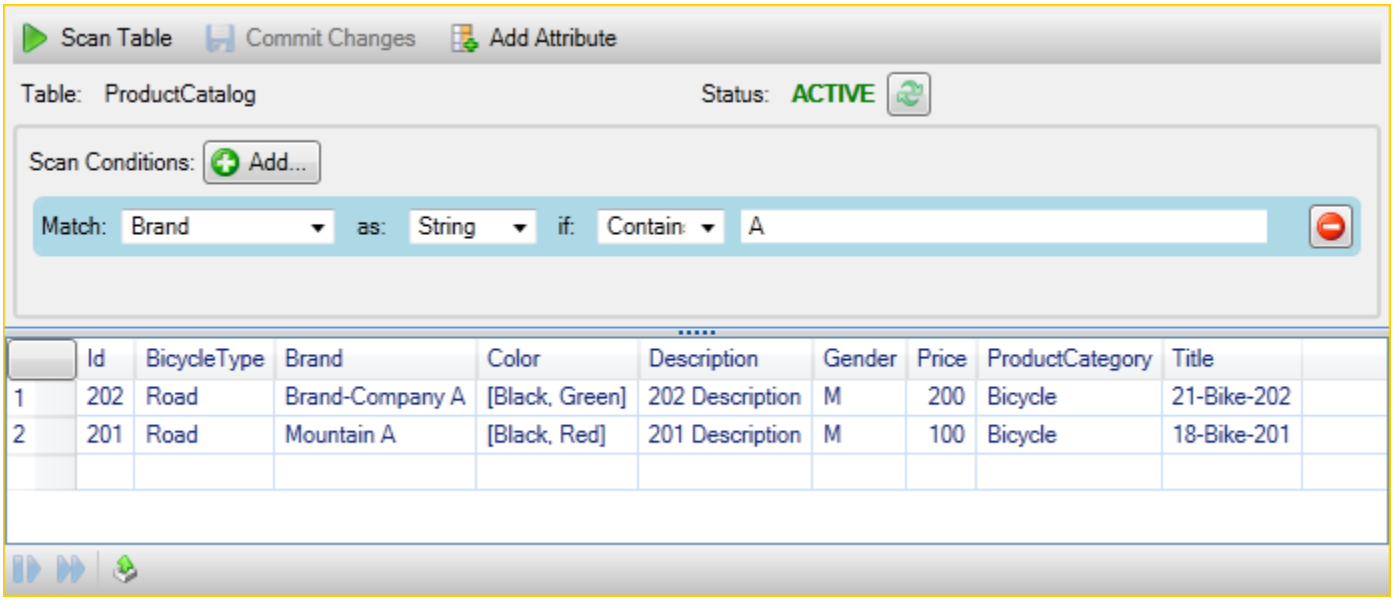


Sie können mit dem Toolkit Scans an Ihren DynamoDB-Tabellen durchführen. In einem Scan definieren Sie eine Reihe von Kriterien und der Scan führt alle Elemente in der Tabelle auf, die den Kriterien entsprechen. Scans sind teure Operationen und sollten daher mit Vorsicht verwendet werden, um zu vermeiden, dass Produktionsdatenverkehr mit höherer Priorität in der Tabelle unterbrochen wird. Weitere Informationen zur Verwendung des Scanvorgangs finden Sie im Amazon DynamoDB Developer Guide.

So führen Sie im Explorer einen Scan für eine DynamoDB-Tabelle durch AWS

1. Wählen Sie in der Rasteransicht die Schaltfläche scan conditions: add (Scan-Bedingungen: Hinzufügen).
2. Wählen Sie im Scan-Klauseleditor das Attribut, mit dem eine Übereinstimmung abgeglichen werden soll, wie der Wert des Attributs interpretiert werden soll (Zeichenfolge, Zahl, Satzwert), wie die Übereinstimmung sein soll, (z. B. Beginnt mit oder Enthält) und welchem Literalwert entsprochen werden soll.
3. Fügen Sie so viele Scan-Klauseln hinzu, wie für Ihre Suche erforderlich. In den Ergebnissen werden nur die Elemente aufgeführt, die den Kriterien aller Scan-Klauseln entsprechen. Bei dem Scan wird ein Vergleich unter Berücksichtigung der Groß- und Kleinschreibung durchgeführt, wenn mit Zeichenfolgewerten abgeglichen wird.
4. Wählen Sie in der Schaltflächenleiste oben in der Rasteransicht Scan Table (Tabelle scannen).

Zum Entfernen einer Scan-Klausel wählen Sie die rote Schaltfläche mit der weißen Linie rechts von jeder Klausel.



Entfernen Sie alle Scan-Klauseln, und wählen Sie Scan Table (Tabelle scannen) erneut, um zur Ansicht zurückzukehren, die alle Elemente enthält.

Paginierung von Scan-Ergebnissen

Am unteren Rand der Ansicht sehen Sie drei Schaltflächen.

Mit den ersten beiden blauen Schaltflächen können Sie Scan-Ergebnisse paginieren. Die erste Schaltfläche zeigt eine zusätzliche Ergebnisseite an. Die zweite Schaltfläche zeigt 10 zusätzliche Ergebnisseiten an. In diesem Kontext entspricht eine Seite eine Inhalt von 1 MB.

Exportieren von Scan-Ergebnissen in CSV

Anhand der dritten Schaltfläche werden die Ergebnisse des aktuellen Scans in eine CSV-Datei exportiert.

Verwendung AWS CodeCommit mit Visual Studio Team Explorer

Sie können AWS Identity and Access Management (IAM-) Benutzerkonten verwenden, um Git-Anmeldeinformationen zu erstellen und sie zum Erstellen und Klonen von Repositorys in Team Explorer zu verwenden.

Typen von Anmeldeinformationen für AWS CodeCommit

Den meisten AWS Toolkit for Visual Studio Benutzern ist bewusst, dass sie Profile mit AWS Anmeldeinformationen einrichten, die ihre Zugriffs- und Geheimschlüssel enthalten. Diese Anmeldeinformationsprofile werden im Toolkit for Visual Studio verwendet, um die Calls to Service zu aktivieren APIs, z. B. um Amazon S3 S3-Buckets im AWS Explorer aufzulisten oder um eine Amazon-Instance zu starten. EC2 AWS CodeCommit Bei der Integration mit Team Explorer werden diese Anmeldeinformationsprofile ebenfalls verwendet. Für die direkte Arbeit mit Git benötigen Sie jedoch zusätzliche Anmeldeinformationen, genauer gesagt, Git-Anmeldeinformationen für HTTPS-Verbindungen. Informationen zu diesen Anmeldeinformationen (ein Benutzername und ein Passwort) finden Sie unter Einrichtung für HTTPS-Benutzer mit Git-Anmeldeinformationen im AWS CodeCommit Benutzerhandbuch.

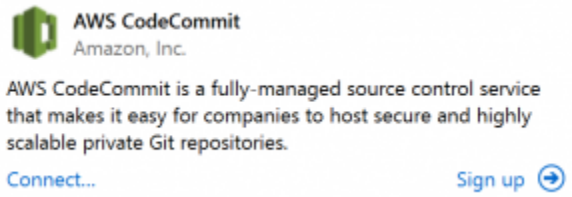
Sie können die Git-Anmeldeinformationen AWS CodeCommit nur für IAM-Benutzerkonten erstellen. Es ist nicht möglich, sie für ein Root-Konto zu erstellen. Sie können bis zu zwei Gruppen dieser Anmeldeinformationen für den Service erstellen. Obwohl Sie eine Gruppe von Anmeldeinformationen als inaktiv markieren können, werden inaktive Gruppen weiterhin Ihrem Grenzwert von zwei Gruppen zugerechnet. Beachten Sie, dass Sie Anmeldeinformationen jederzeit löschen und neu erstellen können. Wenn Sie sie in Visual Studio verwenden AWS CodeCommit , werden Ihre herkömmlichen

AWS Anmeldeinformationen für die Arbeit mit dem Dienst selbst verwendet, z. B. wenn Sie Repositorys erstellen und auflisten. Wenn Sie mit den tatsächlich gehosteten Git-Repositorys arbeiten AWS CodeCommit, verwenden Sie die Git-Anmeldeinformationen.

Im Rahmen der Unterstützung für AWS CodeCommit erstellt und verwaltet das Toolkit for Visual Studio diese Git-Anmeldeinformationen automatisch für Sie und ordnet sie Ihrem AWS Anmeldeinformationsprofil zu. Sie müssen sich nicht darum kümmern, die richtigen Anmeldeinformationen bereitzuhalten, wenn Sie Git-Operationen im Team Explorer durchführen möchten. Sobald Sie mit Ihrem AWS Anmeldeinformationsprofil eine Verbindung zu Team Explorer hergestellt haben, werden die zugehörigen Git-Anmeldeinformationen automatisch verwendet, wenn Sie mit einer Git-Remote arbeiten.

Verbindung herstellen zu AWS CodeCommit

Wenn Sie das Team Explorer-Fenster in Visual Studio 2015 oder höher öffnen, wird im Bereich Hosted Service Providers von Manage Connections ein AWS CodeCommit Eintrag angezeigt.

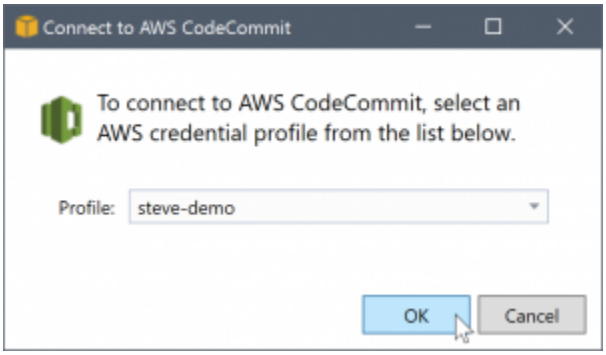


Wenn Sie Anmelden wählen, wird die Amazon Web Services Services-Startseite in einem Browserfenster geöffnet. Was passiert, wenn Sie Connect wählen, hängt davon ab, ob das Toolkit for Visual Studio ein Anmeldeinformationsprofil mit AWS Zugriffs- und Geheimschlüsseln finden kann, damit es in AWS Ihrem Namen Anrufe tätigen kann. Möglicherweise haben Sie mithilfe der neuen Seite Erste Schritte, die in der IDE angezeigt wird, ein Anmeldeinformationsprofil eingerichtet, wenn das Toolkit for Visual Studio keine lokal gespeicherten Anmeldeinformationen finden kann. Oder Sie haben möglicherweise das Toolkit for Visual Studio AWS Tools for Windows PowerShell, das oder das verwendet AWS CLI und haben bereits AWS Anmeldeinformationsprofile für das Toolkit for Visual Studio zur Verfügung.

Wenn Sie Connect wählen, startet das Toolkit for Visual Studio den Prozess, um ein Anmeldeinformationsprofil zu finden, das in der Verbindung verwendet werden soll. Wenn das Toolkit for Visual Studio kein Anmeldeinformationsprofil finden kann, öffnet es ein Dialogfeld, in dem Sie aufgefordert werden, die Zugriffs- und Geheimschlüssel für Ihr Profil einzugeben. AWS-Konto Es wird dringend empfohlen, ein IAM-Benutzerkonto und keine Root-Anmeldeinformationen zu verwenden. Wie bereits erwähnt, können Sie außerdem die schließlich benötigten Git-Anmeldeinformationen

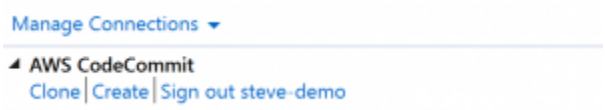
nur für IAM-Benutzer erstellen. Sobald die Zugriffs- und Geheimschlüssel bereitgestellt und das Anmeldeinformationsprofil erstellt wurde, ist die Verbindung zwischen Team Explorer und AWS CodeCommit Team Explorer einsatzbereit.

Wenn das Toolkit for Visual Studio mehr als ein AWS Anmeldeinformationsprofil findet, werden Sie aufgefordert, das Konto auszuwählen, das Sie in Team Explorer verwenden möchten.



Wenn Sie nur ein Anmeldeinformationsprofil haben, umgeht das Toolkit for Visual Studio das Dialogfeld zur Profilauswahl und Sie sind sofort verbunden:

Wenn eine Verbindung zwischen Team Explorer und AWS CodeCommit über Ihre Anmeldeinformationsprofile hergestellt wurde, wird das Einladungsdialogfeld geschlossen und das Verbindungsfenster wird angezeigt.

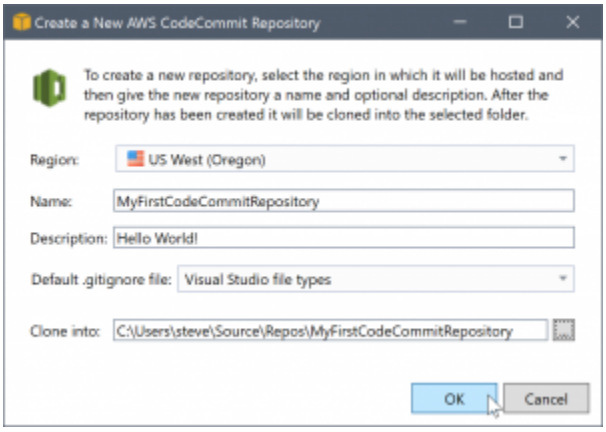


Da Sie nicht über lokale geklonte Repositorys verfügen, werden in dem Bereich nur die Vorgänge angezeigt, die Sie ausführen können: Clone (Klonen), Create (Erstellen) und Sign out (Abmelden). Wie bei anderen Anbietern kann AWS CodeCommit in Team Explorer jeweils nur an ein einziges AWS Anmeldeinformationsprofil gebunden werden. Um das Konto zu wechseln, melden Sie sich über Sign out (Abmelden) ab, um die Verbindung zu entfernen. Sie können dann eine neue Verbindung mit einem anderen Konto herstellen.

Nachdem Sie eine Verbindung hergestellt haben, können Sie ein Repository erstellen, indem Sie auf den Link Create (Erstellen) klicken.

Erstellen eines Repositorys

Wenn Sie auf den Link Erstellen klicken, wird das Dialogfeld Neues AWS CodeCommit Repository erstellen geöffnet.



AWS CodeCommit Repositorys sind nach Regionen organisiert, sodass Sie unter Region die Region auswählen können, in der das Repository gehostet werden soll. Die Liste enthält alle Regionen, in denen dies unterstützt AWS CodeCommit wird. Sie geben den Namen (erforderlich) und eine Beschreibung (optional) für das neue Repository an.

Im Standardverhalten des Dialogfelds wird der Repository-Name an den Speicherort des Ordners für das neue Repository angehängt. (Wenn Sie den Namen eingeben, wird auch der Speicherort des Ordners aktualisiert.) Wenn Sie einen anderen Ordnernamen verwenden möchten, bearbeiten Sie den Ordnerpfad Clone into (Klonen nach), nachdem Sie den Repository-Namen eingegeben haben.

Sie können automatisch eine erste `.gitignore`-Datei für das Repository erstellen. Das AWS Toolkit for Visual Studio bietet einen integrierten Standard für Visual Studio-Dateitypen. Sie können auch auf die Datei verzichten oder auf eine benutzerdefinierte vorhandene Datei zurückgreifen, die Sie in allen Repositorys wiederverwenden möchten. Wählen Sie einfach Use custom (Angepasstes verwenden) in der Liste aus und navigieren Sie zu der benutzerdefinierten Datei, die verwendet werden soll.

Sobald Sie über einen Namen und einen Speicherort für das Repository verfügen, können Sie auf OK klicken und mit dem Erstellen des Repositorys beginnen. Das Toolkit for Visual Studio fordert den Dienst auf, das Repository zu erstellen und dann das neue Repository lokal zu klonen. Dabei wird ein erster Commit für die .gitignore-Datei hinzugefügt, falls Sie eine verwenden. An diesem Punkt beginnen Sie, mit der Git-Remote zu arbeiten, sodass das Toolkit for Visual Studio jetzt Zugriff auf die zuvor beschriebenen Git-Anmeldeinformationen benötigt.

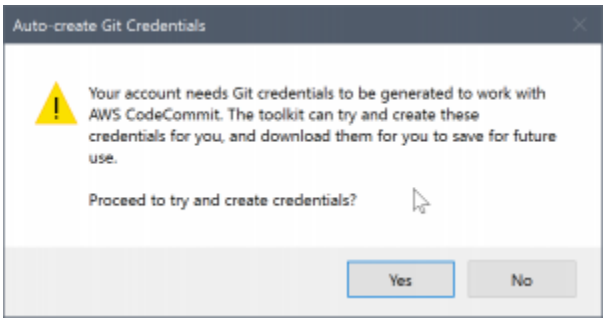
Einrichten von Git-Anmeldeinformationen

Bis jetzt haben Sie AWS Zugriffs- und geheime Schlüssel verwendet, um den Dienst zur Erstellung Ihres Repositorys aufzufordern. Jetzt müssen Sie mit Git selbst arbeiten, um den eigentlichen Klonvorgang durchzuführen, und Git versteht keine AWS Zugriffs- und Geheimschlüssel. Stattdessen

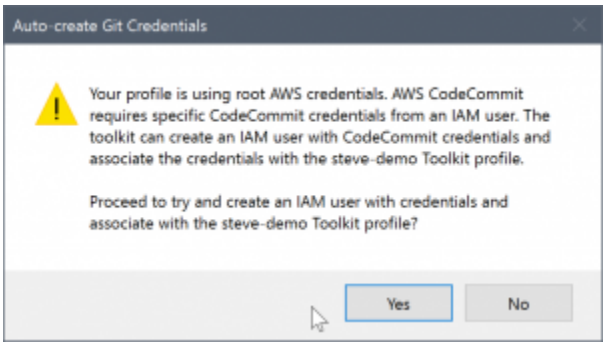
müssen Sie Git die Anmeldeinformationen (Benutzername und Passwort) angeben, die für eine HTTPS-Verbindung mit dem Remote-Repository verwendet werden sollen.

Wie unter Setting up Git credentials beschrieben, müssen die verwendeten Git-Anmeldeinformationen einem IAM-Benutzer zugeordnet werden. Sie können sie nicht für Root-Anmeldeinformationen generieren. Du solltest deine AWS Anmeldeinformationsprofile immer so einrichten, dass sie IAM-Benutzerzugriffs- und geheime Schlüssel und keine Root-Schlüssel enthalten. Das Toolkit for Visual Studio kann versuchen, Git-Anmeldeinformationen AWS CodeCommit für Sie einzurichten und sie dem AWS Anmeldeinformationsprofil zuzuordnen, das Sie zuvor für die Verbindung in Team Explorer verwendet haben.

Wenn Sie im Dialogfeld Neues AWS CodeCommit Repository erstellen auf OK klicken und das Repository erfolgreich erstellt haben, überprüft das Toolkit for Visual Studio das AWS Anmeldeinformationsprofil, das in Team Explorer verbunden ist, um festzustellen, ob Git-Anmeldeinformationen für AWS CodeCommit existieren und lokal mit dem Profil verknüpft sind. Falls ja, weist das Toolkit for Visual Studio Team Explorer an, den Klonvorgang für das neue Repository zu starten. Wenn Git-Anmeldeinformationen nicht lokal verfügbar sind, überprüft das Toolkit for Visual Studio den Typ der Kontoanmeldeinformationen, die für die Verbindung in Team Explorer verwendet wurden. Wenn es sich um Anmeldeinformationen für einen IAM-Benutzer handelt, wie empfohlen, wird die folgende Meldung angezeigt.

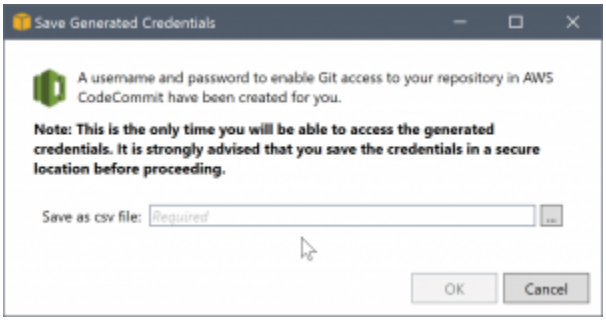


Wenn es sich um Root-Anmeldeinformationen handelt, wird stattdessen die folgende Meldung angezeigt.



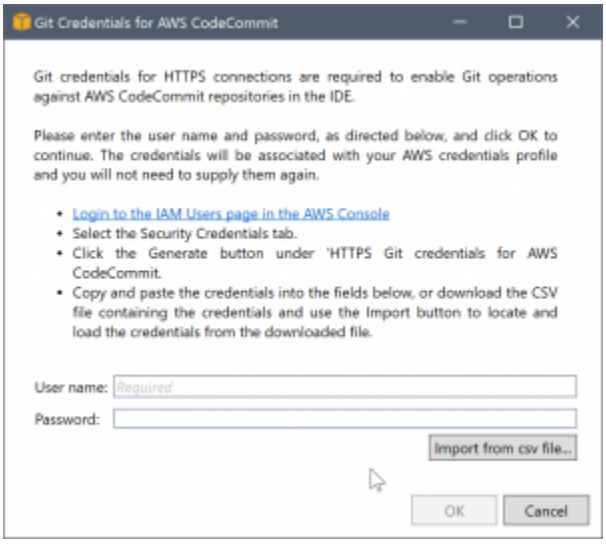
In beiden Fällen bietet das Toolkit for Visual Studio an, zu versuchen, die erforderlichen Git-Anmeldeinformationen für Sie zu erstellen. Im ersten Szenario wird für die Erstellung lediglich eine Gruppe von Git-Anmeldeinformationen für den IAM-Benutzer benötigt. Wenn ein Root-Konto verwendet wird, versucht das Toolkit for Visual Studio zunächst, einen IAM-Benutzer zu erstellen, und fährt dann mit der Erstellung von Git-Anmeldeinformationen für diesen neuen Benutzer fort. Wenn das Toolkit for Visual Studio einen neuen Benutzer erstellen muss, wendet es die verwaltete AWS CodeCommit Power-User-Richtlinie auf dieses neue Benutzerkonto an. Diese Richtlinie erlaubt nur den Zugriff auf AWS CodeCommit und ermöglicht die Ausführung aller Operationen mit AWS CodeCommit Ausnahme des Löschens des Repositorys.

Wenn Sie Anmeldeinformationen erstellen, können Sie sie nur einmal anzeigen. Daher fordert Sie das Toolkit for Visual Studio auf, die neu erstellten Anmeldeinformationen als `.csv` Datei zu speichern, bevor Sie fortfahren.



Dies wird ebenfalls dringend empfohlen. Speichern Sie sie außerdem an einem sicheren Ort.

Es kann vorkommen, dass das Toolkit for Visual Studio Anmeldeinformationen nicht automatisch erstellen kann. Beispielsweise haben Sie möglicherweise bereits die maximale Anzahl von Git-Anmeldeinformationen für AWS CodeCommit (zwei) erstellt, oder Sie verfügen möglicherweise nicht über ausreichende programmatische Rechte, damit das Toolkit for Visual Studio die Arbeit für Sie erledigt (wenn Sie als IAM-Benutzer angemeldet sind). In diesen Fällen können Sie sich bei der anmelden, AWS Management Console um die Anmeldeinformationen zu verwalten, oder sie von Ihrem Administrator anfordern. Sie können sie dann in das AWS CodeCommit Dialogfeld „Git-Anmeldeinformationen für“ eingeben, das im Toolkit for Visual Studio angezeigt wird.

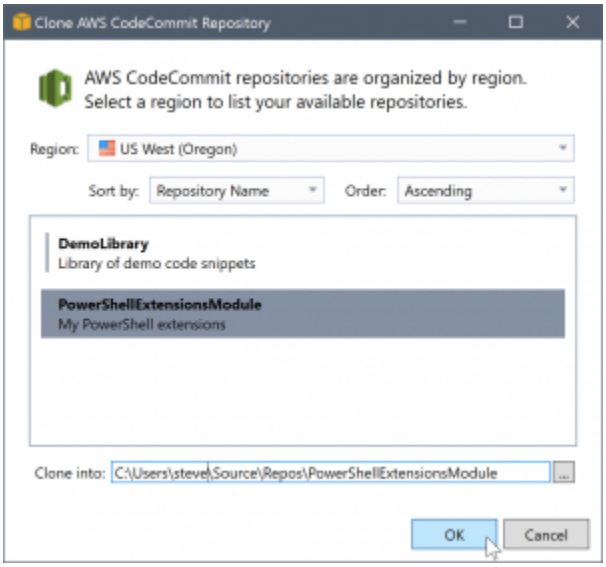


Nachdem die Anmeldeinformationen für Git verfügbar sind, wird mit dem Klonvorgang für das neue Repository fortgefahren (siehe die Fortschrittsanzeige für den Vorgang im Team Explorer). Wenn Sie eine Standard-`.gitignore`-Datei angewendet haben, wird für diese ein Commit im Repository mit dem Kommentar „Erster Commit“ durchgeführt.

Damit wurden das Einrichten von Anmeldeinformationen und das Erstellen eines Repositorys im Team Explorer vollständig erläutert. Sobald die erforderlichen Anmeldeinformationen vorhanden sind, sehen Sie bei der future Erstellung neuer Repositorys nur noch das Dialogfeld Neues AWS CodeCommit Repository erstellen.

Klonen eines Repositorys

Um ein vorhandenes Repository zu klonen, kehren Sie zum Verbindungsfenster von Team Explorer zurück. AWS CodeCommit Klicken Sie auf den Link Klonen, um das Dialogfeld AWS CodeCommit Repository klonen zu öffnen, und wählen Sie dann das zu klonende Repository und den Speicherort auf der Festplatte aus, an dem Sie es platzieren möchten.



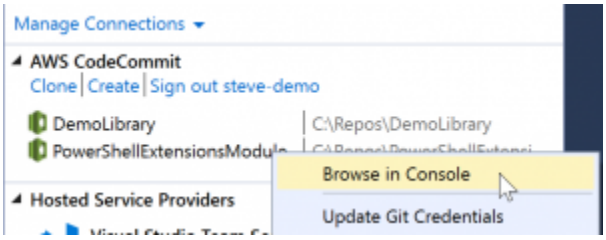
Sobald Sie die Region ausgewählt haben, fragt das Toolkit for Visual Studio den Dienst ab, um die Repositorys zu ermitteln, die in dieser Region verfügbar sind, und zeigt sie im zentralen Listenbereich des Dialogfelds an. Der Name und eine optionale Beschreibung jedes Repositorys werden ebenfalls angezeigt. Sie können die Liste nach Repository-Namen oder Datum der letzten Änderung und aufsteigend oder absteigend neu sortieren.

Wenn Sie das Repository ausgewählt haben, können Sie den Zielspeicherort für den Klonvorgang auswählen. Dies ist standardmäßig derselbe Repository-Speicherort, der auch in anderen Plug-ins des Team Explorers verwendet wird. Sie können jedoch zu einem anderen Standort navigieren oder diesen eingeben. Standardmäßig wird an den ausgewählten Pfad der Repository-Name angehängt. Wenn Sie jedoch einen bestimmten Pfad angeben möchten, bearbeiten Sie einfach das Textfeld, nachdem Sie den Ordner ausgewählt haben. Der Text in dem Feld, wenn Sie auf OK klicken, wird zu dem Ordner, in dem Sie das geklonte Repository finden.

Nachdem Sie das Repository und einen Speicherordner ausgewählt haben, klicken Sie auf OK, um mit dem Klonvorgang fortzufahren. Genau wie beim Erstellen eines Repositorys wird der gemeldete Fortschritt des Klonvorgangs im Team Explorer angezeigt.

Verwenden von Repositorys

Wenn Sie lokale Repositorys klonen oder erstellen, beachten Sie, dass die lokalen Repositorys für die Verbindung im Verbindungsbereich im Team Explorer unter den Vorgangs-Links angezeigt werden. Diese Einträge bieten Ihnen eine bequeme Möglichkeit, auf das Repository zuzugreifen, um die Inhalte zu durchsuchen. Klicken Sie einfach mit der rechten Maustaste auf das Repository und wählen Sie Browse in Console (In Konsole durchsuchen) aus.



Sie können auch Update Git Credentials (Git-Anmeldeinformationen aktualisieren) verwenden, um die gespeicherten Git-Anmeldeinformationen, die dem Anmeldeinformationsprofil zugeordnet sind, zu aktualisieren. Dies ist nützlich, wenn Sie die Anmeldeinformationen rotiert haben. Der Befehl öffnet das AWS CodeCommit Dialogfeld „Git-Anmeldeinformationen für“, in dem Sie die neuen Anmeldeinformationen eingeben oder importieren können.

Git-Vorgänge auf die Repositorys funktionieren erwartungsgemäß. Sie können lokale Commits durchführen und wenn Sie bereit sind, Ihre Änderungen freizugeben, verwenden Sie die Synchronisierungsoption im Team Explorer. Da die Git-Anmeldeinformationen bereits lokal gespeichert und mit unserem verbundenen AWS Anmeldeinformationsprofil verknüpft sind, werden wir nicht aufgefordert, sie für Operationen mit der AWS CodeCommit Fernbedienung erneut einzugeben.

CodeArtifact In Visual Studio verwenden

AWS CodeArtifact ist ein vollständig verwalteter Artefakt-Repository-Service, der es Unternehmen erleichtert, Softwarepakete, die für die Anwendungsentwicklung verwendet werden, sicher zu speichern und gemeinsam zu nutzen. Sie können ihn CodeArtifact mit gängigen Build-Tools und Paketmanagern wie dem.NET Core NuGet CLIs und Visual Studio verwenden. Sie können auch so konfigurieren CodeArtifact , dass Pakete aus einem externen, öffentlichen Repository wie NuGet.org abgerufen werden.

In CodeArtifact werden Ihre Pakete in Repositorys gespeichert, die dann innerhalb einer Domain gespeichert werden. Das AWS Toolkit for Visual Studio vereinfacht die Konfiguration von Visual Studio mit Ihren CodeArtifact Repositorys und macht es einfach, Pakete in Visual Studio sowohl CodeArtifact NuGet direkt als auch von.org zu nutzen.

Fügen Sie Ihr CodeArtifact Repository als NuGet Paketquelle hinzu

Um Pakete aus Ihrem zu konsumieren CodeArtifact, müssen Sie Ihr Repository als Paketquelle im NuGet Paketmanager in Visual Studio hinzufügen

Um Ihr Repository als Paketquelle hinzuzufügen

1. Navigieren Sie im AWS Explorer zu Ihrem Repository im AWS CodeArtifactKnoten.
2. Öffnen Sie das Kontextmenü (mit der rechten Maustaste) für das Repository, das Sie hinzufügen möchten, und wählen Sie dann NuGet Quellendpunkt kopieren aus.
3. Navigieren Sie im Menü Tools > Optionen zu NuGet Paketquellen unter dem Knoten Package Manager.
4. Wählen Sie Package Paketquellen das Pluszeichen (+) aus, bearbeiten Sie den Namen und fügen Sie die NuGet Quellendpunkt-URL, die Sie zuvor kopiert haben, in das Feld Quelle ein.
5. Aktivieren Sie das Kontrollkästchen neben der neu hinzugefügten Paketquelle, um sie zu aktivieren.

> **Note**
>
> Wir empfehlen, eine externe Verbindung zu NuGet.org zu Ihrem hinzuzufügen CodeArtifact und die nuget.org-Paketquelle in Visual Studio zu deaktivieren. Wenn Sie eine externe Verbindung verwenden, werden alle aus NuGet.org abgerufenen Abhängigkeiten in gespeichert. CodeArtifact Falls NuGet.org aus irgendeinem Grund ausfällt, sind die benötigten Pakete weiterhin verfügbar. Weitere Informationen zu externen Verbindungen finden Sie unter Hinzufügen einer externen Verbindung im AWS CodeArtifact Benutzerhandbuch.

6. Wählen Sie OK, um das Menü zu schließen.

Weitere Informationen zur Verwendung CodeArtifact mit Visual Studio finden Sie unter Verwendung CodeArtifact mit Visual Studio im AWS CodeArtifact Benutzerhandbuch.

Amazon RDS von AWS Explorer

Amazon Relational Database Service (Amazon RDS) ist ein Service, mit dem Sie relationale SQL-Datenbanksysteme in der Cloud bereitstellen und verwalten können. Amazon RDS unterstützt drei Arten von Datenbanksystemen:

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

Weitere Informationen finden Sie im Amazon RDS-Benutzerhandbuch.

Viele der hier besprochenen Funktionen sind auch über die AWS Management Console für Amazon RDS verfügbar.

Themen

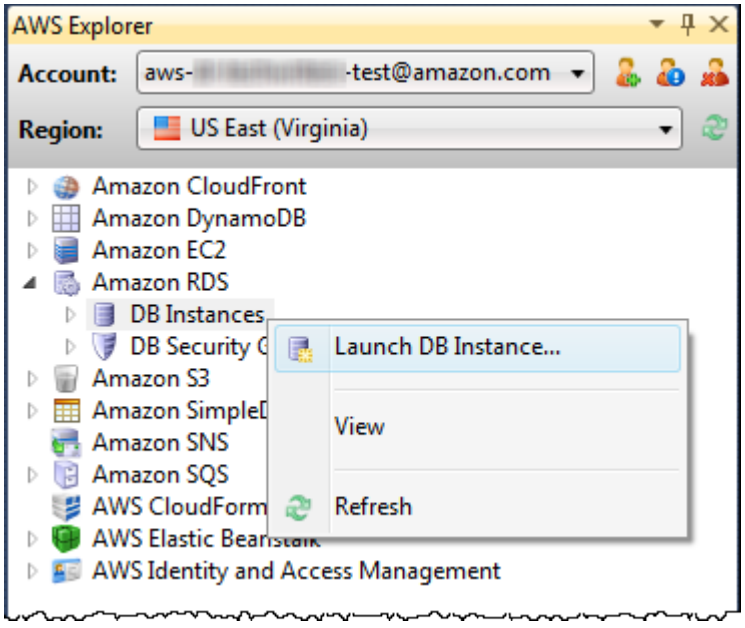
- Starten Sie eine Amazon RDS-Datenbank-Instance
- Erstellen einer Microsoft SQL Server-Datenbank in einer RDS-Instance
- Amazon RDS-Sicherheitsgruppen

Starten Sie eine Amazon RDS-Datenbank-Instance

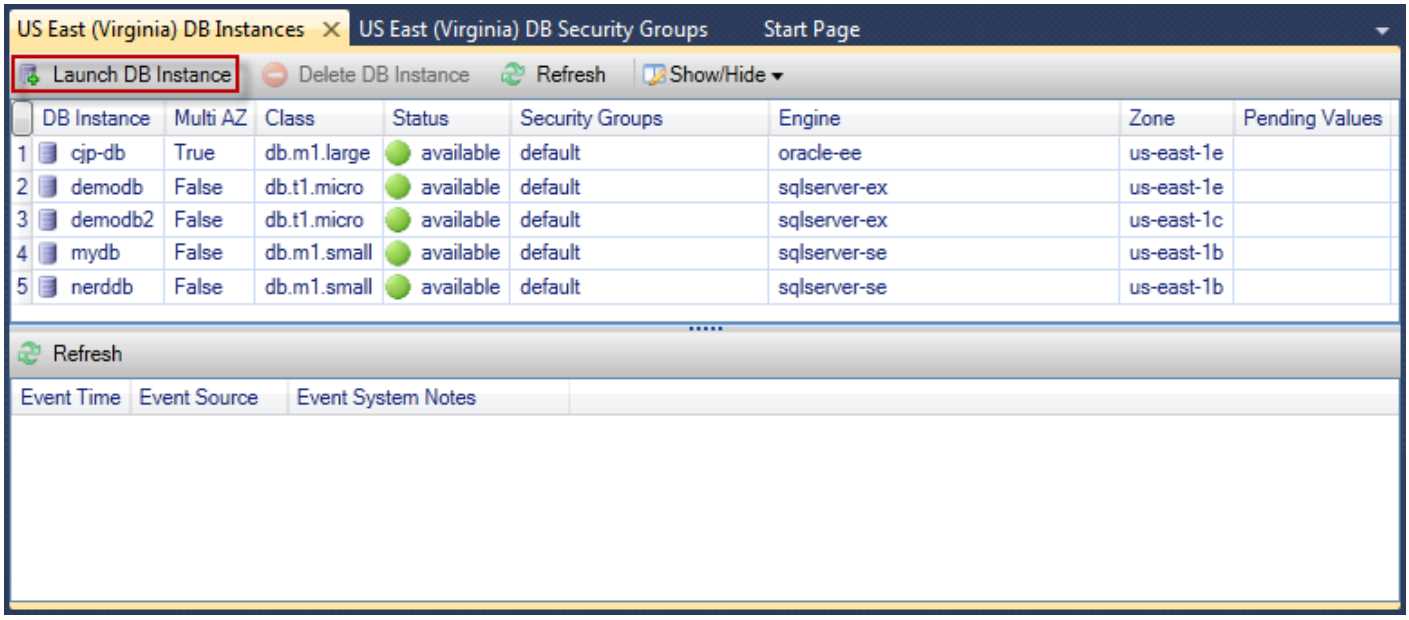
Mit AWS Explorer können Sie eine Instance jeder der von Amazon RDS unterstützten Datenbank-Engines starten. In der folgenden schrittweise Anleitung wird das Starten einer Instance von Microsoft SQL Server Standard Edition beschrieben. Die Vorgehensweise ist jedoch bei allen unterstützten Engines ähnlich.

So starten Sie eine Amazon RDS-Instance

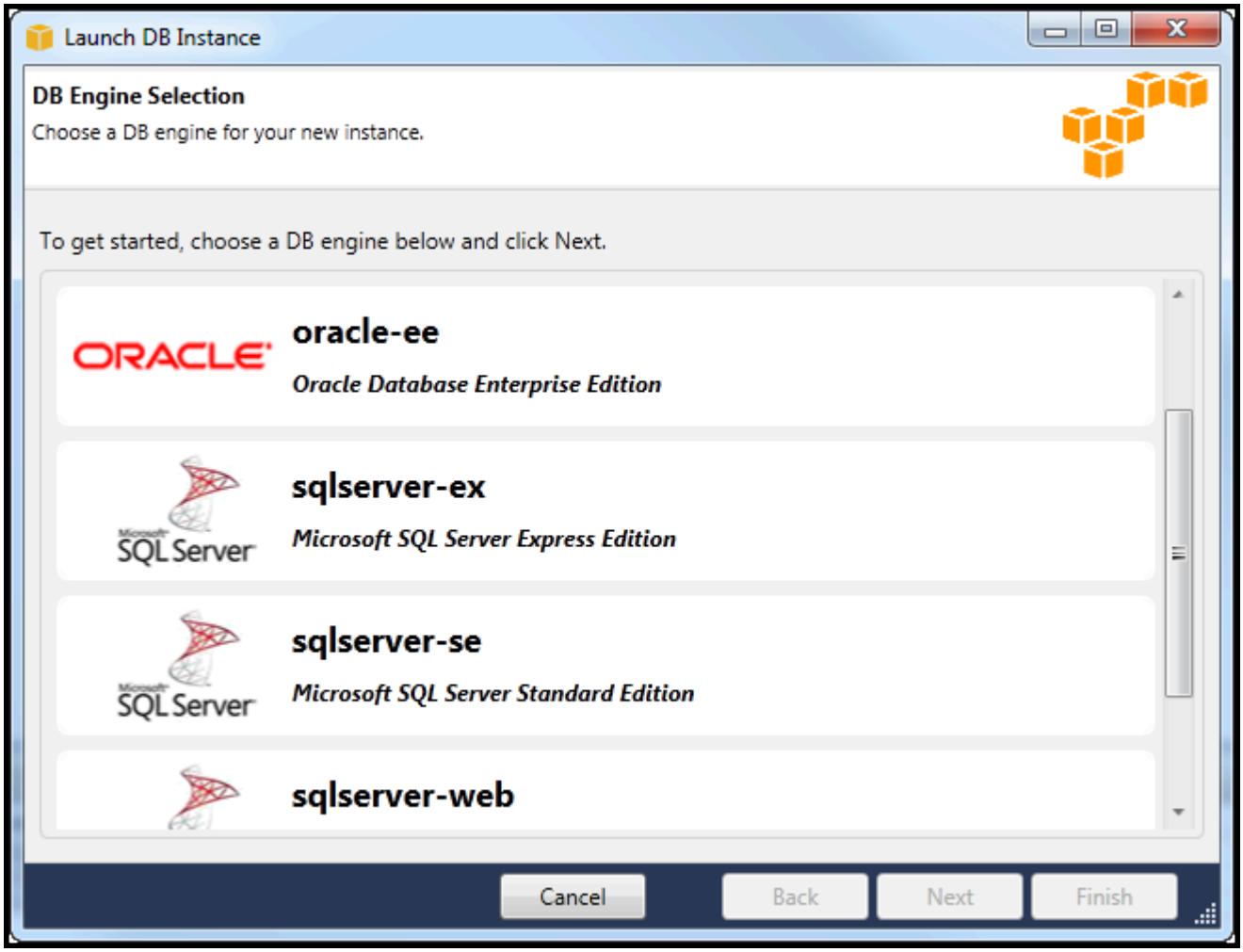
1. Öffnen Sie im AWS Explorer das Kontextmenü (Rechtsklick) für den Amazon RDS-Knoten und wählen Sie Launch DB Instance.



   Alternativ können Sie auf der Registerkarte DB Instances die Option Launch DB Instance (DB-Instance starten) wählen.



2. Wählen Sie im Feld DB Engine Selection (DB-Engine-Auswahl) den zu startenden Datenbank-Engine-Typ aus. Wählen Sie für diese Anleitung Microsoft SQL Server Standard Edition (sqlserver-se), und klicken Sie dann auf Next (Weiter).



3. Wählen Sie im Dialogfeld DB Engine Instance Options (DB-Engine-Instance-Optionen) die Konfigurationsoptionen aus.

   Im Abschnitt DB Engine Instance Options and Class (DB-Engine-Instance-Optionen und -Klasse) können Sie die folgenden Einstellungen festlegen:

   License model (Lizenzmodell)

Engine-Typ	License
Microsoft SQL Server	license-included
MySql	general-public-license
Oracle	bring-your-own-license

Das Lizenzmodell variiert je nach Art der Datenbank-Engine-Typ. Engine-Typ-Lizenz Microsoft SQL Server-Lizenz inklusive Oracle MySql general-public-license bring-your-own-license

DB Instance Version

Wählen Sie die Version des Datenbank-Engine aus, die Sie verwenden möchten. Wenn nur eine Version unterstützt wird, ist diese bereits für Sie ausgewählt.

DB-Instance-Klasse

Wählen Sie die Instance-Klasse für den Datenbank-Engine aus. Die Preise für Instance-Klassen variieren. Weitere Informationen finden Sie unter Amazon RDS – Preise.

Perform a multi AZ deployment

Wählen Sie diese Option, um eine Multi-AZ-Bereitstellung für verbesserte Datenbeständigkeit und Verfügbarkeit zu erstellen. Amazon RDS stellt eine Standby-Kopie Ihrer Datenbank in einer anderen Availability Zone bereit und verwaltet diese für den automatischen Failover bei einem geplanten oder ungeplanten Ausfall. Weitere Informationen zu den Preisen für Multi-AZ-Bereitstellungen finden Sie im Preisabschnitt der Amazon RDS-Detailseite. Diese Option wird nicht für Microsoft SQL Server unterstützt.

Upgrade minor versions automatically

Wählen Sie diese Option, damit kleinere Versionsupdates für Ihre RDS-Instances AWS automatisch für Sie durchgeführt werden.

Im Abschnitt RDS Database Instance (RDS-Datenbank-Instance) können Sie folgende Einstellungen festlegen:

Allocated Storage (Zugewiesener Speicher)

Engine	Minimum (GB)	Maximum (GB)
MySQL	5	1024
Oracle Enterprise Edition	10	1024
Microsoft SQL Server Express Edition	30	1024

Engine	Minimum (GB)	Maximum (GB)
Microsoft SQL Server Standard Edition	250	1024
Microsoft SQL Server Web Edition	30	1024

Die Minimal- und Maximalwerte für den zugewiesenen Speicher hängen vom Datenbank-Engine-Typ ab. Engine Minimum (GB) Maximum (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

Geben Sie einen Namen für die Datenbank-Instance an. Bei diesem Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Sie wird im AWS Explorer in Kleinbuchstaben angezeigt.

Master User Name (Master-Benutzername

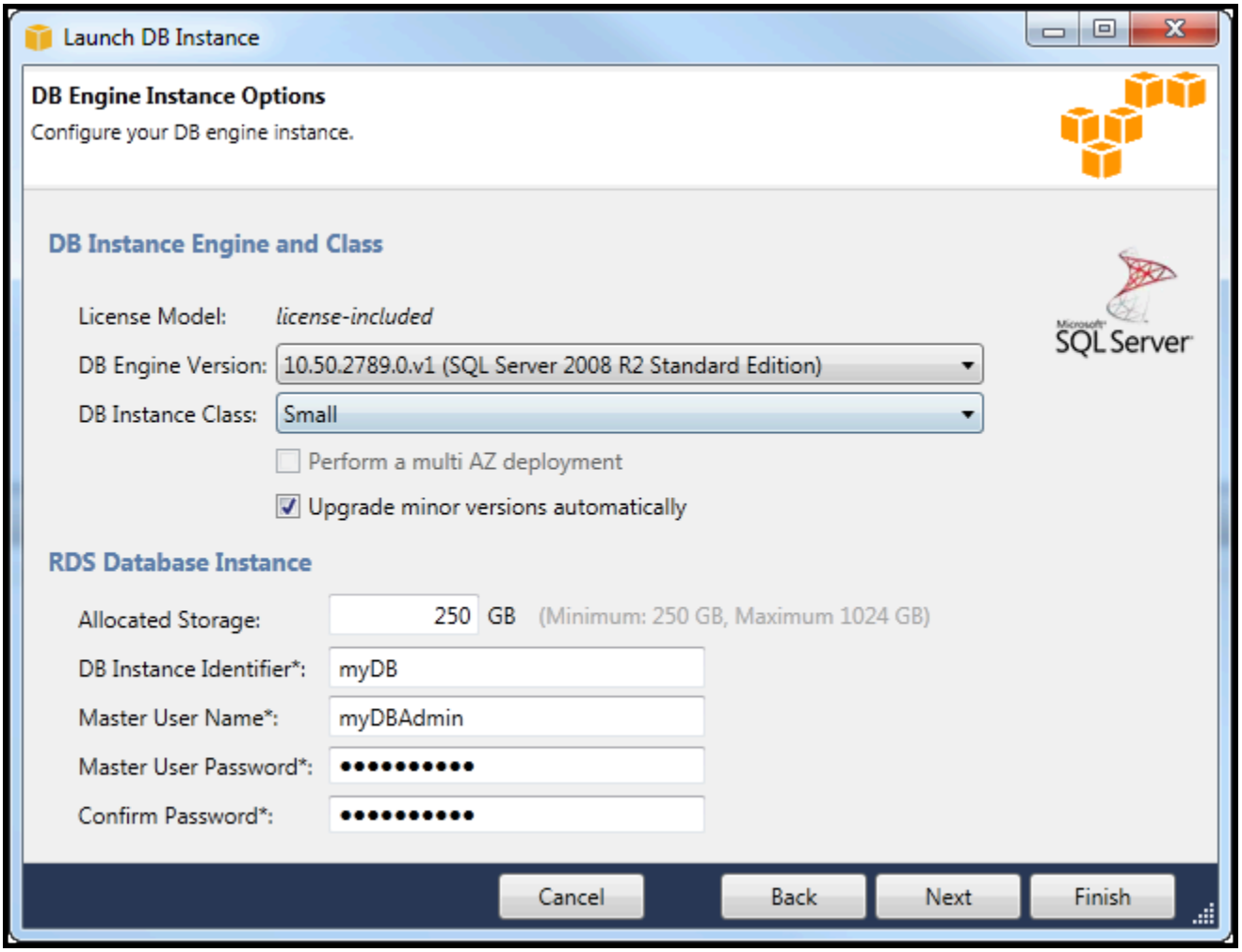
Geben Sie einen Namen für den Administrator der Datenbank-Instance ein.

