Guía del usuario

AWS Kit de herramientas con Amazon Q

AWS Kit de herramientas con Amazon Q: Guía del usuario

Table of Contents

AWS Kit de herramientas con Amazon Q

Esta es la guía del usuario de AWS Toolkit for Visual Studio. Si está buscando el Kit de herramientas de AWS para Visual Studio Code, consulte la Guía del usuario de AWS Toolkit for Visual Studio Code.

Qué es el Kit de herramientas para Visual Studio

AWS Toolkit for Visual Studio Es un complemento para el IDE de Visual Studio que facilita el desarrollo, la depuración y la implementación de aplicaciones.NET que utilizan Amazon Web Services. El Toolkit for Visual Studio es compatible con las versiones 2019 y posteriores de Visual Studio. Para obtener más información sobre cómo descargar e instalar el kit, consulte el tema Instalación y configuración de esta Guía del usuario.

> **Note**
>
> El Toolkit for Visual Studio también se publicó para las versiones 2008, 2010, 2012, 2013, 2015 y 2017 de Visual Studio. Sin embargo, estas versiones ya no son compatibles. Para obtener más información, consulte el tema Instalación y configuración de esta Guía del usuario.

El Kit de herramientas para Visual Studio contiene las siguientes características para mejorar su experiencia de desarrollo.

AWS Explorador

Se puede acceder a la ventana de herramientas del AWS explorador en el menú Ver del IDE y le permite interactuar con AWS los servicios de Visual Studio. Para obtener una lista de AWS los servicios y características compatibles, consulte el tema Cómo trabajar con AWS servicios de esta Guía del usuario.

Amazon Q

Hable con un desarrollador de Amazon Q en Visual Studio para hacerle preguntas sobre la creación AWS y obtener ayuda con el desarrollo de software. Amazon Q puede explicar conceptos de

codificación y fragmentos de código, generar código y pruebas unitarias y mejorar el código mediante la depuración o la refactorización.

Para instalar y configurar Amazon Q para el Toolkit for Visual Studio, consulte el tema Introducción de esta Guía del usuario. Para obtener más información sobre cómo trabajar con Amazon Q Developer, consulte el tema Amazon Q Developer in IDE en la Guía del usuario para desarrolladores de Amazon Q. Para obtener información detallada sobre los planes y precios de Amazon Q, consulta la guía de precios de Amazon Q.

Información relacionada

Para abrir un tema o ver los temas pendientes actualmente, visite https://github.com/aws/ aws-toolkit-visual-studio /issues.

Para obtener más información acerca de Visual Studio, visite https://visualstudio.microsoft.com/vs/.

Amazon Q

¿Qué es Amazon Q?

A partir del 30 de abril de 2024, Amazon CodeWhisperer pasa a formar parte de Amazon Q Developer, lo que incluye sugerencias de código en línea y escaneos de seguridad.

Para obtener más información sobre cómo trabajar con Amazon Q Developer en AWS Toolkit for Visual Studio, consulte el tema Amazon Q Developer in IDEs en la Guía del usuario para desarrolladores de Amazon Q. Para obtener información detallada sobre los planes y precios de Amazon Q, consulta la guía de precios de Amazon Q.

Descarga del Kit de herramientas para Visual Studio

Puede descargar, instalar y configurar el Kit de herramientas para Visual Studio en Visual Studio Marketplace en su IDE. Para obtener instrucciones detalladas, consulte la sección Instalación del Kit de herramientas de AWSpara Visual Studio en el tema Introducción de esta Guía del usuario.

Descarga del Kit de herramientas en Visual Studio Marketplace

Descargue los archivos de instalación del Kit de herramientas para Visual Studio desde el sitio de descargas de AWS para Visual Studio en su navegador web.

Kits de herramientas de IDE adicionales de AWS

Además del kit de herramientas para Visual StudioAWS, también ofrece kits de herramientas IDE para VS Code y. JetBrains

Enlaces al AWS Toolkit for Visual Studio Code

- Siga este enlace para descargar el AWS Toolkit for Visual Studio Code desde VS Code Marketplace.
- Para obtener más información sobre el AWS Toolkit for Visual Studio Code, consulte la Guía del usuario de AWS Toolkit for Visual Studio Code.

Enlaces al AWS Toolkit for JetBrains

- Siga este enlace para descargarlo AWS Toolkit for JetBrains del JetBrains Marketplace.
- Para obtener más información sobre el AWS Toolkit for JetBrains, consulte la Guía del usuario de AWS Toolkit for JetBrains.

Introducción

El AWS Toolkit for Visual Studio hace que sus servicios y recursos de AWS estén disponibles directamente desde su entorno de desarrollo integrado (IDE) de Visual Studio.

Para ayudarle a empezar, en los siguientes temas se explica cómo preparar, instalar y configurar el AWS Toolkit for Visual Studio.

Temas

Instalación y configuración del AWS Toolkit for Visual Studio

En los temas siguientes se describe cómo descargar, instalar, configurar y desinstalar el AWS Toolkit for Visual Studio.

Temas

Requisitos previos

A continuación se enumeran los requisitos previos para configurar las versiones compatibles del AWS Toolkit for Visual Studio.

- Visual Studio 19 o una versión posterior
- Windows 10 o una versión posterior
- Acceso de administrador a Windows y a Visual Studio
- Credenciales AWS de IAM activas

> **Note**
>
> AWS Toolkit for Visual Studio Hay versiones no compatibles de las disponibles para Visual Studio 2008, 2010, 2012, 2013, 2015 y 2017. Para descargar una versión no compatible, vaya a la página de AWS Toolkit for Visual Studio y elija la versión que desee en la lista de enlaces de descarga.
> Para obtener más información sobre las credenciales de IAM o para crear una cuenta, vaya a la puerta de enlace de la consola de AWS.

Instalación del AWS Toolkit for Visual Studio

Para instalarlo AWS Toolkit for Visual Studio, busque su versión de Visual Studio mediante los siguientes procedimientos y complete los pasos necesarios. Los enlaces de descarga de todas las versiones AWS Toolkit for Visual Studio se encuentran en la página de AWS Toolkit for Visual Studioinicio.

> **Note**
>
> Si tiene problemas durante la instalación AWS Toolkit for Visual Studio, consulte el tema Solución de problemas de instalación de esta guía.

Instalación del AWS Toolkit for Visual Studio para Visual Studio 2022

Para instalar AWS Toolkit for Visual Studio 2022 desde Visual Studio, complete los siguientes pasos:

1. En el menú principal, vaya a Extensiones y seleccione Administrar extensiones.
2. En el cuadro de búsqueda, busque AWS.
3. Pulse el botón Descargar de la versión que corresponda de Visual Studio 2022 y siga las instrucciones de instalación.

   > **Note**
   >
   > Es posible que tenga que cerrar y reiniciar Visual Studio manualmente para completar el proceso de instalación.

4. Cuando se hayan completado la descarga y la instalación, puede abrirlas AWS Toolkit for Visual Studio seleccionando el AWS Explorador en el menú Ver.

Instalación del AWS Toolkit for Visual Studio para Visual Studio 2019

Para instalar AWS Toolkit for Visual Studio 2019 desde Visual Studio, complete los siguientes pasos:

1. En el menú principal, vaya a Extensiones y seleccione Administrar extensiones.
2. En el cuadro de búsqueda, busque AWS.
3. Pulse el botón Descargar de Visual Studio 2017 y 2019 y siga las instrucciones.

