Leitfaden

AWS Toolkit for Visual Studio

AWS Toolkit for Visual Studio: Leitfaden

Table of Contents

AWS Toolkit for Visual Studio

Dies ist das Benutzerhandbuch für AWS Toolkit for Visual Studio. 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 Toolkit for Visual Studio

Das AWS Toolkit for Visual Studio ist ein Plug-in für die Visual Studio-IDE, das Ihnen das Entwickeln, Debuggen und Bereitstellen von.NET-Anwendungen, die Amazon Web Services verwenden, erleichtert. Das Toolkit for Visual Studio wird für Visual Studio-Versionen 2019 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 und 2017 veröffentlicht. Diese Versionen werden jedoch nicht mehr unterstützt. Weitere Informationen finden Sie im Thema Installation und Einrichtung in diesem Benutzerhandbuch.

Das Toolkit for Visual Studio enthält die folgenden Funktionen, um Ihre Entwicklungserfahrung zu verbessern.

AWS Entdecker

Das AWS Explorer-Toolfenster, das im View-Menü der IDE verfügbar ist, ermöglicht es Ihnen, mit vielen AWS Diensten innerhalb der Visual Studio-IDE zu interagieren. Zu den unterstützten Datendiensten gehören Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS) und Amazon. CloudFront AWS Explorer bietet auch Zugriff auf Amazon Elastic Compute Cloud (Amazon EC2) -Management, AWS Identity and Access Management (IAM) Benutzer- und Richtlinienmanagement, die Bereitstellung serverloser Anwendungen und Funktionen sowie die Bereitstellung von Webanwendungen für AWS Lambda und. AWS Elastic Beanstalk AWS CloudFormation

Verwaltung von Anmeldeinformationen und Regionen

AWS Explorer unterstützt mehrere AWS Konten (einschließlich IAM-Benutzerkonten) und Regionen und ermöglicht es Ihnen, die angezeigte Ansicht einfach von einem Konto zu einem anderen zu ändern oder Ressourcen und Dienste in verschiedenen Regionen anzuzeigen und zu verwalten.

Amazon EC2

Im AWS Explorer können Sie verfügbare Amazon Machine Images (AMIs) anzeigen, Amazon EC2 EC2-Instances aus diesen AMIs erstellen und dann mithilfe von Windows Remote Desktop eine Verbindung zu diesen Instances herstellen. AWS Explorer bietet auch unterstützende Funktionen, wie z. B. die Möglichkeit, Schlüsselpaare und Sicherheitsgruppen zu erstellen und zu verwalten.

AWS Lambda

Sie können Lambda verwenden, um Ihre serverlosen .NET Core C#-Funktionen und serverlosen Anwendungen zu hosten. Verwenden Sie Vorlagen, um schnell neue serverlose Projekte zu erstellen und einen Ausgangspunkt für die Entwicklung Ihrer serverlosen Anwendung zu haben.

AWS CodeCommit

CodeCommit ist in Visual Studio Team Explorer integriert. Dies macht es einfach, in CodeCommit der IDE gespeicherte Repositorys zu klonen und zu erstellen und mit Quellcodeänderungen zu arbeiten.

Amazon-DynamoDB

DynamoDB ist ein schneller, hoch skalierbarer, hochverfügbarer, kostengünstiger, nichtrelationaler Datenbankservice. Das Toolkit for Visual Studio bietet Funktionen für die Arbeit mit Amazon DynamoDB in einem Entwicklungskontext. Mit dem Toolkit for Visual Studio können Sie Attribute in DynamoDB-Tabellen erstellen und bearbeiten und Scanvorgänge für Tabellen ausführen.

Amazon S3

Sie können Inhalte schnell und einfach per Drag-and-Drop in Amazon S3-Buckets hochladen oder Inhalte von Amazon S3 herunterladen. Darüber hinaus können Sie Berechtigungen, Metadaten und Tags bequem für Objekte in Buckets angeben.

Amazon RDS

AWS Explorer kann Ihnen helfen, Amazon RDS-Assets in Visual Studio zu erstellen und zu verwalten. Amazon RDS-Instances, die Microsoft SQL Server verwenden, können auch zum Server Explorer von Visual Studio hinzugefügt werden.

AWS Elastic Beanstalk

Sie können Elastic Beanstalk verwenden, um Ihre .NET-Webanwendungsprojekte bereitzustellen. AWS Sie haben die Möglichkeit, Ihre Anwendung in einer Umgebung mit einer einzelnen Instance oder einer komplett lastverteilten, automatisch skalierten Umgebung in IDE bereitzustellen. Zudem können Sie neue Versionen Ihrer Anwendung schnell und bequem bereitstellen, ohne Visual Studio zu verlassen. Wenn Ihre Anwendung SQL Server in Amazon RDS verwendet, kann der Bereitstellungsassistent auch die Konnektivität zwischen Ihrer Anwendungsumgebung in Elastic Beanstalk und der Datenbank-Instance in Amazon RDS einrichten. Das Toolkit for Visual Studio umfasst auch das eigenständige Befehlszeilen-Bereitstellungstool. Verwenden Sie das Bereitstellungstool, um die automatische Bereitstellung in den Erstellungsvorgang aufzunehmen oder um die Bereitstellung in anderen Skriptszenarien außerhalb von Visual Studio einzuschließen.

AWS CloudFormation

Sie können das Toolkit for Visual Studio verwenden, um Vorlagen im AWS CloudFormation JSON-Format mit Unterstützung für Editor IntelliSense und Syntaxhervorhebung zu bearbeiten. Mit einer AWS CloudFormation Vorlage beschreiben Sie die Ressourcen, die Sie instanziieren möchten, um Ihre Anwendung zu hosten. Von der IDE aus stellen Sie dann die Vorlage bereit. AWS CloudFormation Die in der Vorlage beschriebenen Ressourcen werden für Sie bereitgestellt. So können Sie sich ganz auf die Entwicklung der Anwendungsfunktionalität konzentrieren.

AWS Identity and Access Management (ICH BIN)

Im AWS Explorer können Sie IAM-Benutzer, -Rollen und -Richtlinien erstellen und Benutzern Richtlinien zuordnen.

Verwandte Informationen

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

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

Amazon Q und Amazon CodeWhisperer

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 Thema Amazon Q Developer in IDEs im Amazon Q Developer User Guide. Detaillierte Informationen zu Plänen und Preisen für Amazon Q finden Sie im Amazon Q-Preisleitfaden.

Herunterladen des Toolkit for Visual Studio

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

Herunterladen des Toolkits aus dem Visual Studio Marketplace

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

Zusätzliche IDE Toolkits von AWS

Zusätzlich zum Toolkit for Visual Studio bietet AWS auch IDE Toolkits für VS-Code und JetBrains.

AWS Toolkit for Visual Studio Code Links

- Folgen Sie diesem Link, um die aus dem VS Code Marketplace herunterzuladenAWS Toolkit for Visual Studio Code.
- Weitere Informationen über finden AWS Toolkit for Visual Studio CodeSie im AWS Toolkit for Visual Studio Code-Benutzerhandbuch.

AWS Toolkit for JetBrains Links

- Folgen Sie diesem Link, um die vom Marketplace herunterzuladenAWS Toolkit for JetBrains. JetBrains
- Weitere Informationen zu finden AWS Toolkit for JetBrainsSie im AWS Toolkit for JetBrains-Benutzerhandbuch.

Erste Schritte

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

In den folgenden Themen wird beschrieben, wie Sie die installieren, einrichten und konfigurierenAWS 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**
>
> Falls 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

Die meisten Dienste und Ressourcen von Amazon Web Services (AWS) werden über ein AWS Konto verwaltet. Für die Nutzung von ist kein AWS Konto erforderlich. Ohne Verbindung sind die AWS Toolkit for Visual Studio Funktionen des Toolkit jedoch eingeschränkt.

Wenn Sie zuvor ein AWS Konto eingerichtet und sich über einen anderen AWS Dienst (z. B. den AWS Command Line Interface) authentifiziert haben, erkennt das Toolkit for Visual Studio Ihre Anmeldeinformationen automatisch.

Voraussetzungen

Wenn Sie noch kein Konto haben AWS oder noch kein Konto erstellt haben, gibt es drei Hauptschritte, um das Toolkit for Visual Studio mit Ihrem AWS Konto zu verbinden:

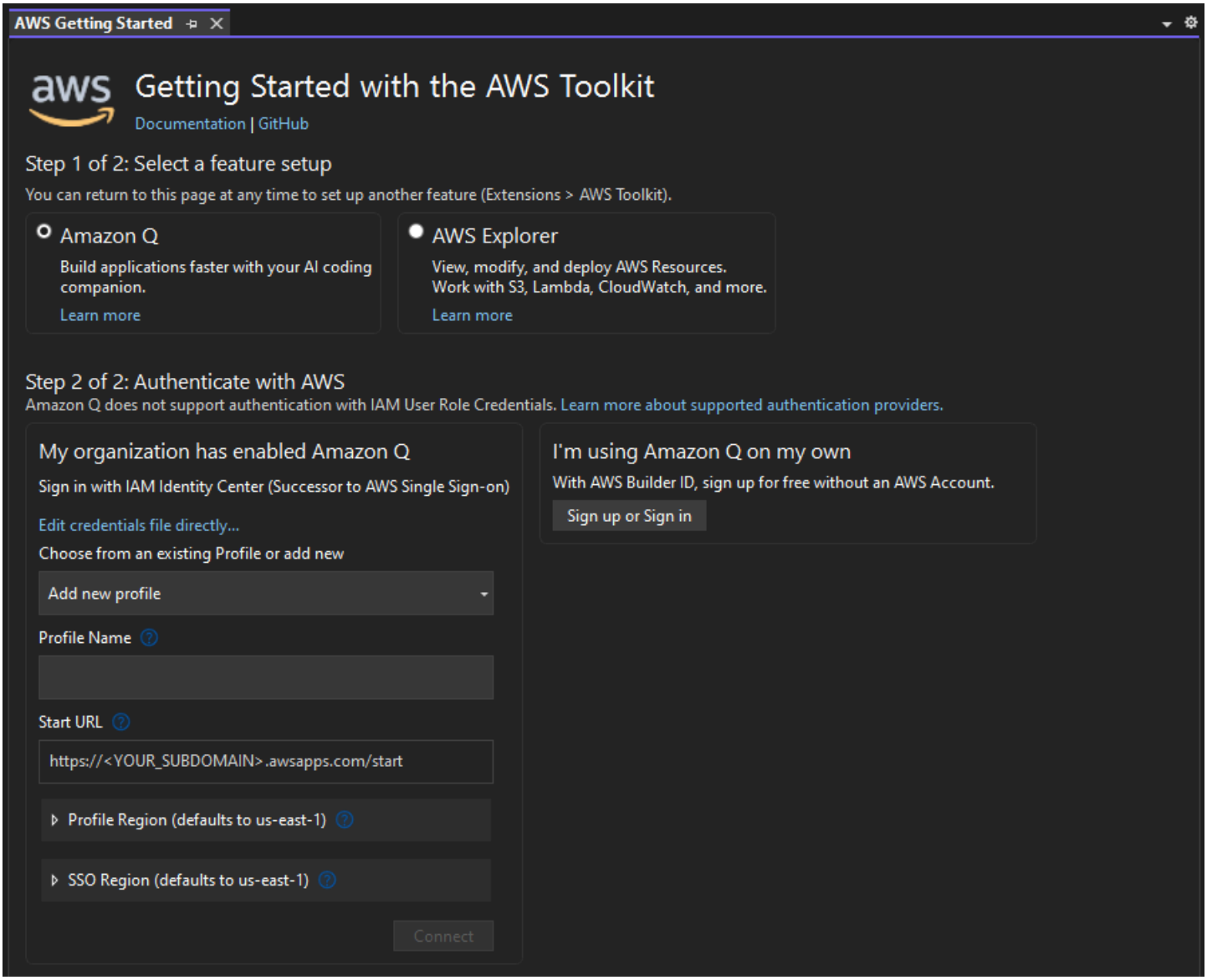
1. Registrierung für ein AWS Konto: Sie können sich über das Anmeldeportal für ein AWS Konto AWS registrieren. Ausführliche Informationen zur Einrichtung eines neuen AWS Kontos finden Sie im Thema „Übersicht“ im AWS Setup-Benutzerhandbuch.

2. Authentifizierung einrichten: Es gibt drei Hauptmethoden, um sich mit Ihrem AWS Konto aus dem Toolkit for Visual Studio zu authentifizieren. Weitere Informationen zu den einzelnen Methoden finden Sie im Thema Authentifizierung und Zugriff in diesem Benutzerhandbuch.
3. Authentifizierung über das Toolkit: Sie können über das Toolkit eine Verbindung mit Ihrem AWS Konto herstellen, indem Sie die Verfahren in den folgenden Abschnitten dieses Benutzerhandbuchs ausführen. AWS

Über das Toolkit eine AWS Verbindung herstellen

Um vom Toolkit for Visual Studio aus eine Verbindung zu Ihren AWS Konten herzustellen, öffnen Sie die Benutzeroberfläche Erste Schritte mit der AWS Toolkit-Benutzeroberfläche (Verbindungsbenutzeroberfläche), indem Sie das folgende Verfahren ausführen.

1. Erweitern Sie im Visual Studio-Hauptmenü die Option Erweiterungen und dann das AWS Toolkit.
2. Wählen Sie in den AWS Toolkit-Menüoptionen die Option Erste Schritte aus.
3. Die Benutzeroberfläche „Erste Schritte mit der AWS Toolkit-Verbindung“ wird in Visual Studio geöffnet.



In der folgenden Tabelle wird beschrieben, welche Authentifizierungsmethoden mit den einzelnen Funktionen kompatibel sind. Weitere Informationen zu den drei Authentifizierungsmethoden AWS IAM Identity Center, AWS Identity and Access Management Anmeldeinformationen und AWS Builder-ID finden Sie im Inhaltsverzeichnis Authentifizierung und Zugriff in diesem Benutzerhandbuch.

> **Note**
>
> Derzeit müssen Sie bei der Arbeit mit CodeCatalyst dem Toolkit for Visual Studio nur mit Ihrer AWS Builder-ID autorisieren, wenn Sie ein Repository eines Drittanbieters klonen.

Amazon Q-Entwickler	AWS Entdecker	Amazon CodeCatalyst
☑ AWS Builder-ID	☒ AWS Builder-ID	☑ AWS Builder-ID
☑ IAM-Identitätszentrum	☑ IAM-Identitätszentrum	☒ IAM-Identitätszentrum
☒ AWS IAM-Anmeldeinformationen	☑ AWS IAM-Anmeldeinformationen	☒ AWS IAM-Anmeldeinformationen

Authentifizierung für Amazon Q Developer

Um mit Amazon Q Developer zu beginnen, authentifizieren Sie sich und stellen Sie eine Verbindung mit Ihren AWS IAM Identity Center oder AWS Builder ID-Anmeldeinformationen her.

Die folgenden Verfahren beschreiben, wie Sie das Toolkit authentifizieren und mit Ihrem Konto verbinden. AWS

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

1. Wählen Sie auf der Benutzeroberfläche Erste Schritte mit der AWS Toolkit-Verbindung das Amazon Q Developer-Radial aus, um die Amazon Q Developer-Authentifizierungsoptionen zu erweitern.

   > **Note**
   >
   > Wenn keine gespeicherten Anmeldeinformationen vorhanden sind, fahren Sie mit Schritt 3 fort, um Ihre IAM Identity Center-Anmeldeinformationen hinzuzufügen oder zu aktualisieren.

2. Erweitern Sie im Bereich Meine Organisation hat Amazon Q Developer aktiviert das Drop-down-Menü Aus einem vorhandenen Profil auswählen oder neues hinzufügen, um aus Ihrer Liste der gespeicherten Anmeldeinformationen auszuwählen.
3. Wählen Sie im Drop-down-Menü Profiltyp die Option AWS IAM Identity Center
4. Geben Sie im Textfeld Profilname den Namen **`Profile Name`** des IAM Identity Center-Profils 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, und klicken Sie dann auf die Schaltfläche Connect, um das Dialogfeld Mit AWS IAM Identity Center anmelden zu öffnen.
8. Wählen Sie im Dialogfeld „Mit AWS IAM Identity Center anmelden“ die Schaltfläche „Weiter zum Browser“, um die Website „Anfrage AWS autorisieren“ in Ihrem Standard-Webbrowser zu öffnen.
9. Vergewissern Sie sich, dass der Sicherheitscode in Ihrer IDE mit dem Bestätigungscode für die AWS Autorisierungsanfrage übereinstimmt, der in Ihrem Webbrowser angezeigt wird, und klicken Sie auf Absenden und fortfahren, um fortzufahren.
10. 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.

Authentifizieren Sie sich und stellen Sie eine Verbindung mit einer Builder-ID AWS her

1. Wählen Sie auf der Benutzeroberfläche Erste Schritte mit der AWS Toolkit-Verbindung das Amazon Q Developer-Radial aus, um die Amazon Q Developer-Authentifizierungsoptionen zu erweitern.
2. Wählen Sie im Abschnitt Ich verwende Amazon Q Developer eigenständig auf die Schaltfläche Registrieren oder Anmelden, um das Dialogfeld Mit AWS Builder-ID anmelden zu öffnen.
3. Wählen Sie die Schaltfläche Weiter zum Browser, um die Website „Anfrage AWS autorisieren“ in Ihrem Standard-Webbrowser zu öffnen.
4. Vergewissern Sie sich, dass der Sicherheitscode in Ihrer IDE mit dem Bestätigungscode für die AWS Autorisierungsanfrage übereinstimmt, der in Ihrem Webbrowser angezeigt wird, und klicken Sie auf Absenden und fortfahren, um fortzufahren.
5. 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.

Authentifizierung für den Explorer AWS

Um mit der Arbeit mit dem AWS Explorer über das Toolkit zu beginnen, authentifizieren Sie sich und stellen Sie eine Verbindung entweder mit Ihren IAM Identity Center- oder IAM-Anmeldeinformationen her.

In den folgenden Verfahren wird beschrieben, wie Sie das Toolkit authentifizieren und mit Ihrem Konto verbinden. AWS

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

1. Wählen Sie auf der Benutzeroberfläche Erste Schritte mit der AWS Toolkit-Verbindung das AWS Explorer-Radial aus, um die Amazon Q Developer-Authentifizierungsoptionen zu erweitern.
2. Wählen Sie im Dropdown-Menü **`Profile Type`** die Option AWS IAM Identity Center aus.
3. Geben Sie im Textfeld Profilname das **`Profile Name`** IAM Identity Center-Profil ein, das Sie verwenden möchten.
4. Geben Sie im Textfeld Start-URL **`Start URL`** die an Ihre IAM Identity Center-Anmeldeinformationen angehängte URL ein.
5. 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.
6. 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.
7. Wählen Sie die Schaltfläche Weiter zum Browser, um die Website „Anfrage AWS autorisieren“ in Ihrem Standard-Webbrowser zu öffnen.
8. Vergewissern Sie sich, dass der Sicherheitscode in Ihrer IDE mit dem Bestätigungscode für die AWS Autorisierungsanfrage übereinstimmt, der in Ihrem Webbrowser angezeigt wird, und klicken Sie auf Senden und Fortfahren, um fortzufahren.
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.

Authentifizieren Sie sich und stellen Sie eine Verbindung mit IAM-Anmeldeinformationen her

1. Wählen Sie auf der Benutzeroberfläche Erste Schritte mit der AWS Toolkit-Verbindung das AWS Explorer-Radial aus, um die Amazon Q Developer-Authentifizierungsoptionen zu erweitern.
2. Wählen Sie im **`Profile Type`** Drop-down-Menü die Option IAM-Benutzerrolle aus.
3. Geben Sie im Textfeld Profilname den Namen **`Profile Name`** des Profils ein, mit dem Sie sich authentifizieren möchten.
4. Geben Sie im Textfeld Access Key ID die **`Access Key ID`** für das Profil ein, mit dem Sie sich authentifizieren möchten.

5. Geben Sie im Textfeld Geheimer Schlüssel den Wert **`Secret Key`** für das Profil ein, mit dem Sie sich authentifizieren möchten.
6. Geben Sie im Dropdownmenü Speicherort (standardmäßig Datei mit gemeinsamen Anmeldeinformationen) an, ob Sie Ihre Anmeldeinformationen mit einer Datei mit gemeinsamen Anmeldeinformationen oder mit .NET Encrypted Stored speichern möchten.
7. Wählen Sie im Drop-down-Menü Profilregion (standardmäßig us-east-1) die Profilregion aus, die mit dem Profil verknüpft ist, mit dem Sie sich authentifizieren möchten.

Behebung von Installationsproblemen des AWS Toolkit for Visual Studio

Es ist bekannt, dass die folgenden Informationen häufig auftretende Installationsprobleme bei der Installation von behebenAWS Toolkit for Visual Studio.

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

Administratorberechtigungen für Visual Studio

Für die AWS Toolkit for Visual Studio Erweiterung sind Administratorberechtigungen erforderlich, um sicherzustellen, dass alle AWS Dienste und Funktionen zugänglich sind.

Wenn Sie über lokale Administratorberechtigungen verfügen, ist es möglich, dass sich Ihre Administratorberechtigungen nicht direkt auf Ihre Visual Studio-Instanz erstrecken.

Um Visual Studio lokal mit Administratorrechten zu starten:

1. Suchen Sie unter Windows den Visual Studio-Anwendungsstarter (Symbol).
2. Öffnen Sie das Kontextmenü für das Visual Studio-Symbol (Rechtsklick), um das Kontextmenü zu öffnen.
3. Wählen Sie im Kontextmenü die Option Als Administrator ausführen aus.

So starten Sie Visual Studio mit Administratorrechten aus der Ferne:

1. Suchen Sie in Windows den Anwendungsstarter für die Anwendung, mit der Sie eine Verbindung zu Ihrer Remote-Instanz von Visual Studio herstellen.
2. Öffnen Sie das Kontextmenü der Anwendung (Rechtsklick), 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 Administratoranmeldeinformationen zu bestätigen.

Abrufen eines Installationsprotokolls

Wenn Sie die Schritte im vorherigen Abschnitt mit Administratorberechtigungen ausgeführt haben und bestätigt wurde, dass Sie Visual Studio mit Administratorberechtigungen 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. Ersetzen Sie `[file path to log file]` durch den Dateinamen und den vollständigen Dateipfad des Verzeichnisses, in dem das Installationsprotokoll erstellt werden soll. Ein Beispiel für den `vsixinstaller` Befehl mit Ihrem angegebenen Dateipfad und Dateinamen sieht wie folgt aus:

   ```
   vsixinstaller /logFile:C:\Users\Documents\install-log.txt [file path to AWSToolkitPackage.vsix]
   ```
5. Ersetzen Sie `[file path to Toolkit installation file]` 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 Ihr 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 mit Visual Studio beheben, anstatt mit. AWS Toolkit for Visual Studio

Den -Support kontaktieren

Wenn du alle Abschnitte in diesem Handbuch gelesen hast und zusätzliche Ressourcen oder Unterstützung benötigst, kannst du dir auf der AWS Toolkit for Visual StudioGithub-Issues-Website frühere Probleme ansehen oder ein neues Problem öffnen.

Gehen Sie wie folgt vor, um die Lösung Ihres Problems zu beschleunigen:

- Überprüfen Sie frühere und aktuelle Probleme, um festzustellen, 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 durch die Installation der AWS Toolkit for Visual Studio oder anderer Erweiterungen erhalten haben.
- Hängen Sie Ihre AWS Toolkit for Visual Studio Installations-Logfiles an die neue Ausgabe an.

Profile und Fensterbindung

Profile und das Toolkit for Visual Studio

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

- DasAWS Explorer-Fenster ist jeweils an ein einzelnes Profil und eine Region gebunden. Windows wurde standardmäßig vomAWS Explorer aus für dieses gebundene Profil und diese Region geöffnet.
- Nachdem ein neues Fenster geöffnet wurde, können Sie diese Instanz desAWS Explorers verwenden, um zu einem anderen Profil oder einer anderen Region zu wechseln.
- Das Toolkit für die Veröffentlichungstools und -funktionen von Visual Studio verwendet standardmäßig automatisch das Profil und die Region, die imAWS Explorer festgelegt sind.
- Wenn ein neues Profil oder eine neue Region in einem Veröffentlichungstool, einem Assistenten oder einer Funktion angegeben wird: Alle danach erstellten Ressourcen verwenden 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.
- DerAWS Explorer speichert das letzte Profil und die Region, die zuletzt angegeben wurden, und die Werte der allerletzten geschlossenen Visual Studio-Instanz werden beibehalten.

Authentifizierung und Zugriff

Sie müssen sich nicht authentifizieren, AWS um mit dem AWS Toolkit for Visual Studio zu arbeiten. Die meisten AWS Ressourcen werden jedoch über ein AWS Konto verwaltet. Um auf alle Dienste und Funktionen des AWS Toolkit for Visual Studio 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 der AWS Toolkit for Visual Studio finden Sie im Abschnitt zur IAM Identity Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.

Authentifizierung mit IAM Identity Center über 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 für die Authentifizierung mit Ihrem AWS Konto über einrichten. 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 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 das für 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 für AWS SDKs und Tools 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.

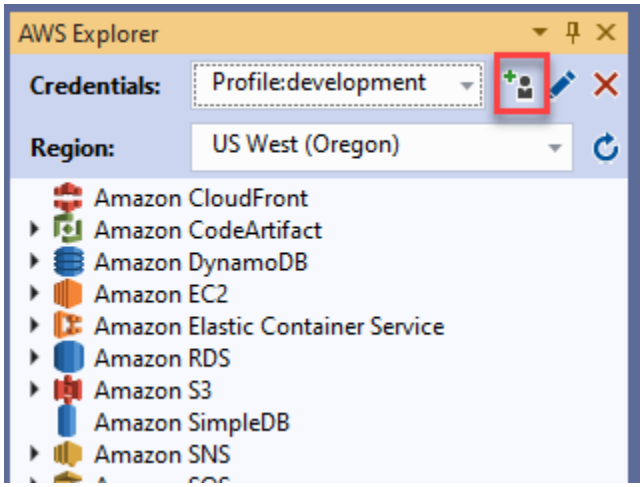
Eine Anmeldeinformationsdatei erstellen

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 Referenzhandbuch zu AWS SDKs und Tools.

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

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 https://console.aws.amazon.com/iam auf.

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 https://console.aws.amazon.com/iam auf.
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 übernimmt. 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.

Mit AWS Diensten arbeiten

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

Themen

Amazon CodeCatalyst für das AWS Toolkit für Visual Studio

Was ist Amazon CodeCatalyst?

Amazon CodeCatalyst ist ein Cloud-basierter Kollaborationsraum für Softwareentwicklungsteams. Mit dem AWS Toolkit für Visual Studio können Sie CodeCatalyst Ressourcen direkt vom AWS Toolkit for

Visual Studio aus anzeigen und verwalten. Weitere Informationen CodeCatalyst dazu finden Sie im CodeCatalystAmazon-Benutzerhandbuch.

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

Themen

Erste Schritte mit Amazon CodeCatalyst und dem AWS Toolkit für Visual Studio

Gehen Sie wie folgt CodeCatalyst vor, um mit der Arbeit mit Amazon über das AWS Toolkit für Visual Studio zu beginnen.

Themen

Installation des AWS Toolkits für Visual Studio

Bevor Sie das AWS Toolkit für Visual Studio in Ihre CodeCatalyst Konten integrieren, stellen Sie sicher, dass Sie eine aktuelle Version von AWS Toolkit for Visual Studio verwenden. Einzelheiten zur Installation und Einrichtung der neuesten Version von AWS Toolkit for Visual Studio finden Sie im Abschnitt Einrichten des AWS Toolkits für Visual Studio in diesem Benutzerhandbuch.

CodeCatalystKonto und AWS Builder-ID erstellen

Zusätzlich zur Installation der neuesten Version des AWS Toolkit for Visual Studio benötigen Sie eine aktive AWS Builder-ID und ein aktives CodeCatalyst Builder-Konto, um eine Verbindung mit AWS Toolkit for Visual Studio herzustellen. Wenn Sie keine aktive AWS Builder-ID oder kein

aktives CodeCatalyst Builder-Konto haben, finden Sie im CodeCatalyst Abschnitt Einrichtung mit im CodeCatalystBenutzerhandbuch weitere Informationen.

> **Note**
>
> Eine AWS Builder-ID unterscheidet sich von Ihren AWS Anmeldeinformationen. Anweisungen zur Registrierung und Authentifizierung mit einer AWS Builder-ID finden Sie im Thema Authentifizierung und Zugriff: AWS Builder-ID in diesem Benutzerhandbuch. Detaillierte Informationen zu AWS Builder-IDs finden Sie im Thema AWSBuilder-ID im AWSGeneral Reference User Guide.

AWSToolkit for Visual Studio verbinden mit CodeCatalyst

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

1. Wählen Sie im Menü Git 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 Mit AWS Builder-ID verbinden 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 und Ihrem CodeCatalyst Konto zu bestätigen. Wenn der Verbindungsvorgang abgeschlossen ist, wird eine Bestätigung CodeCatalyst angezeigt, die besagt, dass das Schließen Ihres Browsers sicher ist.

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

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

Themen

- Klonen Sie ein Repository

Klonen Sie ein Repository

CodeCatalystist ein Cloud-basierter Dienst, für den 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 Ihren lokalen Computer klonen und bei der nächsten Verbindung mit der Cloud mit Ihrem CodeCatalyst Projekt synchronisieren.

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

1. Wählen Sie im Menü Git 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 in diesem Benutzerhandbuch aus, bevor Sie fortfahren.

3. Wählen Sie den Bereich und das Projekt aus, aus denen Sie ein Repository klonen möchten.
4. Wählen Sie im Abschnitt 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 zu klonen.

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

Fehlerbehebung

Im Folgenden finden Sie Themen zur Problembehandlung zur Behebung bekannter Probleme bei der Arbeit mit Amazon CodeCatalyst über das AWS Toolkit für Visual Studio.

Themen

Anmeldeinformationen

Wenn beim Versuch, ein Git-basiertes Repository zu klonen, ein Dialogfeld angezeigt wird, in dem Sie nach Anmeldeinformationen gefragt werdenCodeCatalyst, ist Ihr AWSCodeCommitCredential-Helper möglicherweise global konfiguriert, was zu Interferenzen führt. CodeCatalyst Weitere Informationen zur AWS CodeCommit Anmeldeinformationshilfe finden Sie im Abschnitt Schritte zum Einrichten von HTTPS-Verbindungen zu AWS CodeCommit Repositorys unter Windows mit dem AWS CLI-Anmeldeinformationshelfer im Benutzerhandbuch. AWSCodeCommit

Gehen Sie wie folgt vor, um den AWSCodeCommitCredential-Helfer darauf zu beschränken, nur CodeCommit URLs zu verarbeiten.

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 aus, um Ihr Repository zu klonen.

Amazon CloudWatch Protokollintegration for Visual Studio

Der Amazon CloudWatch Protokollintegration von derAWSToolkit for Visual Studio bietet Ihnen die Möglichkeit, zu überwachen, zu speichern und darauf zuzugreifen CloudWatch Protokolliert Ressourcen, ohne Ihre IDE verlassen zu müssen. Für weitere Informationen zum Einrichten der CloudWatch service und Vorgehensweise bei der Arbeit mit CloudWatch Logs-Funktionen finden Sie unter den folgenden Themen.

Themen

Einrichten von CloudWatch Protokollintegration für Visual Studio

Bevor Sie Amazon verwenden können CloudWatch Logs-Integration mit dem Toolkit for Visual Studio benötigen Sie einAWSKonto. Sie können ein neues erstellenAWSKonto aus demAWSAnmeldenSeite. Die meisten CloudWatch Protokollfunktionen, die im Toolkit for Visual Studio verfügbar sind, sind mit aktivemAWS-Anmeldeinformationen. Wenn eine bestimmte Funktion eine zusätzliche Konfiguration erfordert, sind die Anforderungen in den entsprechenden Abschnitten desArbeiten mit CloudWatch ProtokolleHandbuch.

Weitere Informationen und Optionen zum Einrichten CloudWatch Logs finden Sie imEinrichtenim Amazonas-Bereich CloudWatch Leitfaden für Protokolle.

Arbeiten mit CloudWatch Protokollgruppen

Amazon CloudWatch Protokollgruppen ermöglicht Ihnen das Überwachen, Speichern und Aufrufen CloudWatch -Protokolle ausAWSToolkit for Visual Studio. Zugriff haben auf CloudWatch Protokolliert Funktionen — ohne dass Sie Ihre IDE verlassen müssen — Verbessert die Effizienz durch Vereinfachung der CloudWatch Protokolliert den Entwicklungsprozess und reduziert Störungen Ihres Arbeitsablaufs. In den folgenden Themen wird beschrieben, wie Sie mit den grundlegenden Features und Funktionen des CloudWatch (Protokollieren von bis

Themen

- Zusätzlicher Zugriff auf CloudWatchProtokolle

CloudWatch -Protokollgruppen

EIN`log group`ist eine Gruppe von`log streams`, die dieselben Einstellungen für die Aufbewahrung, Überwachung und Zugriffskontrolle besitzen. Es gibt keine Begrenzung dazu, wie viele Protokoll-Streams zu einer Protokollgruppe gehören können.

Anzeigen von -Protokollgruppen

Die`View Log Groups`-Funktion zeigt eine Liste der Protokollgruppen CloudWatchProtokollgruppen

Um auf die Funktion „Protokollgruppen anzeigen“ zuzugreifen, öffnen Sie die CloudWatch Protokollgruppen

1. FromAWSExplorer, erweiternAmazon CloudWatchaus.
2. Doppelklicken Sie-Protokollgruppenoder öffnen Sie das Kontextmenü (rechte Maustaste) und wählen SieAnzeigenausCloudWatch --Protokollgruppenaus.

> **Note**
>
> Die CloudWatch Der Protokollgruppen-Explorer wird im selben Fensterspeicherort wie der Solutions Explorer geöffnet.

Filtern von Protokollgruppen

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

1. FromCloudWatch Protokollgruppenden Cursor in die Suchleiste oben im Fenster.
2. Geben Sie ein Präfix ein, das sich auf die Protokollgruppen bezieht, nach denen Sie suchen.
3. CloudWatch Protokollgruppenwird automatisch aktualisiert und zeigt Ergebnisse an, die mit den Suchbegriffen übereinstimmen, die Sie im vorherigen Schritt angegeben haben.

Löschen von bis

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

1. FromCloudWatch Protokollgruppenklicken Sie mit der rechten Maustaste auf die Protokollgruppen, die Sie löschen möchten.
2. Bestätigen Sie, dass Sie die aktuell ausgewählte Protokollgruppen löschen möchten, wenn Sie dazu aufgefordert werden.
3. Die Wahl desJalöscht die ausgewählte Protokollgruppe und aktualisiert dann dieCloudWatch Protokollgruppenaus.

(Protokollgruppen)

Um die aktuelle Liste der Protokollgruppen zu aktualisieren, die in derCloudWatch --Protokollgruppen, wählen SieAktualisierungssymbol-Button befindet sich in derSymbolleisteaus.

ARN der Protokollgruppe kopieren

Führen Sie die unten beschriebenen Schritte aus, um den ARN einer bestimmten Protokollgruppe zu kopieren.

1. FromCloudWatch Protokollgruppenklicken Sie mit der rechten Maustaste auf die Protokollgruppe, aus der Sie einen ARN kopieren möchten.
2. Wählen Sie das SymbolARN kopierenOption aus dem Menü.
3. Der ARN ist jetzt in Ihre lokale Zwischenablage kopiert und kann eingefügt werden.

CloudWatch Protokollstreams

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

> **Note**
>
> Beachten Sie beim Anzeigen von Protokollstreams die folgenden Eigenschaften:
>
> - Standardmäßig sind die Log-Streams nach dem Zeitstempel des letzten Ereignisses sortiert.
> - Spalten, die mit einem Log-Stream verknüpft sind, können entweder in aufsteigender oder absteigender Reihenfolge sortiert werden, indem Sie dieCaretzeichenbefindet sich in den Spaltenüberschriften.
> - Gefilterte Einträge können nur sortiert werden nachProtokollstreamnameaus.

Protokollstreams

1. FromCloudWatch ProtokollgruppenDoppelklicken Sie auf eine Protokollgruppen oder klicken Sie mit der rechten Maustaste auf eine ProtokollgruppenAnzeigen von Protokollstreamaus dem Kontextmenü.
2. Eine neue Registerkarte öffnet sich in derDokument, das eine Liste von Log-Streams enthält, die mit Ihrer Log-Gruppe verknüpft sind.

Filtern von Protokollstreams

1. FromProtokollstreamsauf der RegisterkarteDokumentden Cursor in der Suchleiste.
2. Geben Sie ein Präfix ein, das sich auf den gesuchten Protokollstream bezieht.
3. Während der Eingabe wird die aktuelle Anzeige automatisch aktualisiert, um Ihre Log Streams nach Ihren Eingaben zu filtern.

Protokollstreams

Um die aktuelle Liste der Log-Streams zu aktualisieren, die in derDokumentauf der Seite ausAktualisierungssymbol-Button, befindet sich in derSymbolleisteausSuchleisteaus.

Protokollstreams

Führen Sie die unten beschriebenen Schritte aus, um den ARN eines bestimmten Protokollstreams zu kopieren.

1. FromProtokollstreamsauf der RegisterkarteDokumentklicken Sie mit der rechten Maustaste auf den Protokollstreams, aus dem Sie einen ARN kopieren möchten.
2. Wählen Sie das SymbolARN kopierenOption aus dem Menü.
3. Der ARN ist jetzt in Ihre lokale Zwischenablage kopiert und kann eingefügt werden.

Protokollstreams

DieExromlädt den ausgewählten Protokollstream herunter und speichert ihn lokal, wo er von benutzerdefinierten Tools und Software zur weiteren Verarbeitung aufgerufen werden kann.

1. FromProtokollstreamsauf der RegisterkarteDokumentklicken Sie mit der rechten Maustaste auf den Protokollstreams, den Sie herunterladen möchten.

2. Klicken Sie aufExromausExportieren in eine TextdateiDialog.
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 SieOKAYaus. Der Status des Downloads wird imVisual Studio-Aufgabenstatuscenter

CloudWatch Protokollereignisse

Protokollereignisse sind Aufzeichnungen von einigen Aktivitäten, die von der überwachten Anwendung oder Ressource aufgezeichnet werden CloudWatchaus.

-Protokollieren von -

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 umgebrochenen Text: Sie können umgebrochenen Text umschalten, indem Sie auf ein Ereignis klicken.
- Text-Wrap-Schaltfläche: befindet sich im`document window` **`toolbar`**aktiviert und deaktiviert diese Schaltfläche den Textumbruch für alle Einträge.
- Nachrichten in die Zwischenablage kopieren: Wählen Sie die Nachrichten aus, die Sie kopieren möchten, klicken Sie mit der rechten Maustaste auf die Auswahl und wählenKopieren(Tastaturbefehl)`Ctrl + C`) enthalten.

Anzeigen von --Ereignissen

1. FromDokumenteine Registerkarte aus, die eine Liste von Log-Streams enthält.
2. Doppelklicken Sie auf einen Protokollstream oder klicken Sie mit der rechten Maustaste auf einen Protokollstream undAnzeigen von Protokollstreamaus.
3. Eine neue-Protokollereignisseöffnet sich imDokument, das eine Tabelle mit Protokollereignissen enthält, die mit dem von Ihnen ausgewählten Log-Stream verknüpft sind.

Filtern von Protokollereignissen

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

So filtern Sie Ihre Log-Ereignisse nach Inhalt:

1. From-Protokollereignisseauf der RegisterkarteDokumentden Cursor in die Suchleiste oben im Fenster.
2. Geben Sie einen Begriff oder eine Phrase ein, 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 Phrasen mit nicht alphanumerischen Zeichen in doppelte Anführungszeichen (*""*) einschließen. Weitere Informationen zu Filtermustern finden Sie in derFilter- und MustersyntaxThema im Amazonas CloudWatch Leitfaden.

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

1. From-Protokollereignisseauf der RegisterkarteDokumentauf der Seite ausKalendergruppe-Button, befindet sich in derSymbolleisteaus.
2. Geben Sie mithilfe der bereitgestellten Felder den Zeitraum an, der durchsucht werden soll.
3. Die gefilterten Ergebnisse werden automatisch aktualisiert, wenn Sie die Datums- und Zeitbeschränkungen angeben.

> **Note**
>
> DieLöschen von FilterOption löscht alle Ihre aktuellen date-and-time -Filtergruppen.

Aktualisereignisse

Um die aktuelle Liste der Protokollereignisse zu aktualisieren, die in der-Protokollereignisseauf der Registerkarte auf der RegisterkarteAktualisierungssymbol-Button, befindet sich in derSymbolleisteaus.

Zusätzlicher Zugriff auf CloudWatchProtokolle

Sie können auf zugreifen CloudWatch ProtokollgruppenAWSDienstleistungen und Ressourcen direkt aus demAWSToolkit in Visual Studio.

Lambda

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

> **Note**
>
> Ihre Lambda-Ausführungsrolle muss über entsprechende Berechtigungen verfügen, um Protokollprotokolle CloudWatchprotokolle. Weitere Informationen zu den Lambda-Berechtigungen, die für CloudWatch Logs finden Sie imhttps://docs.aws.amazon.com/lambda/latest/dg/monitoring-cloudwatchlogs.html#monitoring-cloudwatchlogs-prereqs

1. FromAWSToolkit-Explorer, erweiternLambdaaus.
2. rechte Maustaste auf die Funktion, die Sie anzeigen möchten, und wählen SieAnzeigen von Protokollen, um die zugehörigen Log-Streams imDokumentFenster.

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

1. FromAWSToolkit-Explorer, erweiternLambdaaus.
2. rechte Maustaste auf die Funktion, die Sie anzeigen möchten, und wählen SieView-Funktionum die Funktionsansicht in derDokumentFenster.
3. From`function view`ausProtokollewerden die Log-Streams angezeigt, die mit der ausgewählten Lambda-Funktion verknüpft sind.

ECS

Führen Sie das folgende Verfahren aus, um Protokollressourcen anzuzeigen, die mit einem ECS Task-Container verknüpft sind.

> **Note**
>
> Damit der Amazon ECS-Service Protokolle an CloudWatchmuss jeder Container für eine bestimmte Amazon ECS-Aufgabe die erforderliche Konfiguration erfüllen. Weitere Informationen zur erforderlichen Einrichtung und Konfiguration finden Sie in der AnleitungVerwendung derAWS-Protokollstreamaus.

1. FromAWSToolkit-Explorer, erweiternAmazon ECSaus.
2. Wählen Sie den Amazon ECS-Cluster aus, den Sie anzeigen möchten, um einen neuenECS-Clusterauf der RegisterkarteDokumentFenster.
3. Über das Navigationsmenü auf der linken Seite desECS-Clusterauf der Registerkarte.Aufgaben, um alle mit dem Cluster verknüpften Tasks aufzulisten.
4. FromAufgabenanzeigen, wählen Sie eine Aufgabe aus und wählen SieAnzeigen von ProtokollenLink, der sich in der unteren linken Ecke befindet.

   > **Note**
   >
   > Diese Anzeige listet alle im Cluster enthaltenen Aufgaben auf, die`View Logs`Link ist nur für jede Aufgabe sichtbar, die die erforderliche Protokollkonfiguration erfüllt.
   >
   > - Wenn eine Aufgabe nur mit einem einzelnen Container verknüpft ist,Anzeigen von ProtokollenLink öffnet den Logstream dieses Containers.
   > - Wenn eine Aufgabe mit mehreren Containern verknüpft ist,Anzeigen von ProtokollenLink öffnet dasAnzeigen CloudWatch Protokolle für ECS-Aufgabeverwenden Sie dasContainer:Dropdown-Menü, um den Container auszuwählen, für den Sie Logs anzeigen möchten, und wählen Sie dannOKAYaus.

5. Eine neue Registerkarte öffnet sich in derDokumentFenster mit den Log-Streams, die Ihrer Containerauswahl zugeordnet sind.

Verwalten von Amazon EC2 Instances

AWSAWS Explorer bietet eine detaillierte Ansicht von Amazon Machine Images (AMI) und Amazon Elastic Compute Cloud (Amazon EC2) -Instances. Innerhalb der Visual Studio-Entwicklungsumgebung können Sie in diesen Ansichten eine Amazon EC2 Instance von einem

AMI starten, eine Verbindung zu dieser Instance herstellen und die Instance entweder stoppen oder beenden. Sie können die Instances-Ansicht verwenden, um aus Ihren Instances AMIs zu erstellen. Weitere Informationen finden Sie unter Create an AMI from an Amazon EC2 Instance.

Die Ansichten für Amazon Machine Images und Amazon EC2 Instances

AusAWSSie können im Explorer Ansichten von Amazon Machine Images (AMIs) und Amazon EC2 Instances anzeigen lassen. In :AWSExplorer, erweitern Sie dasAmazon EC2-Knoten.

Um die AMIs-Ansicht anzuzeigen, öffnen Sie im ersten AMIs-Subknoten das Kontextmenü (Rechtsklick) und wählen dann View (Anzeigen).

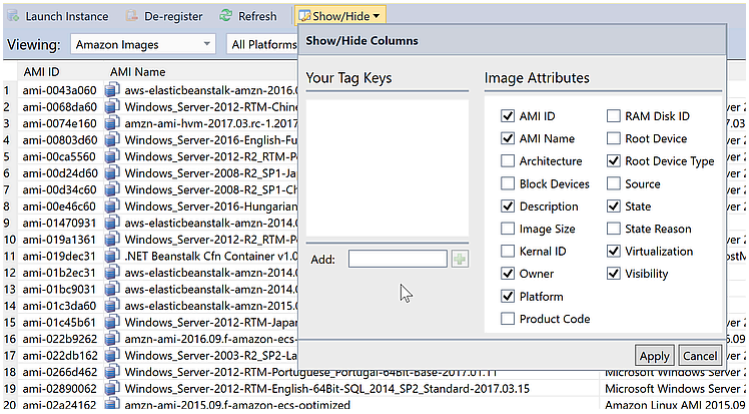
Um die Amazon EC2 Instances-Ansicht anzuzeigen, öffnen Sie im Instances-Knoten das Kontextmenü (Rechtsklick) und wählen dann View (Anzeigen).

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

- Die Ansichten sind auf die in angegebene Region ausgerichtetAWSExplorer (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. Die erste Ansicht zeigt AMIs aller Plattformtypen an (Windows oder Linux), die dem unterAWSExplorer.

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

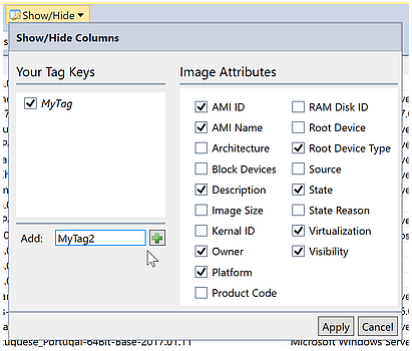
Markieren von AMIs, Instances und Volumes

Sie können auch die OptionShow/HideDropdown-Liste für das Hinzufügen von Tags für AMIs, Amazon EC2 Instances oder Volumes, die Ihnen gehören. Tags sind Name-Wert-Paare, mit denen Sie Ihren AMIs, Instances und Volumes Metadaten anfügen können. Tagnamen beziehen sich sowohl auf Ihr Konto als auch separat auf Ihre AMIs und Instances. Beispielsweise gibt es keinen Konflikt, wenn Sie denselben Tagnamen für Ihre AMIs und Ihre Instances verwenden. Bei den Tagnamen muss die Groß- und Kleinschreibung nicht berücksichtigt werden.

Weitere Informationen zu Tags erhalten Sie unterVerwenden von TagsimAmazon EC2-Benutzerhandbuch für Linux-Instancesaus.

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 einem AMI oder Amazon EC2 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 mindestens ein Wert mit dem Tag verknüpft ist, wird das Tag imAWS Management Consoleaus.

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 jedoch erhalten, gemeinsam mit allen Tagwerten, die mit AMIs, Instances oder Volumes verknüpft sind.

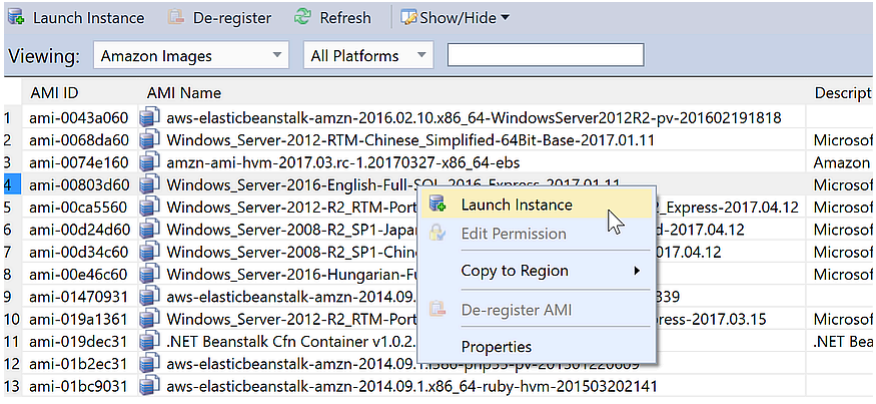
> **Note**
>
> Wenn Sie ein Tag imShow/HideDropdown-Liste, die keine zugeordneten Werte enthält,AWSToolkit löscht das Tag vollständig. Es wird dann nicht mehr in der Listenansicht und auch nicht mehr in der Dropdown-Liste Show/Hide (Einblenden/Ausblenden) angezeigt. Wenn Sie dieses Tag erneut nutzen möchten, verwenden Sie das Dialogfeld Show/Hide (Einblenden/Ausblenden), um es wieder zu erstellen.

Starten einer Amazon EC2 Instance

AWSDer Explorer bietet die Funktionalität, die für das Starten einer Amazon EC2 Instance erforderlich ist. In diesem Abschnitt wird ein Amazon Machine Image (AMI) ausgewählt, konfiguriert und dann als Amazon EC2 Instance gestartet.

So starten Sie eine Windows Server Amazon EC2 Instance

1. Wählen Sie oben in der AMIs-Ansicht aus der Dropdown-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 Launch New Amazon EC2 Instance (Neue Amazon EC2-Instance starten) das AMI für Ihre Anwendung.

   Instance-Typ

   Wählen Sie den Typ der zu startenden EC2 Instance aus. Eine Liste der Instance-Typen sowie Preisinformationen finden Sie auf der Seite EC2 Pricing.

   Name

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

   Schlüsselpaar

   Ein Schlüsselpaar wird verwendet, um das Windows-Passwort abzurufen, mit dem Sie sich über das Remote Desktop Protocol (RDP) bei der EC2 Instance 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 finden`%LOCALAPPDATA%\AWSToolkit\keypairs`(typischerweise: `C:\Users\<user>\AppData\Local\AWSToolkit\keypairs`) enthalten. Sie können das verschlüsselte key pair in eine`.pem`file.

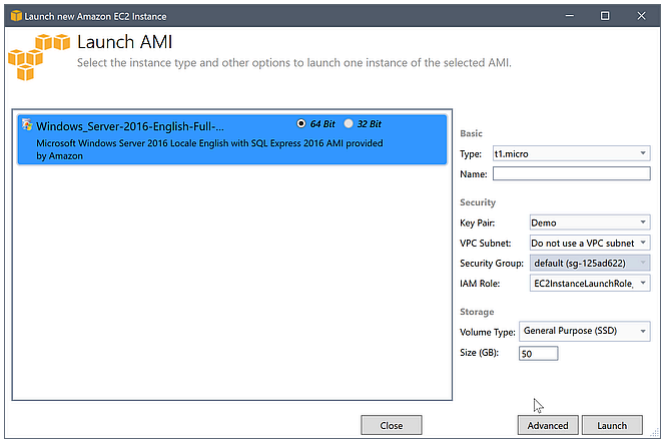
   a. In Visual Studio wählen SieAnzeigenKlicken Sie aufAWSExploreraus.
   b. Klicken Sie auf Amazon EC2 und wählen Sie Key Pairs (Schlüsselpaare).
   c. Die Schlüsselpaare werden aufgelistet, und die über das Toolkit erstellten/verwalteten Schüsselpaare werden als Stored in AWSToolkit (In AWSToolkit gespeichert) markiert.
   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 den Netzwerkverkehrstyp, den die EC2 Instance akzeptiert. Wählen Sie eine Sicherheitsgruppe aus, die eingehenden Datenverkehr auf Port 3389, dem von RDP verwendeten Port, zulässt, sodass Sie eine Verbindung zur EC2 Instance herstellen können. Weitere Informationen zur Verwendung des Toolkits für die Erstellung von Sicherheitsgruppen finden Sie unterVerwalten von SicherheitsgruppenAWSExploreraus.