Master User Password (Masterbenutzerpasswort)

Geben Sie ein Passwort für den Administrator der Datenbank-Instance ein.

Confirm Password

Geben Sie das Passwort erneut ein, um zu überprüfen, ob es korrekt ist.



1. Im Dialogfeld Additional Options können Sie die folgenden Einstellungen festlegen:

   Database Port (Datenbankport

   Dies ist der TCP-Port, über den die Instance im Netzwerk kommuniziert. Wenn Ihr Computer über eine Firewall auf das Internet zugreift, legen Sie für diesen Wert einen Port fest, für den Ihre Firewall Datenverkehr zulässt.

   Availability Zone

   Verwenden Sie diese Option, wenn Sie möchten, dass die Instance in einer bestimmten Availability Zone in Ihrer Region gestartet wird. Die Datenbank-Instance, die Sie angegeben haben, ist möglicherweise nicht in allen Availability Zones in einer bestimmten Region verfügbar.

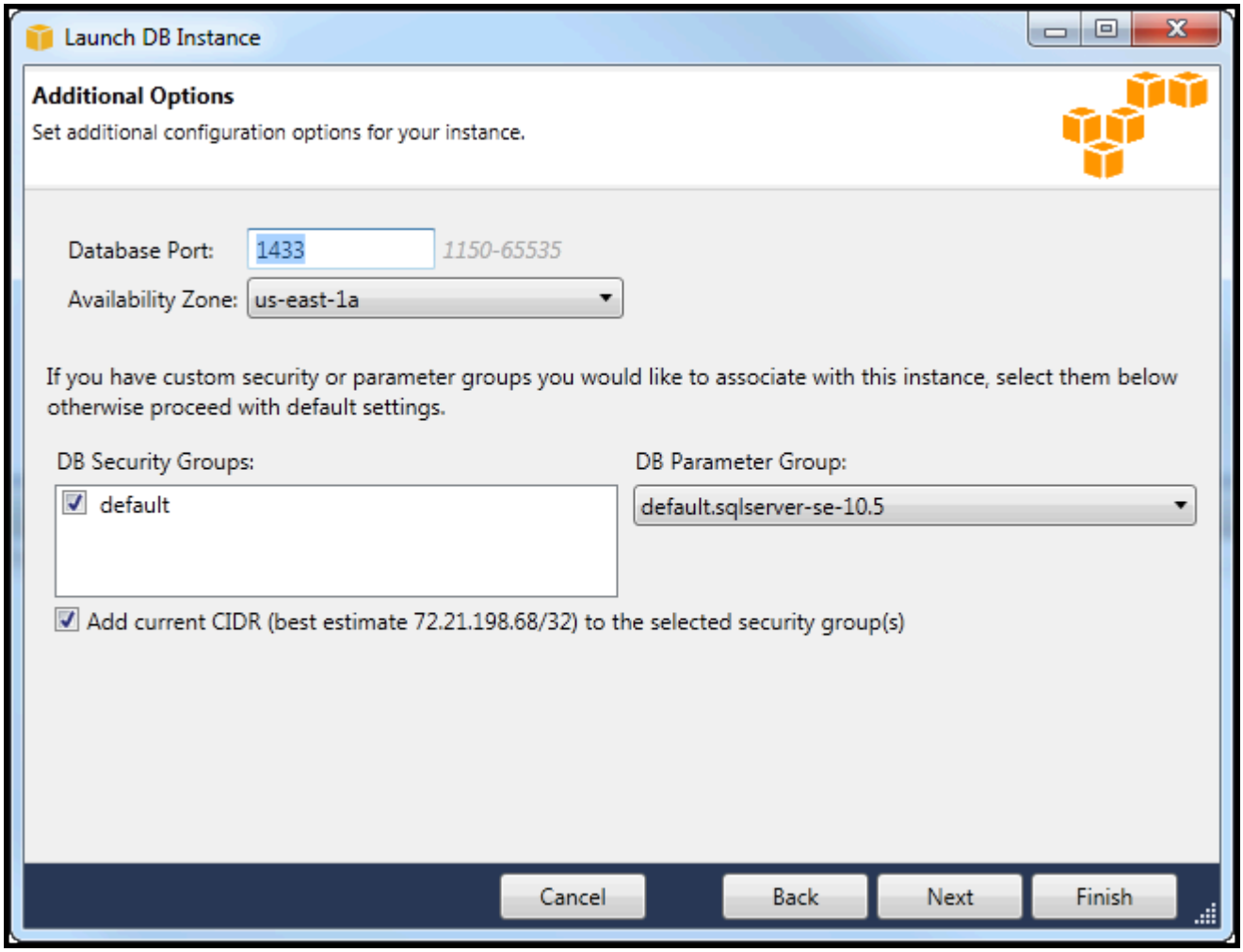
RDS-Sicherheitsgruppe

Wählen Sie eine RDS-Sicherheitsgruppe (oder -gruppen) aus, die mit der Instance verknüpft werden. RDS-Sicherheitsgruppen geben die IP-Adresse und die EC2 Amazon-Instances an, AWS-Konten die auf Ihre Instance zugreifen dürfen. Weitere Informationen über Amazon RDS-Sicherheitsgruppen finden Sie unter Amazon RDS Security Groups. Das Toolkit for Visual Studio versucht, Ihre aktuelle IP-Adresse zu ermitteln, und bietet die Option, diese Adresse zu den mit Ihrer Instanz verknüpften Sicherheitsgruppen hinzuzufügen. Wenn Ihr Computer jedoch über eine Firewall auf das Internet zugreift, ist die IP-Adresse, die das Toolkit erzeugt, möglicherweise nicht korrekt. Wenden Sie sich an Ihren Systemadministrator, um festzustellen, welche IP-Adresse verwendet werden muss.

DB-Parametergruppe

(Optional) Wählen Sie in der Dropdown-Liste eine DB-Parametergruppe aus, die mit Ihrer Instance verknüpft wird. DB-Parametergruppen ermöglichen Ihnen das Ändern der Standardkonfiguration für die Instance. Weitere Informationen finden Sie im Amazon Relational Database Service-Benutzerhandbuch und in diesem Artikel.

Wenn Sie in diesem Dialogfeld Einstellungen festgelegt haben, wählen Sie Next (Weiter).

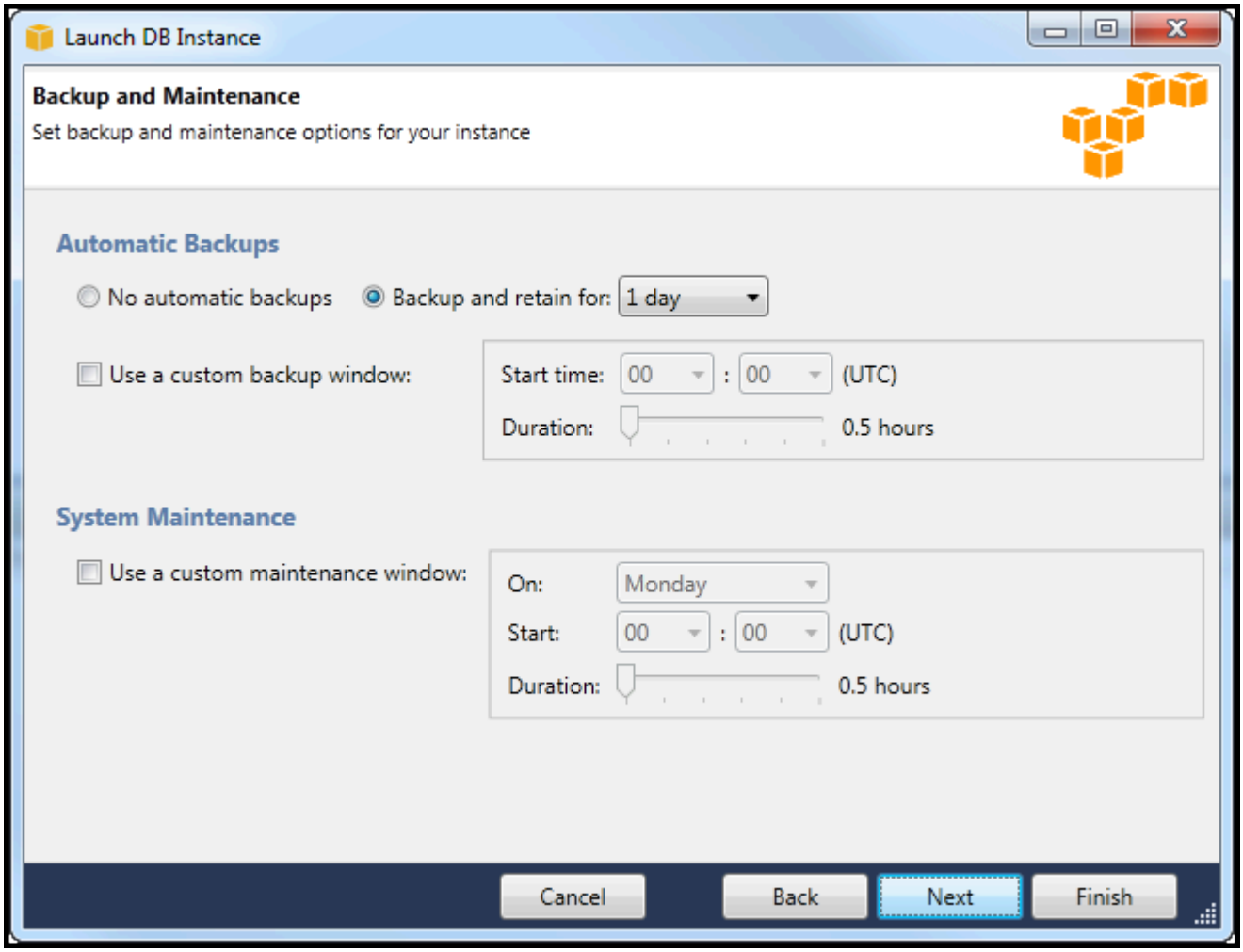


2. Im Dialogfeld Sicherung und Wartung können Sie angeben, ob Amazon RDS Ihre Instance sichern soll und wenn ja, wie lange das Backup aufbewahrt werden soll. Zudem können Sie ein Zeitfenster für die Ausführung der Sicherungen angeben.

   In diesem Dialogfeld können Sie auch angeben, ob Amazon RDS die Systemwartung an Ihrer Instance durchführen soll. Die Wartung umfasst routinemäßige Patches und die Aktualisierung von Nebenversionen.

   Das Zeitfenster für die Systemwartung darf sich nicht mit dem für die Sicherungen überschneiden.

   Wählen Sie Weiter.



3. Im letzten Dialogfeld des Assistenten können Sie die Einstellungen für Ihre Instance überprüfen. Wenn Sie die Einstellungen ändern möchten, klicken Sie auf die Schaltfläche Back (Zurück). Wenn alle Einstellungen korrekt sind, wählen Sie Launch (Starten).

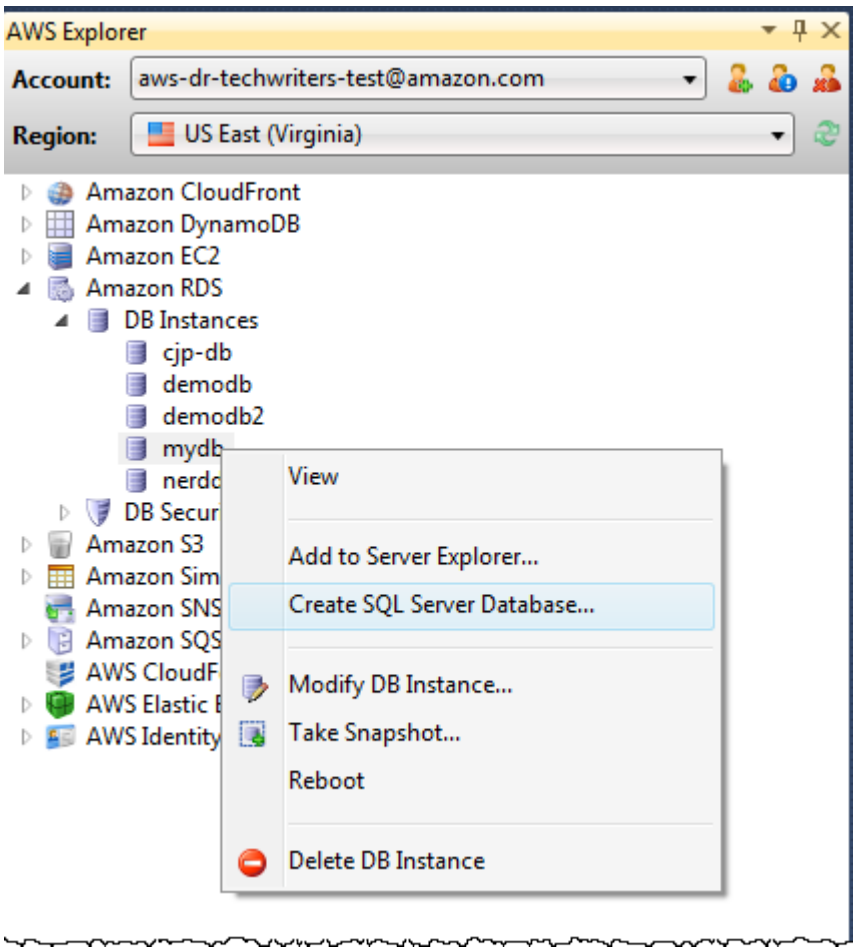
Erstellen einer Microsoft SQL Server-Datenbank in einer RDS-Instance

Microsoft SQL Server ist so konzipiert, dass Sie nach dem Start einer Amazon RDS-Instance eine SQL Server-Datenbank in der RDS-Instance erstellen müssen.

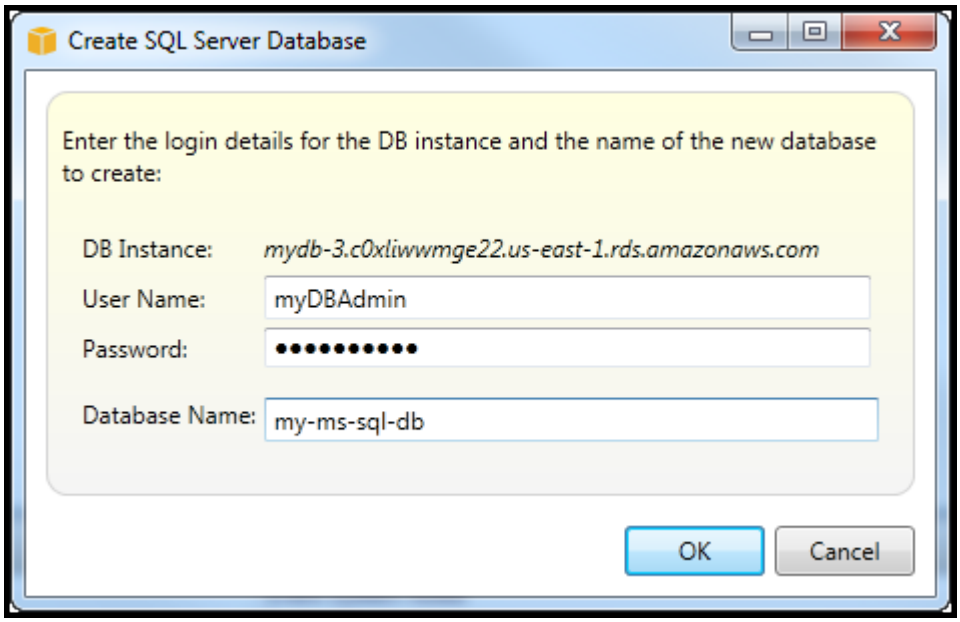
Informationen zum Erstellen einer Amazon RDS-Instance finden Sie unter Starten einer Amazon RDS-Datenbank-Instance.

So erstellen Sie eine Microsoft SQL Server-Datenbank:

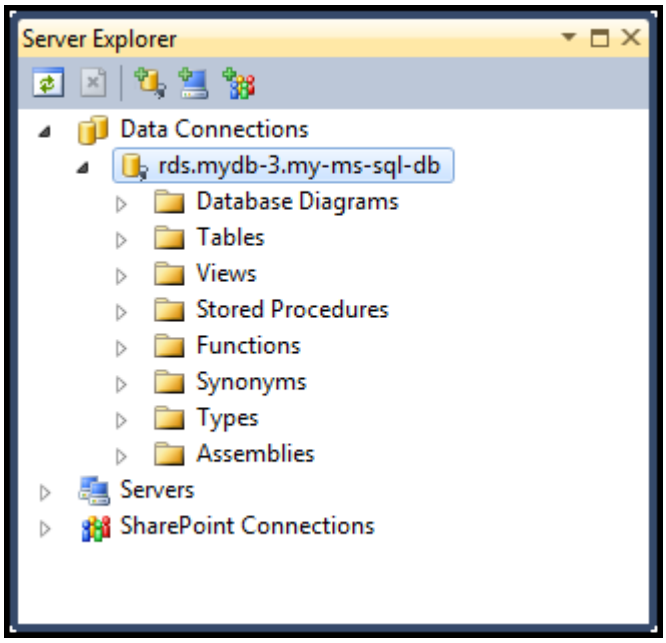
1. Öffnen Sie im AWS Explorer das Kontextmenü (Rechtsklick) für den Knoten, der Ihrer RDS-Instanz für Microsoft SQL Server entspricht, und wählen Sie Create SQL Server Database aus.



2. Geben Sie im Dialogfeld Create SQL Server Database (SQL Server-Datenbank erstellen) das beim Erstellen der RDS-Instance festgelegte Passwort sowie einen Namen für die Microsoft SQL Server-Datenbank ein und klicken Sie dann auf OK.



3. Das Toolkit for Visual Studio erstellt die Microsoft SQL Server-Datenbank und fügt sie dem Visual Studio Server Explorer hinzu.



Amazon RDS-Sicherheitsgruppen

Mit Amazon RDS-Sicherheitsgruppen können Sie den Netzwerkzugriff auf Ihre Amazon RDS-Instances verwalten. Bei Sicherheitsgruppen geben Sie Gruppen von IP-Adressen mithilfe der CIDR-Notation an, und nur Netzwerkverkehr, der von diesen Adressen ausgeht, wird von Ihrer Amazon RDS-Instance erkannt.

Obwohl sie auf ähnliche Weise funktionieren, unterscheiden sich Amazon RDS-Sicherheitsgruppen von EC2 Amazon-Sicherheitsgruppen. Es ist möglich, Ihrer EC2 RDS-Sicherheitsgruppe eine Sicherheitsgruppe hinzuzufügen. Alle EC2 Instances, die Mitglieder der EC2 Sicherheitsgruppe sind, können dann auf die RDS-Instances zugreifen, die Mitglieder der RDS-Sicherheitsgruppe sind.

Weitere Informationen zu Amazon RDS-Sicherheitsgruppen finden Sie unter RDS-Sicherheitsgruppen. Weitere Informationen zu EC2 Amazon-Sicherheitsgruppen finden Sie im EC2 Benutzerhandbuch.

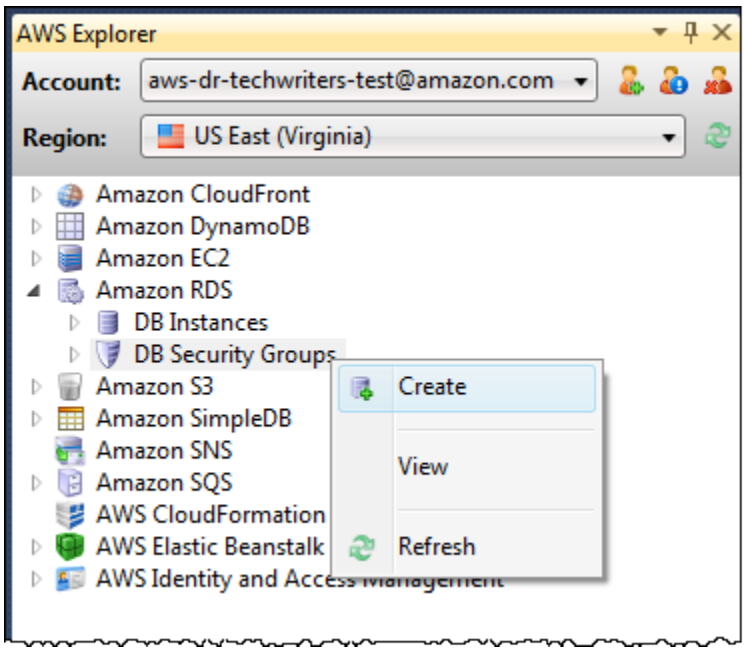
Erstellen Sie eine Amazon RDS-Sicherheitsgruppe

Sie können das Toolkit for Visual Studio verwenden, um eine RDS-Sicherheitsgruppe zu erstellen. Wenn Sie das AWS Toolkit verwenden, um eine RDS-Instanz zu starten, können Sie mit dem Assistenten eine RDS-Sicherheitsgruppe angeben, die mit Ihrer Instanz verwendet werden soll. Mit

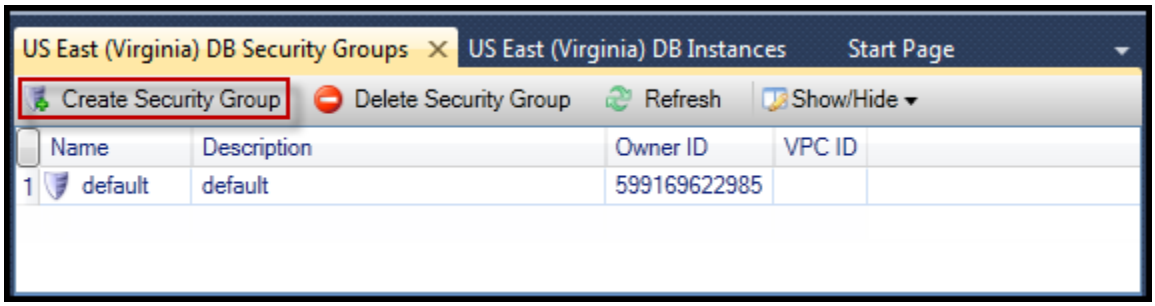
den folgenden Schritten können Sie diese Sicherheitsgruppe erstellen, bevor Sie den Assistenten starten.

So erstellen Sie eine Amazon RDS-Sicherheitsgruppe:

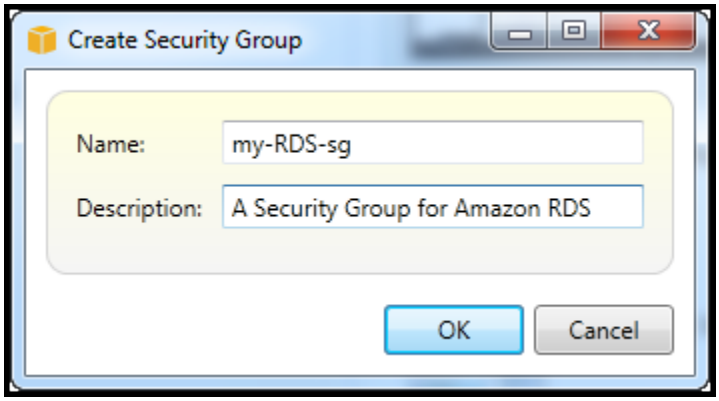
1. Erweitern Sie im AWS Explorer den Amazon RDS-Knoten, öffnen Sie das Kontextmenü (Rechtsklick) für den Unterknoten DB Security Groups und wählen Sie Create.



   Alternativ können Sie auf der Registerkarte Security Groups (Sicherheitsgruppen) die Option Create Security Group (Sicherheitsgruppe erstellen) auswählen. Wenn diese Registerkarte nicht angezeigt wird, öffnen Sie das Kontextmenü (Rechtsklick) für den DB Security Groups (DB-Sicherheitsgruppen)-Subknoten und wählen View (Anzeigen) aus.



2. Geben Sie im Dialogfeld Create Security Group (Sicherheitsgruppe erstellen) einen Namen und eine Beschreibung für die Sicherheitsgruppe ein und wählen Sie dann OK aus.



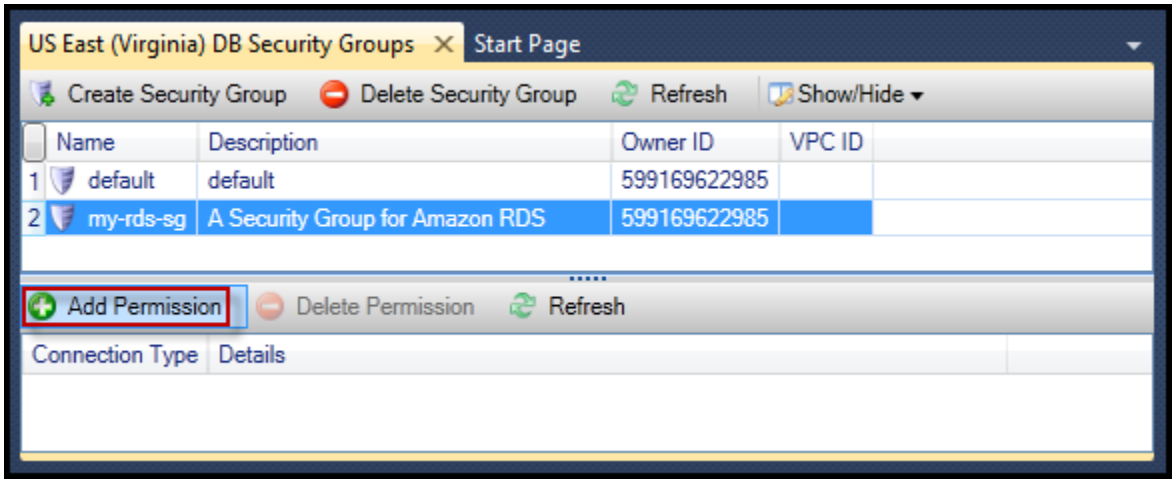
Zugriffsberechtigungen für eine Amazon RDS-Sicherheitsgruppe festlegen

Standardmäßig bietet eine neue Amazon RDS-Sicherheitsgruppe keinen Netzwerkzugriff. Um den Zugriff auf Amazon RDS-Instances zu aktivieren, die die Sicherheitsgruppe verwenden, verwenden Sie das folgende Verfahren, um deren Zugriffsberechtigungen festzulegen.

So konfigurieren Sie den Zugriff für eine Amazon RDS-Sicherheitsgruppe:

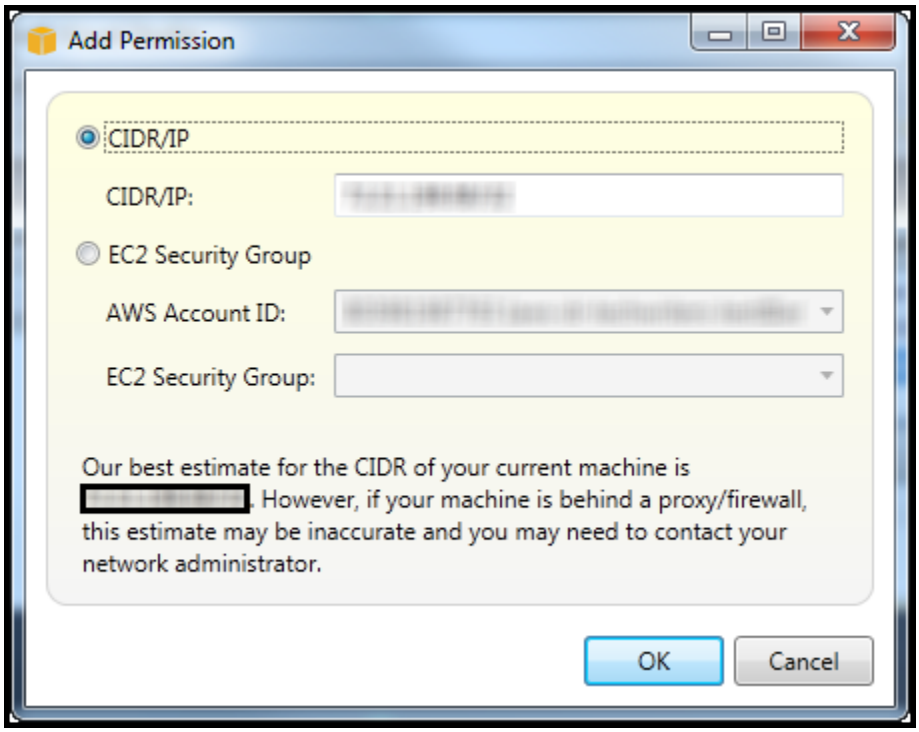
1. Wählen Sie auf der Registerkarte Security Groups (Sicherheitsgruppen) in der Listenansicht die Sicherheitsgruppe aus. Wenn die Sicherheitsgruppe nicht in der Liste angezeigt wird, wählen Sie Refresh (Aktualisieren) aus. Wenn Ihre Sicherheitsgruppe immer noch nicht in der Liste erscheint, stellen Sie sicher, dass Sie die Liste für die richtige AWS Region ansehen. Die Registerkarten für Sicherheitsgruppen im AWS Toolkit sind regionsspezifisch.

   Wenn keine Registerkarten für Sicherheitsgruppen angezeigt werden, öffnen Sie im AWS Explorer das Kontextmenü (mit der rechten Maustaste) für den Unterknoten DB-Sicherheitsgruppen und wählen Sie Ansicht aus.
2. Wählen Sie Add Permission (Berechtigung hinzufügen).



Schaltfläche Add Permissions (Berechtigungen hinzufügen) auf der Registerkarte Security Groups (Sicherheitsgruppen)

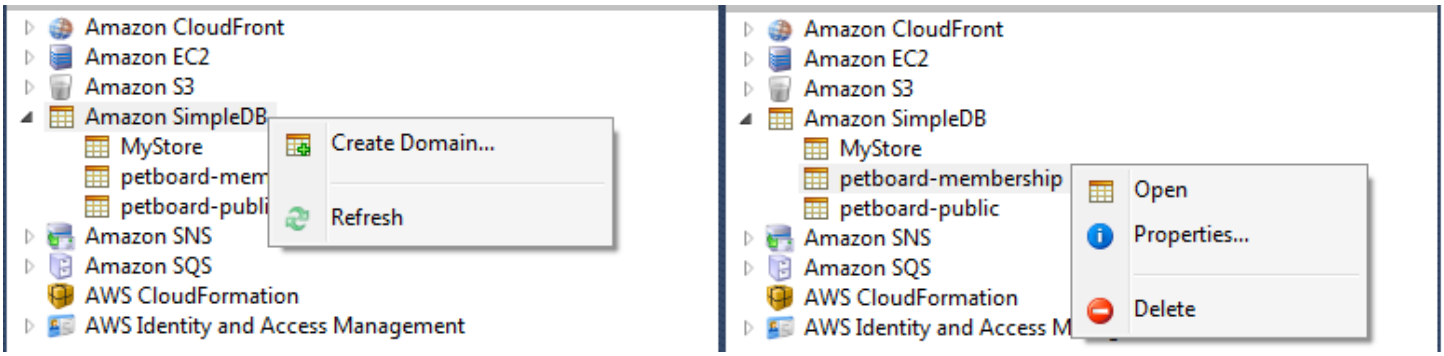
3. Im Dialogfeld „Berechtigung hinzufügen“ können Sie mithilfe der CIDR-Notation angeben, welche IP-Adressen auf Ihre RDS-Instance zugreifen können, oder Sie können angeben, welche EC2 Sicherheitsgruppen auf Ihre RDS-Instance zugreifen können. Wenn Sie EC2 Sicherheitsgruppe wählen, können Sie den Zugriff für alle EC2 Instances angeben, die einer AWS-Konto Zugriffsberechtigung zugeordnet sind, oder Sie können eine EC2 Sicherheitsgruppe aus der Dropdownliste auswählen.



Das AWS Toolkit versucht, Ihre IP-Adresse zu ermitteln und das Dialogfeld automatisch mit der entsprechenden CIDR-Spezifikation auszufüllen. Wenn Ihr Computer jedoch über eine Firewall auf das Internet zugreift, ist die vom Toolkit bestimmte CIDR möglicherweise nicht korrekt.

Amazon SimpleDB vom Explorer aus verwenden AWS

AWS Der Explorer zeigt alle Amazon SimpleDB-Domains an, die mit dem aktiven AWS Konto verknüpft sind. Im AWS Explorer können Sie Amazon SimpleDB-Domänen erstellen oder löschen.

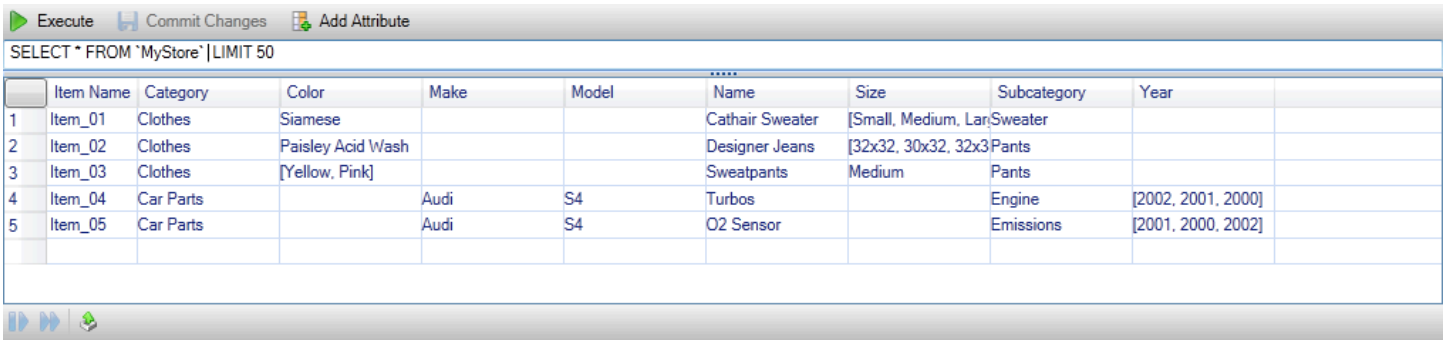


Create, delete, or open Amazon SimpleDB domains associated with your account

Ausführen von Abfragen und Bearbeiten der Ergebnisse

AWS Explorer kann auch eine Rasteransicht einer Amazon SimpleDB-Domain anzeigen, von der aus Sie die Elemente, Attribute und Werte in dieser Domain anzeigen können. Sie können Abfragen ausführen, um ausschließlich eine Teilmenge der Domänenelemente anzeigen zu lassen. Sie haben die Möglichkeit, die Werte für das entsprechende Attribut eines Elements zu bearbeiten, indem Sie auf eine Zelle doppelklicken. Sie können der Domäne auch neue Attribute hinzufügen.

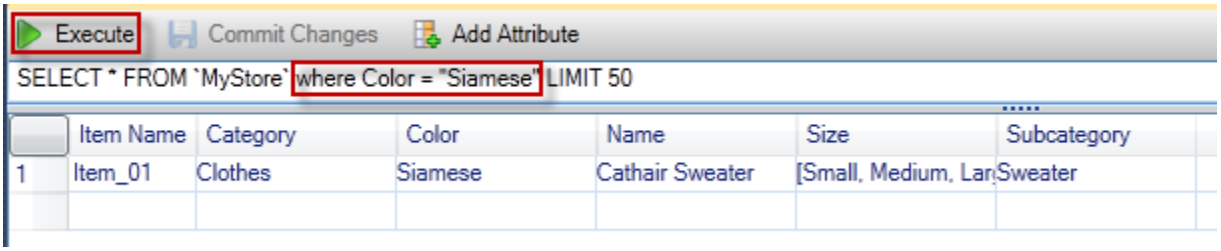
Die hier angezeigte Domain stammt aus dem Amazon SimpleDB SimpleDB-Beispiel, das im Lieferumfang von enthalten ist. AWS SDK für .NET



	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

Um eine Abfrage auszuführen, geben Sie diese in das Textfeld oben in der Rasteransicht ein und wählen dann Execute (Ausführen) aus. Die Ansicht wird so gefiltert, dass ausschließlich die Elemente angezeigt werden, die Ihrer Abfrage entsprechen.

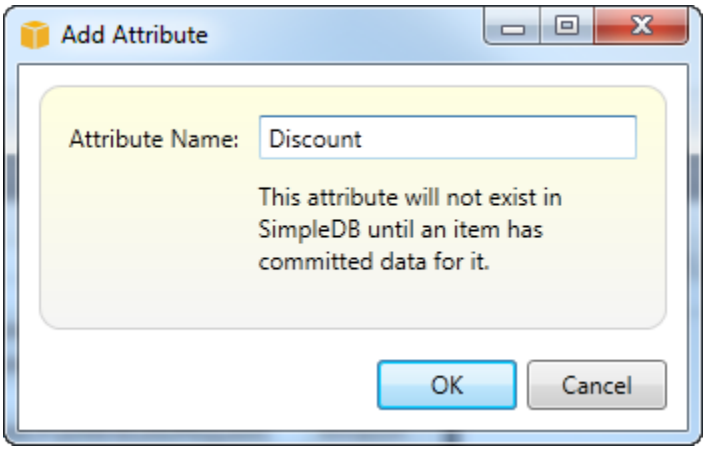


Execute query from AWS Explorer

Um die mit einem Attribut verknüpften Werte zu bearbeiten, doppelklicken Sie auf die entsprechende Zelle, bearbeiten die Werte und wählen dann Commit Changes (Änderungen commiten) aus.

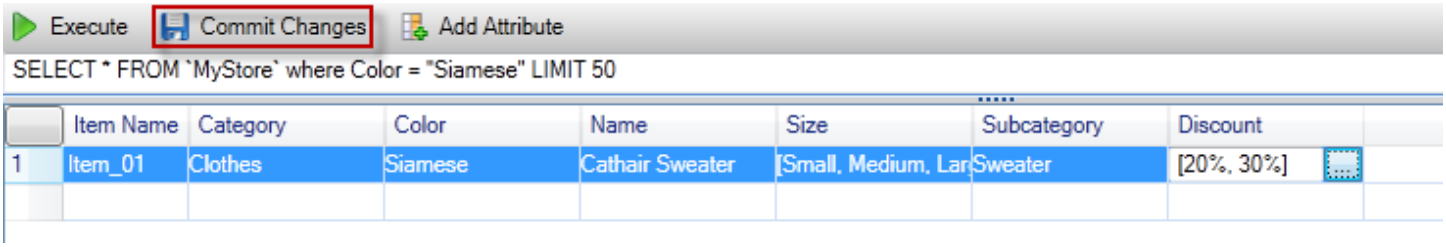
Hinzufügen eines Attributs

Wenn Sie ein Attribut hinzufügen möchten, wählen Sie oben in der Ansicht Add Attribute (Attribut hinzufügen) aus.



Attribut hinzufügen dialog box

Um das neue Attribut in die Domäne aufzunehmen, müssen Sie mindestens für ein Element einen Wert zum Attribut hinzufügen. Dann wählen Sie die Schaltfläche Commit Changes (Änderungen commiten) aus.



Commit changes for a new attribute

Paginierung von Abfrageergebnissen

Am unteren Rand der Ansicht sehen Sie drei Schaltflächen.

Paginate and export buttons

Mit den ersten beiden Schaltflächen können Sie Abfrageergebnisse paginieren. Die erste Schaltfläche zeigt eine zusätzliche Ergebnisseite an. Die zweite Schaltfläche zeigt 10 zusätzliche Ergebnisseiten an. In diesem Kontext entspricht eine Seite 100 Zeilen oder der Anzahl der Ergebnisse, die mit dem LIMIT-Wert wurde, wenn dieser in der Abfrage enthalten ist.

Exportieren in CSV

Die letzte Schaltfläche exportiert die aktuellen Ergebnisse in eine CSV-Datei.

Amazon SQS vom Explorer aus AWS verwenden

Amazon Simple Queue Service (Amazon SQS) ist ein flexibler Warteschlangenservice, der die Nachrichtenübertragung zwischen verschiedenen Ausführungsprozessen in einer Softwareanwendung ermöglicht. Amazon SQS SQS-Warteschlangen befinden sich in der AWS Infrastruktur, aber die Prozesse, die Nachrichten weiterleiten, können sich lokal, auf EC2 Amazon-Instances oder auf einer Kombination davon befinden. Amazon SQS ist ideal für die Koordination der Arbeitsverteilung auf mehrere Computer.

Mit dem Toolkit for Visual Studio können Sie Amazon SQS SQS-Warteschlangen anzeigen, die dem aktiven Konto zugeordnet sind, Warteschlangen erstellen und löschen und Nachrichten über Warteschlangen senden. (Mit aktivem Konto meinen wir das im Explorer ausgewählte Konto.) AWS

Weitere Informationen zu Amazon SQS finden Sie in der Dokumentation unter Einführung in SQS. AWS

Erstellen einer Warteschlange

Sie können im AWS Explorer eine Amazon SQS SQS-Warteschlange erstellen. Der ARN und die URL für die Warteschlange basieren auf der Kontonummer des aktiven Kontos und dem bei der Erstellung angegebenen Warteschlangennamen.

So erstellen Sie eine Warteschlange

1. Öffnen Sie im AWS Explorer das Kontextmenü (Rechtsklick) für den Amazon SQS-Knoten und wählen Sie dann Create Queue.
2. Geben Sie im Dialogfeld Create Queue (Warteschlange erstellen) den Warteschlangennamen, den Standardwert der Zeitbeschränkung für die Sichtbarkeit sowie den Standardwert für die Bereitstellungsverzögerung an. Die Standardwerte der Zeitbeschränkung für die Sichtbarkeit sowie der Bereitstellungsverzögerung werden in Sekunden angegeben. Die Standardzeitbeschränkung für die Sichtbarkeit ist die Zeitspanne, in der eine Mitteilung für potenzielle Empfangsprozesse sichtbar ist, nachdem ein bestimmter Prozess die Mitteilung übernommen hat. Die Standardbereitstellungsverzögerung ist die Zeitspanne ab dem Senden der Mitteilung bis zu ihrem ersten Anzeigen in potenziellen Empfangsprozessen.
3. Wählen Sie OK aus. Die neue Warteschlange erscheint als Subknoten unter dem Amazon SQS-Knoten.

Löschen einer Warteschlange

Sie können bestehende Warteschlangen aus dem AWS Explorer löschen. Wenn Sie eine Warteschlange löschen, ist keine der mit dieser Warteschlange verknüpften Mitteilungen mehr verfügbar.

So löschen Sie eine Warteschlange

1. Öffnen Sie im AWS Explorer die Kontextmenüs (Rechtsklick) für die Warteschlange, die Sie löschen möchten, und wählen Sie dann Löschen.

Verwalten von Warteschlangeneigenschaften

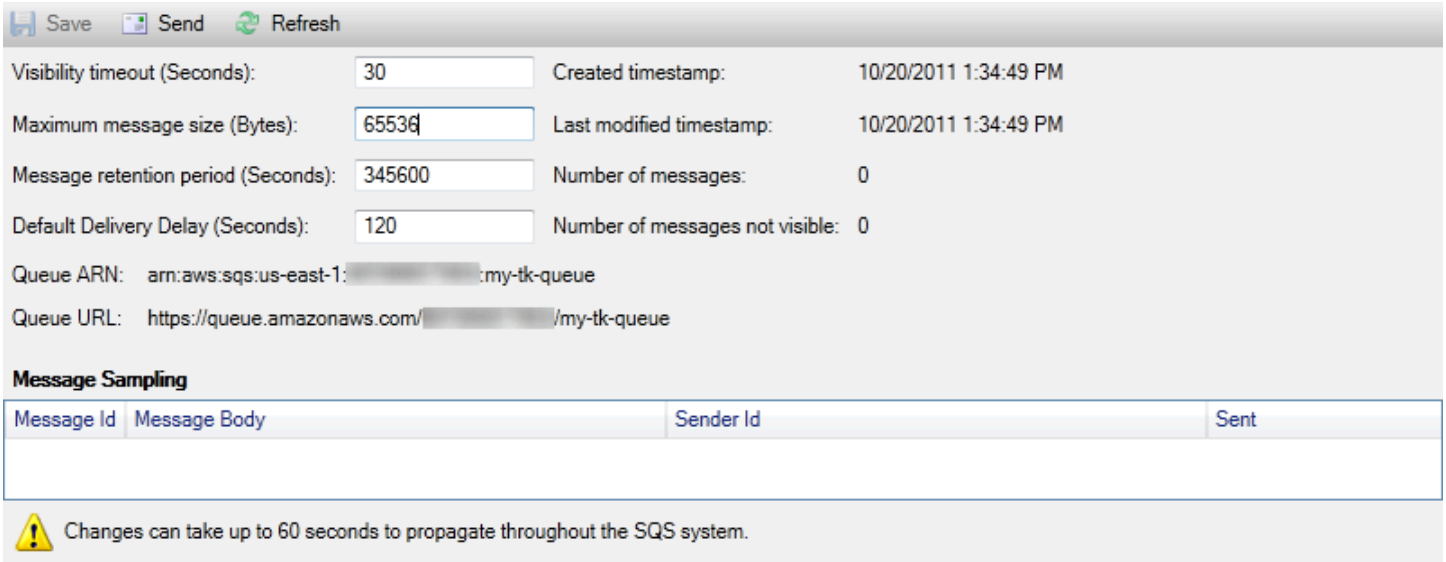
Sie können die Eigenschaften für jede der im AWS Explorer angezeigten Warteschlangen anzeigen und bearbeiten. Außerdem können Sie in dieser Eigenschaftenansicht Mitteilungen an die Warteschlange senden.

So verwalten Sie Warteschlangeneigenschaften:

- Öffnen Sie im AWS Explorer das Kontextmenü (Rechtsklick) für die Warteschlange, deren Eigenschaften Sie verwalten möchten, und wählen Sie dann Warteschlange anzeigen.

  In der Eigenschaftenansicht der Warteschlange können Sie die Zeitbeschränkung für die Sichtbarkeit, die maximale Mitteilungsgröße, den Aufbewahrungszeitraum sowie die

Standardbereitstellungsverzögerung bearbeiten. Die Standardbereitstellungsverzögerung kann außer Kraft gesetzt werden, wenn Sie eine Mitteilung senden. Im folgenden Screenshot handelt es sich beim verdeckten Text um die Kontonummernkomponente des ARN und der URL der Warteschlange.



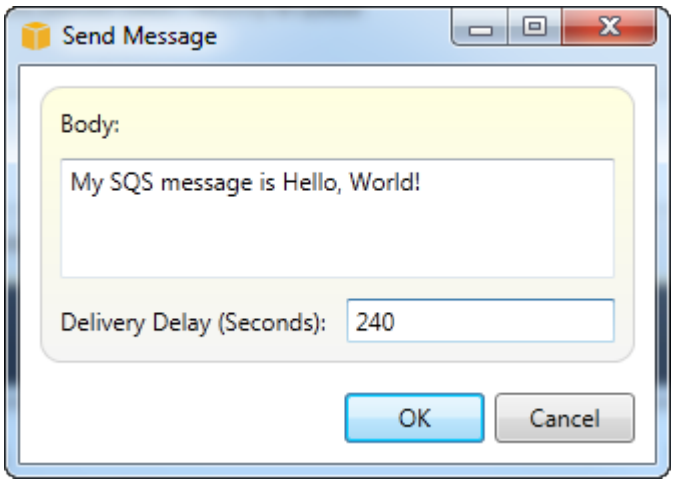
SQS queue properties view

Senden einer Mitteilung an eine Warteschlange

Sie können in der Warteschlangen-Eigenschaftenansicht Mitteilungen an die Warteschlange senden.