> **Note**
>
> Es posible que tenga que cerrar y reiniciar Visual Studio manualmente para completar el proceso de instalación.

4. Cuando se hayan completado la descarga y la instalación, puede abrirlas AWS Toolkit for Visual Studio seleccionando el AWS Explorador en el menú Ver.

Desinstalando el AWS Toolkit for Visual Studio

Para desinstalarlo AWS Toolkit for Visual Studio, busque su versión de Visual Studio mediante los siguientes procedimientos y complete los pasos necesarios.

Desinstalar el AWS Toolkit for Visual Studio para Visual Studio 2022

Para desinstalar AWS Toolkit for Visual Studio 2022 de Visual Studio, complete los siguientes pasos:

1. En el menú principal, vaya a Extensiones y seleccione Administrar extensiones.
2. En el menú de navegación Administrar extensiones, expande el encabezado Instalado.
3. Localice la extensión AWS Toolkit for Visual Studio 2022 y pulse el botón Desinstalar.

> **Note**
>
> Si AWS Toolkit for Visual Studio no está visible en la sección Instalados del menú de navegación, es posible que deba reiniciar Visual Studio.

4. Siga las indicaciones que aparecen en pantalla para completar el proceso.

Desinstalar el AWS Toolkit for Visual Studio para Visual Studio 2019

Para desinstalar AWS Toolkit for Visual Studio 2019 de Visual Studio, complete los siguientes pasos:

1. En el menú principal, vaya a Herramientas y seleccione Administrar extensiones.
2. En el menú de navegación Administrar extensiones, expande el encabezado Instalado.
3. Localice la extensión AWS Toolkit for Visual Studio 2019 y pulse el botón Desinstalar.
4. Siga las indicaciones que aparecen en pantalla para completar el proceso.

Desinstalar el AWS Toolkit for Visual Studio para Visual Studio 2017

Para desinstalar AWS Toolkit for Visual Studio 2017 en Visual Studio, complete los siguientes pasos:

1. En el menú principal, vaya a Herramientas y seleccione Extensiones y actualizaciones.
2. En el menú de navegación Extensiones y actualizaciones, expande el encabezado Instalado.
3. Localice la extensión AWS Toolkit for Visual Studio 2017 y pulse el botón Desinstalar.
4. Siga las indicaciones que aparecen en pantalla para completar el proceso.

Desinstalar el AWS Toolkit for Visual Studio para Visual Studio 2013 o 2015

Para desinstalar AWS Toolkit for Visual Studio 2013 o 2015, complete los siguientes pasos:

1. Desde el panel de control de Windows, abra Programas y características.

   > **Note**
   >
   > Puede abrir Programas y características inmediatamente ejecutando `appwiz.cpl` en la línea de comandos de Windows o desde el cuadro de diálogo Ejecutar de Windows.

2. En la lista de programas instalados, abra el menú contextual (clic con el botón derecho) de Herramientas de AWS para Windows.
3. Seleccione Desinstalar y siga las instrucciones para completar el proceso de desinstalación.

> **Note**
>
> El directorio Muestras no se elimina durante el proceso de desinstalación. Este directorio se conserva por si se han modificado las muestras. Se debe eliminar manualmente.

Conectarse a AWS

La mayoría de los servicios y recursos de Amazon Web Services (AWS) se administran a través de una AWS cuenta. No es necesaria una AWS cuenta para utilizarlos AWS Toolkit for Visual Studio, pero las funciones del kit de herramientas están limitadas sin conexión.

Si ha configurado previamente una AWS cuenta y la autenticación a través de otro AWS servicio (como el AWS Command Line Interface), el Toolkit for Visual Studio detectará automáticamente sus credenciales.

Requisitos previos

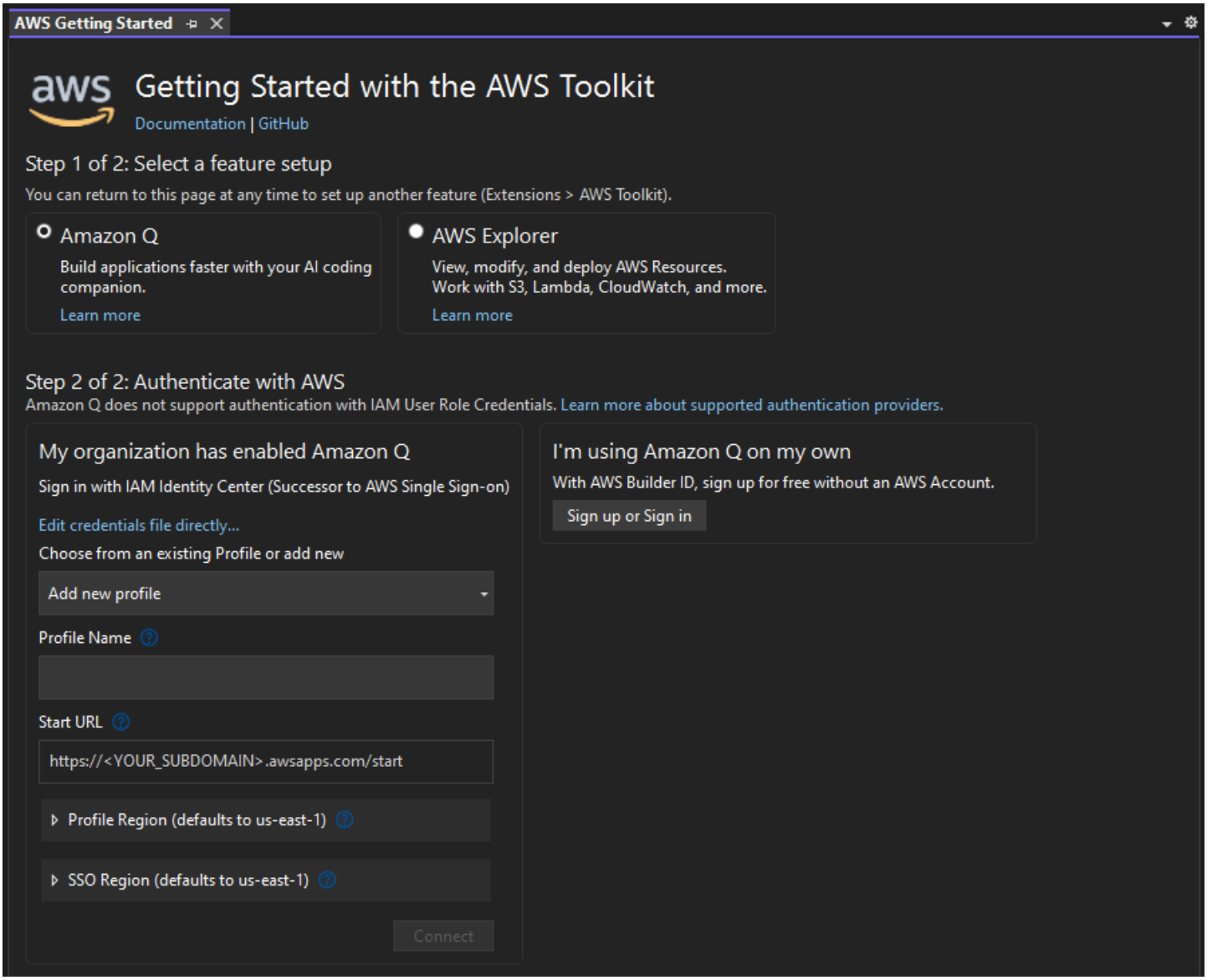
Si es la primera vez que ha creado una cuenta AWS o no la ha creado, debe seguir tres pasos principales para conectar el Toolkit for Visual Studio con AWS su cuenta:

1. Crear una AWS cuenta: puede crear una AWS cuenta desde el portal de AWS registro. Para obtener información detallada sobre cómo configurar una AWS cuenta nueva, consulta el tema de descripción general de la Guía del usuario de AWS configuración.
2. Configuración de la autenticación: existen tres métodos principales para autenticarse con la AWS cuenta del Toolkit for Visual Studio. Para obtener más información sobre cada uno de estos métodos, consulte el tema Autenticación y acceso de esta Guía del usuario.
3. Autenticación AWS desde el kit de herramientas: puede conectarse con su AWS cuenta desde el kit de herramientas siguiendo los procedimientos de las siguientes secciones de esta Guía del usuario.

Conectarse a desde el kit AWS de herramientas

Para conectarse a sus AWS cuentas desde el Toolkit for Visual Studio, abra la interfaz de usuario Getting Started with AWS the Toolkit (interfaz de usuario de conexión) siguiendo este procedimiento.

1. En el menú principal de Visual Studio, expanda las extensiones y, a continuación, expanda el AWS kit de herramientas.
2. En las opciones del menú del AWS kit de herramientas, seleccione Cómo empezar.
3. La interfaz de usuario de conexión para empezar con el AWS kit de herramientas se abre en Visual Studio.



En la siguiente tabla se describen los métodos de autenticación compatibles con cada característica. Para obtener más información sobre cada uno de los tres métodos de autenticación AWS IAM Identity Center, AWS Identity and Access Management las credenciales y el AWS identificador de compilación, consulte el índice de autenticación y acceso de esta guía del usuario.

> **Note**
>
> En la actualidad, al trabajar con CodeCatalyst el Toolkit for Visual Studio, solo es necesario que autorice con AWS su ID de creador al clonar un repositorio de terceros.

Amazon Q Developer	AWS Explorador	Amazon CodeCatalyst
☑ ID de AWS constructor	☒ ID de AWS constructor	☑ ID de AWS constructor
☑ Centro de identidades de IAM	☑ Centro de identidades de IAM	☒ Centro de identidad de IAM
☒ AWS Credenciales de IAM	☑ AWS Credenciales de IAM	☒ Credenciales de AWS IAM

Autenticación para desarrolladores de Amazon Q

Para empezar a usar Amazon Q Developer, autentícate y conéctate con tus credenciales de ID AWS IAM Identity Center o de AWS Builder ID.

Los siguientes procedimientos describen cómo autenticar y conectar el kit de herramientas con su cuenta de AWS .

Autentíquese y conéctese con el Centro de identidades de IAM

1. En la interfaz de usuario de conexión Getting Started with the AWS Toolkit, seleccione la radial Amazon Q Developer para ampliar las opciones de autenticación de Amazon Q Developer.

   > **Note**
   >
   > Si no hay credenciales almacenadas, continúe con el paso 3 para añadir o actualizar las credenciales del IAM Identity Center.

2. En la sección Mi organización ha habilitado Amazon Q Developer, expande el menú desplegable Elegir entre un perfil existente o añadir un nuevo para elegir de la lista de credenciales almacenadas.
3. En el menú desplegable del tipo de perfil, selecciona AWS IAM Identity Center

4. En el campo de texto Nombre del perfil, introduzca el perfil **`Profile Name`** del Centro de Identidad de IAM con el que desee autenticarse.
5. En el campo de texto URL de inicio, introduzca la **`Start URL`** que está adjunta a sus credenciales del IAM Identity Center.
6. En el menú desplegable Región del perfil (por defecto es us-east-1), seleccione la región del perfil definida por el perfil de usuario del Centro de identidades de IAM con el que se está autenticando.
7. En el menú desplegable Región de SSO (por defecto es us-east-1), seleccione la región de SSO definida por las credenciales del IAM Identity Center y, a continuación, pulse el botón Connect para abrir el cuadro de diálogo Iniciar sesión con IAM Identity Center. AWS
8. En el cuadro de diálogo Iniciar sesión con el Centro de Identidad de AWS IAM, pulse el botón Ir al navegador para abrir el sitio de solicitudes de AWS autorización en su navegador web predeterminado.
9. Siga las instrucciones del navegador web predeterminado, recibirá una notificación cuando se complete el proceso de autorización, podrá cerrar el navegador de forma segura y volver a Visual Studio.

Autenticate y conéctate con un ID de constructor AWS

1. En la interfaz de usuario de conexión Getting Started with the AWS Toolkit, seleccione la radial Amazon Q Developer para ampliar las opciones de autenticación de Amazon Q Developer.
2. En la sección Estoy usando Amazon Q Developer on my own, selecciona el botón Registrarse o Iniciar sesión para abrir el cuadro de diálogo Iniciar sesión con AWS Builder ID.
3. Pulse el botón Ir al navegador para abrir el sitio de solicitud de AWS autorización en su navegador web predeterminado.
4. Siga las instrucciones del navegador web predeterminado, recibirá una notificación cuando se complete el proceso de autorización, podrá cerrar el navegador de forma segura y volver a Visual Studio.

Autenticación para el explorador AWS

Para empezar a trabajar con el AWS Explorer desde el kit de herramientas, autentifíquese y conéctese con sus credenciales del IAM Identity Center o con las credenciales de IAM.

Los siguientes procedimientos describen cómo autenticar y conectar el kit de herramientas con su cuenta de AWS .

Autentíquese y conéctese con el Centro de identidades de IAM

1. En la interfaz de usuario de conexión Getting Started with the AWS Toolkit, seleccione la radial AWS Explorer para ampliar las opciones de autenticación de Amazon Q Developer.
2. En el menú desplegable **`Profile Type`**, elija AWS IAM Identity Center.
3. En el campo de texto del nombre del perfil, introduzca el perfil **`Profile Name`** del IAM Identity Center que desee utilizar.
4. En el campo de texto URL de inicio, introduzca la **`Start URL`** que está adjunta a sus credenciales del IAM Identity Center.
5. En el menú desplegable Región del perfil (por defecto es us-east-1), seleccione la región del perfil definida por el perfil de usuario del Centro de identidades de IAM con el que se está autenticando.
6. En el menú desplegable Región de SSO (por defecto es us-east-1), seleccione la región de SSO definida por las credenciales del centro de identidad de IAM.
7. Pulse el botón Ir al navegador para abrir el sitio de solicitud de AWS autorización en su navegador web predeterminado.
8. Siga las instrucciones del navegador web predeterminado, recibirá una notificación cuando se complete el proceso de autorización, podrá cerrar el navegador de forma segura y volver a Visual Studio.