Instance-Profil

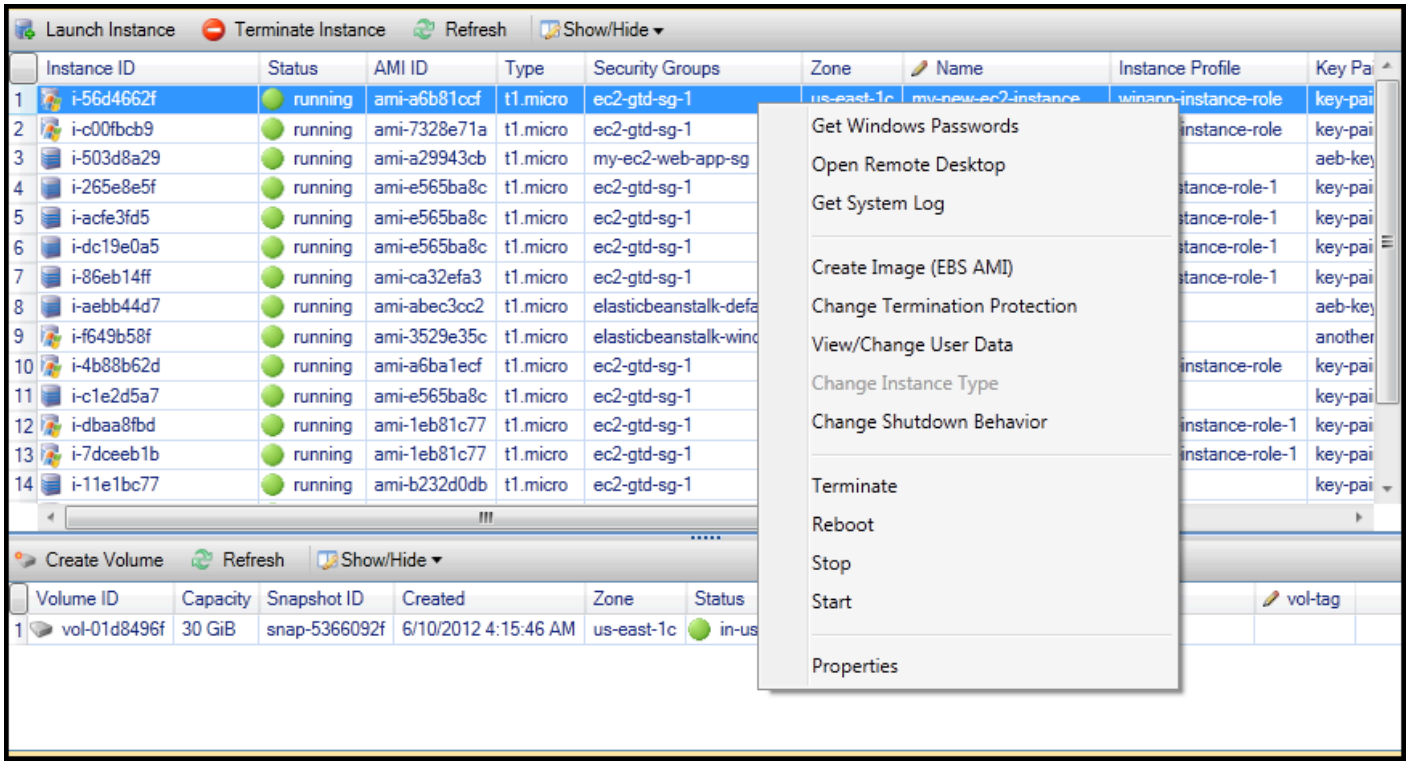
Das Instance-Profil ist ein logischer Container für eine IAM-Rolle. Wenn Sie ein Instance-Profil auswählen, ordnen Sie der EC2 Instance die entsprechende IAM-Rolle zu. IAM-Rollen werden anhand von Richtlinien konfiguriert, die den Zugriff auf Amazon Web Services und Kontoressourcen regeln. Wenn eine EC2 Instance einer IAM-Rolle zugeordnet ist, wird Anwendungssoftware, die auf der Instance ausgeführt wird, mit den durch die IAM-Rolle festgelegten Berechtigungen ausgeführt. Auf diese Weise kann Anwendungssoftware ausgeführt werden, ohne dassAWSIhre eigenen Anmeldeinformationen, die die Software sicherer machen. Weitere Informationen über IAM-Rollen finden Sie im IAM User Guide.



EC2-Dialogfeld Launch AMI (AMI starten)

4. Wählen Sie Launch (Starten) aus.

In :AWSExplorer, auf derInstancesUnterknoten vonAmazon EC2Öffnen Sie das Kontextmenü (rechte Maustaste) und wählen Sie dannAnzeigenaus. DieAWSDaraufhin zeigt das Toolkit die Liste der Amazon EC2 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.



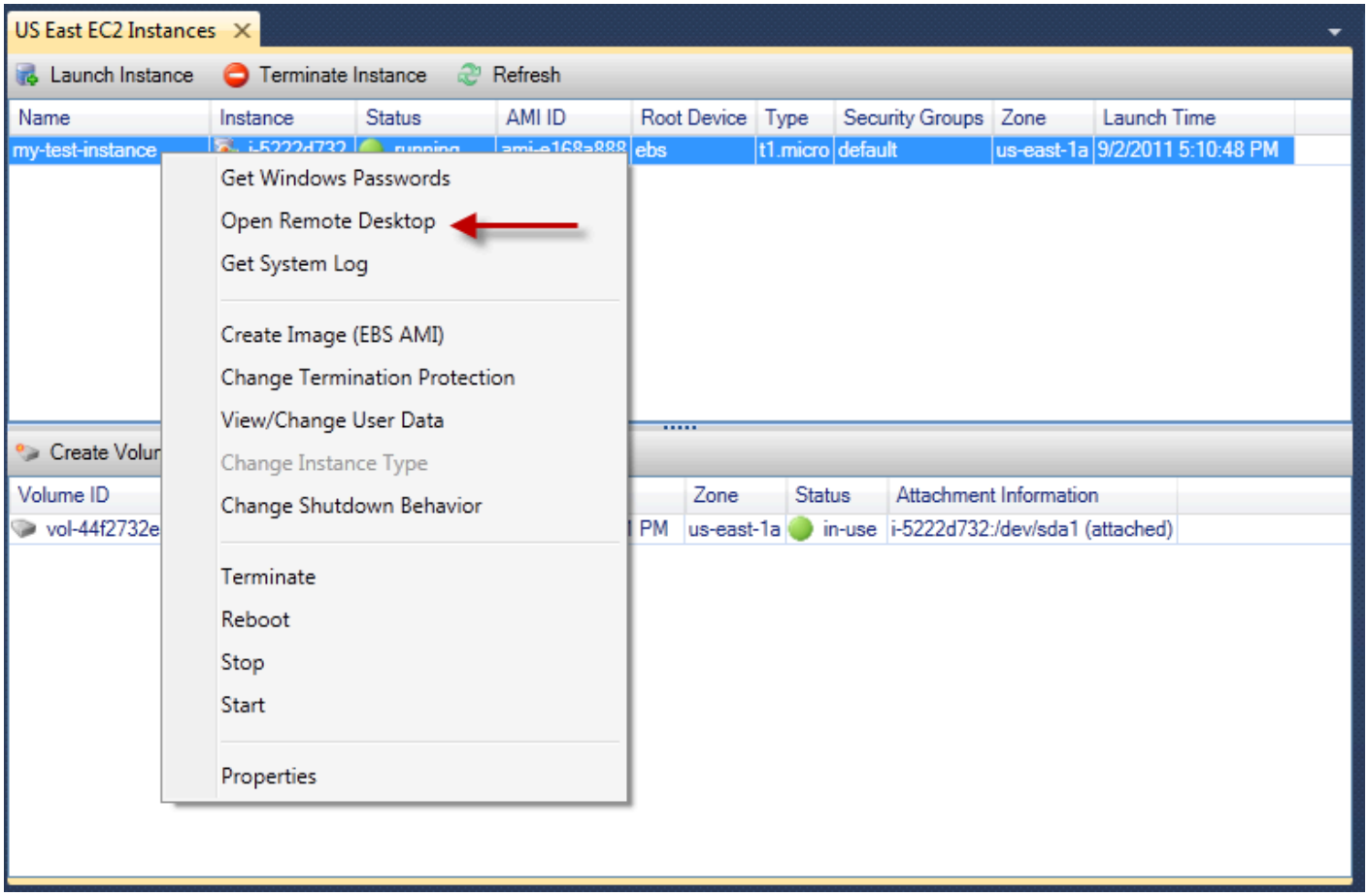
Herstellen einer Verbindung mit einer Amazon EC2 Instance

Sie können Windows Remote Desktop verwenden, um eine Verbindung mit einer Windows Server-Instance herzustellen. Zur Authentifizierung wird derAWSMit dem Toolkit haben Sie die Möglichkeit, das Administratorpasswort für die Instance abzurufen, oder Sie können einfach das mit der Instance verknüpfte, gespeicherte key pair verwenden. 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 Instance-Liste mit der rechten Maustaste auf die Windows Server-Instance, mit der Sie sich verbinden möchten. Wählen Sie aus dem Kontextmenü Open Remote Desktop (Remote Desktop öffnen).

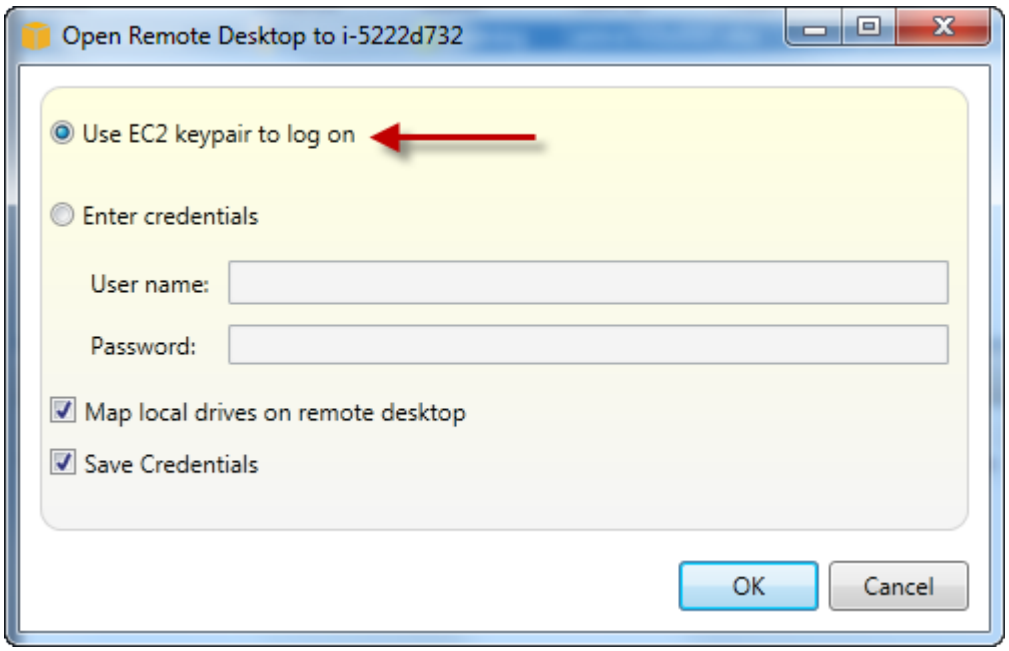
   Wenn Sie sich mit dem Administratorpasswort authentifizieren möchten, müssen Sie hierfür Get Windows Passwords (Windows-Passwörter abrufen) wählen.



EC2 Instance-Kontextmenü

2. Wählen Sie im Dialogfeld Open Remote Desktop (Remote Desktop öffnen) die Option Use EC2 keypair to log on (EC2-Schlüsselpaar für Anmeldung verwenden) und dann OK.

   Wenn Sie kein key pair mit demAWSGeben Sie Toolkit die PEM-Datei an, die den privaten Schlüssel enthält.

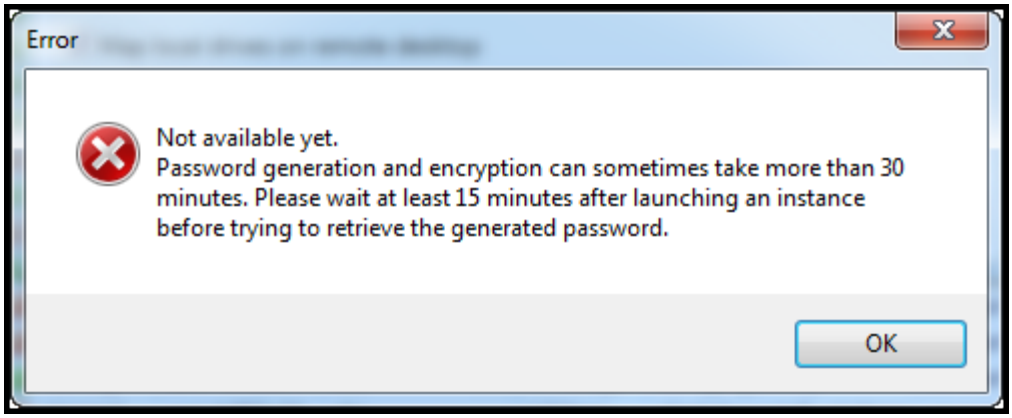


Dialogfeld "Open Remote Desktop (Remotedesktop öffnen)"

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

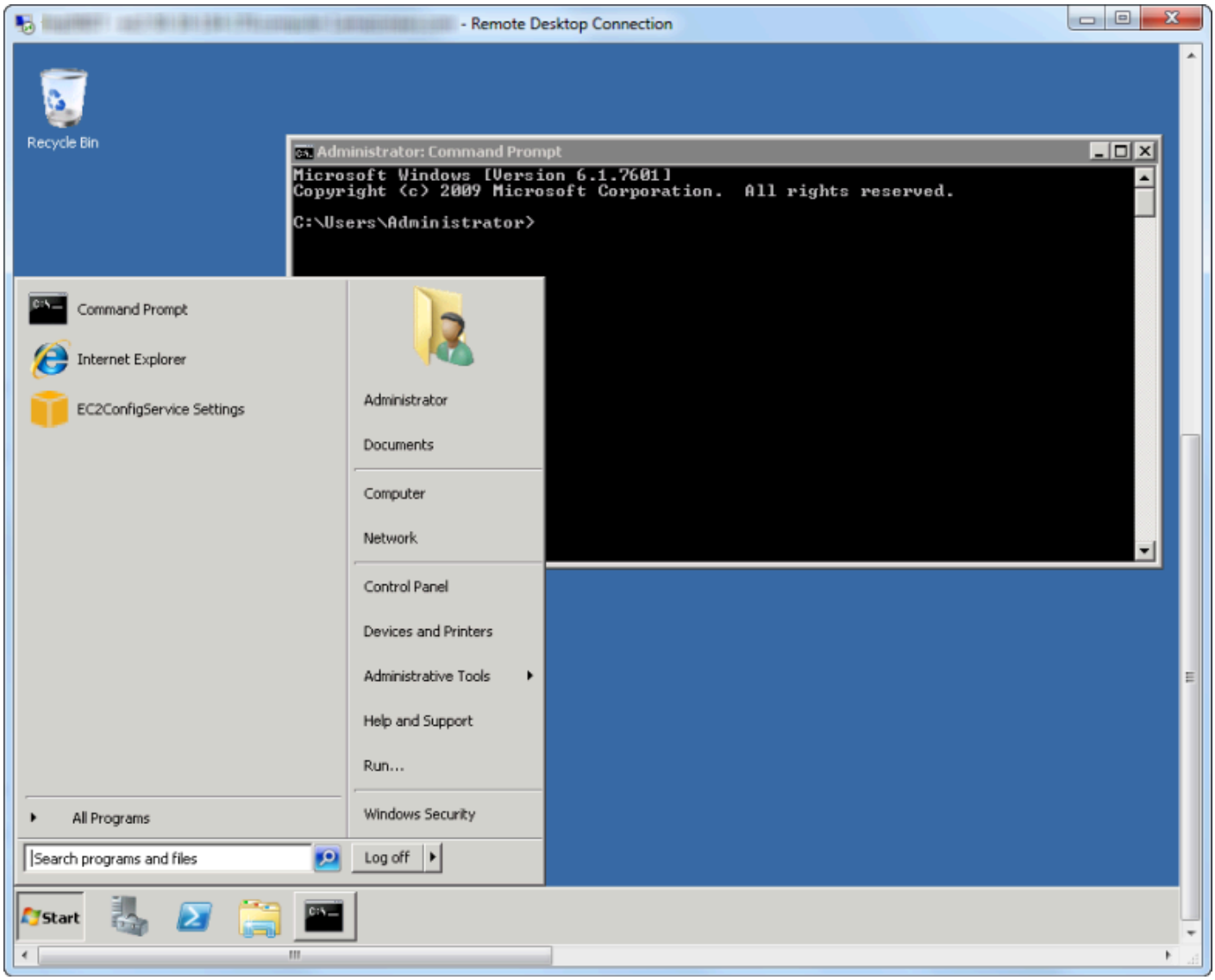
   Wenn nce erst kürzlich gestartet wurde und Sie keine Verbindung herstellen können, gibt es dafür zwei mögliche Ursachen:

   - 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 Amazon EC2 Instance.

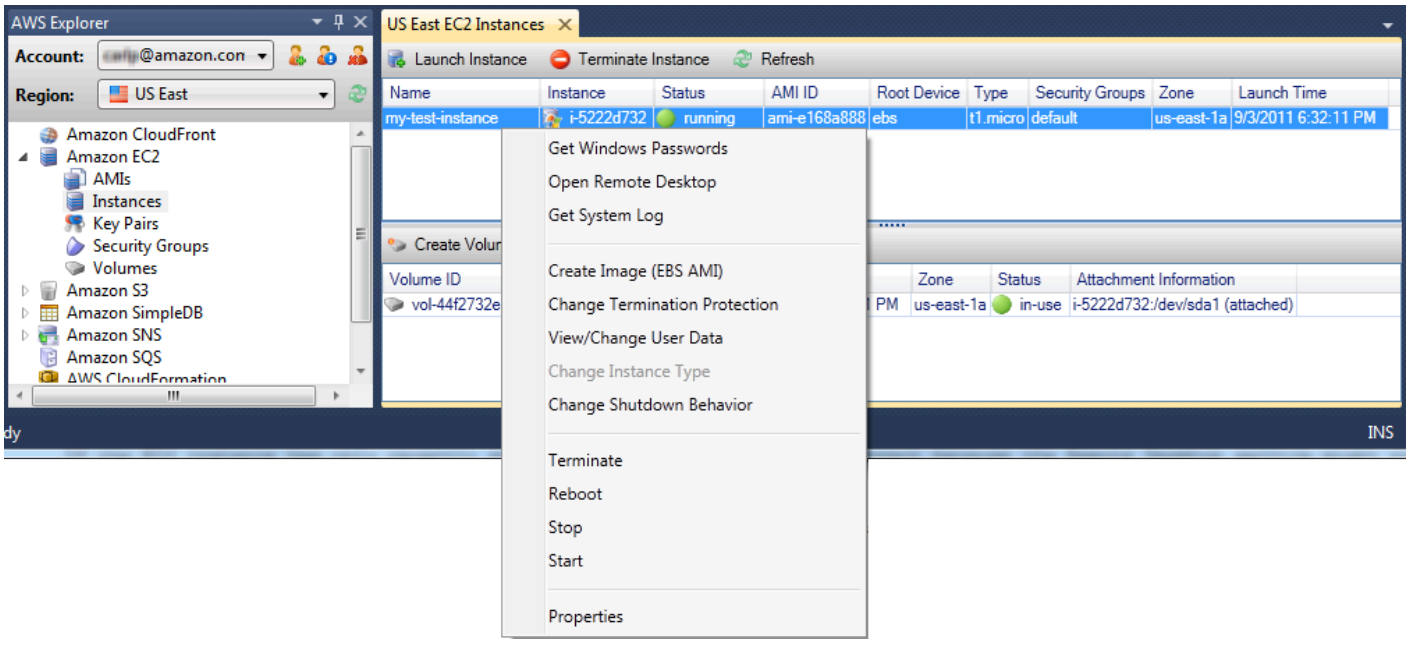
Verwendung derAWSSie können eine laufende Amazon EC2 Instance in Visual Studio stoppen oder beenden. Um die Instance beenden zu können, muss die EC2 Instance ein Amazon EBS -Volume verwenden. Wenn die EC2 Instance nicht mit einem Amazon EBS-Volume ausgeführt wird, steht Ihnen lediglich die Option zur Verfügung, 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 (Stoppen oder Beenden) wird Ihnen ab diesem Zeitpunkt keine Gebühren mehr für die EC2 Instance berechnet. Wenn Sie eine Instance stoppen, wird Ihnen jedoch weiterhin der EBS-Speicher in Rechnung gestellt, der nach dem Stoppen der Instance bestehen bleibt.

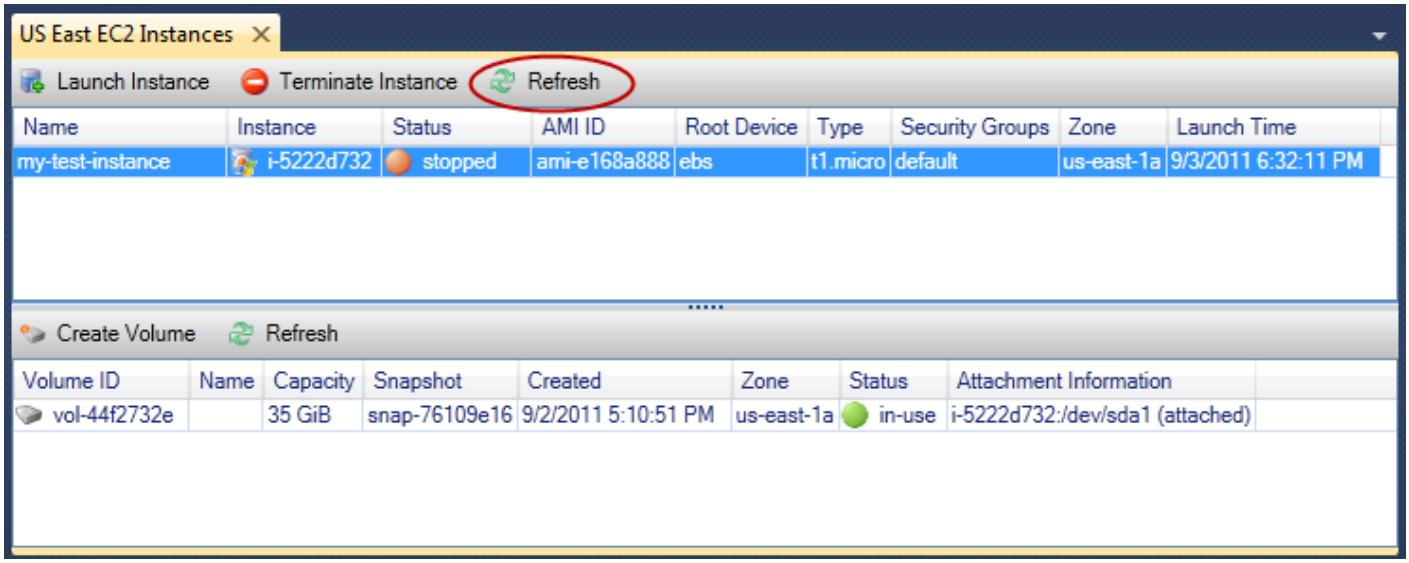
Eine weitere Möglichkeit zum Beenden einer Instanz besteht darin, mit Remote Desktop eine Verbindung mit der Instance herzustellen und dann aus dem Windows Start-Menü den Befehl Shutdown (Herunterfahren) zu verwenden. Sie können die Instance so konfigurieren, dass sie bei diesem Szenario entweder gestoppt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

So stoppen Sie eine Amazon EC2 Instance

1. In :AWSExplorer, erweitern Sie dasAmazon EC2Knoten, öffnen Sie das Kontextmenü (rechte Maustaste) fürInstancesKlicken Sie auf und danach aufAnzeigenaus. 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.

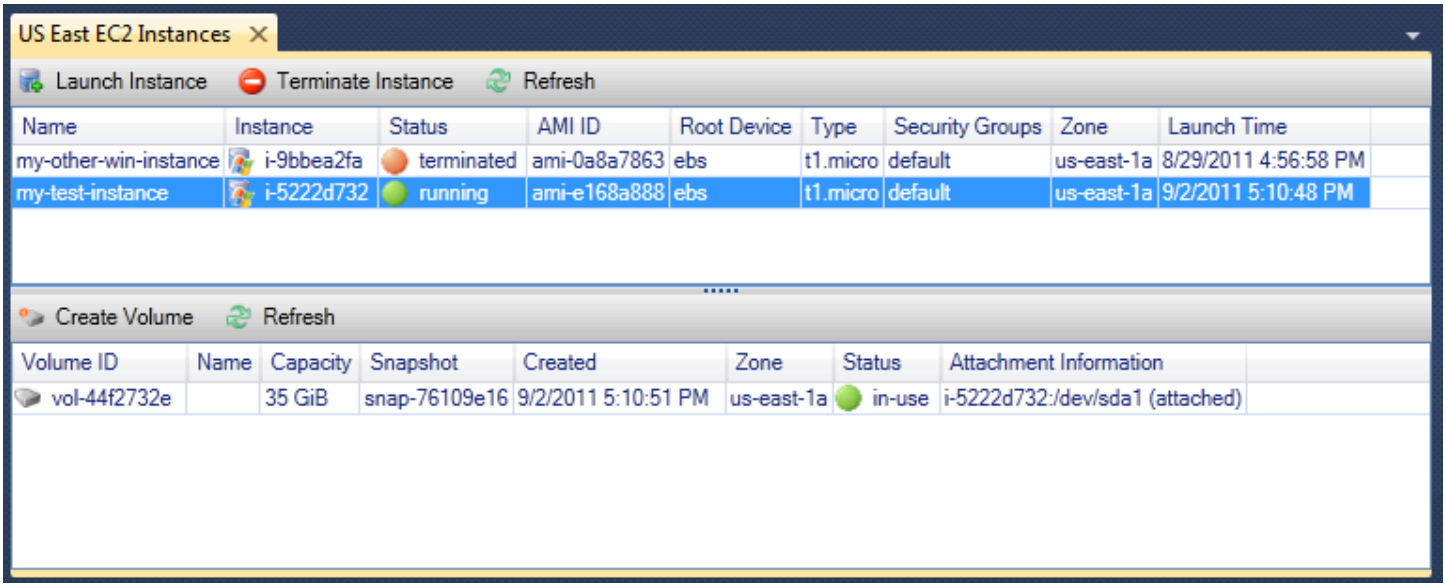


2. Wählen Sie oben in der Liste Instances die Option Refresh (Aktualisieren), damit die Statusänderung der Amazon EC2 instance angezeigt wird. Da die Instance eher gestoppt als beendet wurde, ist das mit der Instance verknüpfte EBS-Volume noch aktiv.



Beendete Instances bleiben sichtbar

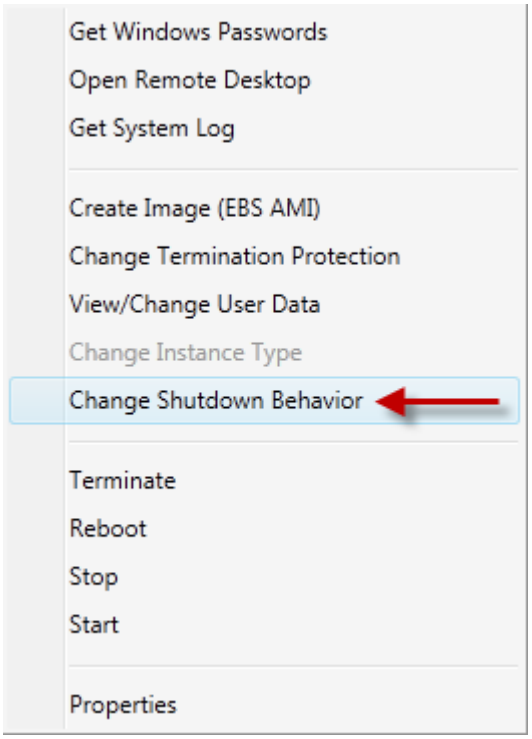
Wenn Sie eine Instance beenden, bleibt diese weiterhin in der Instance-Liste neben den laufenden oder gestoppten Instances sichtbar. IrgendwannAWSSie fordert diese Instances wieder zurück und sie verschwinden aus der Liste. Beendete Instances werden Ihnen nicht in Rechnung gestellt.



So legen Sie das Verhalten einer EC2 Instance beim Herunterfahren fest

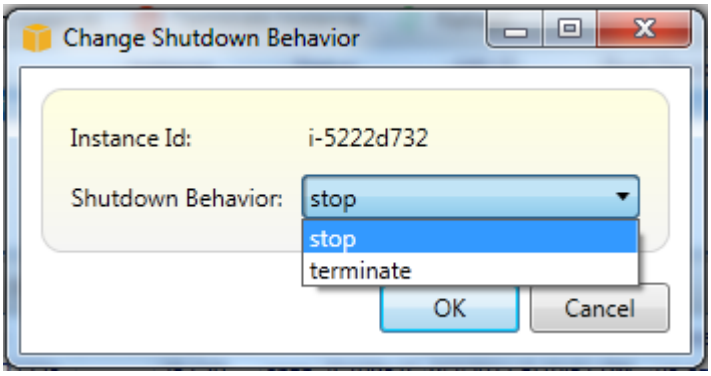
DieAWSMit dem Toolkit können Sie festlegen, ob eine Amazon EC2 Instance gestoppt oder beendet werden sollHerunterfahrenwird aus derstartenMenü.

1. Klicken Sie in der Liste Instances mit der rechten Maustaste auf eine Amazon EC2 Instance und wählen Sie dann Change shutdown behavior (Verhalten beim Herunterfahren 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

AWSDer Explorer bietet eine detaillierte Ansicht 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. In :AWSÖffnen Sie im Explorer das Kontextmenü (Rechtsklick) für den zu verwaltenden Cluster, und wählen Sie dannAnzeigenaus.
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 Edit (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. In :AWSÖffnen Sie im Explorer das Kontextmenü (Rechtsklick) für den Cluster, der zu beendende Aufgaben enthält, und wählen Sie dannAnzeigenaus.
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. In :AWSÖffnen Sie im Explorer das Kontextmenü (Rechtsklick) für den Cluster, der einen zu löschenden Service enthält, und wählen Sie dannAnzeigenaus.
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 die Option OK aus. Wenn der Cluster gelöscht wird, wird er aus demAWSExplorer.

Löschen eines Clusters

Sie können einen Amazon Elastic Container Service-Cluster löschenAWSExplorer.

Löschen eines Clusters

1. In :AWSÖffnen Sie im Explorer das Kontextmenü (rechte Maustaste) für den zu löschenden Cluster, den Sie löschen möchten, unter der-Cluster-Knoten vonAmazon ECSund wählen Sie dannLöschenaus.
2. Wählen Sie im Dialogfeld Delete Cluster die Option OK aus. Wenn der Cluster gelöscht wird, wird er aus demAWSExplorer.

Erstellen eines Repositorys

Sie können ein Amazon Elastic Container Registry-Repository erstellenAWSExplorer.

So erstellen Sie ein Repository

1. In :AWSÖffnen Sie das Kontextmenü (Rechtsklick) desRepositorysKnoten unterAmazon ECSund wählen Sie dannErstellen eines Repositorysaus.
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 im Amazon Elastic Container Registry-Repository löschenAWSExplorer.

So löschen Sie ein Repository

1. In :AWSÖffnen Sie das Kontextmenü (Rechtsklick) desRepositorysKnoten unterAmazon ECSund wählen Sie dannLöschen des Repositorysaus.
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).

Verwalten von SicherheitsgruppenAWSExplorer

Mit dem Toolkit for Visual Studio können Sie Sicherheitsgruppen erstellen und konfigurieren, die mit Amazon Elastic Compute Cloud (Amazon EC2) Instances verwendet werden undAWS CloudFormationaus. Wenn Sie Amazon EC2 EC2-Instances starten oder eine Anwendung auf bereitstellenAWS CloudFormationangeben, geben Sie eine Sicherheitsgruppe an, die mit den Amazon EC2 Instances verknüpft werden soll. (Bereitstellung aufAWS CloudFormationerstellt Amazon EC2 EC2-Instances.)

Eine Sicherheitsgruppe ist wie eine Firewall für eingehenden Netzwerkverkehr. Mit der Sicherheitsgruppe wird angegeben, welche Netzwerkverkehrstypen auf einer Amazon EC2 EC2-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.

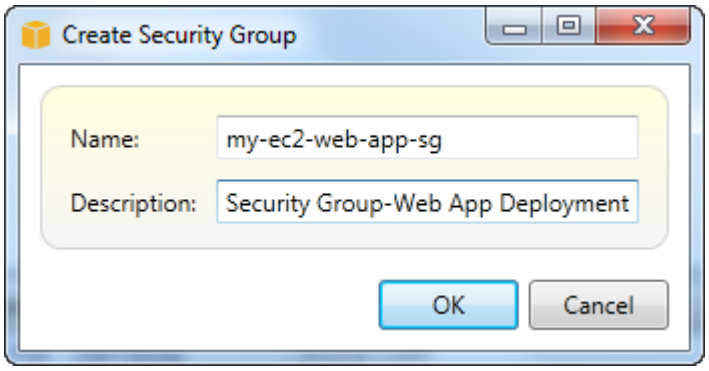
Erstellen einer Sicherheitsgruppe

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. In :AWSExplorer, unter demAmazon EC2-Knoten öffnen Sie das Kontextmenü (rechte Maustaste) imSicherheitsgruppen-Knoten, und wählen Sie dannAnzeigenaus.
2. Wählen Sie auf der Registerkarte EC2 Security Groups (EC2-Sicherheitsgruppen) die Option Create Security Group (Sicherheitsgruppe erstellen).

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.

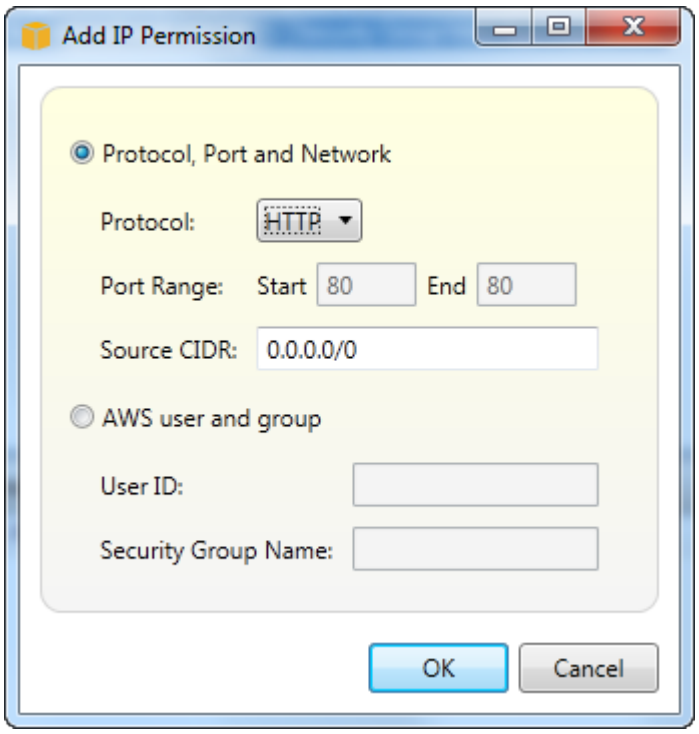


Hinzufügen von Berechtigungen zu einer Sicherheitsgruppe

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.

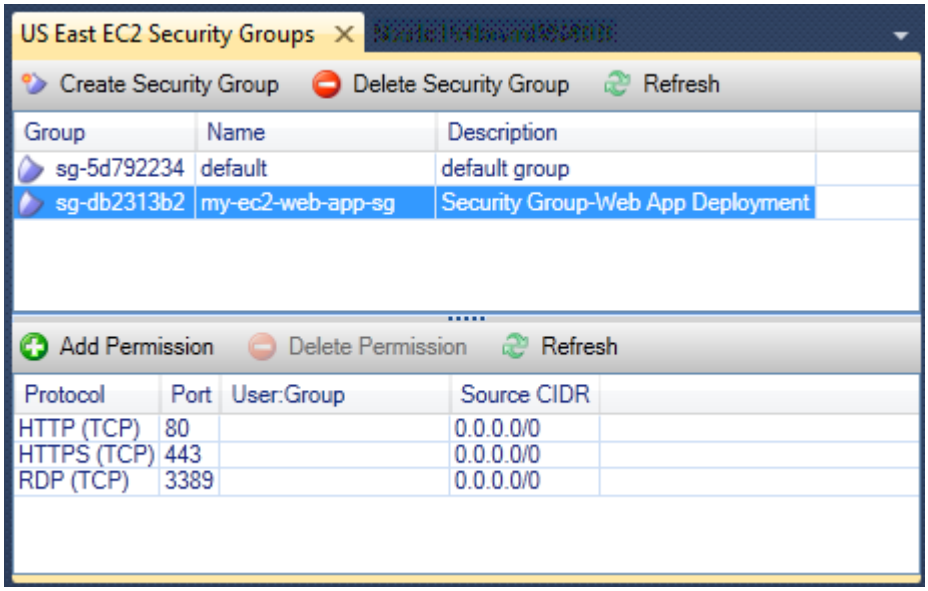
So fügen Sie einer Sicherheitsgruppe Berechtigungen hinzu

1. Wählen Sie auf der Registerkarte EC2 Security Groups (EC2-Sicherheitsgruppen) eine Sicherheitsgruppe aus und klicken Sie dann auf die Schaltfläche Add Permission (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. Klicken Sie auf OK.



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 Amazon EC2-Instances in dieser Sicherheitsgruppe eingehenden Netzwerkverkehr von Amazon EC2 Instances

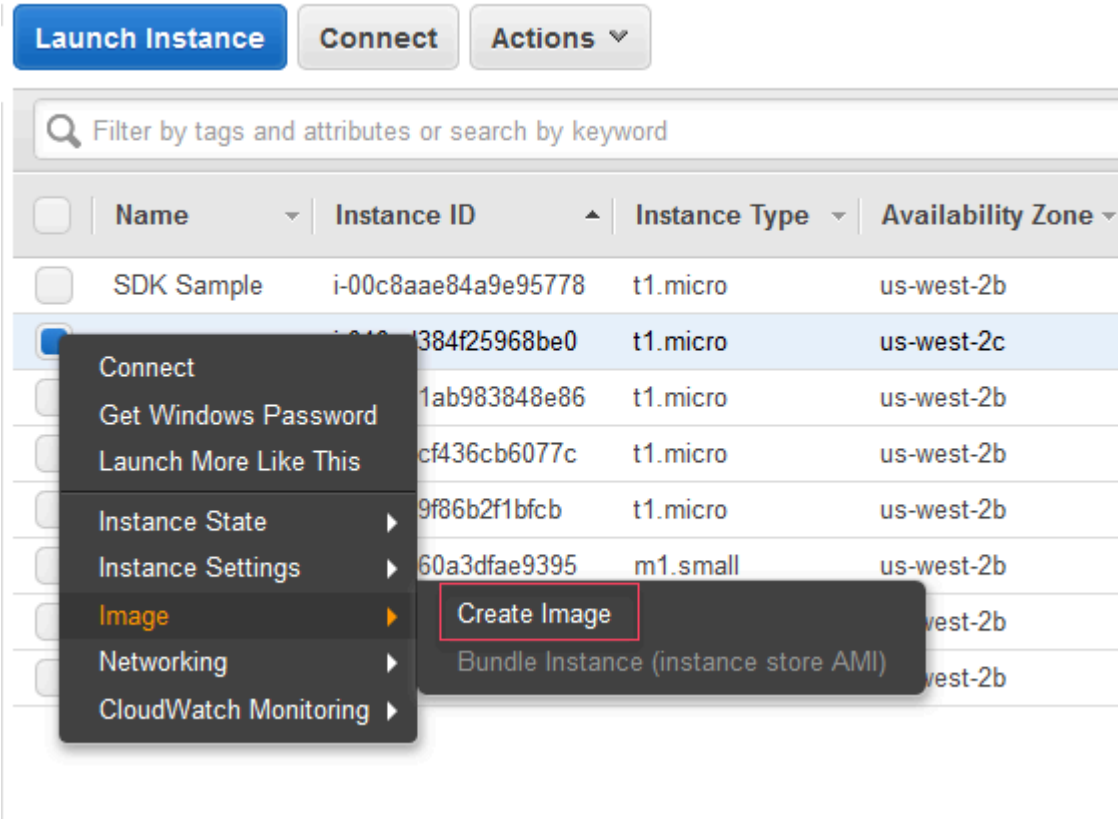
in der angegebenen Sicherheitsgruppe. Sie müssen auch die Benutzer-ID angeben, um den Sicherheitsgruppennamen eindeutig zu machen. Die Namen von Sicherheitsgruppen müssen nicht in allenAWSaus. Weitere Informationen zu Sicherheitsgruppen erhalten Sie unter EC2 documentation.

Erstellen eines AMI aus einer EC2 Instance

Sie können in der Amazon EC2 Instances (Amazon EC2-Instances)-Ansicht Amazon Machine Images (AMIs) aus laufenden oder gestoppten Instances erstellen. Weitere Informationen zu AMIs finden Sie unter dem Thema Amazon Machine Images (AMI) im Amazon Elastic Compute Cloud-Benutzerhandbuch für Windows-Instances.

So erstellen Sie ein AMI aus einer Instance:

1. Klicken Sie mit der rechten Maustaste auf die Instance, die Sie als Grundlage für ein AMI verwenden möchten, und wählen Sie Create Image (Image erstellen) aus dem Kontextmenü.

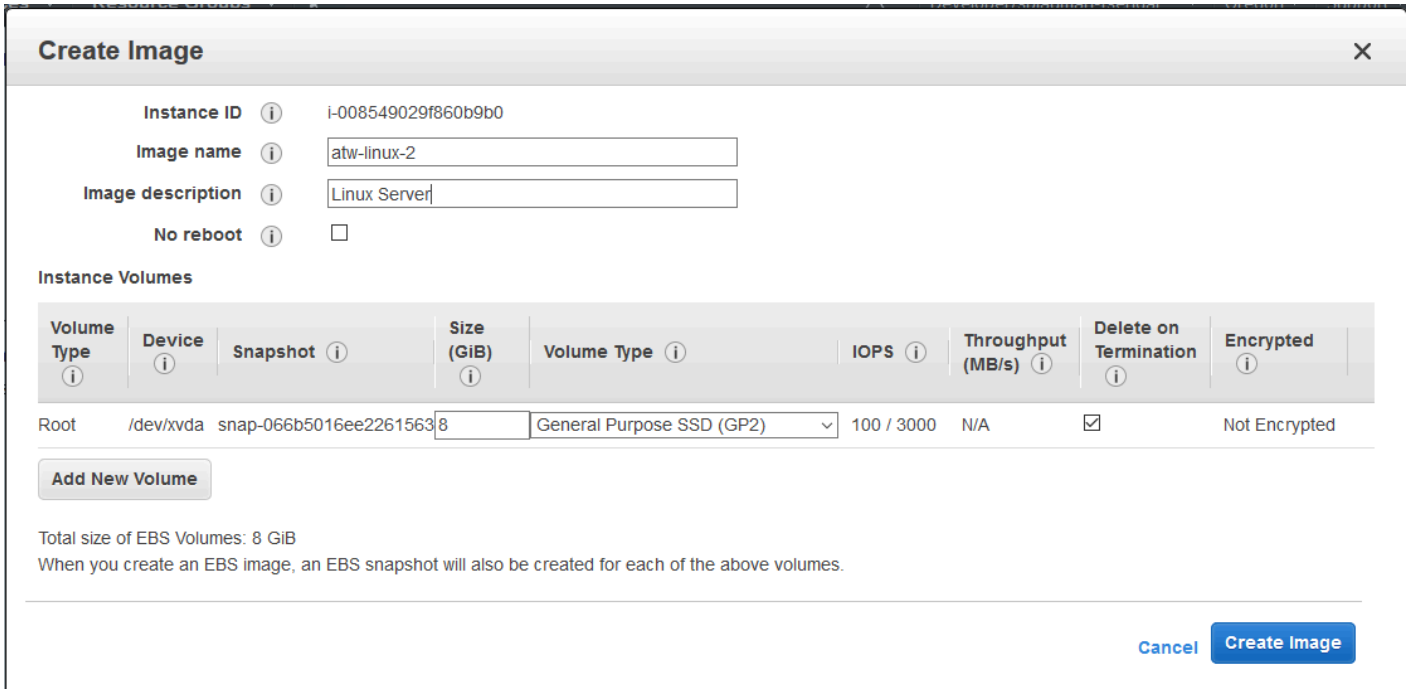


Kontextmenü Create Image (Image erstellen)

2. Geben Sie im Dialogfeld Create Image (Image erstellen) einen einzigartigen Namen und eine Beschreibung ein und wählen Sie dann Create Image (Image erstellen) aus. Standardmäßig fährt Amazon EC2 die Instance herunter, erstellt Snapshots von allen angefügten Volumes, erstellt und

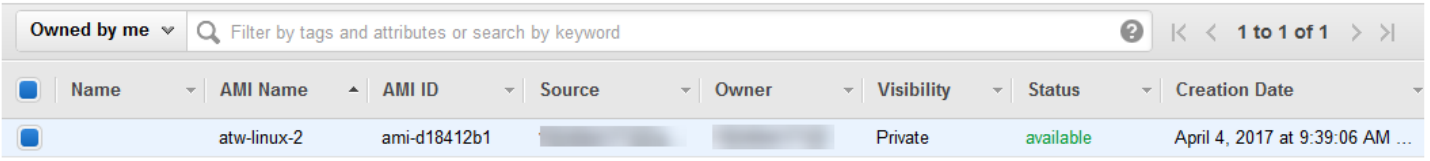
registriert das AMI und startet die Instance dann neu. Wählen Sie Kein Neustart, wenn Sie nicht möchten, dass Ihre Instance heruntergefahren wird.

> **Warning**
>
> Wenn Sie No reboot (Kein Neustart) wählen, können wir die Dateisystemintegrität des erstellten Abbilds nicht garantieren.



Dialogfeld Create Image (Image erstellen)

Es kann einige Minuten dauern, bis das AMI erstellt ist. Nachdem es erstellt wurde, wird es in der AMIs-Ansicht imAWS Explorer angezeigt. Um diese Ansicht anzuzeigen, doppelklicken Sie imAWS Explorer auf den Knoten Amazon EC2 | AMIs. Wählen Sie in der Dropdown-Liste Viewing (Anzeigen) die Option Owned By Me (In meinem Besitz) aus, um Ihre AMIs anzuzeigen. Möglicherweise müssen Sie die Schaltfläche Refresh (Aktualisieren) wählen, damit das AMI angezeigt wird. Wenn das AMI zum ersten Mal angezeigt wird, kann es sich noch kurze Zeit im ausstehenden Modus befinden. Nach ein paar Minuten wechselt es jedoch in einen verfügbaren Zustand.



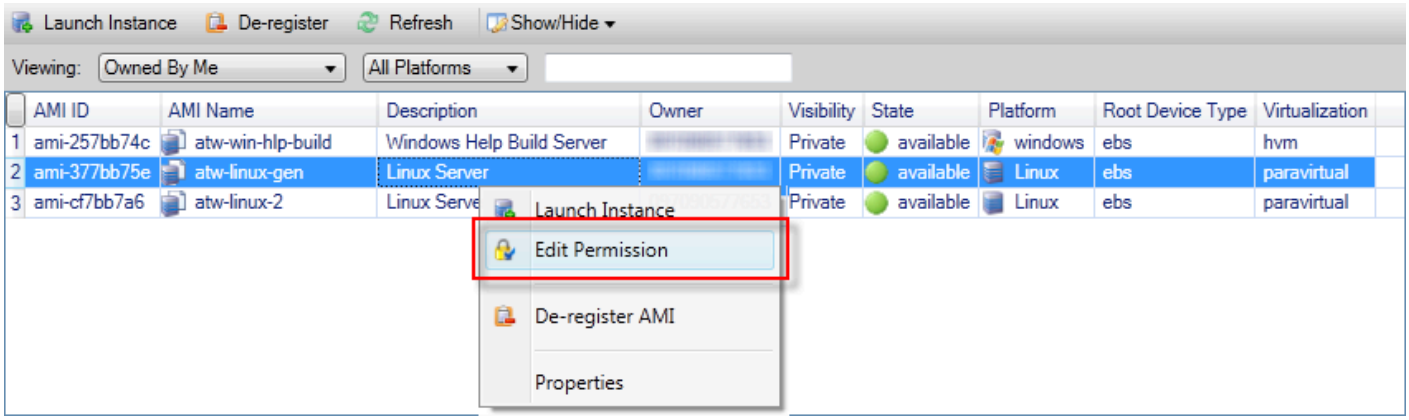
Liste der erstellten AMIs

Einrichten von Startberechtigungen für ein Amazon Machine Image

In der-AMIsAnzeigen von nAWS-Explorer. Sie können das Dialogfeld Set AMI Permissions (AMI-Berechtigungen festlegen) verwenden, um Berechtigungen von AMIs zu kopieren.

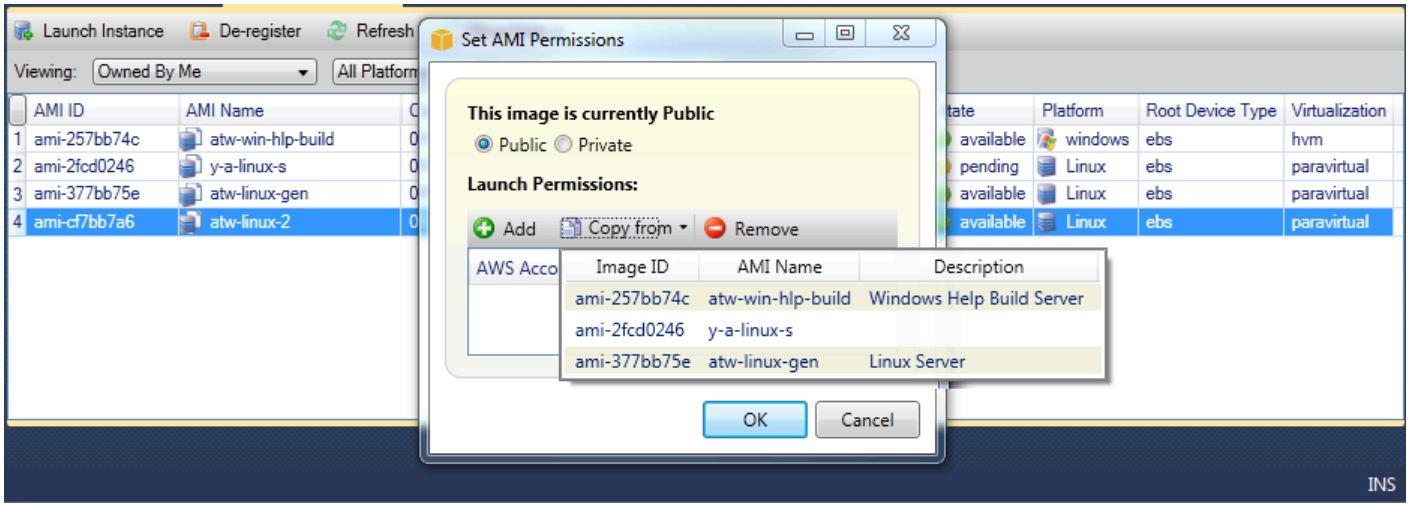
So richten Sie Berechtigungen für ein AMI ein:

1. In der-AMIsAnzeigen von nAWSÖffnen Sie im Explorer das Kontextmenü (Rechtsklick) für ein AMI und wählen dannBearbeiten von Berechtigungenaus.



2. Im Dialogfeld Set AMI Permissions (AMI-Berechtigungen festlegen) sind drei Optionen verfügbar:
   - Um Startgenehmigung zu erteilen, wählen SieAdd, und geben Sie die Kontonummer für dieAWSBenutzer, dem Sie die Startberechtigung erteilen.
   - Um einem der Startberechtigung wieder zu entziehen, wählen Sie dessen KontonummerAWSBenutzer, von dem Sie Startberechtigung entfernen, und wählenRemoveaus.
   - 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 Liste Copy-from (Kopieren von) wiederholen, um Berechtigungen von mehreren AMIs auf das Ziel-AMI zu kopieren.

DieCOPY ausDie Liste enthält nur die AMIs des Kontos, das zum Zeitpunkt des-AMIsAnsicht wurde vonAWS-Explorer. Folglich werden in der Liste Copy-from (Kopieren von) möglicherweise gar keine AMIs angezeigt, wenn das aktive Konto keine weiteren AMIs besitzt.



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 virtuellen Netzwerk starten, das Sie definiert haben. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur vonAWSaus. Weitere Informationen finden Sie im Amazon VPC-Benutzerhandbuch.

Das Toolkit for Visual Studio ermöglicht Entwicklern den Zugriff auf VPC-Funktionalität, die auch über dieAWS Management Consoleaber aus der Visual Studio-Entwicklungsumgebung. DieAmazon VPC-Knoten vonAWSDer Explorer umfasst Unterknoten für die folgenden Bereiche.

- VPCs
- Subnets
- Elastische IP-Adressen
- Internet-Gateways
- Netzwerk-ACLs
- Routing-Tabellen

- Sicherheitsgruppen

Erstellen einer öffentlichen-privaten VPC für die Bereitstellung mitAWS 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 Amazon EC2 EC2-Instance, die eine 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 minimal erforderliche VPC-Konfiguration für die Bereitstellung einer AWS Elastic Beanstalk-Umgebung in einer VPC. In diesem Szenario befinden sich die Amazon EC2 EC2-Instances, die Ihre Anwendung hosten, im privaten Subnetz. Der Load Balancer von Elastic Load Balancing, der den eingehenden Datenverkehr an Ihre Anwendung weiterleitet, befindet sich im öffentlichen Subnetz.