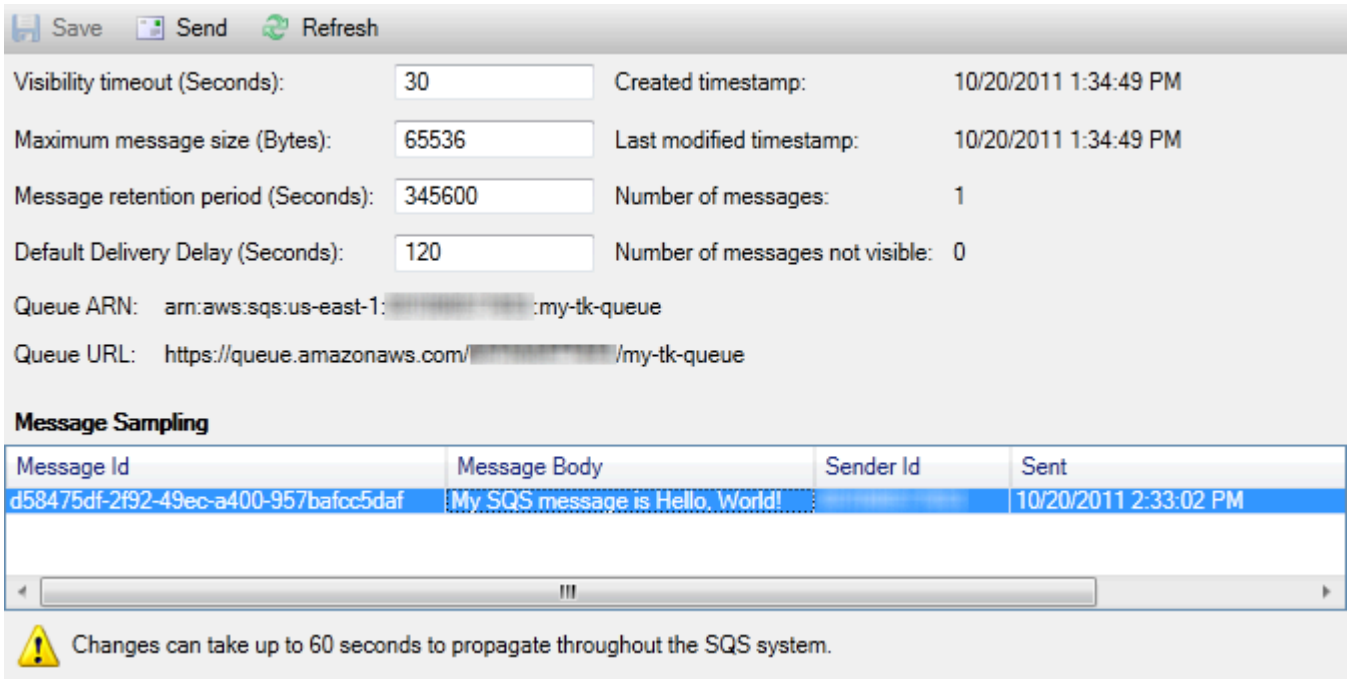
So senden Sie eine Nachricht

1. Wählen Sie oben in der Warteschlangen-Eigenschaftenansicht die Schaltfläche Send (Senden) aus.
2. Geben Sie die Mitteilung ein. (Optional) Geben Sie einen Wert für die Bereitstellungsverzögerung ein, mit dem der Standardwert für die Warteschlange überschrieben wird. Im folgenden Beispiel wurde die Verzögerung mit einem Wert von 240 Sekunden überschrieben Wählen Sie OK aus.



Nachricht senden dialog box

3. Warten Sie ungefähr 240 Sekunden (vier Minuten). Die Nachricht wird im Abschnitt Message Sampling (Nachrichten-Sampling) der Warteschlangen-Eigenschaftenansicht angezeigt.



SQS properties view with sent message

Beim Zeitstempel in der Warteschlangen-Eigenschaftenansicht handelt es sich um die Uhrzeit, zu der Sie die Schaltfläche Send (Senden) geklickt haben. Im Zeitstempel ist die Verzögerung nicht mit eingeschlossen. Daher kann die Uhrzeit, zu der die Mitteilung in der Warteschlange erscheint und für die Empfänger verfügbar ist, eine spätere sein als die des Zeitstempels. Der Zeitstempel wird in der Ortszeit ihres Computers angezeigt.

Identitäts- und Zugriffsverwaltung

AWS Identity and Access Management (IAM) ermöglicht es Ihnen, den Zugriff auf Ihre AWS-Konten und Ressourcen sicherer zu verwalten. Mit IAM können Sie mehrere Benutzer in Ihrem Hauptbenutzer (Root) erstellen. AWS-Konto Diese Benutzer können ihre eigenen Anmeldeinformationen haben: Passwort, Zugriffsschlüssel-ID und geheimer Schlüssel, aber alle IAM-Benutzer teilen sich eine einzige Kontonummer.

Sie können die Ressourcenzugriffsebene jedes IAM-Benutzers verwalten, indem Sie dem Benutzer IAM-Richtlinien zuordnen. Sie können beispielsweise einem IAM-Benutzer eine Richtlinie zuordnen, die dem Benutzer Zugriff auf den Amazon S3 S3-Service und die zugehörigen Ressourcen in Ihrem Konto gewährt, die jedoch keinen Zugriff auf andere Dienste oder Ressourcen gewährt.

Für eine effizientere Zugriffsverwaltung können Sie IAM-Gruppen erstellen, bei denen es sich um Sammlungen von Benutzern handelt. Wenn Sie der Gruppe eine Richtlinie zuweisen, wird sie auf alle Benutzer angewendet, die Mitglied der Gruppe sind.

Neben der Verwaltung von Berechtigungen auf Benutzer- und Gruppenebene unterstützt IAM auch das Konzept der IAM-Rollen. Wie Benutzer und Gruppen können Sie auch IAM-Rollen Richtlinien zuordnen. Anschließend können Sie die IAM-Rolle einer EC2 Amazon-Instance zuordnen. Anwendungen, die auf der EC2 Instance ausgeführt werden, können AWS mithilfe der von der IAM-Rolle bereitgestellten Berechtigungen darauf zugreifen. Weitere Informationen zum Verwenden von IAM-Rollen mit dem Toolkit finden Sie unter Create an IAM Role. Weitere Informationen zu IAM finden Sie im IAM-Benutzerhandbuch.

Erstellen und Konfigurieren eines IAM-Benutzers

Mit IAM-Benutzern können Sie anderen Zugriff auf Ihre Daten gewähren. AWS-Konto Indem Sie IAM-Benutzern Richtlinien zuordnen, können Sie genau festlegen, auf welche Ressourcen ein IAM-Benutzer Zugriff hat und welche Vorgänge er mit diesen Ressourcen durchführen darf.

Es hat sich bewährt, dass alle Benutzer, die auf ein zugreifen, dies als IAM-Benutzer tun AWS-Konto sollten — auch der Besitzer des Kontos. Dadurch wird sichergestellt, dass, wenn die Anmeldeinformationen für einen der IAM-Benutzer kompromittiert werden, nur diese Anmeldeinformationen deaktiviert werden können. Es ist nicht notwendig, die Root-Anmeldeinformationen für das Konto zu deaktivieren oder zu ändern.

Im Toolkit for Visual Studio können Sie einem IAM-Benutzer Berechtigungen zuweisen, indem Sie dem Benutzer entweder eine IAM-Richtlinie anhängen oder den Benutzer einer Gruppe zuweisen.

IAM-Benutzer, die einer Gruppe zugewiesen sind, leiten ihre Berechtigungen aus den Richtlinien ab, die der Gruppe zugewiesen sind. Weitere Informationen finden Sie unter Create an IAM Group (Erstellen einer IAM-Gruppe) und Add an IAM User to an IAM Group (Hinzufügen eines IAM-Benutzers zu einer IAM-Gruppe).

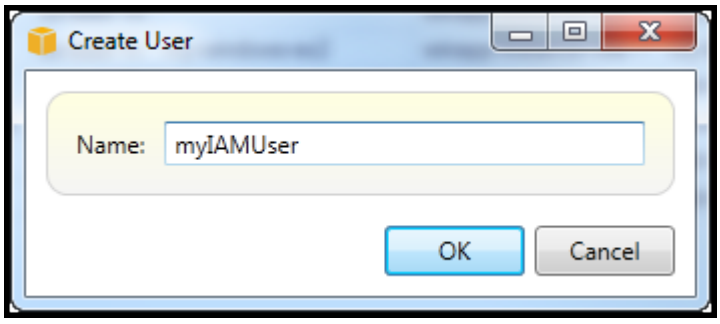
Mit dem Toolkit for Visual Studio können Sie auch AWS Anmeldeinformationen (Zugriffsschlüssel-ID und geheimer Schlüssel) für den IAM-Benutzer generieren. Weitere Informationen finden Sie unter Generate Credentials for an IAM User.

Das Toolkit for Visual Studio unterstützt die Angabe von IAM-Benutzeranmeldeinformationen für den Zugriff auf Dienste über AWS Explorer. Da IAM-Benutzer in der Regel keinen vollen Zugriff auf alle Amazon Web Services haben, sind einige Funktionen im AWS Explorer möglicherweise nicht verfügbar. Wenn Sie den AWS Explorer verwenden, um Ressourcen zu ändern, während das aktive Konto ein IAM-Benutzer ist, und dann das aktive Konto auf das Root-Konto umstellen, sind die Änderungen möglicherweise erst sichtbar, wenn Sie die Ansicht im AWS Explorer aktualisieren. Um die Anzeige zu aktualisieren, wählen Sie die Schaltfläche „Refresh ()“ aus.

Informationen zur Konfiguration von IAM-Benutzern über finden Sie unter Arbeiten mit Benutzern und Gruppen im IAM-Benutzerhandbuch. AWS Management Console

So erstellen Sie einen IAM-Benutzer

1. Erweitern Sie im AWS Explorer den AWS Identity and Access ManagementKnoten, öffnen Sie das Kontextmenü (Rechtsklick) für Benutzer und wählen Sie dann Create User aus.
2. Geben Sie im Dialogfeld „Benutzer erstellen“ einen Namen für den IAM-Benutzer ein und wählen Sie „OK“. Dies ist der IAM-freundliche Name. Informationen zu Namensbeschränkungen für IAM-Benutzer finden Sie im IAM-Benutzerhandbuch.



Create an IAM user

Der neue Benutzer wird als Unterknoten unter Benutzer unter dem Knoten angezeigt. AWS Identity and Access Management

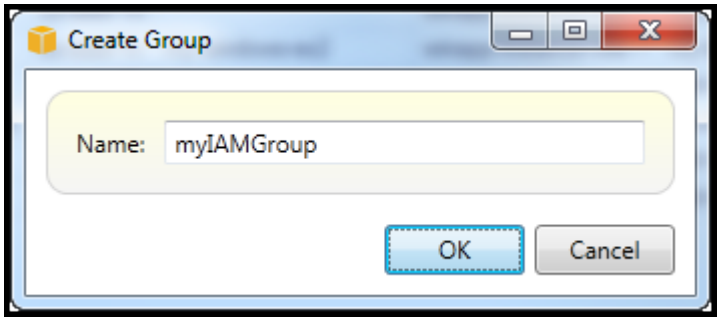
Informationen zum Erstellen einer Richtlinie und zum Zuweisen dieser zu einem Benutzer finden Sie unter Create an IAM Policy.

Erstellen einer IAM-Gruppe

Gruppen bieten eine Möglichkeit, IAM-Richtlinien auf eine Sammlung von Benutzern anzuwenden. Informationen zur Verwaltung von IAM-Benutzern und -Gruppen finden Sie unter Arbeiten mit Benutzern und Gruppen im IAM-Benutzerhandbuch.

So erstellen Sie eine IAM-Gruppe

1. Öffnen Sie im AWS Explorer unter Identity and Access Management das Kontextmenü (Rechtsklick) für Gruppen und wählen Sie Gruppe erstellen aus.
2. Geben Sie im Dialogfeld „Gruppe erstellen“ einen Namen für die IAM-Gruppe ein und wählen Sie „OK“.



Create IAM group

Die neue IAM-Gruppe wird unter dem Unterknoten Gruppen von Identity and Access Management angezeigt.

Informationen zum Erstellen einer Richtlinie und zum Anhängen dieser Richtlinie an die IAM-Gruppe finden Sie unter Erstellen einer IAM-Richtlinie.

Hinzufügen eines IAM-Benutzers zu einer IAM-Gruppe

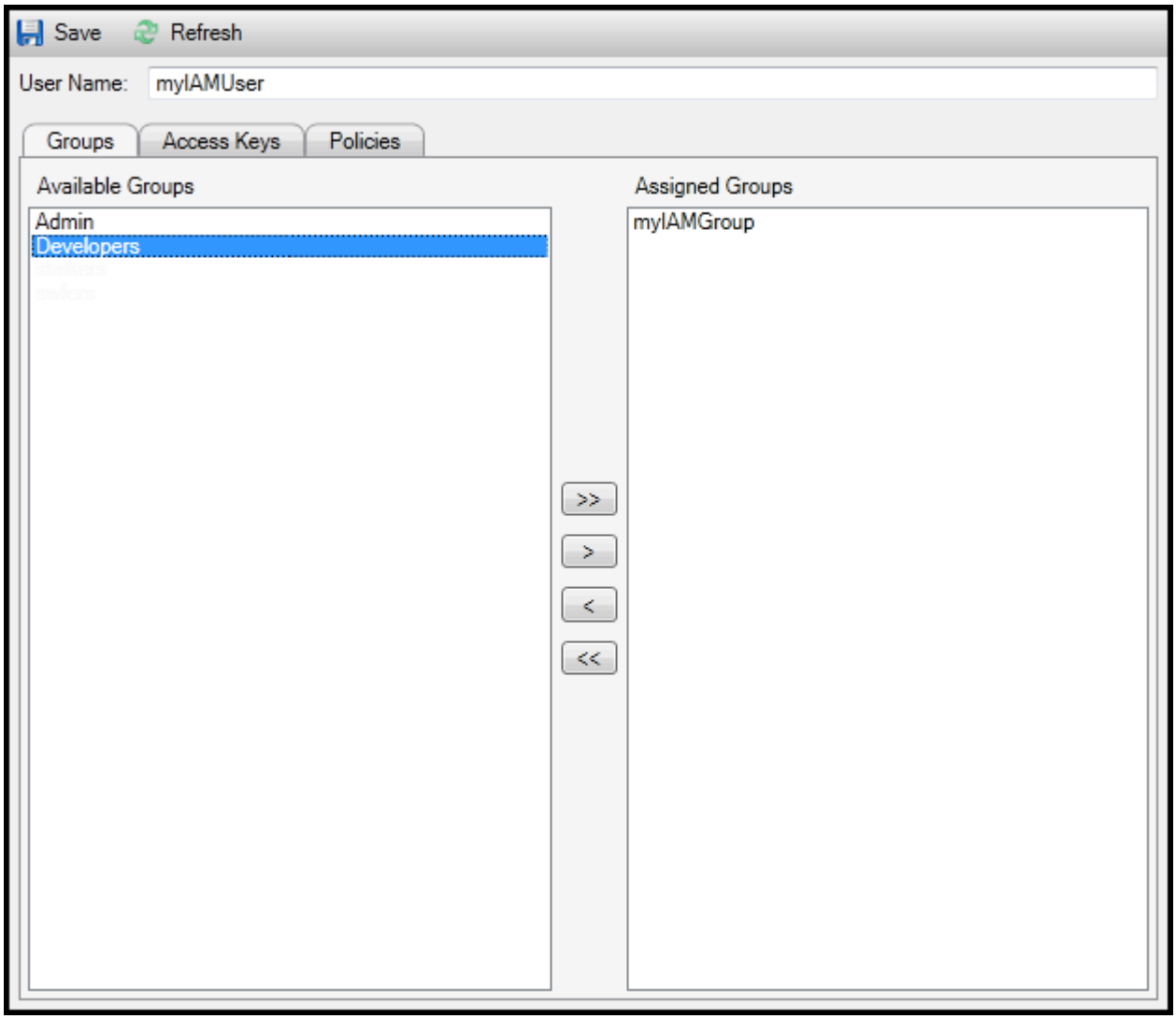
IAM-Benutzer, die Mitglieder einer IAM-Gruppe sind, erhalten Zugriffsberechtigungen aus den Richtlinien, die der Gruppe zugeordnet sind. Der Zweck einer IAM-Gruppe besteht darin, die Verwaltung von Berechtigungen für eine Sammlung von IAM-Benutzern zu vereinfachen.

Informationen darüber, wie die einer IAM-Gruppe zugewiesenen Richtlinien mit den Richtlinien interagieren, die IAM-Benutzern zugewiesen sind, die Mitglieder dieser IAM-Gruppe sind, finden Sie im IAM-Benutzerhandbuch unter Verwaltung von IAM-Richtlinien.

Im AWS Explorer fügen Sie IAM-Benutzer über den Unterknoten Benutzer und nicht über den Unterknoten Gruppen zu IAM-Gruppen hinzu.

So fügen Sie einen IAM-Benutzer einer IAM-Gruppe hinzu

1. Öffnen Sie im AWS Explorer unter Identity and Access Management das Kontextmenü (Rechtsklick) für Benutzer und wählen Sie Bearbeiten.



Assign an IAM user to a IAM group

2. Im linken Bereich der Registerkarte Gruppen werden die verfügbaren IAM-Gruppen angezeigt. Im rechten Bereich werden die Gruppen angezeigt, in denen der angegebene IAM-Benutzer bereits Mitglied ist.

Um den IAM-Benutzer zu einer Gruppe hinzuzufügen, wählen Sie im linken Bereich die IAM-Gruppe und dann die Schaltfläche **>** aus.

Um den IAM-Benutzer aus einer Gruppe zu entfernen, wählen Sie im rechten Bereich die IAM-Gruppe aus und klicken Sie dann auf die Schaltfläche **<**.

Um den IAM-Benutzer allen IAM-Gruppen hinzuzufügen, wählen Sie die Schaltfläche **>>**. Um den IAM-Benutzer aus allen Gruppen zu entfernen, klicken Sie auf ähnliche Weise auf die Schaltfläche **<<**.

Um mehrere Gruppen auszuwählen, wählen Sie sie nacheinander aus. Sie müssen nicht die STRG-Taste gedrückt halten. Wenn Sie eine Gruppe aus Ihrer Auswahl entfernen möchten, wählen Sie einfach ein zweites Mal aus.

3. Wenn Sie mit der Zuweisung des IAM-Benutzers zu IAM-Gruppen fertig sind, wählen Sie Speichern.

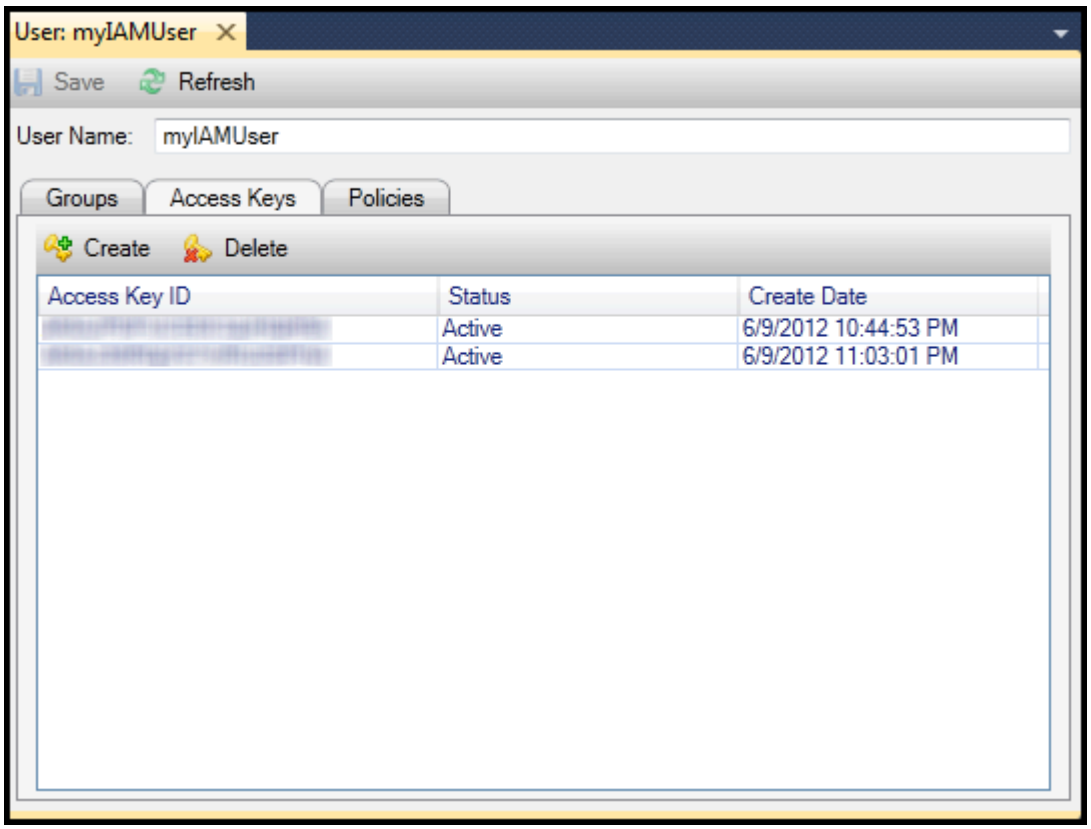
Generieren Sie Anmeldeinformationen für einen IAM-Benutzer

Mit Toolkit for Visual Studio können Sie die Zugriffsschlüssel-ID und den geheimen Schlüssel generieren, die für API-Aufrufe verwendet werden. AWS Diese Schlüssel können auch für den Zugriff auf Amazon Web Services über das Toolkit angegeben werden. Weitere Informationen zum Angeben von Anmeldeinformationen für die Verwendung mit dem Toolkit finden Sie unter „Anmeldeinformationen“. Weitere Informationen zum sicheren Umgang mit Anmeldeinformationen finden Sie unter Bewährte Methoden für die Verwaltung von AWS Zugriffsschlüsseln.

Das Toolkit kann nicht verwendet werden, um ein Passwort für einen IAM-Benutzer zu generieren.

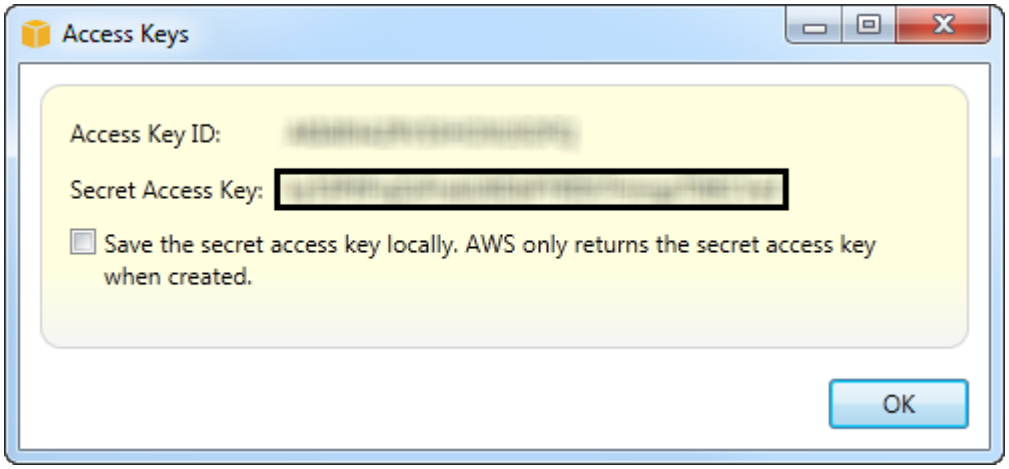
So generieren Sie Anmeldeinformationen für einen IAM-Benutzer

1. Öffnen Sie im AWS Explorer das Kontextmenü (Rechtsklick) für einen IAM-Benutzer und wählen Sie Bearbeiten.



2. Wählen Sie zum Generieren von Anmeldeinformationen auf der Registerkarte Access Keys (Zugriffsschlüssel) die Option Create (Erstellen) aus.

   Sie können nur zwei Sätze von Anmeldeinformationen pro IAM-Benutzer generieren. Wenn Sie bereits zwei Sätze von Anmeldeinformationen generiert haben und einen weiteren erstellen möchten, müssen Sie zunächst einen der vorhandenen Sätze löschen.

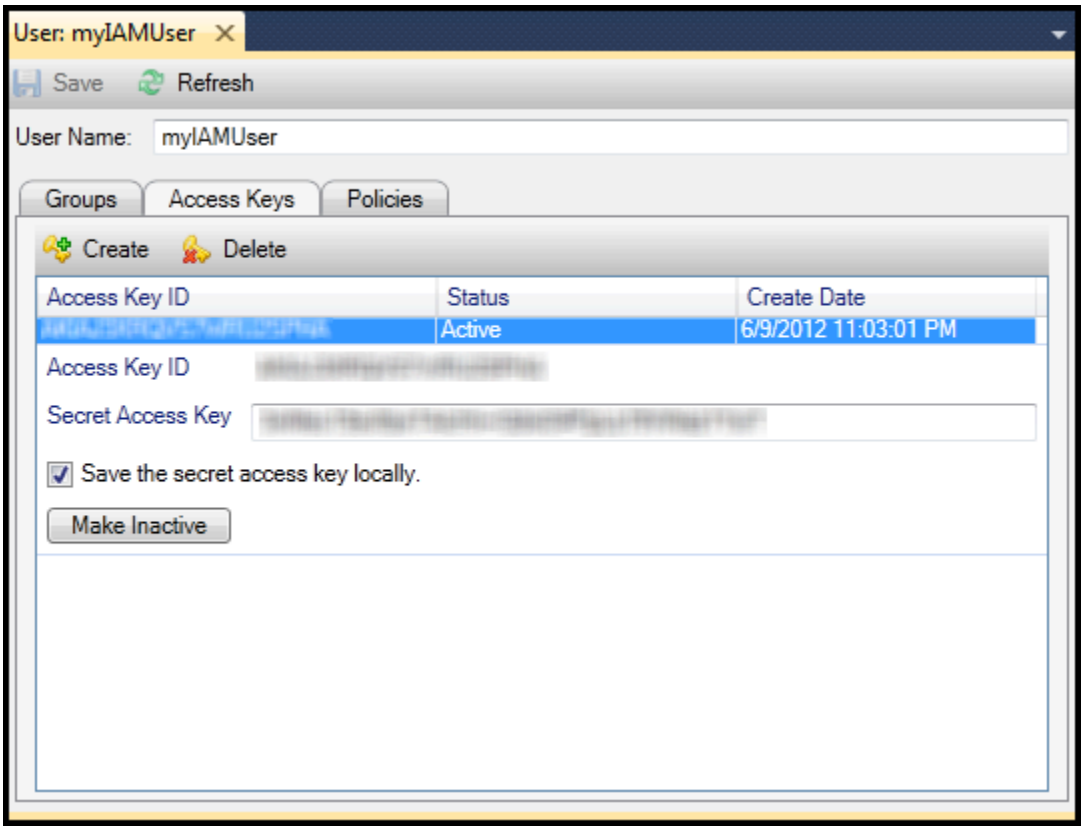


   reate credentials for IAM user

Wenn Sie möchten, dass das Toolkit eine verschlüsselte Kopie Ihres geheimen Zugriffsschlüssels auf Ihrem lokalen Laufwerk speichert, wählen Sie Geheimen Zugriffsschlüssel lokal speichern aus. AWS gibt den geheimen Zugriffsschlüssel nur zurück, wenn er erstellt wurde. Sie können den geheimen Zugriffsschlüssel auch im Dialogfeld kopieren und an einem sicheren Ort speichern.

3. Wählen Sie OK aus.

Nachdem Sie die Anmeldeinformationen generiert haben, können Sie diese auf der Registerkarte Access Keys (Zugriffsschlüssel) anzeigen. Wenn Sie die Option zur lokalen Speicherung des geheimen Schlüssels durch das Toolkit auswählen, wird er hier angezeigt.



Create credentials for IAM user

Wenn Sie den geheimen Schlüssel selbst gespeichert haben und möchten, dass das Toolkit diesen auch speichert, geben Sie den geheimen Zugriffsschlüssel im Feld Secret Access Key (Secret-Zugriffsschlüssel) ein und wählen dann Save the secret access key locally (Zugriffsschlüssel lokal speichern) aus.

Zum Deaktivieren der Anmeldeinformationen wählen Sie Make Inactive (Interaktiv) aus. (Sie können dies tun, wenn Sie vermuten, dass die Anmeldeinformationen kompromittiert wurden. Sie können die Anmeldeinformationen erneut aktivieren, wenn Sie die Zusicherung erhalten, dass sie sicher sind.)

Erstellen einer IAM-Rolle

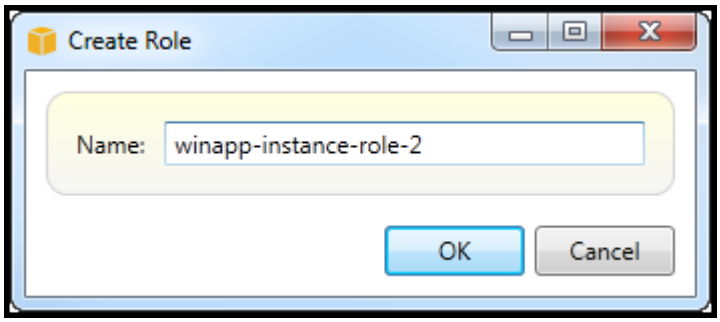
Das Toolkit for Visual Studio unterstützt die Erstellung und Konfiguration von IAM-Rollen. Genau wie bei Benutzern und Gruppen können Sie Richtlinien an IAM-Rollen anhängen. Anschließend können Sie die IAM-Rolle einer EC2 Amazon-Instance zuordnen. Die Zuordnung zur EC2 Instance erfolgt über ein Instance-Profil, das ein logischer Container für die Rolle ist. Anwendungen, die auf der EC2 Instance ausgeführt werden, erhalten automatisch die Zugriffsebene, die in der mit der IAM-Rolle verknüpften Richtlinie festgelegt ist. Dies gilt auch dann, wenn die Anwendung keine anderen AWS Anmeldeinformationen angegeben hat.

Sie können beispielsweise eine Rolle erstellen und dieser Rolle eine Richtlinie zuordnen, die den Zugriff nur auf Amazon S3 beschränkt. Nachdem Sie diese Rolle einer EC2 Instance zugewiesen haben, können Sie eine Anwendung auf dieser Instance ausführen. Die Anwendung hat dann Zugriff auf Amazon S3, jedoch nicht auf andere Dienste oder Ressourcen. Der Vorteil dieses Ansatzes besteht darin, dass Sie sich nicht um die sichere Übertragung und Speicherung von AWS Anmeldeinformationen auf der EC2 Instance kümmern müssen.

Weitere Informationen zu IAM-Rollen finden Sie unter Arbeiten mit IAM-Rollen im IAM-Benutzerhandbuch. Beispiele für den Zugriff auf Programme AWS mithilfe der mit einer EC2 Amazon-Instance verknüpften IAM-Rolle finden Sie in den AWS Entwicklerhandbüchern für Java, .NET, PHP und Ruby (Anmeldeinformationen mithilfe von IAM einrichten, IAM-Rolle erstellen und Mit IAM-Richtlinien arbeiten).

So erstellen Sie eine IAM-Rolle

1. Öffnen Sie im AWS Explorer unter Identity and Access Management das Kontextmenü (Rechtsklick) für Rollen und wählen Sie dann Rollen erstellen aus.
2. Geben Sie im Dialogfeld „Rolle erstellen“ einen Namen für die IAM-Rolle ein und klicken Sie auf OK.



Create IAM role

Die neue IAM-Rolle wird unter Rollen in Identity and Access Management angezeigt.

Weitere Informationen zum Erstellen einer Richtlinie und zum Zuweisen dieser zu einer Rolle finden Sie unter Create an IAM Policy.

Erstellen einer IAM-Richtlinie

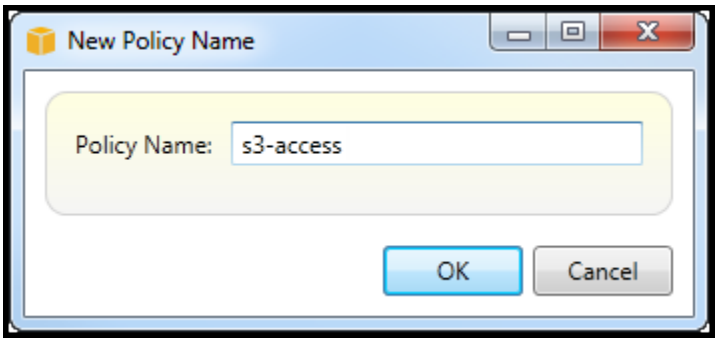
Richtlinien sind für IAM von grundlegender Bedeutung. Richtlinien können IAM-Entitäten wie Benutzern, Gruppen oder Rollen zugeordnet werden. Richtlinien geben die Zugriffsebene für einen Benutzer, eine Gruppe oder eine Rolle an.

So erstellen Sie eine IAM-Richtlinie

Erweitern Sie im AWS Explorer den AWS Identity and Access ManagementKnoten und dann den Knoten für den Entitätstyp (Gruppen, Rollen oder Benutzer), an den Sie die Richtlinie anhängen möchten. Öffnen Sie beispielsweise ein Kontextmenü für eine IAM-Rolle und wählen Sie Bearbeiten aus.

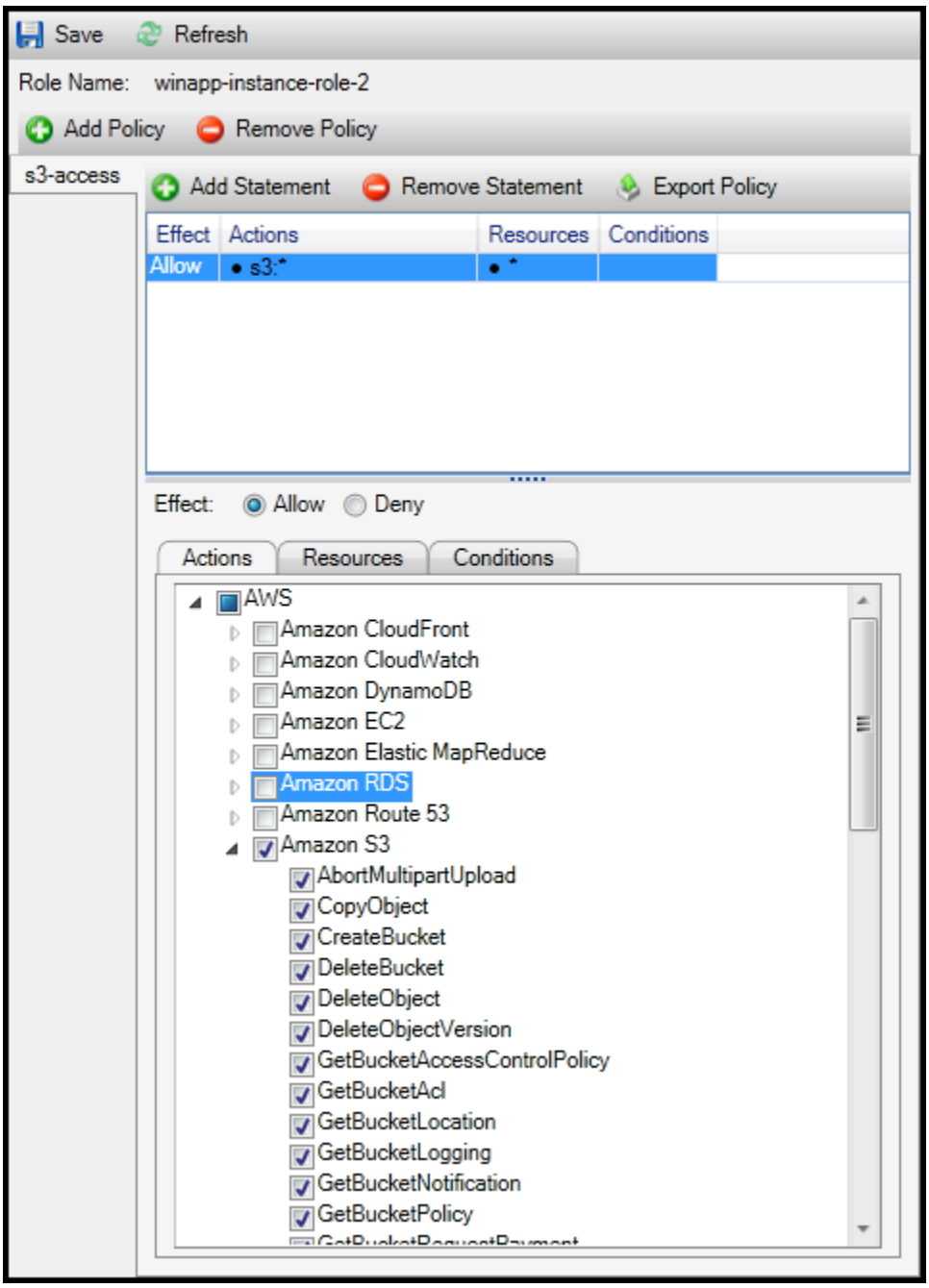
Ein mit der Rolle verknüpfter Tab wird im AWS Explorer angezeigt. Wählen Sie den Link Add Policy (Richtlinie hinzufügen) aus.

Geben Sie im Dialogfeld Policy Name (Richtlinienname) einen Namen für die Richtlinie ein (zum Beispiel s3-access).



New Policy Name dialog box

Fügen Sie im Richtlinieneditor Richtlinienanweisungen hinzu, um die Zugriffsebene anzugeben, die der Rolle gewährt werden soll (in diesem Beispiel winapp-instance-role -2), die der Richtlinie zugeordnet ist. In diesem Beispiel bietet eine Richtlinie vollen Zugriff auf Amazon S3, aber keinen Zugriff auf andere Ressourcen.



Specify IAM policy

Für eine genauere Zugriffskontrolle können Sie die Unterknoten im Richtlinien-Editor erweitern, um Aktionen im Zusammenhang mit Amazon Web Services zuzulassen oder zu verbieten.

Wenn Sie die Richtlinie bearbeitet haben, wählen Sie den Link Save (Speichern) aus.

AWS Lambda

Entwickeln und implementieren Sie Ihre .NET Core-basierten C#-Lambda-Funktionen mit dem. AWS Toolkit for Visual Studio AWS Lambda ist ein Rechendienst, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Das Toolkit for Visual Studio AWS Lambda enthält.NET Core-Projektvorlagen für Visual Studio.

Weitere Informationen zu AWS Lambda finden Sie im AWS Lambda Developer Guide.

Weitere Informationen zu.NET Core finden Sie im Microsoft.NET Core-Handbuch. Weitere Informationen zu .NET Core-Voraussetzungen und Installationsanweisungen für Windows-, macOS- und Linux-Plattformen finden Sie unter .NET Core Downloads.

In den folgenden Themen wird beschrieben, wie AWS Lambda Sie mit dem Toolkit for Visual Studio arbeiten.

Themen

Grundlegendes AWS Lambda Projekt

Sie können eine Lambda-Funktion mithilfe von Microsoft.NET Core-Projektvorlagen erstellen, in der AWS Toolkit for Visual Studio.

Erstellen Sie ein Visual Studio-.NET-Core-Lambda-Projekt

Sie können Lambda-Visual Studio-Vorlagen und -Blueprints verwenden, um Ihre Projektinitialisierung zu beschleunigen. Lambda-Blueprints enthalten vorgefertigte Funktionen, die die Erstellung einer flexiblen Projektgrundlage vereinfachen.

> **Note**
>
> Der Lambda-Dienst hat Datenbeschränkungen für verschiedene Pakettypen. Ausführliche Informationen zu Datenlimits finden Sie unter dem Thema Lambda-Kontingente im AWS Lambda-Benutzerhandbuch.

So erstellen Sie ein Lambda-Projekt in Visual Studio

1. Erweitern Sie in Visual Studio das Menü Datei, erweitern Sie Neu und wählen Sie dann Projekt aus.
2. Stellen Sie im Dialogfeld „Neues Projekt“ die Dropdown-Felder Sprache, Plattform und Projekttyp auf „Alle“ ein und geben Sie dann aws lambda in das Suchfeld ein. Wählen Sie die AWS Vorlage Lambda Project (.NET Core — C#).
3. Geben **`AWSLambdaSample`** Sie im Feld Name den gewünschten Speicherort für die Datei ein und wählen Sie dann Erstellen, um fortzufahren.
4. Wählen Sie auf der Seite „Blueprint auswählen“ den Blueprint „Leere Funktion“ und anschließend „Fertig stellen“ aus, um das Visual Studio-Projekt zu erstellen.

Überprüfen der Projektdateien

Es gibt zwei Projektdateien, die überprüft werden müssen: `aws-lambda-tools-defaults.json` und. `Function.cs`

Das folgende Beispiel zeigt die `aws-lambda-tools-defaults.json` Datei, die automatisch als Teil Ihres Projekts erstellt wird. Mithilfe der Felder in dieser Datei können Sie Build-Optionen festlegen.

> **Note**
>
> Die Projektvorlagen in Visual Studio enthalten viele verschiedene Felder. Beachten Sie Folgendes:
>
> - Funktionshandler: gibt die Methode an, die ausgeführt wird, wenn die Lambda-Funktion ausgeführt wird
> - Wenn Sie einen Wert im Function-Handler-Feld angeben, wird dieser Wert im Veröffentlichungsassistenten automatisch aufgefüllt.

- Wenn Sie die Funktion, Klasse oder Assembly umbenennen, müssen Sie auch das entsprechende Feld in der Datei aktualisieren. `aws-lambda-tools-defaults.json`