Autentíquese y conéctese con las credenciales de IAM

1. En la interfaz de usuario de conexión Getting Started with the AWS Toolkit, seleccione la radial AWS Explorer para ampliar las opciones de autenticación de Amazon Q Developer.
2. **`Profile Type`**En el menú desplegable, elija el rol de usuario de IAM.
3. En el campo de texto del nombre **`Profile Name`** del perfil, introduzca el perfil con el que desea autenticarse.
4. En el campo de texto del identificador de clave de acceso, introduzca **`Access Key ID`** el del perfil con el que desee autenticarse.
5. En el campo de texto de la clave secreta, introduce **`Secret Key`** la del perfil con el que deseas autenticarte.

6. En el menú desplegable Ubicación de almacenamiento (el valor predeterminado es Archivo de credenciales compartidas), especifique si desea almacenar sus credenciales en un archivo de credenciales compartidas o almacenadas cifradas de.NET.
7. En el menú desplegable Región del perfil (por defecto es us-east-1), selecciona la región del perfil que está adjunta al perfil con el que deseas autenticarte.

Solución de problemas de instalación del AWS Toolkit for Visual Studio

Se sabe que la siguiente información resuelve problemas de instalación comunes al configurar el AWS Toolkit for Visual Studio.

Si se produce un error durante la instalación AWS Toolkit for Visual Studio o no está claro si la instalación se ha completado o no, revise la información de cada una de las siguientes secciones.

Permisos de administrador de Visual Studio

La AWS Toolkit for Visual Studio extensión requiere permisos de administrador para garantizar que se pueda acceder a todos los AWS servicios y funciones.

Si tiene permisos de administrador local, es posible que sus permisos de administrador no se extiendan directamente a su instancia de Visual Studio.

Para iniciar Visual Studio con permisos de administrador en local:

1. Desde Windows, busque el lanzador de aplicaciones de Visual Studio (icono).
2. Abra el menú contextual (haga clic con el botón derecho) del icono de Visual Studio para abrir el menú contextual.
3. Seleccione Ejecutar como administrador en el menú contextual.

Para iniciar Visual Studio con permisos de administrador en remoto:

1. Desde Windows, busque el iniciador de aplicaciones de la aplicación que esté utilizando para conectarse a su instancia remota de Visual Studio.
2. Abra el menú contextual (haga clic con el botón derecho) del icono de la aplicación para abrir el menú contextual.
3. Seleccione Ejecutar como administrador en el menú contextual.

> **Note**
>
> Tanto si ejecuta el programa de forma local como si se conecta en remoto, es posible que Windows le pida que confirme sus credenciales administrativas.

Obtención de un registro de instalación

Si ha completado los pasos de la sección anterior Permisos de administrador que se encuentra más arriba y ha confirmado que está ejecutando Visual Studio o se está conectando al programa con permisos de administrador, la obtención de un archivo de registro de instalación puede ayudarle a diagnosticar otros problemas.

Para instalarla manualmente AWS Toolkit for Visual Studio desde un `.vsix` archivo y generar un archivo de registro de la instalación, siga estos pasos.

1. En la página de AWS Toolkit for Visual Studioinicio, siga el enlace de descarga y guarde el `.vsix` archivo de la AWS Toolkit for Visual Studio versión que desee instalar.
2. En el menú principal de Visual Studio, expanda el encabezado Herramientas, expanda el submenú de la línea de comandos y, a continuación, elija Símbolo del sistema para desarrolladores de Visual Studio.
3. En Símbolo del sistema para desarrolladores de Visual Studio, introduzca el comando `vsixinstaller` con el siguiente formato:

   ```
   vsixinstaller /logFile:[file path to log file] [file path to Toolkit installation file]
   ```
4. Sustituya `[file path to log file]` por el nombre y la ruta completa del archivo del directorio en el que desee crear el registro de instalación. Un ejemplo del comando `vsixinstaller` con la ruta y el nombre de archivo especificados tiene el siguiente aspecto:

   ```
   vsixinstaller /logFile:C:\Users\Documents\install-log.txt [file path to AWSToolkitPackage.vsix]
   ```
5. Sustituya `[file path to Toolkit installation file]` por la ruta completa del directorio en el se encuentra `AWSToolkitPackage.vsix`.

   Un ejemplo del comando `vsixinstaller` con la ruta completa del archivo de instalación del kit de herramientas debe tener el siguiente aspecto:

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

6. Compruebe que el nombre y las rutas del archivo son correctos y, a continuación, ejecute el comando `vsixinstaller`.

   Un ejemplo del comando `vsixinstaller` completo tiene este aspecto:

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

Instalación de diferentes extensiones de Visual Studio

Si ha obtenido un archivo de registro de instalación y sigue sin poder determinar por qué se produce un error en el proceso de instalación, compruebe si puede instalar otras extensiones de Visual Studio. La instalación de otras extensiones distintas de Visual Studio puede proporcionar información adicional sobre los problemas de instalación. En caso de que no puedas instalar ninguna extensión de Visual Studio, puede que tengas que solucionar los problemas con Visual Studio, en lugar de AWS Toolkit for Visual Studio hacerlo.

Cómo contactar con soporte de

Si ya ha revisado todas las secciones de esta guía y necesita más recursos o asistencia adicional, puede consultar casos de problemas anteriores o abrir un caso nuevo desde Problemas de Github y el AWS Toolkit for Visual Studio.

Para ayudar a agilizar la solución del problema, siga estos pasos:

- Compruebe los casos de problemas anteriores y los actuales para comprobar si alguien se ha topado antes con una situación similar.
- Tome notas detalladas de cada paso que haya tomado para solucionar el problema.
- Guarde todos los archivos de registro que haya obtenido al instalar la AWS Toolkit for Visual Studio u otras extensiones.
- Adjunta los archivos AWS Toolkit for Visual Studio de registro de instalación a la nueva edición.

Perfiles y encuadernación de ventanas

Perfiles y enlace de ventanas para Toolkit for Toolkit for Visual Studio

Cuando trabaje con las herramientas de publicación, los asistentes y otras funciones del Toolkit for Visual Studio, tenga en cuenta lo siguiente:

- La ventana delAWS explorador está enlazada a un solo perfil y región a la vez. Windows se abrió desde elAWS explorador de forma predeterminada para ese perfil y región enlazados.
- Después de abrir una nueva ventana, puede usar esa instancia delAWS Explorador para cambiar a un perfil o región diferente.
- Las herramientas y funciones de publicación del Toolkit for Visual Studio utilizan automáticamente de forma predeterminada el perfil y la región establecidos en elAWS Explorador.
- Si se especifica un nuevo perfil o región en una herramienta, asistente o función de publicación, todos los recursos que se creen posteriormente seguirán utilizando la nueva configuración de perfil y región.
- Si tiene varias instancias de Visual Studio abiertas, cada instancia se puede vincular a un perfil y una región diferentes.
- ElAWS Explorador guarda el último perfil y la última región que se especificaron y los valores de la última instancia de Visual Studio cerrada persistirán.