Weitere Informationen zur Network Address Translation (NAT) finden Sie unterNAT-InstancesimAmazon Virtual Private Cloud Cloud-Benutzerhandbuchaus. 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

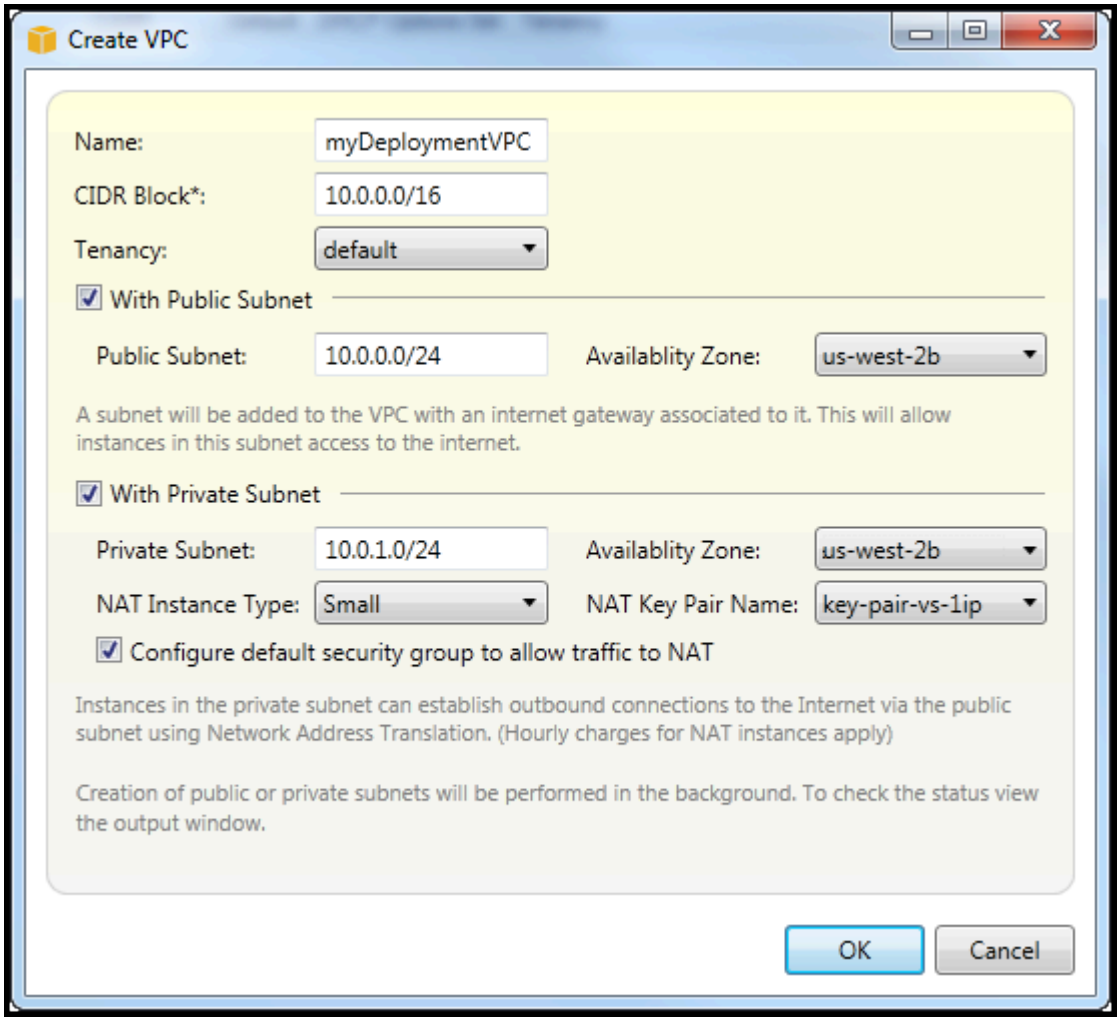
1. In derAmazon VPC-KnotenAWSExplorer, öffne dasVPCsUnterknoten und anschließend ausErstellen einer VPCaus.

2. Konfigurieren Sie die VPC wie folgt:

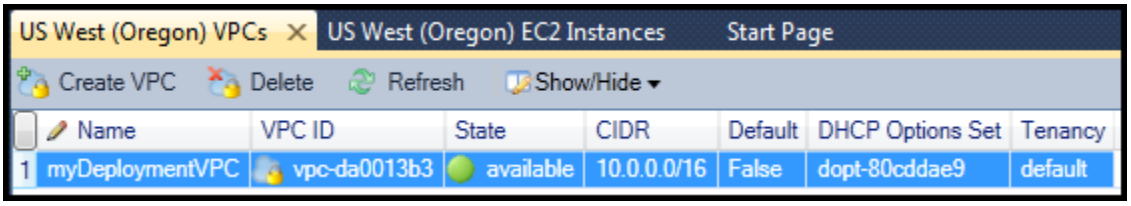
   - Geben Sie einen Namen für Ihre VPC ein.
   - Aktivieren Sie die Kontrollkästchen With Public Subnet (Mit öffentlichem Subnetz) und With Private Subnet (Mit privatem Subnetz).
   - Wählen Sie in der Dropdown-Liste Availability Zone für jedes Subnetz eine Availability Zone aus. Verwenden Sie unbedingt 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 Amazon EC2 EC2-Instance verwendet, die die Network Address Translation 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 Amazon EC2 EC2-Instance verwendet, die die Network Address Translation 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).

   Klicken Sie auf OK.

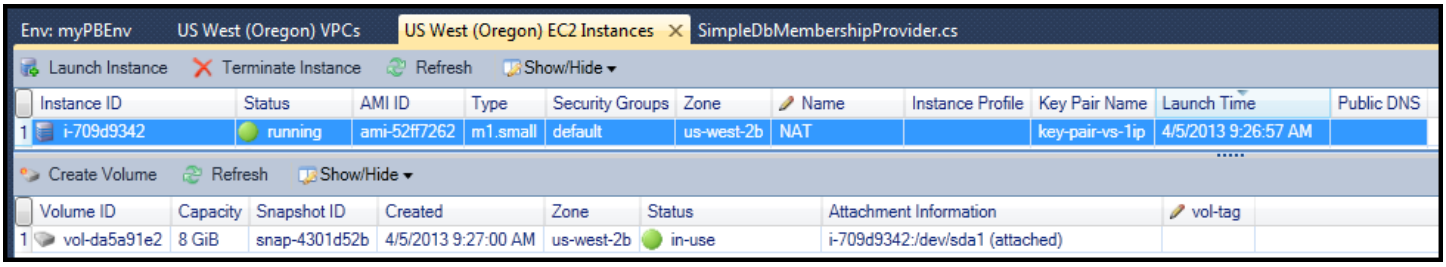


Sie können sich die neue VPC im.VPCsTabulator inAWS-Explorer.



Es dauert einen Moment, bis die NAT-Instance gestartet wird. Wenn es verfügbar ist, können Sie es anzeigen, indem Sie dieAmazon EC2-KnotenAWSExplorer und öffnen Sie dann denInstancesUnterknoten.

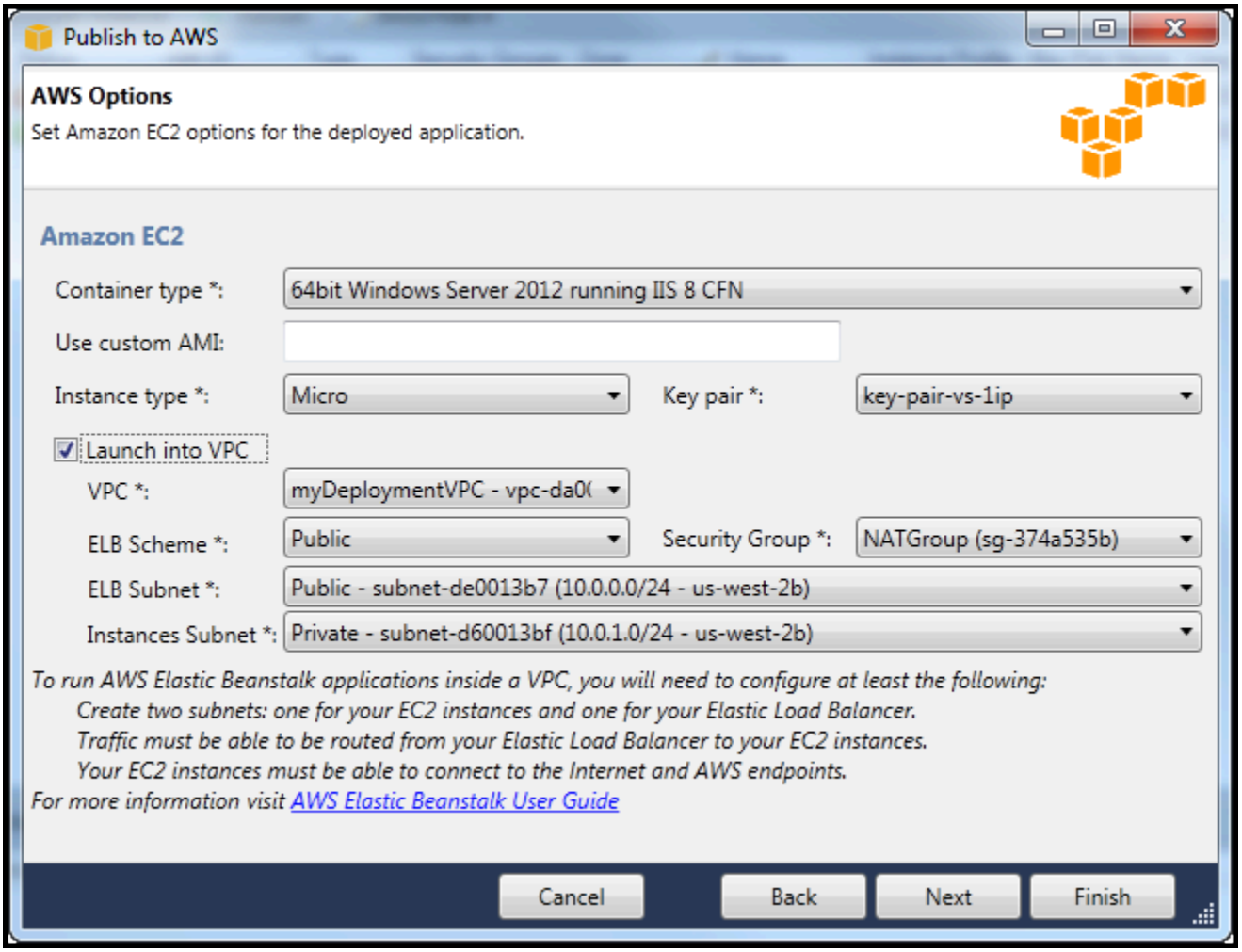
Importieren in &S3;AWS Elastic BeanstalkDas (Amazon EBS) -Volume wird automatisch für die NAT-Instance erstellt. Weitere Informationen über Elastic Beanstalk finden Sie unterAWS Elastic Beanstalk(EBS)imAmazon EC2-Benutzerhandbuch für Linux-Instancesaus.



Wenn SieBereitstellen einer Anwendung auf einerAWS Elastic BeanstalkUmweltund entscheiden Sie sich, die Umgebung in einer VPC zu starten, das Toolkit füllt diePublish to (Zu &CW; veröffentlichen)Amazon Web Services-Dialogfeld mit den Konfigurationsinformationen für Ihre VPC.

Das Toolkit füllt das Dialogfeld nur mit Informationen von VPCs aus, die im Toolkit erstellt wurden, nicht von VPCs, die mit derAWS Management Consoleaus. 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

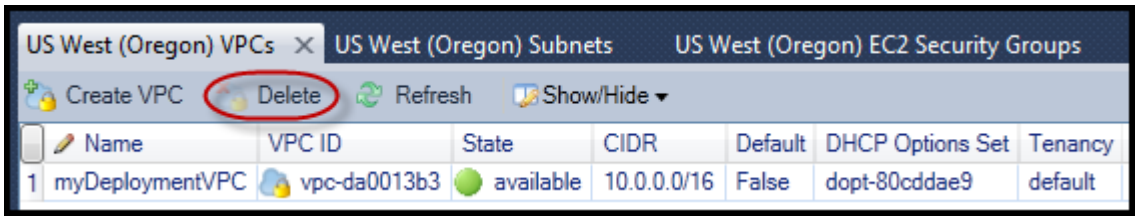
Zum Löschen der VPC müssen Sie zunächst alle Amazon EC2 EC2-Instances in der VPC beenden.

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

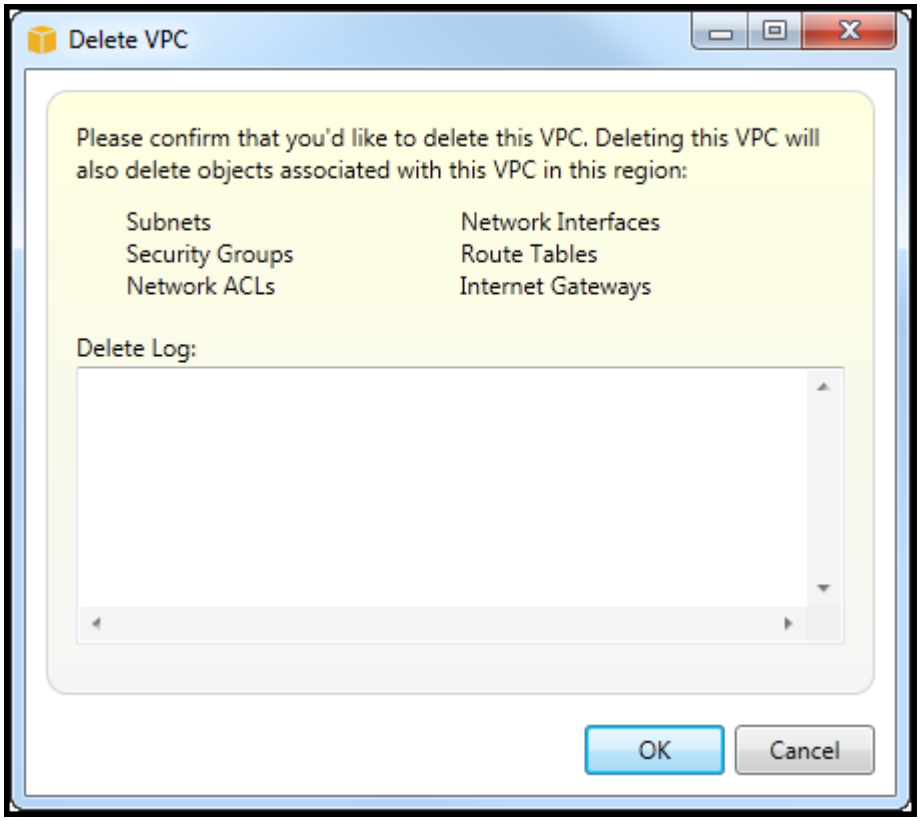
   Wenn Sie versuchen, die Instances, auf denen Ihre Anwendung gehostet wird, direkt zu beenden, ohne die Umgebung zu löschen, erstellt der Auto Scaling Scaling-Dienst automatisch neue Instances, um die gelöschten zu ersetzen. Weitere Informationen finden Sie im Auto Scaling Developer Guide.
2. Löschen 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 Vorlagen-Editors für Visual Studio

Das Toolkit for Visual Studio enthält 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 Stack oder einer Beispielvorlage kopiert) unter Verwendung des bereitgestellten 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 allgemeiner Aktionen für Ihre Vorlage von Visual Studio aus.

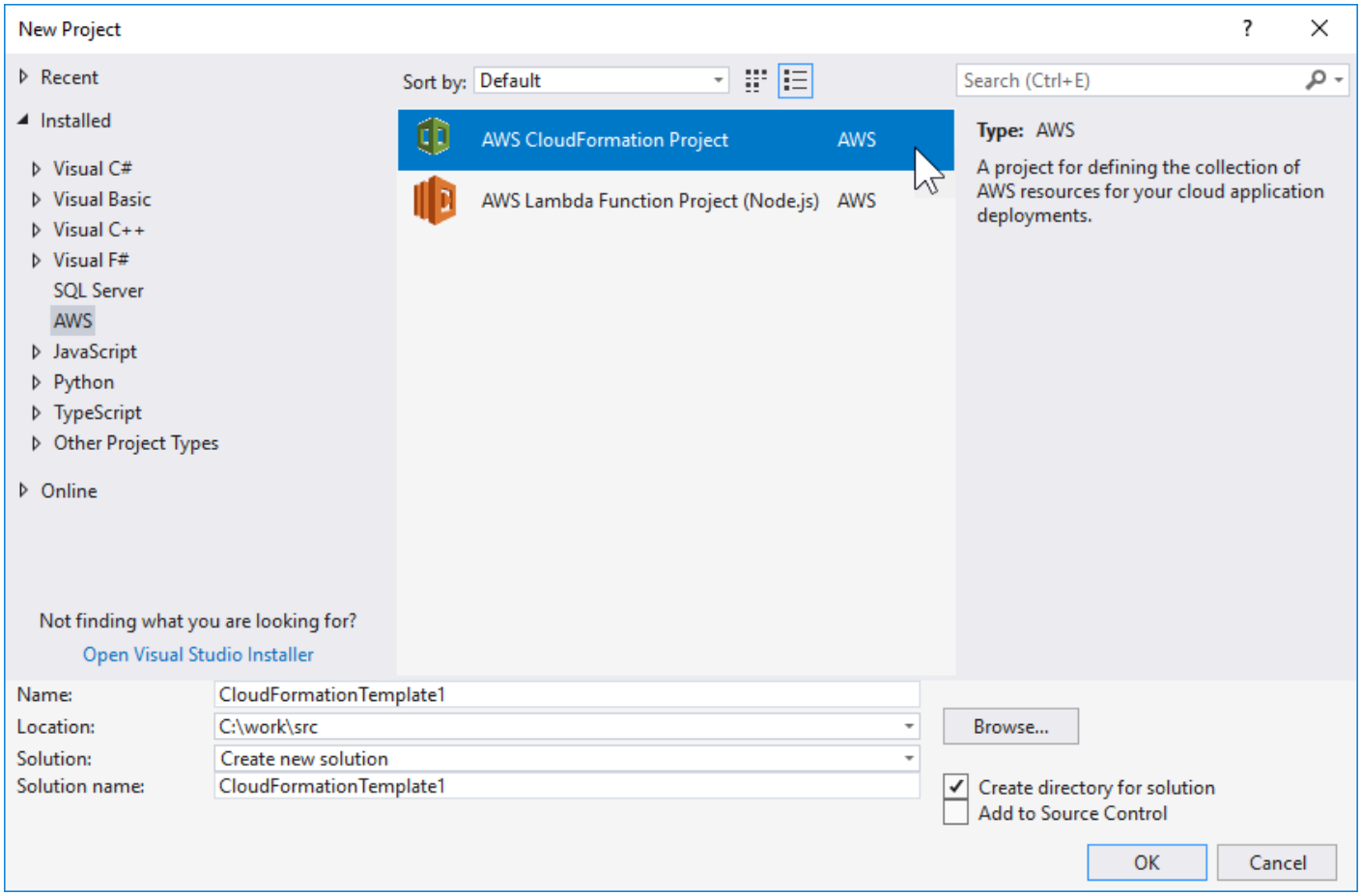
Themen

Erstellen eines AWS CloudFormation-Vorlagenprojekts in Visual Studio

So erstellen Sie ein Vorlageprojekt:

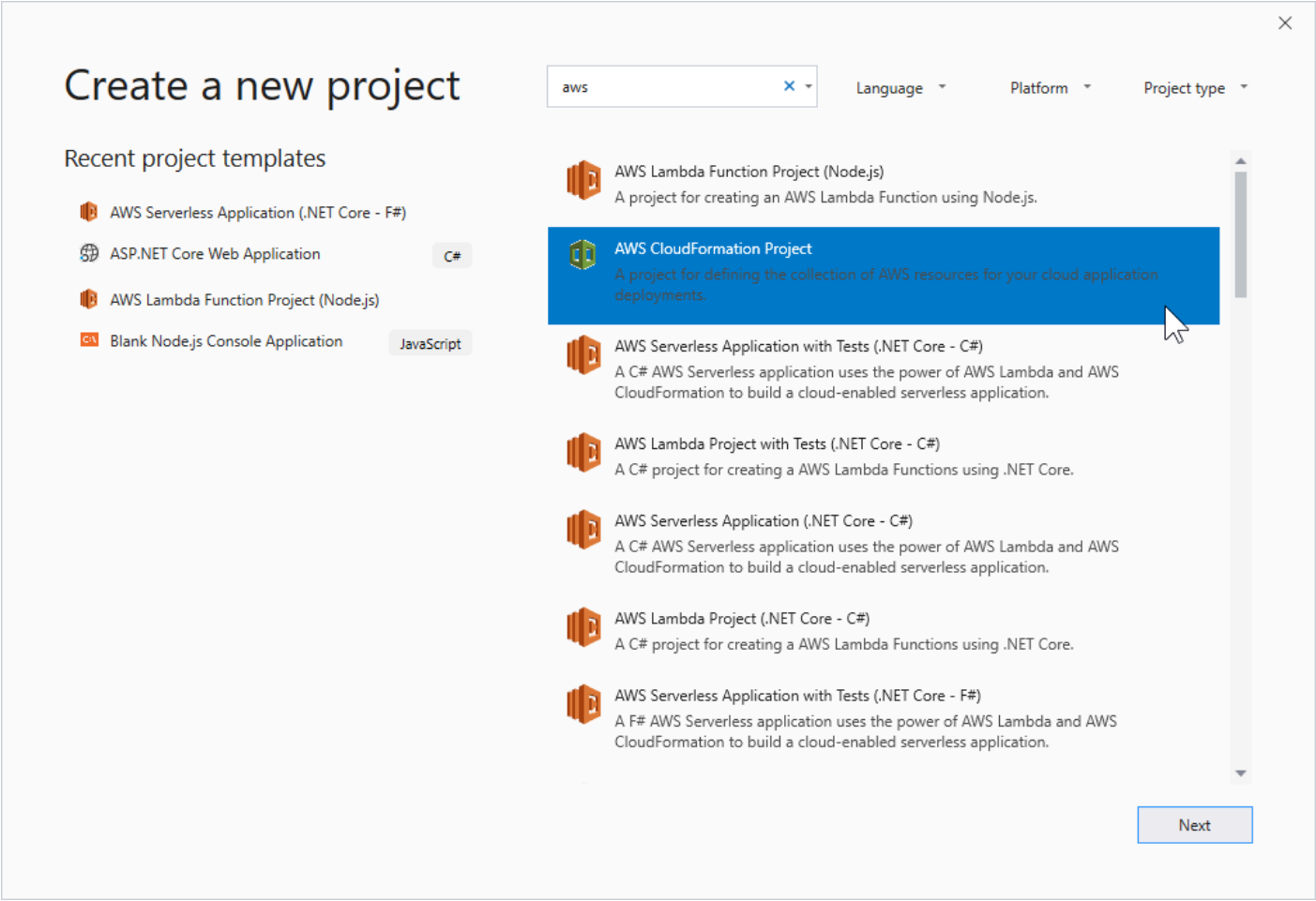
1. Wählen Sie in Visual Studio File (Datei), New (Neu) und dann Project (Projekt) aus.
2. Für Visual Studio 2017:

   In derNeues -Projekt-Dialogfeld erweiternInstalliertund wähleAWSaus.



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.



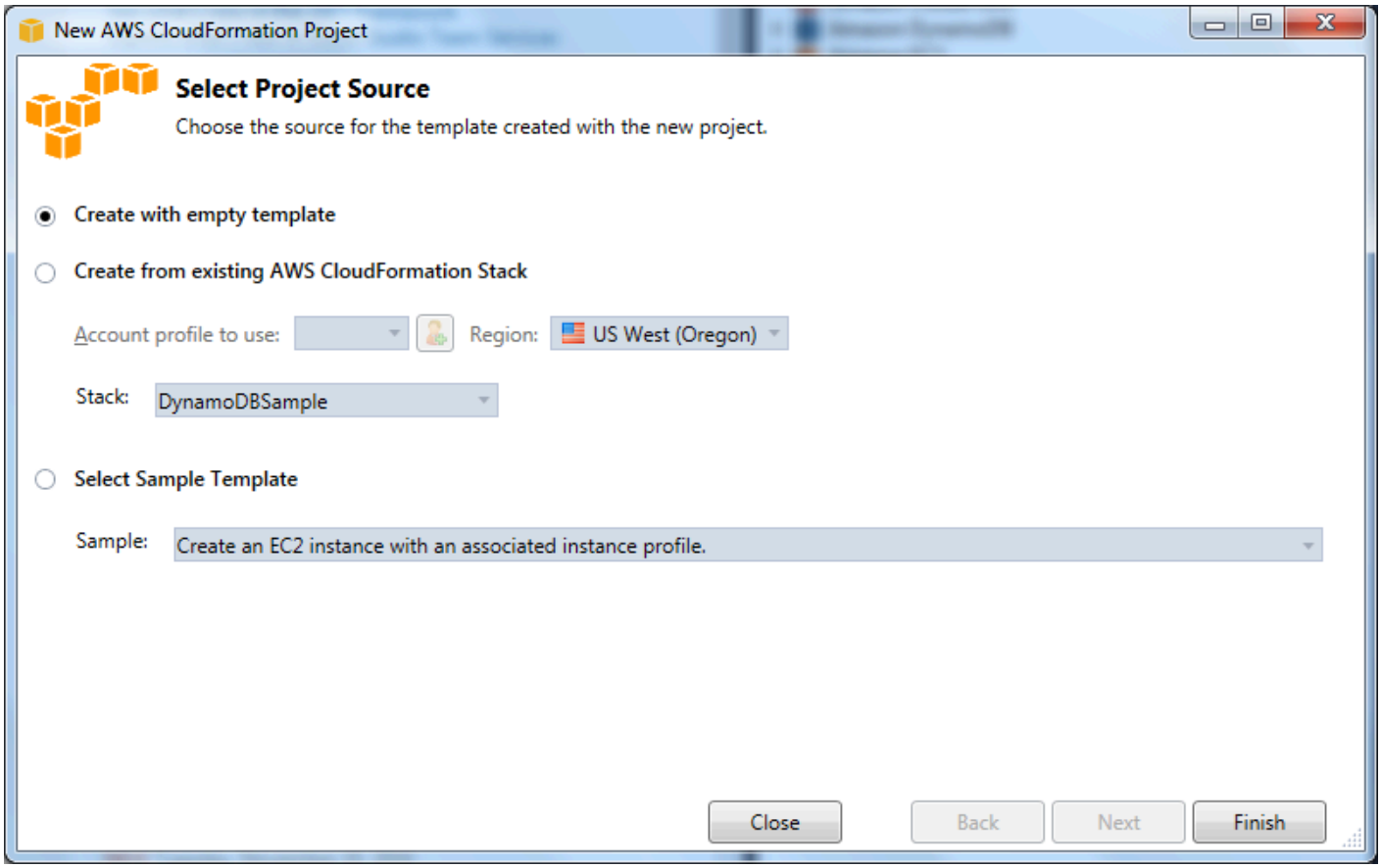
3. SelectAWSCloudFormation-Projekt-Vorlage.
4. Für Visual Studio 2017:

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

   Für Visual Studio 2019:

   Klicken Sie auf Next (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.
   - Mit Create from existingAWS|CFN| StapelGeneriert eine Vorlage aus einem vorhandenen Stack in IhremAWSKonto. (Der Stack muss nicht den Status `CREATE_COMPLETE` aufweisen.)

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

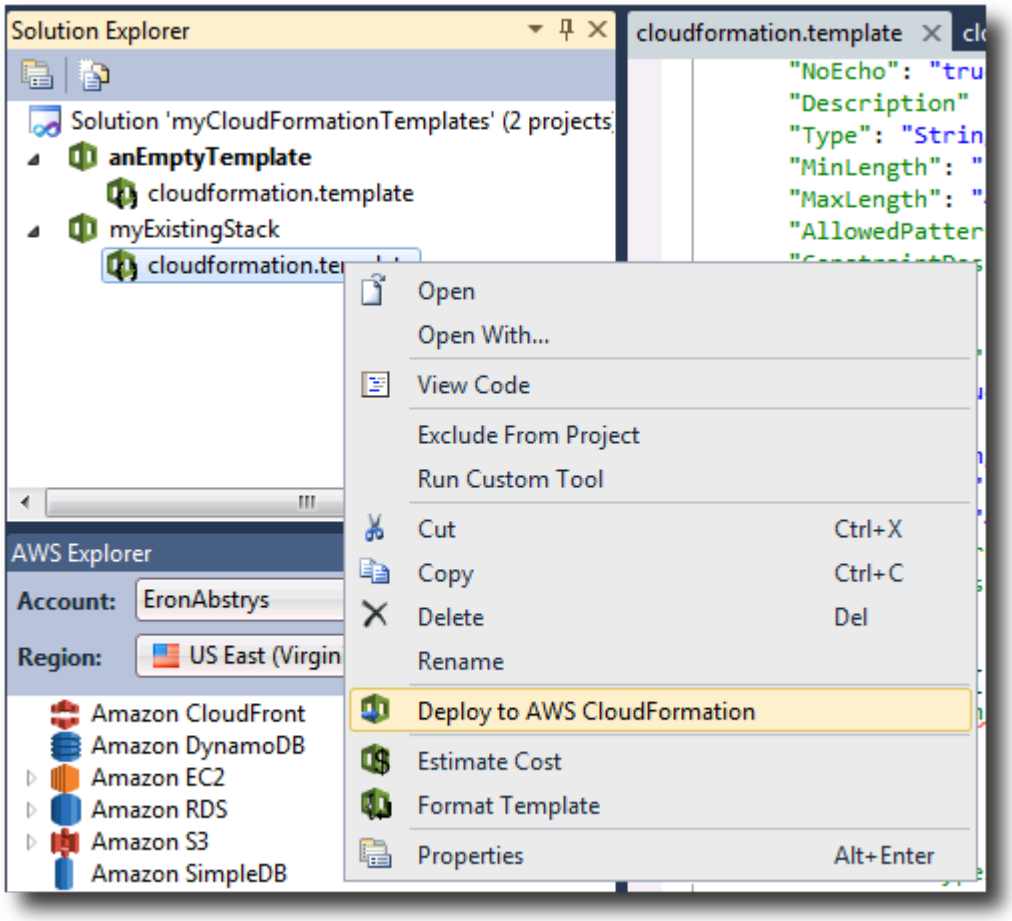


6. Klicken Sie auf AWS CloudFormationFinish (Abschließen), um die Erstellung des -Vorlageprojekts abzuschließen.

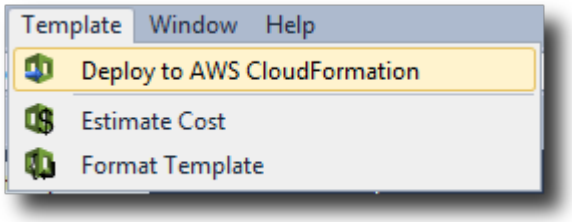
Bereitstellen einer AWS CloudFormation-Vorlage in Visual Studio

So stellen Sie eine CFN-Vorlage bereit

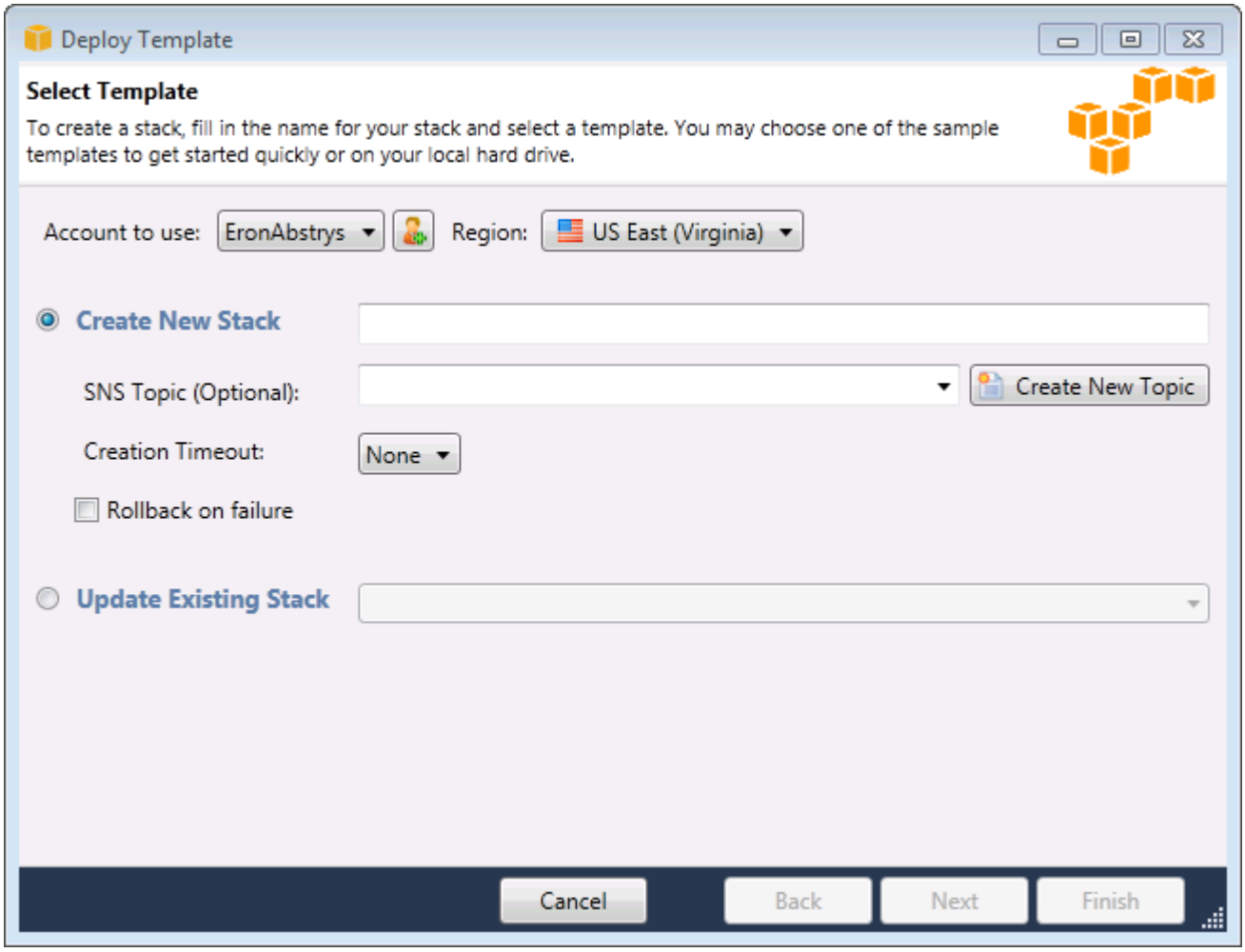
1. Öffnen Sie im Solution Explorer das Kontextmenü (rechte Maustaste) für die Vorlage, die Sie bereitstellen möchten, und wählen Sie die OptionBereitstellen inAWS CloudFormationaus.



Alternativ können Sie die derzeit bearbeitete Vorlage bereitstellen, indem Sie im-VorlageMenü, wählen SieBereitstellen inAWS CloudFormationaus.



2. Auf derVorlage bereitstellenWählen Sie dieAWS-Kontoum den Stack und die Region zu starten, 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 (Erstellungs-Timeout), um anzugeben, wie viel Zeit AWS CloudFormation für die Stack-Erstellung gewähren soll, bevor der Vorgang als fehlgeschlagen gilt (und rückgängig gemacht wird, sofern die Option Rollback on failure (Rollback bei Fehler) nicht aktiviert 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

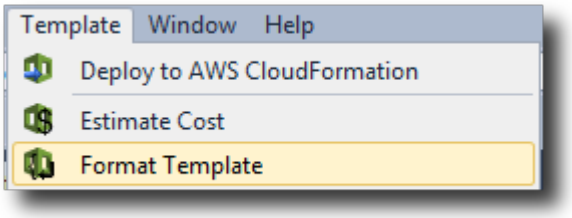
diese Option deaktiviert, wenn der Stack für Debugging-Zwecke aktiv bleiben soll, auch wenn er nicht vollständig gestartet wurde.

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

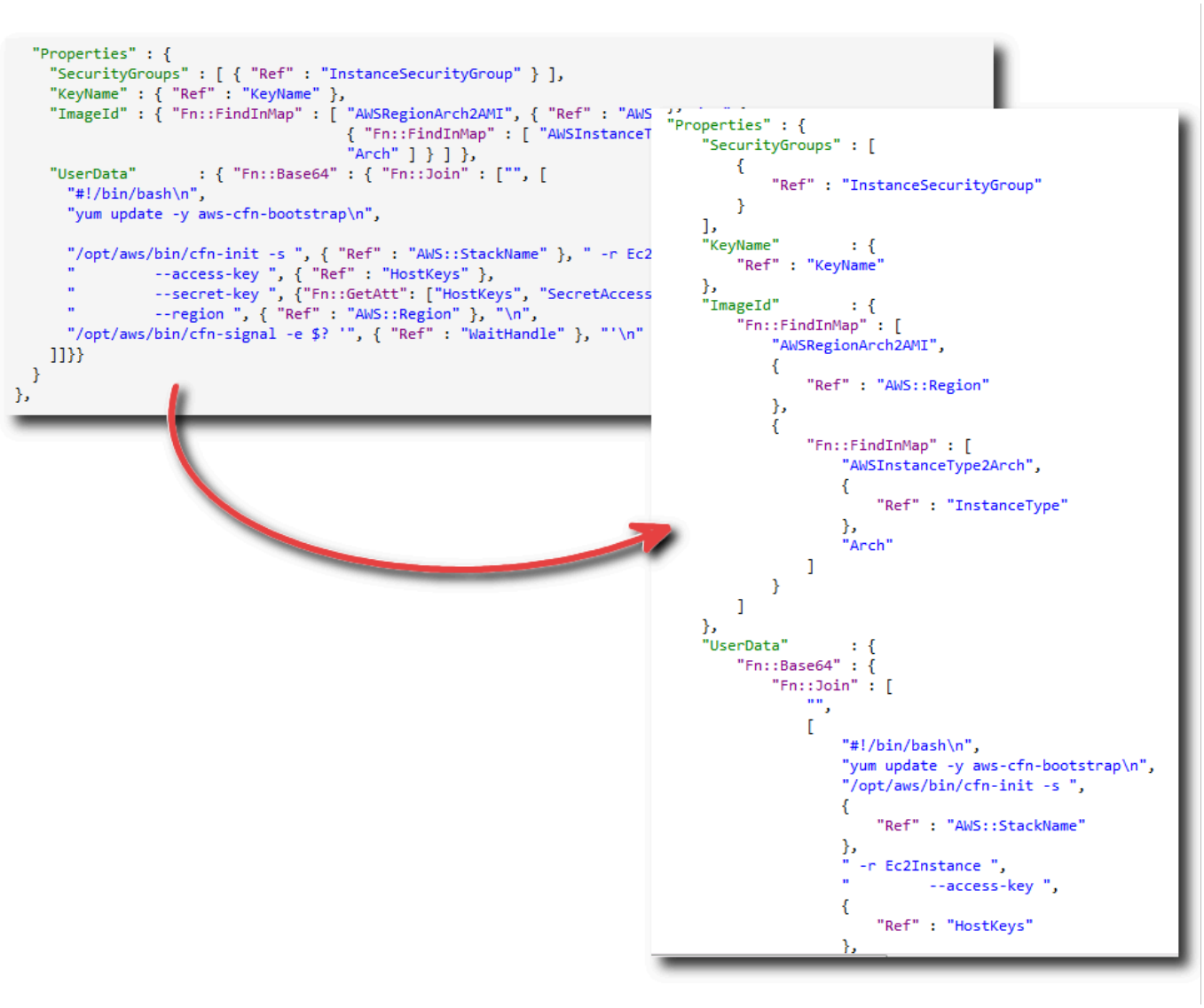
Formatieren einer AWS CloudFormation-Vorlage in Visual Studio

- 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.



Verwenden von Amazon S3AWSExplorer

Mit Amazon Simple Storage Service (Amazon S3) können Sie Daten über jede Internetverbindung speichern und abrufen. Alle in Amazon S3 gespeicherten Daten sind mit Ihrem Konto verknüpft und standardmäßig nur für Sie zugänglich. Mit dem Toolkit for Visual Studio können Sie Daten in Amazon S3 speichern sowie anzeigen, verwalten, abrufen und verteilen.

Amazon S3 verwendet das Konzept von Buckets, die Sie sich als Dateisysteme oder logische Laufwerke vorstellen können. Buckets können Ordner enthalten, ähnlich Verzeichnissen, und Objekte, ähnlich Dateien. In diesem Abschnitt verwenden wir diese Konzepte beim Durchgehen der vom Toolkit for Visual Studio bereitgestellten Amazon S3-Funktionen.

> **Note**
>
> Zum verwenden dieses Tools muss Ihre IAM-Richtlinie Berechtigungen für dies`s3:GetBucketAcl`,`s3:GetBucket`, und`s3:ListBucket`Aktionen. Weitere Informationen finden Sie unterÜbersicht überAWSIAM-Richtlinienaus.

Erstellen eines Amazon-S3-Buckets

Der Bucket ist die grundlegende Speichereinheit in Amazon S3.

So erstellen Sie einen S3-Bucket

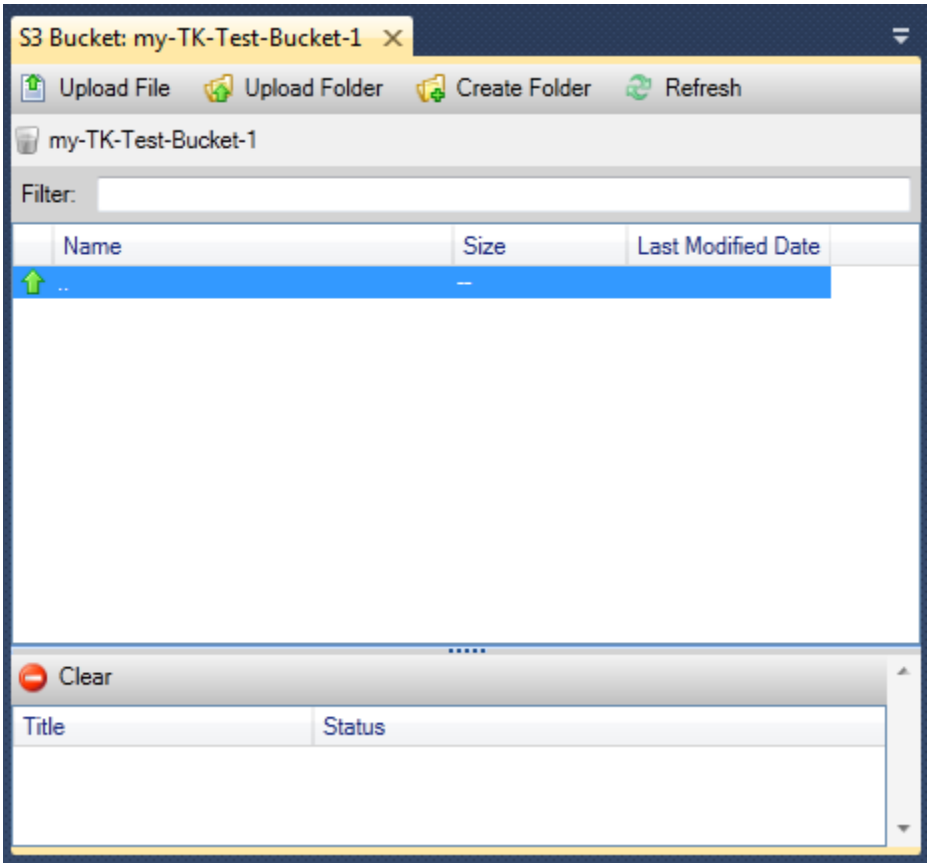
1. In :AWSÖffnen Sie das Kontextmenü (rechte Maustaste) für dasAmazon S3-Knoten, und wählen Sie dannCreate Bucketaus.
2. Geben Sie im Dialogfeld Create Bucket (Bucket erstellen) einen Namen für den Bucket ein. Bucket-Namen müssen überall eindeutig seinAWSaus. Informationen zu weiteren Einschränkungen finden Sie in der Amazon S3-Dokumentation.
3. Klicken Sie auf OK.

Verwalten von Amazon S3 S3-BucketsAWSExplorer

In :AWSIn Explorer sind die folgenden Vorgänge verfügbar, wenn Sie ein Kontextmenü (rechte Maustaste) 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 diese Ansicht des Buckets auch aufrufen, indem Sie in auf den Bucket-Namen klickenAWS-Explorer



Eigenschaften

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

- Festlegen von Amazon S3 S3-Berechtigungen für:
  - Sie als Bucket-Eigentümer
  - alle Benutzer, die beiAWSaus.
  - Alle Benutzer mit Zugriff auf das Internet
- Aktivieren der Protokollierung für den Bucket
- Einrichten einer Benachrichtigung über den Amazon Simple Notification Service (Amazon SNS), damit Sie bei Datenverlusten benachrichtigt werden, wenn Sie Reduced Redundancy Storage (RRS) verwenden. RRS ist eine Amazon S3 S3-Speicheroption, die eine geringere Beständigkeit 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 Richtlinien mit AWS Identity and Access Management (IAM) 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 das Anzeigen mehrteiliger Uploads. Amazon S3 unterstützt die Aufteilung von Uploads großer Objekte in Teile, um den Upload-Vorgang 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.

Hochladen von Dateien und Ordnern in Amazon S3

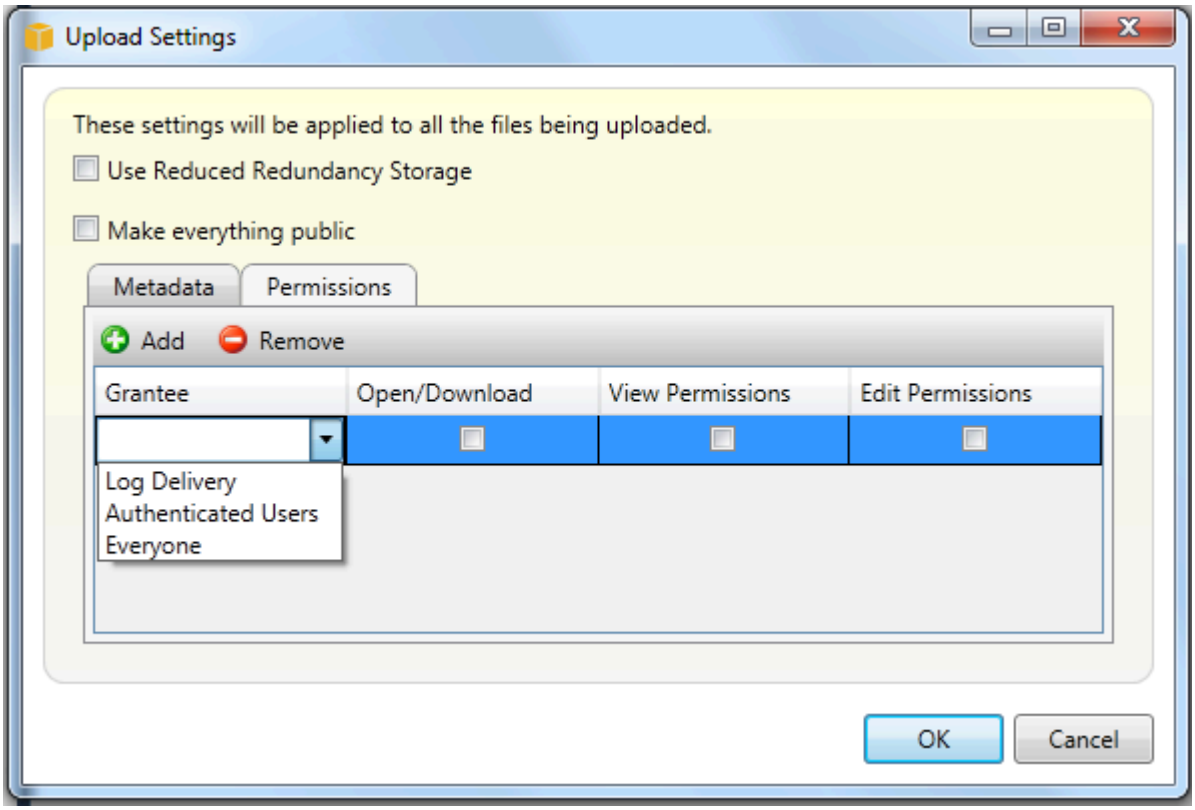
Sie könnenAWSZum Übertragen von Dateien oder ganzen Ordnern von Ihrem lokalen Computer in Ihre Buckets.

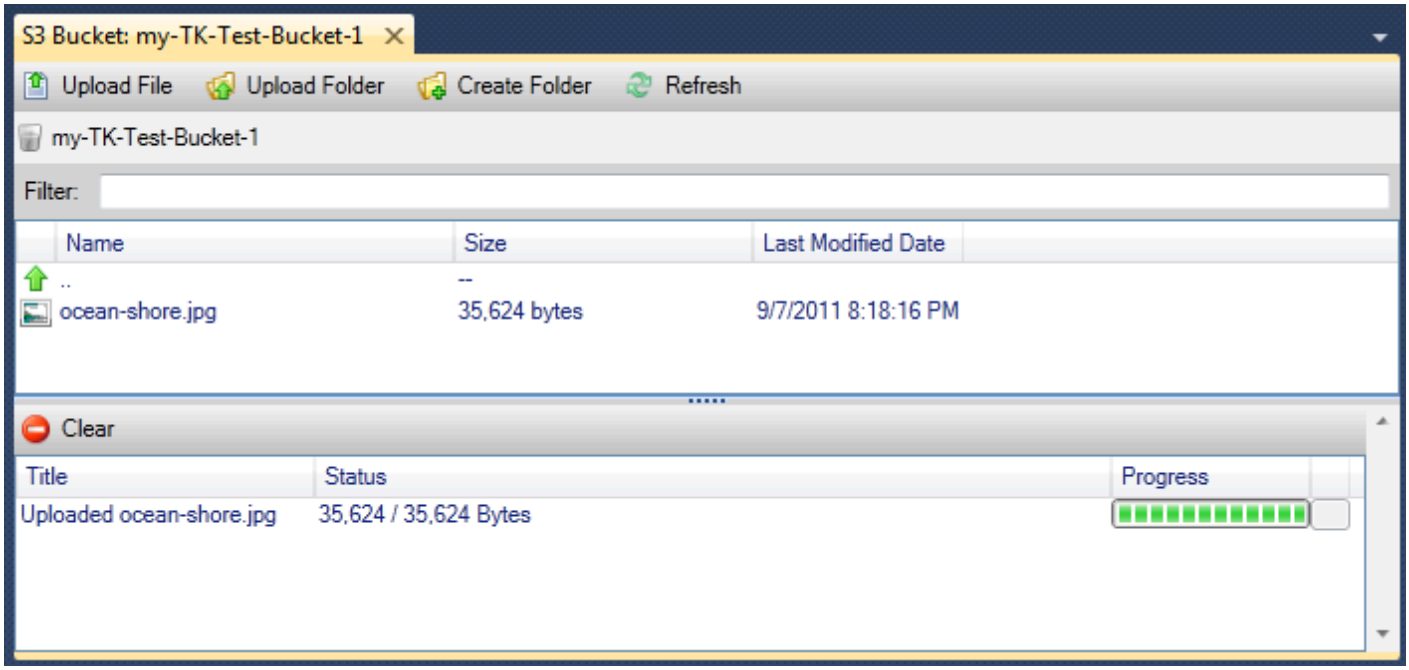
> **Note**
>
> Wenn Sie Dateien oder Ordner hochladen, die den gleichen Namen aufweisen wie bereits im Amazon S3 S3-Bucket vorhandene Dateien oder Ordner, überschreiben Ihre hochgeladenen Dateien die vorhandenen Dateien ohne Vorwarnung.

Laden Sie wie folgt eine Datei nach S3 hoch:

1. In :AWSExplorer, erweitern Sie dasAmazon S3-Knoten, doppelklicken Sie auf einen Bucket oder öffnen Sie das Kontextmenü (rechte Maustaste) für den Bucket und wählen SieDurchsuchenaus.
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).

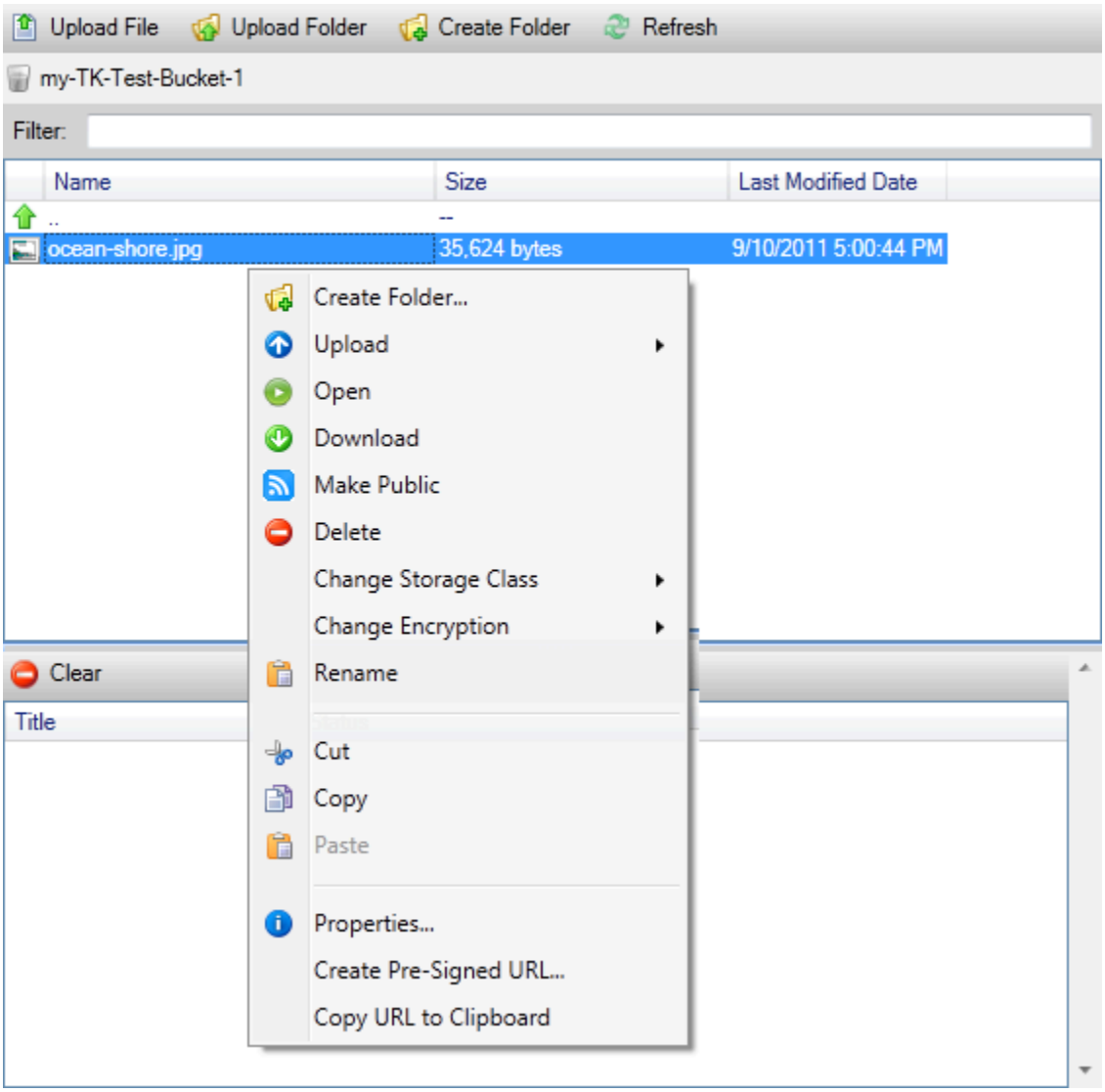
Im Dialogfeld Upload Settings (Upload-Einstellungen) können Sie Metadaten und Berechtigungen für die Dateien oder Ordner, die Sie hochladen, festlegen. Das Aktivieren des Kontrollkästchens Make everything public (Alles als öffentlich festlegen) entspricht dem festlegen der Berechtigungen Open/Download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





Amazon S3 S3-DateiVorgänge vonAWS-Toolkit for Visual Studio

Wenn Sie eine Datei in der Amazon S3 S3-Ansicht auswählen und das Kontextmenü öffnen (rechte Maustaste), können Sie verschiedene Aktionen mit 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.