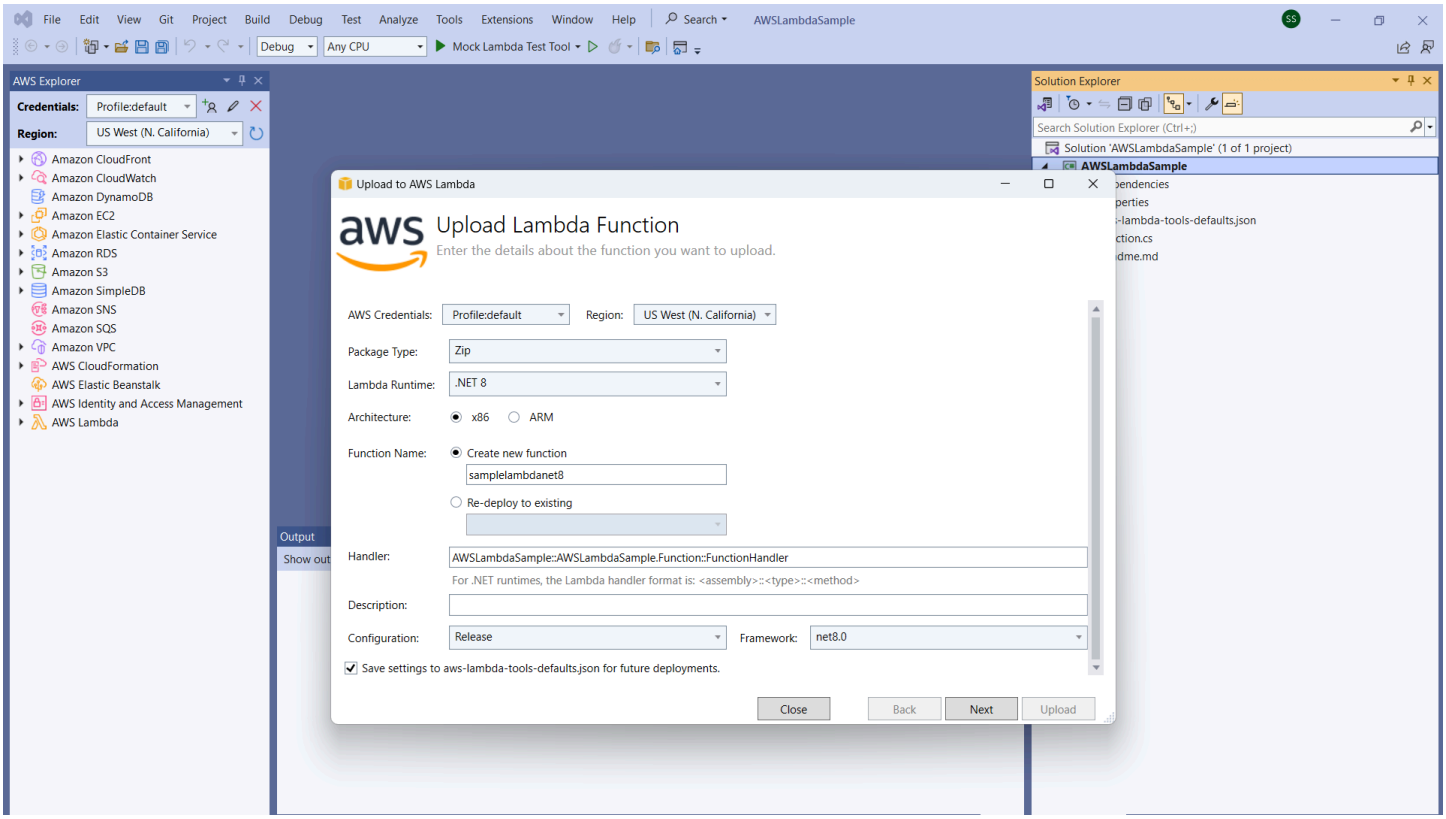
```
{
  "Information": [
    "This file provides default values for the deployment wizard inside Visual Studio
 and the AWS Lambda commands added to the .NET Core CLI.",
    "To learn more about the Lambda commands with the .NET Core CLI execute the
 following command at the command line in the project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

Untersuchen Sie die `Function.cs` Datei. `Function.cs`definiert die C#-Funktionen, die als Lambda-Funktionen verfügbar gemacht werden sollen. Dies `FunctionHandler` ist die Lambda-Funktionalität, die ausgeführt wird, wenn die Lambda-Funktion ausgeführt wird. In diesem Projekt ist eine Funktion definiert:`FunctionHandler`, die den Eingabetext `ToUpper()` aufruft.

Ihr Projekt ist jetzt bereit, auf Lambda veröffentlicht zu werden.

Auf Lambda veröffentlichen

Das folgende Verfahren und das folgende Bild zeigen, wie Sie Ihre Funktion mit dem AWS Toolkit for Visual Studio auf Lambda hochladen.



Veröffentlichen Sie Ihre Funktion auf Lambda

1. Navigieren Sie zum AWS Explorer, indem Sie View erweitern und AWS Explorer auswählen.
2. Öffnen Sie im Solution Explorer das Kontextmenü für das Projekt, das Sie veröffentlichen möchten (klicken Sie mit der rechten Maustaste darauf), und wählen Sie dann In AWS Lambda veröffentlichen, um das Fenster Lambda-Funktion hochladen zu öffnen.
3. Füllen Sie im Fenster Lambda-Funktion hochladen die folgenden Felder aus:

    a. Pakettyp: Wählen Sie**`Zip`**. Als Ergebnis des Build-Prozesses wird eine ZIP-Datei erstellt und auf Lambda hochgeladen. Alternativ können Sie den Pakettyp wählen**`Image`**. Das Tutorial: Basic Lambda Project Creating Docker Image beschreibt, wie Sie mit Package Type veröffentlichen. **`Image`**

    b. Lambda Runtime: Wählen Sie Ihre Lambda Runtime aus dem Drop-down-Menü aus.

    c. Architektur: Wählen Sie die radiale Architektur für Ihre bevorzugte Architektur aus.

    d. Funktionsname: Wählen Sie das Radial für Neue Funktion erstellen aus und geben Sie dann einen Anzeigenamen für Ihre Lambda-Instanz ein. Auf diesen Namen wird sowohl vom AWS Explorer als auch von AWS Management Console Displays verwiesen.

e. Handler: Verwenden Sie dieses Feld, um einen Funktionshandler anzugeben. Beispiel: **`AWSLambdaSample::AWSLambdaSample.Function::FunctionHandler`**.

f. (Optional) Beschreibung: Geben Sie beschreibenden Text ein, der zusammen mit Ihrer Instanz angezeigt werden soll, und zwar aus dem AWS Management Console.

g. Konfiguration: Wählen Sie Ihre bevorzugte Konfiguration aus dem Drop-down-Menü aus.

h. Framework: Wählen Sie Ihr bevorzugtes Framework aus dem Drop-down-Menü aus.

i. Einstellungen speichern: Wählen Sie dieses Feld, um Ihre aktuellen Einstellungen `aws-lambda-tools-defaults.json` als Standard für future Bereitstellungen zu speichern.

j. Wählen Sie Weiter, um zum Fenster mit den erweiterten Funktionsdetails zu gelangen.

4. Füllen Sie im Fenster „Erweiterte Funktionsdetails“ die folgenden Felder aus:

   a. Rollenname: Wählen Sie eine Rolle aus, die Ihrem Konto zugeordnet ist. Die Rolle stellt temporäre Anmeldeinformationen für alle AWS Serviceanfragen bereit, die über den Code in der Funktion getätigt werden. Wenn Sie keine Rolle haben, scrollen Sie in der Dropdownauswahl zu Neue Rolle basierend auf AWS verwalteter Richtlinie und wählen Sie dann aus AWSLambdaBasicExecutionRole. Diese Rolle hat nur minimale Zugriffsberechtigungen.

   > **Note**
   >
   > Ihr Konto muss berechtigt sein, die ListPolicies IAM-Aktion auszuführen. Andernfalls ist die Liste mit den Rollennamen leer und Sie können den Vorgang nicht fortsetzen.

   b. (Optional) Wenn Ihre Lambda-Funktion auf Ressourcen in einer Amazon VPC zugreift, wählen Sie die Subnetze und Sicherheitsgruppen aus.

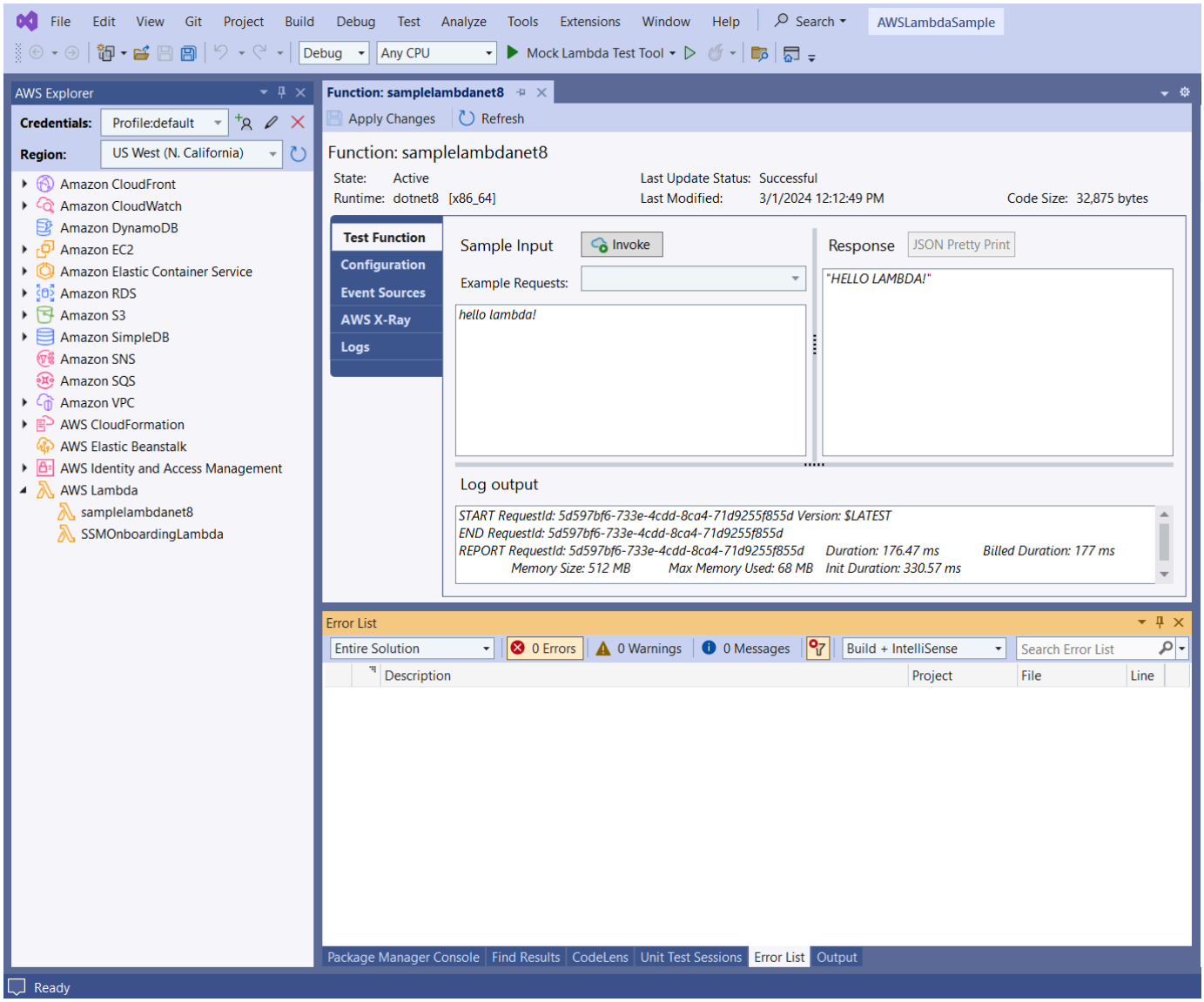
   c. (Optional) Legen Sie alle Umgebungsvariablen fest, die Ihre Lambda-Funktion benötigt. Die Schlüssel werden automatisch mit dem kostenlosen Standard-Serviceschlüssel verschlüsselt. Alternativ können Sie einen AWS KMS Schlüssel angeben, für den eine Gebühr anfällt. KMS ist ein verwalteter Service, mit dem Sie Schlüssel zum Verschlüsseln Ihrer Daten erstellen und steuern können. Wenn Sie einen AWS KMS Schlüssel haben, können Sie ihn aus der Liste auswählen.

5. Wählen Sie Hochladen, um das Fenster mit der Upload-Funktion zu öffnen und den Upload-Vorgang zu starten.

> **Note**
>
> Die Seite mit den Upload-Funktionen wird angezeigt, während die Funktion in hochgeladen wird. AWS Um den Assistenten nach dem Hochladen geöffnet zu lassen, sodass Sie den Bericht ansehen können, deaktivieren Sie unten im Formular die Option Assistent bei erfolgreichem Abschluss automatisch schließen, bevor der Upload abgeschlossen ist.
> Nachdem die Funktion hochgeladen wurde, ist Ihre Lambda-Funktion live. Die Seite Funktion: Ansicht wird geöffnet und zeigt die Konfiguration Ihrer neuen Lambda-Funktion an.

6. Geben Sie auf der Registerkarte Testfunktion `hello lambda!` in das Texteingabefeld ein und wählen Sie dann Invoke, um Ihre Lambda-Funktion manuell aufzurufen. Ihr Text erscheint auf der Registerkarte „Antwort“ und wurde in Großbuchstaben umgewandelt.

> **Note**
>
> Sie können die Ansicht Function: jederzeit erneut öffnen, indem Sie im AWS Explorer unter dem Knoten auf Ihre bereitgestellte Instanz doppelklicken. AWS Lambda



7. (Optional) Um zu bestätigen, dass Sie Ihre Lambda-Funktion erfolgreich veröffentlicht haben, melden Sie sich bei der an AWS Management Console und wählen Sie dann Lambda aus. In der Konsole werden alle Ihre veröffentlichten Lambda-Funktionen angezeigt, einschließlich der soeben erstellten.

Aufräumen

Wenn Sie mit diesem Beispiel nicht weiterentwickeln möchten, löschen Sie die von Ihnen bereitgestellte Funktion, damit Ihnen nicht genutzte Ressourcen in Ihrem Konto nicht in Rechnung gestellt werden.

> **Note**
>
> Lambda überwacht Lambda-Funktionen automatisch für Sie und meldet Metriken über Amazon. CloudWatch Informationen zur Überwachung und Problembehebung Ihrer Funktion finden Sie im CloudWatch Thema Troubleshooting and Monitoring AWS Lambda Functions with Amazon im AWS Lambda Developer Guide.

Um Ihre Funktion zu löschen

1. Erweitern Sie im AWS Explorer den AWS LambdaKnoten.
2. Klicken Sie mit der rechten Maustaste auf Ihre bereitgestellte Instanz und wählen Sie dann Löschen.

AWS Lambda Basisprojekt: Docker-Image erstellen

Sie können das Toolkit for Visual Studio verwenden, um Ihre AWS Lambda Funktion als Docker-Image bereitzustellen. Mit Docker haben Sie mehr Kontrolle über Ihre Laufzeit. Sie können beispielsweise benutzerdefinierte Laufzeiten wie .NET 8.0 wählen. Sie stellen Ihr Docker-Image auf die gleiche Weise bereit wie jedes andere Container-Image. Dieses Tutorial ist Tutorial: Basic Lambda Project sehr ähnlich, mit zwei Unterschieden:

- Ein Dockerfile ist im Projekt enthalten.
- Eine alternative Veröffentlichungskonfiguration wird ausgewählt.

Informationen zu Lambda-Container-Images finden Sie unter Lambda Deployment Packages im AWS Lambda Developer Guide.

Weitere Informationen zur Arbeit mit Lambda AWS Toolkit for Visual Studio finden Sie im AWS Toolkit for Visual Studio Thema Verwenden der AWS Lambda Vorlagen in diesem Benutzerhandbuch.

Erstellen Sie ein Visual Studio-.NET-Core-Lambda-Projekt

Sie können Lambda Visual Studio-Vorlagen und -Blueprints verwenden, um Ihre Projektinitialisierung zu beschleunigen. Lambda-Blueprints enthalten vorgefertigte Funktionen, die die Erstellung einer flexiblen Projektgrundlage vereinfachen.

So erstellen Sie ein Visual Studio-.NET Core Lambda-Projekt

1. Erweitern Sie in Visual Studio das Menü Datei, erweitern Sie Neu und wählen Sie dann Projekt aus.
2. Stellen Sie im Dialogfeld „Neues Projekt“ die Dropdown-Felder Sprache, Plattform und Projekttyp auf „Alle“ ein und geben Sie dann **`aws lambda`** in das Suchfeld ein. Wählen Sie die AWS Vorlage Lambda Project (.NET Core — C#).
3. Geben Sie **`AWSLambdaDocker`** im Feld Projektname den Speicherort Ihrer Datei ein und wählen Sie dann Erstellen aus.
4. Wählen Sie auf der Seite „Blueprint auswählen“ den Blueprint .NET 8 (Container Image) aus, und klicken Sie dann auf Fertig stellen, um das Visual Studio-Projekt zu erstellen. Sie können jetzt die Struktur und den Code des Projekts überprüfen.

Projektdateien überprüfen

In den folgenden Abschnitten werden die drei Projektdateien untersucht, die mit dem.NET 8-Blueprint (Container Image) erstellt wurden:

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

1. Dockerfile

A `Dockerfile` führt drei Hauptaktionen aus:

- `FROM`: Legt das Basis-Image fest, das für dieses Image verwendet werden soll. Dieses Basisimage stellt .NET Runtime, Lambda Runtime und ein Shell-Skript bereit, das einen Einstiegspunkt für den Lambda.NET-Prozess bereitstellt.
- `WORKDIR`: Legt das interne Arbeitsverzeichnis des Images fest als. `/var/task`
- `COPY`: Kopiert die während des Build-Prozesses generierten Dateien von ihrem lokalen Speicherort in das Arbeitsverzeichnis des Images.

Die folgenden optionalen `Dockerfile` Aktionen können Sie angeben:

- `ENTRYPOINT`: Das Basis-Image enthält bereits ein. Dabei handelt es sich um den Startvorgang`ENTRYPOINT`, der ausgeführt wird, wenn das Image gestartet wird. Wenn Sie Ihren eigenen angeben möchten, überschreiben Sie diesen Basiseinstiegspunkt.
- `CMD`: Gibt an, AWS welchen benutzerdefinierten Code Sie ausführen möchten. Es erwartet einen vollständig qualifizierten Namen für Ihre benutzerdefinierte Methode. Diese Zeile muss entweder direkt in das Dockerfile aufgenommen werden oder kann während des Veröffentlichungsvorgangs angegeben werden.

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

Das Folgende ist ein Beispiel für ein Dockerfile, das mit dem.NET 8-Blueprint (Container Image) erstellt wurde.

```
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

Die `aws-lambda-tools-defaults.json` Datei wird verwendet, um Standardwerte für den Toolkit for Visual Studio Studio-Bereitstellungsassistenten und .NET Core CLI anzugeben. In der folgenden

Liste werden Felder beschrieben, die Sie in Ihrer `aws-lambda-tools-defaults.json` Datei festlegen können.

- `profile`: legt Ihr AWS Profil fest.
- `region`: legt die AWS Region fest, in der Ihre Ressourcen gespeichert werden.
- `configuration`: legt die Konfiguration fest, die für die Veröffentlichung Ihrer Funktion verwendet wurde.
- `package-type`: legt den Typ des Bereitstellungspakets auf ein Container-Image oder ein ZIP-Dateiarchiv fest.
- `function-memory-size`: legt die Speicherzuweisung für Ihre Funktion in MB fest.
- `function-timeout`: Timeout ist die maximale Zeit in Sekunden, die eine Lambda-Funktion ausführen kann. Sie können dies in Schritten von 1 Sekunde bis zu einem Maximalwert von 15 Minuten anpassen.
- `docker-host-build-output-dir`: legt das Ausgabeverzeichnis des Build-Prozesses fest, das den Anweisungen in der entspricht. `Dockerfile`
- `image-command`: ist ein vollständig qualifizierter Name für Ihre Methode, der Code, für den die Lambda-Funktion ausgeführt werden soll. Die Syntax lautet:. `{Assembly}::{Namespace}.{ClassName}::{MethodName}` Weitere Informationen finden Sie unter Handler-Signaturen. Wenn `image-command` Sie diese Einstellung festlegen, wird dieser Wert später im Veröffentlichungsassistenten von Visual Studio vorab aufgefüllt.

Im Folgenden finden Sie ein Beispiel für eine aws-lambda-tools-defaults JSON-Datei, die mit dem.NET 8-Blueprint (Container Image) erstellt wurde.

```
{
  "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

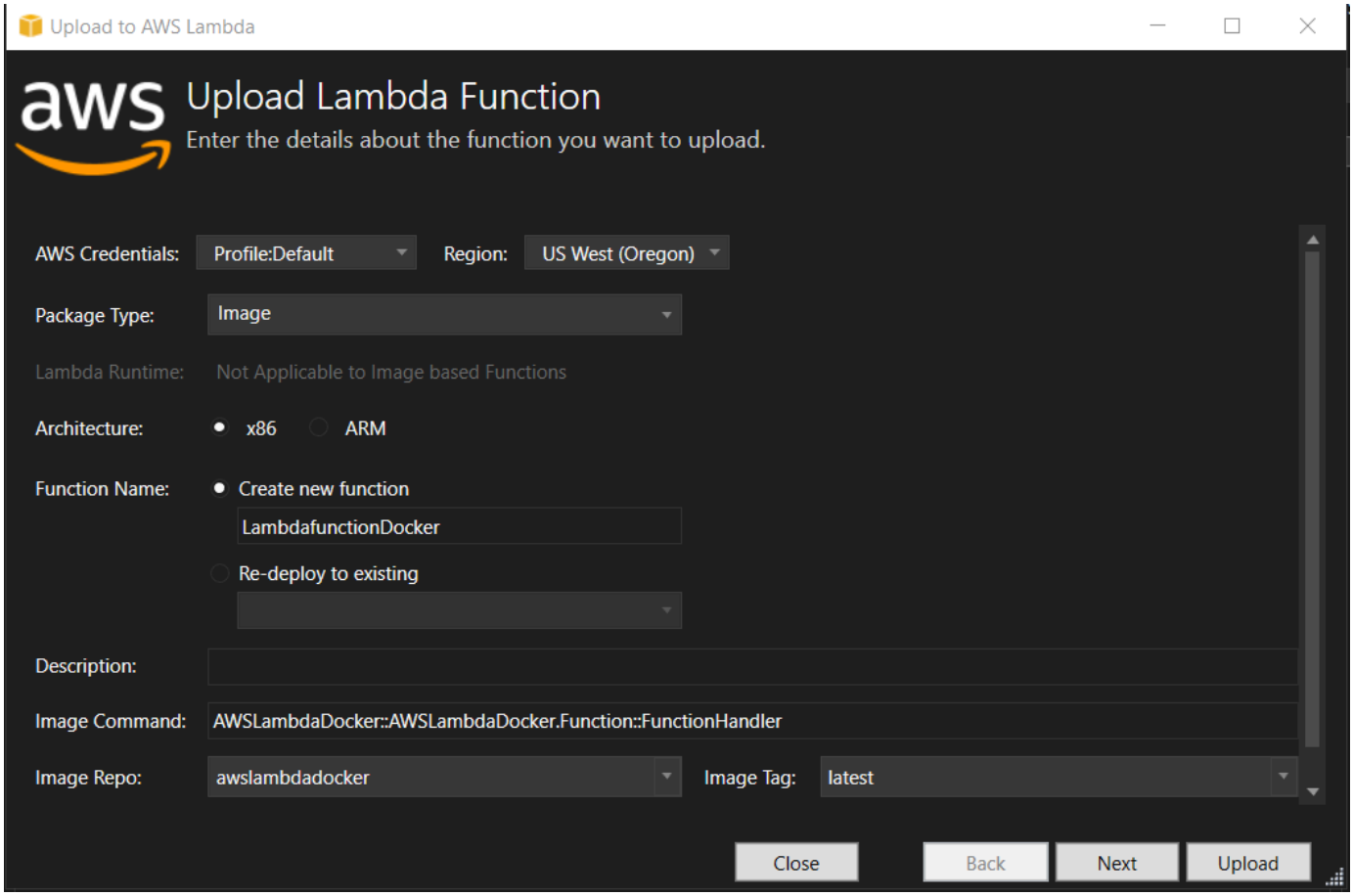
Die `Function.cs` Datei definiert die C#-Funktionen, die als Lambda-Funktionen verfügbar gemacht werden sollen. Das `FunctionHandler` ist die Lambda-Funktionalität, die ausgeführt wird, wenn die Lambda-Funktion ausgeführt wird. `FunctionHandler`Ruft in diesem Projekt den `ToUpper()` Eingabetext auf.

Auf Lambda veröffentlichen

Docker-Images, die durch den Build-Prozess generiert werden, werden in Amazon Elastic Container Registry (Amazon ECR) hochgeladen. Amazon ECR ist eine vollständig verwaltete Docker-Container-Registry, die Sie zum Speichern, Verwalten und Bereitstellen von Docker-Container-Images verwenden. Amazon ECR hostet das Image, auf das Lambda dann verweist, um die programmierte Lambda-Funktionalität bereitzustellen, wenn es aufgerufen wird.

Um Ihre Funktion auf Lambda zu veröffentlichen

1. Öffnen Sie im Solution Explorer das Kontextmenü für das Projekt (klicken Sie mit der rechten Maustaste darauf) und wählen Sie dann Veröffentlichen, AWS Lambda um das Fenster Lambda-Funktion hochladen zu öffnen.
2. Gehen Sie auf der Seite Lambda-Funktion hochladen wie folgt vor:



a. Als Pakettyp **`Image`** wurde automatisch als Pakettyp ausgewählt, da der Veröffentlichungsassistent eine `Dockerfile` in Ihrem Projekt erkannt hat.

b. Geben Sie unter Funktionsname einen Anzeigenamen für Ihre Lambda-Instanz ein. Dieser Name ist der Referenzname, der sowohl im AWS Explorer in Visual Studio als auch im angezeigt wird AWS Management Console.

c. Geben Sie unter Beschreibung den Text ein, der zusammen mit Ihrer Instanz im angezeigt werden soll AWS Management Console.

d. Geben Sie für Image Command einen vollqualifizierten Pfad zu der Methode ein, die die Lambda-Funktion ausführen soll: **`AWSLambdaDocker::AWSLambdaDocker.Function::FunctionHandler`**

> **Note**
>
> Jeder hier eingegebene Methodenname überschreibt alle CMD-Anweisungen in der Dockerfile. Die Eingabe von Image Command ist nur optional, WENN Sie eine Anweisung `CMD` zum Starten der Lambda-Funktion `Dockerfile` enthalten.

e. Geben Sie für Image Repo den Namen einer neuen oder vorhandenen Amazon Elastic Container Registry ein. Das Docker-Image, das der Build-Prozess erstellt, wird in diese Registry hochgeladen. Die Lambda-Definition, die veröffentlicht wird, wird auf dieses Amazon ECR-Image verweisen.

f. Geben Sie für Image-Tag ein Docker-Tag ein, das mit Ihrem Image im Repository verknüpft werden soll.

g. Wählen Sie Weiter.

3. Wählen Sie auf der Seite mit den erweiterten Funktionsdetails unter Rollenname eine Rolle aus, die Ihrem Konto zugeordnet ist. Die Rolle wird verwendet, um temporäre Anmeldeinformationen für alle Amazon Web Services Services-Aufrufe bereitzustellen, die durch den Code in der Funktion ausgeführt werden. Wenn Sie noch keine Rolle haben, wählen Sie Neue Rolle basierend auf AWS verwalteter Richtlinie und wählen Sie dann AWSLambdaBasicExecutionRole.

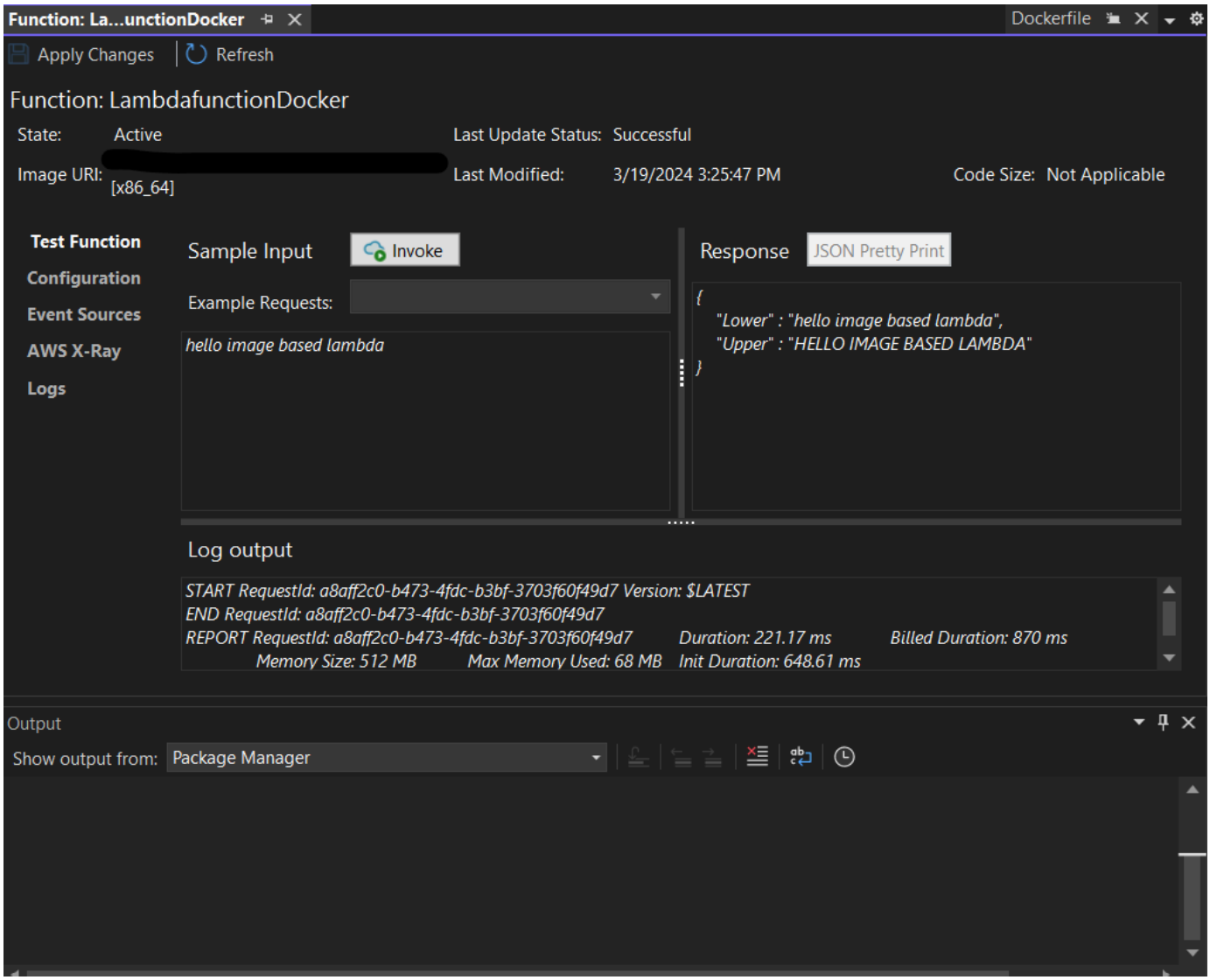
> **Note**
>
> Ihr Konto muss über die Berechtigung zum Ausführen der ListPolicies IAM-Aktion verfügen. Andernfalls ist die Liste mit den Rollennamen leer.

4. Wählen Sie Hochladen, um den Upload- und Veröffentlichungsvorgang zu starten.

> **Note**
>
> Die Seite mit den Upload-Funktionen wird angezeigt, während die Funktion hochgeladen wird. Der Veröffentlichungsprozess erstellt dann das Image auf der Grundlage der Konfigurationsparameter, erstellt bei Bedarf das Amazon ECR-Repository, lädt das Image in das Repository hoch und erstellt das Lambda, das auf dieses Repository mit diesem Image verweist.

Nachdem die Funktion hochgeladen wurde, wird die Funktionsseite geöffnet und die Konfiguration Ihrer neuen Lambda-Funktion wird angezeigt.

5. Um die Lambda-Funktion manuell aufzurufen, geben Sie auf der Registerkarte Testfunktion den Text in das **`hello image based lambda`** Freitexteingabefeld für die Anforderung ein und wählen Sie dann Aufrufen. Ihr in Großbuchstaben konvertierter Text wird als Antwort angezeigt.



6. Um das Repository anzuzeigen, wählen Sie im AWS Explorer unter Amazon Elastic Container Service die Option Repositories aus.

   Sie können die Ansicht Function: jederzeit erneut öffnen, indem Sie im AWS Explorer unter dem Knoten auf Ihre bereitgestellte Instance doppelklicken. AWS Lambda

> **Note**
>
> Wenn Ihr AWS Explorer-Fenster nicht geöffnet ist, können Sie es über Ansicht -> Explorer andocken AWS

7. Beachten Sie zusätzliche bildspezifische Konfigurationsoptionen auf der Registerkarte Konfiguration. Diese Registerkarte bietet eine Möglichkeit, die, und `ENTRYPOINTCMD`, `WORKDIR` die möglicherweise in der Dockerfile angegeben wurden, zu überschreiben. Beschreibung ist die Beschreibung, die Sie (falls vorhanden) beim Hochladen/Veröffentlichen eingegeben haben.

Aufräumen

Wenn Sie mit diesem Beispiel nicht weiterentwickeln möchten, denken Sie daran, die bereitgestellte Funktion und das ECR-Image zu löschen, damit Ihnen nicht genutzte Ressourcen in Ihrem Konto in Rechnung gestellt werden.

- Funktionen können gelöscht werden, indem Sie mit der rechten Maustaste auf Ihre bereitgestellte Instanz klicken, die sich im AWS Explorer unter dem Knoten befindet. AWS Lambda
- Repositorys können im AWS Explorer unter dem Amazon Elastic Container Service -> Repositories gelöscht werden.

Nächste Schritte

Informationen zum Erstellen und Testen von Lambda-Images finden Sie unter Using Container Images with Lambda.

Informationen zur Bereitstellung von Container-Images, zu Berechtigungen und zum Überschreiben von Konfigurationseinstellungen finden Sie unter Funktionen konfigurieren.

Tutorial: Erstellen und Testen einer serverlosen Anwendung mit AWS Lambda

Sie können mithilfe einer Vorlage eine serverlose Lambda-Anwendung erstellen AWS Toolkit for Visual Studio . Zu den Lambda-Projektvorlagen gehört eine Vorlage für eine AWS serverlose Anwendung, bei der es sich um die AWS Toolkit for Visual Studio Implementierung des AWS Serverless Application Model (AWSSAM) handelt. Mit diesem Projekttyp können Sie eine Sammlung

von AWS Lambda Funktionen entwickeln und diese mit allen erforderlichen AWS Ressourcen als gesamte Anwendung bereitstellen, um die Bereitstellung AWS CloudFormation zu orchestrieren.

Voraussetzungen und Informationen zur Einrichtung von finden Sie unter Verwenden der AWS Lambda-Vorlagen im AWS Toolkit for Visual Studio. AWS Toolkit for Visual Studio

Themen

- Erstellen Sie ein neues AWS serverloses Anwendungsprojekt
- Überprüfen der Dateien der serverlosen Anwendung
- Bereitstellen der serverlosen Anwendung
- Testen der serverlosen Anwendung

Erstellen Sie ein neues AWS serverloses Anwendungsprojekt

AWS Serverlose Anwendungsprojekte erstellen Lambda-Funktionen mit einer AWS CloudFormation serverlosen Vorlage. AWS CloudFormation Mithilfe von Vorlagen können Sie zusätzliche Ressourcen wie Datenbanken definieren, IAM-Rollen hinzufügen und mehrere Funktionen gleichzeitig bereitstellen. Dies unterscheidet sich von AWS Lambda-Projekten, die sich auf die Entwicklung und Bereitstellung einer einzigen Lambda-Funktion konzentrieren.

Das folgende Verfahren beschreibt, wie Sie ein neues Projekt für AWS serverlose Anwendungen erstellen.

1. Erweitern Sie in Visual Studio das Menü Datei, erweitern Sie Neu und wählen Sie dann Projekt aus.
2. Stellen Sie im Dialogfeld „Neues Projekt“ sicher, dass die Dropdown-Felder Sprache, Plattform und Projekttyp auf „Alle...“ gesetzt sind, und geben Sie **`aws lambda`** in das Suchfeld ein.
3. Wählen Sie die AWS Vorlage Serverlose Anwendung mit Tests (.NET Core — C#) aus.

   > **Note**
   >
   > Es ist möglich, dass die Vorlage AWS Serverlose Anwendung mit Tests (.NET Core — C#) nicht ganz oben in den Ergebnissen angezeigt wird.

4. Klicken Sie auf Weiter, um das Dialogfeld Neues Projekt konfigurieren zu öffnen.

5. Geben **`ServerlessPowertools`**Sie im Dialogfeld „Neues Projekt konfigurieren“ den Namen ein und füllen Sie dann die verbleibenden Felder nach Ihren Wünschen aus. Wählen Sie die Schaltfläche „Erstellen“, um mit dem Dialogfeld „Blueprint auswählen“ fortzufahren.
6. Wählen Sie im Dialogfeld „Blueprint auswählen“ die Option „Powertools for AWS Lambda Blueprint“ und anschließend „Fertig stellen“, um das Visual Studio-Projekt zu erstellen.

Überprüfen der Dateien der serverlosen Anwendung

Die folgenden Abschnitte bieten einen detaillierten Überblick über drei Dateien für serverlose Anwendungen, die für Ihr Projekt erstellt wurden:

1. serverless.template
2. Functions.cs
3. aws-lambda-tools-defaults.json

1. serverlose Vorlage

Eine `serverless.template` Datei ist eine AWS CloudFormation Vorlage für die Deklaration Ihrer serverlosen Funktionen und anderer Ressourcen. AWS Die in diesem Projekt enthaltene Datei enthält eine Deklaration für eine einzelne Lambda-Funktion, die über das Amazon API Gateway als `HTTP *Get*` Operation verfügbar gemacht wird. Sie können diese Vorlage bearbeiten, um die bestehende Funktion anzupassen oder weitere Funktionen und andere Ressourcen hinzuzufügen, die für Ihre Anwendung erforderlich sind.

Im Folgenden wird ein Beispiel für eine `serverless.template`-Datei dargestellt:

```
{
  "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/"
      }
    }
  }
}
```

Beachten Sie, dass viele der `...AWS:: Serverless::Function...` Deklarationsfelder den Feldern einer Lambda-Projektbereitstellung ähneln. Powertools Logging, Metrics und Tracing werden über die folgenden Umgebungsvariablen konfiguriert:

- POWERTOOLS_SERVICE_NAME= ServerlessGreeting
- POWERTOOLS_LOG_LEVEL=Informationen
- POWERTOOLS_LOGGER_CASE= PascalCase
- PowerTools_Tracer_Capture_Response=Wahr
- PowerTools_Tracer_Capture_Error=Wahr
- POWERTOOLS_METRICS_NAMESPACE= ServerlessGreeting

Definitionen und zusätzliche Informationen zu den Umgebungsvariablen finden Sie auf der Powertools-Website für Referenzen. AWS Lambda

2. Functions.cs

`Functions.cs`ist eine Klassendatei, die eine C#-Methode enthält, die einer einzelnen Funktion zugeordnet ist, die in der Vorlagendatei deklariert ist. Die Lambda-Funktion reagiert auf `HTTP Get` Methoden von API Gateway. Das Folgende ist ein Beispiel für die `Functions.cs` Datei:

```
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`stellt die Standardwerte für den AWS Bereitstellungsassistenten in Visual Studio und die AWS Lambda Befehle bereit, die zur.NET Core CLI hinzugefügt wurden. Im Folgenden finden Sie ein Beispiel für die `aws-lambda-tools-defaults.json` Datei, die in diesem Projekt enthalten ist:

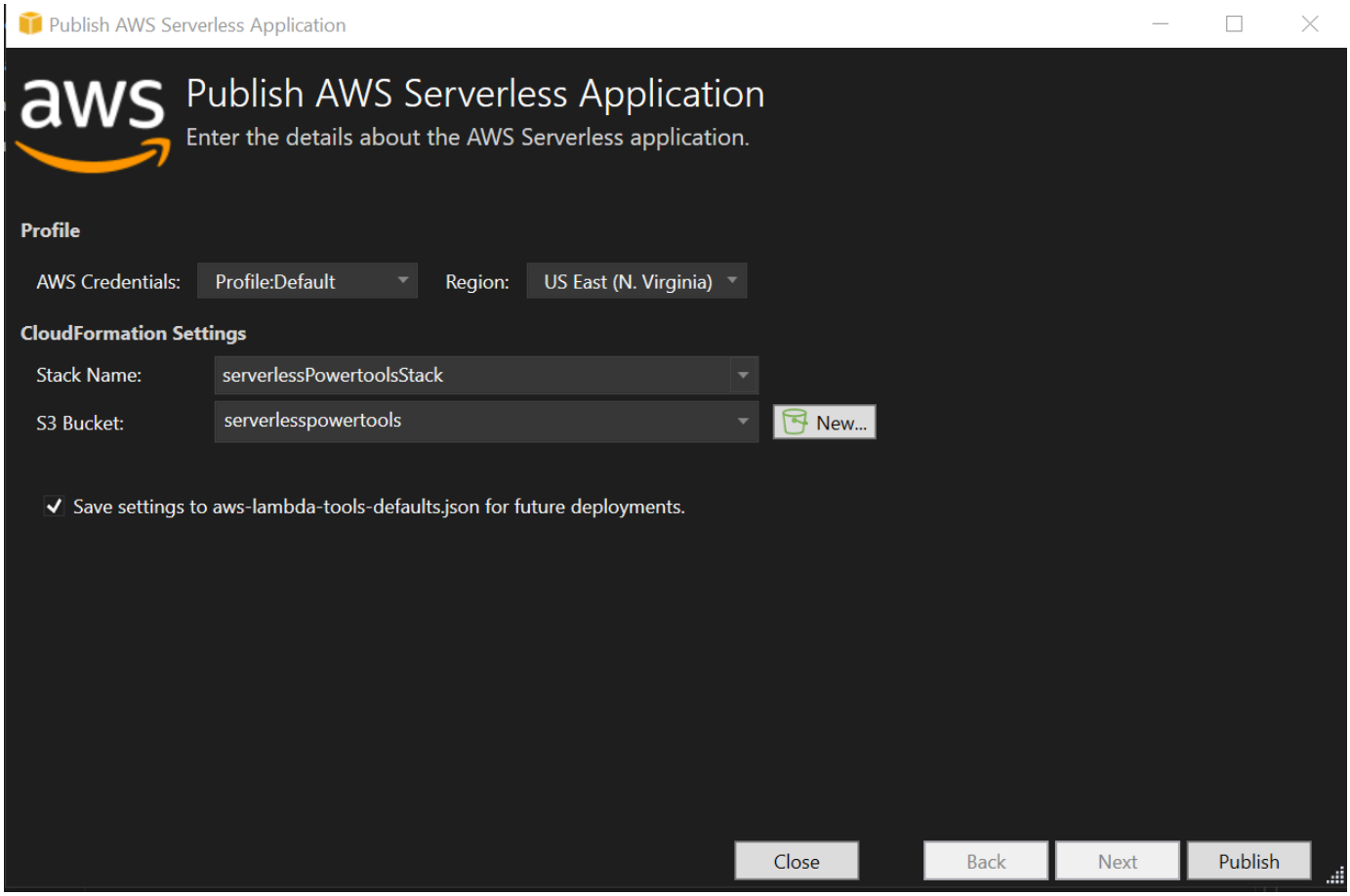
```
{
  "profile": "Default",
  "region": "us-east-1",
  "configuration": "Release",
  "s3-prefix": "ServerlessPowertools/",
  "template": "serverless.template",
  "template-parameters": ""
}
```

Bereitstellen der serverlosen Anwendung

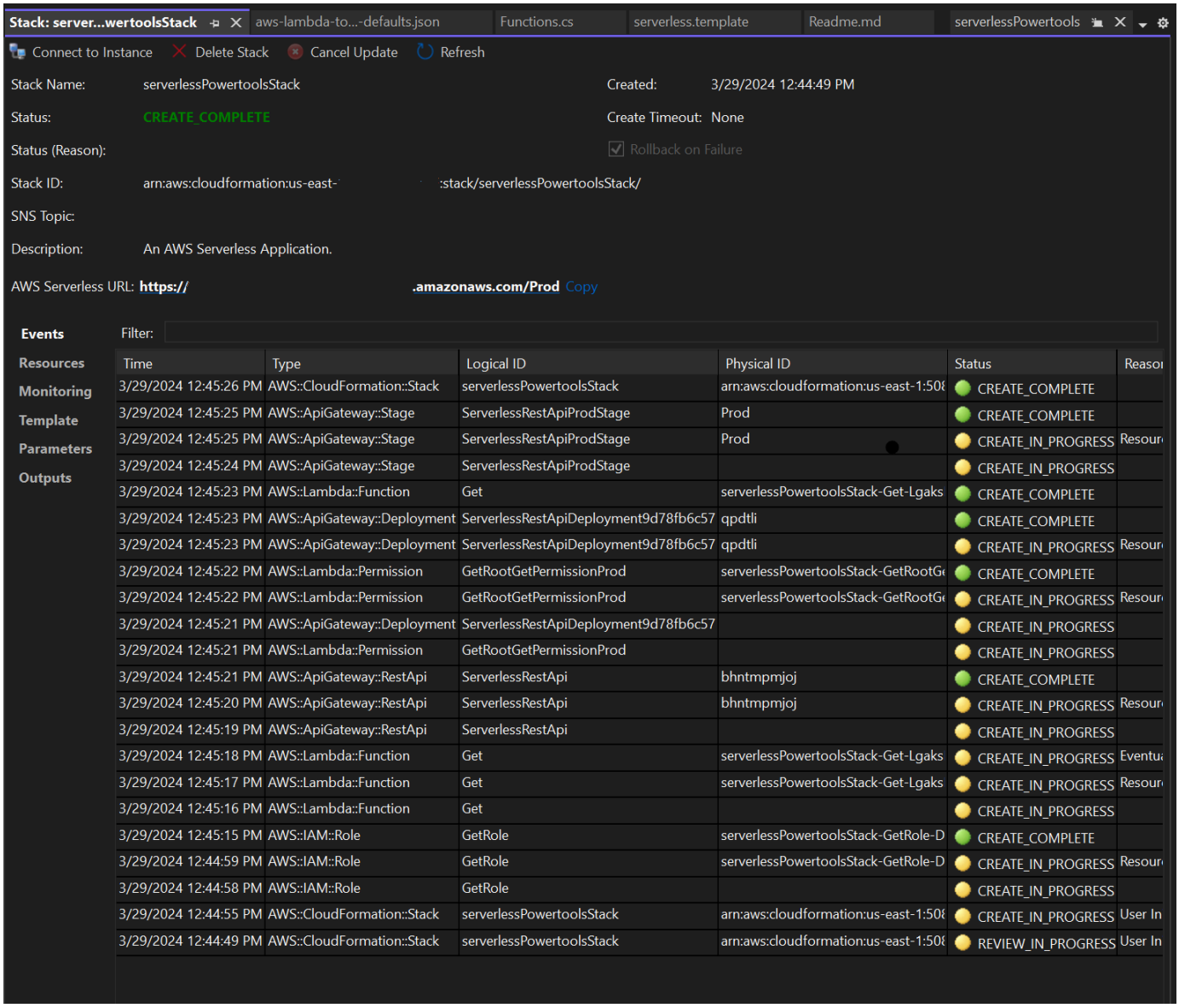
Gehen Sie wie folgt vor, um Ihre serverlose Anwendung bereitzustellen

1. Öffnen Sie im Solution Explorer das Kontextmenü für Ihr Projekt (Rechtsklick) und wählen Sie In AWS Lambda veröffentlichen, um das Dialogfeld AWS Serverlose Anwendung veröffentlichen zu öffnen.
2. Geben Sie im Dialogfeld AWS Serverlose Anwendung veröffentlichen im Feld Stackname einen Namen für den AWS CloudFormation Stack-Container ein.
3. Wählen Sie im Feld S3-Bucket einen Amazon S3 S3-Bucket aus, in den Ihr Anwendungspaket hochgeladen werden soll, oder wählen Sie New... klicken Sie und geben Sie den Namen eines neuen Amazon S3 S3-Buckets ein. Wählen Sie dann Publish to Publish (Veröffentlichen), um Ihre Anwendung bereitzustellen.

> **Note**
>
> Ihr AWS CloudFormation Stack und Ihr Amazon S3 S3-Bucket müssen in derselben AWS Region existieren. Die übrigen Einstellungen für Ihr Projekt sind in der `serverless.template` Datei definiert.



4. Das Stack-Ansichtsfenster wird während des Veröffentlichungsvorgangs geöffnet. Wenn die Bereitstellung abgeschlossen ist, wird im Feld Status Folgendes angezeigt:`CREATE_COMPLETE`.



Testen der serverlosen Anwendung

Wenn die Erstellung des Stacks abgeschlossen ist, können Sie Ihre Anwendung mithilfe der AWS serverlosen URL anzeigen. Wenn Sie dieses Tutorial abgeschlossen haben, ohne zusätzliche Funktionen oder Parameter hinzuzufügen, wird beim Zugriff auf Ihre AWS serverlose URL der folgende Satz in Ihrem Webbrowser angezeigt:. `Hello Powertools for AWS Lambda (.NET)`

Tutorial: Erstellen einer Amazon Rekognition-Lambda-Anwendung

Dieses Tutorial zeigt Ihnen, wie Sie eine Lambda-Anwendung erstellen, die Amazon Rekognition verwendet, um Amazon S3 S3-Objekte mit erkannten Labels zu kennzeichnen.

Voraussetzungen und Informationen zur Einrichtung von finden Sie unter Verwenden der AWS Lambda-Vorlagen im AWS Toolkit for Visual Studio. AWS Toolkit for Visual Studio

Erstellen Sie ein Visual Studio-.NET Core Lambda Image Rekognition-Projekt

Das folgende Verfahren beschreibt, wie Sie eine Amazon Rekognition Lambda-Anwendung aus dem erstellen. AWS Toolkit for Visual Studio

> **Note**
>
> Nach der Erstellung verfügt Ihre Anwendung über eine Lösung mit zwei Projekten: dem Quellprojekt, das Ihren Lambda-Funktionscode zur Bereitstellung auf Lambda enthält, und einem Testprojekt, das xUnit verwendet, um Ihre Funktion lokal zu testen.
> Manchmal kann Visual Studio nicht alle NuGet Referenzen für Ihre Projekte finden. Das liegt daran, dass Blueprints Abhängigkeiten erfordern, aus NuGet denen abgerufen werden muss. Wenn neue Projekte erstellt werden, ruft Visual Studio nur lokale Verweise ab und keine Remote-Verweise von. NuGet Um Fehler zu NuGet beheben, klicken Sie mit der rechten Maustaste auf Ihre Verweise und wählen Sie Pakete wiederherstellen.

1. Erweitern Sie in Visual Studio das Menü Datei, erweitern Sie Neu und wählen Sie dann Projekt aus.
2. Vergewissern Sie sich, dass im Dialogfeld „Neues Projekt“ die Dropdown-Felder Sprache, Plattform und Projekttyp auf „Alle...“ gesetzt sind, und geben Sie **`aws lambda`** in das Suchfeld ein.
3. Wählen Sie die Vorlage AWS Lambda mit Tests (.NET Core — C#) aus.
4. Klicken Sie auf Weiter, um das Dialogfeld Neues Projekt konfigurieren zu öffnen.
5. Geben Sie im Dialogfeld „Neues Projekt konfigurieren“ ImageRekognition "als Namen ein und füllen Sie dann die verbleibenden Felder nach Ihren Wünschen aus. Wählen Sie die Schaltfläche „Erstellen“, um mit dem Dialogfeld „Blueprint auswählen“ fortzufahren.
6. Wählen Sie im Dialogfeld „Blueprint auswählen“ den Blueprint „Bildbeschriftungen erkennen“ und anschließend „Fertig stellen“, um das Visual Studio-Projekt zu erstellen.

> **Note**
>
> Dieser Blueprint bietet Code zum Abhören von Amazon S3 S3-Ereignissen und verwendet Amazon Rekognition, um Labels zu erkennen und sie dem S3-Objekt als Tags hinzuzufügen.

Projektdateien überprüfen

In den folgenden Abschnitten werden diese Projektdateien untersucht:

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

1. Function.cs

In der `Function.cs` Datei ist das erste Codesegment das Assemblyattribut, das sich oben in der Datei befindet. Standardmäßig akzeptiert Lambda nur Eingabeparameter und Rückgabetypen vom Typ`System.IO.Stream`. Sie müssen einen Serializer registrieren, um typisierte Klassen für Eingabeparameter und Rückgabetypen zu verwenden. Das Assembly-Attribut registriert den Lambda-JSON-Serializer, der Streams in `Newtonsoft.Json` typisierte Klassen konvertiert. Sie können den Serializer auf Assembly- oder Methodenebene festlegen.

Im Folgenden finden Sie ein Beispiel für das Assembly-Attribut:

```
// 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
```

Die Klasse enthält zwei Konstruktoren. Der erste ist ein Standardkonstruktor, der verwendet wird, wenn Lambda Ihre Funktion aufruft. Dieser Konstruktor erstellt die Amazon S3- und Amazon Rekognition Service-Clients. Der Konstruktor ruft auch die AWS Anmeldeinformationen für diese Clients aus der IAM-Rolle ab, die Sie der Funktion bei der Bereitstellung zuweisen. Die AWS Region für die Clients ist auf die Region festgelegt, in der Ihre Lambda-Funktion ausgeführt wird. In diesem Blueprint möchten Sie dem Amazon S3 S3-Objekt nur dann Tags hinzufügen, wenn der Amazon Rekognition Rekognition-Service ein Mindestmaß an Vertrauen in das Label hat. Dieser Konstruktor

prüft die Umgebungsvariable `MinConfidence`, um das Mindestmaß an Vertrauen zu ermitteln. Sie können diese Umgebungsvariable bei der Bereitstellung der Lambda-Funktion festlegen.

Im Folgenden finden Sie ein Beispiel für den Konstruktor der ersten Klasse in: `Function.cs`

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

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

Das folgende Beispiel zeigt, wie der zweite Konstruktor zum Testen verwendet werden kann. Das Testprojekt konfiguriert seine eigenen S3- und Rekognition-Clients und übergibt sie:

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

Das Folgende ist ein Beispiel für die `FunctionHandler` Methode in der Datei. `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` ist die Methode, die Lambda aufruft, nachdem die Instance erstellt wurde. Beachten Sie, dass der Eingabeparameter vom Typ `S3Event` und nicht `Stream` ist. Dies ist aufgrund des registrierten Lambda-JSON-Serializers möglich. Das `S3Event` enthält alle Informationen über das in Amazon S3 ausgelöste Ereignis. Die Funktion durchläuft alle S3-Objekte, die Teil des Ereignisses waren, und weist Rekognition an, die Bezeichner zu ermitteln. Nachdem die Bezeichner ermittelt wurden, werden sie dem S3-Objekt als Tags hinzugefügt.