Autenticación y acceso

No necesita autenticarse para empezar AWS a trabajar con el AWS Toolkit for Visual Studio. Sin embargo, la mayoría de AWS los recursos se administran a través de una AWS cuenta. Para acceder a todos los servicios y funciones del AWS Toolkit for Visual Studio, necesitará al menos dos tipos de autenticación de cuentas:

1. Ya sea AWS Identity and Access Management (IAM) o AWS IAM Identity Centerautenticación para sus cuentas. AWS La mayoría de AWS los servicios y recursos se administran a través de IAM y del IAM Identity Center.
2. El AWS Builder ID es opcional para algunos otros servicios. AWS

Los siguientes temas contienen detalles adicionales e instrucciones de configuración para cada tipo de credencial y método de autenticación.

Temas

- AWS Las credenciales del IAM Identity Center están en AWS Toolkit for Visual Studio
- AWS Credenciales de IAM
- AWS ID de constructor
- Autenticación multifactor (MFA) en el Kit de herramientas para Visual Studio
- Configuración de credenciales externas

AWS Las credenciales del IAM Identity Center están en AWS Toolkit for Visual Studio

AWS IAM Identity Center es la mejor práctica recomendada para gestionar la autenticación de su AWS cuenta.

Para obtener instrucciones detalladas sobre cómo configurar el Centro de Identidad de IAM para los kits de desarrollo de software (SDK) y el AWS Toolkit for Visual Studio, consulte la sección de autenticación del Centro de Identidad de IAM de la Guía de referencia de los AWS SDK y las herramientas.

Autenticación con el Centro de Identidad de IAM desde el AWS Toolkit for Visual Studio

Para autenticarse en el Centro de Identidad de IAM desde el AWS Toolkit for Visual Studio añadiendo un perfil del Centro de Identidad de IAM a su `config` archivo `credentials` o archivo, siga estos pasos.

1. En el editor de texto que prefiera, abra la información de AWS credenciales almacenada en el archivo. `<hone-directory>\.aws\credentials`
2. En el `credentials file`, en la sección `[default]`, añada una plantilla para un perfil específico del IAM Identity Center. La siguiente es una plantilla de ejemplo:

> **Important**
>
> No utilice la palabra profile al crear una entrada en el archivo `credential` porque crearía un conflicto con las convenciones de nomenclatura del archivo `credential`. Incluya el prefijo `profile_` únicamente cuando configure un perfil con nombre en el archivo `config`.

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

- **`sso_start_url`**: la URL que apunta al portal de usuario del IAM Identity Center de su organización.
- **`sso_region`**: la AWS región que contiene el host del portal de IAM Identity Center. Puede ser diferente de la AWS región especificada más adelante en el `region` parámetro predeterminado.
- **`sso_account_id`**: el ID de AWS cuenta que contiene el rol de IAM con el permiso que desea conceder a este usuario del IAM Identity Center.
- **`sso_role_name`**: el nombre del rol de IAM que define los permisos que tiene el usuario cuando utiliza el perfil para obtener credenciales mediante el IAM Identity Center.

- **`region`**: la AWS región predeterminada en la que inicia sesión este usuario del Centro de identidades de IAM.

> **Note**
>
> También puede añadir un perfil habilitado para el Centro de Identidad de IAM AWS CLI ejecutando el `aws configure sso` comando. Tras ejecutar este comando, debe proporcionar valores para la URL de inicio del Centro de Identidad de IAM (`sso_start_url`) y la AWS Región (`region`) que aloja el directorio del Centro de Identidad de IAM.
> Para obtener más información, consulte Configuración de la AWS CLI para usar el inicio de sesión AWS único en la Guía del AWS Command Line Interface usuario.

Iniciar sesión con el IAM Identity Center

Al iniciar sesión con un perfil de IAM Identity Center, se inicia el navegador predeterminado con el `sso_start_url` especificado en su `credential file`. Debe verificar sus datos de inicio de sesión en el IAM Identity Center antes de poder acceder a sus AWS recursos. AWS Toolkit for Visual Studio Si sus credenciales caducan, tendrá que repetir el proceso de conexión para obtener nuevas credenciales temporales.

AWS Credenciales de IAM

AWS Las credenciales de IAM se autentican con su AWS cuenta mediante claves de acceso almacenadas localmente.

En las siguientes secciones se describe cómo configurar las credenciales de IAM para autenticarse con su AWS cuenta desde. AWS Toolkit for Visual Studio

> **Important**
>
> Antes de configurar las credenciales de IAM para autenticarse con su AWS cuenta, tenga en cuenta lo siguiente:
>
> - Si ya configuraste las credenciales de IAM a través de otro AWS servicio (como el AWS AWS CLI), las AWS Toolkit for Visual Studio detectará automáticamente.

- AWS recomienda usar la AWS IAM Identity Center autenticación. Para obtener información adicional sobre las prácticas recomendadas de AWS IAM, consulte la sección Prácticas recomendadas de seguridad en IAM de la Guía del usuario de AWS Identity and Access Management.
- Para evitar riesgos de seguridad, no utilice a los usuarios de IAM para la autenticación cuando desarrolle software especialmente diseñado o trabaje con datos reales. En su lugar, utilice la federación con un proveedor de identidades como. AWS IAM Identity Center Para obtener más información, consulte ¿Qué es el IAM Identity Center? en la Guía del usuario de AWS IAM Identity Center .

Creación de un usuario de IAM

Antes de configurar la AWS Toolkit for Visual Studio autenticación con tu AWS cuenta, debes completar el paso 1: Crea tu usuario de IAM y el paso 2: Introduce tus claves de acceso en el tema Autenticar con credenciales a largo plazo de la Guía de referencia de herramientas y AWS SDK.

> **Note**
>
> El paso 3: actualizar el archivo de credenciales compartidas es opcional.
> Si completas el paso 3, AWS Toolkit for Visual Studio detectará automáticamente tus credenciales en. `credentials file`
> Si no ha completado el paso 3, le guiará AWS Toolkit for Visual Studio por el proceso de creación de un archivo de credenciales, tal y `credentials file` como se describe en la sección Creación de un archivo de credenciales a partir de esa AWS Toolkit for Visual Studio sección, que se encuentra más abajo.

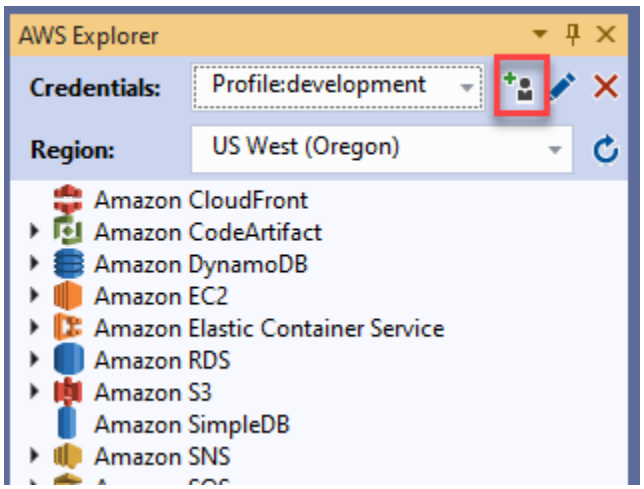
Creación de un archivo credentials

Para añadir un usuario o crear un `credentials file` desde el AWS Toolkit for Visual Studio:

> **Note**
>
> Cuando se agrega un nuevo perfil de usuario desde el kit de herramientas:
>
> - Si ya existe un `credentials file`, la información del nuevo usuario se añade al archivo existente.