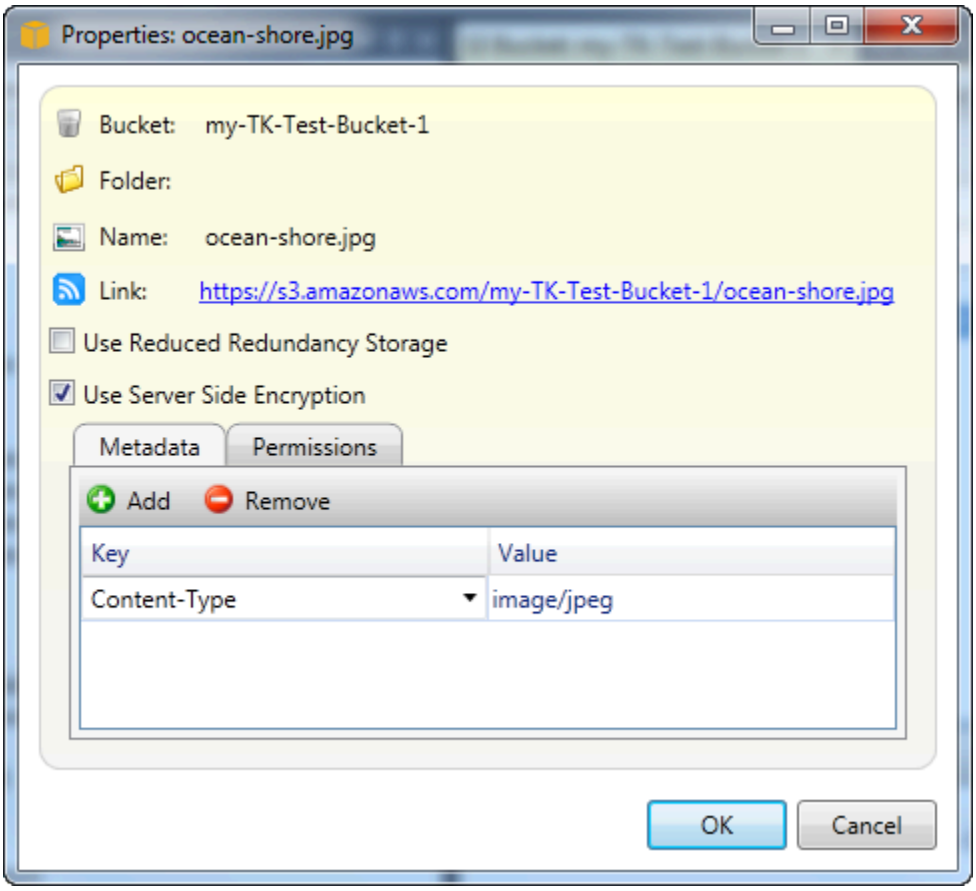
Ausschneiden | Kopieren | Einfügen

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 auswählen,

öffnet das Toolkit for Visual Studio die Datei in Ihrem Standard-Browser. 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, wird empfohlen, vorsignierte URLs zu erstellen und zu verteilen.



Vorsignierte URL erstellen

Ermöglicht das Erstellen einer zeitlich eingeschränkten vorsignierten URL, die Sie verteilen können, damit andere Benutzer Zugriff auf Ihre in Amazon S3 gespeicherten Inhalte erhalten.

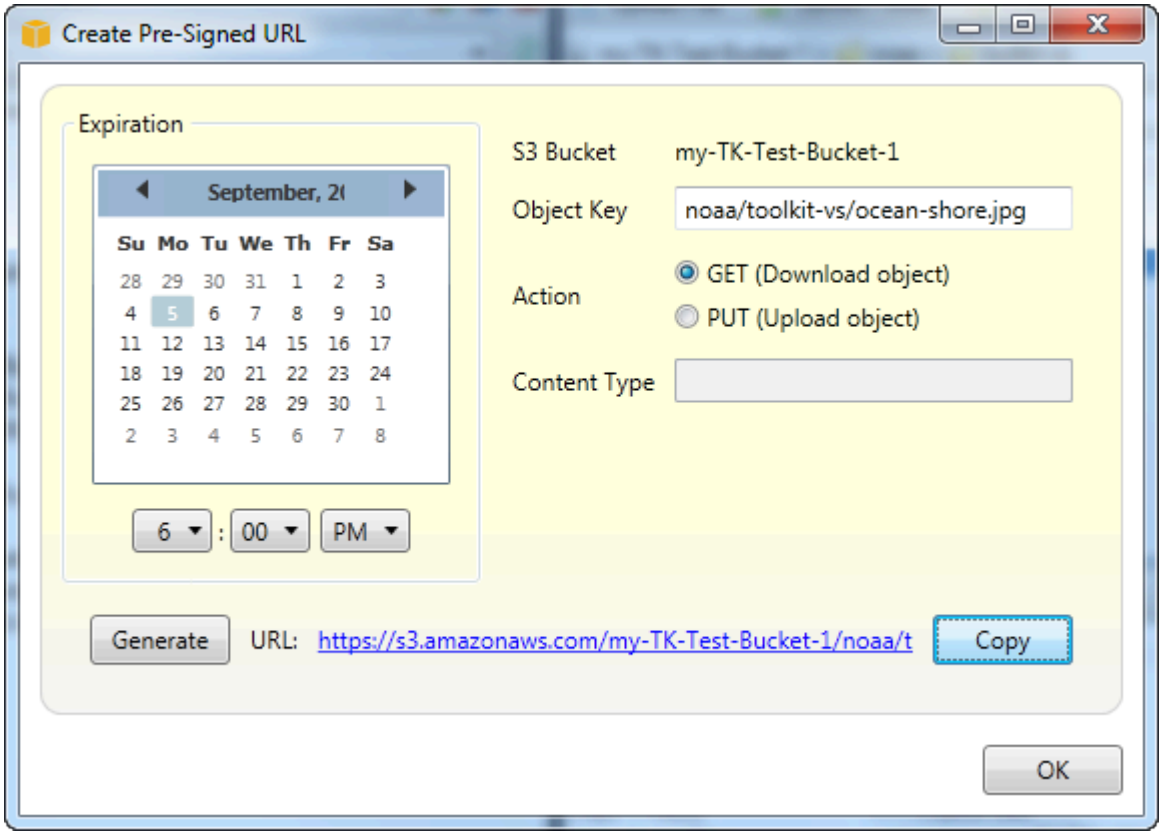
Erstellen einer vorsignierten URL

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.

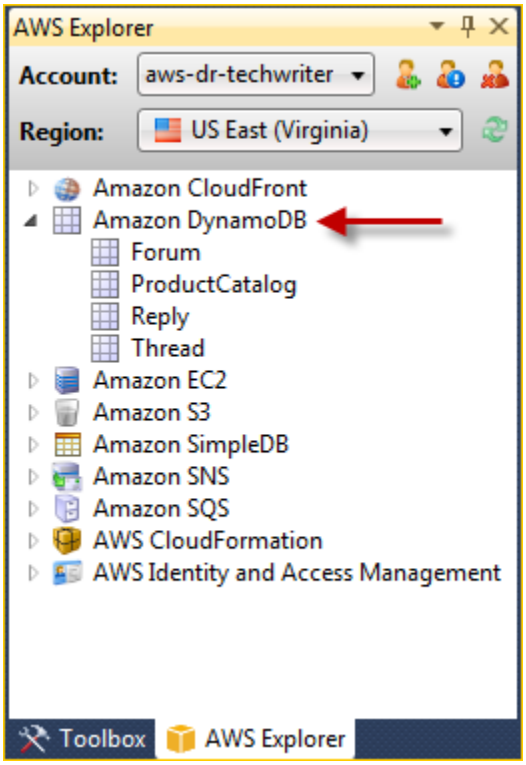
2. Wählen Sie die Schaltfläche Generate (Generieren) aus.
3. Wählen Sie zum Kopieren der URL in die Zwischenablage Copy (Kopieren) aus.



Verwenden von DynamoDBAWSExplorer

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 verfügt über die Funktionalität für das Arbeiten mit DynamoDB in einem Entwicklungskontext. Weitere Informationen über DynamoDB finden Sie unterDynamoDBauf der Amazon Web Services Services-Website.

Im Toolkit for Visual StudioAWSDer Explorer zeigt alle mit dem aktiven verknüpften DynamoDB-Tabellen anAWS-Kontoaus.



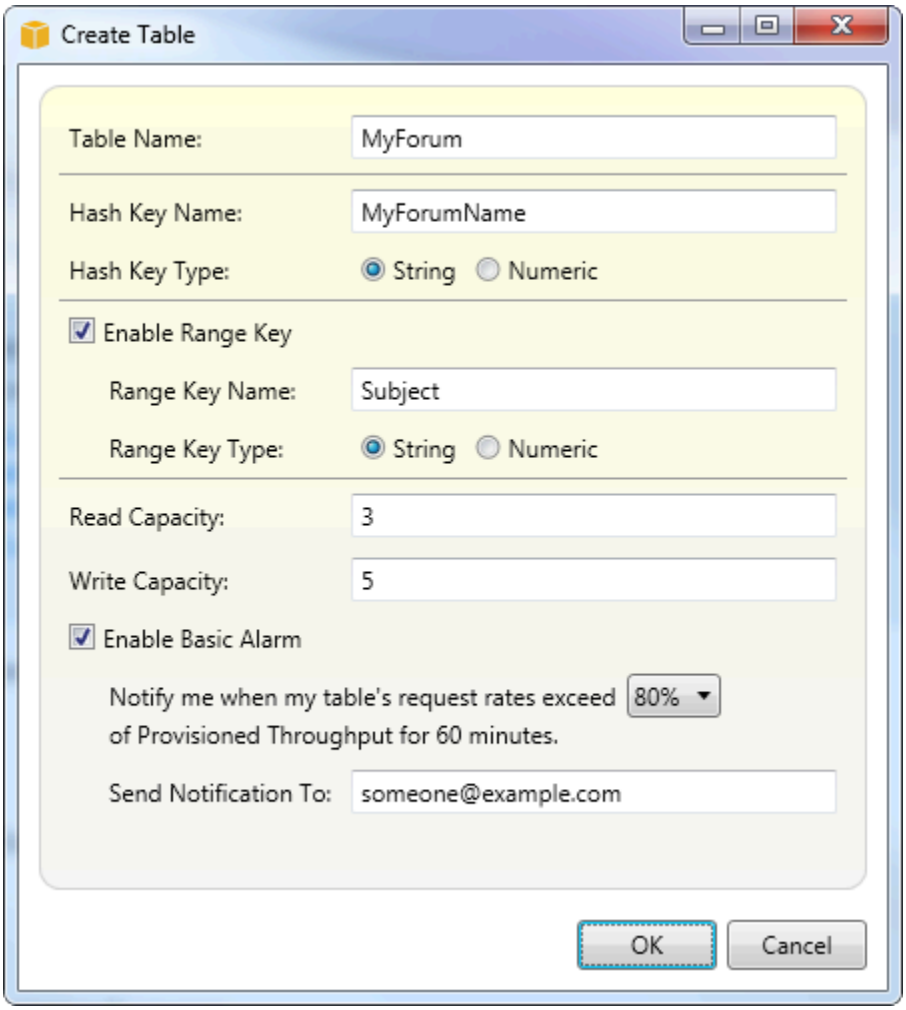
Erstellen einer DynamoDB-Tabelle

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

So erstellen Sie eine -Tabelle inAWSExplorer

1. In :AWSExplorer öffnen Sie das Kontextmenü (rechte Maustaste) fürAmazon DynamoDBKlicken Sie auf und danach aufCreate tableaus.
2. Geben Sie im Create Table (Tabelle erstellen)-Assistenten unter Table Name (Tabellenname)einen Namen für die Tabelle ein.
3. In derHash-Schlüsselname, geben Sie ein primäres Hash-Schlüsselattribut ein undHash-Schlüsseltyp-Schaltflächen, wählen Sie den Typ des Hash-Schlüssels. DynamoDB Primärschlüssel-Attribut einen ungeordneten Hash-Index und mit dem primären Schlüsselattribut einen optionalen sortierten Bereichsindex. Weitere Informationen zum primären Hash-Schlüsselattribut finden Sie im.Primärschlüssel-Abschnitt imEntwicklerhandbuch für Amazon DynamoDBaus.
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.

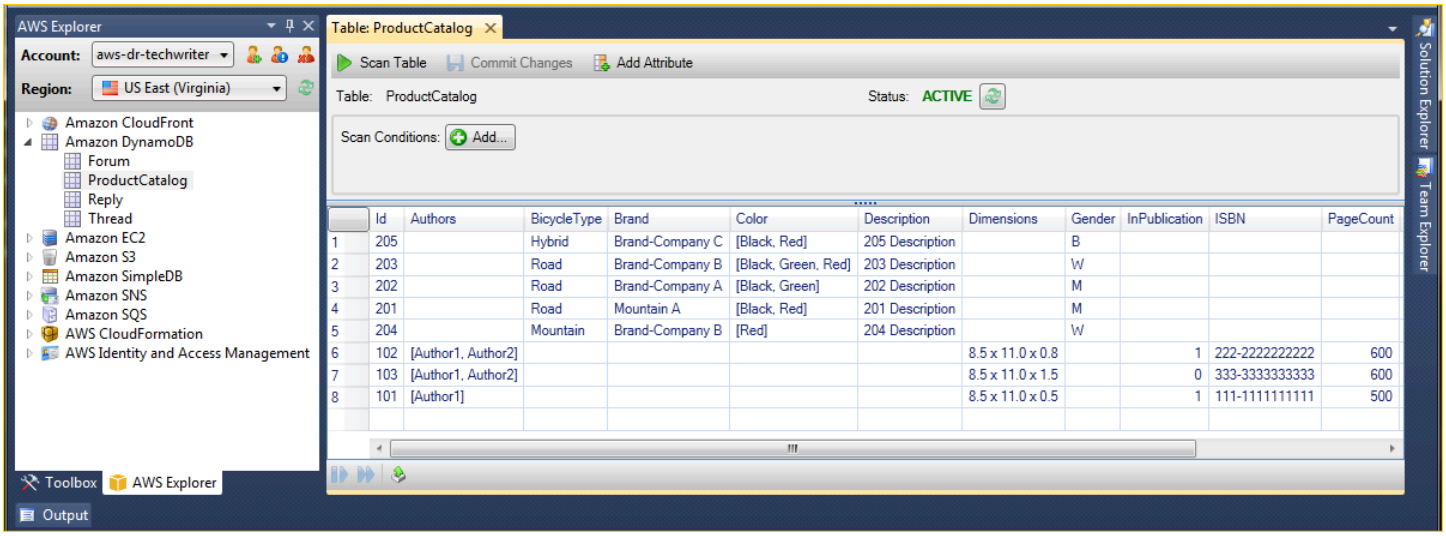


Weitere Informationen zu DynamoDB-Tabellen finden Sie unterDatenmodellkonzepte - Tabellen, Elemente und Attributeaus.

Anzeigen einer DynamoDB-Tabelle als Raster

Sie öffnen eine Raster Ansicht einer Ihrer DynamoDB-TabellenAWSDoppelklicken Sie im Explorer auf den Subknoten, 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.

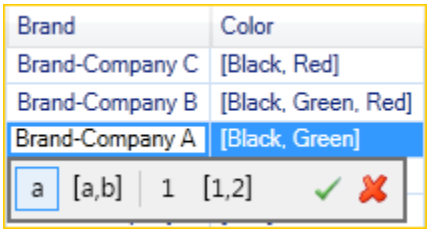
Der Wert eines Attributs kann eine Zeichenfolge oder eine Zahl sein. Manche Attribute verfügen über einen Wert, der aus einem Satz von Zeichenfolgen oder Zahlen besteht. Satzwerte werden als eine durch Komma getrennte Liste in eckigen Klammern angezeigt.



	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

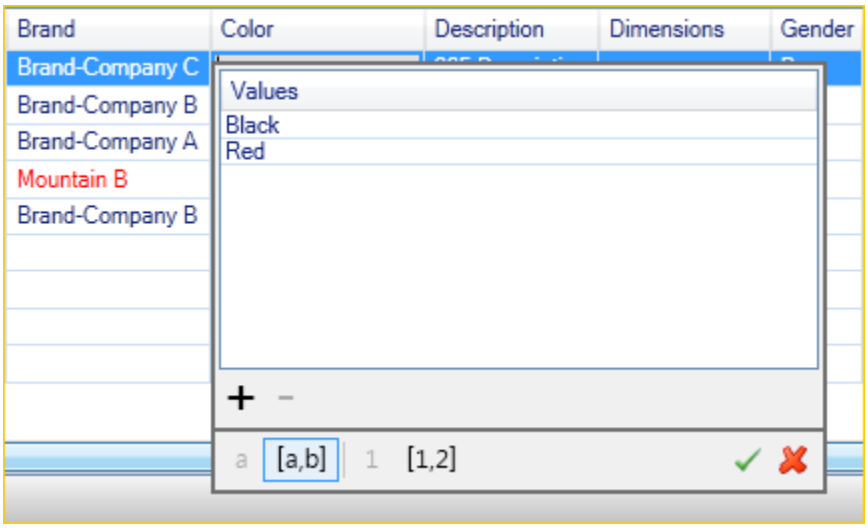
Bearbeiten und Hinzufügen von Attributen und Werten

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.

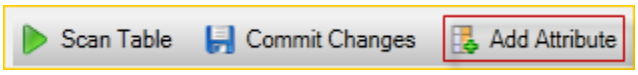


Wählen Sie nach dem Bearbeiten des Attributwerts das grüne Häkchen, um Ihre Änderungen zu bestätigen. Wenn Sie die Änderungen verwerfen möchten, wählen Sie das rote X.

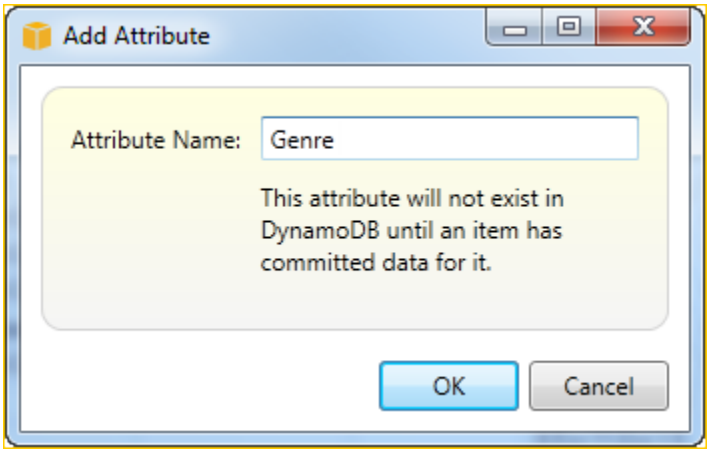
Nachdem Sie Ihre Änderungen bestätigt haben, wird der Attributwert rot angezeigt. Dies bedeutet, dass das Attribut aktualisiert wurde, der neue Wert jedoch noch nicht in die DynamoDB-Datenbank geschrieben wurde. Um Ihre Änderungen wieder in DynamoDB zu schreiben, wählen SieÄnderungen übernehmenaus. Um 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

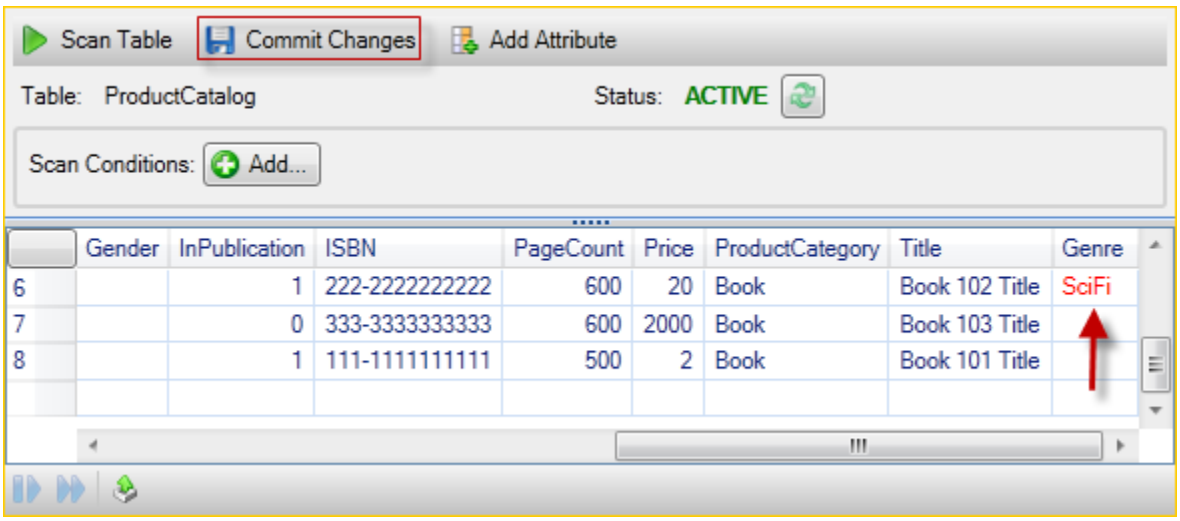
In der Rasteransicht können Sie der Tabelle auch Attribute hinzufügen. Wählen Sie Add Attribute (Attribut hinzuzufügen), um ein neues Attribut hinzuzufügen.



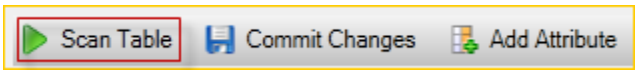
Geben Sie im Dialogfeld Add Attribut (Attribut hinzuzufügen) einen Namen für das Attribut ein und wählen Sie dann OK aus.



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

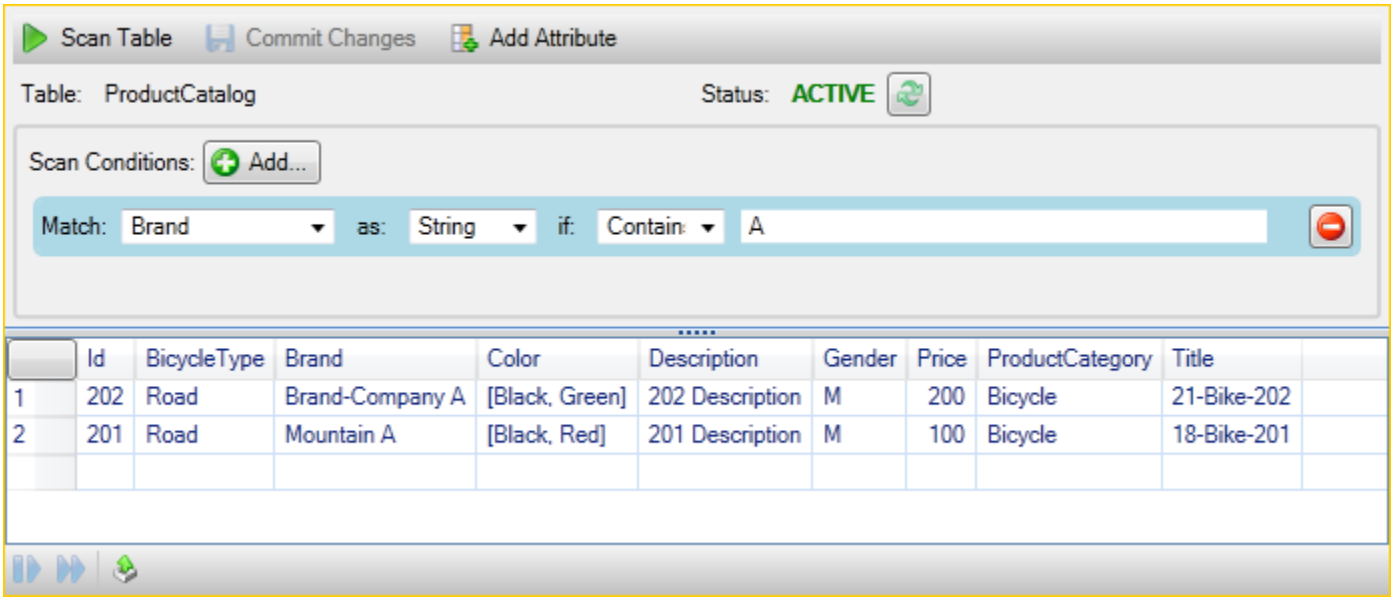


Sie können Ihre DynamoDB-Tabellen mit dem Toolkit scannen. In einem Scan definieren Sie eine Reihe von Kriterien und der Scan führt alle Elemente in der Tabelle auf, die den Kriterien entsprechen. Scans sind teure Operationen und sollten daher mit Vorsicht verwendet werden, um zu vermeiden, dass Produktionsdatenverkehr mit höherer Priorität in der Tabelle unterbrochen wird. Weitere Informationen über die Verwendung der Scan-Operation finden Sie im.Entwicklerhandbuch für Amazon DynamoDBaus.

Sie führen einen Scan einer DynamoDB-Tabelle ausAWSExplorer

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.

benutzenAWS CodeCommitMit dem Team Explorer von Visual Studio

Sie könnenAWS Identity and Access Management(IAM) -Benutzerkonten zum Erstellen von Git-Anmeldeinformationen und zum Erstellen und Klonen von Repositorys aus dem Team Explorer.

Anmeldeinformationstypen für AWS CodeCommit

Die meistenAWS Toolkit for Visual StudioBenutzer sind sich der Einrichtung bewusstAWSAnmeldeinformationsprofile, die Zugriffs- und geheimen Schlüssel enthalten. Mit diesen Anmeldeinformationen werden im Toolkit for Visual Studio die Aufrufe an Service-APIs umgesetzt, beispielsweise zum Auflisten von Amazon S3 S3-Buckets inAWSExplorer oder um eine Amazon EC2 Instance zu starten. Die Integration von AWS CodeCommit in Team Explorer nutzt diese Anmeldeinformationsprofile ebenfalls. Für die direkte Arbeit mit Git benötigen Sie jedoch zusätzliche Anmeldeinformationen, genauer gesagt, Git-Anmeldeinformationen für HTTPS-Verbindungen. Über diese Anmeldeinformationen (Benutzername und Passwort) können Sie unterEinrichtung für HTTPS-Benutzer, die Git-Anmeldeinformationen verwendenimAWS CodeCommit-Benutzerhandbuchaus.

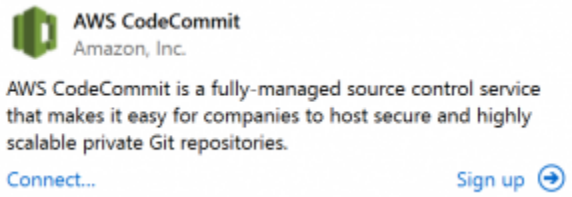
Sie können die Git-Anmeldeinformationen fürAWS CodeCommitnur für IAM-Benutzerkonten.
Es ist nicht möglich, sie für ein Root-Konto zu erstellen. Sie können bis zu zwei Gruppen dieser Anmeldeinformationen für den Service erstellen. Obwohl Sie eine Gruppe von Anmeldeinformationen als inaktiv markieren können, werden inaktive Gruppen weiterhin Ihrem Grenzwert von zwei Gruppen zugerechnet. Beachten Sie, dass Sie Anmeldeinformationen jederzeit löschen und neu erstellen können. Wenn Sie es verwendenAWS CodeCommitaus Visual Studio, Ihrem traditionellenAWSAnmeldeinformationen werden für die Arbeit mit dem Service verwendet, z. B. beim

Erstellen und Auflisten von Repositorys. Bei der Arbeit mit den in AWS CodeCommit gehosteten Git-Repositorys verwenden Sie die Git-Anmeldeinformationen.

Im Rahmen der Unterstützung fürAWS CodeCommiterstellt und verwaltet das Toolkit for Visual Studio automatisch diese Git-Anmeldeinformationen und verknüpft sie mit IhremAWSAnmeldeinformationsprofil. Sie müssen sich nicht darum kümmern, die richtigen Anmeldeinformationen bereitzuhalten, wenn Sie Git-Operationen im Team Explorer durchführen möchten. Sobald Sie sich mit Ihrem Team Explorer verbindenAWSAnmeldeinformationsprofil, die zugehörigen Git-Anmeldeinformationen werden automatisch verwendet, wenn Sie mit einer Git-Fernbedienung arbeiten.

Herstellen einer Verbindung mit AWS CodeCommit

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

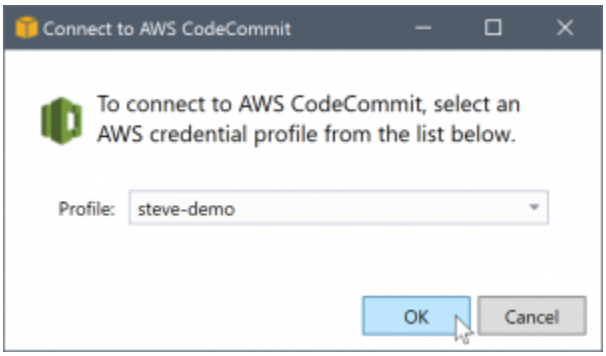


AuswahlRegistrierenöffnet die Homepage von Amazon Web Services in einem Browserfenster. Was geschieht, wenn Sie sich entscheidenVerbindenhängt davon ab, ob das Toolkit for Visual Studio ein Anmeldeinformationsprofil mitAWSZugriff und geheime Schlüssel, um Anrufe zu tätigenAWSIn Ihrem Namen. Möglicherweise haben Sie ein Anmeldeinformationsprofil auf der neuen Seite „Getting Started“ eingerichtet, die in der IDE angezeigt wird, wenn das Toolkit for Visual Studio keine lokal gespeicherten Anmeldeinformationen finden kann. Oder Sie haben vielleicht das Toolkit for Visual Studio verwendet, dasAWS Tools for Windows PowerShelloder dasAWS CLIund haben schonAWSAnmeldeinformationsprofile, die für das Toolkit for Visual Studio verfügbar sind.

Wenn Sie sich fürVerbindenbeginnt das Toolkit for Visual Studio mit dem Auffinden eines Anmeldeinformationsprofils, das für die Verbindung verwendet werden kann. Wenn das Toolkit for Visual Studio kein Anmeldeinformationsprofil finden kann, wird ein Dialogfeld geöffnet, in dem Sie aufgefordert werden, den Zugriffs- und den geheimen Schlüssel für IhreAWS-Kontoaus. 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 der Zugriffs- und der geheime Schlüssel angegeben wurden und

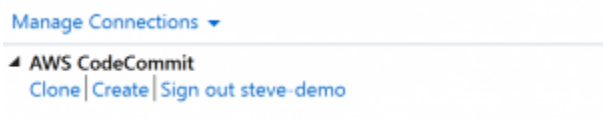
das Anmeldeinformationsprofil erstellt wurde, ist die Verbindung zwischen dem Team Explorer und AWS CodeCommit einsatzbereit.

Wenn das Toolkit for Visual Studio mehrere findetAWSAnmeldeinformationsprofil, werden Sie dazu aufgefordert, das gewünschte Konto für die Verwendung im Team Explorer auszuwählen.



Wenn Sie nur über ein Anmeldeinformationsprofil verfügen, übergeht das Toolkit for Visual Studio das Auswahldialogfeld für das Profil und es wird sofort eine Verbindung hergestellt:

Wenn eine Verbindung zwischen dem Team Explorer und AWS CodeCommit über Ihr Anmeldeinformationsprofil hergestellt wurde, wird das Einladungsdialogfeld geschlossen und der Verbindungsbereich wird angezeigt.

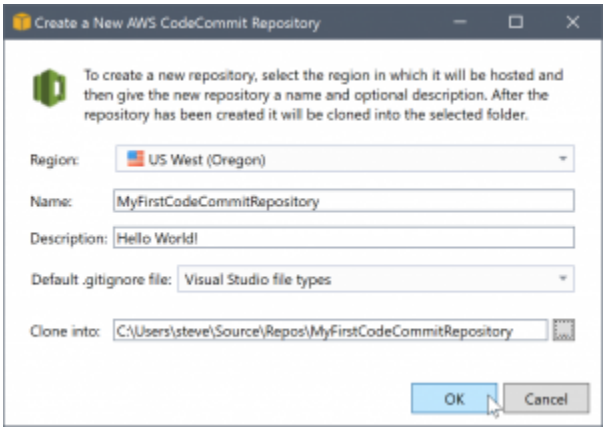


Da Sie nicht über lokale geklonte Repositorys verfügen, werden in dem Bereich nur die Vorgänge angezeigt, die Sie ausführen können: Klonen,Geben Sie einen Namen für den Benutzer ein und klicken Sie dann auf, undAbmeldenaus. Wie andere AnbieterAWS CodeCommitIm Team Explorer kann nur an einen einzigen gebunden werdenAWSAnmeldeinformationsprofil zu einem bestimmten Zeitpunkt. 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 das klickenGeben Sie einen Namen für den Benutzer ein und klicken Sie dann auflink, dasErstellen eines neuenAWS CodeCommitAblageDas Dialogfeld wird geöffnet.



AWS CodeCommit-Repositorys sind nach Region eingeteilt, daher können Sie unter Region die Region auswählen, in der das Repository gehostet werden soll. Die Liste enthält alle Regionen, in denen AWS CodeCommit unterstützt 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 vom Service an, das Repository zu erstellen und dann lokal zu klonen. Dabei wird ein erster Commit für die .gitignore-Datei hinzugefügt, sofern Sie eine verwenden. Nun beginnen Sie mit der Arbeit mit dem Git-Remote-Repository, daher benötigt das Toolkit for Visual Studio jetzt die zuvor beschriebenen Git-Anmeldeinformationen.

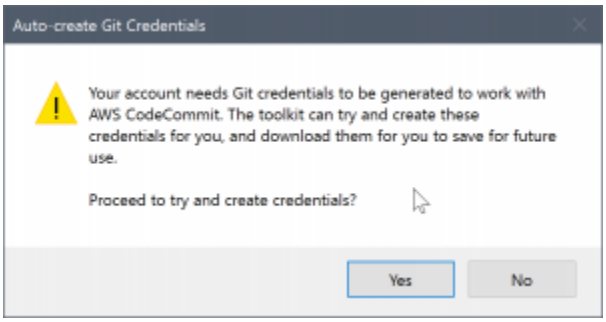
Einrichten von Git-Anmeldeinformationen

Bis zu diesem Punkt hast du benutztAWSZugriffs- und geheime Schlüssel, um anzufordern, dass der Service Ihr Repository erstellt. Jetzt müssen Sie mit Git selbst arbeiten, um den Klonvorgang durchzuführen, und Git versteht es nichtAWSZugriff und geheime Schlüssel. Stattdessen müssen

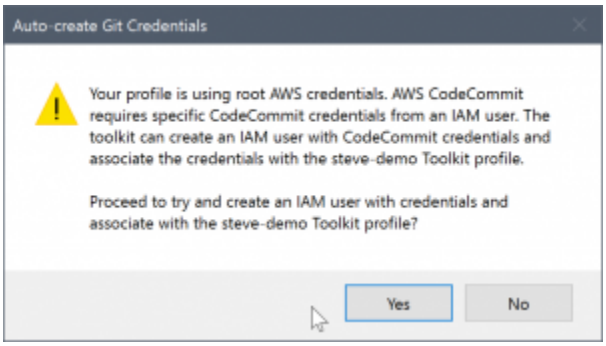
Sie Git die Anmeldeinformationen (Benutzername und Passwort) angeben, die für eine HTTPS-Verbindung mit dem Remote-Repository verwendet werden sollen.

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. Sie sollten immer Ihre einrichtenAWSAnmeldeinformationsprofile, die IAM-Benutzerzugriffs- und geheime Schlüssel enthalten, und nicht Root-Schlüssel. Das Toolkit for Visual Studio kann versuchen, Git-Anmeldeinformationen fürAWS CodeCommitfür dich und verbinde sie mit demAWSAnmeldeinformationen, mit dem Sie zuvor im Team Explorer eine Verbindung hergestellt haben.

Wenn Sie sich fürOKAYimErstellen eines neuenAWS CodeCommitAblageund erstellt erfolgreich das Repository, überprüft das Toolkit for Visual Studio dieAWSAnmeldeinformationen, das im Team Explorer verbunden ist, um festzustellen, ob Git-Anmeldeinformationen fürAWS CodeCommitexistieren und sind lokal mit dem Profil verknüpft. In diesem Fall weist das Toolkit for Visual Studio den Team Explorer an, den Klonvorgang für das neue Repository durchzuführen. Wenn keine lokalen Git-Anmeldeinformationen verfügbar sind, überprüft das Toolkit for Visual Studio den Typ der Kontoanmeldeinformationen, die für die Verbindung im Team Explorer verwendet wurden. Wenn es sich um Anmeldeinformationen für einen IAM-Benutzer handelt, wie empfohlen, wird die folgende Meldung angezeigt.

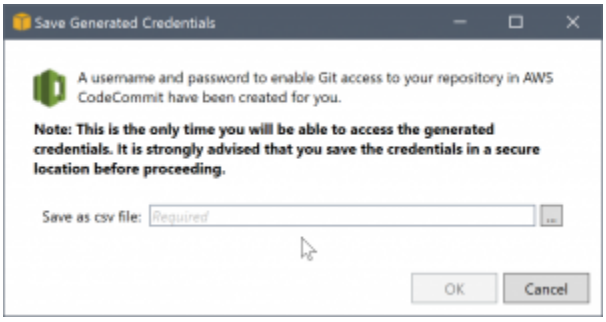


Wenn es sich um Root-Anmeldeinformationen handelt, wird stattdessen die folgende Meldung angezeigt.



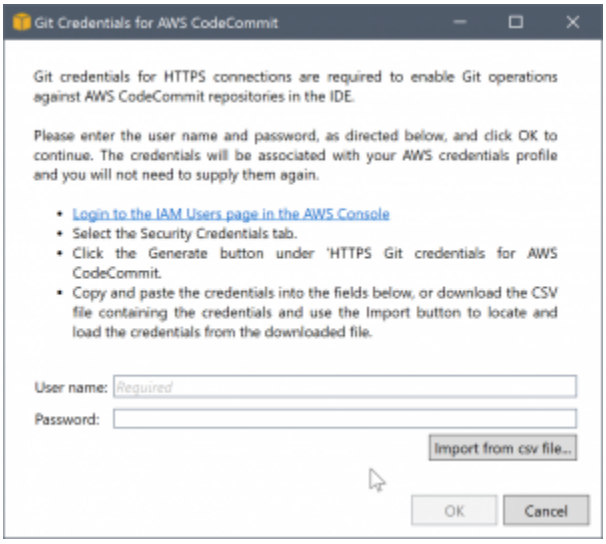
In beiden Fällen bietet das Toolkit for Visual Studio die Möglichkeit, die erforderlichen Git-Anmeldeinformationen für Sie zu erstellen. Im ersten Szenario wird für die Erstellung lediglich eine Gruppe von Git-Anmeldeinformationen für den IAM-Benutzer benötigt. Wenn ein Root-Konto verwendet wird, versucht das Toolkit for Visual Studio zuerst, einen IAM-Benutzer zu erstellen, und erstellt dann Git-Anmeldeinformationen für diesen neuen Benutzer. Wenn das Toolkit for Visual Studio einen neuen Benutzer erstellen muss, wendet es dieAWS CodeCommitVon Power User verwaltete Richtlinie für dieses neue Benutzerkonto. Diese Richtlinie ermöglicht nur den Zugriff auf AWS CodeCommit und lässt alle mit AWS CodeCommit durchgeführten Vorgänge mit Ausnahme des Löschens von Repositorys zu.

Wenn Sie Anmeldeinformationen erstellen, können Sie sie nur einmal anzeigen. Daher fordert das Toolkit for Visual Studio Sie auf, die neu erstellten Anmeldeinformationen als `.csv`-Datei und fährt dann fort.



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

In einigen Fällen kann das Toolkit for Visual Studio Anmeldeinformationen möglicherweise nicht automatisch erstellen. Möglicherweise haben Sie z. B. bereits die maximale Anzahl von Git-Anmeldeinformationen fürAWS CodeCommit(zwei) oder Sie verfügen nicht über ausreichende programmgesteuerte Rechte, damit das Toolkit for Visual Studio die Arbeit für Sie erledigen kann (wenn Sie als IAM-Benutzer angemeldet sind). In diesen Fällen können Sie sich bei derAWS Management ConsoleUm die Anmeldeinformationen zu verwalten oder sie von Ihrem Administrator zu erhalten. Sie können sie dann imGit-Anmeldeinformationen fürAWS CodeCommit-Dialogfeld, das das Toolkit for Visual Studio anzeigt.

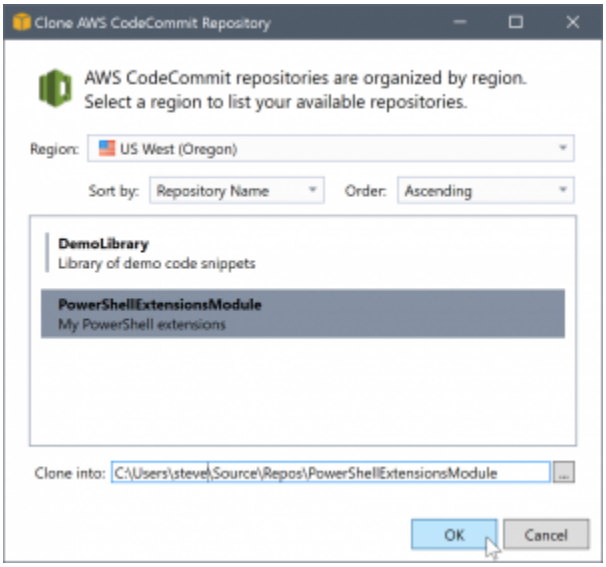


Nachdem die Anmeldeinformationen für Git verfügbar sind, wird mit dem Klonvorgang für das neue Repository fortgefahren (siehe die Fortschrittsanzeige für den Vorgang im Team Explorer). Wenn Sie eine Standard-`.gitignore`-Datei angewendet haben, wird für diese ein Commit im Repository mit dem Kommentar „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, wird beim Erstellen neuer Repositorys in Zukunft nur noch dasErstellen eines neuenAWS CodeCommitAblageDialogfeld selbst.

Klonen eines Repositorys

Um ein vorhandenes Repository zu klonen, kehren Sie zum Verbindungsbereich für AWS CodeCommit im Team Explorer zurück. Klicken Sie auf das SymbolKlonenLink zum Öffnen desKlonenAWS CodeCommitAblage-Dialogfeld und wählen Sie dann das zu klonende Repository und den Speicherort auf dem Datenträger aus, an dem es platziert werden soll.



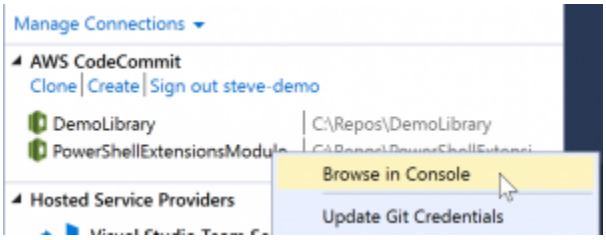
Nachdem Sie die Region ausgewählt haben, fragt das Toolkit for Visual Studio den Service ab, um die in dieser Region verfügbaren Repositorys zu ermitteln. Diese werden dann im zentralen Listenbereich des Dialogfelds angezeigt. Der Name und eine optionale Beschreibung jedes Repositorys werden ebenfalls 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 denGit-Anmeldeinformationen fürAWS CodeCommit-Dialogfeld, 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. Weil die Git-Anmeldeinformationen bereits lokal gespeichert und mit unseren verbundenen verknüpft sindAWSAnmeldeinformationsprofil, wir werden nicht dazu aufgefordert, sie für Vorgänge mit demAWS CodeCommitremote.

Verwenden von CodeArtifact in Visual Studio

AWS CodeArtifactist ein vollständig verwalteter Artefakt-Repository-Service, mit dem Unternehmen Softwarepakete für die Anwendungsentwicklung auf einfache Weise speichern und teilen können. Sie können CodeArtifact mit gängigen Build-Tools und Paketmanagern wie NuGet und .NET Core CLIs und Visual Studio verwenden. Sie können CodeArtifact auch so konfigurieren, dass Pakete aus einem externen, öffentlichen Repository wieNuget.orgaus.

In CodeArtifact werden Ihre Pakete in Repositorys gespeichert, die dann in einer Domäne gespeichert werden. DieAWS Toolkit for Visual Studiovereinfacht die Konfiguration von Visual Studio mit Ihren CodeArtifact-Repositorys und macht es einfach, Pakete in Visual Studio sowohl von CodeArtifact direkt als auch von Nuget.org zu konsumieren.

Fügen Sie Ihr CodeArtifact-Repository als NuGet-Paketquelle hinzu

Um Pakete aus Ihrem CodeArtifact zu konsumieren, müssen Sie Ihr Repository als Packabe-Quelle imNuGet-Paketmanagerim Visual Studio

So fügen Sie Ihr Repository als Paketquelle hinzu

1. In :AWSExplorer, navigieren Sie zu Ihrem Repository imAWS CodeArtifact-Knoten.

2. Öffnen Sie das Kontextmenü (rechte Maustaste) für das Repository, das Sie hinzufügen möchten, und wählen SieNuGet-Quellendpunkt kopierenaus.
3. Navigieren Sie zuPaketquellenunter demNuGet-Paketmanager-Knoten imExtras > OptionenMenü.
4. In :Paketquellenwählen Sie das Pluszeichen aus (+), bearbeiten Sie den Namen und fügen Sie die NuGet-Quellendpunkt-URL ein, die Sie zuvor in derSourcefield.
5. Aktivieren Sie das Kontrollkästchen neben Ihrer neu hinzugefügten Paketquelle, um es zu aktivieren.

> **Note**
>
> Wir empfehlen, eine externe Verbindung zuNuget.orgzu Ihrem CodeArtifact und Deaktivieren desnuget.orgPaketquelle in Visual Studio. Bei Verwendung einer externen Verbindung werden alle Abhängigkeiten ausNuget.orgwerden in CodeArtifact gespeichert. WennNuget.orggeht aus irgendeinem Grund aus, die Pakete, die Sie benötigen, sind weiterhin verfügbar. Weitere Informationen zu externen Verbindungen finden Sie unterEine externe Verbindung hinzufügenimAWS CodeArtifact-Benutzerhandbuchaus.

6. Klicken Sie aufOKAYum das Menü zu schließen.

Weitere Informationen zur Verwendung von CodeArtifact mit Visual Studio finden Sie unterVerwenden Sie CodeArtifact mit Visual StudioimAWS CodeArtifact-Benutzerhandbuchaus.

Amazon RDS vonAWSExplorer

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 Datenbank-Systemtypen:

- 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 beschriebenen Funktionalitäten sind auch über dieAWS-Managementkonsolefür Amazon RDS.

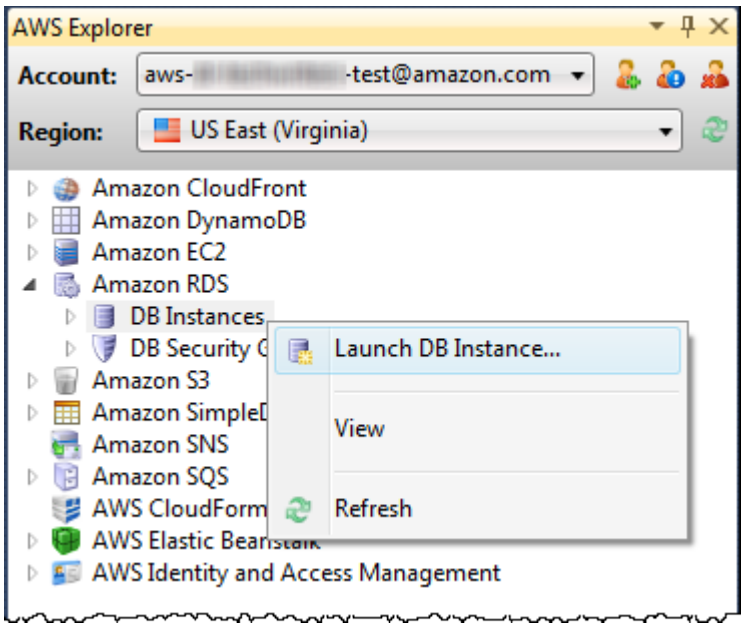
Themen

Starten einer Amazon RDS-Datenbank-Instance

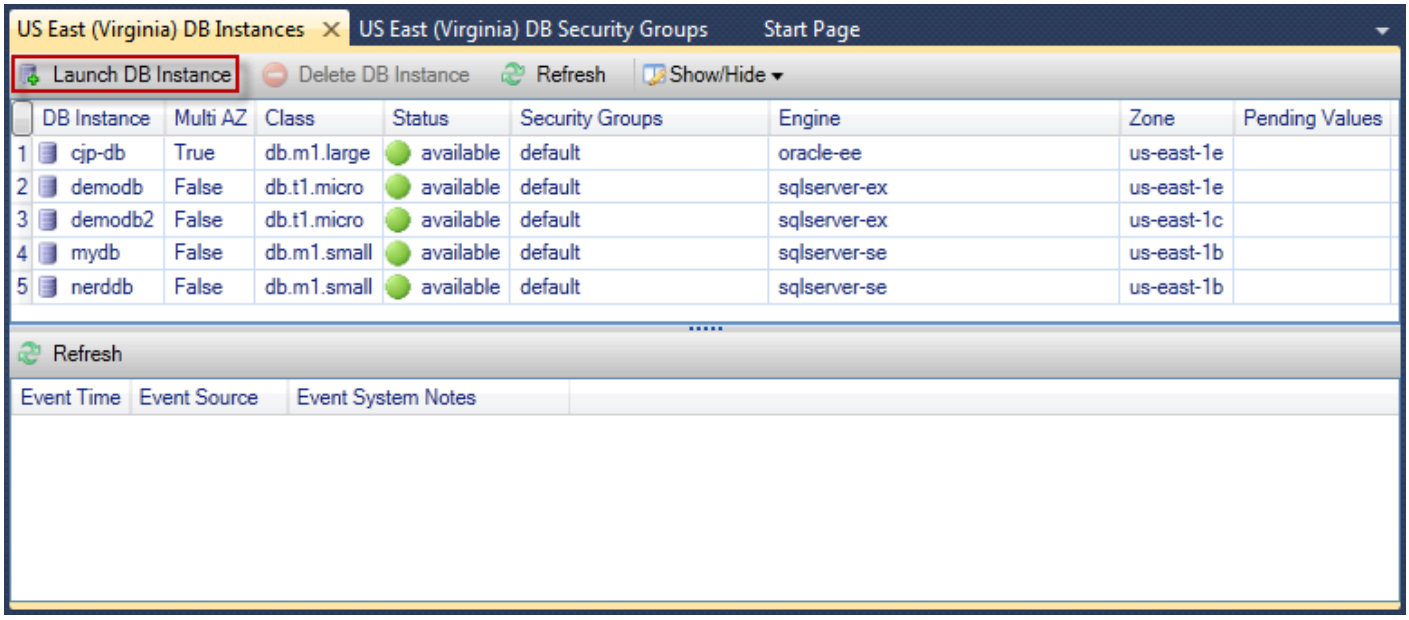
mitAWSIm Explorer können Sie Instances jeder der von Amazon RDS unterstützten Datenbank-Engines starten. In der folgenden schrittweise Anleitung wird das Starten einer Instance von Microsoft SQL Server Standard Edition beschrieben. Die Vorgehensweise ist jedoch bei allen unterstützten Engines ähnlich.