> **Note**
>
> Der Code enthält Aufrufe von`Console.WriteLine()`. Wenn die Funktion in Lambda ausgeführt wird, werden alle Aufrufe zu Amazon CloudWatch Logs `Console.WriteLine()` umgeleitet.

2. aws-lambda-tools-defaults.json

Die `aws-lambda-tools-defaults.json` Datei enthält Standardwerte, die der Blueprint so festgelegt hat, dass einige Felder im Bereitstellungsassistenten vorab ausgefüllt werden. Es ist auch hilfreich bei der Festlegung von Befehlszeilenoptionen für die Integration mit.NET Core CLI.

Um auf die .NET Core CLI-Integration zuzugreifen, navigieren Sie zum Projektverzeichnis der Funktion und geben Sie Folgendes ein**`dotnet lambda help`**.

> **Note**
>
> Der Funktionshandler gibt an, welche Methode Lambda als Antwort auf die aufgerufene Funktion aufrufen soll. Das Format dieses Feldes ist:. `<assembly-name>::<full-type-name>::<method-name>` Der Namespace muss im Typnamen enthalten sein.

Bereitstellen der Funktion

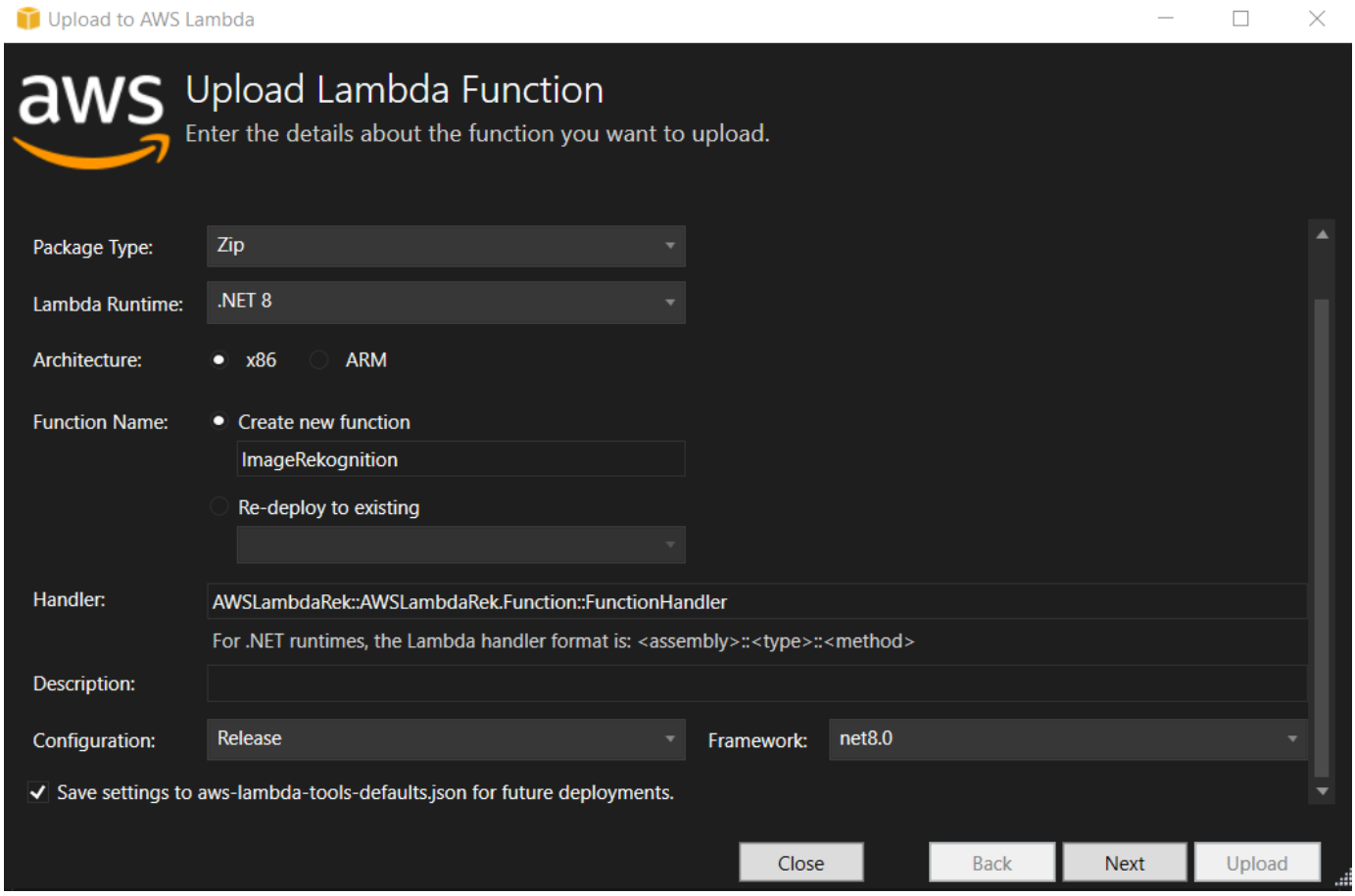
Das folgende Verfahren beschreibt, wie Sie Ihre Lambda-Funktion bereitstellen.

1. Klicken Sie im Solution Explorer mit der rechten Maustaste auf das Lambda-Projekt und wählen Sie In AWS Lambda veröffentlichen, um das Fenster Hochladen in zu AWS Lambda öffnen.

   > **Note**
   >
   > Die voreingestellten Werte werden aus der `aws-lambda-tools-defaults.json` Datei abgerufen.

2. Geben Sie AWS Lambda im Fenster „Hochladen in“ einen Namen in das Feld „Funktionsname“ ein und klicken Sie dann auf „Weiter“, um zum Fenster „Erweiterte Funktionsdetails“ zu gelangen.

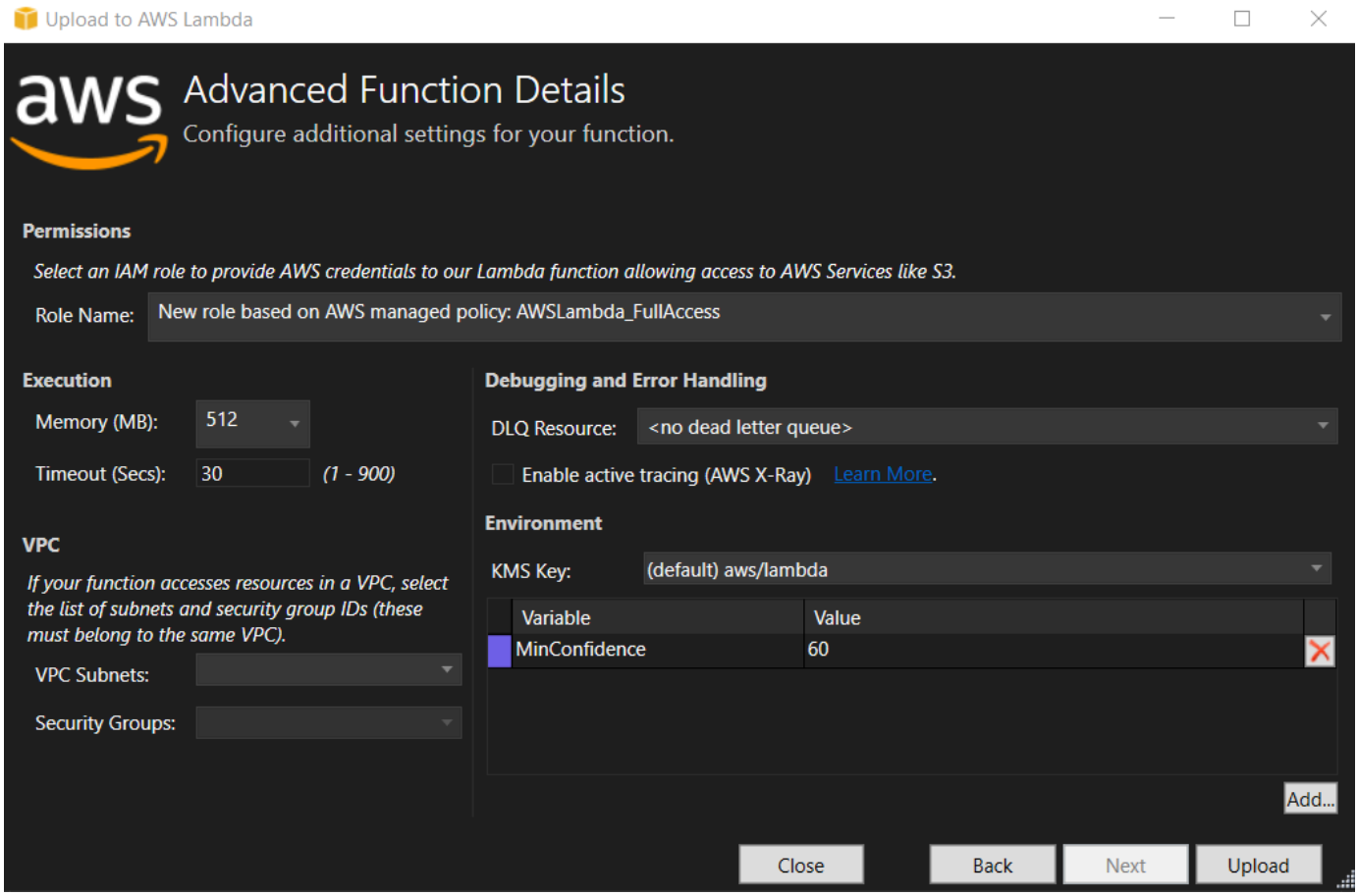
   > **Note**
   >
   > In diesem Beispiel wird der Funktionsname verwendet**`ImageRekognition`**.



3. Wählen Sie im Fenster Erweiterte Funktionsdetails eine IAM-Rolle aus, die Ihrem Code die Erlaubnis erteilt, auf Ihre Amazon S3- und Amazon Rekognition Rekognition-Ressourcen zuzugreifen.

> **Note**
>
> Wenn Sie diesem Beispiel folgen, wählen Sie die Rolle aus. `AWSLambda_FullAccess`

4. Setzen Sie die Umgebungsvariable `MinConfidence` auf 60 und wählen Sie dann Upload, um den Bereitstellungsprozess zu starten. Der Veröffentlichungsvorgang ist abgeschlossen, wenn die Funktionsansicht im AWS Explorer angezeigt wird.



5. Nach einer erfolgreichen Bereitstellung konfigurieren Sie Amazon S3 so, dass seine Ereignisse an Ihre neue Funktion gesendet werden, indem Sie zur Registerkarte Ereignisquellen navigieren.
6. Wählen Sie auf der Registerkarte Ereignisquellen die Schaltfläche Hinzufügen und dann den Amazon S3 S3-Bucket aus, um eine Verbindung mit Ihrer Lambda-Funktion herzustellen.

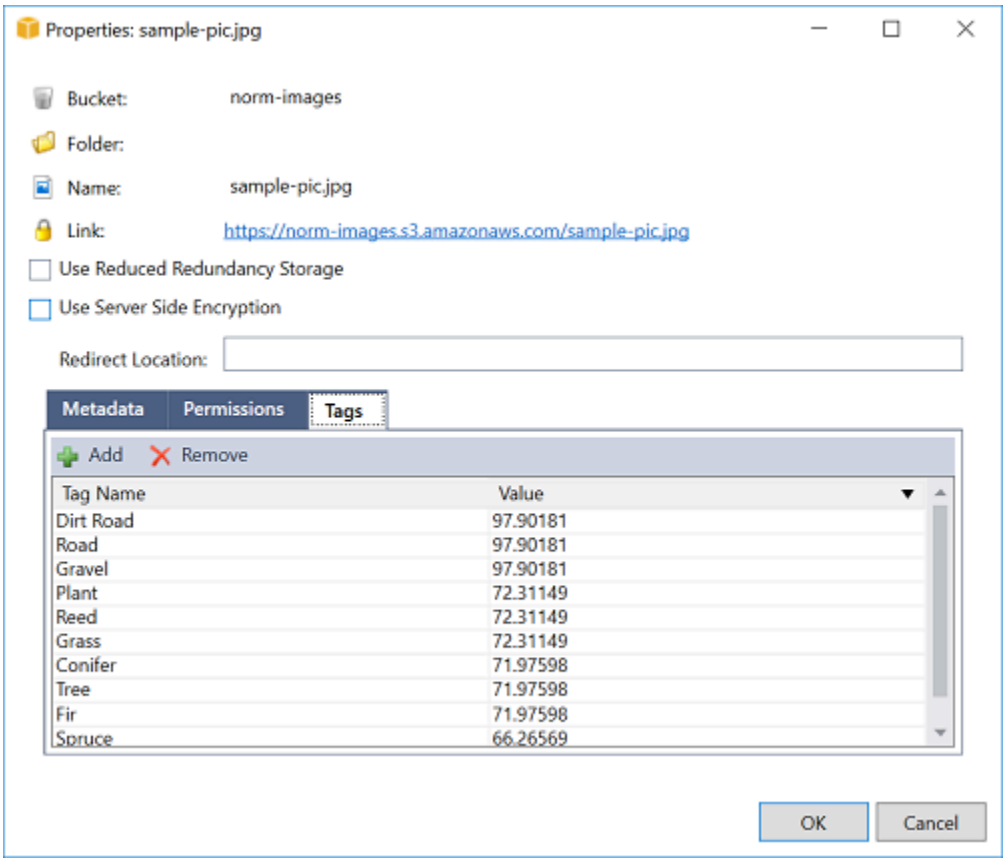
> **Note**
>
> Der Bucket muss sich in derselben AWS Region wie Ihre Lambda-Funktion befinden.

Testen der -Funktion

Nachdem die Funktion nun bereitgestellt und ein S3-Bucket als Ereignisquelle dafür konfiguriert wurde, öffnen Sie im AWS Explorer den S3-Bucket-Browser für den ausgewählten Bucket. Laden Sie anschließend einige Bilder hoch.

Wenn der Upload abgeschlossen ist, können Sie überprüfen, ob Ihre Funktion ausgeführt wurde, indem Sie die Protokolle in der Ansicht Ihrer Funktion einsehen. Oder klicken Sie mit der rechten

Maustaste auf die Bilder im Bucket-Browser und wählen Sie Properties (Eigenschaften) aus. Auf der Registerkarte Tags können Sie die Tags anzeigen, die auf Ihr Objekt angewendet wurden.



Tutorial: Verwenden von Amazon Logging Frameworks mit AWS Lambda zum Erstellen von Anwendungsprotokollen

Sie können Amazon CloudWatch Logs verwenden, um die Protokolle Ihrer Anwendung zu überwachen, zu speichern und darauf zuzugreifen. Um Protokolldaten in CloudWatch Logs zu übernehmen, verwenden Sie ein AWS SDK oder installieren Sie den CloudWatch Logs-Agenten, um bestimmte Protokollordner zu überwachen. CloudWatch Logs ist in mehrere gängige.NET-Logging-Frameworks integriert und vereinfacht so Arbeitsabläufe.

Um mit der Arbeit mit CloudWatch Logs und .NET-Logging-Frameworks zu beginnen, fügen Sie Ihrer Anwendung das entsprechende NuGet Paket und die CloudWatch Logs-Ausgabequelle hinzu und verwenden Sie dann Ihre Logging-Bibliothek wie gewohnt. Auf diese Weise kann Ihre Anwendung Nachrichten mit Ihrem .NET-Framework protokollieren, sie an CloudWatch Logs senden und die Protokollmeldungen Ihrer Anwendung in der CloudWatch Logs-Konsole anzeigen. Sie können in der CloudWatch Logs-Konsole auch Metriken und Alarme einrichten, die auf den Protokollnachrichten Ihrer Anwendung basieren.

Zu den unterstützten.NET-Protokollierungsframeworks gehören:

- NLog: Die Ansicht finden Sie im Paket nuget.org NLog .
- Log4net: Die Ansicht finden Sie im nuget.org Log4net-Paket.
- ASP.NET Core Logging Framework: Eine Ansicht finden Sie im Nuget.org ASP.NET Core Logging Framework-Paket.

Im Folgenden finden Sie ein Beispiel für eine `NLog.config` Datei, die sowohl CloudWatch Logs als auch die Konsole als Ausgabe für Protokollnachrichten aktiviert, indem das `AWS.Logger.NLog` NuGet Paket und das Ziel hinzugefügt werden. 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>
```

Die Logging-Plugins bauen alle auf dem auf AWS SDK für .NET und authentifizieren Ihre AWS Anmeldeinformationen in einem Prozess, der dem SDK ähnelt. Im folgenden Beispiel werden die Berechtigungen beschrieben, die für das Logging-Plug-In für den Zugriff auf CloudWatch Logs erforderlich sind:

> **Note**
>
> Bei AWS den.NET-Logging-Plugins handelt es sich um ein Open-Source-Projekt. Weitere Informationen, Beispielen und Anweisungen finden Sie in den Abschnitten zu Beispielen und Anweisungen im AWS GitHubLogging.NET-Repository.

JSON

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

Bereitstellen auf AWS

Das Toolkit for Visual Studio unterstützt die Anwendungsbereitstellung in AWS Elastic Beanstalk Containern oder AWS CloudFormation Stacks.

> **Note**
>
> Wenn Sie Visual Studio Express Edition verwenden:
>
> - Sie können die Docker-CLI verwenden, um Anwendungen in Amazon ECS-Containern bereitzustellen.
> - Sie können die AWS Management Console verwenden, um Anwendungen in Elastic Beanstalk Beanstalk-Containern bereitzustellen.
>
> Für Elastic Beanstalk Beanstalk-Bereitstellungen müssen Sie zunächst ein Web-Deployment-Paket erstellen. Weitere Informationen finden Sie unter Gewusst wie: Erstellen eines Webbereitstellungspakets in Visual Studio. Für die Amazon ECS-Bereitstellung benötigen Sie ein Docker-Image. Weitere Informationen finden Sie unter Visual Studio Tools for Docker.

Themen

Arbeiten mit Publish to AWS in Visual Studio

Publish to AWS ist eine interaktive Bereitstellungserfahrung, die Sie beim Veröffentlichen Ihrer .NET-Anwendungen für AWS Bereitstellungsziele unterstützt und Anwendungen unterstützt, die auf .NET Core 3.1 und höher abzielen. Wenn Sie mit Publish arbeiten, AWS bleibt Ihr Arbeitsablauf innerhalb von Visual Studio erhalten, indem Sie diese Bereitstellungsfunktionen direkt in Ihrer IDE verfügbar machen:

- Die Möglichkeit, Ihre Anwendung mit einem einzigen Klick bereitzustellen.
- Bereitstellungsempfehlungen auf der Grundlage Ihrer Anwendung.
- Automatische Erstellung von Dockerfiles, je nach Relevanz und Anforderung der Umgebung Ihres Bereitstellungsziels (Bereitstellungsziel).
- Optimierte Einstellungen für die Erstellung und Paketierung Ihrer Anwendungen, wie es Ihr Bereitstellungsziel erfordert.

> **Note**
>
> Weitere Informationen zur Veröffentlichung von.NET Framework-Anwendungen finden Sie im Leitfaden Creating and Deployment von.NET-Anwendungen auf Elastic Beanstalk
> Sie können auch über die .NET-CLI auf Publish to AWS zugreifen. Weitere Informationen finden Sie im AWS Handbuch Bereitstellen von.NET-Anwendungen.

Themen

Voraussetzungen

Um .NET-Anwendungen erfolgreich in einem AWS Dienst zu veröffentlichen, installieren Sie Folgendes auf Ihrem lokalen Gerät:

- .NET Core 3.1+ (einschließlich. NET5 und. NET6): Weitere Informationen zu diesen Produkten und Download-Informationen finden Sie auf der Microsoft-Download-Website.
- Node.js 14.x oder neuere Version: Node.js ist zur Ausführung AWS Cloud Development Kit (AWS CDK) erforderlich. Um Node.js herunterzuladen oder weitere Informationen zu zu erhalten, besuchen Sie die Download-Website Node.js.

> **Note**
>
> Publish to AWS verwendet AWS CDK , um Ihre Anwendung und die gesamte Bereitstellungsinfrastruktur als ein einziges Projekt bereitzustellen. Weitere Informationen dazu AWS CDK finden Sie im Cloud Development Kit Kit-Leitfaden.

- (Optional) Docker wird bei der Bereitstellung in einem containerbasierten Service wie Amazon ECS verwendet. Weitere Informationen und den Download von Docker finden Sie auf der Docker-Downloadseite.

Unterstützte Anwendungstypen

Bevor Sie auf einem neuen oder bestehenden Ziel veröffentlichen, erstellen oder öffnen Sie zunächst einen der folgenden Projekttypen in Visual Studio:

- ASP.NET Core-Anwendung
- .NET-Konsolenanwendung
- Blazor-Anwendung WebAssembly

Veröffentlichen von Anwendungen für Ziele AWS

Beim Veröffentlichen auf einem neuen Ziel AWS führt Sie Publish to durch den Prozess, gibt Empfehlungen und verwendet allgemeine Einstellungen. Wenn Sie für ein Ziel veröffentlichen müssen, das zuvor eingerichtet wurde, werden Ihre Einstellungen gespeichert und können angepasst werden, oder sie stehen sofort für die Bereitstellung mit einem Klick zur Verfügung.

> **Note**
>
> Integration der Toolkits mit dem.NET CLI Server:
> Beim Veröffentlichen wird ein .NET-Serverprozess auf dem Localhost gestartet, um den Veröffentlichungsvorgang durchzuführen.

Auf einem neuen Ziel veröffentlichen

Im Folgenden wird beschrieben, wie Sie Ihre Einstellungen für die AWS Bereitstellung veröffentlichen konfigurieren, wenn Sie auf einem neuen Ziel veröffentlichen.

1. Erweitern Sie im AWS Explorer das Dropdownmenü Anmeldeinformationen und wählen Sie dann das AWS Profil aus, das der Region und den AWS Diensten entspricht, die für Ihre Bereitstellung erforderlich sind.
2. Erweitern Sie das Dropdownmenü Region und wählen Sie dann die AWS Region aus, die die AWS Dienste enthält, die für Ihre Bereitstellung erforderlich sind.
3. Öffnen Sie im Bereich Visual Studio Solutions Explorer das Kontextmenü für den Namen des Projekts (klicken Sie mit der rechten Maustaste darauf) und wählen Sie Veröffentlichen unter aus AWS. Dadurch wird Veröffentlichen unter geöffnet AWS.
4. Wählen Sie unter Veröffentlichen bis AWS die Option In neuem Ziel veröffentlichen aus, um eine neue Bereitstellung zu konfigurieren.

   > **Note**
   >
   > Um Ihre standardmäßigen Anmeldeinformationen für die Bereitstellung zu ändern, wählen oder klicken Sie auf den Link Bearbeiten, der sich neben dem Abschnitt Anmeldeinformationen unter Veröffentlichen unter befindet AWS.
   > Um den Zielkonfigurationsprozess zu umgehen, wählen Sie In vorhandenem Ziel veröffentlichen und wählen dann Ihre bevorzugte Konfiguration aus der Liste Ihrer vorherigen Bereitstellungsziele aus.

5. Wählen Sie im Bereich Ziele veröffentlichen einen AWS Service aus, um Ihre Anwendungsbereitstellung zu verwalten.
6. Wenn Sie mit Ihrer Konfiguration zufrieden sind, wählen Sie Veröffentlichen, um den Bereitstellungsprozess zu starten.

   > **Note**
   >
   > Nach dem Initiieren einer Bereitstellung AWS zeigt Publish to die folgenden Statusmeldungen an:
   >
   > - Während des Bereitstellungsvorgangs AWS zeigt Publish to Informationen über den Fortschritt der Bereitstellung an.

- Nach dem Bereitstellungsprozess AWS gibt Publish to an, ob die Bereitstellung erfolgreich war oder fehlgeschlagen ist.
- Nach einer erfolgreichen Bereitstellung bietet der Bereich Ressourcen zusätzliche Informationen zu der erstellten Ressource. Diese Informationen variieren je nach Art der Anwendung und Bereitstellungskonfiguration.

Auf einem vorhandenen Ziel veröffentlichen

Im Folgenden wird beschrieben, wie Sie Ihre .NET-Anwendung erneut auf einem vorhandenen AWS Ziel veröffentlichen.

1. Erweitern Sie im AWS Explorer das Dropdownmenü Anmeldeinformationen und wählen Sie dann das AWS Profil aus, das der Region und den AWS Diensten entspricht, die für Ihre Bereitstellung erforderlich sind.
2. Erweitern Sie das Dropdownmenü Region und wählen Sie dann die AWS Region aus, die die AWS Dienste enthält, die für Ihre Bereitstellung erforderlich sind.
3. Klicken Sie im Bereich Visual Studio Solutions Explorer mit der rechten Maustaste auf den Namen des Projekts und wählen Sie Veröffentlichen in, AWS um Veröffentlichen unter zu öffnen AWS.
4. Wählen Sie unter AWS Veröffentlichen in die Option In vorhandenem Ziel veröffentlichen aus, um Ihre Bereitstellungsumgebung aus einer Liste vorhandener Ziele auszuwählen.

   > **Note**
   >
   > Wenn Sie kürzlich Anwendungen in der AWS Cloud veröffentlicht haben, werden diese Anwendungen unter Veröffentlichen in angezeigt AWS.

5. Wählen Sie das Veröffentlichungsziel aus, für das Sie Ihre Anwendung bereitstellen möchten, und klicken Sie dann auf Veröffentlichen, um den Bereitstellungsprozess zu starten.

Bereitstellen eines AWS Lambda Projekts mit der.NET Core CLI

Das AWS Toolkit for Visual Studio beinhaltet AWS Lambda .NET Core-Projektvorlagen für Visual Studio. Sie können in Visual Studio erstellte Lambda-Funktionen mithilfe der .NET Core-Befehlszeilenschnittstelle (CLI) bereitstellen.

Themen

Voraussetzungen

Bevor Sie Lambda-Funktionen mit .NET Core CLI bereitstellen können, müssen Sie die folgenden Voraussetzungen erfüllen:

- Stellen Sie sicher, dass Visual Studio 2015 Update 3 installiert ist.
- Installieren Sie .NET Core für Windows.
- Richten Sie die .NET Core-CLI für die Arbeit mit Lambda ein. Weitere Informationen finden Sie unter.NET Core CLI im AWS Lambda Developer Guide.
- Installieren Sie das Toolkit for Visual Studio. Weitere Informationen finden Sie unter Installation des AWS Toolkit for Visual Studio.

Verwandte Themen

Die folgenden verwandten Themen können hilfreich sein, wenn Sie die .NET Core CLI verwenden, um Lambda-Funktionen bereitzustellen:

- Weitere Informationen zu Lambda-Funktionen finden Sie unter Was ist AWS Lambda? im AWS Lambda Entwicklerhandbuch.
- Informationen zum Erstellen von Lambda-Funktionen in Visual Studio finden Sie unterAWS Lambda.
- Weitere Informationen zu Microsoft.NET Core finden Sie unter.NET Core in der Online-Dokumentation von Microsoft.

Liste der Lambda-Befehle, die über die .NET Core CLI verfügbar sind

Gehen Sie wie folgt vor, um die Lambda-Befehle aufzulisten, die über die .NET Core-CLI verfügbar sind.

1. Öffnen Sie ein Befehlszeilenfenster und navigieren Sie zu dem Ordner, der ein Visual Studio-.NET Core-Lambda-Projekt enthält.
2. Geben Sie `dotnet lambda --help` ein.

```
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>
```

Veröffentlichen eines .NET Core Lambda-Projekts über die .NET Core CLI

In den folgenden Anweisungen wird davon ausgegangen, dass Sie AWS Lambda eine.NET-Core-Funktion in Visual Studio erstellt haben.

1. Öffnen Sie ein Befehlszeilenfenster und navigieren Sie zu dem Ordner, der Ihr Visual Studio-.NET Core Lambda-Projekt enthält.
2. Geben Sie `dotnet lambda deploy-function` ein.
3. Wenn Sie dazu aufgefordert werden, geben Sie den Namen der bereitzustellenden Funktion ein. Sie können einen neuen Namen oder den Namen einer bereits vorhandenen Funktion verwenden.
4. Wenn Sie dazu aufgefordert werden, geben Sie die AWS Region ein (die Region, in der Ihre Lambda-Funktion bereitgestellt wird).
5. Wenn Sie dazu aufgefordert werden, wählen oder erstellen Sie die IAM-Rolle, die Lambda bei der Ausführung der Funktion annehmen soll.

Nach erfolgreichem Abschluss wird die Mitteilung New Lambda function created angezeigt.

```
C:\Lambda\AWSLambda1\AWSLambda1>dotnet lambda deploy-function
Executing publish command
... invoking 'dotnet publish', working folder 'C:\Lambda\AWSLambda1\AWSLambda1\bin
\Release\netcoreapp1.0\publish'
... publish: Publishing AWSLambda1 for .NETCoreApp,Version=v1.0
... publish: Project AWSLambda1 (.NETCoreApp,Version=v1.0) will be compiled because
 expected outputs are missing
... publish: Compiling AWSLambda1 for .NETCoreApp,Version=v1.0
... publish: Compilation succeeded.
... publish:     0 Warning(s)
... publish:     0 Error(s)
... publish: Time elapsed 00:00:01.2479713
... publish:
... publish: publish: Published to C:\Lambda\AWSLambda1\AWSLambda1\bin\Release
\netcoreapp1.0\publish
... publish: Published 1/1 projects successfully
Zipping publish folder C:\Lambda\AWSLambda1\AWSLambda1\bin\Release
\netcoreapp1.0\publish to C:\Lambda\AWSLambda1\AWSLamb
da1\bin\Release\netcoreapp1.0\AWSLambda1.zip
Enter Function Name: (AWS Lambda function name)
DotNetCoreLambdaTest
Enter AWS Region: (The region to connect to AWS services)
us-west-2
Creating new Lambda function
Select IAM Role that Lambda will assume when executing function:
    1) lambda_exec_LambdaCoreFunction
    2) *** Create new IAM Role ***
1
```

```
New Lambda function created
```

Wenn Sie eine vorhandene Funktion bereitstellen, fragt die Bereitstellungsfunktion nur nach der AWS Region.