- Si el `credentials file` no existe, se crea un archivo nuevo.

1. Desde el AWS explorador, seleccione el icono Nuevo perfil de cuenta para abrir el cuadro de diálogo Nuevo perfil de cuenta.



2. Rellene los campos obligatorios del cuadro de diálogo Nuevo perfil de cuenta y pulse el botón Aceptar para crear el usuario de IAM.

Edición de las credenciales de usuario de IAM desde el kit de herramientas

Para editar las credenciales de usuario de IAM desde el kit de herramientas, siga los siguientes pasos:

1. En el menú desplegable Credenciales del AWS explorador, elija la credencial de usuario de IAM que desee editar.
2. Elija el icono Editar perfil para abrir el cuadro de diálogo Editar perfil.
3. En el cuadro de diálogo Editar perfil, complete las actualizaciones y elija el botón Aceptar para guardar los cambios.

Para eliminar las credenciales de usuario de IAM desde el kit de herramientas, siga los siguientes pasos:

1. En el menú desplegable Credenciales del AWS explorador, elija la credencial de usuario de IAM que desee eliminar.
2. Seleccione el icono Eliminar perfil para abrir el mensaje Eliminar perfil.

3. Confirme que desea eliminar el perfil para eliminarlo de su `Credentials file`.

> **Important**
>
> No es posible editar desde AWS Toolkit for Visual Studio aquellos perfiles que admiten características de acceso avanzadas, como el IAM Identity Center o la autenticación multifactor (MFA) en el cuadro de diálogo Editar perfil. Para realizar cambios en estos tipos de perfiles, debe editar el `credentials file` con un editor de texto.

Edición de las credenciales de usuario de IAM desde el un editor de texto

Además de gestionar los usuarios de IAM con la AWS Toolkit for Visual Studio, puedes editarla `credential files` desde el editor de texto que prefieras. La ubicación predeterminada del `credential file` en Windows es `C:\Users\`*`USERNAME`*`\.aws\credentials`.

Para obtener más información sobre la ubicación y la estructura de los `credential files`, consulte la sección Archivos config y credentials compartidos de la Guía de referencia de herramientas y AWS SDK.

Crear usuarios de IAM desde () AWS Command Line InterfaceAWS CLI

Esta AWS CLI es otra herramienta que puede utilizar para crear un usuario de IAM en el`credentials file`, mediante el comando. `aws configure`

Para obtener información detallada sobre la creación de usuarios de IAM a partir de, AWS CLI consulte la sección Configuración de los AWS CLI temas de la Guía del AWS CLI usuario.

El Kit de herramientas para Visual Studio admite las siguientes propiedades de configuración:

```
aws_access_key_id
aws_secret_access_key
aws_session_token
credential_process
credential_source
external_id
mfa_serial
role_arn
role_session_name
source_profile
```

```
sso_account_id
sso_region
sso_role_name
sso_start_url
```

AWS ID de constructor

AWS El Builder ID es un método de AWS autenticación adicional que puede ser necesario para utilizar determinados servicios o funciones, como la clonación de un repositorio de terceros con Amazon CodeCatalyst.

Para obtener información detallada sobre el método de autenticación de AWS Builder ID, consulta el tema Iniciar sesión con AWS Builder ID en la Guía del usuario de AWS inicio de sesión.

Para obtener información adicional sobre cómo clonar un repositorio CodeCatalyst desde AWS Toolkit for Visual Studio, consulta el CodeCatalyst tema Trabajar con Amazon en esta Guía del usuario.

Autenticación multifactor (MFA) en el Kit de herramientas para Visual Studio

La autenticación multifactor (MFA) es una seguridad adicional para AWS sus cuentas. La MFA exige que los usuarios proporcionen credenciales de inicio de sesión y una autenticación única desde un mecanismo de AWS MFA compatible al acceder a sitios web o servicios. AWS

AWS admite una variedad de dispositivos virtuales y de hardware para la autenticación MFA. El siguiente es un ejemplo de un dispositivo de MFA virtual habilitado a través de una aplicación de smartphone. Para obtener más información sobre las opciones del dispositivo MFA, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Paso 1: creación de un rol de IAM para delegar el acceso a los usuarios de IAM

En el procedimiento siguiente, se describe cómo configurar la delegación de roles para asignar permisos a un usuario de IAM. Para obtener más información acerca de la delegación de roles de IAM, consulte el tema Creación de un rol para delegar permisos a un usuario de IAM en la Guía del usuario de AWS Identity and Access Management .

1. Vaya a la consola de IAM: https://console.aws.amazon.com/iam.
2. En la barra de navegación, seleccione Roles y, a continuación, seleccione Crear rol.
3. En la página Crear un rol, seleccione Otra cuenta de AWS .
4. Escriba el ID de cuenta requerido y marque la casilla de verificación Requerir MFA.

> **Note**
>
> Para encontrar el número de cuenta de 12 cifras (ID), vaya a la barra de navegación en la consola y seleccione Soporte y, a continuación, elija Centro de soporte.

5. Elija Siguiente: permisos.
6. Adjunte las políticas existentes al rol o cree una nueva política para él. Las políticas que elija en esta página determinan a qué AWS servicios puede acceder el usuario de IAM con el kit de herramientas.
7. Tras adjuntar las políticas, seleccione Siguiente: etiquetas para tener la opción de añadir etiquetas de IAM a su rol. Elija Siguiente: revisión para continuar.
8. En la página de revisión, introduzca un Nombre del rol obligatorio (toolkit-role, por ejemplo). También puede añadir una descripción opcional en Descripción del rol.
9. Elija Crear rol.
10. Cuando aparezca el mensaje de confirmación (por ejemplo, "Se ha creado el rol toolkit-role"), elija el nombre del rol en el mensaje.
11. En la página Resumen, seleccione el icono de copia para copiar el ARN del rol y pegarlo en un archivo. (Necesita este ARN al configurar el usuario de IAM para que asuma el rol).

Paso 2: creación de un usuario de IAM que asuma los permisos del rol

Este paso crea un usuario de IAM sin permisos para poder añadir una política en línea.

1. Vaya a la consola de IAM: https://console.aws.amazon.com/iam.
2. En la barra de navegación, elija Usuarios y, a continuación, elija Agregar usuario.
3. En la página Agregar usuario, indique el Nombre de usuario necesario (toolkit-user, por ejemplo) y marque la casilla de verificación Acceso mediante programación.
4. Seleccione Siguiente: permisos, Siguiente: etiquetas y Siguiente: revisar para avanzar por las páginas siguientes. En este momento no va a añadir permisos porque el usuario va a asumir los permisos del rol.

5. En la página Revisión, se le informa de que este usuario no tiene permisos. Seleccione la opción Crear un usuario.
6. En la página Correcto, elija Descargar .csv para descargar el archivo que contiene el ID de clave de acceso y la clave de acceso secreta. (Necesitará ambos al definir el perfil del usuario en el archivo credentials).
7. Elija Close.

Paso 3: añadir una política que permita al usuario de IAM asumir el rol

El siguiente procedimiento crea una política insertada que permite al usuario asumir el rol (y los permisos de dicho rol).