So starten Sie eine Amazon RDS-Instance

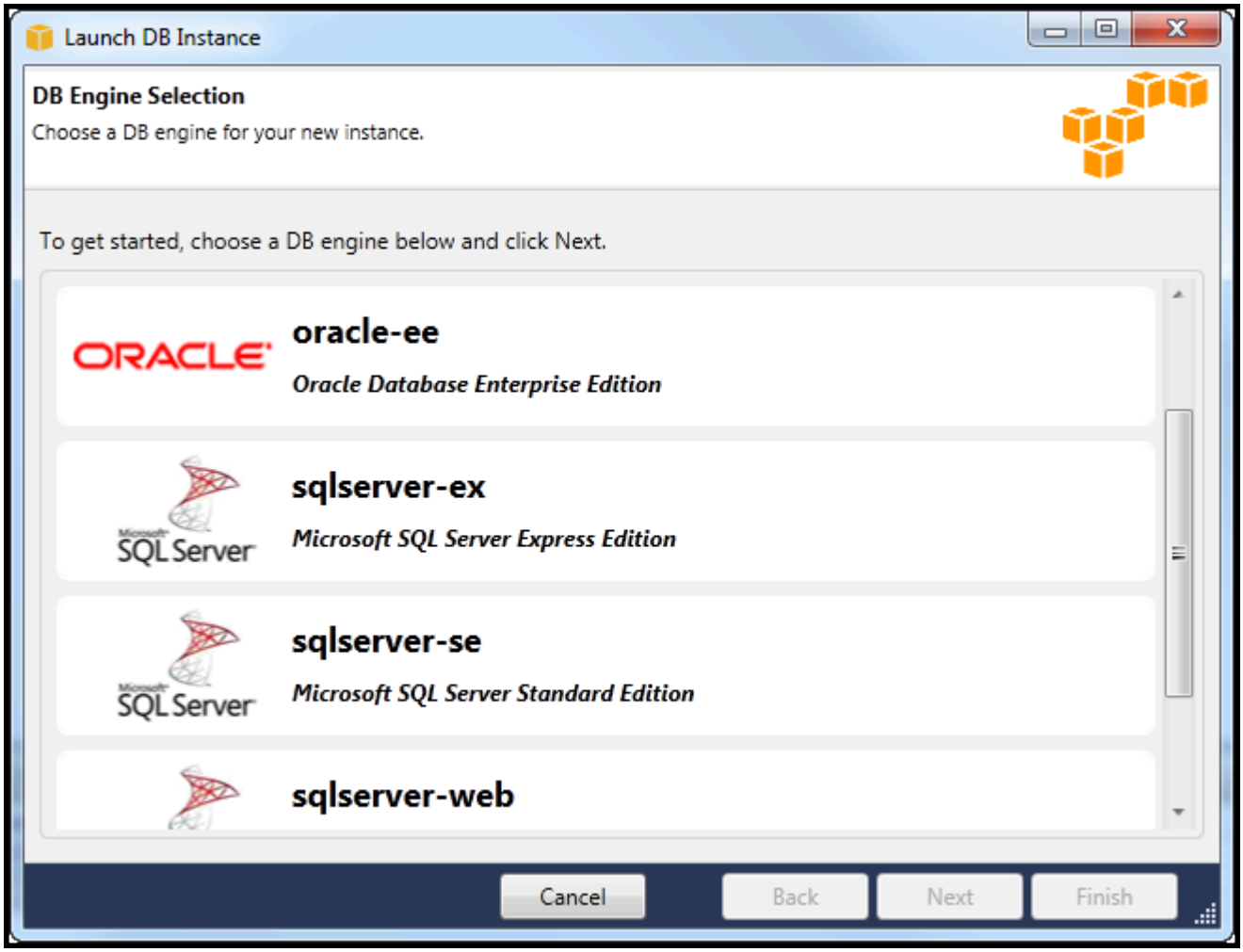
1. In :AWSÖffnen Sie das Kontextmenü (rechte Maustaste) für denAmazon RDSknoten und wählenDB-Instance startenaus.



   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 Type License Microsoft SQL Server license-included MySql general-public-license Oracle 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 zu erstellen und damit die Beständigkeit und Verfügbarkeit der Daten zu verbessern. Amazon RDS sorgt für die Bereitstellung und Verwaltung einer Standby-Kopie Ihrer Datenbank in einer anderen Availability Zone, für ein automatisches Failover im Falle eines geplanten oder ungeplanten Ausfalls. 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 ausAWSFühren Sie automatisch Nebenversionen auf Ihren RDS-Instances aktualisieren.

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

Engine	Minimum (GB)	Maximum (GB)
Microsoft SQL Server Express Edition	30	1024
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. Er wird in Kleinbuchstaben angezeigtAWSExplorer.

Master User Name (Master-Benutzername

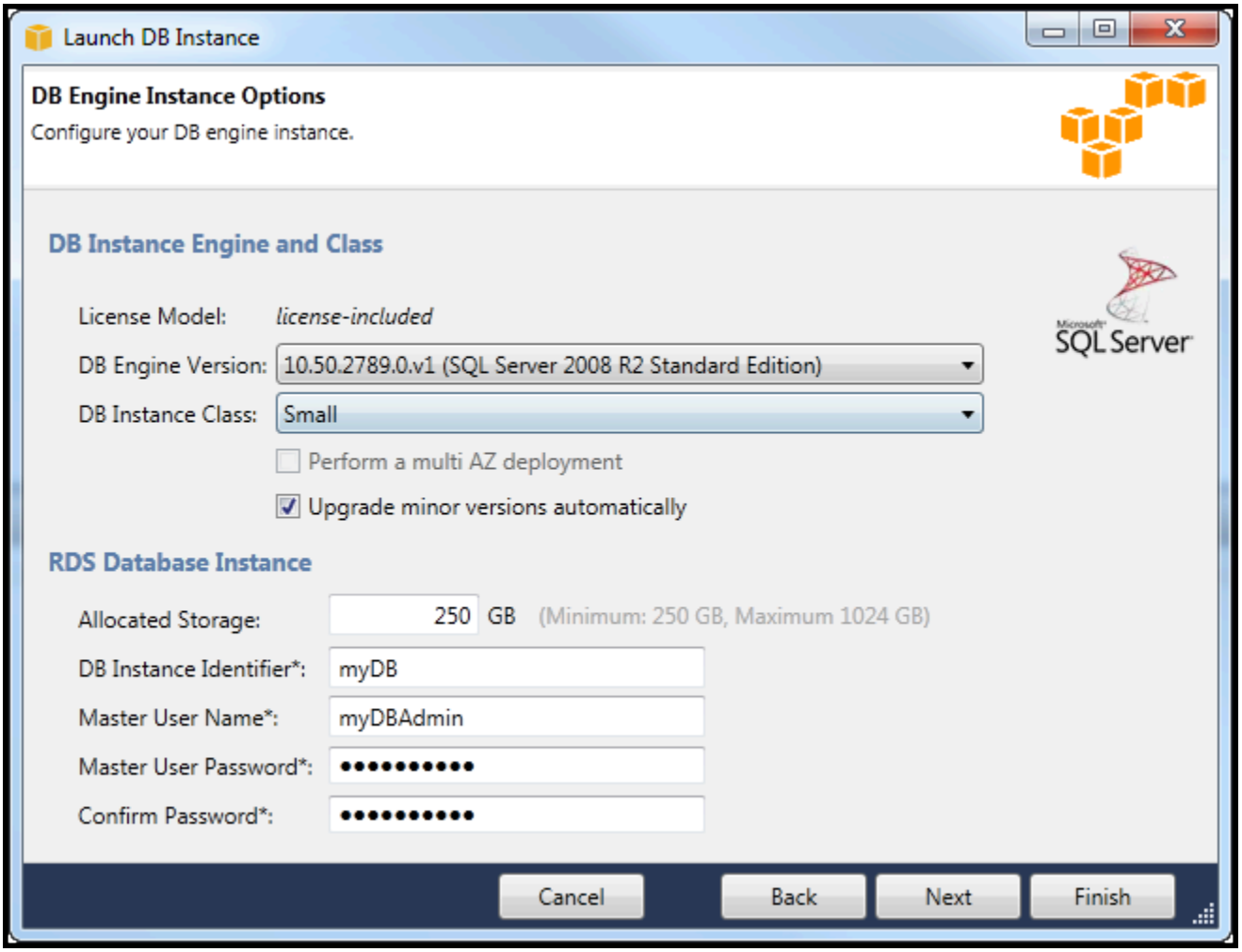
Geben Sie einen Namen für den Administrator der Datenbank-Instance ein.

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.

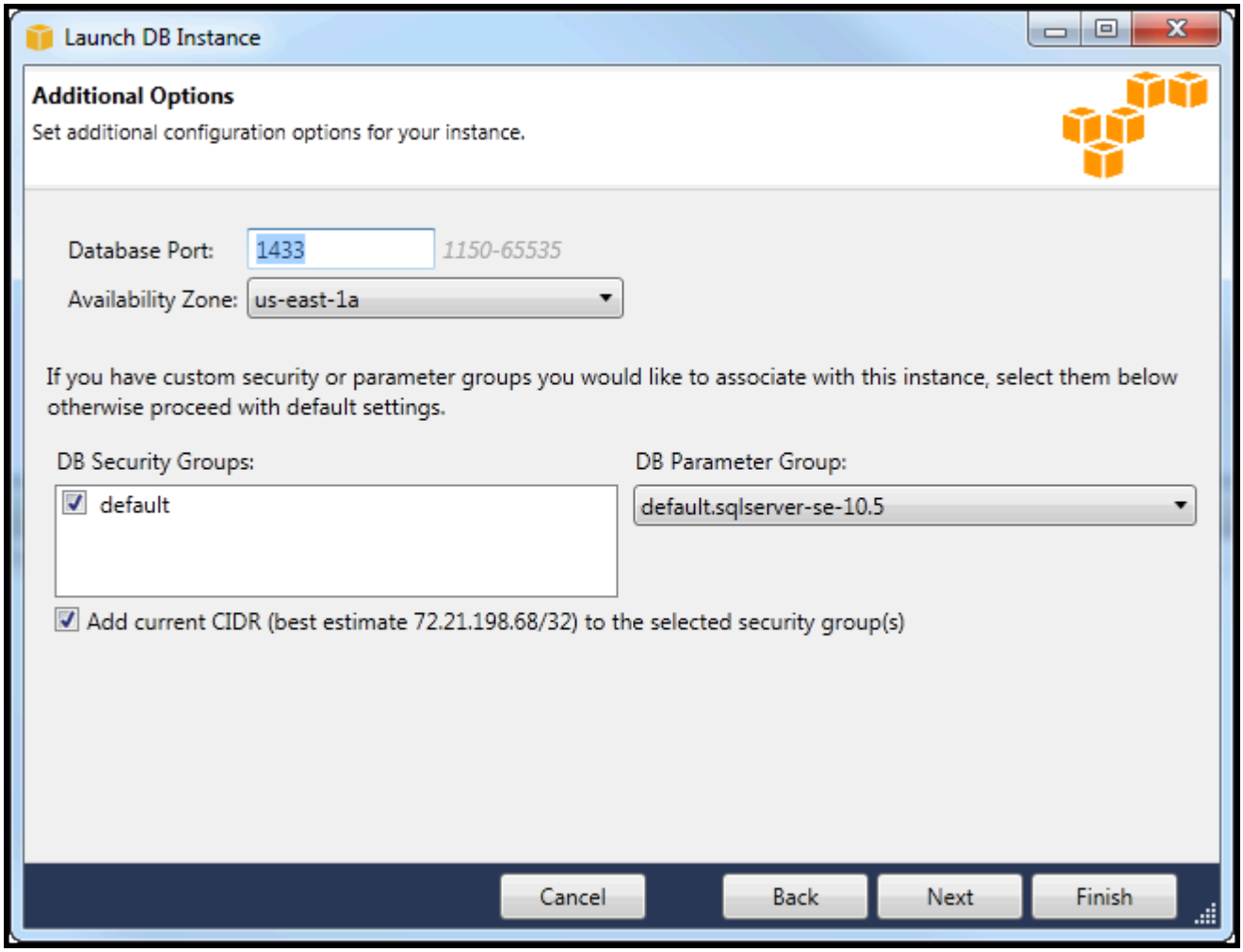
RDS-Sicherheitsgruppe

Wählen Sie eine RDS-Sicherheitsgruppe (oder -gruppen) aus, die mit der Instance verknüpft werden. RDS-Sicherheitsgruppen geben die IP-Adresse, Amazon EC2 EC2-Instances undAWS-Kontendie 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 bestimmen und bietet die Option, diese Adresse den mit Ihrer Instance 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).

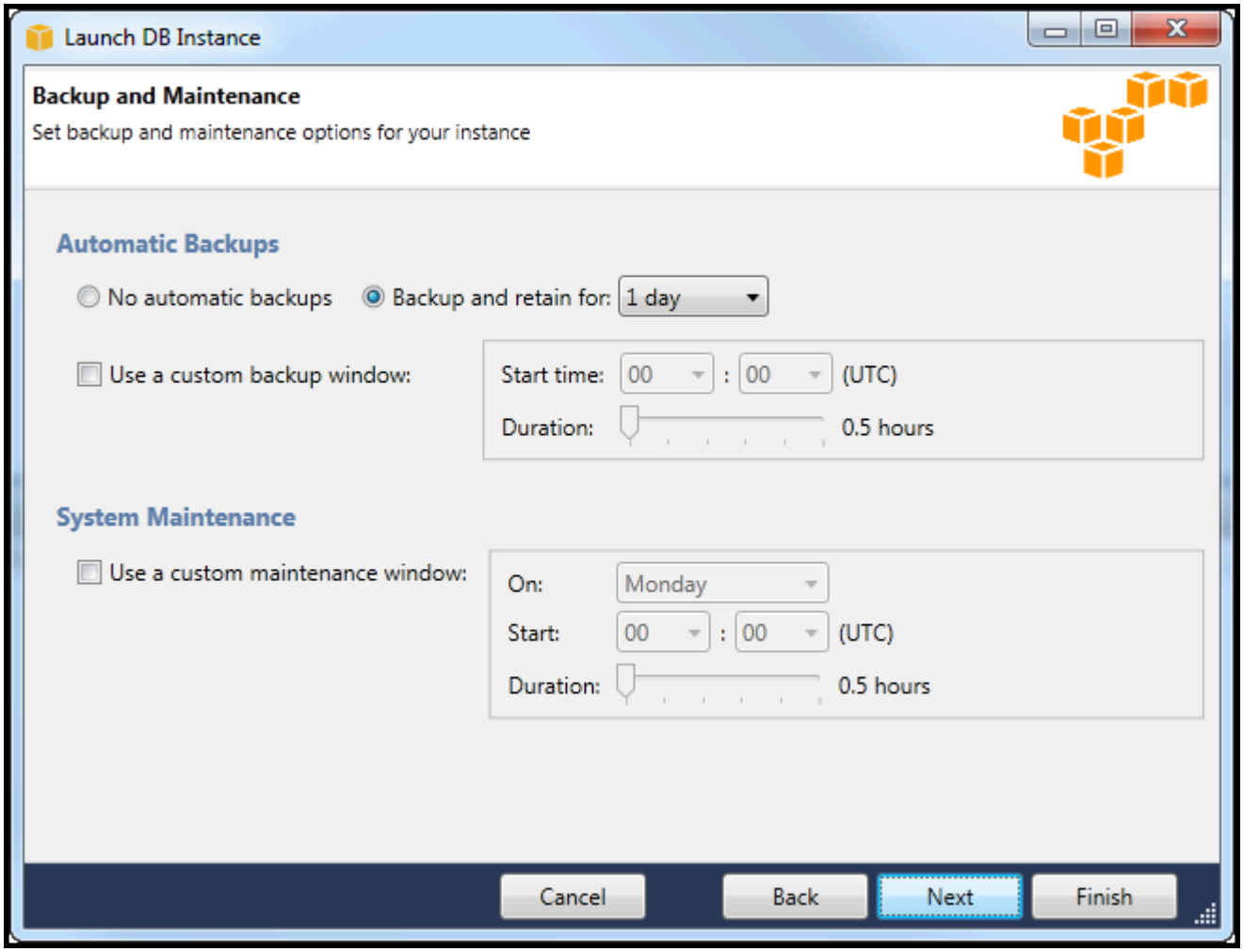


2. DieBackup und WartungIm Dialogfeld können Sie angeben, ob Amazon RDS Ihre Instance sichern soll und wie lange diese Sicherung gespeichert werden soll. Zudem können Sie ein Zeitfenster für die Ausführung der Sicherungen angeben.

   Weiterhin haben Sie die Möglichkeit, in diesem Dialogfeld festzulegen, ob Amazon RDS Systemwartungen auf Ihrer Instance vornehmen 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 Next (Weiter) aus.



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).

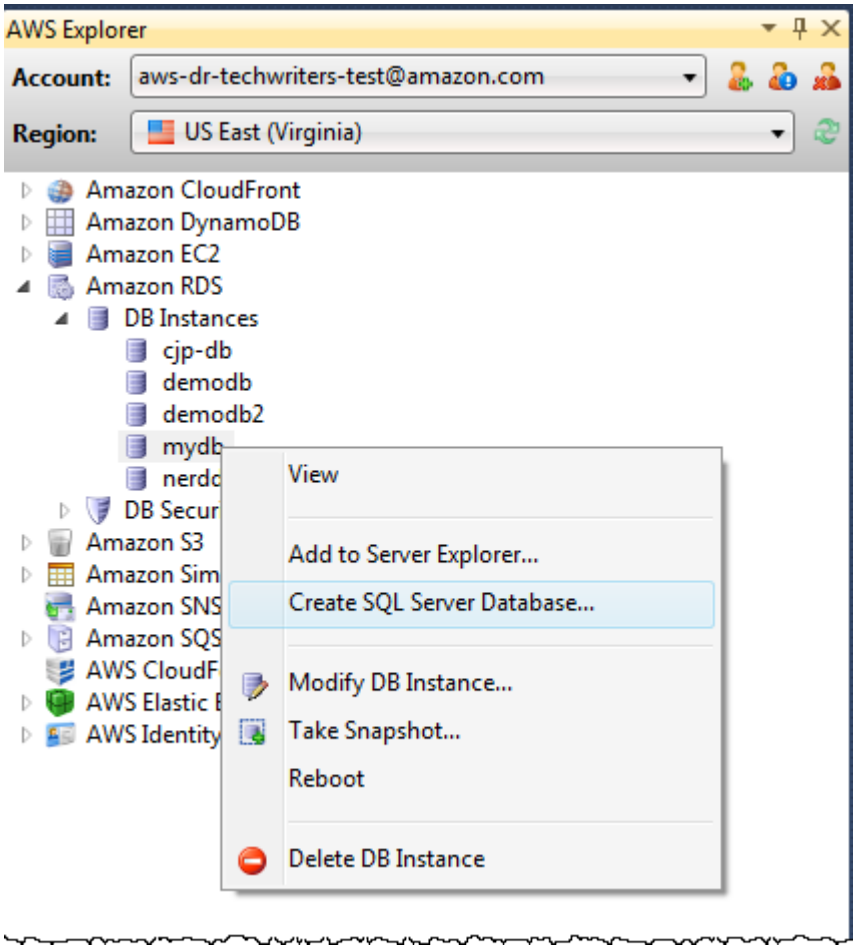
Erstellen einer Microsoft SQL Server-Datenbank in einer RDS-Instance

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

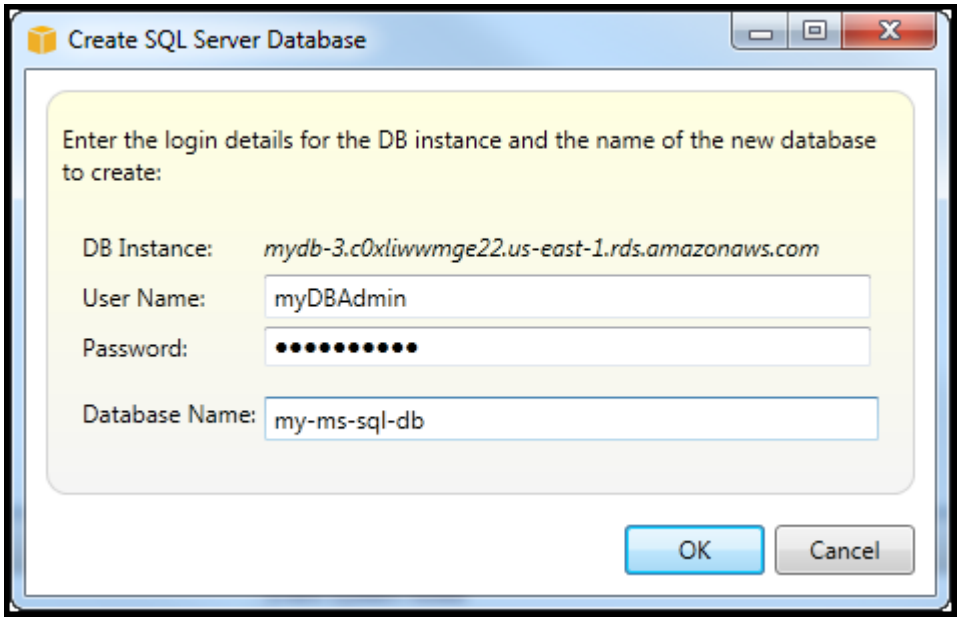
Weitere Informationen zum Erstellen einer Amazon RDS-Instance finden Sie unterStarten einer Amazon RDS-Datenbank-Instanceaus.

So erstellen Sie eine Microsoft SQL Server-Datenbank:

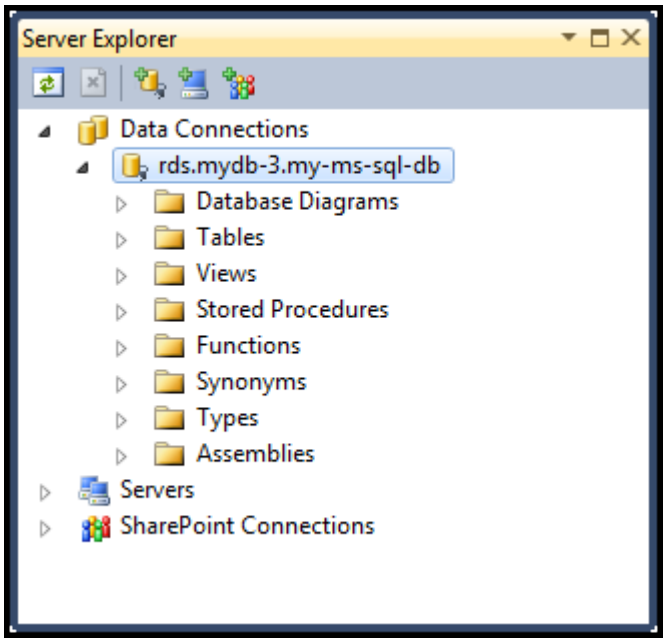
1. In :AWSÖffnen Sie im Explorer das Kontextmenü (rechte Maustaste) für den Knoten Ihrer RDS-Instance für Microsoft SQL Server und klicken Sie dann aufErstellen einer SQL Server-Datenbankaus.



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 daraufhin die Microsoft SQL Server-Datenbank und fügt sie dem Visual Studio Server Explorer hinzu.



Amazon RDS-Sicherheitsgruppen

Amazon RDS-Sicherheitsgruppen ermöglichen Ihnen das Verwalten des Netzwerkzugriffs auf Ihre Amazon RDS-Instances. Mit den Sicherheitsgruppen legen Sie eine Reihe von IP-Adressen mit CIDR-Notation fest, sodass Ihre Amazon RDS-Instance dann ausschließlich den Netzwerkverkehr von diesen Adressen anerkennt.

Die Funktionsweise von Amazon RDS-Sicherheitsgruppen unterscheidet sich zwar, die Sicherheitsgruppen unterscheiden sich zwar, die Gruppen Amazon EC2 sich zwar voneinander. Sie können Ihrer RDS-Sicherheitsgruppe eine EC2-Sicherheitsgruppe hinzufügen. Alle EC2 Instances, die zur EC2-Sicherheitsgruppe gehören, haben dann Zugriff auf die RDS-Instances, die zur RDS-Sicherheitsgruppe gehören.

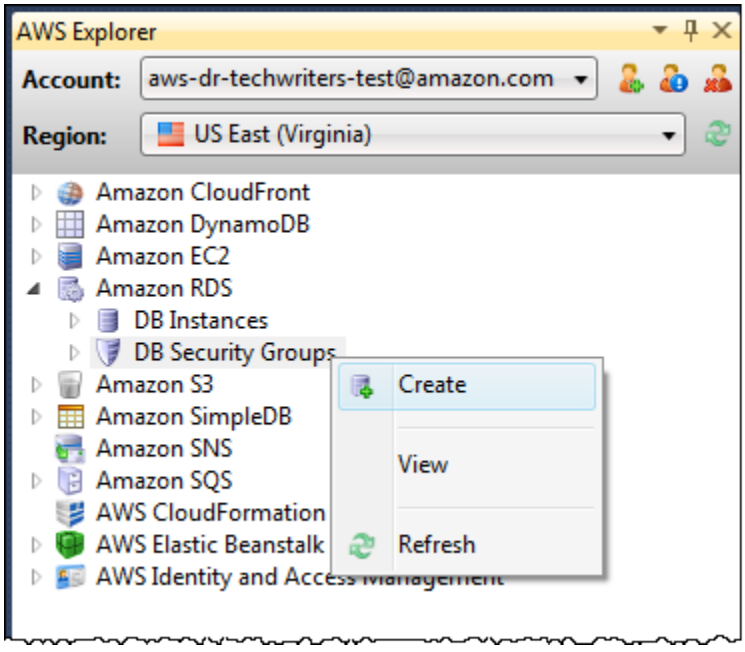
Weitere Informationen zu Amazon RDS-Sicherheitsgruppen finden Sie unterRDS-Sicherheitsgruppenaus. Weitere Informationen zu Amazon EC2-Sicherheitsgruppen finden Sie unterBenutzerhandbuch für EC2aus.

Erstellen Sie eine Amazon RDS-Sicherheitsgruppe

Sie können das Toolkit for Visual Studio verwenden, um eine RDS-Sicherheitsgruppe zu erstellen. Wenn Sie dasAWSMit dem Toolkit zum Starten einer RDS-Instance ermöglicht der Assistent die Möglichkeit, eine RDS-Sicherheitsgruppe für die Verwendung mit Ihrer Instance festzulegen. Mit den folgenden Schritten können Sie diese Sicherheitsgruppe erstellen, bevor Sie den Assistenten starten.

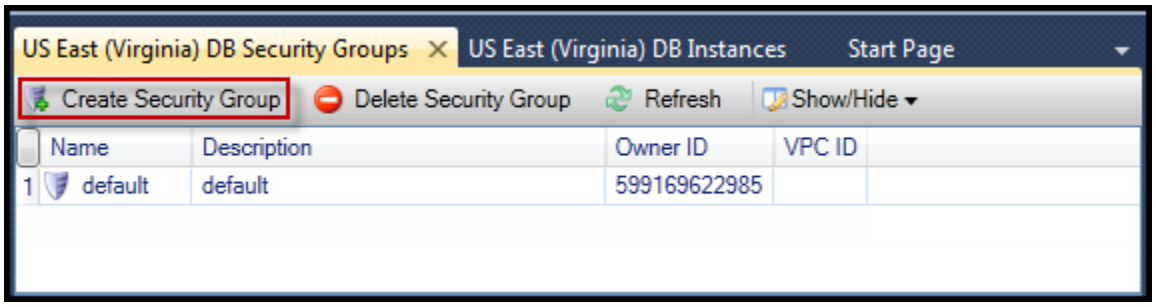
So erstellen Sie eine Amazon RDS-Sicherheitsgruppe:

1. In :AWSExplorer, erweitern Sie dasAmazon RDS-Knoten das Kontextmenü (rechte Maustaste) für dasDB-Sicherheitsgruppenunternoten und wählenGeben Sie einen Namen für den Benutzer ein und klicken Sie dann aufaus.

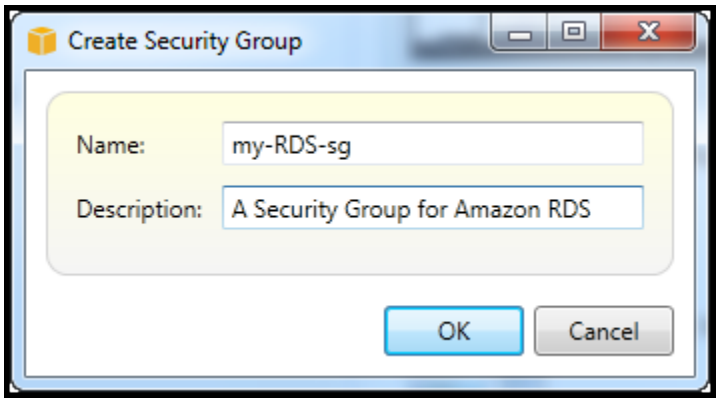


   Alternativ können Sie auf der Registerkarte Security Groups (Sicherheitsgruppen) die Option Create Security Group (Sicherheitsgruppe erstellen) auswählen. Wenn diese Registerkarte nicht

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.



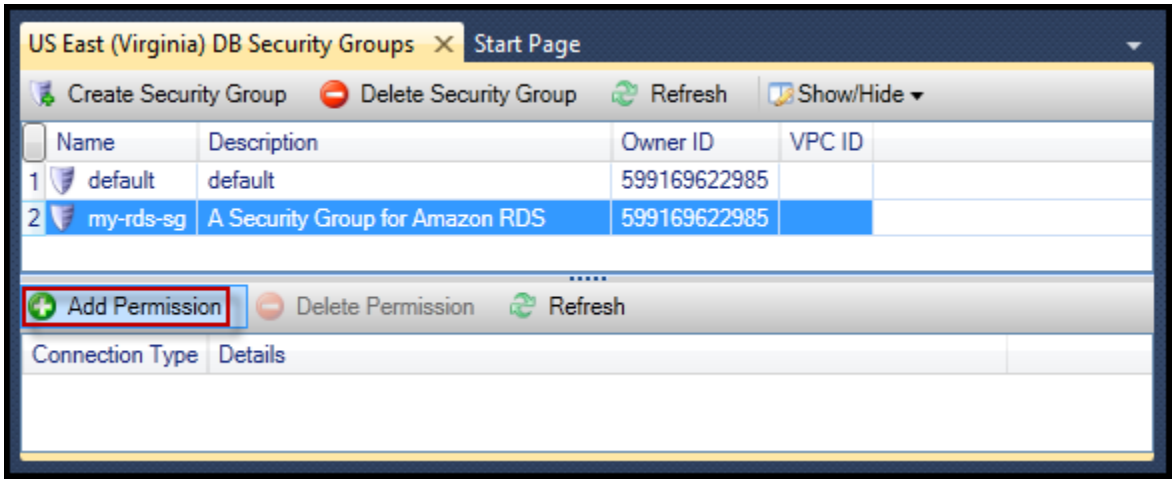
Festlegen von Zugriffsberechtigungen für eine Amazon RDS-Sicherheitsgruppe

Standardmäßig stellt eine neue Amazon RDS-Sicherheitsgruppe keinen Netzwerkzugriff bereit. Um den Zugriff auf Amazon RDS-Instances, die die Sicherheitsgruppe verwenden, zu ermöglichen, führen Sie die folgenden Schritte zur Festlegung der Zugriffsberechtigungen durch.

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

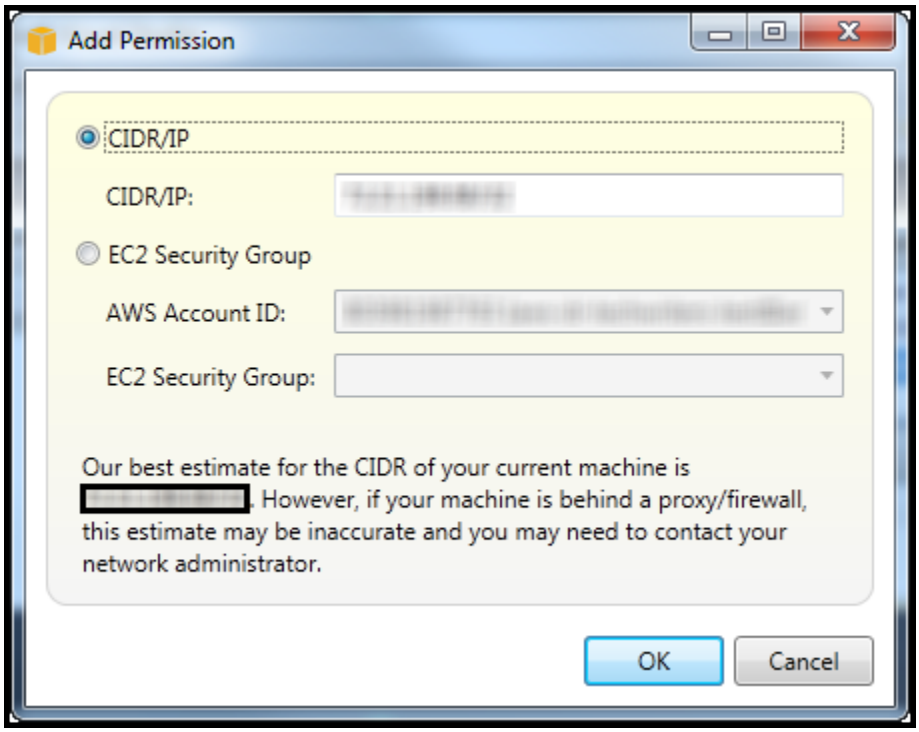
1. Wählen Sie auf der Registerkarte Security Groups (Sicherheitsgruppen) in der Listenansicht die Sicherheitsgruppe aus. Wenn die Sicherheitsgruppe nicht in der Liste angezeigt wird, wählen Sie Refresh (Aktualisieren) aus. Wenn die Sicherheitsgruppe immer noch nicht in der Liste angezeigt wird, überprüfen Sie, ob Sie die Liste für das richtigeAWSRegion. SicherheitsgruppeRegisterkarten imAWSToolkit ist regionsspezifisch.

   Wenn neinSicherheitsgruppeTabs erscheinen, inAWSExplorer, Öffnen Sie das Kontextmenü (rechte Maustaste) für dasDB-Sicherheitsgruppenunternoten und wählenAnzeigenaus.
2. Wählen Sie Add Permission (Berechtigung hinzufügen).



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

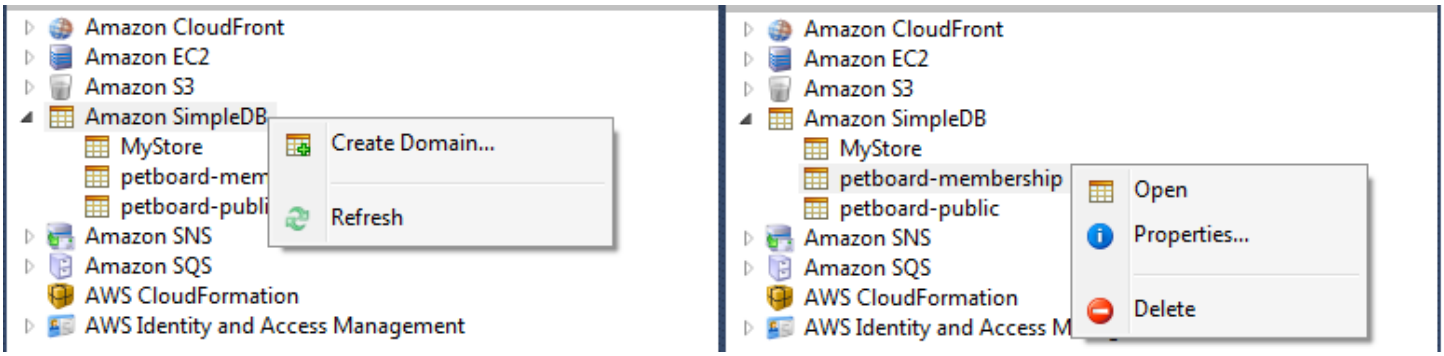
3. Im Dialogfeld Add Permission (Berechtigungen hinzufügen) können Sie CIDR-Notation verwenden, um festzulegen, welche IP-Adressen Zugriff auf Ihre RDS-Instance haben oder welche EC2-Sicherheitsgruppen auf Ihre RDS-Instance zugreifen dürfen. Wenn Sie wählenEC2-Sicherheitsgruppekönnen Sie Zugriff für alle EC2-Instanzen angeben, die mit einemAWS-KontoSie haben Zugriff oder Sie wählen eine EC2-Sicherheitsgruppe aus der Dropdown-Liste aus.



DieAWSToolkit versucht, Ihre IP-Adresse zu bestimmen und gibt automatisch die entsprechende CIDR-Spezifikation in das Dialogfeld ein. Wenn Ihr Computer jedoch über eine Firewall auf das Internet zugreift, ist die vom Toolkit bestimmte CIDR möglicherweise nicht korrekt.

Verwenden von Amazon SimpleDBAWSExplorer

AWSDer AV Explorer zeigt alle mit dem aktiven verknüpften Amazon SimpleDB -Domänen anAWSKonto. AusAWSSie können Amazon SimpleDB -Domänen erstellen oder löschen.

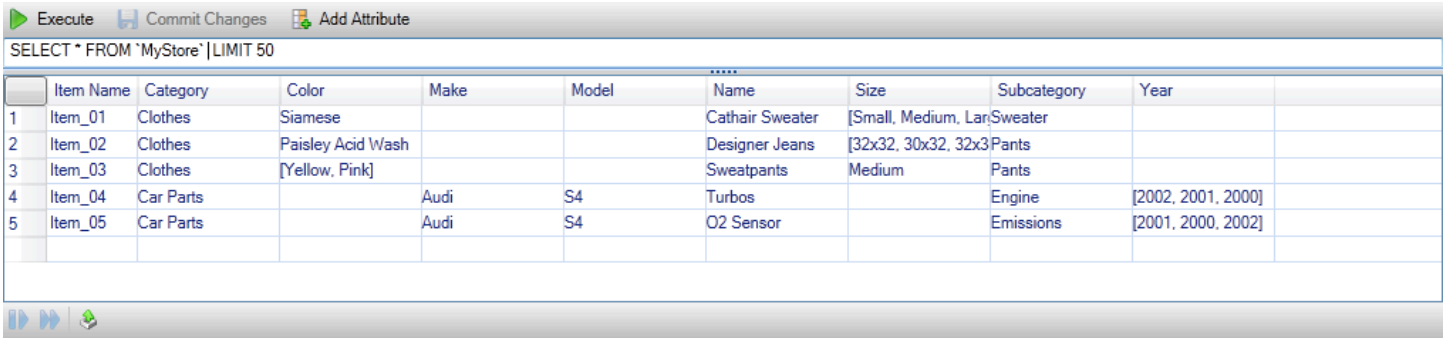


Create, delete, or open Amazon SimpleDB domains associated with your account

Ausführen von Abfragen und Bearbeiten der Ergebnisse

AWSDer Aaster kann -Domänen auch als Raster anzeigen, in denen Sie Elemente, Attribute und Wert in dieser Domäne einsehen 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.

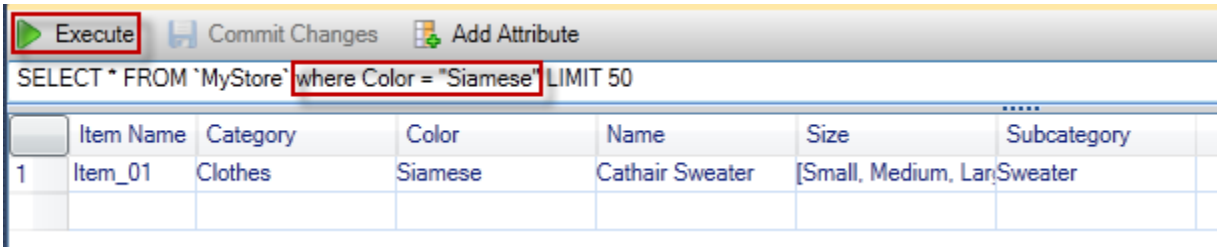
Die hier angezeigte Domäne stammt aus dem Amazon SimpleDB -Beispiel, das imAWS SDK for .NETaus.



	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.

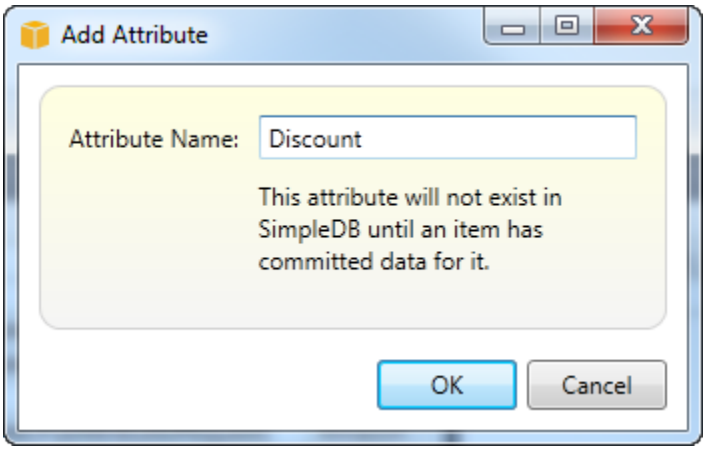


Execute query from AWS Explorer

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.

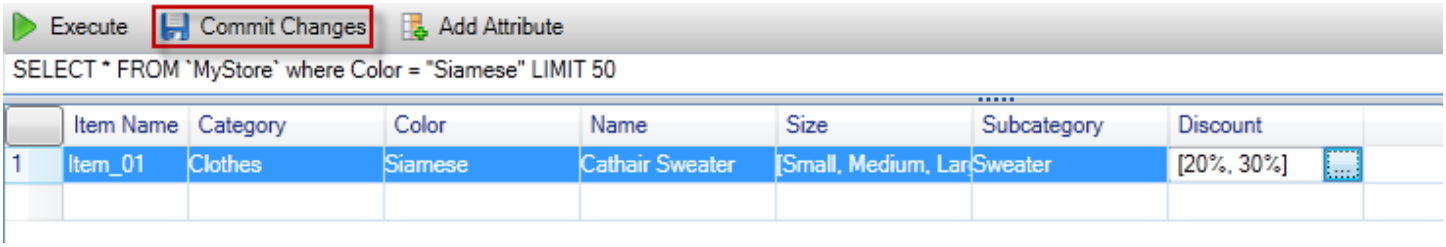
Hinzufügen eines Attributs

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



Hinzufügen von Attribut 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.

Verwenden von Amazon SQSAWSExplorer

Amazon Simple Queue Service (Amazon SQS) ist ein flexibler Warteschlangenservice, der die Weitergabe von Mitteilungen zwischen unterschiedlichen Ausführungsprozessen in einer Softwareanwendung ermöglicht. Amazon SQS SQS-Warteschlangen befinden sich imAWSInfrastruktur, aber die Prozesse, die Nachrichten übergeben, können lokal vorhanden sein, sich auf Amazon EC2 EC2-Instances befinden oder aus einer Kombination dieser beiden Optionen bestehen. Amazon SQS eignet sich ideal zum Koordinieren der Aufgabenverteilung auf mehrere Computer.

Das Toolkit for Visual Studio ermöglicht es Ihnen, Amazon SQS SQS-Warteschlangen, die mit dem aktiven Konto verknüpft sind, anzuzeigen und Warteschlangen zu erstellen oder zu löschen. Darüber hinaus besteht die Möglichkeit, Mitteilungen über Warteschlangen zu senden. (Mit „aktivem Konto“ ist das inAWS-Explorer.)

Weitere Informationen zu Amazon SQS finden Sie unterEinführung in SQSimAWS-Dokumentation.

Erstellen einer Warteschlange

Sie können eine Amazon SQS SQS-Warteschlange erstellenAWS-Explorer. 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. In :AWSÖffnen Sie das Kontextmenü (rechte Maustaste) für dasAmazon SQS-Knoten, und wählen Sie dannErstellen einer Warteschlangeaus.
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. Klicken Sie auf OK. Die neue Warteschlange erscheint als Subknoten unter dem Amazon SQS-Knoten.

Löschen einer Warteschlange

Sie können vorhandene Warteschlangen löschenAWS-Explorer. Wenn Sie eine Warteschlange löschen, ist keine der mit dieser Warteschlange verknüpften Mitteilungen mehr verfügbar.

So löschen Sie eine Warteschlange

1. In :AWSÖffnen Sie im Explorer die Kontextmenüs (rechte Maustaste) für die Warteschlange, die Sie löschen möchten, und wählen Sie dann ausLöschenaus.

Verwalten von Warteschlangeneigenschaften

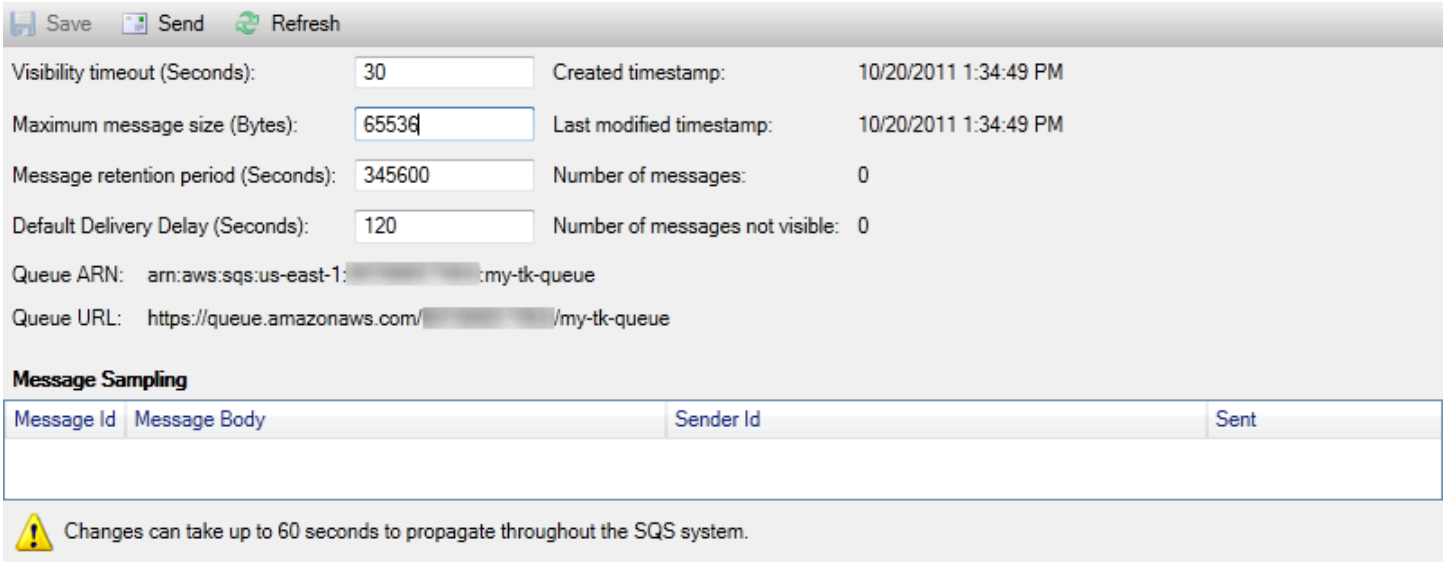
Sie können die Eigenschaften jeder der in angezeigten Warteschlangen ansehen und bearbeitenAWS-Explorer. Außerdem können Sie in dieser Eigenschaftenansicht Mitteilungen an die Warteschlange senden.

So verwalten Sie Warteschlangeneigenschaften:

- In :AWSÖffnen Sie das Kontextmenü (rechte Maustaste) für die Warteschlange, deren Eigenschaften Sie verwalten möchten, und wählen Sie dann ausAnzeigen der Warteschlangeaus.

  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.



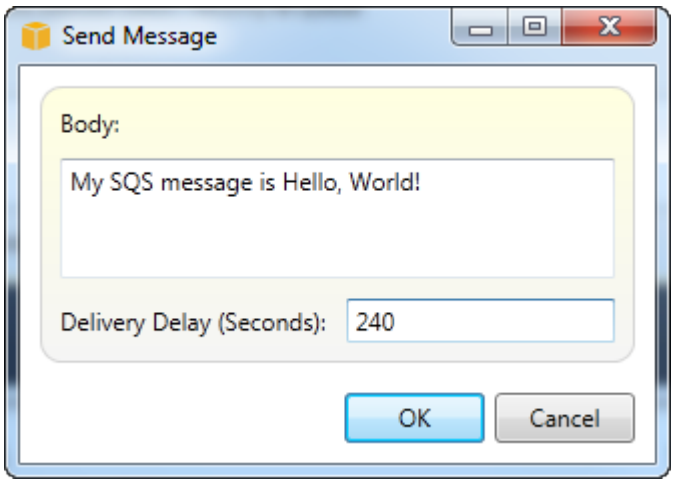
SQS queue properties view

Senden einer Mitteilung an eine Warteschlange

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

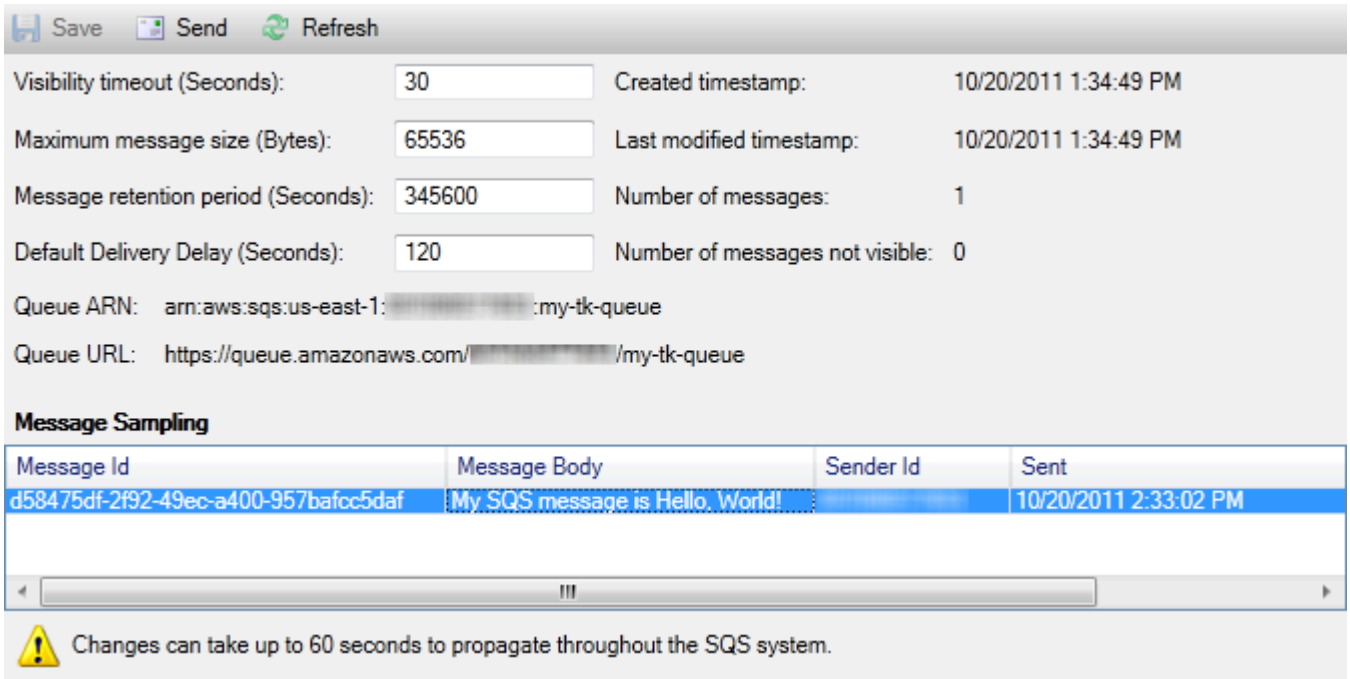
So senden Sie eine Nachricht

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 Klicken Sie auf OK.



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.

Identity and Access Management

AWS Identity and Access ManagementMit (IAM) können Sie den Zugriff auf IhreAWS-Kontenund Ressourcen. Mit IAM können Sie mehrere Benutzer in Ihrem primären Objekt erstellen (Wurzel)AWS-Kontoaus. Diese Benutzer können eigene Anmeldeinformationen (Passwort, Zugriffsschlüssel-ID und geheimen Schlüssel) erhalten, aber alle IAM-Benutzer verwenden dieselbe Kontonummer.

Sie können die Zugriffsebene aller IAM-Benutzer auf eine Ressource verwalten, indem Sie IAM-Richtlinien für den Benutzer anfügen. Sie können beispielsweise einem IAM-Benutzer eine Richtlinie zuweisen, die ihm Zugriff auf den Amazon S3 S3-Dienst und die zugehörigen Ressourcen in Ihrem Konto gewährt, aber nicht auf andere Services oder Ressourcen.

Für eine noch 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 von IAM-Rollen. Wie Benutzer und Gruppen können Sie IAM-Rollen Richtlinien zuweisen. Dann können Sie die IAM-Rolle einer Amazon EC2 Instance zuordnen. Anwendungen, die auf der EC2 Instance ausgeführt werden, können zugreifenAWSVerwenden der von der -IAM-Rolle bereitgestellten Berechtigungen. Weitere Informationen zum Verwenden von IAM-Rollen mit dem Toolkit finden Sie unter Create an IAM Role. Weitere Informationen über IAM finden Sie im.IAM User Guideaus.

Erstellen und Konfigurieren eines IAM-Benutzers

Mit IAM-Benutzern können Sie anderen Benutzern Zugriff auf IhreAWS-Kontoaus. 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.

Als bewährte Methode können alle Benutzer, die Zugriff auf eineAWS-Kontosollte dies als IAM-Benutzer tun — auch der Eigentümer des Kontos. Auf diese Weise wird sichergestellt, dass bei einer Kompromittierung der Anmeldeinformationen eines IAM-Benutzers ausschließlich diese Anmeldeinformationen deaktiviert werden müssen. Es ist nicht notwendig, die Root-Anmeldeinformationen für das Konto zu deaktivieren oder zu ändern.

Sie können vom Toolkit for Visual Studio aus einem IAM-Benutzer Berechtigungen zuweisen, indem Sie eine IAM-Richtlinie für den Benutzer anfügen oder den Benutzer einer Gruppe zuweisen. IAM-Benutzer, die einer Gruppe zugewiesen sind, erhalten alle Berechtigungen von den Richtlinien, die

der Gruppe zugeordnet 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).

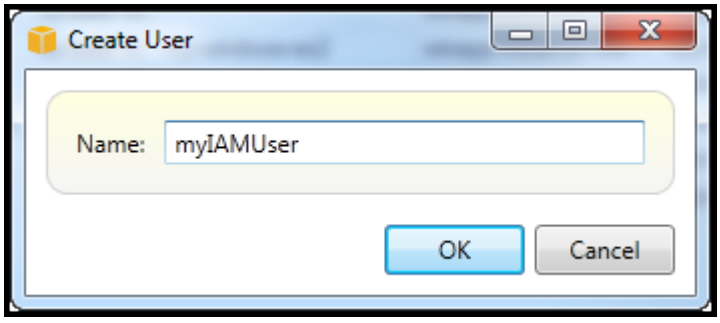
Sie können über das Toolkit for Visual Studio auch generierenAWSAnmeldeinformationen (Zugriffsschlüssel-ID und geheimer Schlüssel) für den IAM-Benutzer. Weitere Informationen finden Sie unter Generate Credentials for an IAM User.