```
C:\Lambda\AWSLambda1\AWSLambda1>dotnet lambda deploy-function
Executing publish command
Deleted previous publish folder
... invoking 'dotnet publish', working folder 'C:\Lambda\AWSLambda1\AWSLambda1\bin
\Release\netcoreapp1.0\publish'
... publish: Publishing AWSLambda1 for .NETCoreApp,Version=v1.0
... publish: Project AWSLambda1 (.NETCoreApp,Version=v1.0) was previously compiled.
 Skipping compilation.
... publish: publish: Published to C:\Lambda\AWSLambda1\AWSLambda1\bin\Release
\netcoreapp1.0\publish
... publish: Published 1/1 projects successfully
Zipping publish folder C:\Lambda\AWSLambda1\AWSLambda1\bin\Release
\netcoreapp1.0\publish to C:\Lambda\AWSLambda1\AWSLamb
da1\bin\Release\netcoreapp1.0\AWSLambda1.zip
Enter Function Name: (AWS Lambda function name)
DotNetCoreLambdaTest
Enter AWS Region: (The region to connect to AWS services)
us-west-2
Updating code for existing function
```

Nachdem Ihre Lambda-Funktion bereitgestellt wurde, ist sie einsatzbereit. Weitere Informationen finden Sie unter Beispiele für die Verwendung von AWS Lambda.

Lambda überwacht Lambda-Funktionen automatisch für Sie und meldet Metriken über Amazon. CloudWatch Informationen zur Überwachung und Problembehebung Ihrer Lambda-Funktion finden Sie unter Fehlerbehebung und Überwachung von AWS Lambda-Funktionen mit Amazon. CloudWatch

Bereitstellung AWS Elastic Beanstalk in Visual Studio mithilfe von AWS Toolkit for Visual Studio mit Amazon Q

AWS Elastic Beanstalk ist ein Service, der den Prozess der Bereitstellung AWS von Ressourcen für Ihre Anwendung vereinfacht. Elastic Beanstalk bietet die gesamte AWS Infrastruktur, die für die Bereitstellung Ihrer Anwendung erforderlich ist. Diese Infrastruktur umfasst:

- EC2 Amazon-Instances, die die ausführbaren Dateien und Inhalte für Ihre Anwendung hosten.
- Eine Auto Scaling Scaling-Gruppe zur Verwaltung der entsprechenden Anzahl von EC2 Amazon-Instances zur Unterstützung Ihrer Anwendung.
- Ein Elastic Load Balancing Load Balancer, der eingehenden Traffic an die EC2 Amazon-Instance mit der größten Bandbreite weiterleitet.

In diesem Abschnitt des Benutzerhandbuchs wird beschrieben, wie Sie mit dem Elastic Beanstalk-Assistenten im AWS Toolkit mit Amazon Q arbeiten. Detaillierte Informationen zu Elastic Beanstalk finden Sie im Developer Guide. AWS Elastic Beanstalk Der Elastic Beanstalk-Assistent für das AWS Toolkit mit Amazon Q wird in den folgenden Themenabschnitten beschrieben.

Themen

Stellen Sie eine herkömmliche ASP.NET-Anwendung auf Elastic Beanstalk bereit

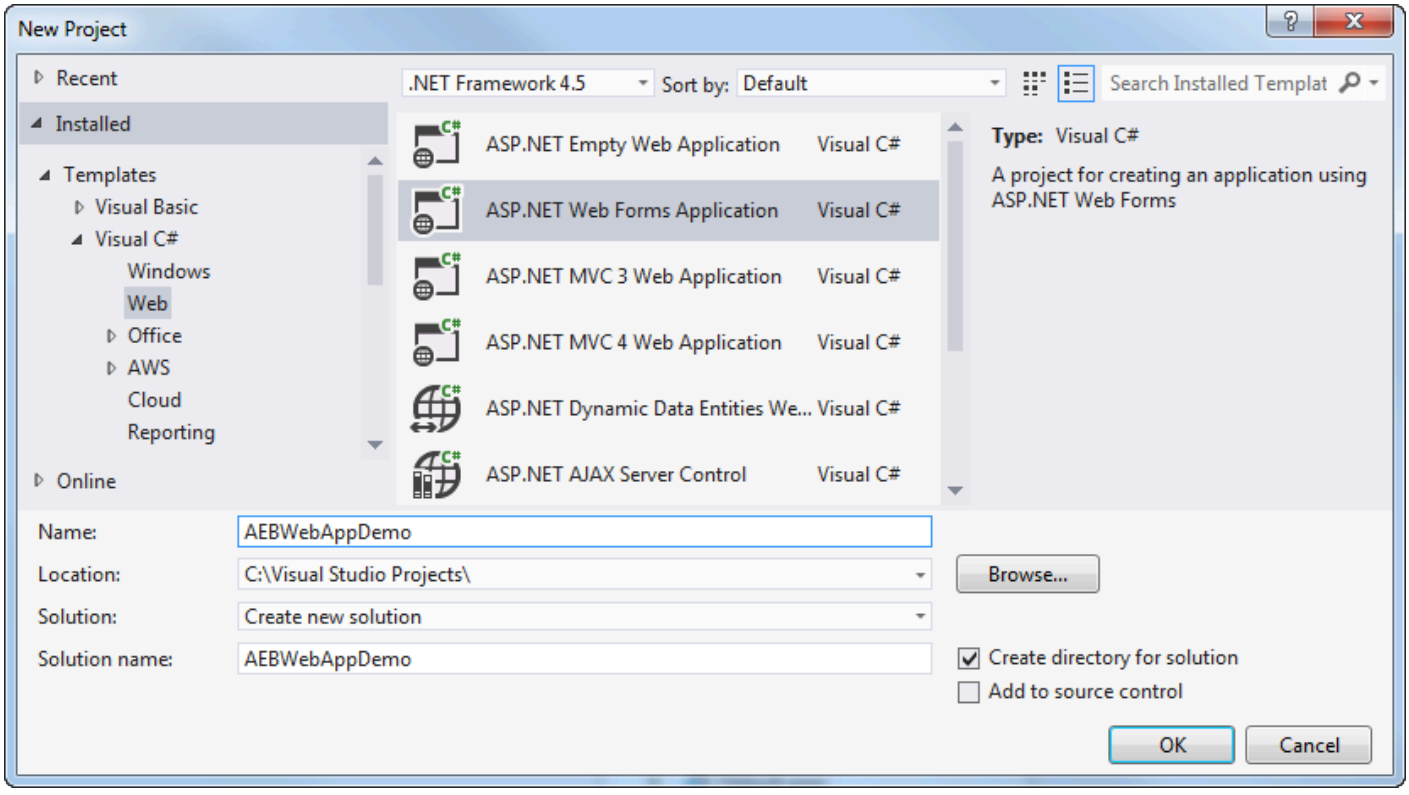
In diesem Abschnitt wird beschrieben, wie Sie den Assistenten für die Veröffentlichung in Elastic Beanstalk verwenden, der als Teil des Toolkit for Visual Studio bereitgestellt wird, um eine Anwendung über Elastic Beanstalk bereitzustellen. Als Übung können Sie eine Instance von einem in Visual Studio integrierten Webanwendungs-Starterprojekt oder Ihr eigenes Projekt verwenden.

> **Note**
>
> Der Assistent unterstützt auch die Bereitstellung von ASP.NET Core-Anwendungen. Informationen zu ASP.NET Core finden Sie im Leitfaden zum AWS .NET-Bereitstellungstool und im aktualisierten Inhaltsverzeichnis Deploying to. AWS

> **Note**
>
> Bevor Sie den Publish to Elastic Beanstalk (Für Elastic Beanstalk bereitstellen)-Assistenten verwenden können, müssen Sie Web Deploy herunterladen und installieren. Der Assistent nutzt Web Deploy, um Internet Information Services (IIS)-Webservern Webanwendungen und Websites bereitzustellen.

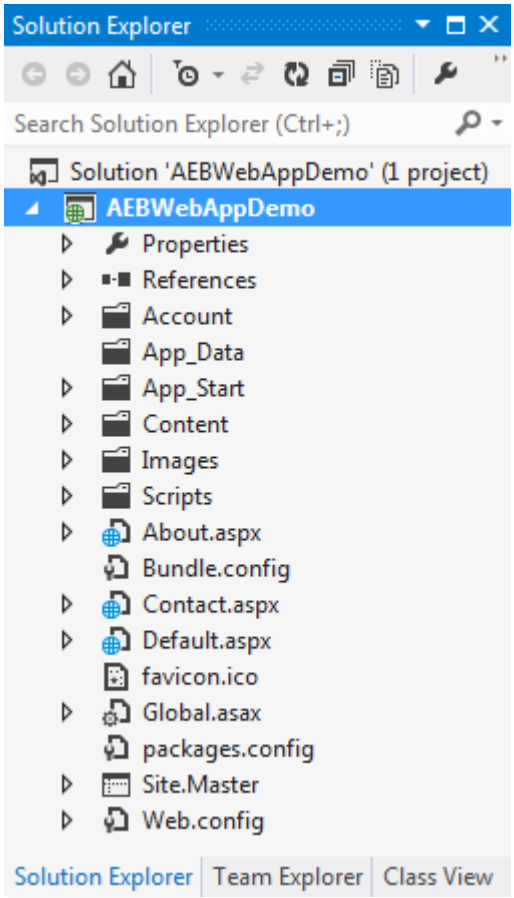
So erstellen Sie ein Beispiel-Webanwendungs-Starterprojekt

1. Wählen Sie im File (Datei)-Menü von Visual Studio New (Neu) aus und dann Project.
2. Erweitern Sie in der Navigationsbereich des Dialogfelds New Project (Neues Projekt) die Option Installed (Installiert), erweitern Sie Templates (Vorlagen) und Visual C#, und wählen Sie dann Web aus.
3. Wählen Sie aus der Liste der Web-Projektvorlagen eine Vorlage, in deren Beschreibung die Wörter `Web` und `Application` enthalten sind. Wählen Sie für dieses Beispiel ASP.NET Web Forms Application (ASP.NET Web Forms-Anwendung) aus.



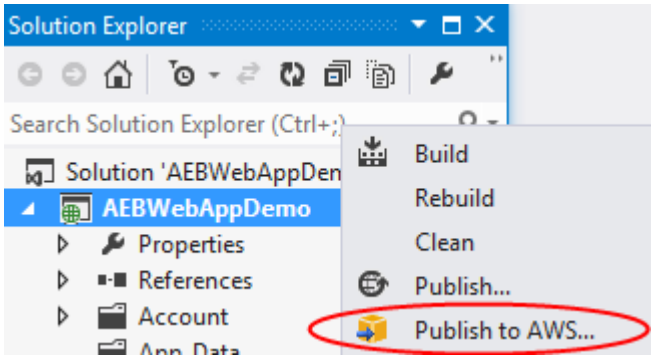
4. Geben Sie im Feld Name die Zeichenfolge `AEBWebAppDemo` ein.

5. Geben Sie im Feld Location (Speicherort) den Pfad zu einem Projektmappenordner auf Ihrem Entwicklungscomputer ein oder klicken Sie auf Browse (Durchsuchen), um einen Projektordner auszuwählen. Klicken Sie anschließend auf Select Folder (Ordner auswählen).
6. Bestätigen Sie die Auswahl des Felds Create directory for solution (Verzeichnis für Lösung erstellen). Prüfen Sie, ob in der Dropdown-Liste Solution (Lösung) die Option Create new solution (Neue Lösung erstellen) ausgewählt ist und klicken Sie dann auf OK. Visual Studio erstellt, basierend auf der ASP.NET-Web Forms Application-Projektvorlage, eine Projektmappe und ein Projekt. Anschließend zeigt Visual Studio den Projektmappen-Explorer an, in dem die neue Lösung und das Projekt zu sehen sind.

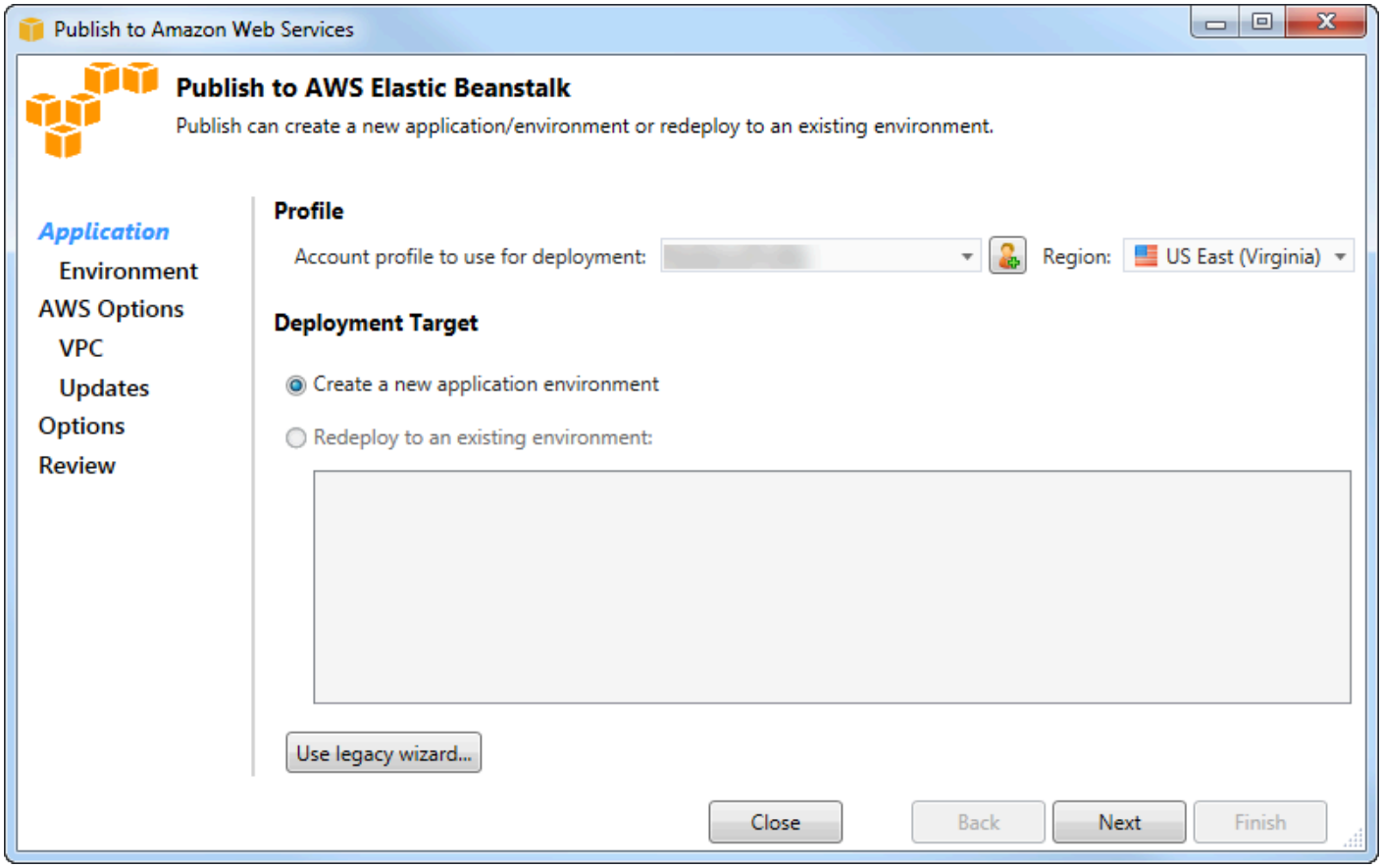


So stellen Sie mit dem "Publish to Elastic Beanstalk"-Assistenten eine Anwendung bereit

1. Öffnen Sie im Solution Explorer das Kontextmenü (Rechtsklick) für den AEBWebAppDemoProjektordner für das Projekt, das Sie im vorherigen Abschnitt erstellt haben, oder öffnen Sie das Kontextmenü für den Projektordner für Ihre eigene Anwendung und wählen Sie In AWS Elastic Beanstalk veröffentlichen.



Der Publish to Elastic Beanstalk (Veröffentlichen zu Elastic Beanstalk)-Assistent wird angezeigt.



2. Wählen Sie unter Profil aus der Dropdownliste Kontoprofil, das für die Bereitstellung verwendet werden soll, das AWS Kontoprofil aus, das Sie für die Bereitstellung verwenden möchten.

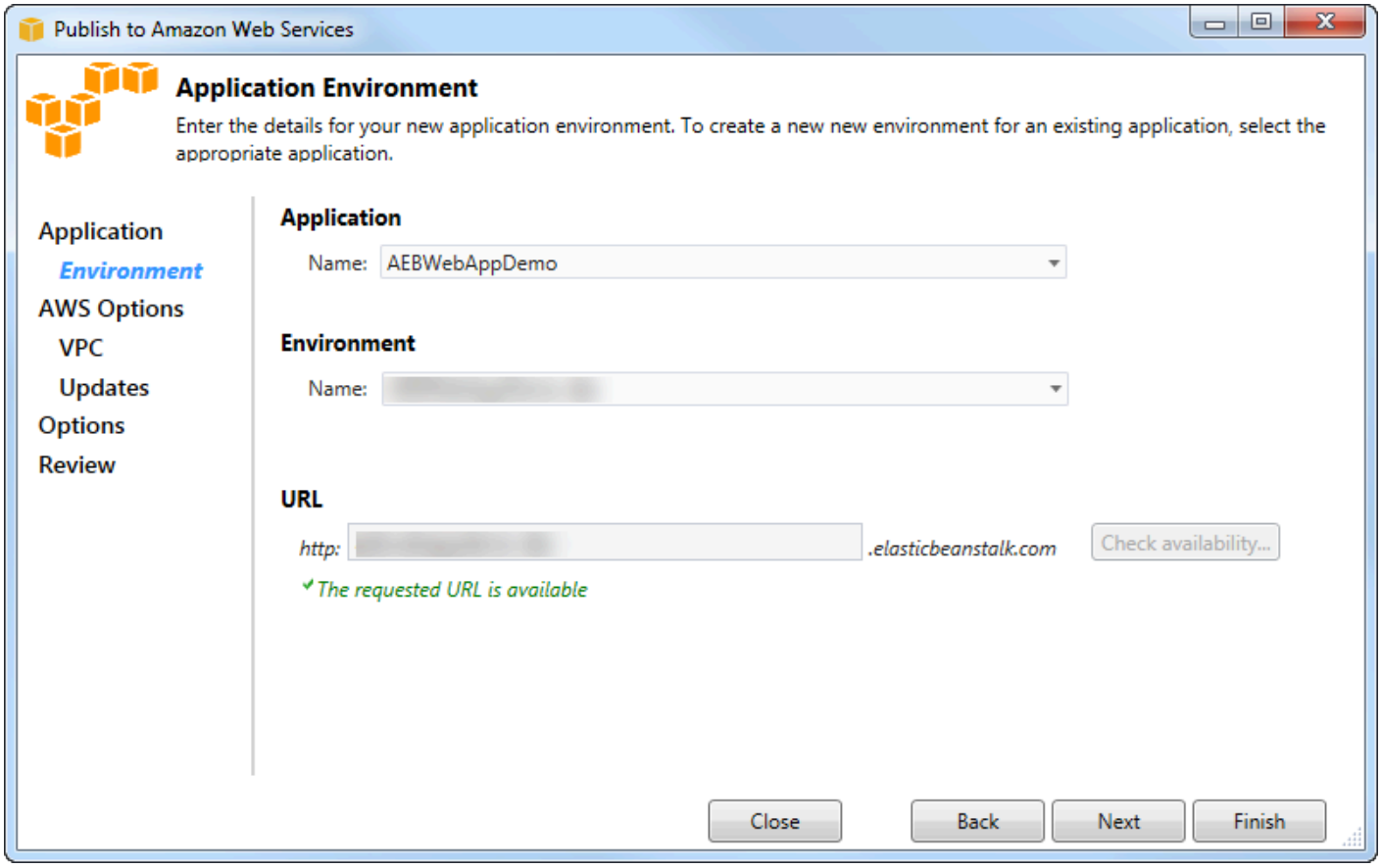
   Wenn Sie ein AWS Konto haben, das Sie verwenden möchten, aber noch kein AWS Kontoprofil dafür erstellt haben, können Sie optional die Schaltfläche mit dem Plussymbol (+) wählen, um ein AWS Kontoprofil hinzuzufügen.

3. Wählen Sie aus der Drop-down-Liste Region die Region aus, in der Elastic Beanstalk die Anwendung bereitstellen soll.

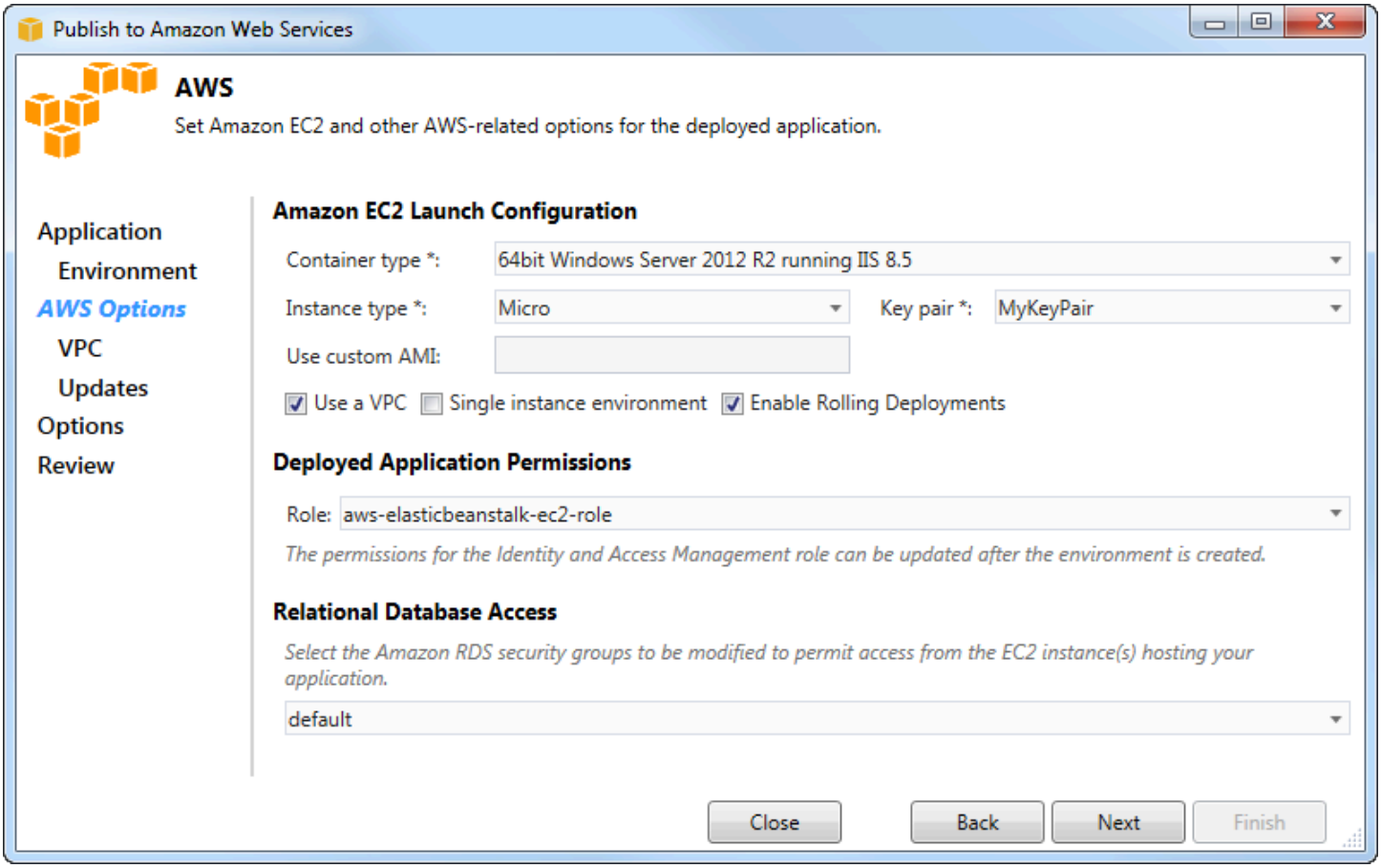
4. In Deployment Target (Bereitstellungsziel) können Sie entweder Create a new application environment (Neue Anwendungsumgebung erstellen) wählen, um eine Anwendung zum ersten Mal bereitzustellen, oder Redeploy to an existing environment (Für eine bestehende Umgebung erneut bereitstellen), um eine bereits verwendete Anwendung erneut bereitzustellen. (Die vorherigen Bereitstellungen wurden möglicherweise entweder mit dem Assistenten oder dem veralteten Standalone Deployment Tool durchgeführt.) Wenn Sie Redeploy to an existing environment (Für eine bestehende Umgebung erneut bereitstellen) wählen, kann es zu Verzögerungen kommen, während der Assistent Informationen aus früheren Bereitstellungen abruft, die aktuell ausgeführt werden.

   > **Note**
   >
   > Für die Option Redeploy to an existing environment (Für eine bestehende Umgebung erneut bereitstellen) wählen Sie aus der Liste eine Umgebung aus und klicken auf Next (Weiter). Der Assistent bringt Sie dann direkt zur Seite Application Options (Anwendungsoptionen). Wenn Sie zu dieser Route gehen möchten, befolgen Sie direkt die Anweisungen weiter unten in diesem Abschnitt, in denen die Verwendung der Seite Application Options (Anwendungsoptionen beschrieben wird.

5. Wählen Sie Weiter.



6. Auf der Seite Application Environment (Anwendungsumgebung), im Bereich Application (Anwendung), finden Sie in der Dropdown-Liste Name Standardnamensvorschläge für die Anwendung. Sie können den Standardnamen ändern, indem Sie aus der Dropdown-Liste einen anderen Namen auswählen.
7. Geben Sie im Bereich Umgebung in der Drop-down-Liste Name einen Namen für Ihre Elastic Beanstalk Beanstalk-Umgebung ein. In diesem Zusammenhang bezieht sich der Begriff Umgebung auf die Infrastruktur, die Elastic Beanstalk für Ihre Anwendung bereitstellt. Möglicherweise wurde bereits ein Standardname in dieser Dropdown-Liste vorgeschlagen. Wenn nicht bereits ein Standard-Name vorgeschlagen wurde, können Sie einen eingeben oder aus der Dropdown-Liste auswählen, falls weitere Namen verfügbar sind. Der Umgebungsname darf nicht länger als 23 Zeichen sein.
8. Im Bereich URL wird im Feld eine Standard-Subdomäne von `.elasticbeanstalk.com` als URL für Ihre Webanwendung vorgeschlagen. Sie können die Standard-Subdomäne ändern, indem Sie einen neuen Subdomänen-Namen eingeben.
9. Wählen Sie Check Availability (Verfügbarkeit prüfen), um sicherzustellen, dass die URL für Ihre Webanwendung nicht bereits verwendet wird.
10. Wenn die URL für Ihre Webanwendung verwendet werden kann, wählen Sie Next (Weiter).



1. Wählen Sie auf der Seite AWS Optionen in Amazon EC2 Launch Configuration aus der Drop-down-Liste Containertyp einen Amazon Machine Image (AMI) -Typ aus, der für Ihre Anwendung verwendet werden soll.
2. Geben Sie in der Drop-down-Liste Instance-Typ einen EC2 Amazon-Instance-Typ an, der verwendet werden soll. Für dieses Beispiel empfehlen wir, Micro zu verwenden. Dadurch werden die Kosten für die Ausführung der Instance minimiert. Weitere Informationen zu den EC2 Amazon-Kosten finden Sie auf der Seite mit den EC2 Preisen.
3. Wählen Sie in der Drop-down-Liste key pair ein EC2 Amazon-Instance-Schlüsselpaar aus, mit dem Sie sich bei den Instances anmelden möchten, die für Ihre Anwendung verwendet werden.
4. Optional können Sie im Feld Use custom AMI (Angepasstes AMI verwenden) ein benutzerdefiniertes AMI festlegen, mit dem das in der Drop-down-Liste Container type angegebene AMI überschrieben wird. Weitere Informationen zum Erstellen eines benutzerdefinierten AMI finden Sie unter Using Custom AMIs im AWS Elastic Beanstalk Developer Guide und Create an AMI from an Amazon EC2 Instance.
5. Wenn Sie Ihre Instances in einer VPC starten möchten, können Sie hierfür das Feld Use a VPC (Eine VPC verwenden) wählen.

6. Wenn Sie eine einzelne EC2 Amazon-Instance starten und dann Ihre Anwendung darauf bereitstellen möchten, wählen Sie optional das Feld Einzelinstanz-Umgebung aus.

   Wenn Sie dieses Kästchen auswählen, erstellt Elastic Beanstalk trotzdem eine Auto Scaling Scaling-Gruppe, konfiguriert sie aber nicht. Wenn Sie die Auto Scaling Scaling-Gruppe später konfigurieren möchten, können Sie die verwenden AWS Management Console.

7. Wenn Sie die Bedingungen, unter denen Ihre Anwendung in den Instances bereitgestellt wird, kontrollieren möchten, wählen Sie das Feld Enable Rolling Deployments (Roling-Bereitstellungen aktivieren) aus. Sie können dieses Feld nur auswählen, wenn das Feld Single instance environment (Einzel-Instance-Umgebung) deaktiviert ist.

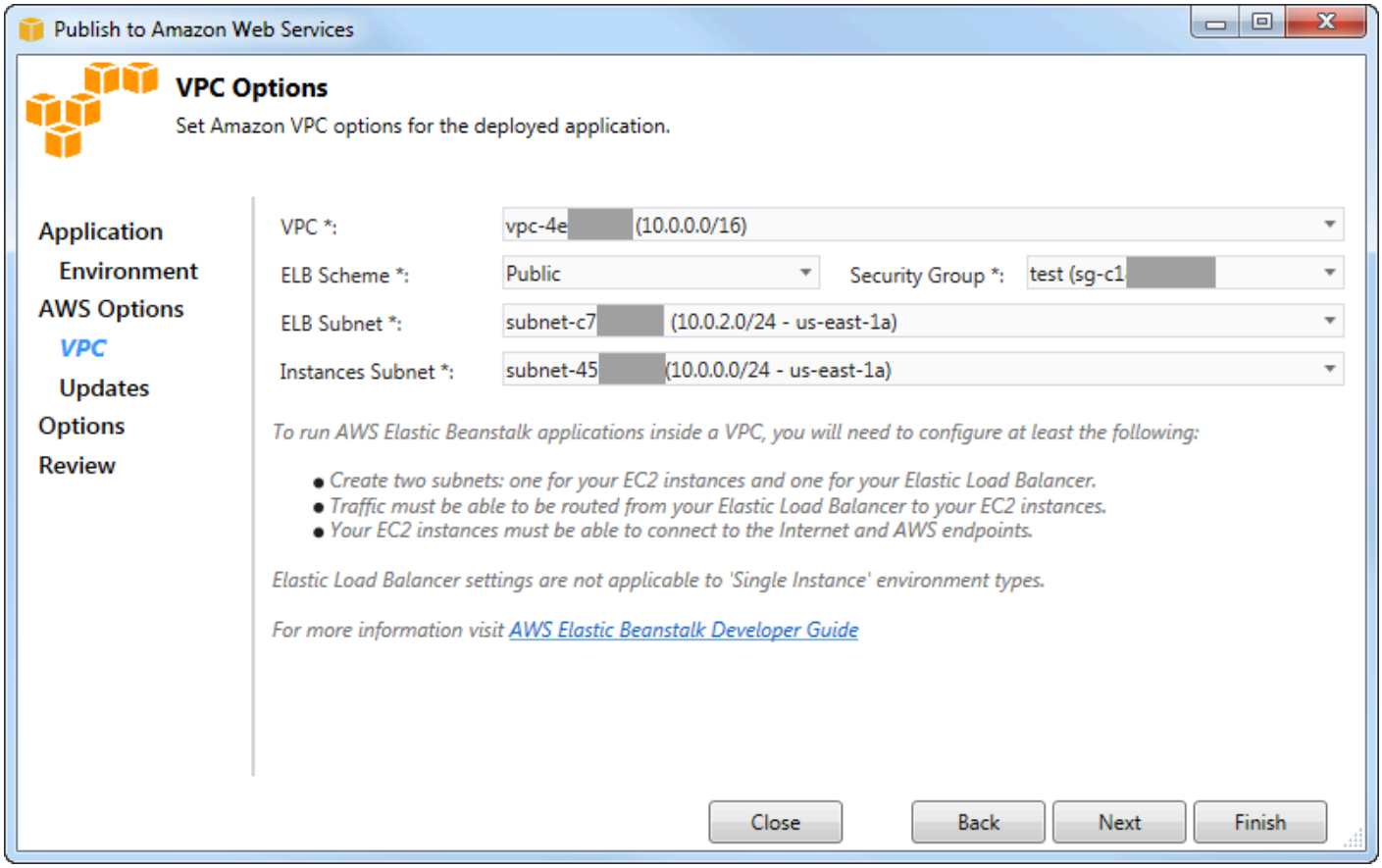
8. Wenn Ihre Anwendung AWS Dienste wie Amazon S3 und DynamoDB verwendet, verwenden Sie am besten eine IAM-Rolle, um Anmeldeinformationen bereitzustellen. Im Bereich Berechtigungen für bereitgestellte Anwendungen können Sie entweder eine bestehende IAM-Rolle auswählen oder eine erstellen, mit der der Assistent Ihre Umgebung startet. Anwendungen, die die verwenden, verwenden AWS SDK für .NET automatisch die von dieser IAM-Rolle bereitgestellten Anmeldeinformationen, wenn sie eine Anfrage an AWS einen Dienst stellen.

9. Wenn Ihre Anwendung auf eine Amazon RDS-Datenbank zugreift, wählen Sie in der Drop-down-Liste im Bereich Relational Database Access die Kästchen neben allen Amazon RDS-Sicherheitsgruppen aus, die der Assistent aktualisiert, sodass Ihre EC2 Amazon-Instances auf diese Datenbank zugreifen können.

10. Wählen Sie Weiter.

    - Wenn Sie Use a VPC (Eine VPC verwenden) ausgewählt haben, wird die Seite VPC Options (VPC-Optionen) angezeigt.
    - Wenn Sie Enable Rolling Deployments (Rolling-Bereitstellungen aktivieren) ausgewählt haben, aber Use a VPC (VPC verwenden) deaktiviert ist, wird die Seite Rolling Deployments (Rolling-Bereitstellungen) angezeigt. Gehen Sie direkt zu den Anweisungen weiter unten in diesem Abschnitt, in denen die Verwendung der Seite Rolling Deployments (Rolling-Bereitstellungen) beschrieben wird.
    - Wenn Sie Use a VPC (Eine VPC verwenden) oder Enable Rolling Deployments (Rolling-Bereitstellungen aktivieren) nicht ausgewählt haben, wird die Seite Application Options (Anwendungsoptionen) angezeigt. Gehen Sie direkt zu den Anweisungen weiter unten in diesem Abschnitt, in denen die Verwendung der Seite Application Options (Anwendungsoptionen) beschrieben wird.

11. Wenn Sie Use a VPC (Eine VPC verwenden) ausgewählt haben, geben Sie auf der Seite VPC Options (VPC-Optionen) die erforderlichen Informationen an, um Ihre Anwendung in einer VPC zu starten.



Die VPC muss bereits erstellt worden sein. Wenn Sie die VPC im Toolkit for Visual Studio erstellt haben, füllt das Toolkit for Visual Studio diese Seite für Sie aus. Wenn Sie die VPC in der AWS Management Console erstellt haben, geben Sie auf dieser Seite Informationen zu Ihrer VPC ein.

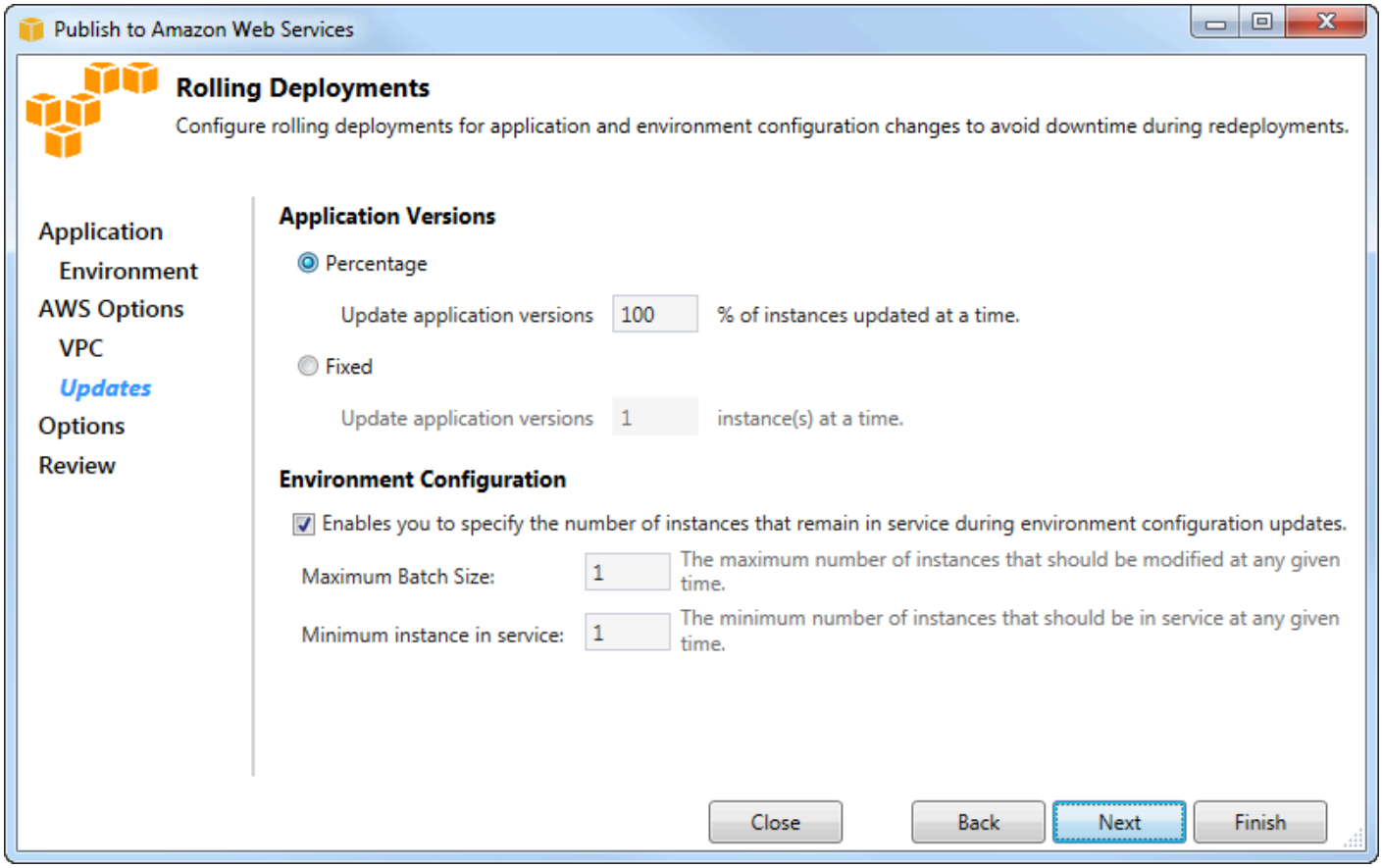
Wichtige Überlegungen für die Bereitstellung in einer VPC

- Ihre VPC muss über mindestens ein öffentliches und ein privates Subnetz verfügen.
- Geben Sie in der Dropdown-Liste ELB Subnet das öffentliche Subnetz an. Das Toolkit for Visual Studio stellt den Elastic Load Balancing Load Balancer für Ihre Anwendung im öffentlichen Subnetz bereit. Das öffentliche Subnetz ist mit einer Routing-Tabelle verknüpft, die über einen Eingang verfügt, der auf ein Internet-Gateway verweist. Sie können ein Internet-Gateway daran erkennen, dass seine ID mit `igw-` (z. B.: `igw-83cddaex`) beginnt. Öffentliche Subnetze, die Sie mit dem Toolkit for Visual Studio erstellen, verfügen über Tagwerte, die sie als öffentlich kennzeichnen.

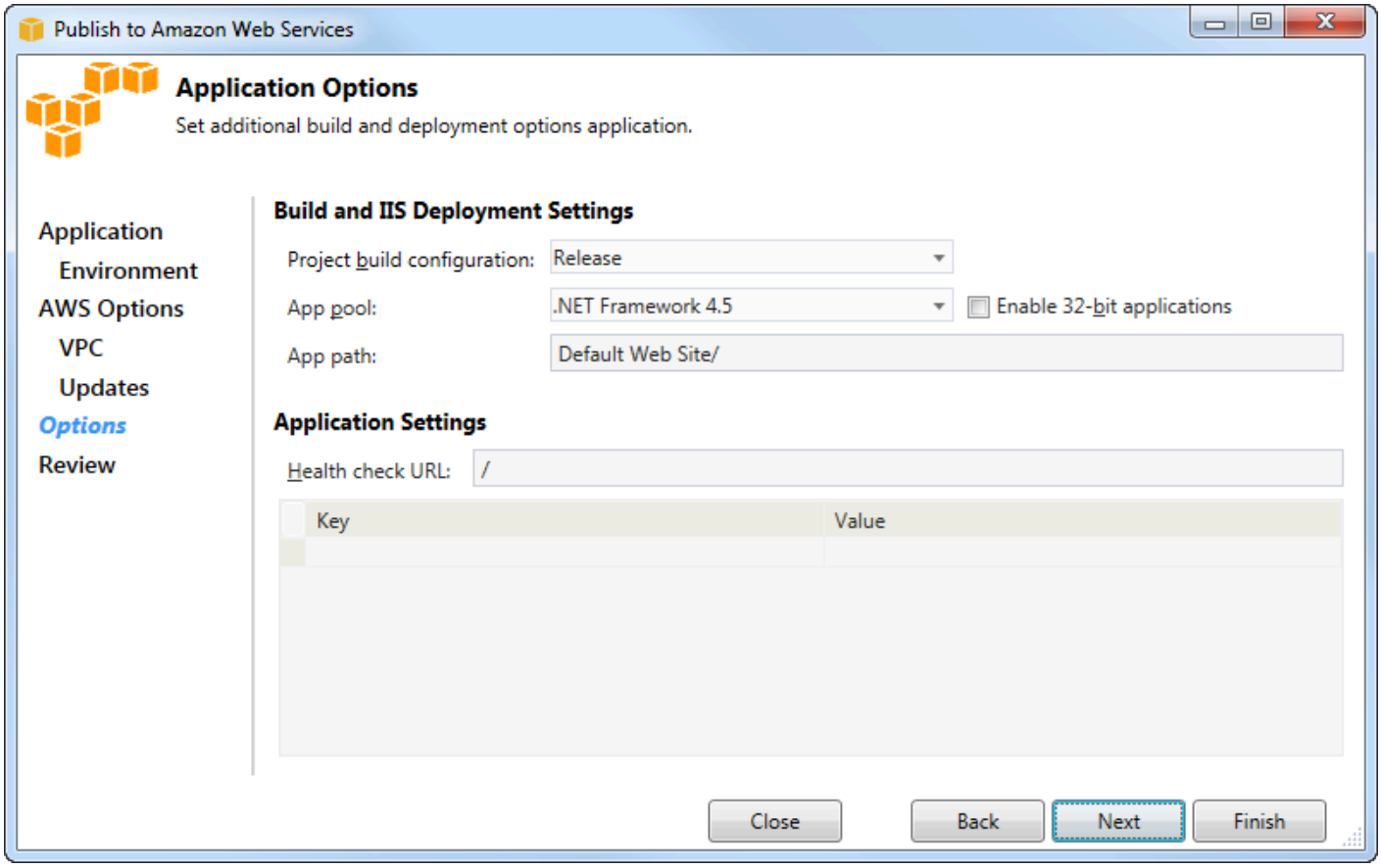
- Geben Sie in der Dropdown-Liste Instances Subnet das private Subnetz an. Das Toolkit for Visual Studio stellt die EC2 Amazon-Instances für Ihre Anwendung im privaten Subnetz bereit.
- Die EC2 Amazon-Instances für Ihre Anwendung kommunizieren vom privaten Subnetz mit dem Internet über eine EC2 Amazon-Instance im öffentlichen Subnetz, die Network Address Translation (NAT) durchführt. Um diese Kommunikation zu ermöglichen, benötigen Sie eine VPC-Sicherheitsgruppe, die zulässt, dass Datenverkehr vom privaten Subnetz zur NAT-Instance fließt. Geben Sie diese VPC-Sicherheitsgruppe in der Dropdown-Liste Security Group an.

Weitere Informationen zur Bereitstellung einer Elastic Beanstalk-Anwendung in einer VPC finden Sie im AWS Elastic Beanstalk Developer Guide.

1. Nachdem Sie alle Informationen auf der Seite VPC Options (VPC-Optionen) eingegeben haben, wählen Sie Next (Weiter).
   - Wenn Sie Enable Rolling Deployments (Rolling-Bereitstellungen aktivieren) ausgewählt haben, wird die Seite Rolling Deployments (Rolling-Bereitstellungen) angezeigt.
   - Wenn Sie Enable Rolling Deployments (Rolling-Bereitstellungen aktivieren) nicht ausgewählt haben, ist die Seite Application Options (Anwendungsoptionen) zu sehen. Gehen Sie direkt zu den Anweisungen weiter unten in diesem Abschnitt, in denen die Verwendung der Seite Application Options (Anwendungsoptionen) beschrieben wird.
2. Wenn Sie Enable Rolling Deployments (Rolling-Bereitstellungen aktivieren) ausgewählt haben, geben Sie auf der Seite Rolling Deployments (Rolling-Bereitstellungen) Informationen zur Art und Weise ein, wie neue Versionen Ihrer Anwendungen in den Instances in einer lastverteilten Umgebung bereitgestellt werden. Wenn beispielsweise vier Instances in Ihrer Umgebung vorhanden sind und Sie den Instance-Typ ändern möchten, können Sie die Umgebung so konfigurieren, dass zwei Instances gleichzeitig geändert werden. So stellen Sie sicher, dass die Anwendung weiterhin ausgeführt wird, während die Änderungen vorgenommen werden.



3. Wählen Sie im Bereich Application Versions eine Option aus, mit der die Bereitstellungen entweder nach einem Prozentsatz oder nach der Anzahl an gleichzeitigen Instances gesteuert werden. Geben Sie den gewünschten Prozentsatz bzw. die gewünschte Zahl an.
4. Optional können Sie auch im Bereich Environment Configuration das Feld auswählen, wenn Sie die Anzahl an Instances festlegen möchten, die während Bereitstellungen weiter ausgeführt werden. Wenn Sie dieses Feld auswählen, legen Sie entweder die maximale Anzahl an Instances fest, die gleichzeitig geändert werden sollen, oder die Mindestanzahl an Instances, die gleichzeitig weiter ausgeführt werden sollen, oder beides.
5. Wählen Sie Weiter.
6. Geben Sie auf der Seite Application Options (Anwendungsoptionen) Informationen zum Build, den Internet Information Services (IIS) und den Anwendungseinstellungen an.



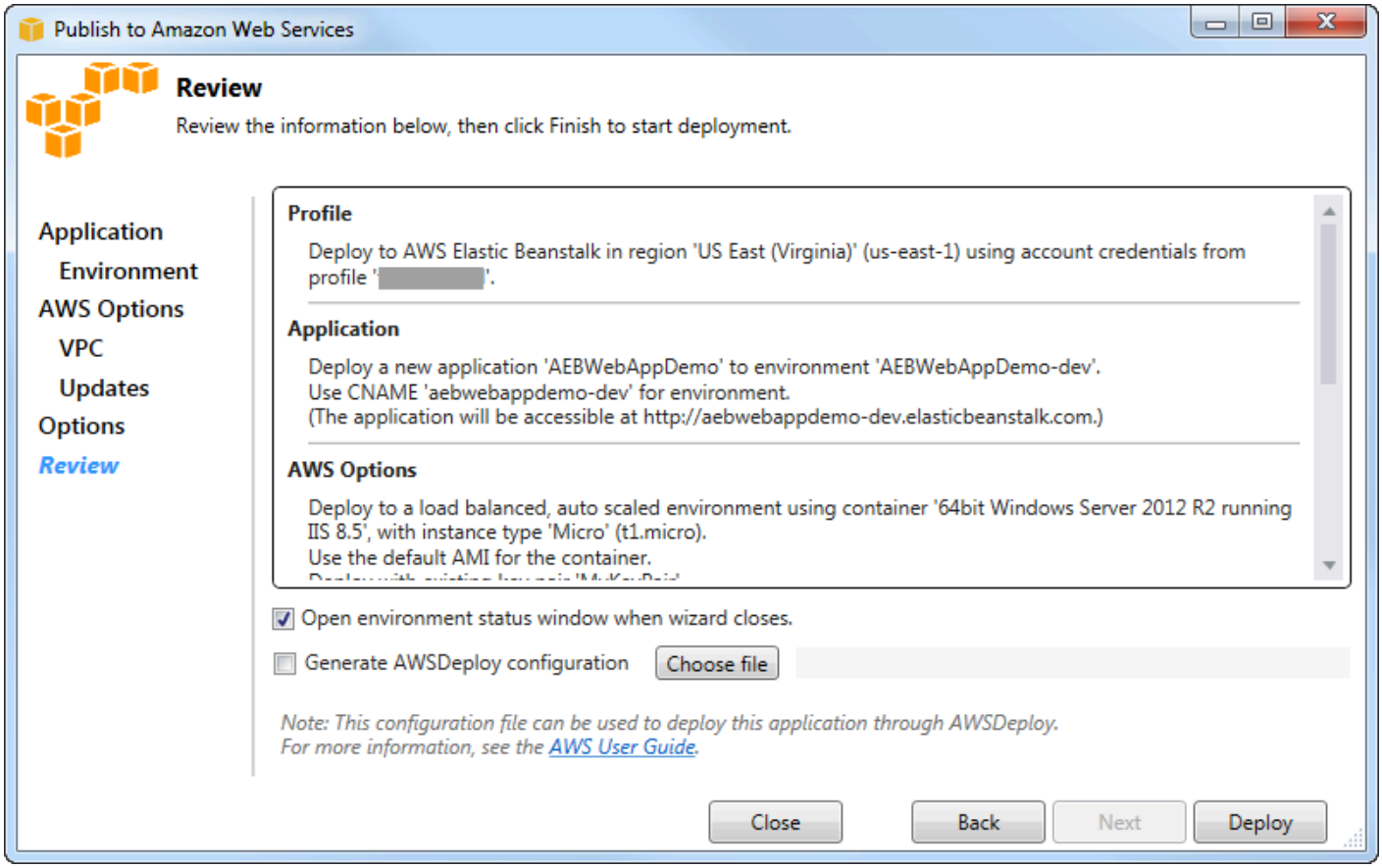
7. Wählen Sie im Bereich Build and IIS Deployment Settings (Build- und IIS-Bereitstellungseinstellungen) aus der Dropdown-Liste Project build configuration (Projekt-Buildkonfiguration) die Ziel-Buildkonfiguration aus. Wenn der Assistent diese findet, wird Release (Version) angezeigt. Andernfalls erscheint die aktive Konfiguration in dieser Box.
8. Wählen Sie aus der Dropdown-Liste App pool (App-Pool) die Version des für Ihre Anwendung erforderlichen .NET Framework aus. Die richtige .NET Framework-Version sollte bereits angezeigt werden.
9. Wenn Sie eine 32-Bit-Anwendung haben, wählen Sie das Feld Enable 32-bit application (32-Bit-Anwendungen aktivieren).
10. Geben Sie im Feld App path (App-Pfad) den Pfad an, den IIS für die Bereitstellung der Anwendung verwenden soll. Standardmäßig ist Default Web Site/ angegeben, wobei es sich in der Regel um den Pfad `c:\inetpub\wwwroot` handelt. Wenn Sie einen anderen Pfad als Default Web Site/ angeben, platziert der Assistent eine Umleitung im Pfad Default Web Site/, die auf den von Ihnen angegebenen Pfad verweist.
11. Geben Sie im Bereich Anwendungseinstellungen im Feld Health Check URL eine URL für Elastic Beanstalk ein, um zu überprüfen, ob Ihre Webanwendung noch reagiert. Diese URL hängt von der Root-Server-URL ab. Die Root-Server-URL ist standardmäßig festgelegt. Wenn die komplette

URL beispielsweise `example.com/site-is-up.html` lautet, würden Sie Folgendes eingeben: `/site-is-up.html`.

12. Im Bereich für Key (Schlüssel) und Value können Sie alle Schlüssel- und Wertepaare festlegen, die Sie der `Web.config`-Datei Ihrer Anwendung hinzufügen möchten.

> **Note**
>
> Obwohl dies nicht empfohlen wird, können Sie den Bereich für Schlüssel und Wert verwenden, um AWS Anmeldeinformationen anzugeben, unter denen Ihre Anwendung ausgeführt werden soll. Der bevorzugte Ansatz besteht darin, eine IAM-Rolle in der Dropdownliste Identity and Access Management Zugriffsverwaltungsrolle auf der Seite AWS Optionen anzugeben. Wenn Sie jedoch AWS Anmeldeinformationen anstelle einer IAM-Rolle verwenden müssen, um Ihre Anwendung auszuführen, wählen AWSAccess Sie in der Zeile Schlüssel die Option Schlüssel aus. Geben Sie in der Zeile Value (Wert) den Zugriffsschlüssel ein. Wiederholen Sie diese Schritte für AWSSecretKey.

13. Wählen Sie Weiter.



14. Prüfen Sie auf der Seite Review (Prüfen) die Optionen, die Sie konfiguriert haben, und wählen Sie das Feld Open environment status window when wizard closes (Umgebungsstatusfenster beim Schließen des Assistenten öffnen) aus.
15. Wenn alles richtig ist, klicken Sie auf Deploy (Bereitstellen).

> **Note**
>
> Wenn Sie die Anwendung bereitstellen, fallen für das aktive Konto Gebühren für die von der Anwendung verwendeten AWS Ressourcen an.

In der Statusleiste von Visual Studio und im Fenster Output (Ausgabe) werden Informationen über die Bereitstellung angezeigt. Dieser Vorgang kann einige Minuten dauern. Wenn die Bereitstellung abgeschlossen ist, wird im Fenster Output (Ausgabe) eine Bestätigung angezeigt.

16. Um das Deployment zu löschen, erweitern Sie im AWS Explorer den Elastic Beanstalk-Knoten, öffnen Sie das Kontextmenü (Rechtsklick) für den Unterknoten für das Deployment und wählen Sie dann Löschen. Das Löschen kann einige Minuten dauern.

Bereitstellen einer ASP.NET-Core-Anwendung auf Elastic Beanstalk (Legacy)

> **Important**
>
> Diese Dokumentation bezieht sich auf ältere Dienste und Funktionen. Aktualisierte Anleitungen und Inhalte finden Sie im Leitfaden für das Bereitstellungstool AWS für.NET und im aktualisierten AWS Inhaltsverzeichnis Deploying to.

AWS Elastic Beanstalk ist ein Dienst, der die Bereitstellung von AWS Ressourcen für Ihre Anwendung vereinfacht. AWS Elastic Beanstalk stellt die gesamte AWS Infrastruktur bereit, die für die Bereitstellung Ihrer Anwendung erforderlich ist.

Das Toolkit for Visual Studio unterstützt die Bereitstellung von ASP.NET Core-Anwendungen AWS mithilfe von Elastic Beanstalk. ASP.NET Core ist die überarbeitete Version von ASP.NET mit einer modularisierten Architektur, dank der die Verwaltungsabhängigkeit auf ein Minimum reduziert wird.

Außerdem optimiert ASP.NET Core Ihre Anwendung, sodass sie in der Cloud ausgeführt werden kann.

AWS Elastic Beanstalk macht es einfach, Anwendungen in einer Vielzahl von verschiedenen Sprachen bereitzustellen. AWS Elastic Beanstalk unterstützt sowohl traditionelle ASP.NET-Anwendungen als auch ASP.NET Core-Anwendungen. In diesem Thema wird die Bereitstellung von ASP.NET-Core-Anwendungen beschrieben.

Verwenden des Bereitstellungsassistenten

Der einfachste Weg, ASP.NET Core-Anwendungen auf Elastic Beanstalk bereitzustellen, ist das Toolkit for Visual Studio.

Wenn Sie das Toolkit bereits für die Bereitstellung herkömmlicher ASP. NET-Anwendungen eingesetzt haben, werden Sie feststellen, dass der Ablauf mit ASP.NET Core ganz ähnlich ist. Die folgenden Schritte führen Sie durch den Bereitstellungsvorgang.

Wenn Sie das Toolkit noch nie zuvor verwendet haben, müssen Sie nach der Installation des Toolkits zunächst Ihre Anmeldeinformationen beim Toolkit registrieren. AWS Einzelheiten dazu finden Sie in der Dokumentation So geben Sie die AWS Sicherheitsanmeldedaten für Ihre Anwendung für Visual Studio an.

Um eine ASP.NET Core-Webanwendung bereitzustellen, klicken Sie im Solution Explorer mit der rechten Maustaste auf das Projekt und wählen Sie Veröffentlichen in AWS... aus.

Wählen Sie auf der ersten Seite des Publish to AWS Elastic Beanstalk Deployment Wizards aus, ob Sie eine neue Elastic Beanstalk Beanstalk-Anwendung erstellen möchten. Eine Elastic Beanstalk-Anwendung ist eine logische Sammlung von Elastic Beanstalk-Komponenten, einschließlich Umgebungen, Versionen und Umgebungskonfigurationen. Der Bereitstellungsassistent erzeugt eine Anwendung, die wiederum eine Sammlung von Anwendungsversionen und Umgebungen enthält. Die Umgebungen enthalten die eigentlichen AWS Ressourcen, auf denen eine Anwendungsversion ausgeführt wird. Jedes Mal, wenn Sie eine Anwendung bereitstellen, wird eine neue Anwendungsversion erstellt und der Assistent verweist die Umgebung auf diese Version. Weitere Informationen zu diesen Konzepten finden Sie in Elastic Beanstalk Components.

Als Nächstes legen Sie Namen für die Anwendung und die erste Umgebung fest. Jeder Umgebung ist ein einzigartiger CNAME zugewiesen, mit dem Sie auf die Anwendung zugreifen können, wenn die Bereitstellung abgeschlossen ist.

Auf der nächsten Seite, AWS Optionen, können Sie die Art der zu AWS verwendenden Ressourcen konfigurieren. Verwenden Sie für dieses Beispiel die Standardwerte, mit Ausnahme des Abschnitts

Key pair (Schlüsselpaar). Schlüsselpaare ermöglichen Ihnen, das Windows-Administratorpasswort abzurufen, sodass Sie sich bei Ihrem Computer anmelden können. Wenn Sie noch kein Schlüsselpaar erstellt haben, können Sie die Option Create new key pair (Neues Schlüsselpaar erstellen) auswählen.

Berechtigungen

Die Seite „Berechtigungen“ wird verwendet, um den EC2 Instances, auf denen Ihre Anwendung ausgeführt wird, AWS Anmeldeinformationen zuzuweisen. Dies ist wichtig, wenn Ihre Anwendung die für den Zugriff AWS SDK für .NET auf andere AWS Dienste verwendet. Wenn Sie keine anderen Services über Ihre Anwendung nutzen, können Sie die Standardeinstellungen für diese Seite beibehalten.

Anwendungsoptionen

Die auf der Seite Application Options angegebenen Details unterscheiden sich von denen für die Bereitstellung herkömmlicher ASP.NET-Anwendungen. Hier legen Sie die Build-Konfiguration und das Framework fest, die zum Verpacken Ihrer Anwendung verwendet werden, sowie den IIS-Ressourcenpfad für die Anwendung.

Nach Abschließen der Seite Application Options klicken Sie auf Next (Weiter), um die Einstellungen zu prüfen und dann auf Deploy (Bereitstellen), um den Bereitstellungsprozess zu beginnen.

Überprüfen des Umgebungsstatus

Nachdem die Anwendung gepackt und hochgeladen wurde AWS, können Sie den Status der Elastic Beanstalk Beanstalk-Umgebung überprüfen, indem Sie die Umgebungsstatusansicht im AWS Explorer in Visual Studio öffnen.

Ereignisse werden in der Statusleiste angezeigt, sobald die Umgebung online ist. Wenn alle Vorgänge abgeschlossen sind, wechselt die Umgebung in den fehlerfreien Status. Klicken Sie auf die URL, um die Website anzuzeigen. Von hier aus können Sie auch die Logs aus der Umgebung oder dem Remote-Desktop in die EC2 Amazon-Instances ziehen, die Teil Ihrer Elastic Beanstalk Beanstalk-Umgebung sind.

Die erste Bereitstellung einer Anwendung dauert etwas länger als nachfolgende erneute Bereitstellungen, da dadurch neue Ressourcen entstehen. AWS Wenn Sie während der Entwicklung über Ihre Anwendung iterieren, können Sie schnell eine neue Bereitstellung vornehmen, indem Sie durch die Assistentenschritte zurückgehen oder mit der rechten Maustaste auf das Projekt klicken und die Option Republish (Erneut veröffentlichen) auswählen.

Veröffentlichen Sie Ihre Anwendung erneut mit den Einstellungen aus dem vorherigen Durchlauf über den Deployment Wizard und laden Sie das Anwendungspaket in die bestehende Elastic Beanstalk Beanstalk-Umgebung hoch.

So geben Sie die AWS Sicherheitsanmeldedaten für Ihre Anwendung an

Das AWS Konto, das Sie im Publish to Elastic Beanstalk-Assistenten angeben, ist das AWS Konto, das der Assistent für die Bereitstellung auf Elastic Beanstalk verwendet.

Obwohl dies nicht empfohlen wird, müssen Sie möglicherweise auch AWS Kontoanmeldedaten angeben, mit denen Ihre Anwendung nach der Bereitstellung auf AWS Dienste zugreift. Der bevorzugte Ansatz besteht darin, eine IAM-Rolle anzugeben. Im Assistenten „Auf Elastic Beanstalk veröffentlichen“ verwenden Sie dazu die Dropdownliste „Identity and Access Management Zugriffsverwaltungsrolle“ auf der Seite „AWS Optionen“. Im Legacy-Assistenten „In Amazon Web Services veröffentlichen“ verwenden Sie dazu die Dropdownliste „IAM-Rolle“ auf der Seite „AWS Optionen“.

Wenn Sie anstelle einer IAM-Rolle AWS Kontoanmeldeinformationen verwenden müssen, können Sie die AWS Kontoanmeldedaten für Ihre Anwendung auf eine der folgenden Arten angeben:

- Verweisen Sie im `appSettings` Element der `Web.config` Projektdatei auf ein Profil, das den AWS Kontoanmeldedaten entspricht. (Informationen zum Erstellen eines Profils finden Sie unter AWS Anmeldeinformationen konfigurieren.) Im folgenden Beispiel werden Anmeldeinformationen angegeben, deren Profilname `myProfile` lautet.