1. En la página Usuarios de la consola de IAM, elija el usuario de IAM que acaba de crear (toolkit-user, por ejemplo).
2. En la pestaña Permisos de la página Resumen, seleccione Añadir política insertada.
3. En la página Crear política, seleccione Elegir un servicio, escriba STS en Buscar un servicio y, a continuación, elija STS en los resultados.
4. En Acciones, comience a introducir el término. AssumeRole Marque la AssumeRolecasilla de verificación cuando aparezca.
5. En la sección Recurso, asegúrese de que esté seleccionada la opción Específico y haga clic en Agregar ARN para restringir el acceso.
6. En el cuadro de diálogo Agregar ARN, en Especificar ARN para el rol, agregue el ARN del rol que creó en el Paso 1.

   Tras añadir el ARN del rol, la cuenta de confianza y el nombre del rol asociados a ese rol aparecen en Cuenta y Nombre de rol con ruta.
7. Elija Agregar.
8. De vuelta a la página Crear política, elija Especificar las condiciones de la solicitud (opcional), marque la casilla de verificación MFA requerida y, a continuación, seleccione Cerrar para confirmar.
9. Elija Revisar la política
10. En la página Revisar la política, escriba un nombre para la política y después elija Crear política.

    La pestaña Permisos muestra la nueva política insertada adjuntada directamente al usuario de IAM.

Paso 4: administración de un dispositivo de MFA virtual para el usuario de IAM

1. Descargue e instale una aplicación de MFA virtual en su smartphone.

   Para obtener una lista de las aplicaciones compatibles, consulte la página de recursos sobre la autenticación multifactor.
2. En la consola de IAM, elija Usuarios en la barra de navegación y, a continuación, elija el usuario que asumirá el rol (en este ejemplo, toolkit-user).
3. En la página Resumen, elija la pestaña Credenciales de seguridad y, en Dispositivo de MFA asignado, elija Administrar.
4. En el panel Administrar dispositivo de MFA, elija Dispositivo de MFA virtual y, a continuación, elija Continuar.
5. En el panel Configurar dispositivo de MFA virtual, seleccione Mostrar código QR y escanee el código con la aplicación de MFA virtual que instaló en su smartphone.
6. Tras escanear el código QR, la aplicación de MFA virtual genera códigos MFA de un solo uso. Introduzca dos códigos de MFA consecutivos en Código de MFA 1 y Código de MFA 2.
7. Elija Asignar MFA.
8. De vuelta a la pestaña Credenciales de seguridad del usuario, copie el ARN del nuevo dispositivo de MFA asignado.

   El ARN incluye su ID de cuenta de 12 dígitos y el formato es similar al siguiente: `arn:aws:iam::123456789012:mfa/toolkit-user`. Necesitará este ARN al definir el perfil de MFA en el siguiente paso.

Paso 5: creación de perfiles para permitir el uso de MFA

El siguiente procedimiento crea los perfiles que permiten la MFA al acceder a AWS los servicios del Toolkit for Visual Studio.

Los perfiles que cree incluyen tres datos que ha copiado y almacenado durante los pasos anteriores:

- Las claves de acceso (ID de clave de acceso y clave de acceso secreta) del usuario de IAM
- El ARN del rol que delega los permisos al usuario de IAM
- El ARN del dispositivo de MFA virtual que está asignado al usuario de IAM

En el archivo de credenciales AWS compartido o en la tienda de SDK que contiene sus AWS credenciales, añada las siguientes entradas:

```
[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
```

En el ejemplo se definen dos perfiles:

- El perfil de `[toolkit-user]` incluye la clave de acceso y la clave de acceso secreta que se generaron y guardaron al crear el usuario de IAM en el Paso 2.
- El perfil de `[mfa]` define cómo se admite la autenticación multifactorial. Hay tres entradas:

  ◦ `source_profile`: especifica el perfil cuyas credenciales se utilizan para asumir el rol especificado por la configuración de `role_arn` en este perfil. En este caso, es perfil `toolkit-user`.

  ◦ `role_arn`: especifica el nombre de recurso de Amazon (ARN) del rol de IAM que desea utilizar para realizar las operaciones solicitadas mediante este perfil. En este caso, es el ARN del rol que creó en el Paso 1.

  ◦ `mfa_serial`: especifica la identificación o el número de serie del dispositivo de MFA que el usuario debe utilizar al asumir un rol. En este caso, es el ARN del dispositivo virtual que configuró en el Paso 3.

Configuración de credenciales externas

Si tiene un método para generar o buscar credenciales que no sea directamente compatible con la AWS, puede agregar al archivo credentials compartido un perfil que contenga la configuración de `credential_process`. Esta configuración especifica un comando externo que se ejecuta para generar o recuperar las credenciales de autenticación que se van a utilizar. Por ejemplo, puede incluir una entrada similar a la siguiente en el archivo `config`:

```
[profile developer]
```

```
credential_process = /opt/bin/awscreds-custom --username helen
```

Para obtener más información sobre el uso de credenciales externas y los riesgos de seguridad asociados, consulte Obtener credenciales mediante un proceso externo en la Guía del usuario de AWS Command Line Interface .

Trabajar con AWS servicios

En los temas siguientes se describe cómo empezar a trabajar con AWS los servicios del AWS Toolkit for Visual Studio.

Temas

Amazon CodeCatalyst para el AWS kit de herramientas de Visual Studio

¿Qué es Amazon CodeCatalyst?

Amazon CodeCatalyst es un espacio de colaboración basado en la nube para equipos de desarrollo de software. Con el AWS kit de herramientas para Visual Studio, puede ver y administrar

CodeCatalyst los recursos directamente desde el AWS kit de herramientas para Visual Studio. Para obtener más información al respectoCodeCatalyst, consulte la Guía del CodeCatalyst usuario de Amazon.

En los siguientes temas se describe cómo conectar el AWS kit de herramientas para Visual Studio CodeCatalyst y cómo trabajar con él a CodeCatalyst través del AWS kit de herramientas para Visual Studio.

Temas

- Introducción a Amazon CodeCatalyst y el AWS kit de herramientas para Visual Studio
- Trabajando con CodeCatalyst los recursos de Amazon del AWS kit de herramientas para Visual Studio
- Solución de problemas

Introducción a Amazon CodeCatalyst y el AWS kit de herramientas para Visual Studio

Para empezar a trabajar con Amazon CodeCatalyst desde el AWS kit de herramientas para Visual Studio, complete lo siguiente.

Temas

- Instalación del AWS kit de herramientas para Visual Studio
- Crear una CodeCatalyst cuenta y un ID de AWS constructor
- Conectar el AWS kit de herramientas para Visual Studio con CodeCatalyst

Instalación del AWS kit de herramientas para Visual Studio

Antes de integrar el AWS kit de herramientas para Visual Studio con sus CodeCatalyst cuentas, asegúrese de utilizar una versión actual de AWS Toolkit for Visual Studio. Para obtener más información sobre cómo instalar y configurar la versión más reciente de AWS Toolkit for Visual Studio, consulte la sección Configuración del AWS kit de herramientas para Visual Studio de esta Guía del usuario.

Crear una CodeCatalyst cuenta y un ID de AWS constructor

Además de instalar la versión más reciente del AWS kit de herramientas para Visual Studio, debe tener un ID y una CodeCatalyst cuenta de AWS Builder activos para conectarse con AWS Toolkit

for Visual Studio. Si no tienes un ID o una CodeCatalyst cuenta de AWS Builder activos, consulta la CodeCatalyst sección Configuración con de la Guía del CodeCatalystusuario.