Das Toolkit for Visual Studio unterstützt die Angabe der IAM-Benutzeranmeldeinformationen für den Zugriff auf Services imAWSExplorer. Da IAM-Benutzer normalerweise nicht über vollständigen Zugriff auf alle Amazon Web Services verfügen, finden einige der Funktionen inAWSDer Explorer ist möglicherweise nicht verfügbar. Wenn SieAWSExplorer, um Ressourcen zu ändern, während das aktive Konto ein IAM-Benutzer ist, und dann das aktive Konto in das Root-Konto ändern, werden die Änderungen erst sichtbar, wenn Sie die Ansicht in aktualisierenAWSExplorer. Um die Anzeige zu aktualisieren, wählen Sie die Schaltfläche „Refresh ()“ aus.

Weitere Informationen zum Konfigurieren von IAM-Benutzern aus demAWS Management Console, navigieren Sie zuArbeiten mit Benutzern und Gruppenim IAM User Guide.

So erstellen Sie einen IAM-Benutzer

1. In :AWSExplorer, erweitern Sie dasAWS Identity and Access ManagementÖffnen Sie das Kontextmenü (rechte Maustaste) fürBenutzerKlicken Sie auf und danach aufBenutzer erstellenaus.
2. In derBenutzer erstellenGeben Sie einen Namen für den IAM-Benutzer ein und wählen Sie dannOKAYaus. Das ist das IAMfreundlicher Nameaus. Weitere Informationen zu Einschränkungen bei Namen für IAM-Benutzer finden Sie unterIAM User Guideaus.



Create an IAM user

Der neue Benutzer erscheint als Subknoten unterBenutzerunter demAWS Identity and Access Management-Knoten.

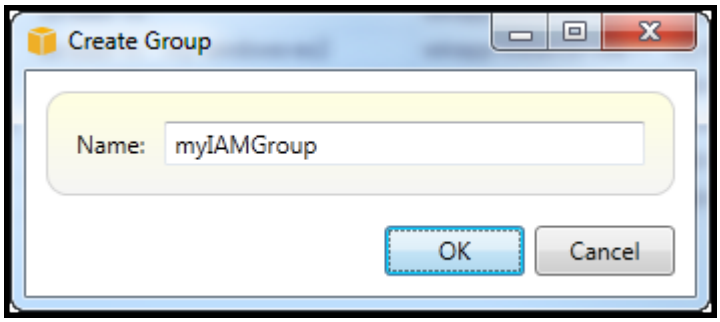
Informationen zum Erstellen einer Richtlinie und zum Zuweisen dieser zu einem Benutzer finden Sie unter Create an IAM Policy.

Erstellen einer IAM-Gruppe

Gruppen bieten eine Möglichkeit, IAM-Richtlinien auf eine Anzahl von Benutzern anzuwenden. Weitere Informationen zum Verwalten von IAM-Benutzern und -Gruppen finden Sie unterArbeiten mit Benutzern und Gruppenim IAM User Guide.

So erstellen Sie eine IAM-Gruppe

1. In :AWSExplorer unterIdentity and Access Managementöffnen Sie das Kontextmenü (rechte Maustaste) für-Gruppenund wähleErstellen einer -Gruppeaus.
2. In derErstellen einer -GruppeGeben Sie einen Namen für die IAM-Gruppe ein und wählen Sie dannOKAYaus.



Create IAM group

Die neue IAM-Gruppe wird unter der-GruppenUnterknoten vonIdentity and Access Managementaus.

Weitere Informationen zum Erstellen einer Richtlinie und zum Zuweisen dieser zu einer IAM-Gruppe finden Sie unterErstellen einer IAM-Richtlinieaus.

Hinzufügen eines IAM-Benutzers zu einer IAM-Gruppe

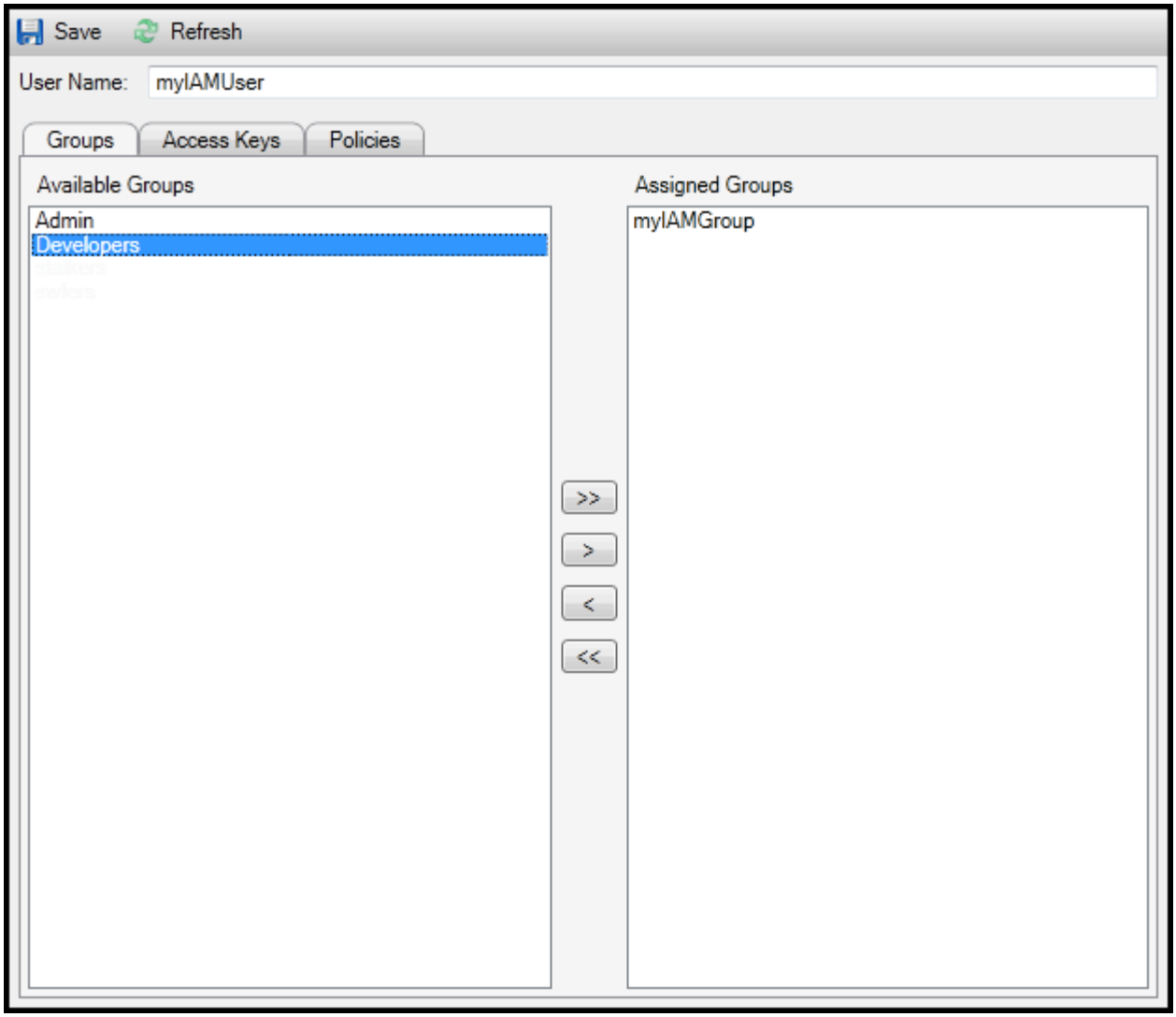
IAM-Benutzer, die Mitglieder einer IAM-Gruppe sind, erhalten alle Zugriffsberechtigungen von den Richtlinien, die der Gruppe zugeordnet sind. Eine IAM-Gruppe soll das Verwalten von Berechtigungen für mehrere IAM-Benutzer vereinfachen.

Weitere Informationen dazu, wie die Richtlinien einer IAM-Gruppe gegenüber denen ausgewertet werden, die IAM-Benutzern in der IAM-Gruppe direkt zugewiesen sind, finden Sie unterVerwalten von IAM-Richtlinien im IAM-Benutzerhandbuchaus.

In :AWSIm Explorer fügen Sie IAM-Gruppen IAM-Gruppen aus demBenutzerUnterknoten, nicht der-GruppenUnterknoten.

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

1. In :AWSExplorer unterIdentity and Access Managementöffnen Sie das Kontextmenü (rechte Maustaste) fürBenutzerund wähleBearbeitenaus.



Assign an IAM user to a IAM group

2. Das linke Fenster des-Gruppenzeigt die verfügbaren IAM-Gruppen an. Im rechten Bereich werden die Gruppen angezeigt, in denen der angegebene IAM-Benutzer bereits Mitglied ist.

   Um einer Gruppe einen IAM-Benutzer hinzuzufügen, wählen Sie im linken Bereich die IAM-Gruppe und dann die Option>Schaltfläche.

Um einen IAM-Benutzer aus einer Gruppe zu entfernen, wählen Sie im rechten Bereich die IAM-Gruppe und dann die Option<Schaltfläche.

Um den IAM-Benutzer allen IAM-Gruppen zuzuweisen, wählen Sie das>>Schaltfläche. Entsprechend entfernen Sie den IAM-Benutzer aus allen Gruppen, indem Sie die Option<<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 das Zuweisen des IAM-Benutzers zu IAM-Gruppen abgeschlossen haben, wählen SieSaveaus.

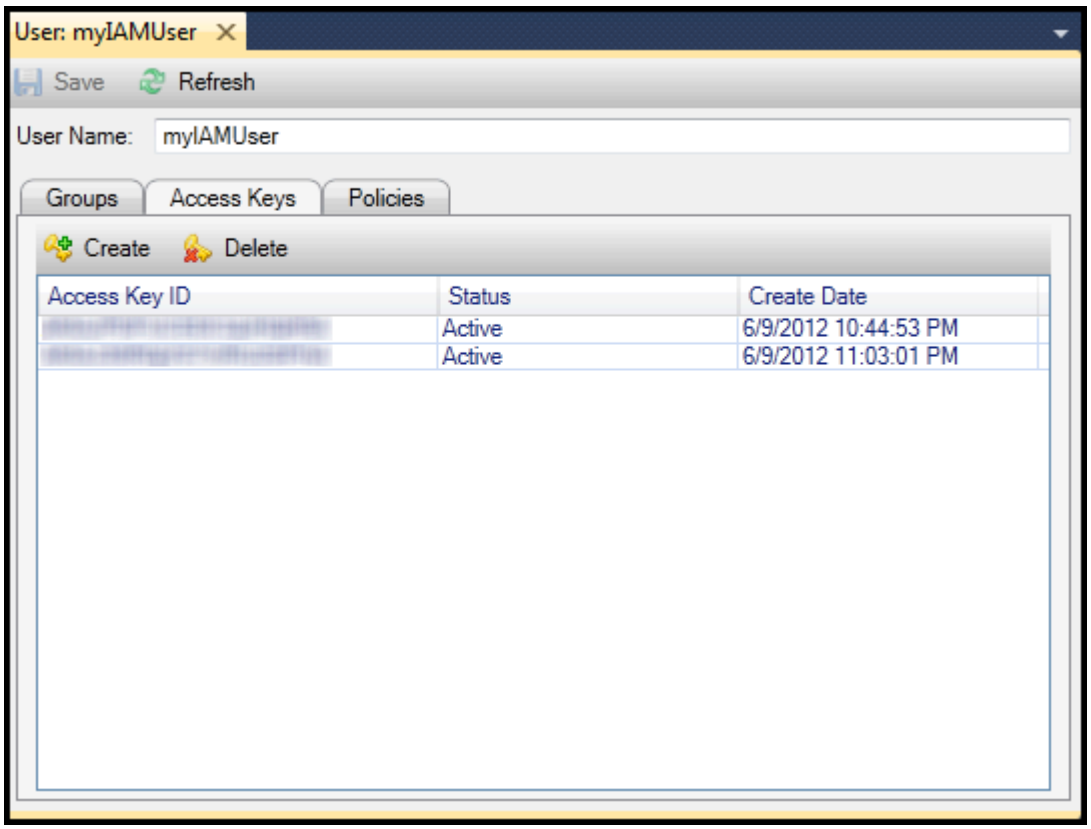
Generieren von Anmeldeinformationen für einen IAM-Benutzer

Mit Toolkit for Visual Studio können Sie die Zugriffsschlüssel-ID und den geheimen Schlüssel für API-Aufrufe für generierenAWSaus. Diese Schlüssel können über das Toolkit auch für den Zugriff auf Amazon Web Services 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 unterBewährte Methoden zum VerwaltenAWSZugriffsschlüsselaus.

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

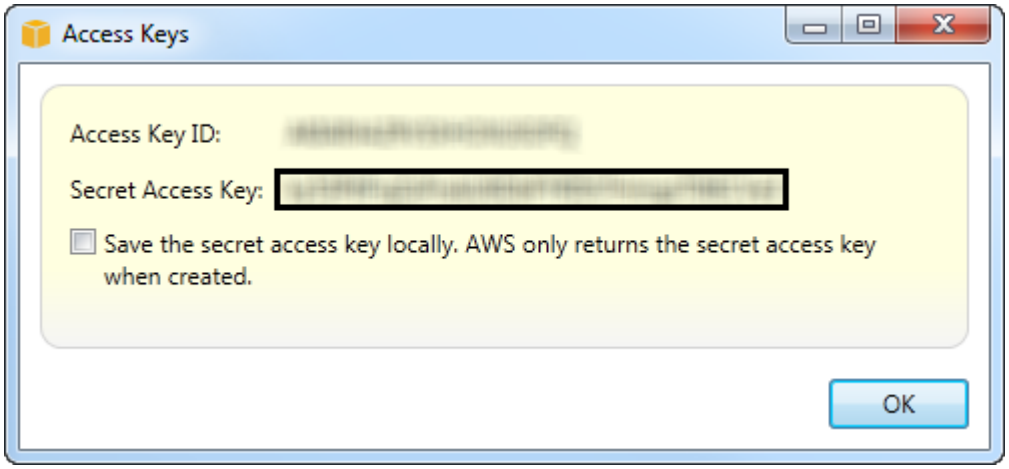
So generieren Sie Anmeldeinformationen für einen IAM-Benutzer

1. In :AWSExplorer öffnen Sie das Kontextmenü (rechte Maustaste) für einen IAM-Benutzer und wählenBearbeitenaus.



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.

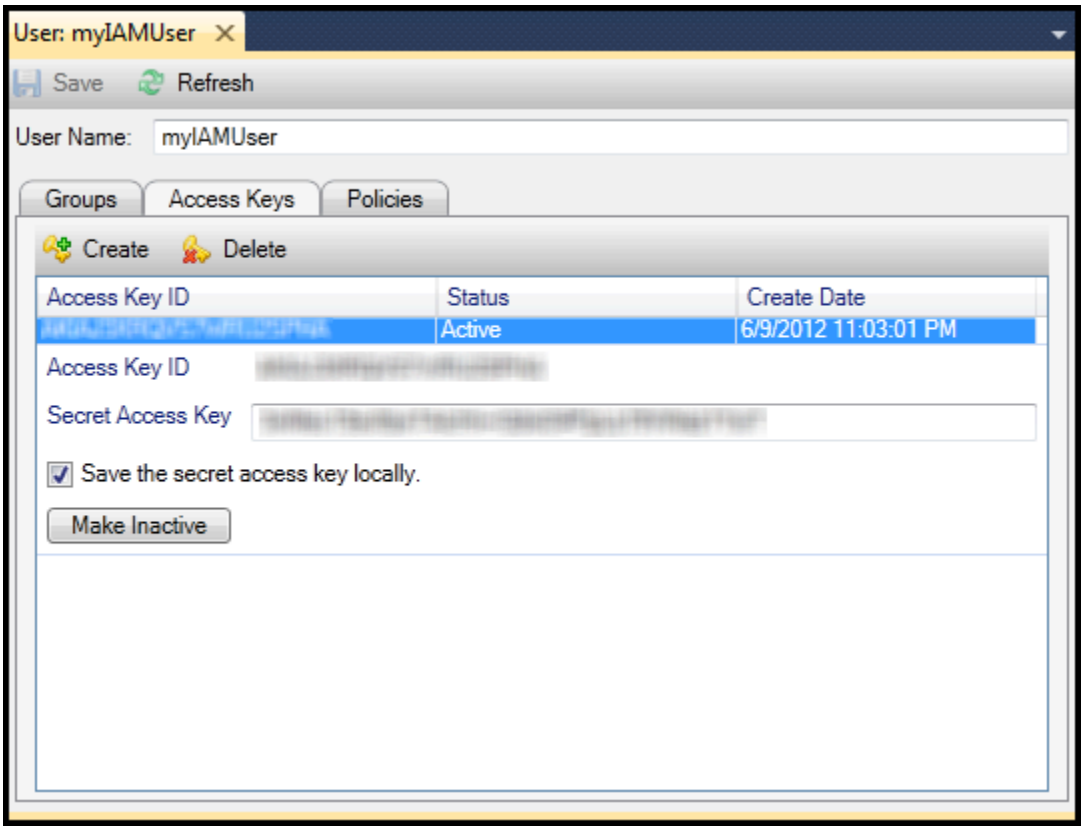


   reate credentials for IAM user

Wenn Sie möchten, dass das Toolkit eine verschlüsselte Kopie Ihres geheimen Zugriffsschlüssels auf dem lokalen Laufwerk speichert, wählen SieSpeichern Sie den geheimen Zugriffsschlüssel lokal.AWSGibt den geheimen Zugriffsschlüssel nur zurück, wenn dieser erstelltaus. Sie können den geheimen Zugriffsschlüssel auch im Dialogfeld kopieren und an einem sicheren Ort speichern.

3. Klicken Sie auf OK.

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. (Verwenden Sie diese Option, wenn Sie vermuten, dass die Anmeldeinformationen kompromittiert wurden. Sie

können die Anmeldeinformationen reaktivieren, wenn Sie sich vergewissert haben, dass sie sicher sind.)

Erstellen einer IAM-Rolle

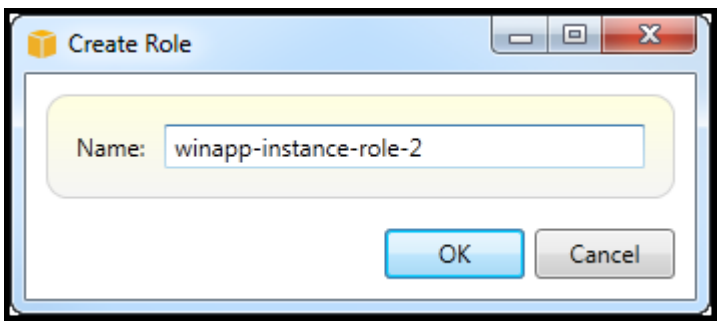
Das Toolkit for Visual Studio unterstützt die Erstellung und Konfiguration von IAM-Rollen. Wie Benutzer und Gruppen können Sie auch IAM-Rollen Richtlinien zuweisen. Dann können Sie die IAM-Rolle einer Amazon EC2 Instance zuordnen. Die Zuordnung zur EC2 Instance wird über ein Instance-Profil verwaltet. Dabei handelt es sich um einen logischen Container für die Rolle. Anwendungen, die in der EC2 Instance automatisch werden, erhalten den durch die Richtlinien für die IAM-Rolle angegebenen Zugriff. Dies gilt auch, wenn die Anwendung keine anderen angegeben wurdeAWS-Anmeldeinformationen.

Sie können beispielsweise eine Rolle erstellen und dieser eine Richtlinie zuweisen, die den Zugriff auf Amazon S3 beschränkt. Nach dem Zuweisen dieser Rolle zu einer EC2 Instance können Sie eine Anwendung in dieser Instance ausführen. Die Anwendung erhält Zugriff auf Amazon S3, aber nicht auf andere Services oder Ressourcen. Dieser Ansatz hat den Vorteil, dass Sie sich nicht um die sichere Übertragung und Speicherung kümmern müssenAWSAnmeldeinformationen für die EC2-Instance.

Weitere Informationen über IAM-Rollen finden Sie unterArbeiten mit IAM-Rollen im IAM-Benutzerhandbuchaus. Für Beispiele für Programme, die darauf zugreifenAWSVerwenden Sie die IAM-Rolle, die mit einer Amazon EC2 EC2-Instance verknüpft ist, gehen Sie zurAWSEntwicklerhandbücher fürJava,.NET,PHPund Ruby (Festlegen von Anmeldeinformationen mithilfe von IAM,Erstellen einer IAM-Rolle, undArbeiten mit IAM-Richtlinien) enthalten.

So erstellen Sie eine IAM-Rolle

1. In :AWSExplorer unterIdentity and Access Managementöffnen Sie das Kontextmenü (rechte Maustaste) fürRollenKlicken Sie auf und danach aufErstellen von -Rollenaus.
2. In derErstellen einer -RolleGeben Sie einen Namen für die IAM-Rolle ein und wählen Sie dannOKAYaus.



Create IAM role

Die neue IAM-Rolle erscheint unterRolleninIdentity and Access Managementaus.

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

Erstellen einer IAM-Richtlinie

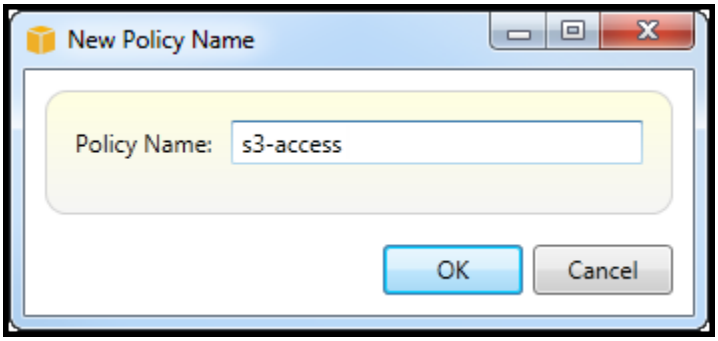
Richtlinien sind elementare Funktionen von IAM. Richtlinien können mit IAM verknüpft werdenEntitätenwie Benutzer, Gruppen oder Rollen. Richtlinien geben die Zugriffsebene für einen Benutzer, eine Gruppe oder eine Rolle an.

So erstellen Sie eine IAM-Richtlinie

In :AWSExplorer, erweitern Sie dasAWS Identity and Access Management-Knoten, erweitern Sie dann den Knoten für den Typ der Entität (-Gruppen,Rollen, oderBenutzer), an die Sie die Richtlinie anhängen. Öffnen Sie beispielsweise ein Kontextmenü für eine IAM-Rolle und wählen Sie dannBearbeitenaus.

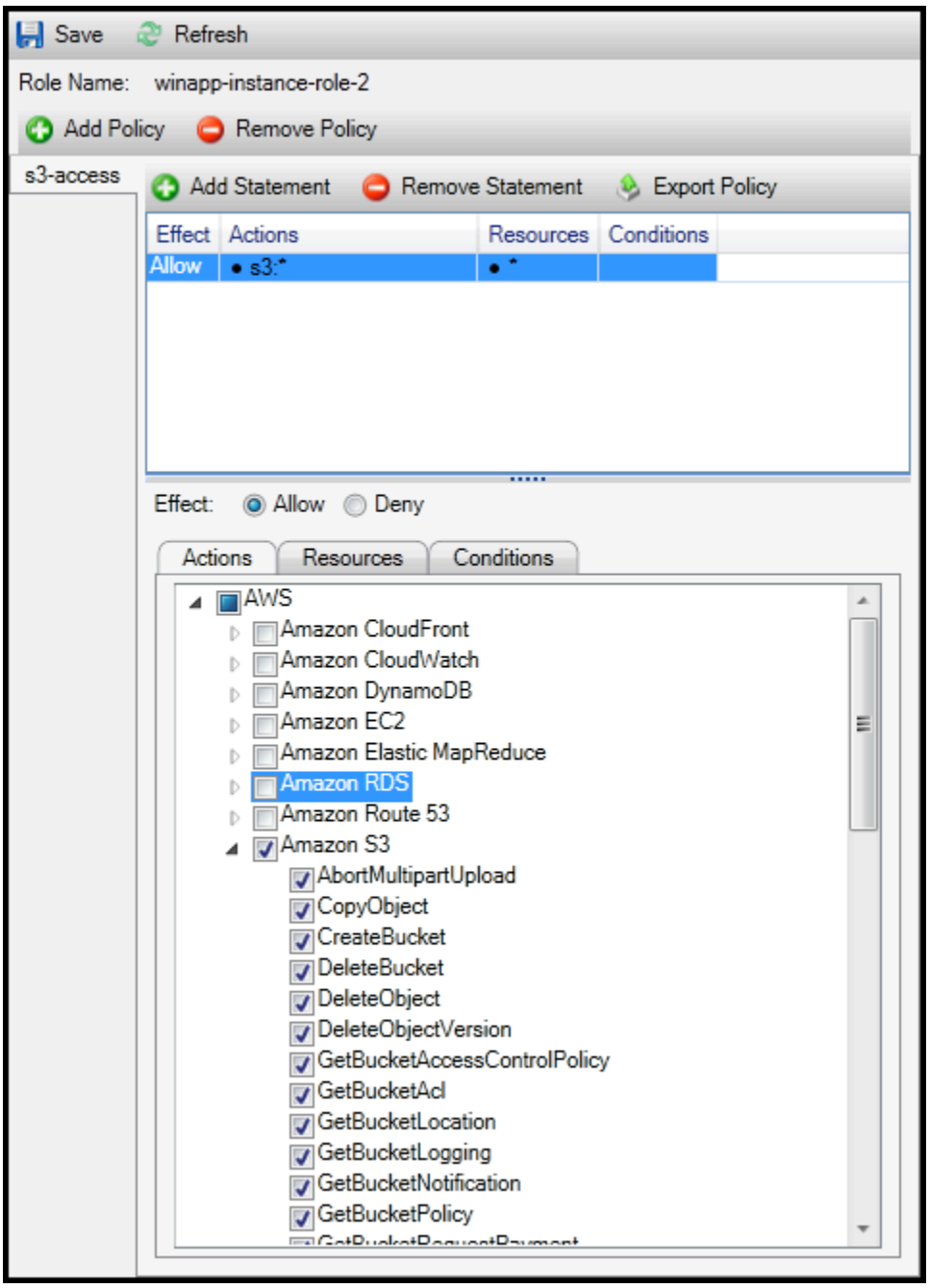
Eine Registerkarte, die mit der Rolle verknüpft ist, wird im Register angezeigtAWSExplorer. Wählen Sie den Link Add Policy (Richtlinie hinzufügen) aus.

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 Richtlinien-Editor Richtlinienanweisungen hinzu, um die Zugriffsebene für die Rolle (in diesem Beispiel winapp-instance-role-2), der die Richtlinie zugewiesen ist, festzulegen. In diesem Beispiel gewährt eine Richtlinie vollständigen Zugriff auf Amazon S3, aber keinen Zugriff auf andere Ressourcen.



Specify IAM policy

Für eine noch genauere Zugriffssteuerung erweitern Sie die Unterknoten im Richtlinien-Editor, um Aktionen im Zusammenhang mit Amazon Web Services zuzulassen oder zu untersagen.

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 AWS Lambda dazu 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
- AWS Lambda Basisprojekt: Docker-Image erstellen
- Tutorial: Erstellen und Testen einer serverlosen Anwendung mit AWS Lambda
- Tutorial: Erstellen einer Amazon Rekognition-Lambda-Anwendung
- Tutorial: Verwenden von Amazon Logging Frameworks mit AWS Lambda zum Erstellen von Anwendungsprotokollen

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#) aus.
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`

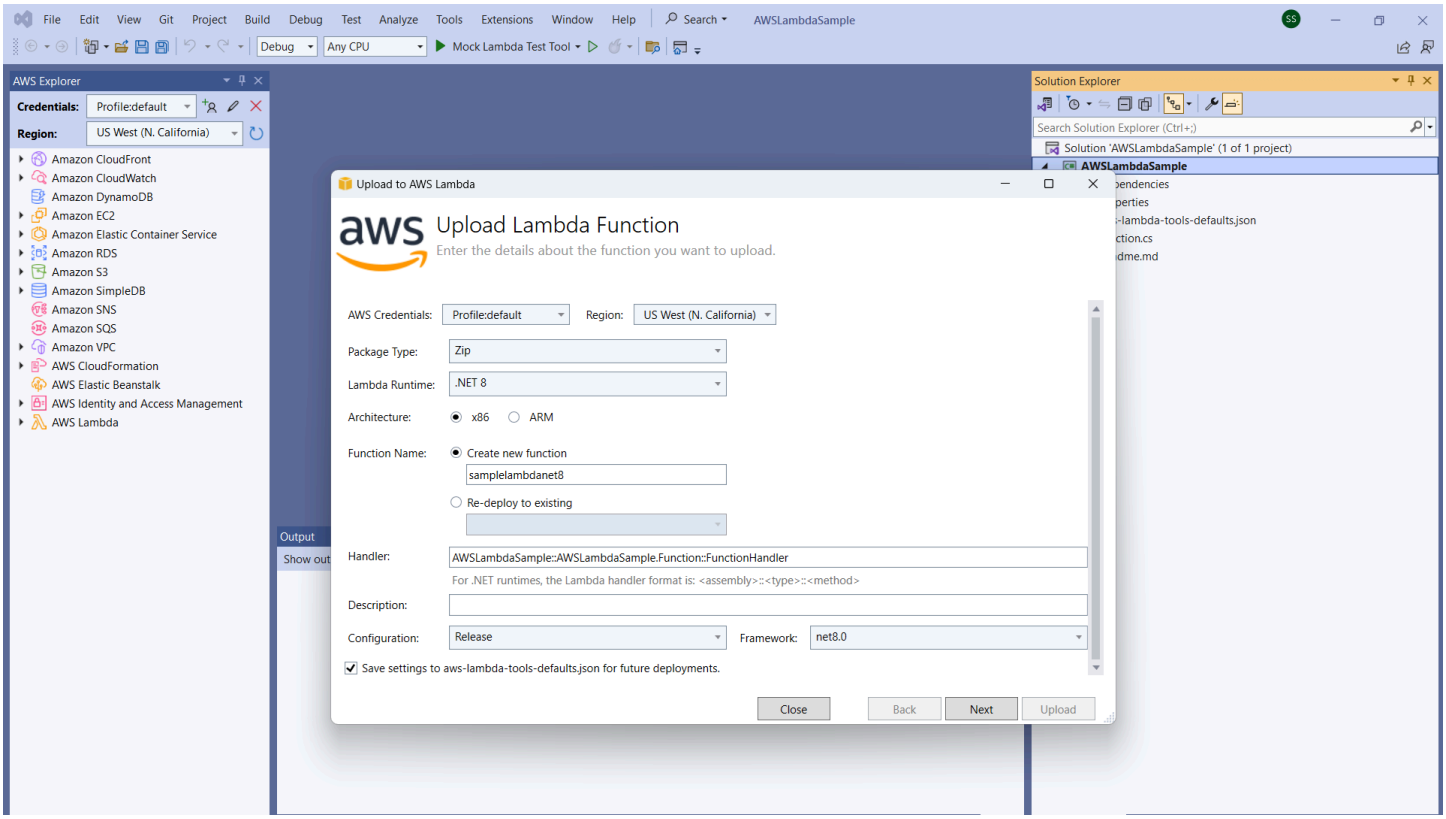
```
{
  "Information": [
    "This file provides default values for the deployment wizard inside Visual Studio
 and the AWS Lambda commands added to the .NET Core CLI.",
    "To learn more about the Lambda commands with the .NET Core CLI execute the
 following command at the command line in the project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

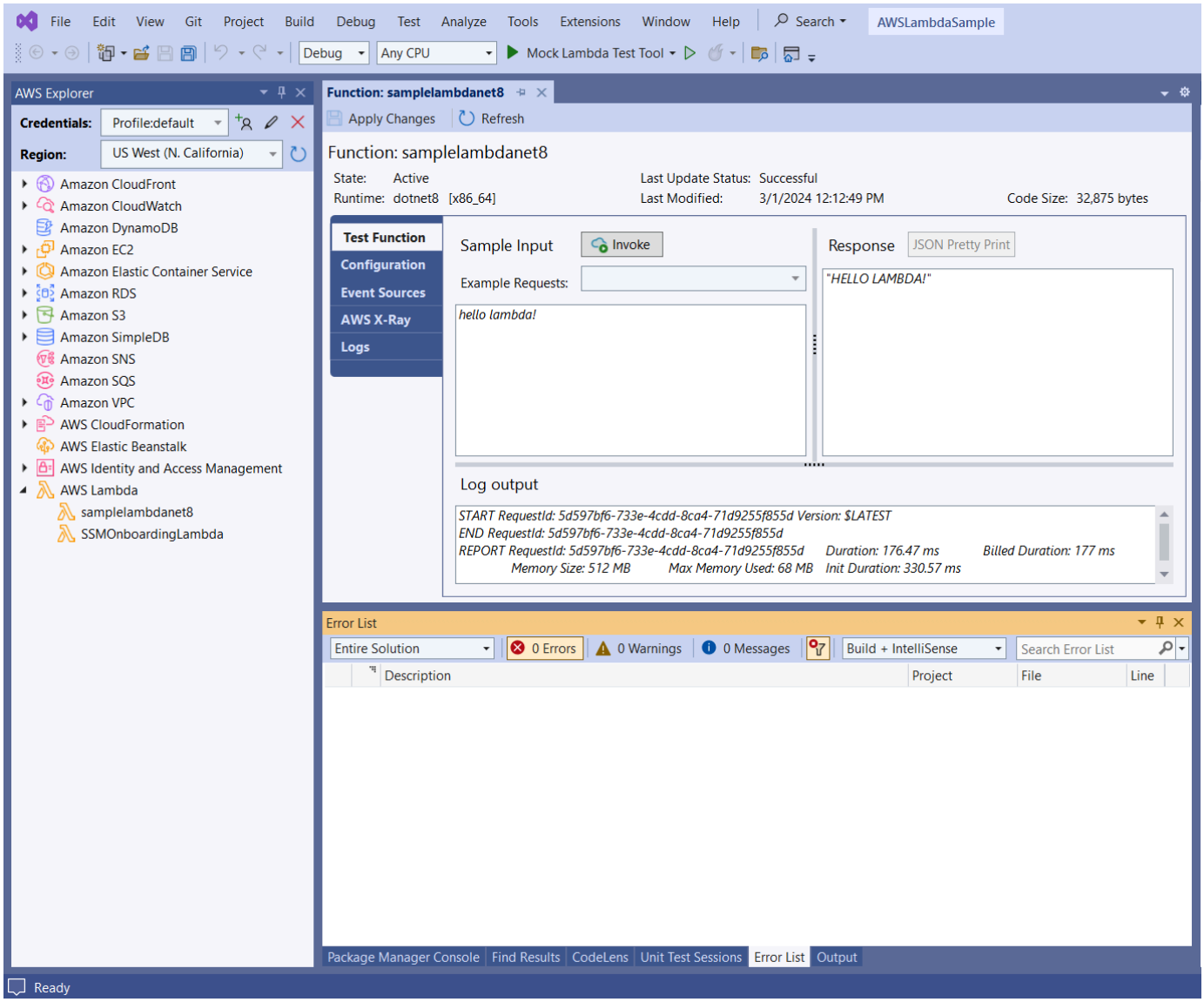
   c. (Optional) Legen Sie alle Umgebungsvariablen fest, die Ihre Lambda-Funktion benötigt. Die Schlüssel werden automatisch mit dem kostenlosen Standard-Serviceschlüssel verschlüsselt. Alternativ können Sie einen AWS KMS Schlüssel angeben, für den eine Gebühr anfällt. KMS ist ein verwalteter Service, mit 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

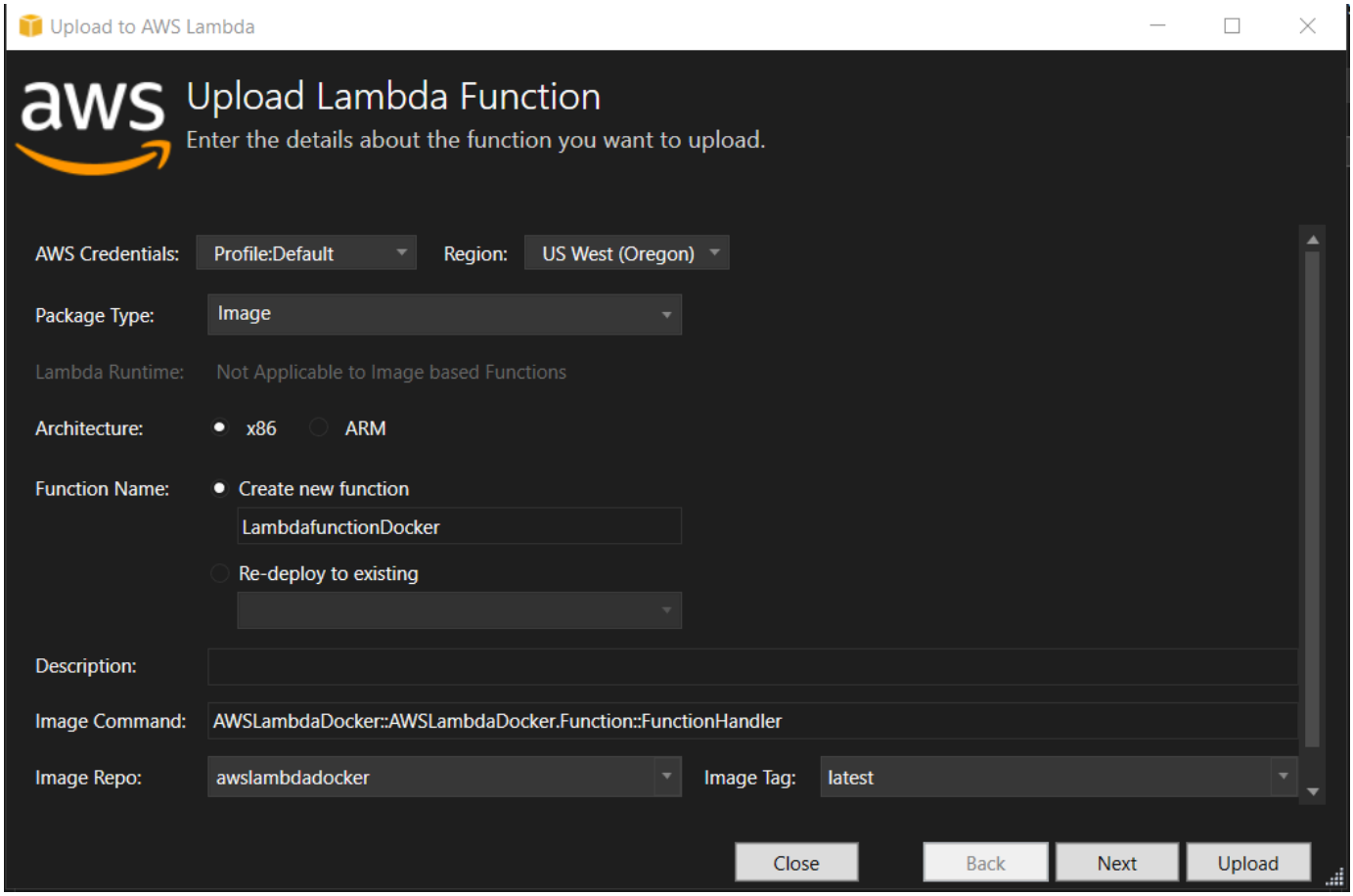
Die `Function.cs` Datei definiert die C#-Funktionen, die als Lambda-Funktionen verfügbar gemacht werden sollen. Das `FunctionHandler` ist die Lambda-Funktionalität, die ausgeführt wird, wenn die Lambda-Funktion ausgeführt wird. `FunctionHandler`Ruft in diesem Projekt den `ToUpper()` Eingabetext auf.

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 aus.

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.

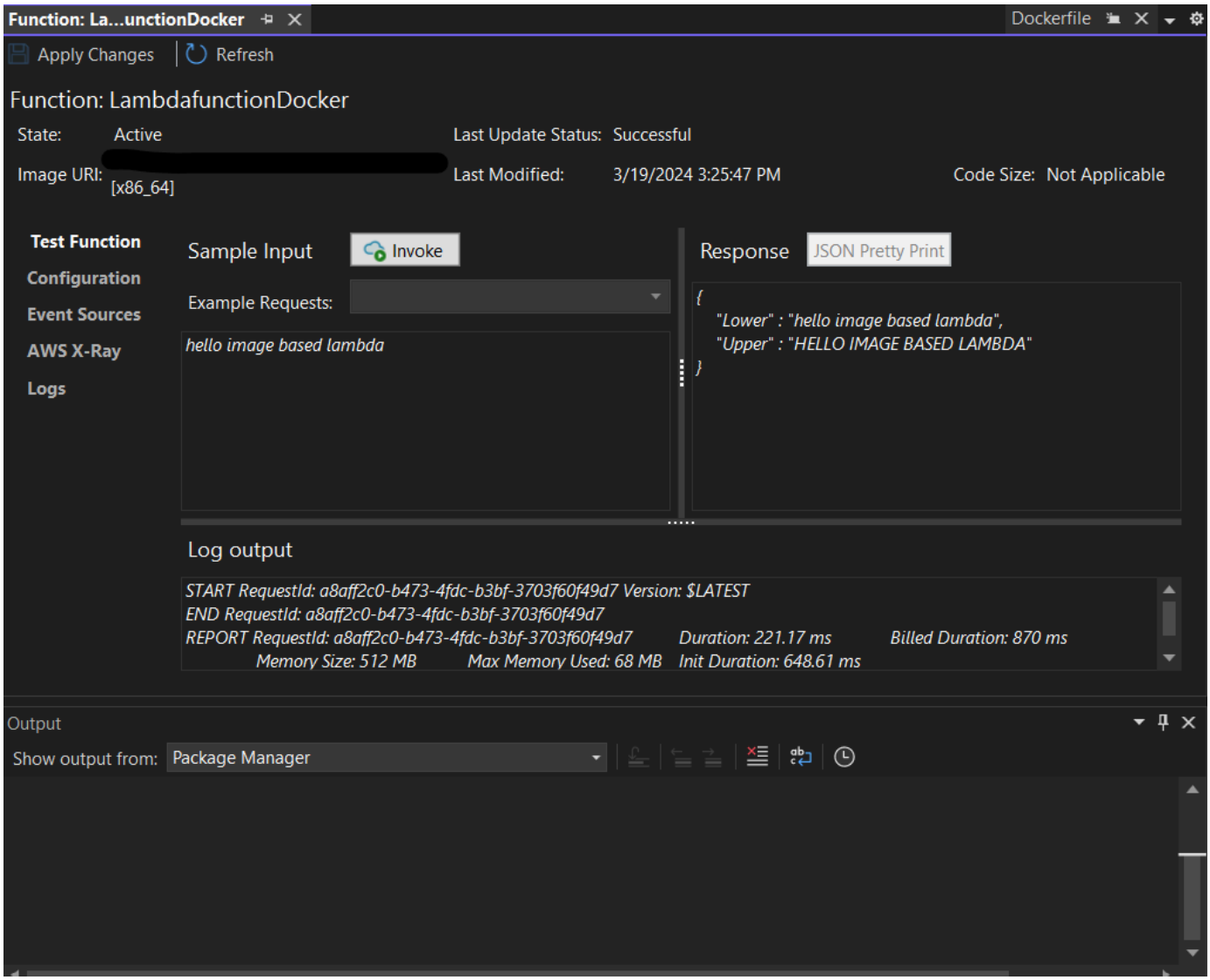
> **Note**
>
> Ihr Konto muss über die Berechtigung zum Ausführen der ListPolicies IAM-Aktion verfügen. Andernfalls ist die Liste mit den Rollennamen leer.

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:

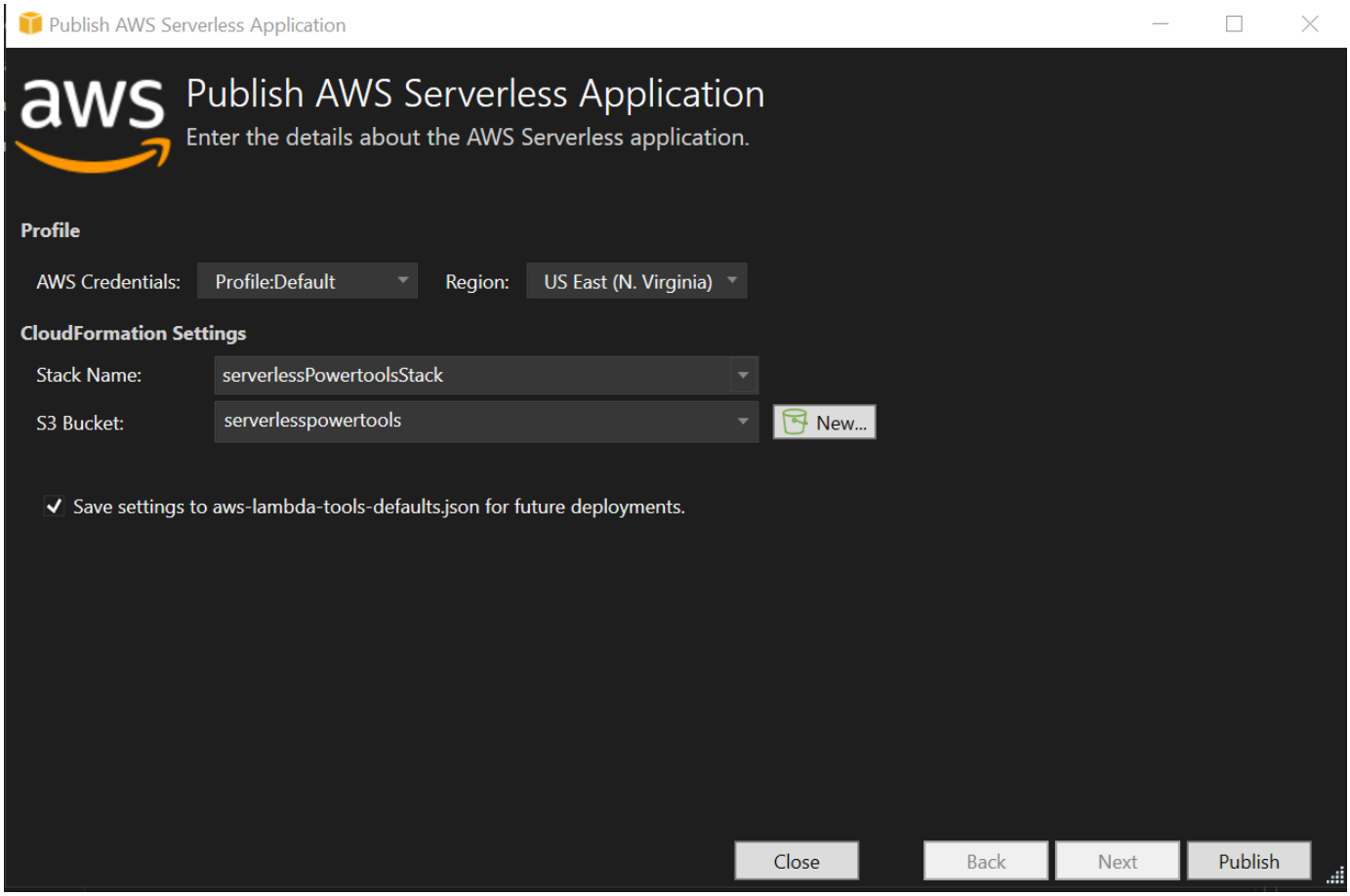
```
{
  "profile": "Default",
  "region": "us-east-1",
  "configuration": "Release",
  "s3-prefix": "ServerlessPowertools/",
  "template": "serverless.template",
  "template-parameters": ""
}
```

Bereitstellen der serverlosen Anwendung

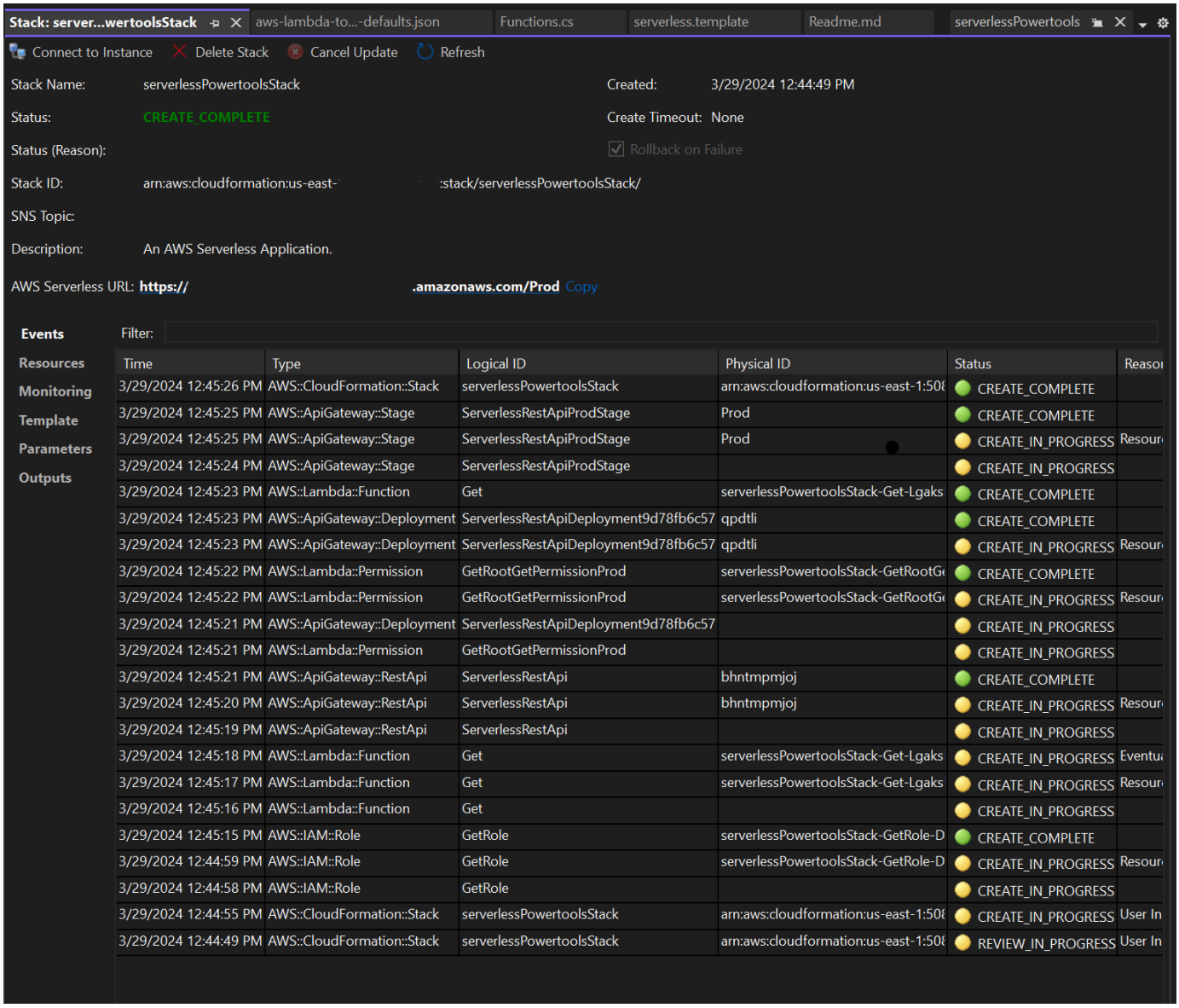
Gehen Sie wie folgt vor, um Ihre serverlose Anwendung bereitzustellen

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

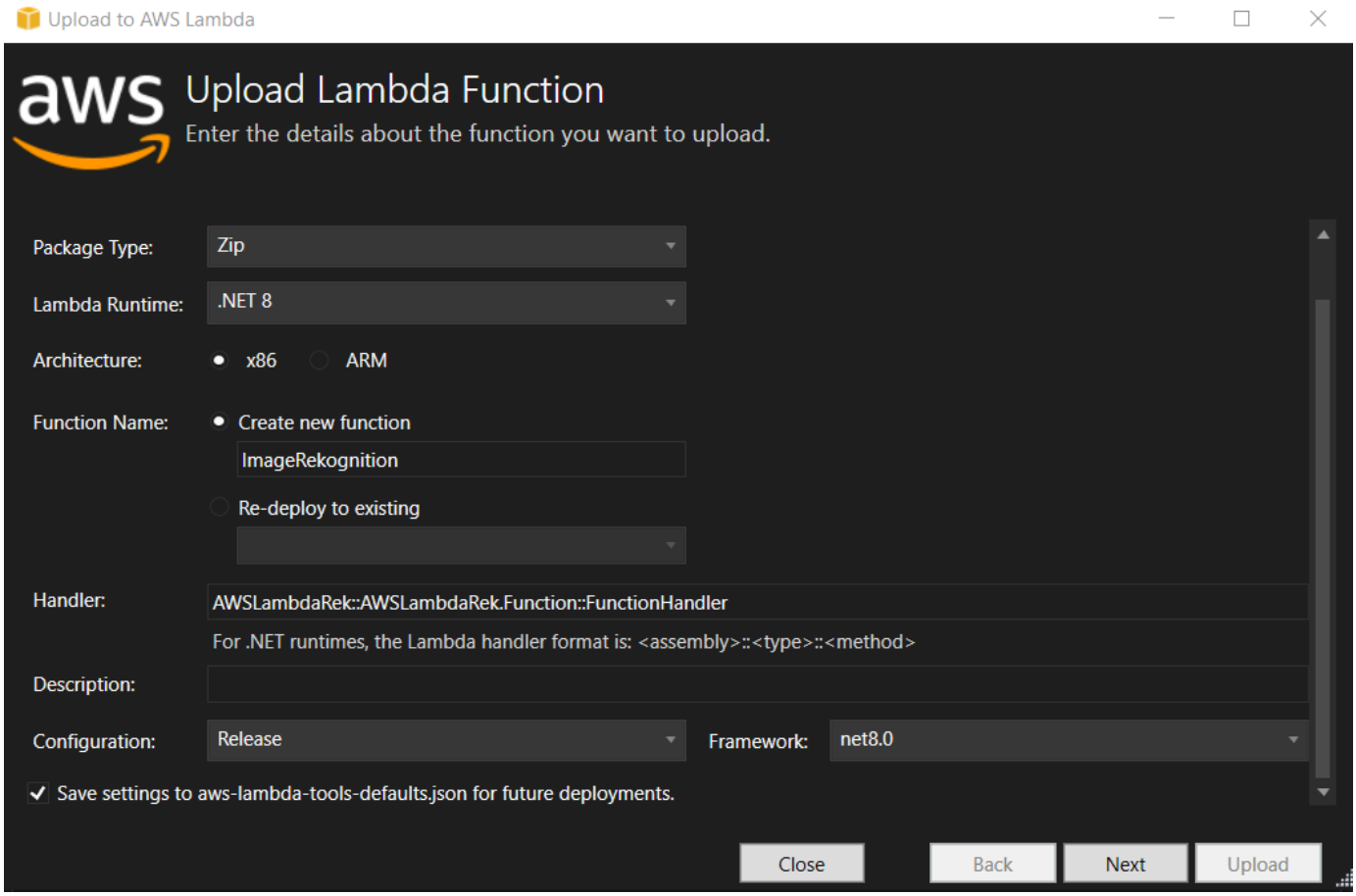
Das folgende Verfahren beschreibt, wie Sie Ihre Lambda-Funktion bereitstellen.

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.

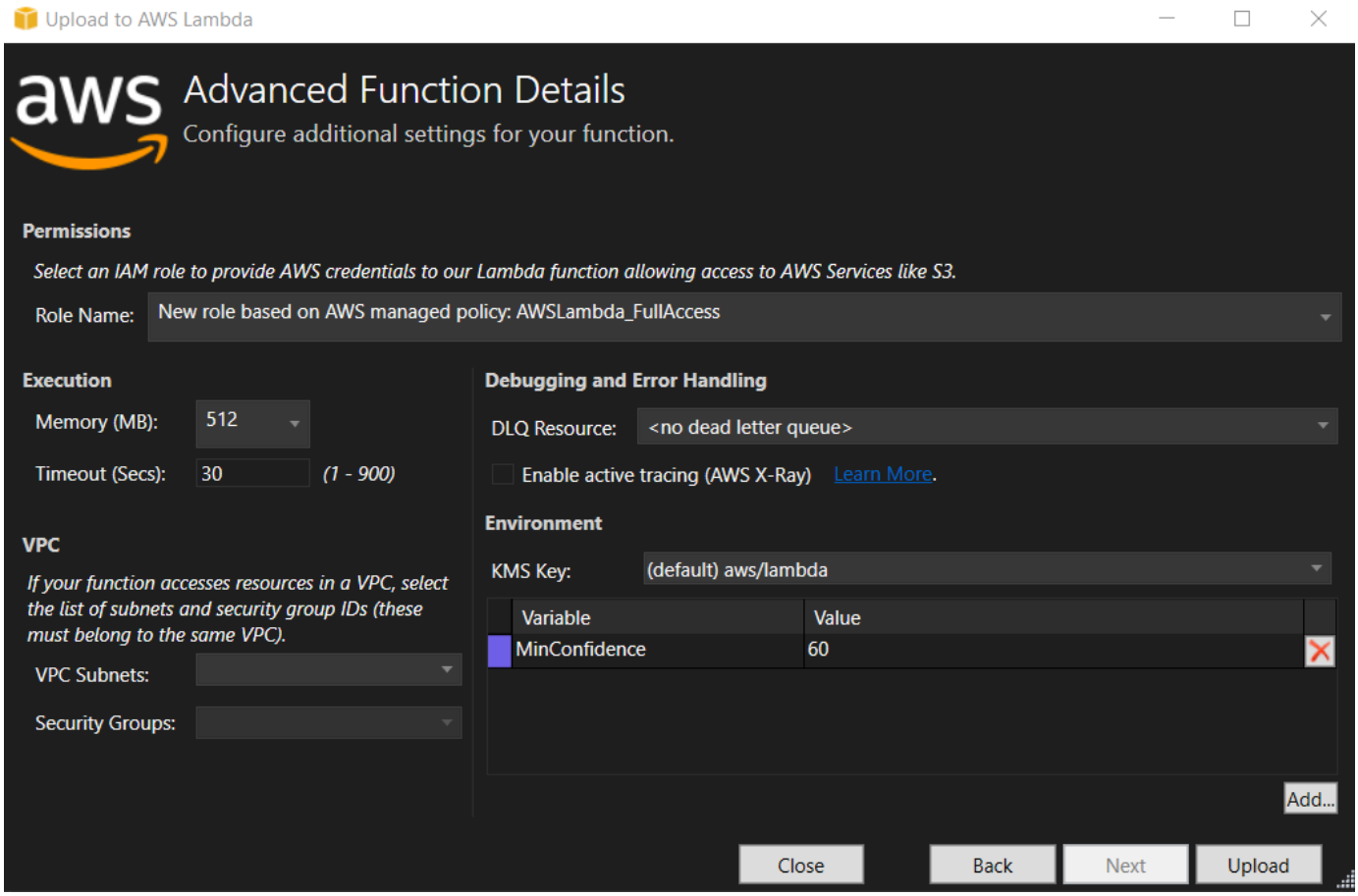
   > **Note**
   >
   > In diesem Beispiel wird der Funktionsname verwendet**`ImageRekognition`**.



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.

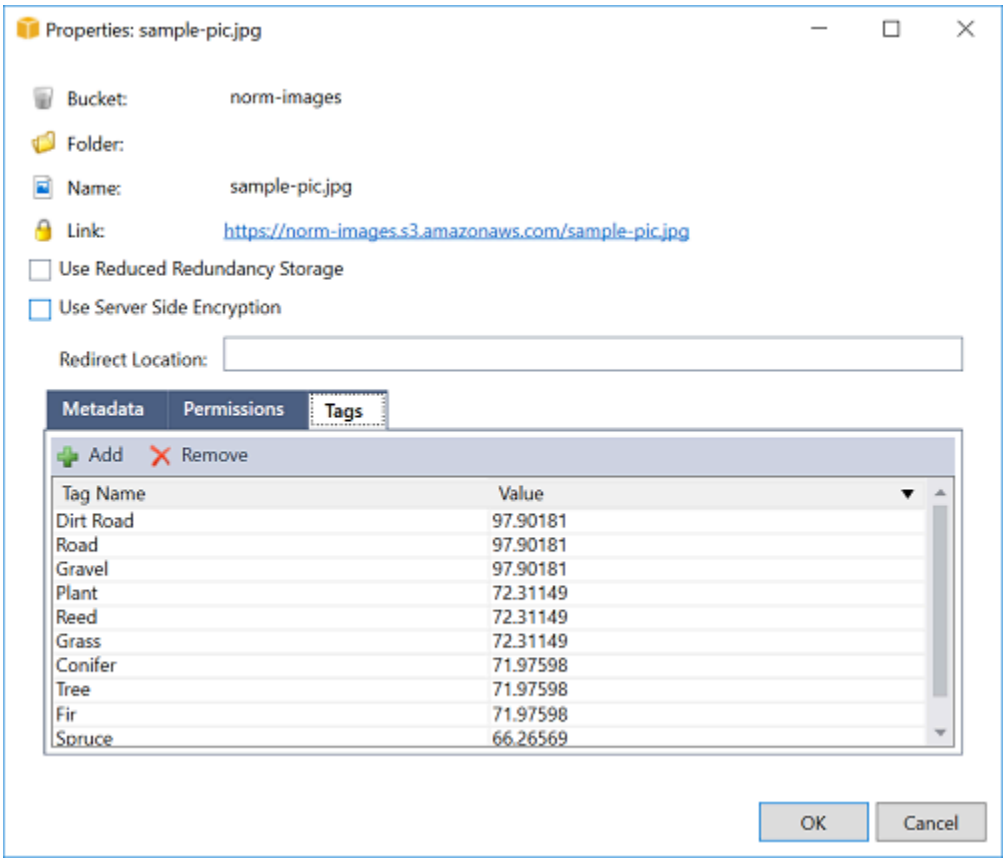
> **Note**
>
> Der Bucket muss sich in derselben AWS Region wie Ihre Lambda-Funktion befinden.

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 nuget.org NLog-Paket.
- 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 for .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, Beispiele und Anweisungen finden Sie in den Abschnitten zu Beispielen und Anweisungen im AWS GitHubLogging.NET-Repository.