  ```
  <appSettings>
    <!-- AWS CREDENTIALS -->
    <add key="AWSProfileName" value="myProfile"/>
  </appSettings>
  ```

- Wenn Sie den Assistenten „In Elastic Beanstalk veröffentlichen“ verwenden, wählen Sie auf der Seite „Anwendungsoptionen“ in der Zeile „Schlüssel“ des Bereichs „Schlüssel“ und „Wert“ aus. AWS AccessKey Geben Sie in der Zeile Value (Wert) den Zugriffsschlüssel ein. Wiederholen Sie diese Schritte für. AWS SecretKey
- Wenn Sie den Legacy-Assistenten Publish to Amazon Web Services (Für Amazon Web Services veröffentlichen) verwenden, wählen Sie auf der Seite Application Options (Anwendungsoptionen) im Bereich Application Credentials (Anwendungsanmeldeinformationen) die Option Use these credentials (Diese Anmeldeinformationen verwenden) aus und geben dann den Zugriffsschlüssel

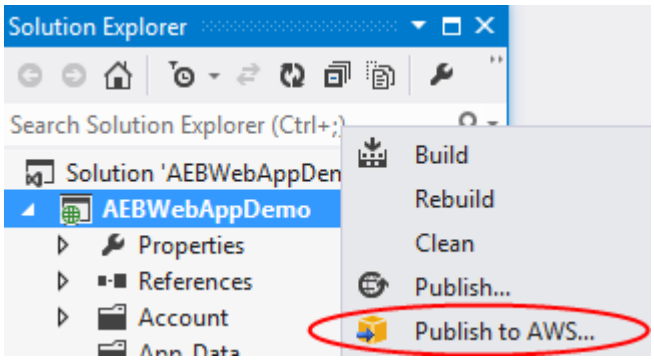
und den geheimen Zugriffsschlüssel in die Felder Access Key (Zugriffsschlüssel) und Secret Key (Secret-Schlüssel) ein.

So veröffentlichen Sie Ihre Anwendung erneut in einer Elastic Beanstalk Beanstalk-Umgebung (Legacy)

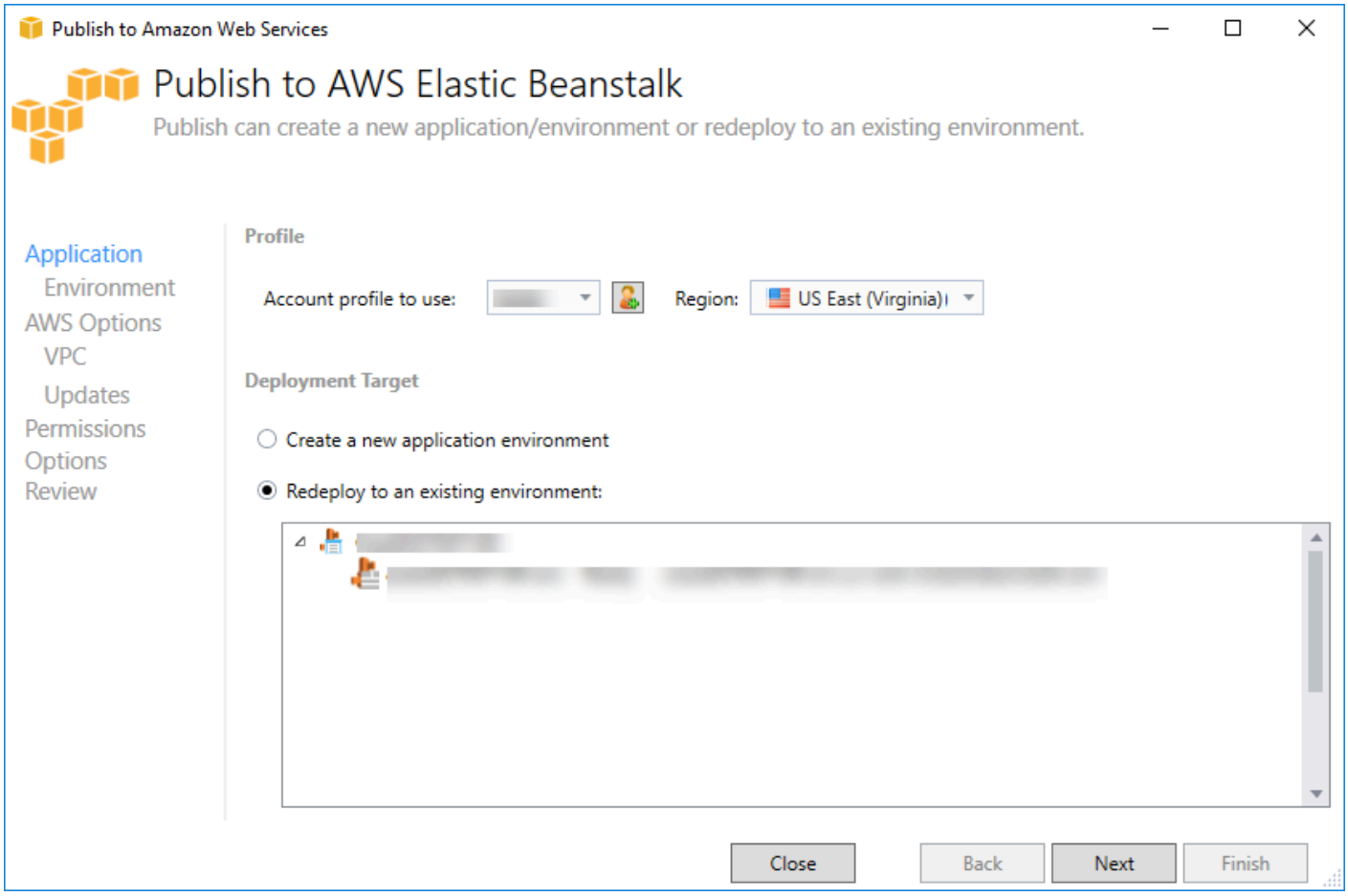
> **Important**
>
> Diese Dokumentation bezieht sich auf ältere Dienste und Funktionen. Aktualisierte Anleitungen und Inhalte finden Sie im Leitfaden zum AWS .NET Deployment Tool.

Sie können an Ihrer Anwendung iterieren, indem Sie einzelne Änderungen vornehmen und dann eine neue Version erneut in Ihrer bereits gestarteten Elastic Beanstalk Beanstalk-Umgebung veröffentlichen.

1. Öffnen Sie im Solution Explorer das Kontextmenü (Rechtsklick) für den AEBWebAppDemoProjektordner für das Projekt, das Sie im vorherigen Abschnitt veröffentlicht haben, und wählen Sie Veröffentlichen in. AWS Elastic Beanstalk

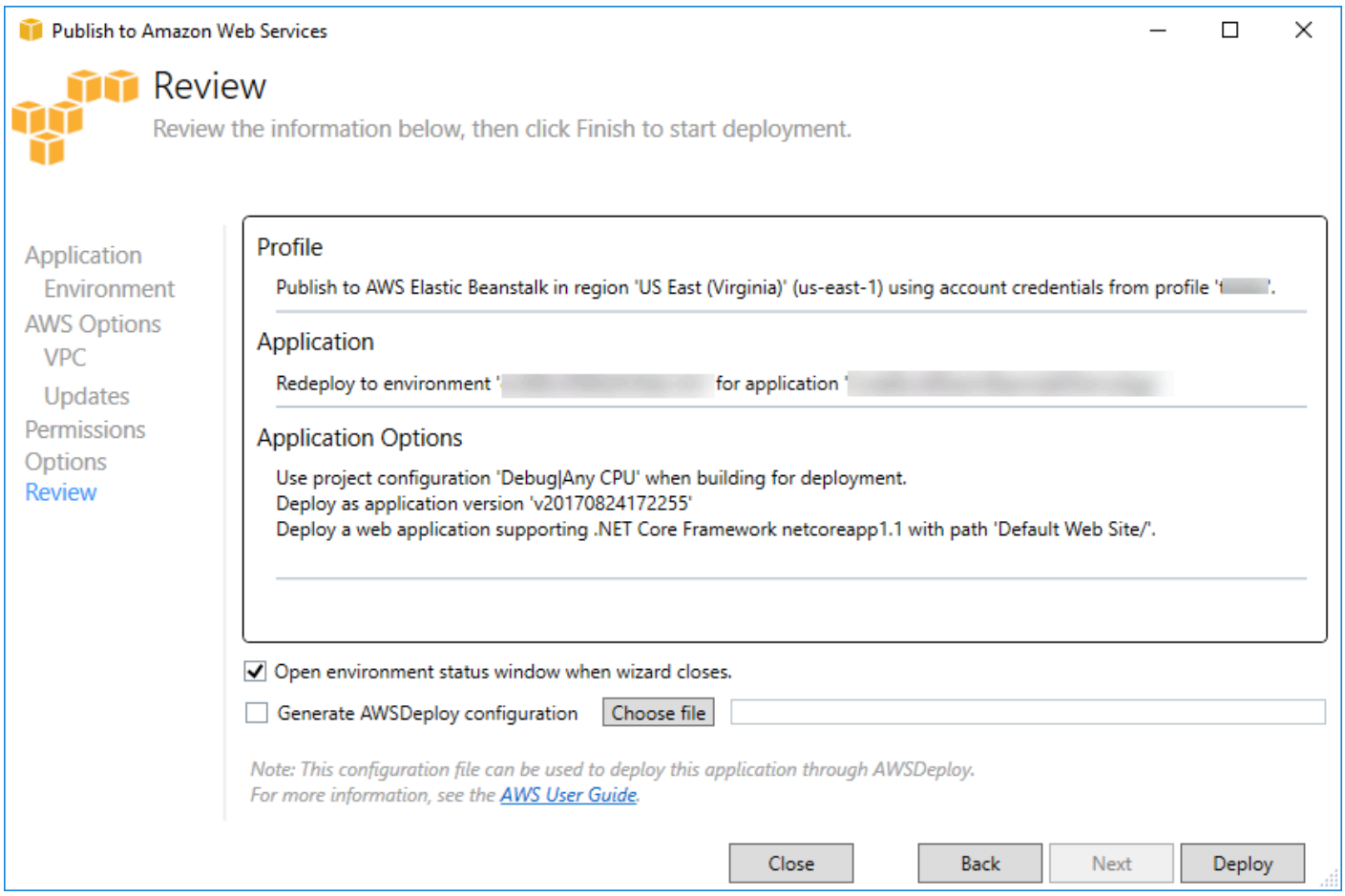


   Der Publish to Elastic Beanstalk (Veröffentlichen zu Elastic Beanstalk)-Assistent wird angezeigt.



2. Wählen Sie Redeploy to an existing environment (Erneut für eine bestehende Umgebung bereitstellen) und wählen Sie die Umgebung, in der Sie zuvor veröffentlicht haben. Klicken Sie auf Weiter.

   Der Review (Prüfen)-Assistent wird angezeigt.



3. Klicken Sie auf Deploy (Bereitstellen). Die Anwendung wird wieder in derselben Umgebung bereitgestellt.

Sie können nicht erneut veröffentlichen, wenn Ihre Anwendung gerade gestartet oder beendet wird.

Benutzerdefinierte Bereitstellung von Elastic Beanstalk-Anwendungen

In diesem Thema wird beschrieben, wie das Deployment-Manifest für den Microsoft Windows-Container von Elastic Beanstalk benutzerdefinierte Anwendungsbereitstellungen unterstützt.

Benutzerdefinierte Anwendungsbereitstellungen sind eine leistungsstarke Funktion für fortgeschrittene Benutzer, die die Leistungsfähigkeit von Elastic Beanstalk nutzen möchten, um ihre AWS Ressourcen zu erstellen und zu verwalten, aber die vollständige Kontrolle darüber haben möchten, wie ihre Anwendung bereitgestellt wird. Für eine benutzerdefinierte Anwendungsbereitstellung erstellen Sie PowerShell Windows-Skripts für die drei verschiedenen Aktionen, die Elastic Beanstalk ausführt. Die Installationsaktion wird verwendet, wenn eine Bereitstellung begonnen wird. Die Neustartaktion kommt zum Einsatz, wenn die

`RestartAppServer`-API entweder vom Toolkit oder über die Webkonsole aufgerufen wird. Die Aktion zum Deinstallieren wird auf vorherige Bereitstellungen angewendet, wenn eine neue Bereitstellung zur Verfügung steht.

Beispiel: Sie verfügen über eine ASP.NET-Anwendung, die Sie bereitstellen möchten, und Ihr Dokumentationsteam hat eine statische Website geschrieben, die in die Bereitstellung mit eingeschlossen werden soll. Um dies durchzuführen, kann Ihre Bereitstellungsmanifestdatei so geschrieben werden:

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

Die aufgeführten Skripts für jede Aktion müssen sich in dem Anwendungspaket befinden, das sich auf die Bereitstellungsmanifestdatei bezieht. Für dieses Beispiel enthält das Anwendungspaket auch eine documentation.zip-Datei mit einer statischen Website, die von Ihrem Dokumentationsteam erstellt wurde.

Das `install.ps1`-Skript extrahiert die ZIP-Datei und richtet den IIS-Pfad ein.

```
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}
```

Da Ihre Anwendung in IIS ausgeführt wird, wird durch die Neustartaktion ein Zurücksetzen des IIS ausgelöst.

```
iisreset /timeout:1
```

Zum Deinstallieren von Skripten müssen alle Einstellungen und Dateien, die während der Installationsstufe verwendet wurden, gelöscht werden. Auf diese Weise können Sie verhindern, dass es bei der Installation der neuen Version zu einer Kollision mit vorherigen Bereitstellungen kommt. In diesem Beispiel müssen Sie die IIS-Anwendung für die statische Website sowie die Website-Dateien entfernen.

```
powershell.exe -Command {Remove-WebApplication -Name documentation}
Remove-Item -Recurse -Force 'c:\inetpub\wwwroot\documentation'
```

Mit diesen Skriptdateien und der documentation.zip-Datei, die sich in Ihrem Anwendungspaket befinden, wird bei der Bereitstellung zunächst die ASP.NET-Anwendung erzeugt und dann die Website der Dokumentation bereitgestellt.

Für dieses Beispiel wählen wir ein einfaches Beispiel, das eine einfache statische Website bereitstellt. Mit der Bereitstellung benutzerdefinierter Anwendungen können Sie jedoch jede Art von Anwendung bereitstellen und Elastic Beanstalk die AWS Ressourcen dafür verwalten lassen.

Benutzerdefinierte ASP.NET Core Elastic Beanstalk Beanstalk-Bereitstellungen

In diesem Thema wird beschrieben, wie die Bereitstellung funktioniert und wie Sie Bereitstellungen anpassen können, wenn Sie ASP.NET Core-Anwendungen mit Elastic Beanstalk und dem Toolkit for Visual Studio erstellen.

Nachdem Sie den Bereitstellungsassistenten im Toolkit for Visual Studio abgeschlossen haben, bündelt das Toolkit die Anwendung und sendet sie an Elastic Beanstalk. Als erster Schritt bei der Erstellung des Anwendungspakets wird die Anwendung mithilfe der neuen dotnet CLI mit dem Befehl publish auf die Veröffentlichung vorbereitet. Das Framework und die Konfiguration werden von den Einstellungen im Assistenten an den Befehl publish weitergegeben. Wenn Sie also Release für `configuration` und netcoreapp1.0 für das `framework` ausgewählt haben, führt das Toolkit den folgenden Befehl aus:

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

Nach Ausführung des Befehls publish schreibt das Toolkit das neue Bereitstellungsmanifest in den Veröffentlichungsordner. Das Deployment-Manifest ist eine JSON-Datei mit dem Namen aws-windows-deployment-manifest.json, die der Elastic Beanstalk Windows-Container (Version 1.2 oder höher) liest, um zu bestimmen, wie die Anwendung bereitgestellt werden soll. Beispiel: Für eine ASP.NET Core-Anwendung, die Sie im Stammverzeichnis von IIS bereitstellen möchten, erzeugt das Toolkit eine Manifestdatei, die wie folgt aussieht:

```
{
  "manifestVersion": 1,
  "deployments": {

    "aspNetCoreWeb": [
      {
        "name": "app",
        "parameters": {
          "appBundle": ".",
          "iisPath": "/",
          "iisWebSite": "Default Web Site"
        }
      }
    ]
  }
}
```

Die Eigenschaft `appBundle` gibt an, wo sich die Anwendungsbits im Bezug auf die Manifestdatei befinden. Diese Eigenschaft kann entweder auf ein Verzeichnis oder auf eine ZIP-Datei verweisen. Die Eigenschaften `iisPath` und `iisWebSite` geben an, wo die Anwendung in IIS gehostet werden soll.

Anpassen der Manifest-Datei

Das Toolkit schreibt die Manifestdatei nur dann, wenn nicht bereits eine im Veröffentlichungsordner existiert. Wenn die Datei vorhanden ist, aktualisiert das Toolkit die Eigenschaften `appBundleiisPath` und `iisWebSite` in der ersten Anwendung in der Liste des Manifestabschnitts `aspNetCoreWeb`. Auf diese Weise können Sie Ihrem Projekt die Datei aws-windows-deployment-manifest.json hinzufügen und das Manifest anpassen. Fügen Sie dazu für eine ASP.NET Core-Webanwendung in Visual Studio eine neue JSON-Datei zum Stammverzeichnis des Projekts hinzu und nennen Sie sie aws-windows-deployment-manifest .json.

Das Manifest muss den Namen aws-windows-deployment-manifest.json haben und sich im Stammverzeichnis des Projekts befinden. Der Elastic Beanstalk Beanstalk-Container sucht im Stammverzeichnis nach dem Manifest und ruft, falls er es findet, das Deployment-Tooling auf. Wenn die Datei nicht existiert, greift der Elastic Beanstalk Beanstalk-Container auf das ältere Deployment-Tooling zurück, das davon ausgeht, dass es sich bei dem Archiv um ein msdeploy-Archiv handelt.

Um sicherzustellen, dass der `publish`-Befehl von dotnet CLI das Manifest mit einschließt, aktualisieren Sie die `project.json`-Datei, um die Manifestdatei in den Abschnitt "Include" unter `include` in `publishOptions` aufzunehmen.

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

Nachdem Sie das Manifest deklariert haben, damit es in die App aufgenommen wird, können Sie weitere Konfigurationen zur Bereitstellung der Anwendung vornehmen. Sie können das Deployment

über das hinaus anpassen, was der Deployment Wizard unterstützt. AWS hat ein JSON-Schema für die aws-windows-deployment-manifestJSON-Datei definiert, und als Sie das Toolkit for Visual Studio installiert haben, hat das Setup die URL für das Schema registriert.

Wenn Sie `windows-deployment-manifest.json` öffnen, wird die ausgewählte Schema-URL im Schema-Dropdown-Feld angezeigt. Sie können zu der URL navigieren, um eine komplette Beschreibung der möglichen Einstellungen in der Manifestdatei zu erhalten. Wenn das Schema ausgewählt ist, stellt Visual Studio IntelliSense während der Bearbeitung das Manifest bereit.

Sie können beispielsweise den IIS-Anwendungspool konfigurieren, unter dem die Anwendung ausgeführt wird. Am folgenden Beispiel sehen Sie, wie Sie einen IIS-Anwendungspool ("customPool") definieren können, der den Prozess alle 60 Minuten recycelt und ihn mithilfe von `"appPool": "customPool"` der Anwendung zuweist.

```
{
  "manifestVersion": 1,
  "iisConfig": {
    "appPools": [
      {
        "name": "customPool",
        "recycling": {
          "regularTimeInterval": 60
        }
      }
    ]
  },
  "deployments": {
    "aspNetCoreWeb": [
      {
        "name": "app",
        "parameters": {
          "appPool": "customPool"
        }
      }
    ]
  }
}
```

Darüber hinaus kann das Manifest PowerShell Windows-Skripts so deklarieren, dass sie vor und nach den Installations-, Neustarts- und Deinstallationsaktionen ausgeführt werden. Das folgende Manifest führt beispielsweise das PowerShell Windows-Skript aus, `PostInstallSetup.ps1`

um weitere Einrichtungsarbeiten durchzuführen, nachdem die ASP.NET Core-Anwendung auf IIS bereitgestellt wurde. Stellen Sie beim Hinzufügen solcher Skripts sicher, dass die Skripts dem Abschnitt "include" unter "publishOptions" in der `project.json`-Datei hinzugefügt werden, ebenso wie bei der `aws-windows-deployment-manifest.json`-Datei. Wenn Sie dies nicht tun, werden die Skripts nicht als Teil des Befehls publish der dotnet CLI aufgenommen.

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

Und was ist mit .ebextensions?

Die Elastic Beanstalk Beanstalk-.ebextensions-Konfigurationsdateien werden wie alle anderen Elastic Beanstalk Beanstalk-Container unterstützt. Um .ebextensions in eine ASP.NET Core-Anwendung einzuschließen, fügen Sie das `.ebextensions`-Verzeichnis dem Abschnitt `include` unter `publishOptions` in der `project.json`-Datei hinzu. Weitere Informationen über .ebextensions finden Sie im Elastic Beanstalk-Entwicklerhandbuch.

Support mehrerer Anwendungen für.NET und Elastic Beanstalk

Mithilfe des Deployment-Manifests können Sie mehrere Anwendungen in derselben Elastic Beanstalk Beanstalk-Umgebung bereitstellen.

Das Bereitstellungsmanifest unterstützt ASP.NET Core-Webanwendungen sowie msdeploy-Dateien für herkömmliche ASP.NET-Anwendungen. Stellen Sie sich vor, Sie hätten mit ASP.NET Core eine neue, faszinierende Anwendung für das Frontend und ein Web-API-Projekt für eine Erweiterungen-API geschrieben. Außerdem hätten Sie eine Admin-App mit dem herkömmlichen ASP.NET. geschrieben.

Der Bereitstellungsassistent des Toolkits konzentriert sich auf die Bereitstellung eines einzelnen Projekts. Wenn Sie von der Bereitstellung mehrerer Anwendungen profitieren möchten, müssen Sie das Anwendungspaket manuell erstellen. Zunächst schreiben Sie die Manifestdatei. Bei diesem Beispiel wird das Manifest in das Stammverzeichnis Ihrer Lösung geschrieben.

Der Bereitstellungsabschnitt im Manifest hat zwei untergeordnete Elemente: ein Array aus bereitzustellenden ASP.NET Core-Webanwendungen und ein Array aus bereitzustellenden msdeploy-Dateien. Sie geben für jede Anwendung den IIS-Pfad sowie den Speicherort der Anwendungsbits im Bezug auf das Manifest an.

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

Nachdem das Manifest geschrieben ist, verwenden Sie Windows, um das Anwendungspaket PowerShell zu erstellen und eine bestehende Elastic Beanstalk Beanstalk-Umgebung zu aktualisieren, um es auszuführen. Das Skript wird unter der Annahme geschrieben, dass es über den Ordner ausgeführt wird, der Ihre Visual Studio-Lösung enthält.

Zunächst müssen Sie im Skript einen Workspace-Ordner einrichten, in dem das Anwendungspaket erstellt wird.

```
$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
}
```

Sobald Sie den Ordner erstellt haben, wird das Frontend vorbereitet. Ebenso wie beim Bereitstellungsassistenten verwenden Sie die dotnet CLI zum Veröffentlichen der Anwendung.

```
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
```

Beachten Sie, dass der Unterordner "Frontend" für den Ausgabeordner verwendet wurde, entsprechend dem von Ihnen im Manifest festgelegten Ordner. Nun führen Sie dieselben Schritt für das Web-API-Projekt durch.

```
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
```

Bei der Administrationswebsite handelt es sich um eine herkömmliche ASP.NET-Anwendung, sodass Sie die dotnet CLI nicht verwenden können. Für die Admin-Anwendung sollten Sie msbuild verwenden, mit Übergabe in das erstellte Zielpaket zum Erzeugen der msdeploy-Datei.

Standardmäßig erstellt das Paketziel die msdeploy-Datei unter dem `obj\Release\Package`-Ordner. Daher müssen Sie die Datei in den Workspace zum Veröffentlichen kopieren.

```
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
```

Um der Elastic Beanstalk Beanstalk-Umgebung mitzuteilen, was mit all diesen Anwendungen geschehen soll, kopieren Sie das Manifest aus Ihrer Lösung in den Publish-Workspace und komprimieren Sie dann den Ordner.

```
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)
```

Jetzt, wo Sie das Anwendungspaket haben, können Sie zur Webkonsole gehen und das Archiv in eine Elastic Beanstalk Beanstalk-Umgebung hochladen. Alternativ können Sie die AWS PowerShell Cmdlets weiterhin verwenden, um die Elastic Beanstalk Beanstalk-Umgebung mit dem Anwendungspaket zu aktualisieren. Stellen Sie sicher, dass Sie das aktuelle Profil und die Region mithilfe `Set-AWSCredentials` von Cmdlets auf das Profil und die Region festgelegt haben, die Ihre Elastic Beanstalk Beanstalk-Umgebung enthalten. `Set-DefaultAWSRegion`

```
Write-Host 'Write application bundle to S3'
# Determine S3 bucket to store application bundle
$s3Bucket = New-EBStorageLocation
Write-S3Object -BucketName $s3Bucket -File $appBundle


$applicationName = "ASPNETCoreOnAWS"
$environmentName = "ASPNETCoreOnAWS-dev"
$versionLabel = [System.DateTime]::Now.Ticks.ToString()

Write-Host 'Update Beanstalk environment for new application bundle'
New-EBApplicationVersion -ApplicationName $applicationName -VersionLabel $versionLabel
 -SourceBundle_S3Bucket $s3Bucket -SourceBundle_S3Key app-bundle.zip
Update-EBEnvironment -ApplicationName $applicationName -EnvironmentName
 $environmentName -VersionLabel $versionLabel
```

Überprüfen Sie nun den Status des Updates entweder auf der Elastic Beanstalk Beanstalk-Umgebungsstatusseite im Toolkit oder in der Webkonsole. Nachdem der Vorgang abgeschlossen ist, können Sie zu jeder Anwendung navigieren, die Sie für den, im Bereitstellungsmanifest angegebenen, IIS-Pfad bereitgestellt haben.

Bereitstellung bei Amazon EC2 Container Service

> **Important**
>
> Die neue AWS Funktion „Veröffentlichen in“ wurde entwickelt, um die Veröffentlichung von.NET-Anwendungen zu vereinfachen AWS. Nachdem Sie Publish Container to ausgewählt haben, werden Sie möglicherweise gefragt, ob Sie zu dieser Veröffentlichungserfahrung wechseln möchten AWS. Weitere Informationen finden Sie unter Arbeiten mit Publish to AWS in Visual Studio.

Amazon Elastic Container Service ist ein hoch skalierbarer, leistungsstarker Container-Management-Service, der Docker-Container unterstützt und es Ihnen ermöglicht, Anwendungen einfach auf einem verwalteten Cluster von EC2 Amazon-Instances auszuführen.

Um Anwendungen auf Amazon Elastic Container Service bereitzustellen, müssen Ihre Anwendungskomponenten für die Ausführung in einem Docker-Container entwickelt werden. Ein Docker-Container ist eine standardisierte Einheit der Softwareentwicklung, die alles beinhaltet, was Ihre Softwareanwendung für die Ausführung benötigt: Code, Laufzeit, Systemtools, Systembibliotheken usw.

Das Toolkit for Visual Studio bietet einen Assistenten, der die Veröffentlichung von Anwendungen über Amazon ECS vereinfacht. Dieser Assistent wird in den folgenden Abschnitten beschrieben.

Weitere Informationen zu Amazon ECS finden Sie in der Elastic Container Service-Dokumentation. Sie enthält eine Übersicht über die Docker-Grundlagen und eine exemplarische Vorgehensweise zum Erstellen eines Clusters.

Themen

- Geben Sie AWS Anmeldeinformationen für Ihre ASP.NET Core 2-Anwendung an
- Bereitstellung einer ASP.NET Core 2.0-App auf Amazon ECS (Fargate) (Legacy)
- Bereitstellen einer ASP.NET Core 2.0-App auf Amazon ECS () EC2

Geben Sie AWS Anmeldeinformationen für Ihre ASP.NET Core 2-Anwendung an

Es gibt zwei Typen von Anmeldeinformationen, die bei der Bereitstellung Ihrer Anwendung in einem Docker-Container relevant sind: Bereitstellungs-Anmeldeinformationen und Instance-Anmeldeinformationen.

Anmeldeinformationen für die Bereitstellung werden vom AWS Assistenten „Container veröffentlichen“ verwendet, um die Umgebung in Amazon ECS zu erstellen. Dies sind beispielsweise Aufgaben, Services, IAM-Rollen, ein Docker-Container-Repository, und, falls von Ihnen ausgewählt, ein Load Balancer.

Instance-Anmeldeinformationen werden von der Instance (einschließlich Ihrer Anwendung) für den Zugriff auf verschiedene AWS Dienste verwendet. Wenn Ihre ASP.NET Core 2.0-Anwendung beispielsweise Amazon S3 S3-Objekte liest und in sie schreibt, benötigt sie entsprechende Berechtigungen. Sie können verschiedene Anmeldeinformationen unter Verwendung verschiedener Methoden basierend auf der Umgebung bereitstellen. Beispielsweise könnte Ihre ASP.NET Core 2-Anwendung auf Development- und Production-Umgebungen ausgelegt sein. Sie könnten mit eine lokale Docker-Instance und Anmeldeinformationen für die Entwicklung und eine definierte Rolle in der Produktion verwenden.

Angeben von Anmeldeinformationen für die Bereitstellung

Das AWS Konto, das Sie im Publish Container to AWS Wizard angeben, ist das AWS Konto, das der Assistent für die Bereitstellung in Amazon ECS verwendet. Das Kontoprofil muss über Berechtigungen für Amazon Elastic Compute Cloud, Amazon Elastic Container Service und verfügen AWS Identity and Access Management.

Wenn Sie feststellen, dass Optionen in Dropdown-Listen fehlen, kann es sein, dass Sie nicht über die entsprechenden Berechtigungen verfügen. Zum Beispiel, wenn Sie einen Cluster für Ihre Anwendung erstellt haben, ihn aber nicht auf der Cluster-Seite „Container im AWS Wizard veröffentlichen“ sehen. Wenn dies der Fall ist, fügen Sie die fehlenden Berechtigungen hinzu und versuchen erneut, den Assistenten auszuführen.

Angabe von Instance-Anmeldeinformationen für die Entwicklung

Für nicht-produktive Umgebungen können Sie Ihre Anmeldeinformationen in der Datei appsettings.<environment>.json konfigurieren. Gehen Sie beispielsweise wie folgt vor, um Ihre

Anmeldeinformationen in der appsettings.Development.json-Datei in Visual Studio 2017 zu konfigurieren:

1. Fügen Sie die AWSSDK .Extensions hinzu. NETCore NuGet .Setup-Paket zu Ihrem Projekt.
2. Fügen Sie AWS Einstellungen zu AppSettings.Development.json hinzu. Die folgende Konfiguration legt `Profile` und `Region` fest.

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

Angabe von Instance-Anmeldeinformationen für die Produktion

Für Produktionsinstanzen empfehlen wir, eine IAM-Rolle zu verwenden, um zu kontrollieren, worauf Ihre Anwendung (und der Service) zugreifen kann. Um beispielsweise eine IAM-Rolle mit Amazon ECS als Service Principal mit Berechtigungen für Amazon Simple Storage Service und Amazon DynamoDB zu konfigurieren, von: AWS Management Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter. https://console.aws.amazon.com/iam/
2. Klicken Sie im Navigationsbereich der IAM-Konsole auf Rollen und wählen Sie dann Rolle erstellen aus.
3. Wählen Sie den Rollentyp AWS Service und dann EC2 Container Service aus.
4. Wählen Sie den Anwendungsfall EC2 Container Service Task aus. Anwendungsfälle werden durch den Service definiert, damit die für den Service erforderliche Vertrauensrichtlinie enthalten ist. Wählen Sie dann Next: Permissions.
5. Wählen Sie die Richtlinien AmazonS3 FullAccess und AmazonDynamoDBFullAccess aus. Markieren Sie das Kontrollkästchen neben der jeweiligen Richtlinie und wählen Sie Next: Review (Weiter: Prüfen),
6. Geben Sie für Role name (Rollenname) einen Rollennamen oder ein Rollennamen-Suffix ein, anhand dessen der Zweck dieser Rolle einfach zu erkennen ist. Rollennamen müssen innerhalb Ihres AWS -Kontos eindeutig sein. Es wird hierbei nicht zwischen Groß- und Kleinschreibung unterschieden. z. B. können Sie keine Rollen erstellen, die `PRODROLE` bzw. `prodrole` heißen. Da

möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung nicht bearbeitet werden.

7. (Optional) Geben Sie im Feld Role description eine Beschreibung für die neue Rolle ein.
8. Prüfen Sie die Rolle und klicken Sie dann auf Create Role (Rolle erstellen).

Sie können diese Rolle als Aufgabenrolle auf der Seite ECS-Aufgabendefinition des Assistenten „Container veröffentlichen“ verwenden. AWS

Weitere Informationen finden Sie unter Verwenden von servicebasierten Rollen.

Bereitstellung einer ASP.NET Core 2.0-App auf Amazon ECS (Fargate) (Legacy)

> **Important**
>
> Diese Dokumentation bezieht sich auf ältere Dienste und Funktionen. Aktualisierte Anleitungen und Inhalte finden Sie im Leitfaden für das Bereitstellungstool AWS für.NET und im aktualisierten AWS Inhaltsverzeichnis Deploying to.

In diesem Abschnitt wird beschrieben, wie Sie den AWS Assistenten zum Veröffentlichen von Containern verwenden, der als Teil des Toolkit for Visual Studio bereitgestellt wird, um eine containerisierte ASP.NET Core 2.0-Anwendung für Linux über Amazon ECS mithilfe des Starttyps Fargate bereitzustellen. Da eine Webanwendung kontinuierlich ausgeführt werden soll, wird sie als Service bereitgestellt.

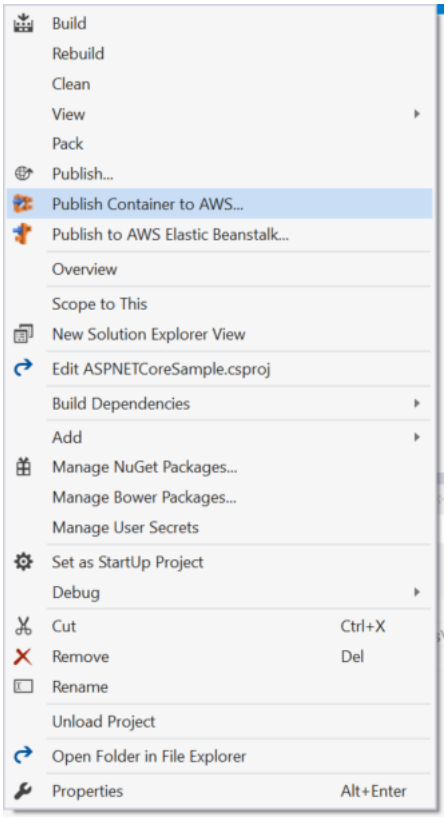
Bevor Sie Ihren Container veröffentlichen

Bevor Sie den AWS Assistenten zum Veröffentlichen von Containern zur Bereitstellung Ihrer ASP.NET Core 2.0-Anwendung verwenden, gehen Sie wie folgt vor:

- Geben Sie Ihre AWS Anmeldeinformationen an und richten Sie Amazon ECS ein.
- Docker-Installation. Sie haben verschiedene Installationsoptionen, einschließlich Docker für Windows.
- Erstellen (oder öffnen) Sie in Visual Studio ein Projekt für eine containerisierte ASP.NET Core 2.0-Anwendung für Linux.

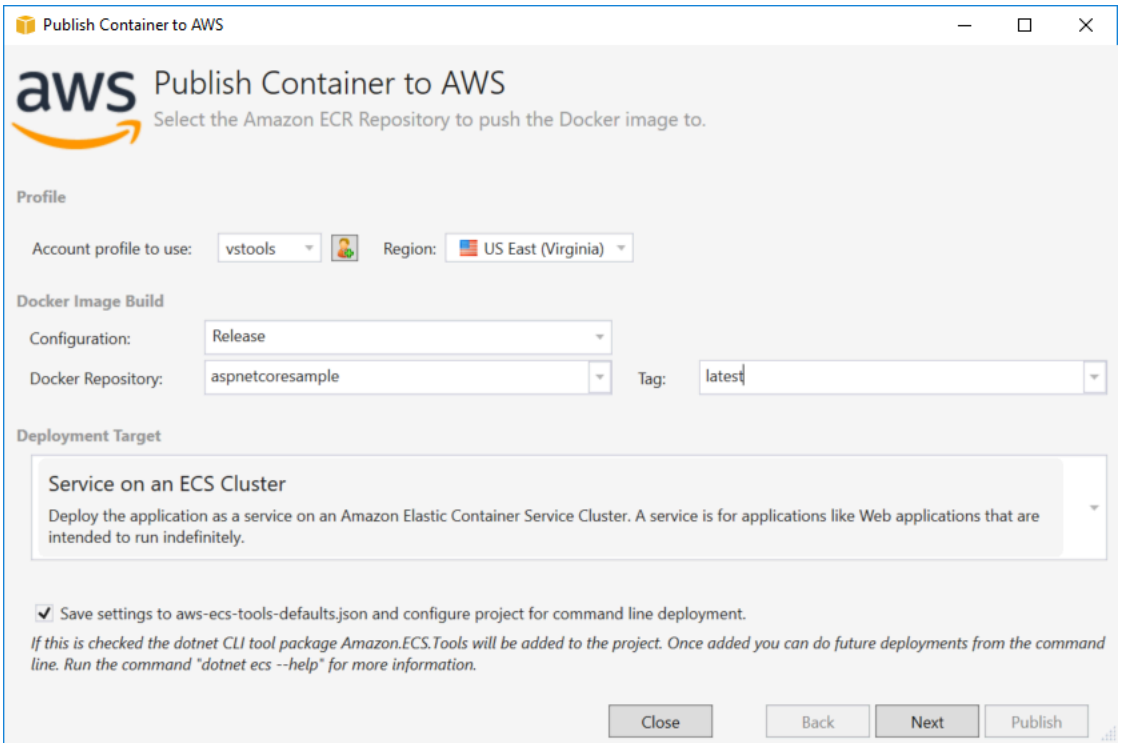
Zugreifen auf den Assistenten zum Veröffentlichen von Containern AWS

Um eine containerisierte ASP.NET Core 2.0-Anwendung für Linux bereitzustellen, klicken Sie im Solution Explorer mit der rechten Maustaste auf das Projekt und wählen Sie Container veröffentlichen unter aus. AWS



Sie können auch im Visual Studio-Build-Menü die Option Container veröffentlichen AWS unter auswählen.

Container im AWS Assistenten veröffentlichen



Account profile to use – Wählen Sie ein zu verwendendes Kontoprofil aus.

Region – Wählen Sie die Bereitstellungsregion aus. Profil und Region werden verwendet, um Ihre Deployment-Umgebungsressourcen einzurichten und die Docker-Standardregistry auszuwählen.

Configuration – Wählen Sie die Docker-Image-Build-Konfiguration aus.

Docker Repository – Wählen Sie ein vorhandenes Docker-Repository aus, oder geben Sie den Namen eines neuen Repositorys ein, das dann erstellt wird. Dies ist das Repository, in das der Build-Container verschoben wird.

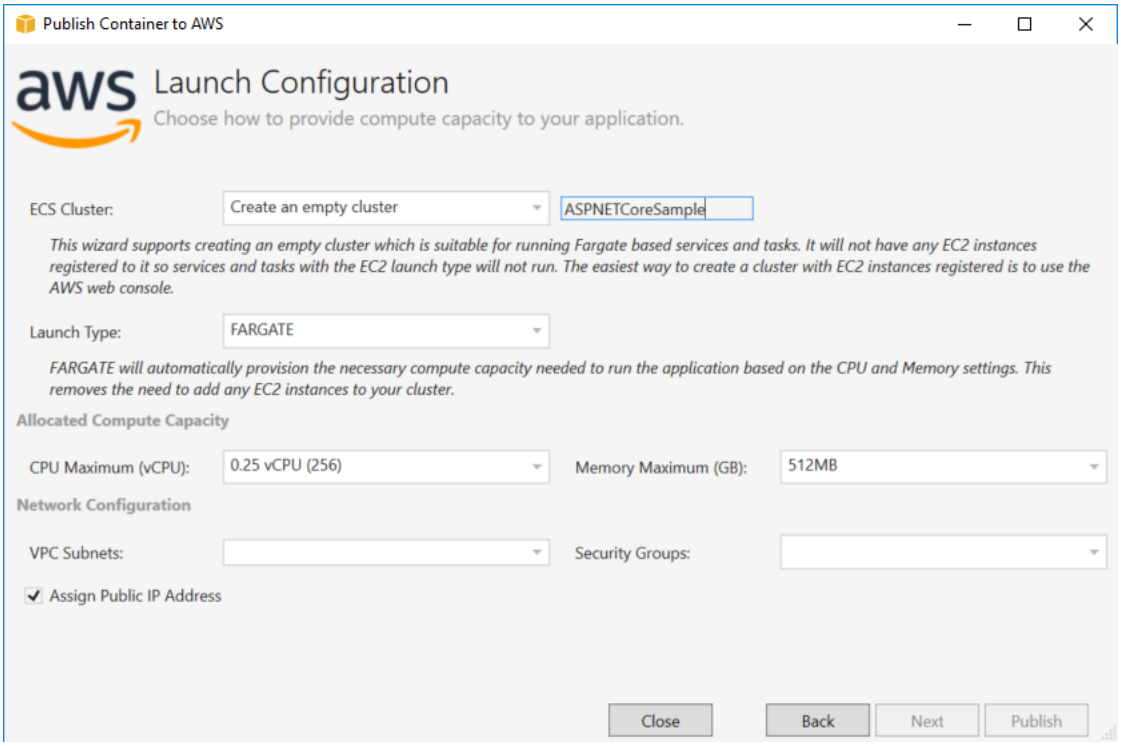
Tag – Wählen Sie ein vorhandenes Tag aus, oder geben Sie den Namen eines neuen Tags ein. Tags können wichtige Details nachverfolgen, wie Version, Optionen oder andere eindeutige Elemente des Docker-Containers.

Deployment Target – Wählen Sie Service on an ECS Cluster (Service auf einem ECS-Cluster). Verwenden Sie diese Bereitstellungsoption, wenn Ihre Anwendung sehr lange ausgeführt werden soll (z. B. eine ASP.NET-Webanwendung).

Einstellungen in **`aws-docker-tools-defaults.json`** speichern und für Befehlszeilenbereitstellung konfigurieren:Aktivieren Sie diese Option, wenn Sie die Flexibilität

genießen möchten, eine Bereitstellung über die Befehlszeile durchzuführen. Verwenden Sie `dotnet ecs deploy` aus Ihrem Projektverzeichnis, das bereitgestellt werden soll, und veröffentlichen Sie den Container mit `dotnet ecs publish`.

Seite Launch Configuration



ECS Cluster – Wählen Sie den Cluster, der Ihr Docker-Image ausführt. Wenn Sie auswählen, einen leeren Cluster zu erstellen, geben Sie einen Namen für den neuen Cluster an.

Launch Type – Wählen Sie FARGATE.

CPU Maximum (vCPU) – Wählen Sie die maximale Rechenkapazität, die für Ihre Anwendung erforderlich ist. Zulässige Bereiche für die CPU- und RAM-Werte finden Sie unter Task-Größe.

Memory Maximum (GB) – Wählen Sie die maximale Arbeitsspeichergröße für Ihre Anwendung.

VPC Subnets – Wählen Sie ein oder mehrere Subnetze in einer einzelnen VPC. Wenn Sie mehr als ein Subnetz wählen, werden Ihre Tasks über diese verteilt. Dies kann die Verfügbarkeit verbessern. Weitere Informationen finden Sie unter Standard-VPC und Standard-Subnetze.

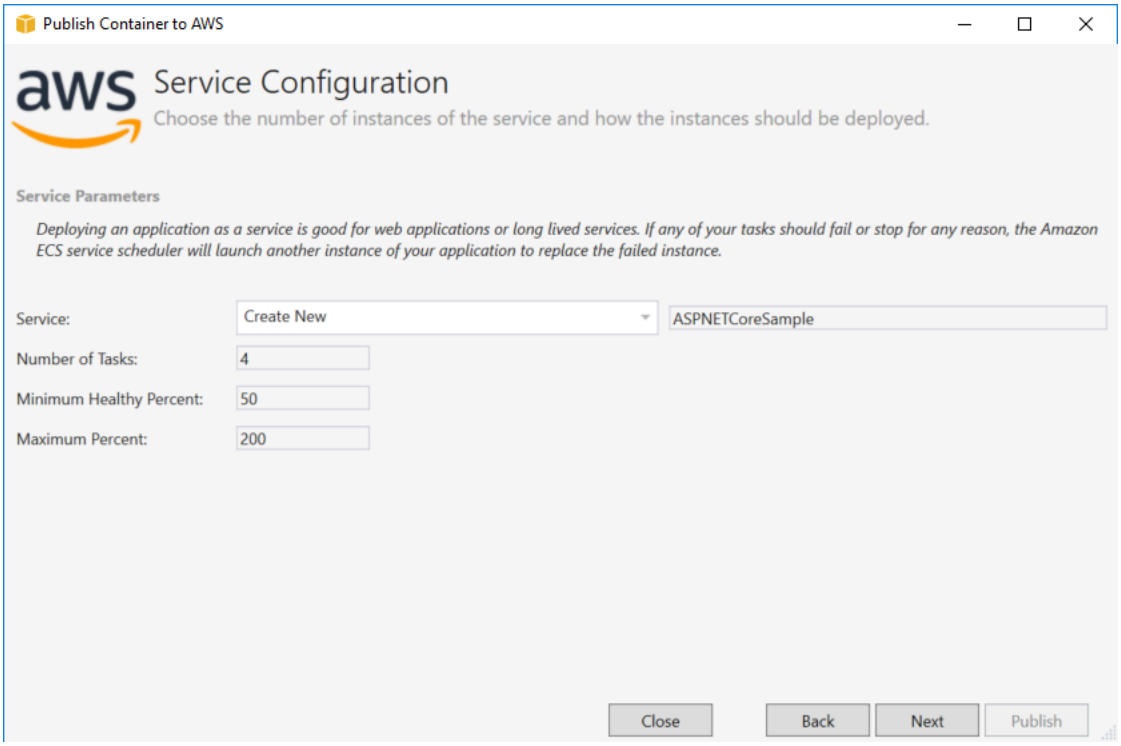
Security Groups – Wählen Sie eine Sicherheitsgruppe.

Eine Sicherheitsgruppe fungiert als Firewall für zugehörige EC2 Amazon-Instances und steuert sowohl den eingehenden als auch den ausgehenden Datenverkehr auf Instance-Ebene.

Standard-Sicherheitsgruppen sind so konfiguriert, dass eingehender Datenverkehr von Instances, die derselben Sicherheitsgruppe zugewiesen sind, sowie der gesamte ausgehende Datenverkehr zugelassen werden. IPv4 Ausgehender Verkehr muss zugelassen sein, sodass der Service das Container-Repository erreichen kann.

Assign Public IP Address – Markieren Sie dies, damit über das Internet auf Ihre Aufgabe zugegriffen werden kann.

Seite Service Configuration



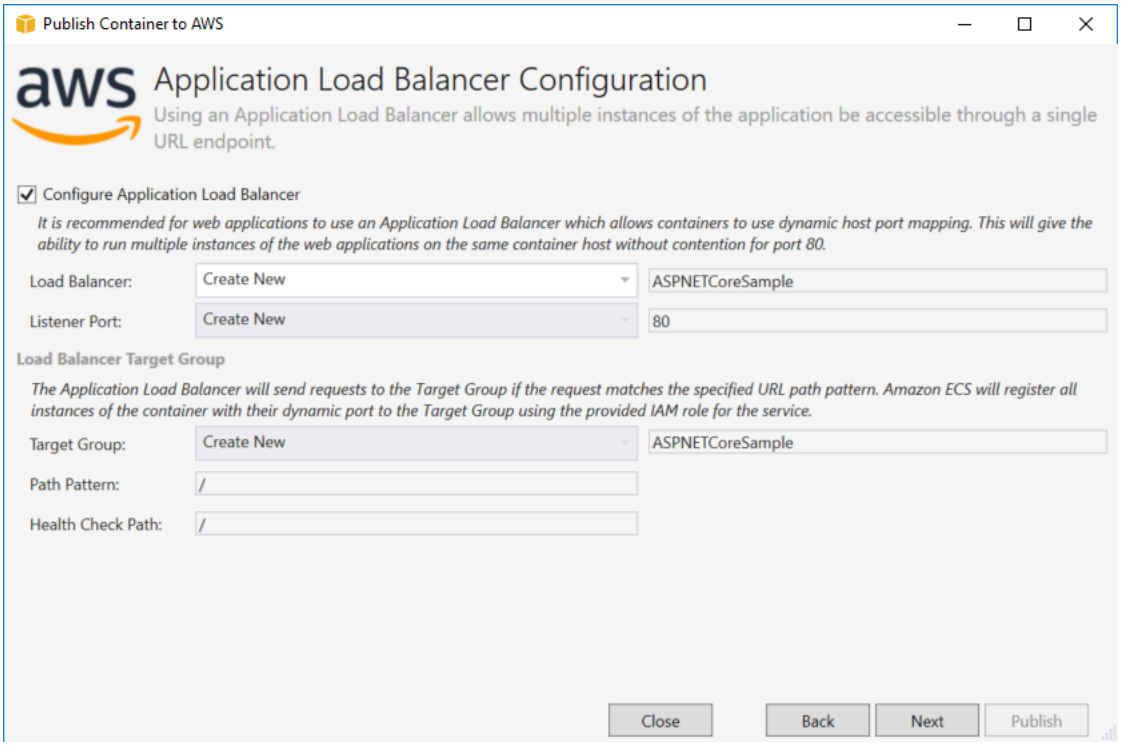
Service – Wählen Sie einen der Services in der Dropdown-Liste, um Ihren Container in einem vorhandenen Service bereitzustellen. Oder wählen Sie Create New (Neu erstellen), um einen neuen Service zu erstellen. Servicenamen in einem Cluster müssen eindeutig sein. Sie können jedoch ähnlich benannte Services in mehreren Clustern innerhalb einer Region oder in mehreren Regionen haben.

Number of tasks – Die Anzahl der Aufgaben an, die bereitgestellt und auf Ihrem Cluster ausgeführt werden sollen. Jede Aufgabe ist eine Instance Ihres Containers.

Minimum Healthy Percent – Der Prozentsatz der Aufgaben, die während einer Bereitstellung im Status `RUNNING` bleiben müssen, aufgerundet auf die nächste ganze Zahl.

Maximum Percent – Der Prozentsatz der Aufgaben, die während einer Bereitstellung im Status `RUNNING` oder `PENDING` bleiben dürfen, aufgerundet auf die nächste ganze Zahl.

Seite Application Load Balancer



Configure Application Load Balancer – Markieren, um einen Application Load Balancer zu konfigurieren.

Load Balancer – Wählen Sie einen vorhandenen Load Balancer aus, oder wählen Sie Create New (Neu erstellen), und geben Sie den Namen für den neuen Load Balancer ein.

Listener Port – Wählen Sie einen vorhandenen Listener Port aus, oder wählen Sie Create New (Neu erstellen), und geben Sie eine Portnummer ein. Für die meisten Webanwendungen ist der Standardport geeignet, `80`.

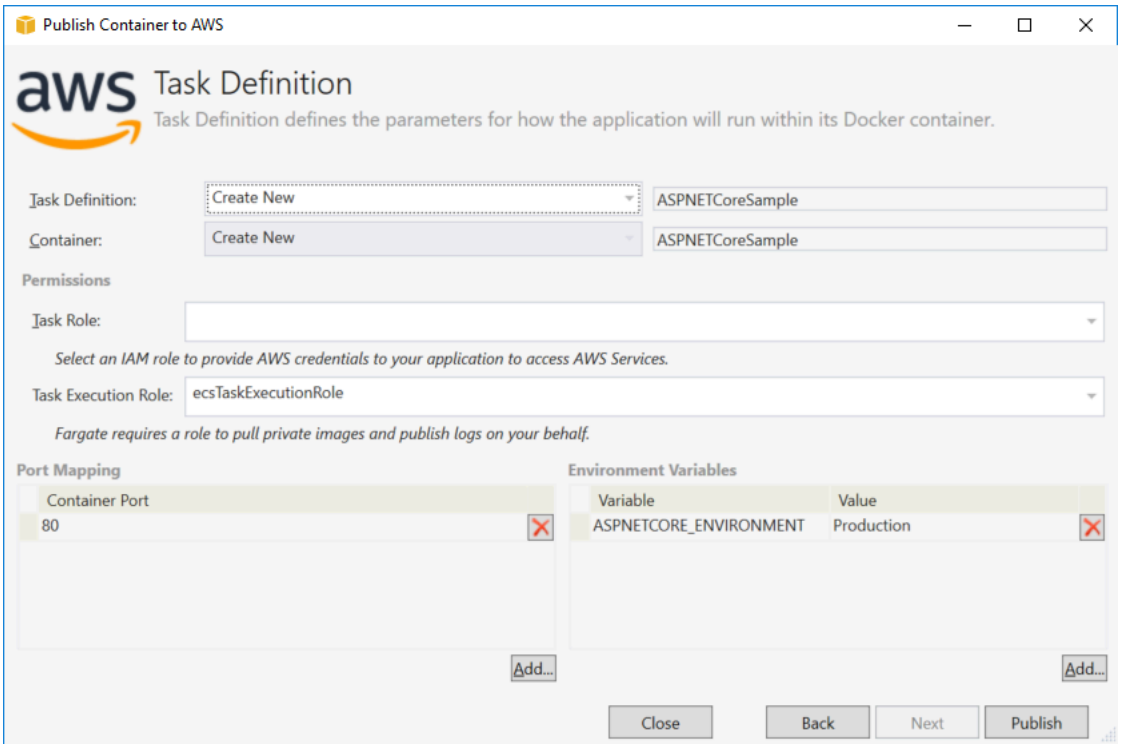
Zielgruppe — Wählen Sie die Zielgruppe aus, für die Amazon ECS die Aufgaben für den Service registrieren soll.

Path Pattern – Der Load Balancer verwendet ein auf dem Pfad basierendes Routing. Übernehmen Sie den Standard `/` oder geben Sie ein anderes Muster ein. Beim Pfadmuster wird die Groß-/Kleinschreibung berücksichtigt, es kann maximal 128 Zeichen lang sein und es enthält einen ausgewählten Zeichensatz.

Health Check Path – Der Ping-Pfad, der als Zielpfad für die Ziele der Zustandsprüfungen gilt. Standardmäßig ist dieser /. Geben Sie gegebenenfalls einen anderen Pfad ein. Wenn der von Ihnen eingegebene Pfad ungültig ist, schlägt die Zustandsprüfung fehl und er wird als fehlerhaft betrachtet.

Wenn Sie mehrere Services bereitstellen und jeder Service auf einen anderen Pfad oder Standort bereitgestellt wird, müssen Sie benutzerdefinierte Pfade überprüfen.

Seite Task Definition



Task Definition – Wählen Sie eine vorhandene Aufgabendefinition aus, oder wählen Sie Create New (Neu erstellen), und geben Sie den Namen für eine neue Aufgabendefinition ein.

Container – Wählen Sie einen vorhandenen Container aus, oder wählen Sie Create New (Neu erstellen), und geben Sie den Namen für einen neuen Container ein.

Aufgabenrolle — Wählen Sie eine IAM-Rolle aus, die über die Anmeldeinformationen verfügt, die Ihre App für den Zugriff auf AWS Services benötigt. So werden Ihrer Anwendung Anmeldeinformationen übergeben. Erfahren Sie, wie Sie AWS Sicherheitsanmeldedaten für Ihre Anwendung angeben.

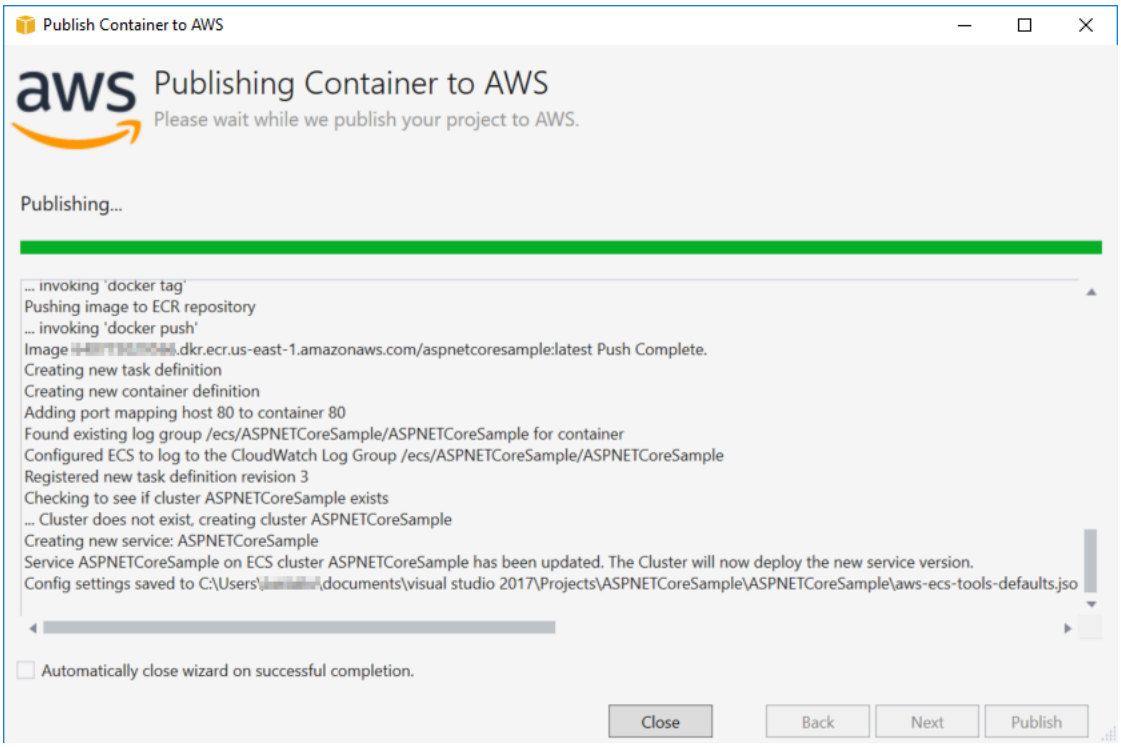
Rolle bei der Aufgabenausführung — Wählen Sie eine Rolle aus, die berechtigt ist, private Images abzurufen und Protokolle zu veröffentlichen. AWS Fargate wird es in Ihrem Namen verwenden.

Port Mapping – Wählen Sie die Port-Nummer auf dem Container, der an den automatisch zugewiesenen Host-Port gebunden ist.

Environment Variables – Umgebungsvariablen für den Container hinzufügen, ändern oder löschen. Sie können sie so anpassen, dass sie zu Ihrer Bereitstellung passen.

Wenn Sie mit der Konfiguration zufrieden sind, klicken Sie auf Publish (Veröffentlichen), um mit dem Bereitstellungsprozess zu beginnen.

Container veröffentlichen auf AWS



Ereignisse werden während der Bereitstellung angezeigt. Der Assistent wird automatisch geschlossen, wenn sie erfolgreich ausgeführt wurde. Sie können diese Einstellung überschreiben, indem Sie die Markierung im Feld unten auf der Seite entfernen.

Sie finden die URL Ihrer neuen Instanzen im AWS Explorer. Erweitern Sie Amazon ECS und Cluster und klicken Sie dann auf Ihren Cluster.

Bereitstellen einer ASP.NET Core 2.0-App auf Amazon ECS () EC2

In diesem Abschnitt wird beschrieben, wie Sie den AWS Assistenten zum Veröffentlichen von Containern verwenden, der als Teil des Toolkit for Visual Studio bereitgestellt wird, um eine containerisierte ASP.NET Core 2.0-Anwendung für Linux über Amazon ECS mithilfe des Starttyps bereitzustellen. EC2 Da eine Webanwendung kontinuierlich ausgeführt werden soll, wird sie als Dienst bereitgestellt.

Bevor Sie Ihren Container veröffentlichen

Bevor Sie den Publish Container AWS zur Bereitstellung Ihrer ASP.NET Core 2.0-Anwendung verwenden, gehen Sie wie folgt vor:

- Geben Sie Ihre AWS Anmeldeinformationen an und richten Sie Amazon ECS ein.
- Docker-Installation. Sie haben verschiedene Installationsoptionen, einschließlich Docker für Windows.
- Erstellen eines Amazon ECS-Clusters basierend auf den Anforderungen Ihrer Webanwendung. Dazu sind nur wenige Schritte erforderlich.
- Erstellen (oder öffnen) Sie in Visual Studio ein Projekt für eine containerisierte ASP.NET Core 2.0-Anwendung für Linux.

Zugreifen auf den Assistenten zum Veröffentlichen von Containern AWS

Um eine containerisierte ASP.NET Core 2.0-Anwendung für Linux bereitzustellen, klicken Sie im Solution Explorer mit der rechten Maustaste auf das Projekt und wählen Sie Container veröffentlichen unter aus. AWS

Sie können auch im Visual Studio-Build-Menü die Option Container veröffentlichen AWS unter auswählen.

Container im AWS Wizard veröffentlichen

Account profile to use – Wählen Sie ein zu verwendendes Kontoprofil aus.

Region – Wählen Sie eine Bereitstellungsregion aus. Profil und Region werden verwendet, um Ihre Deployment-Umgebungsressourcen einzurichten und die Docker-Standardregistry auszuwählen.

Configuration – Wählen Sie die Docker-Image-Build-Konfiguration aus.

Docker Repository – Wählen Sie ein vorhandenes Docker-Repository aus, oder geben Sie den Namen eines neuen Repositorys ein, das dann erstellt wird. Dies ist das Repository, in das das erstellte Container-Image verschoben wird.

Tag – Wählen Sie ein vorhandenes Tag aus, oder geben Sie den Namen eines neuen Tags ein. Tags können wichtige Details nachverfolgen, wie Version, Optionen oder andere eindeutige Elemente des Docker-Containers.

Deployment – Wählen Sie Service on an ECS Cluster (Service auf einem ECS-Cluster). Verwenden Sie diese Bereitstellungsoption, wenn Ihre Anwendung sehr lange ausgeführt werden soll (z. B. eine ASP.NET Core 2.0-Webanwendung).

Einstellungen in **`aws-docker-tools-defaults.json`** speichern und für Befehlszeilenbereitstellung konfigurieren:Aktivieren Sie diese Option, wenn Sie die Flexibilität genießen möchten, eine Bereitstellung über die Befehlszeile durchzuführen. Verwenden Sie `dotnet ecs deploy` aus Ihrem Projektverzeichnis, das bereitgestellt werden soll, und veröffentlichen Sie den Container mit `dotnet ecs publish`.

Seite Launch Configuration

ECS Cluster – Wählen Sie den Cluster, der Ihr Docker-Image ausführt. Sie können mit der AWS Management Console einen ECS-Cluster erstellen.

Starttyp — Wählen Sie EC2. Um den Fargate-Starttyp zu verwenden, lesen Sie nach unter Deploying an ASP.NET Core 2.0 Application to Amazon ECS (Fargate).

Seite Service Configuration

Service – Wählen Sie einen der Services in der Dropdown-Liste, um Ihren Container in einem vorhandenen Service bereitzustellen. Oder wählen Sie Create New (Neu erstellen), um einen neuen Service zu erstellen. Servicenamen in einem Cluster müssen eindeutig sein. Sie können jedoch ähnlich benannte Services in mehreren Clustern innerhalb einer Region oder in mehreren Regionen haben.

Number of tasks – Die Anzahl der Aufgaben an, die bereitgestellt und auf Ihrem Cluster ausgeführt werden sollen. Jede Aufgabe ist eine Instance Ihres Containers.

Minimum Healthy Percent – Der Prozentsatz der Aufgaben, die während einer Bereitstellung im Status `RUNNING` bleiben müssen, aufgerundet auf die nächste ganze Zahl.

Maximum Percent – Der Prozentsatz der Aufgaben, die während einer Bereitstellung im Status `RUNNING` oder `PENDING` bleiben dürfen, aufgerundet auf die nächste ganze Zahl.

Placement Templates – Wählen Sie eine Vorlage für eine Aufgabenplatzierung

Wenn Sie eine Aufgabe in einem Cluster starten, muss Amazon ECS bestimmen, wo die Aufgabe basierend auf den in der Aufgabendefinition angegebenen Anforderungen, beispielsweise CPU und

Arbeitsspeicher, platziert werden soll. Wenn Sie die Anzahl der Aufgaben herunterskalieren, muss Amazon ECS auf ähnliche Weise bestimmen, welche Aufgaben beendet werden sollen.

Die Platzierungsvorlage steuert, wie Aufgaben in einem Cluster gestartet werden:

- AZ Balanced Spread: Verteilt Aufgaben über Availability Zones und über Container-Instances in der Availability Zone.
- AZ Balanced BinPack — verteilt Aufgaben auf Availability Zones und auf Container-Instances mit dem geringsten verfügbaren Speicher.
- BinPack - verteilt Aufgaben auf der Grundlage der geringsten verfügbaren CPU- oder Speichermenge.
- One Task Per Host: Platziert höchstens eine Aufgabe vom Service auf jeder Container-Instance.

Weitere Informationen finden Sie unter Amazon ECS-Aufgabenplatzierung.

Seite Application Load Balancer

Configure Application Load Balancer – Markieren, um einen Application Load Balancer zu konfigurieren.

Select IAM role for service – Wählen Sie eine vorhandene Rolle oder wählen Sie Create New (Neu erstellen), sodass eine neue Rolle erstellt wird.

Load Balancer – Wählen Sie einen vorhandenen Load Balancer aus, oder wählen Sie Create New (Neu erstellen), und geben Sie den Namen für den neuen Load Balancer ein.

Listener Port – Wählen Sie einen vorhandenen Listener Port aus, oder wählen Sie Create New (Neu erstellen), und geben Sie eine Portnummer ein. Für die meisten Webanwendungen ist der Standardport geeignet, `80`.

Target Group – Der Load Balancer sendet standardmäßig Anfragen an registrierte Ziele mithilfe des Ports und des Protokolls, den bzw. das Sie für die Zielgruppe angegeben haben. Sie können diesen Port überschreiben, wenn Sie jedes Ziel bei der Zielgruppe registrieren.

Path Pattern – Der Load Balancer verwendet ein auf dem Pfad basierendes Routing. Übernehmen Sie den Standard `/` oder geben Sie ein anderes Muster ein. Beim Pfadmuster wird die Groß-/Kleinschreibung berücksichtigt, es kann maximal 128 Zeichen lang sein und es enthält einen ausgewählten Zeichensatz.

Health Check Path – Der Ping-Pfad, der als Zielpfad für die Ziele der Zustandsprüfungen gilt. Für die meisten Webanwendungen ist dies standardmäßig `/`, ein geeigneter Wert. Geben Sie gegebenenfalls einen anderen Pfad ein. Wenn der von Ihnen eingegebene Pfad ungültig ist, schlägt die Zustandsprüfung fehl und er wird als fehlerhaft betrachtet.

Wenn Sie mehrere Services bereitstellen und jeder Service auf einen anderen Pfad oder Standort bereitgestellt wird, müssen Sie möglicherweise benutzerdefinierte Pfade überprüfen.

Seite ECS Task Definition

Task Definition – Wählen Sie eine vorhandene Aufgabendefinition aus, oder wählen Sie Create New (Neu erstellen), und geben Sie den Namen für eine neue Aufgabendefinition ein.

Container – Wählen Sie einen vorhandenen Container aus, oder wählen Sie Create New (Neu erstellen), und geben Sie den Namen für einen neuen Container ein.

Memory (MiB) – Geben Sie Werte für Soft Limit oder Hard Limit oder beides an.

Die Soft-Limit-Arbeitsspeichergrenze (in MiB) für die Reservierung für den Container. Docker versucht, den Container-Arbeitsspeicher unter dem Soft Limit zu halten. Der Container mehr Speicher verbrauchen, bis zu dem mit dem Speicherparameter (gegebenenfalls) angegebenen Hard Limit, oder den gesamten verfügbaren Speicher auf der Container-Instance, je nachdem, welcher Wert zuerst erreicht wird.

Die Hard-Limit-Arbeitsspeichergrenze (in MiB), die dem Container bereitgestellt wird. Wenn Ihr Container versucht, das hier angegebene Limit zu überschreiten, wird der Container beendet.

Aufgabenrolle — Wählen Sie eine Aufgabenrolle für eine IAM-Rolle aus, die es dem Container ermöglicht AWS APIs , die in den zugehörigen Richtlinien angegebenen Aufgaben in Ihrem Namen aufzurufen. So werden Ihrer Anwendung Anmeldeinformationen übergeben. Erfahren Sie, wie Sie AWS Sicherheitsanmeldedaten für Ihre Anwendung angeben.

Port-Mapping – Port-Zuordnungen für den Container hinzufügen, ändern oder löschen. Wenn ein Load Balancer aktiviert ist, ist der Host-Port standardmäßig 0, und die Port-Zuordnung erfolgt dynamisch.

Environment Variables – Umgebungsvariablen für den Container hinzufügen, ändern oder löschen.

Wenn Sie mit der Konfiguration zufrieden sind, klicken Sie auf Publish (Veröffentlichen), um mit dem Bereitstellungsprozess zu beginnen.

Container veröffentlichen auf AWS

Ereignisse werden während der Bereitstellung angezeigt. Der Assistent wird automatisch geschlossen, wenn sie erfolgreich ausgeführt wurde. Sie können diese Einstellung überschreiben, indem Sie die Markierung im Feld unten auf der Seite entfernen.

Sie finden die URL Ihrer neuen Instanzen im AWS Explorer. Erweitern Sie Amazon ECS und Cluster und klicken Sie dann auf Ihren Cluster.

Problembehandlung bei AWS Toolkit for Visual Studio

Die folgenden Abschnitte enthalten allgemeine Informationen zur Problembehebung mit den Diensten aus dem Toolkit AWS Toolkit for Visual Studio und der Arbeit mit AWS Diensten aus dem Toolkit.

> **Note**
>
> Informationen set-up-specific zur Installation und Problembehandlung finden Sie im Thema Behebung von Installationsproblemen in diesem Benutzerhandbuch.

Themen

Bewährte Methoden zur Fehlerbehebung

Im Folgenden werden bewährte Methoden zur Behebung von AWS Toolkit for Visual Studio Problemen empfohlen.

- Reparieren Sie Visual Studio und starten Sie Ihr System neu
- Versuchen Sie, Ihr Problem oder Ihren Fehler erneut zu erstellen, bevor Sie einen Bericht senden.
- Machen Sie sich während des Wiederherstellungsvorgangs detaillierte Notizen zu jedem Schritt, jeder Einstellung und jeder Fehlermeldung.
- Sammeln Sie AWS Toolkit-Protokolle. Eine ausführliche Beschreibung, wie Sie Ihre AWS Toolkit-Logs auffinden können, finden Sie im Abschnitt So finden Sie Ihre AWS Logs in diesem Handbuch.
- Suchen Sie im Bereich AWS Toolkit for Visual Studio Probleme des Repositorys nach offenen Anfragen und bekannten Lösungen oder melden Sie Ihr ungelöstes Problem. AWS Toolkit for Visual Studio GitHub

Reparieren Sie Visual Studio und starten Sie Ihr System neu

1. Schließen Sie alle laufenden Instanzen von Visual Studio.

2. Starten Sie Visual Studio Installer im Windows-Startmenü.
3. Führen Sie Repair für die betroffene (n) Installation (en) von Visual Studio aus. Dadurch kann Visual Studio seinen Index der installierten Erweiterungen neu erstellen.
4. Starten Sie Windows neu, bevor Sie Visual Studio neu starten.

So finden Sie Ihre AWS Toolkit-Protokolle

1. Erweitern Sie im Visual Studio-Hauptmenü die Erweiterung Erweiterungen.
2. Wählen Sie das AWS Toolkit aus, um das AWS Toolkit-Menü zu erweitern, und wählen Sie dann Toolkit-Protokolle anzeigen.
3. Wenn der AWS Toolkit-Protokollordner in Ihrem Betriebssystem geöffnet wird, sortieren Sie die Dateien nach Datum und suchen Sie nach allen Protokolldateien, die Informationen zu Ihrem aktuellen Problem enthalten.

Amazon Q-Sicherheitsscans anzeigen und filtern

Um Ihre Amazon Q-Sicherheitsscans in Visual Studio anzuzeigen, öffnen Sie die Visual Studio-Fehlerliste, indem Sie die Überschrift Ansicht im Visual Studio-Hauptmenü erweitern und Fehlerliste auswählen.

Standardmäßig zeigt die Visual Studio-Fehlerliste alle Warnungen und Fehler für Ihre Codebasis an. Um Ihre Amazon Q-Sicherheitsscan-Ergebnisse aus der Visual Studio-Fehlerliste zu filtern, erstellen Sie einen Filter, indem Sie das folgende Verfahren ausführen.

> **Note**
>
> Die Ergebnisse des Amazon Q-Sicherheitsscans sind erst sichtbar, nachdem der Sicherheitsscan ausgeführt und Probleme erkannt wurden.
> Die Ergebnisse des Amazon Q-Sicherheitsscans werden in Visual Studio als Warnungen angezeigt. Um die Ergebnisse des Amazon Q-Sicherheitsscans aus Ihrer Fehlerliste anzuzeigen, muss die Option Warnungen in der Überschrift Fehlerliste ausgewählt werden.

1. Erweitern Sie im Visual Studio-Hauptmenü die Überschrift Ansicht und wählen Sie Fehlerliste, um den Bereich Fehlerliste zu öffnen.

2. Klicken Sie im Bereich Fehlerliste mit der rechten Maustaste auf die Kopfzeile, um das Kontextmenü zu öffnen.
3. Erweitern Sie im Kontextmenü die Option Spalten anzeigen und wählen Sie dann im erweiterten Menü die Option Tool aus.
4. Die Spalte Tool wird zu Ihrer Fehlerliste hinzugefügt.
5. Wählen Sie in der Spaltenüberschrift Tool das Filtersymbol und dann Amazon Q aus, um nach Ergebnissen von Amazon Q-Sicherheitsscans zu filtern.

Das AWS Toolkit ist nicht richtig installiert

Problem:

Innerhalb einer Minute nach dem Start von Visual Studio werden AWS Toolkit for Visual Studio die folgenden Meldungen im Ausgabebereich bzw. in der Infoleiste angezeigt:

```
Some Toolkit components could not be initialized. Some functionality may
not work during this IDE session.

The AWS Toolkit is not properly installed.
```

Solution (Lösung):

Es ist möglich, dass durch die Aktualisierung oder Installation einer Erweiterung einige der internen Cache-Dateien von Visual Studio verloren gingen out-of-sync. Im folgenden Verfahren wird beschrieben, wie diese Dateien beim nächsten Start von Visual Studio neu erstellt werden.

> **Note**
>
> Es ist möglich, dass sich diese Lösung auf Ihre Visual Studio-Anpassungen auswirkt. Nach Abschluss dieses Verfahrens sollte die AWS Toolkit-Erweiterung als installiert aufgeführt sein und keine Fehlermeldung mehr melden. Wenn dieses Problem nach Abschluss der folgenden Schritte weiterhin auftritt, finden Sie weitere Informationen unter Problem #452 im AWS Toolkit for Visual Studio GitHub Repository.

1. Installieren Sie die neueste Version von Visual Studio 2022.

> **Note**
>
> Die erforderliche Mindestversion ist 17.11.5.

2. Schließen Sie alle laufenden Instanzen von Visual Studio.
3. Öffnen Sie in Windows die Entwickler-Eingabeaufforderung als Administrator.
4. Führen Sie in der Entwickler-Befehlszeile den folgenden Befehl aus: `devenv /updateconfiguration /resetExtensions` und warten Sie, bis der Befehl abgeschlossen ist.
5. Starten Sie Visual Studio neu, nachdem der Befehl abgeschlossen ist.
6. In Visual Studio wird die AWS Erweiterung jetzt als installiert aufgeführt und die oben in dieser Ausgabe aufgeführten Fehlermeldungen werden nicht mehr gemeldet.

Firewall- und Proxyeinstellungen

Fehlerbehebung bei den Firewall- und Proxyeinstellungen

Software für Sicherheitsscans kann Ihre Fähigkeit beeinträchtigen, Dateien von AWS Toolkit-Sprachservern herunterzuladen, indem sie Dateien aus Downloads entfernt oder Downloads ganz verhindert.

Um Ihre Firewall- und Proxyeinstellungen zu überprüfen, navigieren Sie von einem Internetbrowser aus, der auf demselben System wie Ihre Visual Studio-Instanz installiert ist, zu https://aws-toolkit-language-servers.amazonaws.com/codewhisperer/0/manifest.json. Wenn Sie auf einen Fehler stoßen oder die Seite nicht geladen werden kann, verhindert möglicherweise eine Firewall oder ein Proxyfilter, dass Sie nicht darauf zugreifen können. `aws-toolkit-language-servers.amazonaws.com`

Benutzerdefinierte Zertifikate

Der AWS Toolkit for Visual Studio verwendet einen Sprachserver, der auf der Runtime Node.js läuft. Ausführliche Informationen dazu, wie Sie überprüfen können, ob Ihr Netzwerk ein benutzerdefiniertes Zertifikat verwendet, finden Sie unter den Einstellungen für die Konfiguration und Anmeldeinformationsdatei im AWS CLI Thema im AWS Command Line InterfaceBenutzerhandbuch für Version 1.

Um Ihre Proxyeinstellungen zu konfigurieren und ein Zertifikat zu definieren, müssen Sie Ihre `HTTPS_PROXY` env-Variable konfigurieren und Windows-Umgebungsvariablen für die Schlüssel `NODE_OPTIONS` und `NODE_EXTRA_CA_CERTS` erstellen.

Gehen Sie wie folgt vor, um Ihre `HTTPS_PROXY` env-Variable zu konfigurieren.

1. Wählen Sie im Visual Studio-Hauptmenü Tools und anschließend Optionen aus.
2. Erweitern Sie im OptionsmenüAWS Toolkit und wählen Sie dann Proxy aus.
3. Definieren Sie im Proxy-Menü Ihren Host und Port.

> **Note**
>
> Informationen zur Konfiguration `HTTPS_PROXY` von finden Sie im AWS CLI Abschnitt Verwenden eines HTTP-Proxys für das entsprechende AWS CLI Thema im AWS Command Line InterfaceBenutzerhandbuch.

Erstellen Sie Windows-Umgebungsvariablen für die folgenden Schlüssel.

- `NODE_OPTIONS = --use-openssl-ca`
- `NODE_EXTRA_CA_CERTS = Path/To/Corporate/Certs`

> **Note**
>
> Weitere Informationen zum Extrahieren von Unternehmensstammzertifikaten finden Sie im Artikel Exportieren eines Zertifikats mit seinem privaten Schlüssel auf learn.microsoft.com. Ausführliche Informationen zu den Schlüsseln der Windows-Umgebungsvariablen finden Sie in der Dokumentation zu Node.js v23.3.0 auf nodejs.org.

Erlaube das Auflisten und weitere Schritte

Firewall-Einstellungen stören nicht nur die AWS Toolkit-Sprachserver, sondern können auch verhindern, dass Amazon Q auf Amazon S3 hochlädt und die Service-API aufruft. Um das Potenzial dieser Fehler zu minimieren, empfehlen wir, den ausgehenden Internetzugang über Port 443 (HTTPS) für die folgenden Endpunkte zuzulassen:

- `https://codewhisperer.us-east-1.amazonaws.com/`
- `https://amazonq-code-transformation-us-east-1-c6160f047e0.s3.amazonaws.com/`
- `https://aws-toolkit-language-servers.amazonaws.com/`
- `https://q.us-east-1.amazonaws.com`
- `https://client-telemetry.us-east-1.amazonaws.com`
- `https://cognito-identity.us-east-1.amazonaws.com`
- `https://oidc.us-east-1.amazonaws.com`

Eine ausführliche Liste der Endpunkte finden Sie im Thema Aktualisieren von Firewalls und Gateways, um den Zugriff zu ermöglichen in diesem Benutzerhandbuch. Ausführliche Informationen zur Konfiguration eines Unternehmens-Proxys für Amazon Q finden Sie im Thema Konfiguration eines Unternehmens-Proxys in Amazon Q im Amazon Q Developer User Guide. Wenn Sie weiterhin auf Probleme mit der Firewall und dem Proxy stoßen, sammeln Sie Ihre AWS Toolkit-Protokolle und wenden Sie sich über den AWS Toolkit for Visual Studio Problembereich des AWS Toolkit for Visual Studio GitHub Repositorys an das AWS Toolkit for Visual Studio Team. Einzelheiten zur Erfassung Ihrer AWS Toolkit-Protokolle finden Sie im Abschnitt „Bewährte Methoden zur Fehlerbehebung“ in diesem Thema im Benutzerhandbuch.

Sicherheit für AWS Toolkit for Visual Studio

Cloud-Sicherheit genießt bei Amazon Web Services (AWS) höchste Priorität. Als AWS -Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat. Sicherheit ist eine gemeinsame Verantwortung von Ihnen und Ihnen. AWS Im Modell der übergreifenden Verantwortlichkeit wird Folgendes mit „Sicherheit der Cloud“ bzw. „Sicherheit in der Cloud“ umschrieben:

Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der alle in der AWS Cloud angebotenen Dienste ausgeführt werden, und für die Bereitstellung von Diensten, die Sie sicher nutzen können. Unsere Sicherheitsverantwortung hat bei uns höchste Priorität AWS, und die Wirksamkeit unserer Sicherheit wird im Rahmen der AWS Compliance-Programme regelmäßig von externen Prüfern getestet und verifiziert.

Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem von Ihnen genutzten AWS Dienst und anderen Faktoren, wie der Sensibilität Ihrer Daten, den Anforderungen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften.

Dieses AWS Produkt oder dieser Service folgt dem Modell der gemeinsamen Verantwortung in Bezug auf die spezifischen Amazon Web Services (AWS) -Services, die es unterstützt. Informationen zur AWS Servicesicherheit finden Sie auf der Seite mit der Dokumentation zur AWS Servicesicherheit und den AWS Services, für die das AWS Compliance-Programm zur Einhaltung der Vorschriften zuständig ist.

Themen

Datenschutz in AWS Toolkit for Visual Studio

Das AWS Modell der mit gilt für den Datenschutz in AWS Toolkit for Visual Studio mit Amazon Q. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle AWS Cloud Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie AWS Toolkit mit Amazon Q oder anderen AWS-Services verwenden, indem Sie die Konsole AWS CLI, API oder AWS SDKs verwenden. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet

werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Identitäts- und Zugriffsverwaltung

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. AWS

Dienstbenutzer — Wenn Sie dies AWS-Services für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Falls Sie auf eine Funktion nicht zugreifen können AWS, finden Fehlerbehebung bei AWS Identität und Zugriff Sie weitere Informationen in der Bedienungsanleitung der von AWS-Service Ihnen verwendeten.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die AWS Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der

Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM verwenden kann AWS, finden Sie in der Benutzeranleitung der von AWS-Service Ihnen verwendeten Software.

IAM-Administrator: Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS verfassen können. Beispiele für AWS identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie im Benutzerhandbuch der AWS-Service von Ihnen verwendeten.

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges

Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Methoden für die Übernahme einer Rolle im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.

- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein

Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter

Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und

der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie AWS-Services arbeiten Sie mit IAM

Einen allgemeinen Überblick darüber, wie die meisten IAM-Funktionen AWS-Services funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Dienste, die mit IAM funktionieren.

Informationen zur Verwendung bestimmter Dienste AWS-Service mit IAM finden Sie im Abschnitt Sicherheit im Benutzerhandbuch des jeweiligen Dienstes.

Fehlerbehebung bei AWS Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `awes:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 awes:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `awes:GetWidget`-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWSübergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder

Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AWS unterstützt werden, finden Sie unter. Wie AWS-Services arbeiten Sie mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Überprüfung der Einhaltung der Vorschriften für dieses AWS Produkt oder diese Dienstleistung

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Dieses AWS Produkt oder dieser Service folgt dem Modell der gemeinsamen Verantwortung in Bezug auf die spezifischen Amazon Web Services (AWS) -Services, die es unterstützt. Informationen zur AWS Servicesicherheit finden Sie auf der Seite mit der Dokumentation zur AWS Servicesicherheit und den AWS Services, für die das AWS Compliance-Programm zur Einhaltung der Vorschriften zuständig ist.

Ausfallsicherheit für dieses AWS Produkt oder diese Dienstleistung

Die AWS globale Infrastruktur basiert auf AWS-Regionen Availability Zones.

AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind.

Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Dieses AWS Produkt oder dieser Service folgt dem Modell der gemeinsamen Verantwortung in Bezug auf die spezifischen Amazon Web Services (AWS) -Services, die es unterstützt. Informationen zur AWS Servicesicherheit finden Sie auf der Seite mit der Dokumentation zur AWS Servicesicherheit und den AWS Services, für die das AWS Compliance-Programm zur Einhaltung der Vorschriften zuständig ist.

Sicherheit der Infrastruktur für dieses AWS Produkt oder diesen Service

Dieses AWS Produkt oder dieser Dienst verwendet Managed Services und ist daher durch die AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf dieses AWS Produkt oder diesen Service zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Dieses AWS Produkt oder dieser Service folgt dem Modell der gemeinsamen Verantwortung in Bezug auf die spezifischen Amazon Web Services (AWS) -Services, die es unterstützt. Informationen zur AWS Servicesicherheit finden Sie auf der Seite mit der Dokumentation zur AWS Servicesicherheit und den AWS Services, für die das AWS Compliance-Programm zur Einhaltung der Vorschriften zuständig ist.

Konfiguration und Schwachstellenanalyse in AWS Toolkit for Visual Studio

Das Toolkit for Visual Studio wird im Visual Studio Marketplace veröffentlicht, sobald neue Funktionen oder Fixes entwickelt werden. Diese Updates beinhalten manchmal Sicherheitsupdates, daher ist es wichtig, das AWS Toolkit mit Amazon Q auf dem neuesten Stand zu halten.

So überprüfen Sie, ob automatische Updates für Erweiterungen aktiviert sind

1. Öffnen Sie den Erweiterungsmanager, indem Sie Tools, Erweiterungen und Updates (Visual Studio 2017) oder Erweiterungen, Erweiterungen verwalten (Visual Studio 2019) wählen.
2. Wählen Sie „Einstellungen für Erweiterungen und Updates ändern“ (Visual Studio 2017) oder „Einstellungen für Erweiterungen ändern“ (Visual Studio 2019).
3. Passen Sie die Einstellungen für Ihre Umgebung an.

Wenn Sie automatische Updates für Erweiterungen deaktivieren möchten, achten Sie darauf, in Intervallen, die für Ihre Umgebung geeignet sind, nach Updates für das AWS Toolkit mit Amazon Q zu suchen.

Dokumenthistorie des AWS Toolkit for Visual Studio Benutzerhandbuchs

Dokumentverlauf

In der folgenden Tabelle werden die wichtigsten aktuellen Änderungen des AWS Toolkit for Visual Studio Benutzerhandbuchs beschrieben. Für Benachrichtigungen über Aktualisierungen dieser Dokumentation können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Aktualisierungen des Inhalts „Erste Schritte“	Aktualisierungen an den Abschnitten „Erste Schritte“ und „Verbindung zum AWS Inhalt herstellen“ wurden vorgenommen, um die an der Benutzeroberfläche vorgenommenen Änderungen widerzuspiegeln.	24. April 2025
Aktualisierung von Firewalls und Gateways, um den Zugriff zu ermöglichen	Listen von Endpunkten und Ressourcen, die für den Zugriff auf alle Services und Funktionen in Amazon Q for Extensions zugelassen werden müssen. AWS Toolkit for Visual Studio	20. März 2025
Fehlerbehebung bei den Firewall- und Proxyeins tellungen	Es wurde ein neues Thema zur Fehlerbehebung hinzugefü gt, das sich mit Firewall- und Proxyeinstellungen für die AWS Toolkit for Visual Studio und Amazon Q befasst.	15. Dezember 2024

Fehlerbehebung beim Installationsupdate	Aktualisierung des Inhalts von Installationsproblemen, um einem Update von Microsoft Rechnung zu tragen.	20. November 2024
Aktualisierungen des Inhalts „Erste Schritte“	Aktualisierungen an den Abschnitten „Erste Schritte“ und „Verbindung zum AWS Inhalt herstellen“ wurden vorgenommen, um die an der Benutzeroberfläche vorgenommenen Änderungen widerzuspiegeln.	24. Oktober 2024
Aktualisierungen für Connecting to AWS	Aktualisierungen an Verbindung zum AWS Inhalt herstellen.	26. September 2024
Aktualisierungen der Amazon EC2 AMI-Inhalte	Inhaltsaktualisierungen wurden vorgenommen, um Änderungen am Amazon EC2 AMI-Prozess und den Verfahren zu dokumentieren.	13. September 2024
AWS Toolkit-Komponenten konnten nicht initialisiert werden	Es wurde ein Thema zur Fehlerbehebung hinzugefügt, um Probleme mit AWS Toolkit for Visual Studio Komponenten zu beheben, die nicht initialisiert werden.	13. September 2024
Amazon Q-Sicherheitsscans anzeigen und filtern	Es wurde ein Thema zur Fehlerbehebung hinzugefügt, das beim Anzeigen und Filtern von Amazon Q-Sicherheitsscans hilft.	31. Juli 2024

Amazon Q für AWS Toolkit for Visual Studio	Amazon Q ist jetzt verfügbar für AWS Toolkit for Visual Studio.	30. Juni 2024
Inhaltsaktualisierungen und Wartung	Aktualisierung von Inhalten aufgrund von Änderungen an der Benutzeroberfläche und den AWS Stilrichtlinien.	6. März 2024
Aktualisierung und Wartung von Inhalten	Aktualisierung von Inhalten aufgrund von Änderungen an der Benutzeroberfläche und den AWS Stilrichtlinien.	6. März 2024
Aktualisierung und Wartung von Inhalten	Aktualisierung von Inhalten aufgrund von Änderungen an der Benutzeroberfläche und den AWS Stilrichtlinien.	6. März 2024
Aktualisierung und Wartung von Inhalten	Aktualisierung von Inhalten aufgrund von Änderungen an der Benutzeroberfläche und den AWS Stilrichtlinien.	6. März 2024
Aktualisierung und Wartung von Inhalten	Aktualisierung von Inhalten aufgrund von Änderungen an der Benutzeroberfläche und den AWS Stilrichtlinien.	6. März 2024
Aktualisierungen der Einrichtung und Authentifizierung	Die Themen zur Einrichtung und Authentifizierung wurden aktualisiert, um die Sicherheit und das Onboarding-Erlebnis im Toolkit zu verbessern. Die Änderungen finden Sie in den Themen TOCs Erste Schritte und Authentifizierung und Zugriff.	22. Juni 2023

Authentifizierung und Zugriff	Die Bereitstellung von AWS Anmeldeinformationen heißt jetzt Authentifizierung und Zugriff. Das Inhaltsverzeichnis und die Unterthemen wurden überarbeitet, um AWS Stil- und Sicherheitsanforderungen zu erfüllen.	4. Mai 2023
Aktualisierungen der Abschnitte und Themen zur Einrichtung	Die Einrichtung der AWS Toolkit for Visual Studio Abschnitte und Themen in diesem Benutzerhandbuch wurde aktualisiert, um das Onboarding-Erlebnis für die zu verbessern AWS Toolkit for Visual Studio.	30. Januar 2023
Aktualisierungen der Abschnitte und Themen zum Einrichten	Die Einrichtung der AWS Toolkit for Visual Studio Abschnitte und Themen in diesem Benutzerhandbuch wurde aktualisiert, um das Onboarding-Erlebnis für die zu verbessern AWS Toolkit for Visual Studio.	30. Januar 2023
AWS Toolkit for Visual Studio Informationen für 2022 wurden hinzugefügt	Support für Visual Studio 2022 wurde dem hinzugefügt AWS Toolkit for Visual Studio.	20. Dezember 2022
Aktualisierungen für Publish to AWS guide	Die Dokumentation wurde aktualisiert, um den Änderungen Rechnung zu tragen, die am Service für den Start von GA vorgenommen wurden.	6. Juli 2022

Titelaktualisierungen und Umzug	Kleinere Titeländerungen wurden vorgenommen, um den Inhalt besser widerzuspiegeln. Der Leitfaden befindet sich jetzt im AWS Leitfaden zur Veröffentlichung.	6. Juli 2022
Bereitstellung für AWS: Titel- und Inhaltsaktualisierungen	Der Abschnitt mit dem offiziellen Titel „Bereitstellung mithilfe des AWS Toolkits“ hat ein aktualisiertes Inhaltsverzeichnis (TOC) und trägt jetzt den Titel: Bereitstellung für. AWS Die folgenden Leitfäden sind veraltet und stehen nicht mehr zur Verfügung: Deploying to Elastic Beanstalk (Legacy) und Deploying to AWS CloudFormation (Legacy). Aktualisierte Inhalte zur Bereitstellung auf Elastic Beanstalk und Cloudformation finden Sie im aktualisierten Inhaltsverzeichnis in diesem Leitfaden.	6. Juli 2022
Die Bereitstellung einer ASP.NET Core 2.0-App (Fargate) ist jetzt ein Legacy-Leitfaden	Diese Dokumentation bezieht sich auf ältere Dienste und Funktionen. Aktualisierte Anleitungen und Inhalte finden Sie im Leitfaden zum AWS .NET Deployment Tool und im aktualisierten AWS Inhaltsverzeichnis Deploying to.	6. Juli 2022

Das Bereitstellen einer ASP.NET-App ist jetzt ein Legacy-Handbuch	Diese Dokumentation bezieht sich auf ältere Dienste und Funktionen. Aktualisierte Anleitungen und Inhalte finden Sie im Leitfaden für das Bereitstellungstool AWS für.NET und im aktualisierten AWS Inhaltsverzeichnis Deploying to.	6. Juli 2022
Das Bereitstellen einer ASP.NET-App ist jetzt ein Legacy-Handbuch	Diese Dokumentation bezieht sich auf ältere Dienste und Funktionen. Aktualisierte Anleitungen und Inhalte finden Sie im Leitfaden für das Bereitstellungstool AWS für.NET und im aktualisierten AWS Inhaltsverzeichnis Deploying to.	6. Juli 2022
Neues Leitfadenthema: Arbeiten mit CloudWatch Protokollen in Visual Studio	Ein neues Übersichtsthema für den Leitfaden zur Integration von Amazon CloudWatch Logs in Visual Studio wurde erstellt.	29. Juni 2022
Neues Leitthema: Einrichtung der CloudWatch Logs-Integration für Visual Studio	Ein neuer Einrichtungsabschnitt für den Leitfaden zur Integration von Amazon CloudWatch Logs in Visual Studio wurde erstellt.	29. Juni 2022

CloudWatch Log-Integration für Visual Studio	Es wurde ein neuer Leitfaden für die Integration von Amazon CloudWatch Logs in Visual Studio erstellt, der folgende Leitfäden enthält: CloudWatch Logs für Visual Studio einrichten und Mit CloudWatch Logs in Visual Studio arbeiten.	29. Juni 2022
Veröffentlichen in AWS	Veröffentlichen unter AWS ist nicht mehr in der Vorschauversion verfügbar. Aktualisierungen, um Änderungen an der Benutzeroberfläche und Verbesserungen der Veröffentlichungsvorschläge widerzuspiegeln.	1. Juni 2022
Neu „Veröffentlichen bis“ als Vorschau AWS verfügbar	Verbessertes Bereitstellungserlebnis, das Sie darüber informiert, welcher AWS Service für Ihre Anwendung am besten geeignet ist.	21. Oktober 2021
SSO- und MFA-Unterstützung für Anmeldeinformationen AWS	Es wurde aktualisiert und dokumentiert nun die neue Unterstützung für AWS Single Sign-On (IAM Identity Center) und die Multi-Faktor-Authentifizierung bei Anmeldeinformationen. AWS	21. April 2021
Grundlegendes AWS Lambda Projekt: Docker-Image erstellen	Unterstützung für Lambda-Container-Images hinzugefügt.	1. Dezember 2020
Inhalt zum Thema Sicherheit	Sicherheitsinhalte hinzugefügt.	6. Februar 2020

Bereitstellung von AWS Anmeldeinformationen	Mit Informationen zum Erstellen von Profilen mit Anmeldeinformationen in der Datei mit gemeinsam genutzten AWS Anmel deinformationen aktualisiert.	20. Juni 2019
Verwenden des AWS Lambda-Projekts im AWS Toolkit for Visual Studio	Support für Visual Studio 2019 wurde dem AWS Toolkit for Visual Studio hinzugefügt.	28. März 2019
Tutorial: Erstellen einer Amazon Rekognition Lambda-Anwendung	Support für Visual Studio 2019 wurde dem AWS Toolkit for Visual Studio hinzugefügt.	28. März 2019
Tutorial: Eine serverlose Anwendung mit AWS Lambda erstellen und testen	Support für Visual Studio 2019 wurde dem AWS Toolkit for Visual Studio hinzugefügt.	28. März 2019
Einrichtung der AWS Toolkit for Visual Studio	Support für Visual Studio 2019 wurde dem hinzugefügt AWS Toolkit for Visual Studio.	28. März 2019
Bereitstellen einer ASP.NET Core 2.0-App (Fargate)	Support für Visual Studio 2019 wurde dem AWS Toolkit for Visual Studio hinzugefügt.	28. März 2019
Bereitstellen einer ASP.NET Core 2.0-App () EC2	Support für Visual Studio 2019 wurde dem AWS Toolkit for Visual Studio hinzugefügt.	28. März 2019
Ein AWS CloudFormation Vorlagenprojekt in Visual Studio erstellen	Support für Visual Studio 2019 wurde dem AWS Toolkit for Visual Studio hinzugefügt.	28. März 2019

Detaillierte Ansichten von Container Service	Es wurden Informationen zu den detaillierten Ansichten der Amazon Elastic Container Service-Cluster und Container -Repositorys hinzugefügt, die von AWS Explorer bereitgestellt werden.	16. Februar 2018
Bereitstellung bei Amazon EC2 Container Service	Es wurden Informationen zur Bereitstellung im Amazon EC2 Container Service hinzugefügt.	16. Februar 2018
Bereitstellung von Container Service mit Fargate	Informationen zur Bereitstellung einer containerisierten ASP.NET Core 2.0-Anwendung für Linux über Amazon ECS mit dem Fargate-Starttyp wurden hinzugefügt.	16. Februar 2018
Bereitstellung von Container Service mit EC2	Es wurden Informationen zur Bereitstellung einer containerisierten ASP.NET Core 2.0-Anwendung für Linux über Amazon ECS unter Verwendung des EC2 Starttyps hinzugefügt.	16. Februar 2018
Anmeldeinformationen für die Bereitstellung bei Amazon EC2 Container Service	Es wurden Informationen zur Angabe von Anmeldeinformationen bei der Bereitstellung im Amazon EC2 Container Service hinzugefügt.	16. Februar 2018

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.