```
{
```

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

Bereitstellen in AWS

Das Toolkit for Visual Studio unterstützt die Bereitstellung von Anwendungen inAWS Elastic Beanstalk Containern oderAWS 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 AWSManagement Console verwenden, um Anwendungen auf Elastic Beanstalk Beanstalk-Containern bereitzustellen.
>
> Für Elastic Beanstalk Beanstalk-Bereitstellungen müssen Sie zunächst ein Webbereitstellungspaket 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

So öffnen Sie denAWSin Visual Studio

Publish to (Zu &CW; veröffentlichen)AWSist eine interaktive Bereitstellungserfahrung, die Sie bei der Veröffentlichung Ihrer .NET-Anwendungen inAWSBereitstellungsziele, die Anwendungen ab .NET Core 3.1 unterstützen. So öffnen Sie denAWShält Ihren Arbeitsablauf in Visual Studio aufrecht, indem Sie diese Bereitstellungsfunktionen direkt von Ihrer IDE aus zur Verfügung stellen:

- Die Möglichkeit, Ihre Anwendung mit einem einzigen Klick bereitzustellen.

- Bereitstellungsempfehlungen basierend auf Ihrer Anwendung.
- Automatische Dockerfile-Erstellung, wie sie für die Umgebung Ihres Bereitstellungsziels relevant und erforderlich ist (Bereitstellungsziel).
- Optimierte Einstellungen für die Erstellung und Paketierung Ihrer Anwendungen, wie es Ihr Bereitstellungsziel erfordert.

> **Note**
>
> Weitere Informationen zum Veröffentlichen von .NET Framework-Anwendungen finden Sie im HandbuchErstellen und Bereitstellen von .NET-Anwendungen in Elastic Beanstalk
> Sie können auch auf Veröffentlichen Sie das SchreibenAWSaus der .NET CLI. Weitere Informationen finden Sie im .Deploy .T-Anwendungen inAWSguide.

Themen

Voraussetzungen

So veröffentlichen Sie .NET-Anwendungen erfolgreich in einerAWS-Dienst 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 derDownload für Microsoftaus.
- Node.js 14.x oder höher: Zum Ausführen wird Node.js benötigtAWS Cloud Development Kit (AWS CDK)aus. Um weitere Informationen über Node.js herunterzuladen oder weitere Informationen zu erhalten, besuchen Sie dieNode.js Downloadseiteaus.

> **Note**
>
> Publish to (Zu &CW; veröffentlichen)AWSnutztAWS CDKum Ihre Anwendung und ihre gesamte Bereitstellungsinfrastruktur als ein einziges Projekt bereitzustellen. Weitere Informationen zuAWS CDKfinden Sie unterCloud Development Kitguide.

- (Optional) Docker wird bei der Bereitstellung für einen containerbasierten Service wie Amazon ECS verwendet. Weitere Informationen und Informationen zum Herunterladen von Docker finden Sie imDocker herunterladen Sie denSeite.

Unterstützte Anwendungstypen

Erstellen oder öffnen Sie zunächst einen der folgenden Projekttypen in Visual Studio, bevor Sie auf einem neuen Ziel veröffentlichen oder ein bestehendes Ziel veröffentlichen:

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

Veröffentlichen von Anwendungen inAWSZielvorgaben

Wenn Sie auf einem neuen Ziel veröffentlichen, sollten Sie Publish toAWSführt Sie durch den Prozess, indem er Empfehlungen ausgibt und allgemeine Einstellungen verwendet. Wenn Sie auf einem zuvor festgelegten Ziel veröffentlichen müssen, werden Ihre Einstellungen gespeichert und können angepasst werden oder sind sofort für die Bereitstellung mit einem Klick verfügbar.

In einem neuen Ziel veröffentlichen

Im Folgenden wird beschrieben, wie Sie Publish to (Zu &AWSBereitstellungseinstellungen, wenn Sie auf einem neuen Ziel veröffentlichen.

1. AusAWSExploreraus, erweitern Sie denErweitern Sie im angezeigten Detailbereich die Optionaus und klicken Sie dann aufAWSProfil, das der Region entspricht undAWSDienste, die für Ihre Bereitstellung erforderlich sind.
2. ErweitSie Sie derRegionaus und klicken Sie dann aufAWSRegion, die dasAWSDienste, die für Ihre Bereitstellung erforderlich sind.
3. Aus Visual StudioExplorer für Lösungenaus, öffnen Sie das Kontextmenü für (rechte Maustaste) für den Namen des Projekts und wählen SiePublish to (Zu &CW; veröffentlichen)AWSaus. Das öffnet sichPublish to (Zu &CW; veröffentlichen)AWSaus.
4. AusPublish to (Zu &CW; veröffentlichen)AWS, wählenVeröffentlichung für neues Zielaus, um eine neue Bereitstellung zu konfigurieren.

> **Note**
>
> Um Ihre Standardbereitstellungsanmeldeinformationen zu ändern, wählen Sie oder klicken SieBearbeitenLink befindet sich neben demErweitern Sie im angezeigten Detailbereich die OptionAbschnitts, inPublish to (Zu &CW; veröffentlichen)AWSaus. Um den Prozess der Zielkonfiguration zu umgehen, wählen SieIn vorhandenem Ziel veröffentlichenund wählen Sie dann Ihre bevorzugte Konfiguration aus der Liste Ihrer vorherigen Bereitstellungsziele aus.

5. AusVeröffentlichen der Zieleaus, klicken Sie auf eineAWSService zur Verwaltung Ihrer Anwendungsbereitstellung.
6. Wenn Sie mit Ihrer Konfiguration zufrieden sind, klicken Sie aufVeröffentlichenaus, um die Bereitstellung zu starten.

> **Note**
>
> Nach dem Initiieren einer BereitstellungPublish to (Zu &CW; veröffentlichen)AWSzeigt die folgenden Statusaktualisierungen an:
>
> - Während des BereitstellungsprozessesPublish to (Zu &CW; veröffentlichen)AWSzeigt Informationen über den Fortschritt der Bereitstellung an.
> - Nach dem BereitstellungsprozessPublish to (Zu &CW; veröffentlichen)AWSzeigt an, ob die Bereitstellung erfolgreich war oder fehlgeschlagen ist.
> - Nach einer erfolgreichen Bereitstellung bietet derRessourcenbietet zusätzliche Informationen über die Ressource, die erstellt wurde. Diese Informationen variieren abhängig von der Art der Anwendung und der Bereitstellungskonfiguration.

In einem vorhandenen Ziel veröffentlichen

Im Folgenden wird beschrieben, wie Sie Ihre .NET-Anwendung erneut in einer vorhandenen veröffentlichenAWSZiel.

1. AusAWSExploreraus, erweitern Sie denErweitern Sie im angezeigten Detailbereich die Optionaus und klicken Sie dann aufAWSProfil, das der Region entspricht undAWSDienste, die für Ihre Bereitstellung erforderlich sind.

2. ErweitSie Sie derRegionaus und klicken Sie dann aufAWSRegion, die dasAWSDienste, die für Ihre Bereitstellung erforderlich sind.
3. Aus Visual StudioExplorer für Lösungenaus, klicken Sie mit der rechten Maustaste auf den Namen des ProjektsPublish to (Zu &CW; veröffentlichen)AWSöffnen Sie denPublish to (Zu &CW; veröffentlichen)AWSaus.
4. AusPublish to (Zu &CW; veröffentlichen)AWS, wählenIn vorhandenem Ziel veröffentlichenaus, um Ihre Bereitstellungsumgebung aus einer Liste vorhandener Ziele auszuwählen.

> **Note**
>
> Wenn Sie kürzlich Anwendungen in derAWSCloud, diese Anwendungen werden in Publish to angezeigtAWSaus.

5. Wählen Sie das Veröffentlichungsziel aus, in dem die Anwendung bereitgestellt werden soll, und klicken Sie dann auf.Veröffentlichenaus, um die Bereitstellung zu starten.

Bereitstellen einesAWS LambdaProjekt mit der .NET Core CLI

Das AWS Toolkit for Visual Studio beinhaltet AWS Lambda .NET Core-Projektvorlagen für Visual Studio. Die in Visual Studio integrierten Lambda-Funktionen können Sie mithilfe der .NET Core-Befehlszeilenschnittstelle (CLI) bereitstellen.

Themen

Voraussetzungen

Bevor Sie mit der .NET Core CLI arbeiten, um Lambda-Funktionen bereitzustellen, müssen die folgenden Voraussetzungen erfüllt sein:

- Stellen Sie sicher, dass Visual Studio 2015 Update 3 installiert ist.
- Install.NET Core für Windowsaus.

- Richten Sie die .NET Core CLI für die Arbeit mit Lambda ein. Weitere Informationen finden Sie unter.NET Core-CLIimAWS LambdaEntwicklerhandbuchaus.
- das Toolkit for Visual Studio installieren. 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 zum Bereitstellen von Lambda-Funktionen verwenden:

- Weitere Informationen über Lambda-Funktionen finden Sie unterWas ist ?AWSLambda?imAWS LambdaEntwicklerhandbuchaus.
- Weitere Informationen zum Erstellen von Lambda-Funktionen in Visual Studio finden Sie unterAWS Lambdaaus.
- Weitere Informationen zu Microsoft .NET-Core finden Sie unter.NET Corein der Online-Dokumentation von Microsoft.

Auflisten der über die .NET Core CLI verfügbaren Lambda-Befehle

Gehen Sie wie folgt vor, um die Lambda-Befehle aufzulisten, die über die .NET Core CLI verfügbar sind.

1. Öffnen Sie ein Eingabeaufforderungsfenster und navigieren Sie zum 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

Bei den folgenden Anweisungen wird davon ausgegangen, dass Sie eine AWS Lambda .NET Core-Funktion in Visual Studio erstellt haben.

1. Öffnen Sie ein Eingabeaufforderungsfenster und navigieren Sie zum Ordner, der Ihr Visual Studio .NET Core Lambda-Projekt enthält.
2. Geben Sie `dotnet lambda deploy-function` ein.
3. Geben Sie auf Aufforderung den Namen der bereitzustellenden -Funktion ein. Sie können einen neuen Namen oder den Namen einer bereits vorhandenen Funktion verwenden.
4. Geben Sie auf Aufforderung dasAWSRegion (die Region, für die Ihre Lambda-Funktion bereitgestellt wird).
5. Wählen Sie auf Aufforderung die IAM-Rolle aus bzw. erstellen Sie diese, die Lambda für die Ausführung der Funktion übernimmt.

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 derAWSRegion :

```
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, kann sie verwendet werden. Weitere Informationen finden Sie unterBeispiele für die Verwendung vonAWSLambdaaus.

Lambda überwacht automatisch Lambda-Funktionen für Sie und meldet Metriken über Amazon CloudWatchaus. Informationen zur Überwachung und Fehlersuche Ihrer Lambda-Funktion finden Sie unterFehlersuche und ÜberwachungAWSLambda-Funktionen mit Amazon CloudWatchaus.

Bereitstellen in Elastic Beanstalk

AWS Elastic Beanstalkist ein Service, der die Bereitstellung vereinfachtAWSRessourcen für Ihre Anwendung. Elastic Beanstalk bietet alleAWSerforderliche Infrastruktur für die Bereitstellung Ihrer Anwendung. Diese Infrastruktur umfasst:

- Amazon EC2 EC2-Instances, die als Host für die ausführbaren Dateien und die Inhalte Ihrer Anwendung dienen.
- Eine Auto Scaling Scaling-Gruppe für die entsprechende Anzahl von Amazon EC2 EC2-Instances zur Unterstützung Ihrer Anwendung.
- Ein Elastic Load Balancing Load Balancer, der eingehenden Datenverkehr an die Amazon EC2 EC2-Instance mit der größten Bandbreite weiterleitet.

Das Toolkit for Visual Studio bietet einen Assistenten, der die Veröffentlichung von Anwendungen über Elastic Beanstalk vereinfacht. Dieser Assistent wird in den folgenden Abschnitten beschrieben.

Weitere Informationen über Elastic Beanstalkfinden Sie im.Elastic Beanstalk-Dokumentationaus.

Themen

- Stellen Sie eine herkömmliche ASP.NET-Anwendung auf Elastic Beanstalk bereit
- Bereitstellen einer ASP.NET Core-Anwendung mit Elastic Beanstalk (Legacy)
- So legen Sie den Wert festAWSSicherheitsanmeldeinformationen für Ihre Anwendung

- So veröffentlichen Sie Ihre Anwendung erneut in einer Elastic Beanstalk Beanstalk-Umgebung (Legacy)
- Benutzerdefinierte Bereitstellung von Elastic Beanstalk-Anwendungen
- Benutzerdefinierte ASP.NET Core-Bereitstellungen in Elastic Beanstalk-Bereitstellungen in
- Support mehrerer Anwendungen für .NET und Elastic Beanstalk

Stellen Sie eine herkömmliche ASP.NET-Anwendung auf Elastic Beanstalk bereit

In diesem Abschnitt wird beschrieben, wie Sie den Assistenten „In Elastic Beanstalk veröffentlichen“ 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.

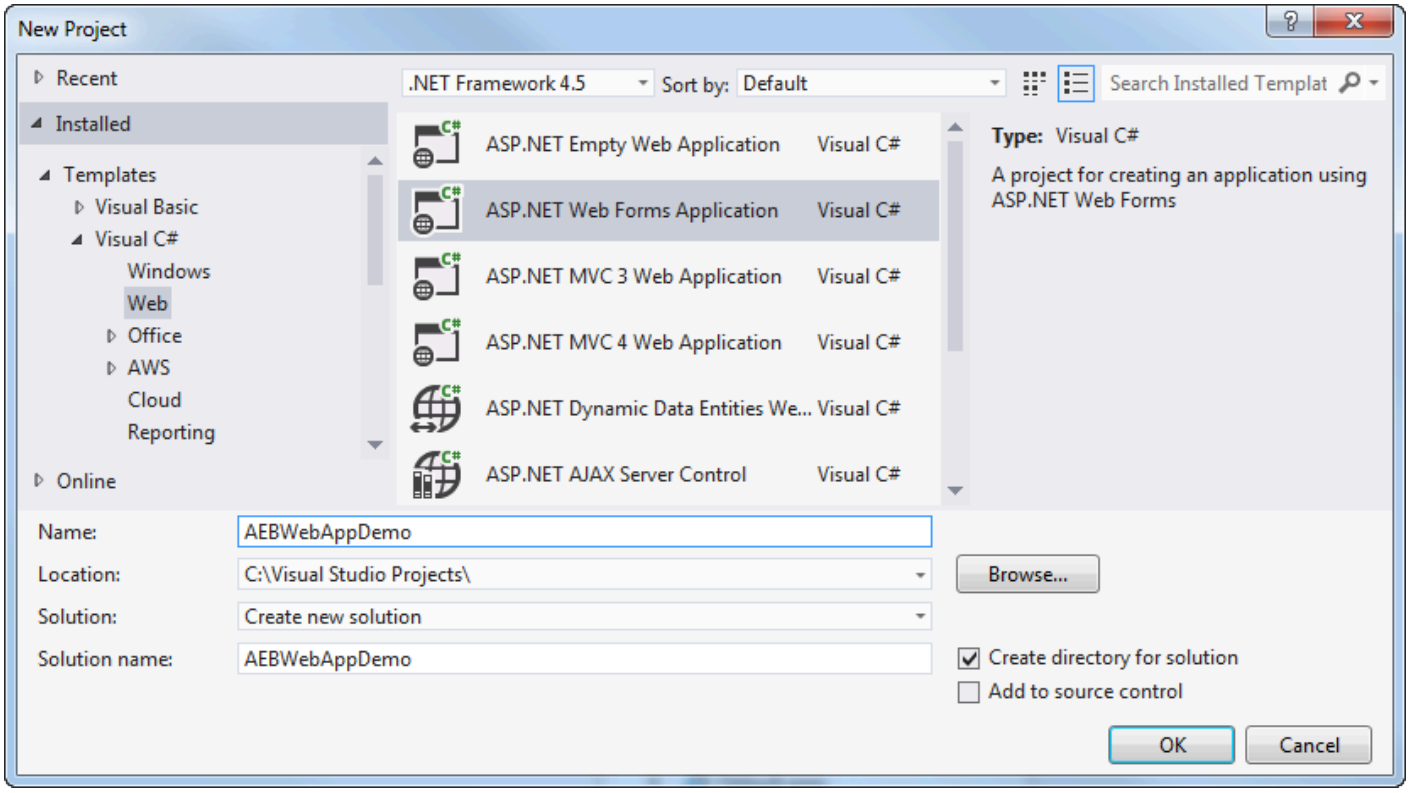
> **Note**
>
> Der Assistent unterstützt auch die Bereitstellung von ASP.NET Core-Anwendungen. Informationen zu ASP.NET Core finden Sie im AWS.NET-Bereitstellungstool und im aktualisierten Deploying toAWS Inhaltsverzeichnis.

> **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.

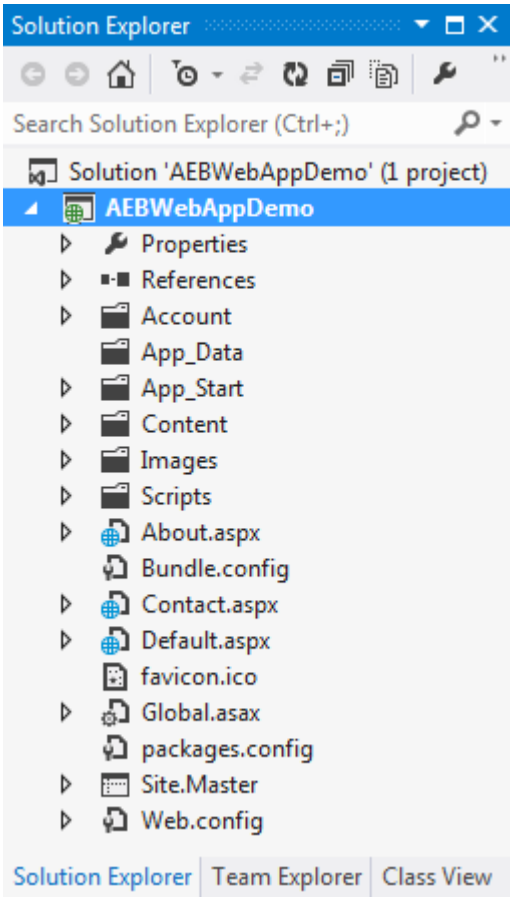
So erstellen Sie ein Beispiel-Webanwendungs-Starterprojekt

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.

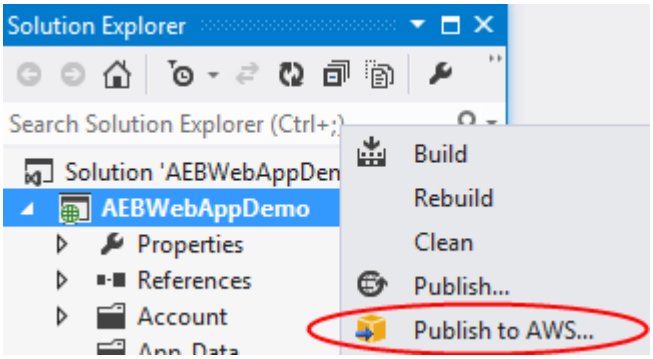


4. Geben Sie im Feld Name die Zeichenfolge `AEBWebAppDemo` ein.
5. Geben Sie im Feld Location (Speicherort) den Pfad zu einem Projektmappenordner auf Ihrem Entwicklungscomputer ein oder klicken Sie auf Browse (Durchsuchen), um einen Projektordner auszuwählen. Klicken Sie anschließend auf Select Folder (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.

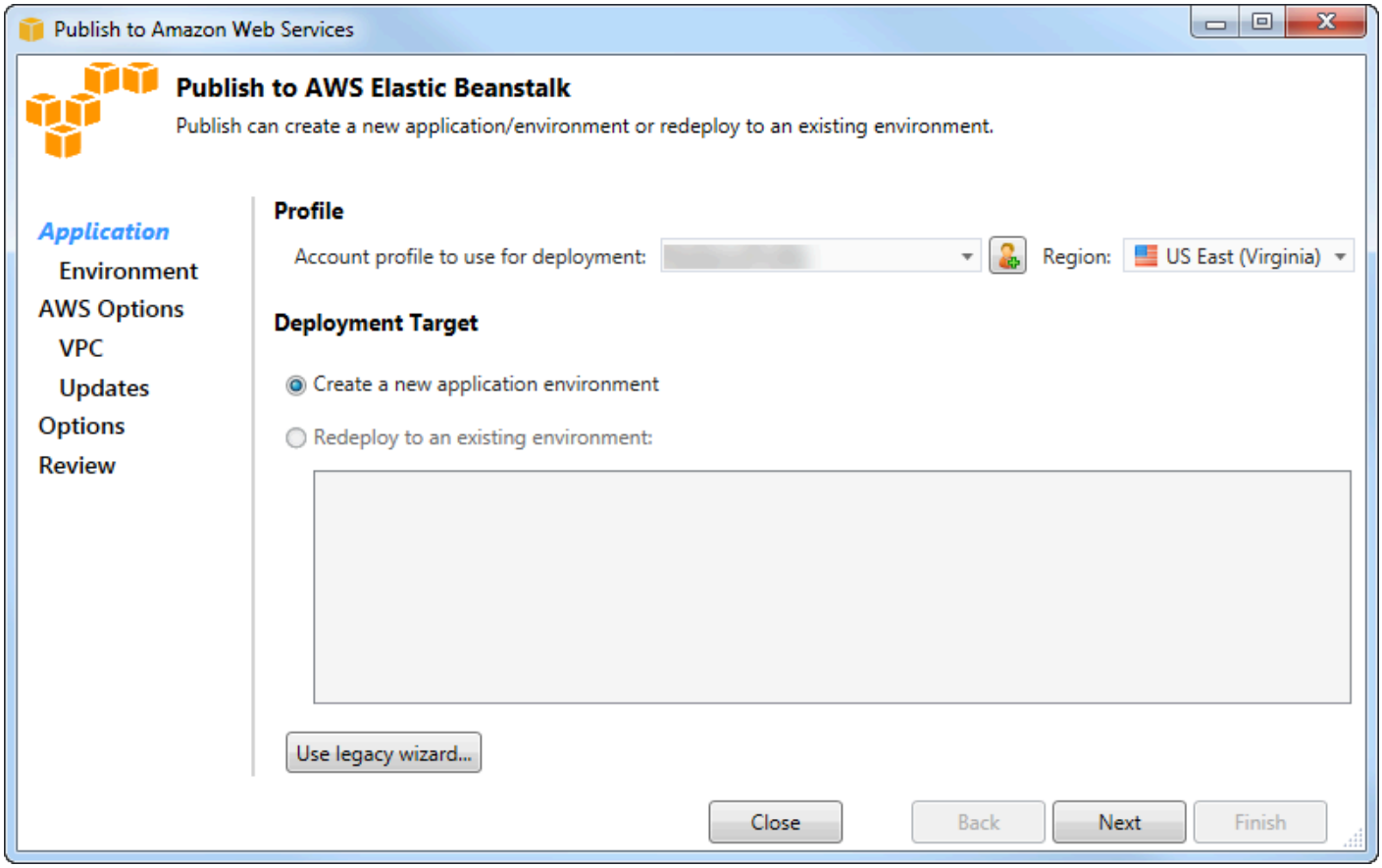


So stellen Sie mit dem "Publish to Elastic Beanstalk"-Assistenten eine Anwendung bereit

1. Öffnen Sie im Solution Explorer das Kontextmenü (Rechtsklick) für den WebAppDemoAEB-Projektordner 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 AWSElastic Beanstalk veröffentlichen.



   Der Publish to Elastic Beanstalk (Veröffentlichen zu Elastic Beanstalk)-Assistent wird angezeigt.



2. Wählen Sie unter Profil aus der Dropdownliste Für die Bereitstellung zu verwendendes Kontoprofil dasAWS Kontoprofil aus, das Sie für die Bereitstellung verwenden möchten.

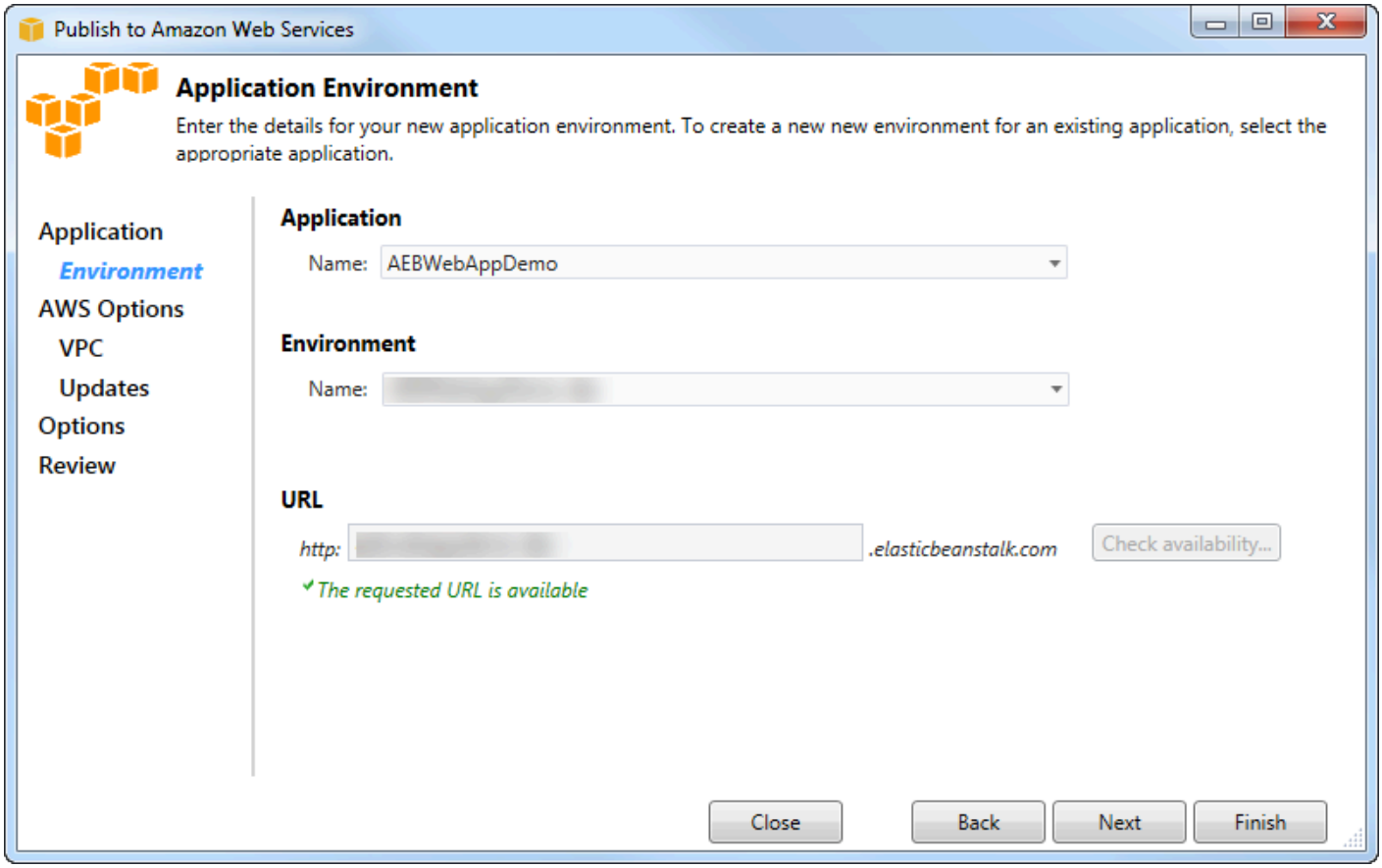
   Wenn Sie einAWS Konto haben, das Sie verwenden möchten, aber noch keinAWS Kontoprofil dafür erstellt haben, können Sie optional die Schaltfläche mit dem Plussymbol (+) wählen, um einAWS Kontoprofil hinzuzufügen.

3. Wählen Sie aus der Dropdownliste 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.

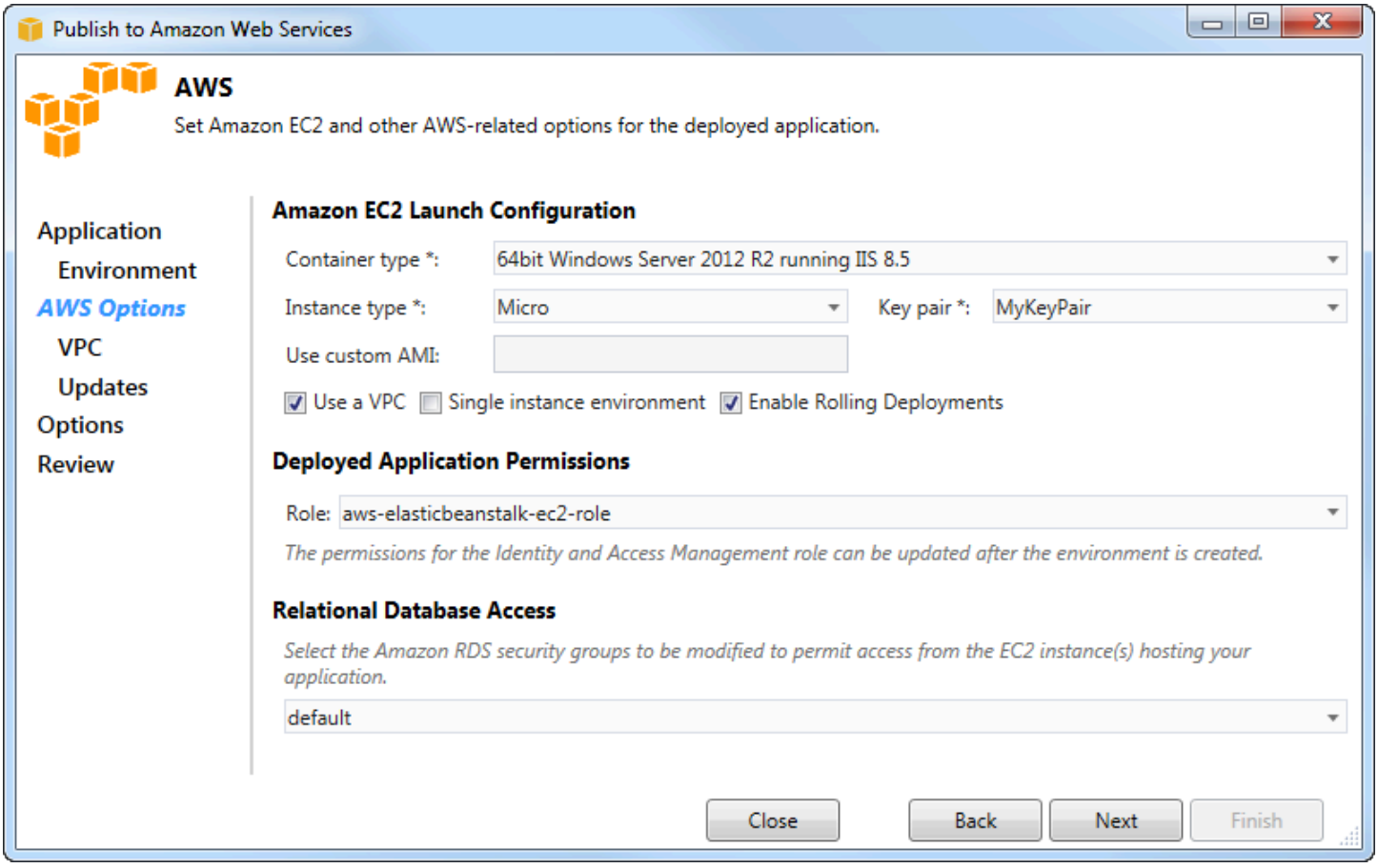
5. Wählen Sie Next (Weiter).



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 Dropdownliste 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).



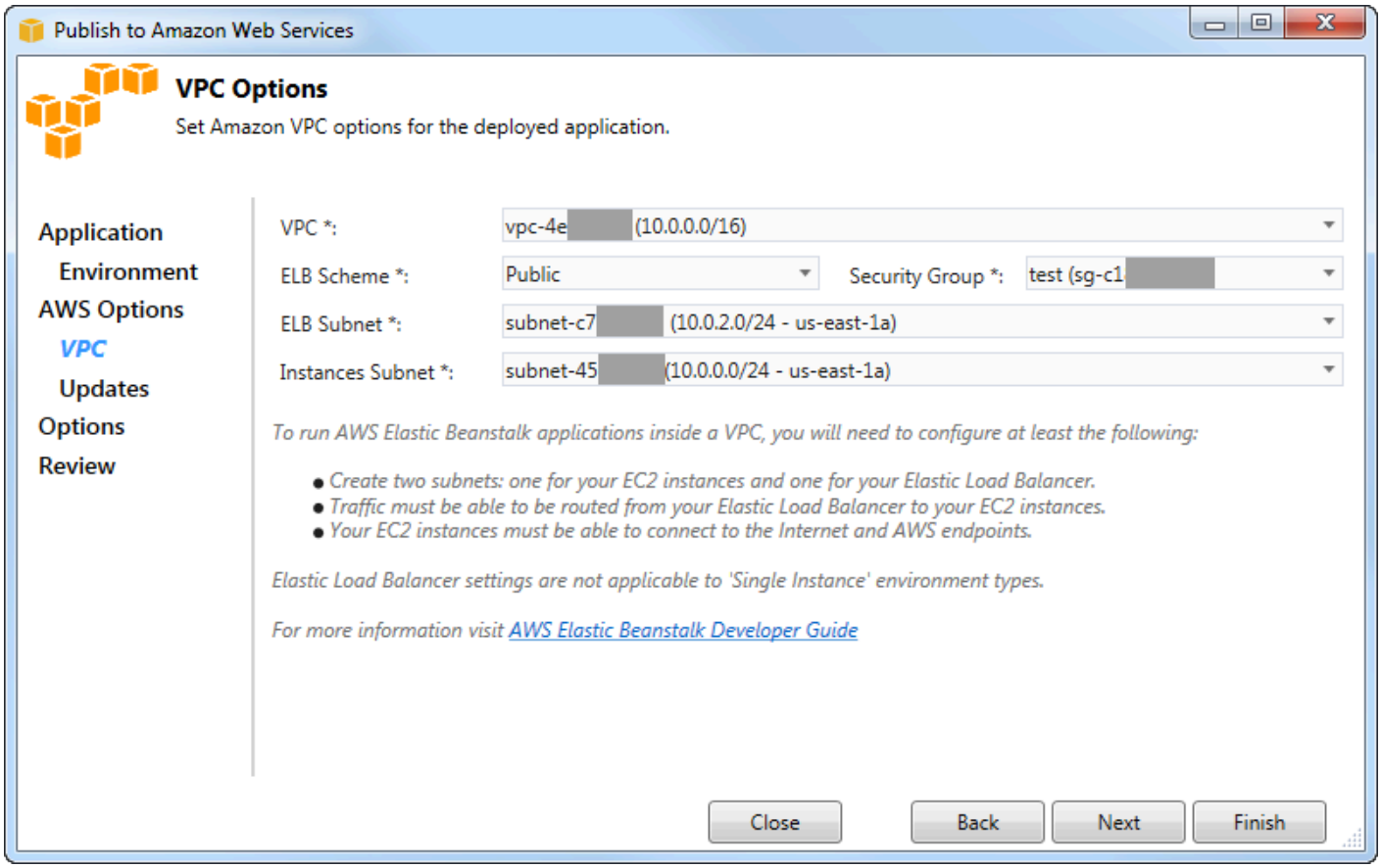
1. Wählen Sie auf der Seite AWSOptionen in der Amazon EC2 EC2-Startkonfiguration aus der Dropdownliste Containertyp einen Amazon Machine Image-Typ (AMI) aus, der für Ihre Anwendung verwendet werden soll.

2. Geben Sie in der Dropdownliste Instance-Typ den zu verwendenden Amazon EC2 EC2-Instance-Typ an. Für dieses Beispiel empfehlen wir, Micro zu verwenden. Dadurch werden die Kosten für die Ausführung der Instance minimiert. Weitere Informationen über Amazon EC2 EC2-Kosten finden Sie auf der EC2-Preise.
3. Wählen Sie in der Dropdownliste key pair ein Amazon EC2 EC2-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 AWSElastic 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 optional eine einzelne Amazon EC2 EC2-Instance starten und dann Ihre Anwendung darauf bereitstellen möchten, wählen Sie das Feld Single-Instance-Umgebung aus.

   Wenn Sie dieses Feld auswählen, erstellt Elastic Beanstalk trotzdem eine Auto Scaling Scaling-Gruppe, konfiguriert sie jedoch nicht. Wenn Sie die Auto Scaling Scaling-Gruppe später konfigurieren möchten, können Sie die verwendenAWS 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 AnwendungAWS Dienste wie Amazon S3 und DynamoDB verwendet, können Sie Anmeldeinformationen am besten mithilfe einer IAM-Rolle bereitstellen. Im Bereich Bereitgestellte Anwendungsberechtigungen können Sie entweder eine vorhandene IAM-Rolle auswählen oder eine erstellen, die der Assistent zum Starten Ihrer Umgebung verwendet. Anwendungen, die den verwenden, verwendenAWS SDK for .NET automatisch die von dieser IAM-Rolle bereitgestellten Anmeldeinformationen, wenn sie eine Anfrage an einenAWS Dienst stellen.
9. Wenn Ihre Anwendung auf eine Amazon RDS-Datenbank zugreift, wählen Sie in der Dropdownliste im Bereich Relational Database Access die Kästchen neben allen Amazon RDS-Sicherheitsgruppen aus, die der Assistent aktualisiert, sodass Ihre Amazon EC2 EC2-Instances auf diese Datenbank zugreifen können.
10. Wählen Sie Next (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 AWSManagement Console erstellt haben, geben Sie auf dieser Seite Informationen zu Ihrer VPC ein.

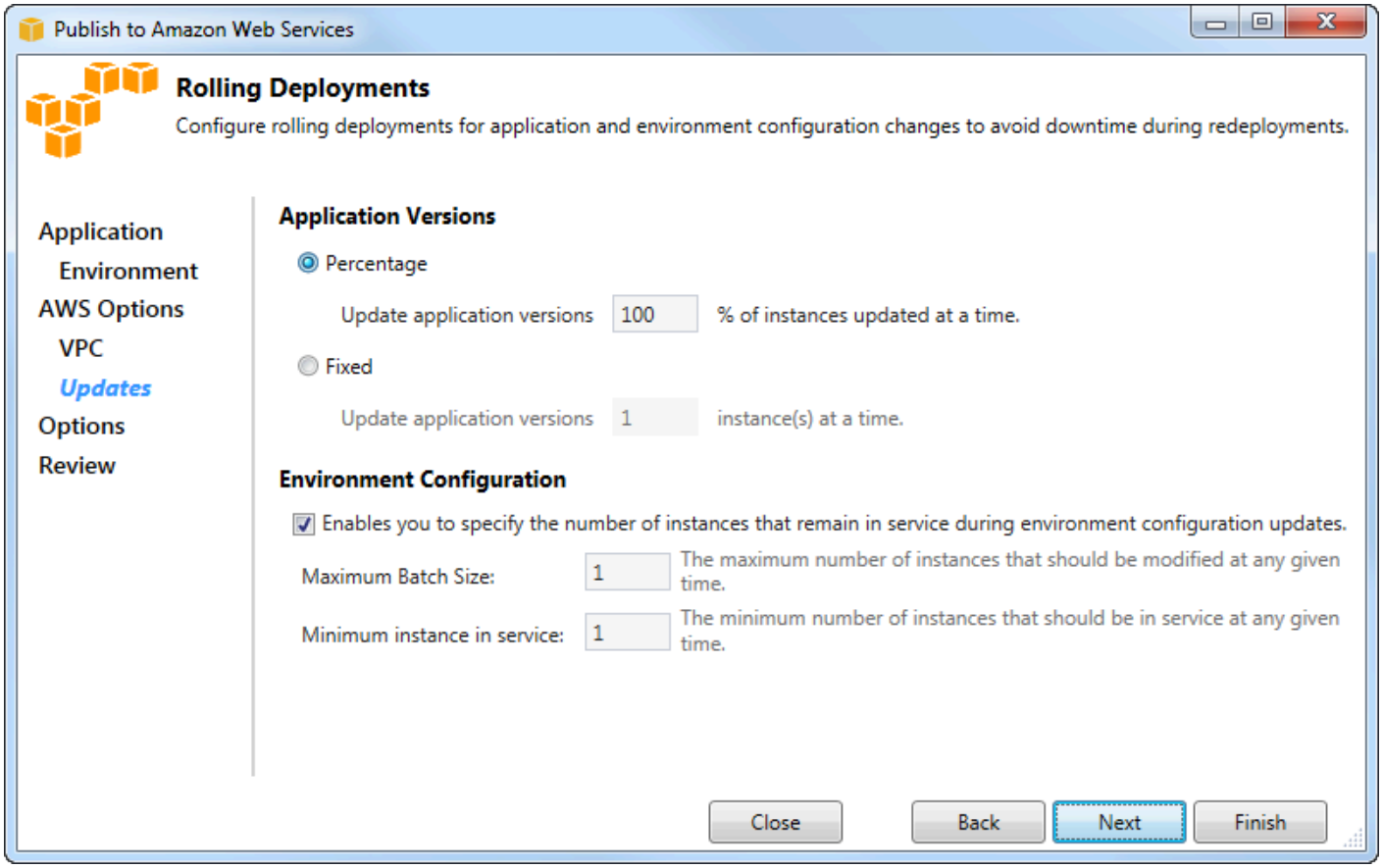
Wichtige Überlegungen für die Bereitstellung in einer VPC

- 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 Tag-Werte, die sie als öffentlich kennzeichnen.
- Geben Sie in der Dropdown-Liste Instances Subnet das private Subnetz an. Das Toolkit for Visual Studio stellt die Amazon EC2 EC2-Instances für Ihre Anwendung im privaten Subnetz bereit.
- Die Amazon EC2 EC2-Instances für Ihre Anwendung kommunizieren vom privaten Subnetz mit dem Internet über eine Amazon EC2 EC2-Instance im öffentlichen Subnetz, die die Netzwerkadressübersetzung (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 auf einer VPC finden Sie im AWSElastic Beanstalk Developer Guide.

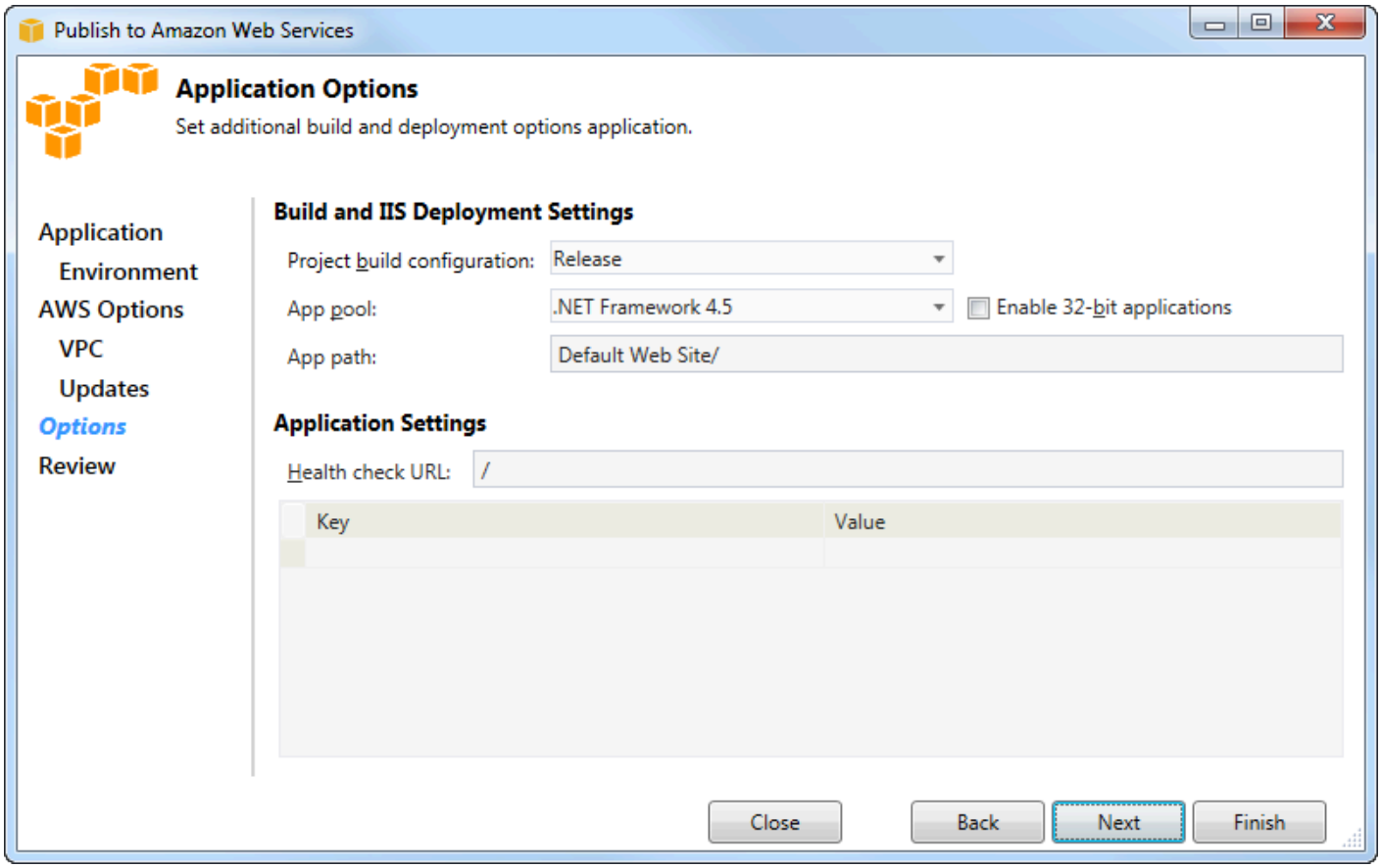
1. Nachdem Sie alle Informationen auf der Seite VPC Options (VPC-Optionen) eingegeben haben, wählen Sie Next (Weiter).
   - Wenn Sie Enable Rolling Deployments (Rolling-Bereitstellungen aktivieren) ausgewählt haben, wird die Seite Rolling Deployments (Rolling-Bereitstellungen) angezeigt.
   - Wenn Sie 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 Next (Weiter).

6. Geben Sie auf der Seite Application Options (Anwendungsoptionen) Informationen zum Build, den Internet Information Services (IIS) und den Anwendungseinstellungen an.

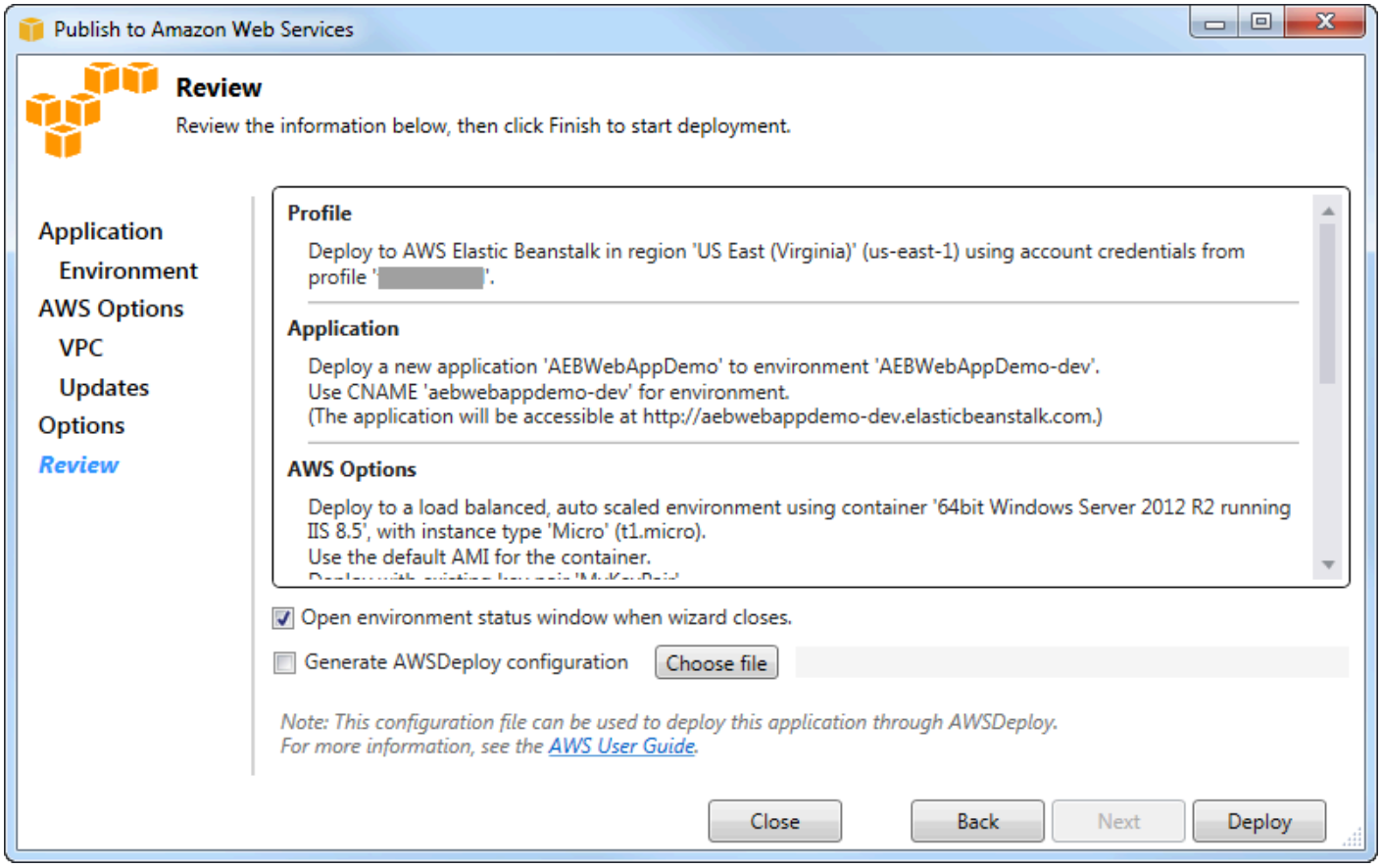


7. Wählen Sie im Bereich Build and IIS Deployment Settings (Build- und IIS-Bereitstellungseinstellungen) aus der Dropdown-Liste Project build configuration (Projekt-Buildkonfiguration) die Ziel-Buildkonfiguration aus. Wenn der Assistent diese findet, wird Release (Version) angezeigt. Andernfalls erscheint 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 in das 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 dieAWS Anmeldeinformationen anzugeben, unter denen Ihre Anwendung ausgeführt werden soll. Der bevorzugte Ansatz besteht darin, eine IAM-Rolle in der Dropdownliste Identity and Access Management Management-Rolle auf der AWSOptionsseite anzugeben. Wenn Sie jedochAWS Anmeldeinformationen anstelle einer IAM-Rolle verwenden müssen, um Ihre Anwendung auszuführen, wählen Sie in der Zeile Schlüssel die Option AWSAccessKey. Geben Sie in der Zeile Value (Wert) den Zugriffsschlüssel ein. Wiederholen Sie diese Schritte für AWSSecretKey.

13. Wählen Sie Next (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 verwendetenAWS 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 imAWS Explorer den Elastic Beanstalk-Knoten, öffnen Sie das Kontextmenü (rechte Maustaste) für den Unterknoten für das Deployment und wählen Sie dann Löschen aus. Das Löschen kann einige Minuten dauern.

Bereitstellen einer ASP.NET Core-Anwendung mit Elastic Beanstalk (Legacy)

> **Important**
>
> Diese Dokumentation bezieht sich auf ältere Dienste und Funktionen. Aktualisierte Anleitungen und Inhalte finden Sie im AWS.NET-Bereitstellungstool und im aktualisierten Verzeichnis Deploying toAWS.

AWS Elastic Beanstalkist ein Dienst, der die Bereitstellung vonAWS Ressourcen für Ihre Anwendung vereinfacht. AWS Elastic Beanstalkstellt die gesamteAWS Infrastruktur bereit, die für die Bereitstellung Ihrer Anwendung erforderlich ist.

Das Toolkit for Visual Studio unterstützt die Bereitstellung von ASP.NET Core-AnwendungenAWS unter Verwendung 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 Beanstalkmacht es einfach, Anwendungen in einer Vielzahl von verschiedenen Sprachen bereitzustellenAWS. 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

ASP.NET Core-Anwendungen lassen sich mit dem Toolkit for Visual Studio am einfachsten mit Elastic Beanstalk bereitstellen.

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 genutzt haben, müssen Sie nach dessen Installation zunächst IhreAWS -Anmeldeinformationen mit dem Toolkit registrieren. Einzelheiten dazu finden Sie in der Dokumentation „So geben Sie dieAWS Sicherheitsanmeldeinformationen 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 unterAWS... aus.

Wählen Sie auf der ersten Seite des Publish toAWS Elastic Beanstalk Deployment-Assistenten 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 tatsächlichenAWS 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, AWSOptionen, können Sie den Typ der zuAWS 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 den verwendetAWS SDK for .NET, um auf andereAWS Dienste zuzugreifen. 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 wurdeAWS, können Sie den Status der Elastic Beanstalk Beanstalk-Umgebung überprüfen, indem Sie die Umgebungsstatusansicht imAWS 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 die Protokolle auch aus der Umgebung oder dem Remote-Desktop in die Amazon EC2 EC2-Instances ziehen, die Teil Ihrer Elastic Beanstalk Beanstalk-Umgebung sind.

Die erste Bereitstellung einer Anwendung dauert etwas länger als die nachfolgende Neubereitstellung, da dadurch neueAWS Ressourcen geschaffen werden. 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 verpackt Ihre Anwendung mithilfe der Einstellungen aus der vorherigen Ausführung des Bereitstellungsassistenten und lädt das Anwendungspaket in die bestehende Elastic Beanstalk Beanstalk-Umgebung hoch.

So legen Sie den Wert festAWSSicherheitsanmeldeinformationen für Ihre Anwendung

DieAWSKonto, das Sie in derIn Elastic Beanstalk veröffentlichenWizard ist derAWS-Konto, das der Assistent für die Bereitstellung in Elastic Beanstalk verwenden wird.

Obwohl dies nicht empfohlen wird, müssen Sie möglicherweise auch Folgendes festlegenAWSKontoanmeldeinformationen, auf die Ihre Anwendung zugreiftAWS-Dienste, nachdem sie bereitgestellt wurden. Wir empfehlen stattdessen das Festlegen einer IAM-Rolle. In derIn Elastic Beanstalk veröffentlichen-Assistenten verwenden Sie dazu über denIdentity and Access Management-Rolle.AWSOptionenangezeigten. Im ErbeIn Amazon Web Services veröffentlichen-Assistenten verwenden Sie dazu über denIAM Role (IAM-Rolle).AWSOptionenangezeigten.

Wenn Sie verwenden müssenAWSKonto-Anmeldeinformationen statt einer IAM-Rolle können Sie dieAWS-Kontoanmeldeinformationen für Ihre Anwendung auf eine der folgenden Arten:

- Verweisen Sie auf ein Profil, das demAWS-Kontoanmeldeinformationen im`appSettings`Element des Projekts`Web.config`file. (Weitere Informationen zum Erstellen eines Profils finden Sie unterKonfigurierenAWSErweitern Sie im angezeigten Detailbereich die Option.) Im folgenden Beispiel werden Anmeldeinformationen angegeben, deren Profilname `myProfile` lautet.

```
<appSettings>
  <!-- AWS CREDENTIALS -->
  <add key="AWSProfileName" value="myProfile"/>
</appSettings>
```

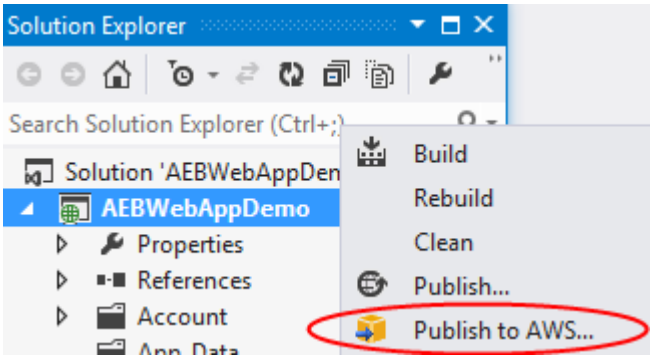
- Verwendeter ComputerIn Elastic Beanstalk veröffentlichen-Assistenten auf derAnwendungsoptionen-Seite in derSchlüsselZeilen-derSchlüsselundValue-Bereich wählen SieAWSAccessKeyaus. Geben Sie in der Zeile Value (Wert) den Zugriffsschlüssel ein. Wiederholen Sie diese Schritte fürAWSSecretKeyaus.
- Wenn 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)

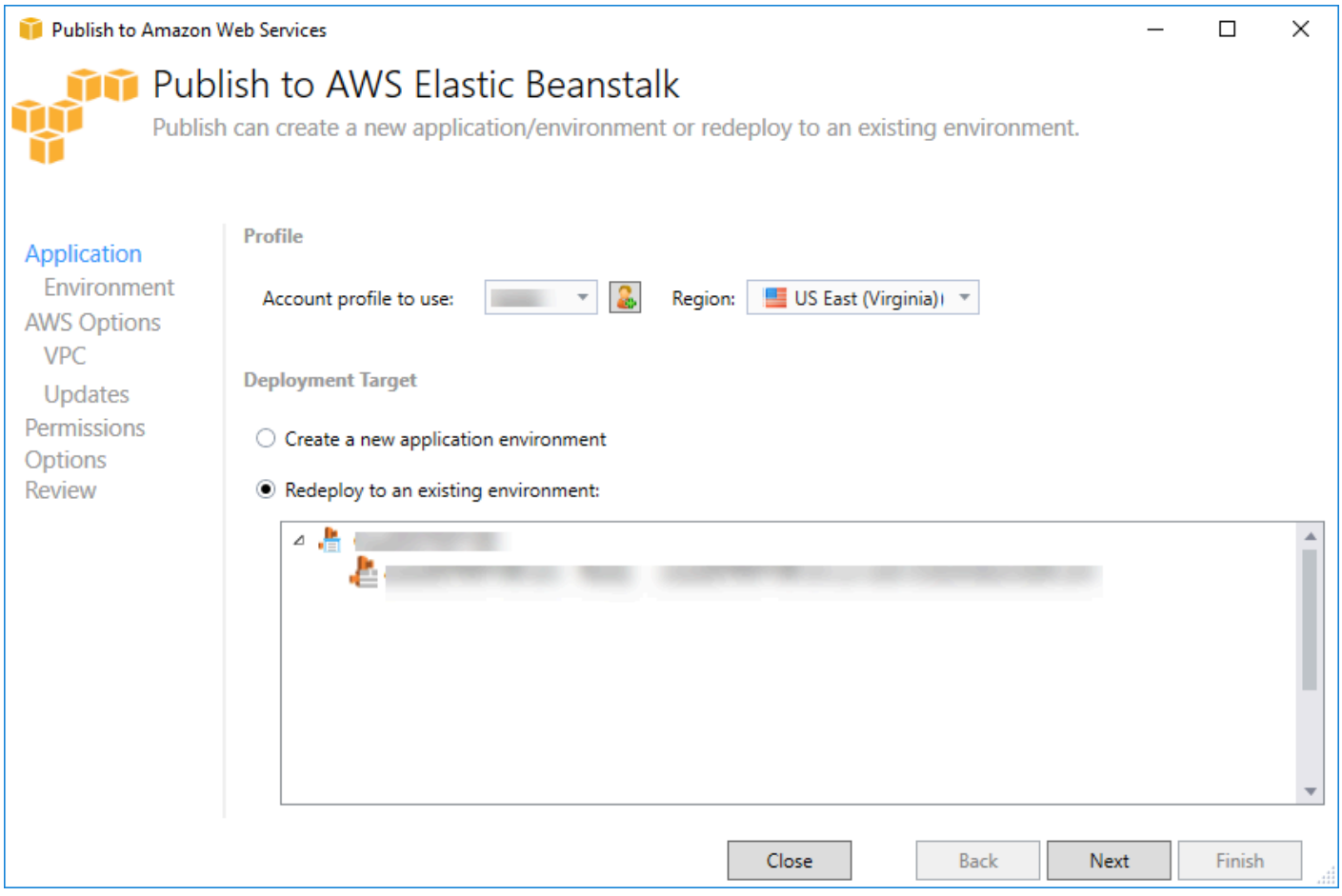
> **Important**
>
> Diese Dokumentation bezieht sich auf ältere Dienste und Funktionen. Aktualisierte Anleitungen und Inhalte finden Sie im AWS.NET-Bereitstellungstool und im aktualisierten Verzeichnis Deploying toAWS.

Sie können Ihre Anwendung iterieren, indem Sie diskrete Änderungen vornehmen und dann eine neue Version erneut in Ihrer bereits gestarteten Elastic Beanstalk Beanstalk-Umgebung veröffentlichen.

1. Öffnen Sie im Solution Explorer (Lösungs-Explorer) das Kontextmenü (mit Rechtsklick) für den WebAppDemoAEB-Projektordner für das Projekt, das Sie im vorherigen Abschnitt veröffentlicht haben, und klicken Sie dann auf Publish to (In veröffentlichen)AWS Elastic Beanstalk.

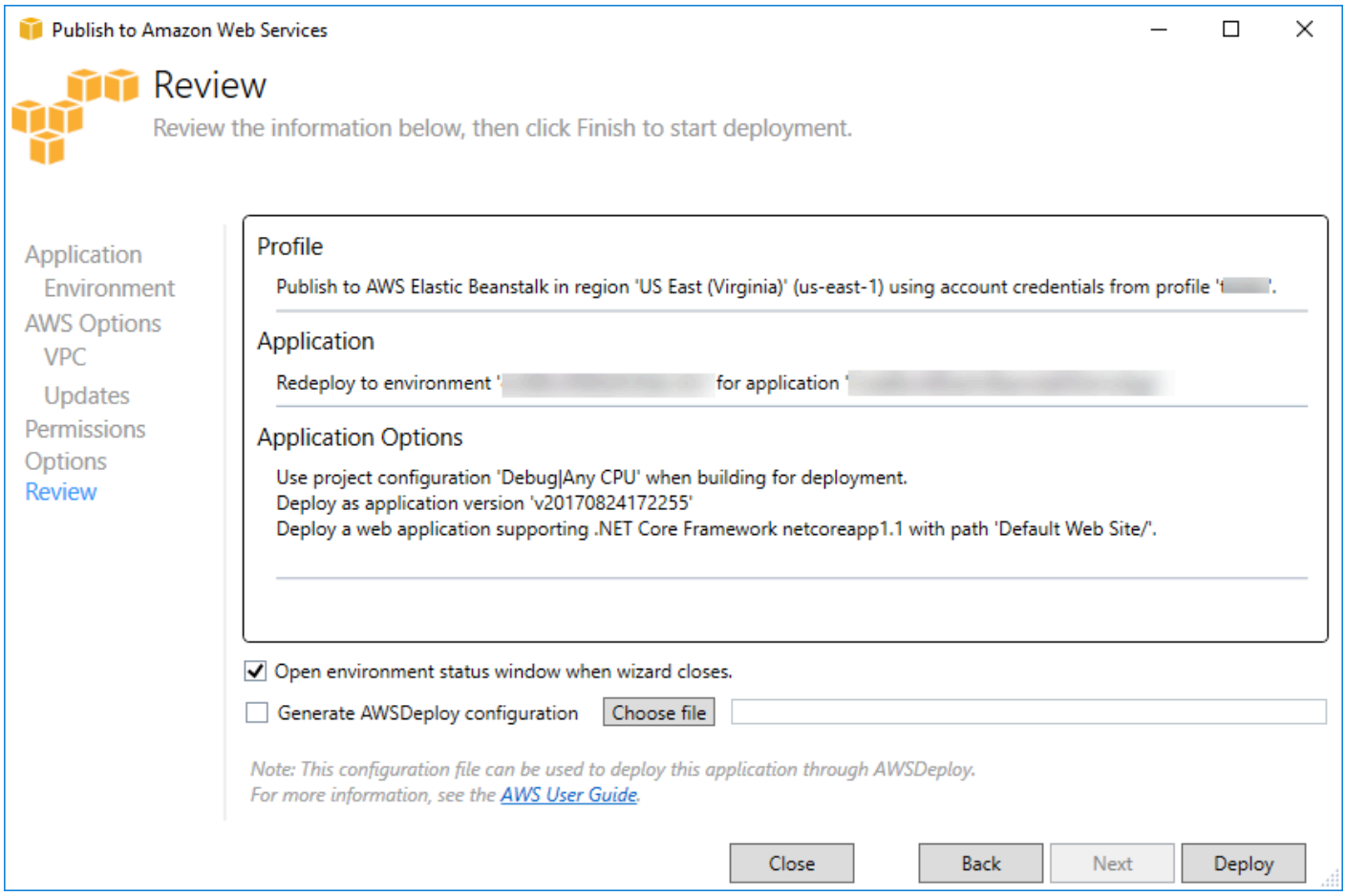


Der Publish to Elastic Beanstalk (Veröffentlichen zu Elastic Beanstalk)-Assistent wird angezeigt.



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 Next (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 die Bereitstellungsmanifest-Datei für den Microsoft Windows-Container in Elastic Beanstalk die benutzerdefinierte Bereitstellung von Anwendungen unterstützt.

Benutzerdefinierte Anwendungsbereitstellungen sind eine wichtige Funktion für fortgeschrittene Benutzer, die die Leistung von Elastic Beanstalk zum Erstellen und Verwalten ihrerAWSRessourcen, möchten aber vollständige Kontrolle darüber, wie ihre Anwendung bereitgestellt wird. Für eine benutzerdefinierte Anwendungsbereitstellung erstellen Sie Windows PowerShell-Skripte für die drei verschiedenen Aktionen, die Elastic Beanstalk durchführt. 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.

Im vorliegende Beispiel wird eine einfache statische Website bereitgestellt, jedoch mit einer benutzerdefinierten Anwendungsbereitstellung, die Sie für jede Art von Anwendung einsetzen können und bei der Sie Elastic Beanstalk die Verwaltung derAWSRessourcen dafür.

Benutzerdefinierte ASP.NET Core-Bereitstellungen in Elastic Beanstalk-Bereitstellungen in

In diesem Thema wird beschrieben, wie die Bereitstellung funktioniert und wie Sie diese anpassen können, wenn Sie mit Elastic Beanstalk und dem Toolkit for Visual Studio ASP.NET Core-Anwendungen erstellen.

Nachdem Sie alle gewünschten Schritte mit dem Bereitstellungsassistenten im Toolkit for Visual Studio abgeschlossen haben, verpackt 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 Bereitstellungsmanifest ist eine JSON-Datei mit dem Namenaws-windows-deployment-manifest.json, den der Elastic Beanstalk -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`. Dies ermöglicht Ihnen, die Datei aws-windows-deployment-manifest.json Ihrem Projekt hinzuzufügen und das Manifest anzupassen. Um dies für eine ASP.NET Core-Webanwendung in Visual Studio auszuführen, fügen Sie dem Stammverzeichnis des Projekts eine neue JSON-Datei hinzu und nennen diese aws-windows-deployment-manifest.json.

Die Manifestdatei muss aws-windows-deployment-manifest.json genannt und im Stammverzeichnis des Projekts gespeichert werden. Der Elastic Beanstalk-Container sucht das Manifest im Stammverzeichnis. Sobald er die Datei gefunden hat, ruft er das Bereitstellungstool auf. Wenn die Datei nicht vorhanden ist, greift der Elastic Beanstalk-Container auf das ältere Bereitstellungstool zurück, das davon ausgeht, dass es sich um einemsdeployArchiv.

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 die Bereitstellung

über die Optionen des Bereitstellungsassistenten hinaus anpassen.AWShat ein JSON-Schema für dasaws-windows-deployment-manifest.json-Dateiund als Sie das Toolkit for Visual Studio installiert haben, wurde bei der Einrichtung 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. Nachdem Sie das Schema ausgewählt haben, stellt Ihnen Visual Studio IntelliSense zur Verfügung, während Sie die Manifestdatei bearbeiten.

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 die Ausführung von Windows PowerShell-Skripts vor und nach Installations-, Neustart- und Deinstallationsaktionen deklarieren. Beispiel: Das folgende Manifest

führt das Windows PowerShell-Skript `PostInstallSetup.ps1` aus, um nach der Bereitstellung der ASP.NET Core-Anwendung auf IIS weitere Konfigurationen vorzunehmen. 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.ebextensions-Konfigurationsdateien werden wie bei allen anderen Elastic Beanstalk-Containern auch 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

Mit dem Bereitstellungsmanifest haben Sie die Möglichkeit, mehrere Anwendungen für dieselbe Elastic Beanstalk-Umgebung bereitzustellen.

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"
        }
      }
    ]
```

```
  }
}
```

Wenn das Manifest geschrieben ist, verwenden Sie Windows PowerShell zum Erstellen des Anwendungspakets und aktualisieren eine vorhandene Elastic Beanstalk-Umgebung, um es darin 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
```

Damit Elastic Beanstalk-Umgebung Informationen erhalten bleibt, was mit all diesen Anwendungen zu tun ist, kopieren Sie das Manifest von Ihrer Lösung in den Workspace zum Veröffentlichen und komprimieren 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)
```

Nun verfügen Sie über das Anwendungspaket und könnten die Datei über die Webkonsole in eine Elastic Beanstalk-Umgebung hochladen. Alternativ können Sie weiterhin die verwendenAWSPowerShell-Cmdlets zum Aktualisieren der Elastic Beanstalk-Umgebung mit dem Anwendungspaket. Vergewissern Sie sich, dass Sie das aktuelle Profil und die Region zum Profil sowie die Region, die Ihre Elastic Beanstalk-Umgebung enthält, festgelegt haben, indem Sie`Set-AWSCredentialsund`Set-DefaultAWSRegion-Cmdlets.

```
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
```

Nun überprüfen Sie den Status der Aktualisierung über die Statusseite der Elastic Beanstalk-Umgebung im Toolkit oder über die Webkonsole. Nachdem der Vorgang abgeschlossen ist, können Sie zu jeder Anwendung navigieren, die Sie für den, im Bereitstellungsmanifest angegebenen, IIS-Pfad bereitgestellt haben.

Bereitstellen in Amazon EC2 Container Service

> **Important**
>
> Das NeuePublish to (Zu &CW; veröffentlichen)AWSFunktion wurde entwickelt, um die Veröffentlichung von .NET-Anwendungen zu vereinfachenAWSaus. Möglicherweise werden Sie gefragt, ob Sie zu diesem Publishing-Erlebnis wechseln möchten, nachdem SiePublish Container toAWSaus. Weitere Informationen finden Sie unter So öffnen Sie denAWSin Visual Studio .

Amazon Elastic Container Service ist ein hoch skalierbarer und äußerst leistungsfähiger Container-Management-Service, der Docker-Container unterstützt und es Ihnen erlaubt, Anwendungen auf einem verwalteten Cluster von Amazon EC2 EC2-Instanzen auf einfache Art zu betreiben.

Für die Bereitstellung von Anwendungen in Amazon Elastic Container Service müssen die Anwendungskomponenten für die Ausführung in einem Docker-Container konzipiert sein. 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 über Amazon ECS finden Sie im.Elastic Container Service Dokumentationaus. Sie enthält eine Übersicht über die Docker-Grundlagen und eine exemplarische Vorgehensweise zum Erstellen eines Clusters.

Themen

Geben Sie anAWSAnmeldeinformationen für Ihre ASP.NET-Core 2

Es gibt zwei Typen von Anmeldeinformationen, die bei der Bereitstellung Ihrer Anwendung in einem Docker-Container relevant sind: Bereitstellungs-Anmeldeinformationen und Instance-Anmeldeinformationen.

Publish Container (Container veröffentlichen) verwendet, umAWSAssistent zum Erstellen der Umgebung in Amazon ECS. 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) verwendet, um auf verschiedene AWS-Services zuzugreifen. Wenn beispielsweise Ihre ASP.NET-Core 2.0-Anwendung Lese- und Schreibvorgänge für Amazon S3 -Objekte macht, 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

DieAWSKonto, das Sie imPublish Container toAWS-Assistent ist derAWS-Konto, den der Assistent für die Bereitstellung auf Amazon ECS verwendet. Das Kontoprofil muss über Berechtigungen für Amazon Elastic Compute Cloud, Amazon Elastic Container Service undAWS Identity and Access Managementaus.

Wenn Sie feststellen, dass Optionen in Dropdown-Listen fehlen, kann es sein, dass Sie nicht über die entsprechenden Berechtigungen verfügen. Wenn Sie beispielsweise einen Cluster für Ihre Anwendung erstellt haben, er aber auf derPublish Container toAWSAssistenten-Cluster-Seite 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 Ihrem Projekt das AWSSDK.Extensions.NETCore.Setup NuGet-Paket hinzu.
2. AddAWSEinstellungen für appsettings.Development.json. 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 Produktions-Instances empfehlen wir die Verwendung einer IAM-Rolle, um zu kontrollieren, worauf Ihre Anwendung (und der Service) zugreifen kann. Um beispielsweise eine IAM-Rolle mit Amazon ECS als Service-Prinzipal mit Berechtigungen für Amazon Simple Storage Service und Amazon DynamoDB von der aus zu konfigurieren, gehen Sie wie folgt vor:AWS Management Console:

1. Melden Sie sich bei der AWS Management Console an, und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Klicken Sie im Navigationsbereich der IAM-Konsole auf Roles und wählen Sie dann Create role.
3. Wählen Sie das SymbolAWS-ServiceRollentyp und wählen Sie dannEC2 Container Serviceaus.
4. Wählen Sie den Anwendungsfall EC2 Container Service Task (EC2-Container-Service-Aufgabe). Anwendungsfälle werden durch den Service definiert, damit die für den Service erforderliche Vertrauensrichtlinie enthalten ist. Klicken Sie dann auf Next (Weiter): Berechtigungen.
5. Wählen Sie die Berechtigungsrichtlinien AmazonS3FullAccess und AmazonDynamoDBFullAccess. Markieren Sie das Kontrollkästchen neben der jeweiligen Richtlinie und wählen Sie dannWeiter: 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. Beispielsweise 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.

Sie können diese Rolle alsAufgabenrolleauf derECS Task DefinitionSeite derPublish Container toAWS-Assistent.

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 AWS.NET-Bereitstellungstool und im aktualisierten Verzeichnis Deploying toAWS.

In diesem Abschnitt wird beschrieben, wie Sie denAWS 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 Fargate-Starttyps bereitzustellen. Da eine Webanwendung kontinuierlich ausgeführt werden soll, wird sie als Service bereitgestellt.

Bevor Sie Ihren Container veröffentlichen

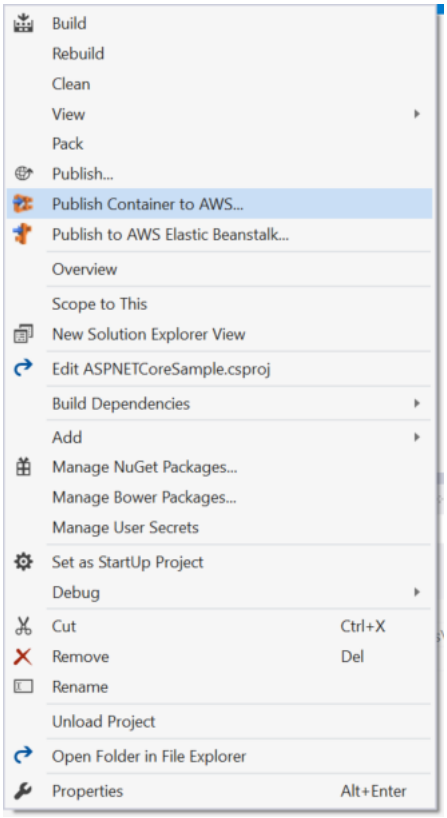
Bevor Sie den Publish Container toAWS Wizard verwenden, um Ihre ASP.NET Core 2.0-Anwendung bereitzustellen:

- Geben Sie IhreAWS Anmeldeinformationen an und richten Sie sich mit 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-App für Linux.

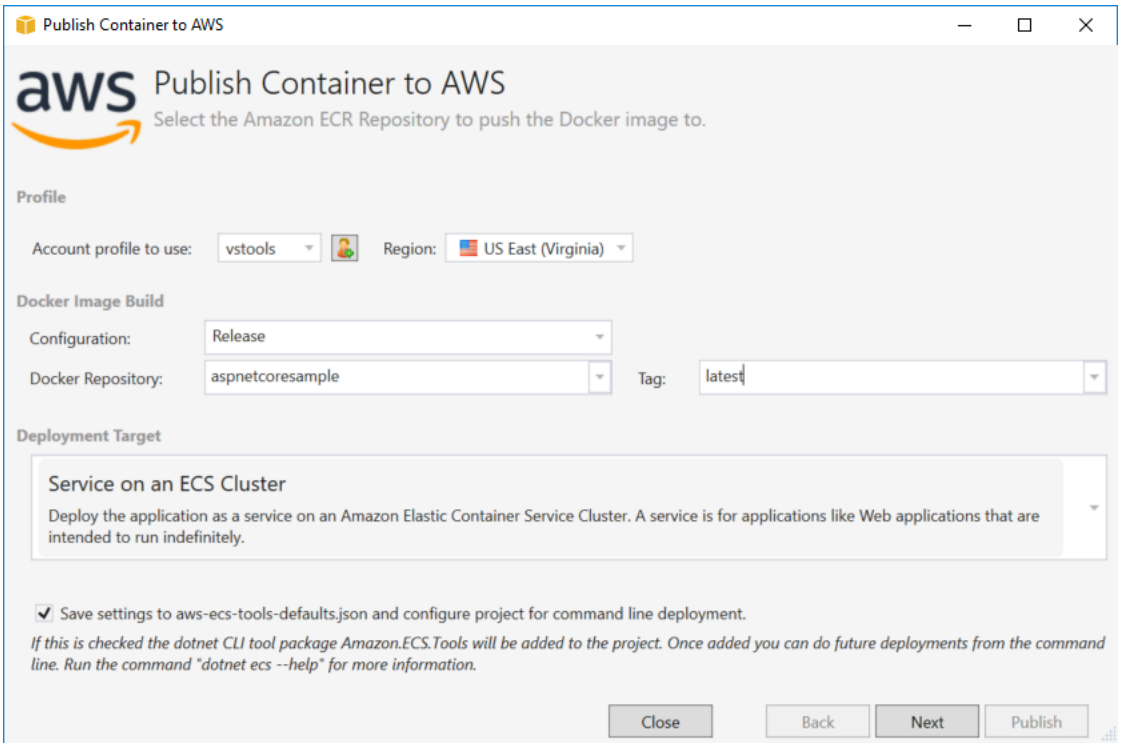
Zugreifen auf den Publish Container toAWS Wizard

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 unterAWS.



Sie können auch im Visual StudioAWS Build-Menü die Option Container veröffentlichen für auswählen.

Container imAWS 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.

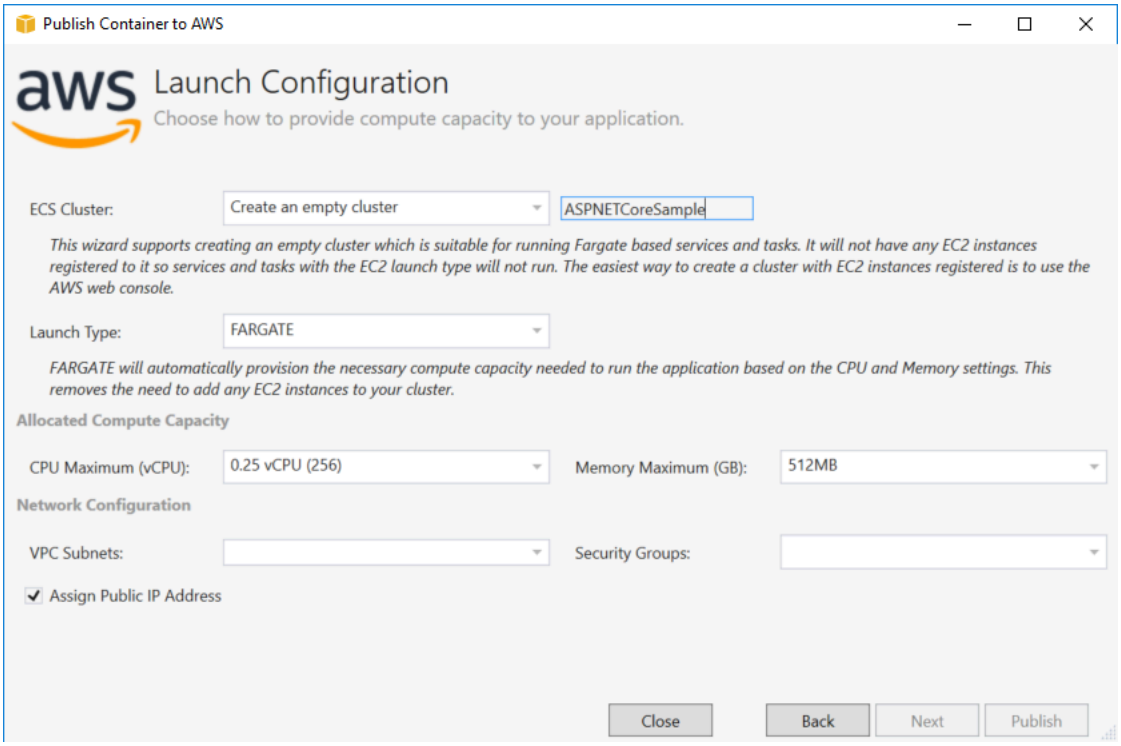
Tag – Wählen Sie ein vorhandenes Tag aus, oder geben Sie den Namen eines neuen Tags ein. Tags können wichtige Details nachverfolgen, wie Version, Optionen oder andere eindeutige Elemente des Docker-Containers.

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.

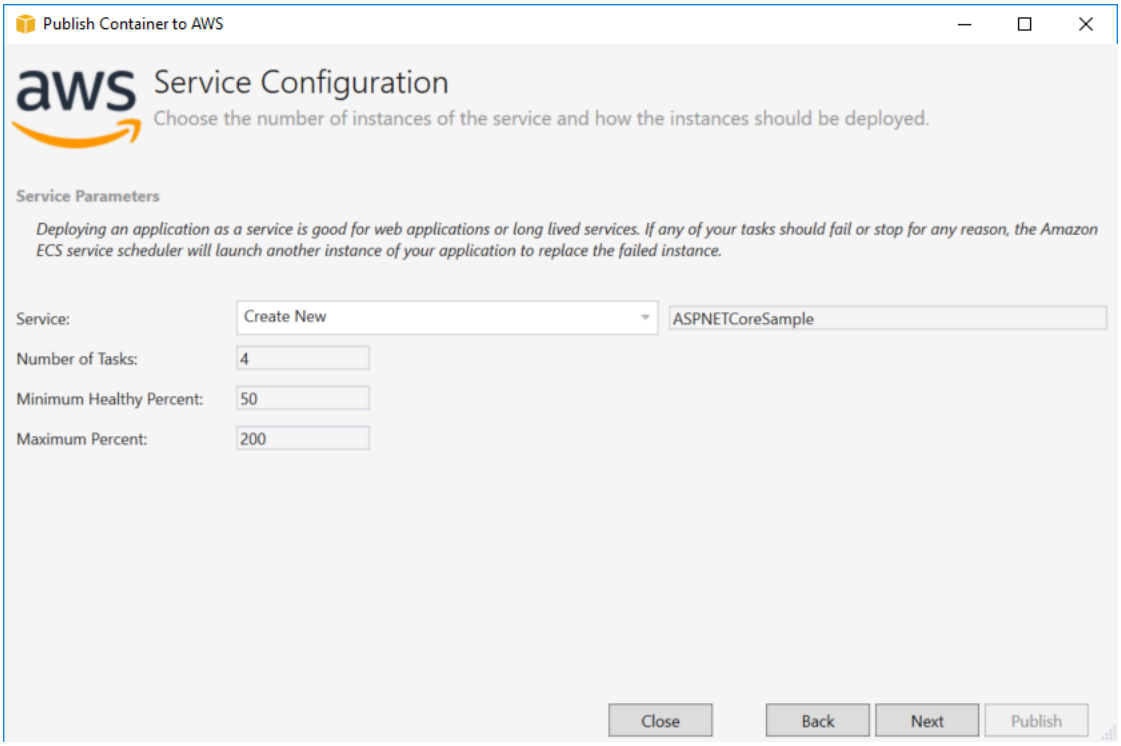
Security Groups – Wählen Sie eine Sicherheitsgruppe.

Eine Sicherheitsgruppe fungiert als Firewall für zugeordnete Amazon EC2 Instances. Sie steuern den ein- und ausgehenden Datenverkehr auf Instance-Ebene.

Standard-Sicherheitsgruppen sind so konfiguriert, dass der eingehende Datenverkehr zugelassen wird, der Instances derselben Sicherheitsgruppe zugewiesen ist, ebenso wie der gesamte ausgehende IPv4-Datenverkehr. 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



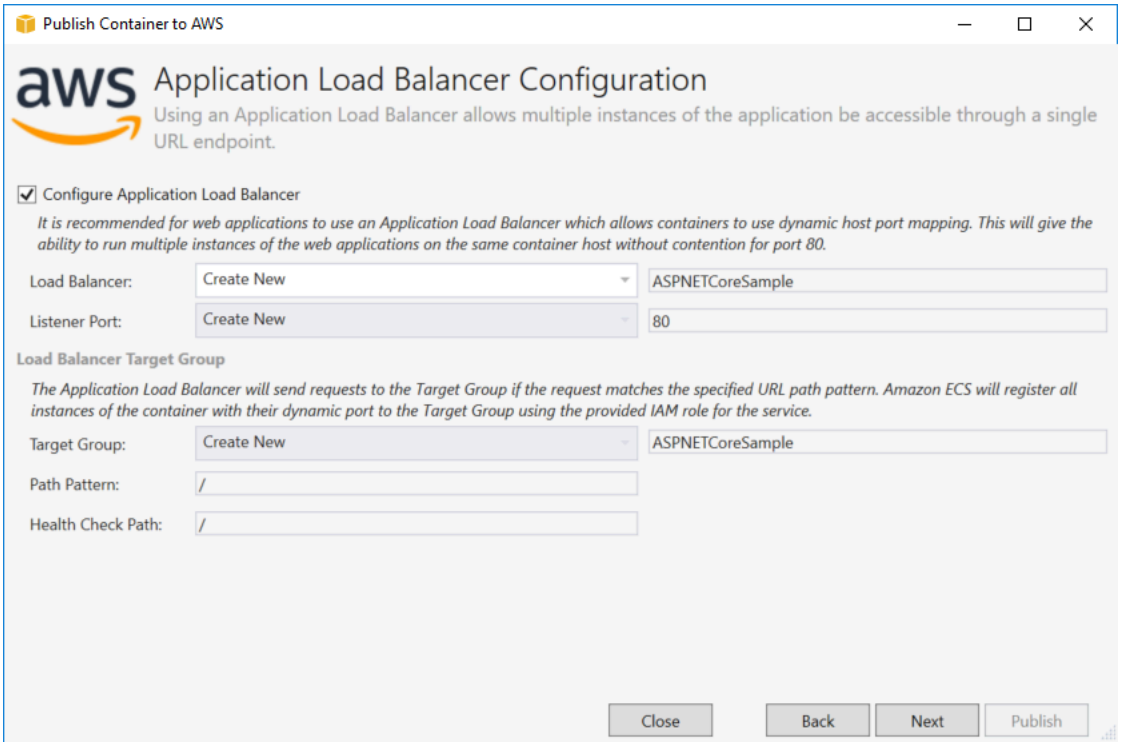
Service – Wählen Sie einen der Services in der Dropdown-Liste, um Ihren Container in einem vorhandenen Service bereitzustellen. Oder wählen Sie Create New (Neu erstellen), um einen neuen Service zu erstellen. Servicenamen in einem Cluster müssen eindeutig sein. Sie können jedoch ähnlich benannte Services 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`.

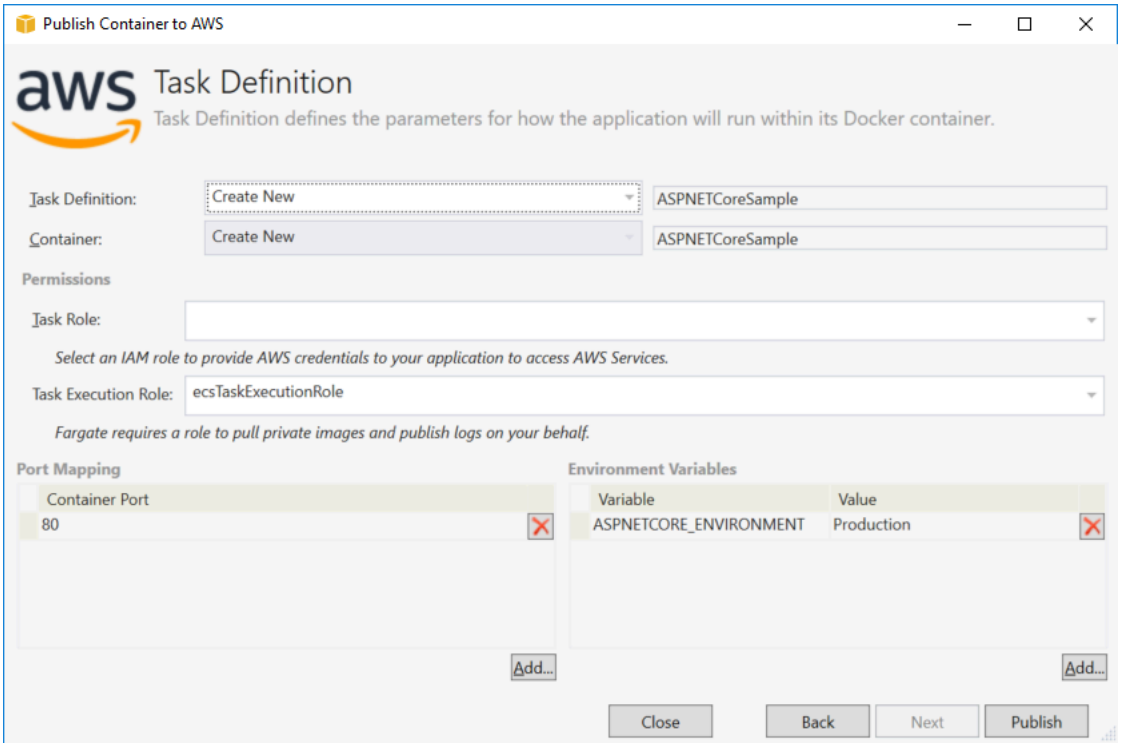
Zielgruppe — Wählen Sie die Zielgruppe aus, für die Amazon ECS die Aufgaben für den Service registrieren soll.

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 aufAWS Dienste benötigt. So werden Ihrer Anwendung Anmeldeinformationen übergeben. Erfahren Sie, wie SieAWS Sicherheitsanmeldeinformationen für Ihre Anwendung angeben.

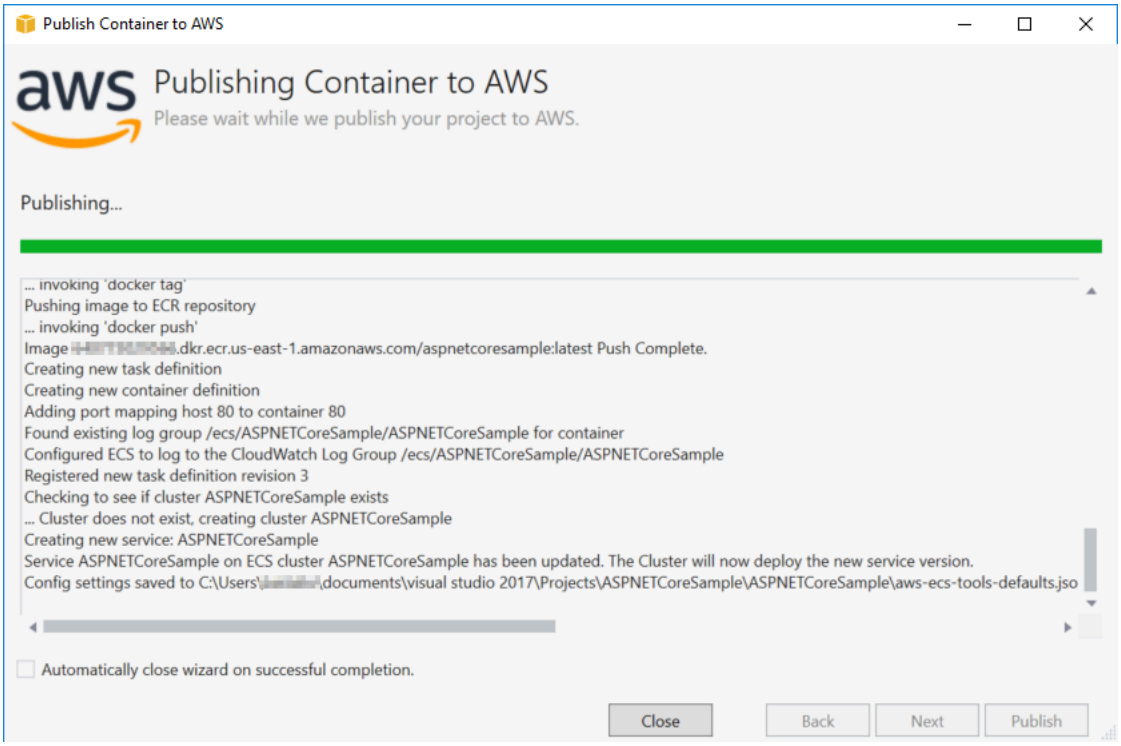
Rolle zur Aufgabenausführung — Wählen Sie eine Rolle mit Berechtigungen zum Abrufen privater Bilder und zum Veröffentlichen von Protokollen aus. AWS Fargate wird es in Ihrem Auftrag verwenden.

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 inAWS



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.

Die URL Ihrer neuen Instanzen finden Sie imAWS Explorer. Erweitern Sie Amazon ECS und Cluster und klicken Sie dann auf Ihren Cluster.

Bereitstellung einer ASP.NET Core 2.0-App für Amazon ECS (EC2)

In diesem Abschnitt wird die Verwendung vonPublish Container inAWSAssistent, der im Toolkit for Visual Studio bereitgestellt wird, eine auf Container ausgelegte ASP.NET-Core 2.0-Anwendung für

Linux über Amazon ECS unter Verwendung des EC2-Starttyps bereitstellen. Da eine Webanwendung kontinuierlich ausgeführt werden soll, wird sie als Service bereitgestellt.

Bevor Sie Ihren Container veröffentlichen

Bevor Sie dasPublish Container inAWSUm Ihre ASP.NET Core 2.0-Anwendung bereitzustellen:

- Geben Sie IhreAWSReferenzenundSetup mit Amazon ECSaus.
- 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 ASP.NET Core 2.0-Containerapp, die auf Linux ausgerichtet ist.

Zugriff auf den Publish Container toAWSWizard

Um eine auf Container ausgelegte ASP.NET Core 2.0 Anwendung für Linux bereitzustellen, klicken Sie mit der rechten Maustaste im Projektmappen-Explorer auf das Projekt und wählenPublish Container inAWSaus.

Sie können auch auswählenPublish Container inAWSim Visual Studio Build-Menü.

Publish Container inAWSAssistent

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 haben folgende OptionenErstellen eines ECS-ClustersVerwendung desAWS-Managementkonsole.

Launch Type – 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 über Availability Zones und über Container-Instances mit der geringsten verfügbaren Menge an Arbeitsspeicher.
- BinPack: Verteilt Aufgaben basierend auf der geringsten verfügbaren Menge von CPU oder Arbeitsspeicher.
- 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 Task-Rolle für eine IAM-Rolle, die dem Container gestattet,AWSAPIs, die in den zugehörigen Richtlinien in Ihrem Namen angegeben sind. So werden Ihrer Anwendung Anmeldeinformationen übergeben. Siehe .AngebenAWSSicherheitsanmeldeinformationen für Ihre Anwendungaus.

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.

Publish Container inAWS

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 Instances in derAWSExplorer. 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 Fehlerbehebung zu den Diensten aus dem Toolkit AWS Toolkit for Visual Studio und zur Arbeit mit den 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.

- 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

So finden Sie Ihre AWS Toolkit-Logs

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 CodeWhisperer Sign In und Sign Out sind deaktiviert

Wenn Sie ein Problem mit dem CodeWhisperer Service haben, bei dem sowohl die Menüelemente Anmelden als auch Abmelden deaktiviert sind, beheben Sie das Problem, indem Sie die folgenden Schritte ausführen.

1. Navigieren Sie im Windows-Datei-Explorer zum AWS Toolkit-Cache-Ordner unter:`%LOCALAPPDATA%/aws/toolkits/language-servers/CodeWhisperer`.
2. Löschen Sie den Inhalt des Cache-Ordners.
3. Schließt die aktuelle Lösung und öffnet sie erneut.

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 AWS Verantwortung von Ihnen und Ihnen. 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 gilt für den Datenschutz in AWS Toolkit for Visual Studio. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der die AWS Cloud gesamte Infrastruktur läuft. 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 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).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- 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 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

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 mit Toolkit for Visual Studio oder anderen Tools arbeiten und die Konsole, die API oder AWS SDKs AWS-Services verwenden. AWS CLI 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 Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern 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. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer 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 des von AWS-Service Ihnen verwendeten.

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, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. 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 Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS 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. Sie können darauf zugreifen, 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 und verwenden Sie diese, 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 einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten 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 Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen 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 Verwenden von IAM-Rollen 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 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 So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. 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 EC2 ausgeführte Anwendungen — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS

Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

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. Berechtigungen in den Richtlinien bestimmen, ob die 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 bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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 Erstellen von IAM-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 eingebundenen Richtlinie wählen, finden Sie unter Auswahl 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.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

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.
- Service Control Policies (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 innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs 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. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, 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 unterWie 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 So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien 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:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

> **Note**
>
> AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- 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— Auf diese AWS-Service Weise erhalten Sie 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. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- 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 Toolkit for Visual Studio 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 Toolkit for Visual Studio zu suchen.

Dokumenthistorie des AWS Toolkit for Visual Studio Benutzerhandbuchs

Letzte Aktualisierung der Dokumentation: 21. April 2021

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
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
Aktualisierung und Wartung von Inhalten	Aktualisierung von Inhalten aufgrund von Änderungen an der Benutzeroberfläche und den AWS Stilrichtlinien.	6. März 2024

Aktualisierungen bei 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 Inhaltsverzeichnissen „Erste Schritte“ und „Authentifizierung und Zugriff“.	22. Juni 2023
Authentifizierung und Zugriff	Das Bereitstellen 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
Neues allgemeines Thema zur Problembehandlung	Das Thema Problembehandlung enthält allgemeine Informationen zur Fehlerbehebung für die AWS Toolkit for Visual Studio und die zugehörigen Dienste.	30. April 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

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 auf Amazon EC2 Container Service	Es wurden Informationen zur Bereitstellung für den 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	Informationen zur Bereitstellung einer containerisierten ASP.NET Core 2.0-Anwendung für Linux über Amazon ECS mit dem EC2-Starttyp wurden hinzugefügt.	16. Februar 2018
Anmeldeinformationen für die Bereitstellung auf Amazon EC2 Container Service	Es wurden Informationen zum Angeben von Anmeldeinformationen bei der Bereitstellung für den 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.