> **Note**
>
> Un ID de AWS constructor es diferente de tus AWS credenciales. Para obtener instrucciones sobre cómo registrarse y autenticarse con un ID de AWS Builder, consulte el tema Autenticación y acceso: AWS Builder ID de esta Guía del usuario.
> Para obtener información detallada sobre los ID de AWS Builder, consulte el tema AWSBuilder ID de la Guía del usuario de referencia AWS general.

Conectar el AWS kit de herramientas para Visual Studio con CodeCatalyst

Para conectar AWS Toolkit for Visual Studio con su CodeCatalyst cuenta, siga estos pasos.

1. En el elemento del menú Git de Visual Studio, elija Clone Repository... .
2. En la sección Buscar un repositorio, selecciona Amazon CodeCatalyst como proveedor.
3. En la sección Conexión, elija Conectar con AWS Builder ID para abrir la CodeCatalyst consola en su navegador web preferido.
4. Desde tu navegador, introduce tu ID de AWS Builder en el campo proporcionado y sigue las instrucciones para continuar.
5. Cuando se le solicite, seleccione Permitir para confirmar la conexión entre AWS Toolkit for Visual Studio y su CodeCatalyst cuenta. Cuando finalice el proceso de conexión, CodeCatalyst aparecerá una confirmación que indica que es seguro cerrar el navegador.

Trabajando con CodeCatalyst los recursos de Amazon del AWS kit de herramientas para Visual Studio

Las siguientes secciones proporcionan una descripción general de las funciones de administración de CodeCatalyst recursos de Amazon Amazon que están disponibles para el AWS kit de herramientas para Visual Studio.

Temas

- Clonar un repositorio

Clonar un repositorio

CodeCatalystes un servicio basado en la nube que requiere que esté conectado a la nube para trabajar en CodeCatalyst proyectos. Para trabajar en un proyecto de forma local, puedes clonar CodeCatalyst repositorios en tu máquina local y sincronizarlos con tu CodeCatalyst proyecto la próxima vez que te conectes a la nube.

Para clonar un repositorio en su máquina local, siga estos pasos.

1. En el elemento del menú Git de Visual Studio, elija Clone Repository... .
2. En la sección Buscar un repositorio, selecciona Amazon CodeCatalyst como proveedor.

> **Note**
>
> Si la sección Conexión muestra un `Not Connected` mensaje, complete los pasos de la sección Autenticación y acceso: AWS Builder ID de esta guía del usuario antes de continuar.

3. Elige el espacio y el proyecto desde los que quieres clonar un repositorio.
4. En la sección Repositorios, selecciona el repositorio que deseas clonar.
5. En la sección Ruta, elige la carpeta en la que quieres clonar tu repositorio.

> **Note**
>
> Esta carpeta debe estar vacía inicialmente para que la clonación se realice correctamente.

6. Seleccione Clonar para empezar a clonar el repositorio.
7. Una vez clonado el repositorio, Visual Studio cargará la solución clonada

> **Note**
>
> Si Visual Studio no abre la solución en el repositorio clonado, las opciones de Visual Studio se pueden ajustar desde la configuración Cargar automáticamente la solución al abrir un repositorio de Git, que se encuentra en la Configuración global de Git, del menú Control de código fuente.

Solución de problemas

Los siguientes son temas de solución de problemas para solucionar problemas conocidos al trabajar con Amazon CodeCatalyst desde el AWS kit de herramientas para Visual Studio.

Temas

Credentials

Si aparece un cuadro de diálogo en el que se solicitan credenciales al intentar clonar un repositorio basado en git desdeCodeCatalyst, es posible que su asistente de AWS CodeCommit credenciales esté configurado globalmente y cause interferencias con. CodeCatalyst Para obtener información adicional sobre el asistente de AWS CodeCommit credenciales, consulte los pasos de configuración de las conexiones HTTPS a los AWS CodeCommit repositorios de Windows con la sección auxiliar de credenciales de la AWS CLI de la Guía del usuario. AWSCodeCommit

Para limitar el AWSCodeCommitasistente de credenciales a gestionar únicamente CodeCommit las URL, siga estos pasos.

1. abre el archivo de configuración global de git en: `%userprofile%\.gitconfig`
2. Busque la siguiente sección en su archivo:

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

3. Cambie esa sección por la siguiente:

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

4. Guarda los cambios y, a continuación, completa los pasos para clonar tu repositorio.

Amazon CloudWatch Integración de registros para Visual Studio

Amazon CloudWatch Integración de registros desdeAWSEl Toolkit for Visual Studio le brinda la capacidad de monitorear, almacenar y acceder CloudWatch Registra los recursos sin tener que salir del IDE. Para obtener más información CloudWatch servicio y cómo trabajar con CloudWatch Funciones de registro, elija entre los siguientes temas.

Temas

Configuración de CloudWatch Integración de registros para Visual Studio

Antes de poder usar Amazon CloudWatch Integración de registros con Toolkit for Visual Studio, necesita unAWSaccount. Puede crear un nuevoAWSCuenta de laAWSinicie sesiónsitio:. La mayoría de CloudWatch Se puede acceder a las funciones de registro que están disponibles en el Toolkit for Visual Studio conAWSCredenciales de . Si una función en particular requiere una configuración adicional, los requisitos se incluyen en las secciones correspondientes de laUso de CloudWatch Registrosguide.

Para obtener información adicional y opciones sobre la configuración CloudWatch Registros, consulte laConfiguración inicialsección de Amazon CloudWatch Guía de registros.

Uso de CloudWatch logs de Visual Studio

Amazon CloudWatch La integración de logs le permite monitorizar, almacenar y obtener acceso CloudWatch Registros desde lasAWSToolkit for Visual Studio. Tener acceso a CloudWatch Las funciones de registro, sin necesidad de salir de su IDE, mejoran la eficiencia al simplificar la CloudWatch Registra el proceso de desarrollo y reduce las interrupciones en el flujo de trabajo. En los temas siguientes se describe cómo trabajar con las características y funciones básicas del CloudWatch Integración de registros

Temas

CloudWatch Grupos de registros

UNA`log group`es un grupo de`log streams`que comparten la misma configuración de retención, monitorización y control de acceso. No hay límites en el número de flujos de registros que pueden pertenecer a un grupo de registros.

Consulta de grupos

La`View Log Groups`muestra una lista de logs de los grupos de logs en CloudWatchExplorador de logs.

Para acceder a la función Ver grupos de registros y abrir el CloudWatch Explorador de logs Grupos de logs, lleve a cabo los siguientes pasos.

1. Desde lasAWSExplorer, expandaAmazon CloudWatch.
2. Doble clicGrupos de registroso abra el menú contextual (haga clic con el botón derecho) y seleccioneVista, para abrirCloudWatch Explorador de logs.

> **Note**
>
> La CloudWatch El Explorador de grupos de registro se abrirá en la misma ubicación de ventana que el Explorador de soluciones.

Filtrado de logs

Su cuenta individual puede contener miles de grupos de registro diferentes. Para simplificar la búsqueda de grupos específicos, utilice la`filtering`característica que se describe a continuación.

1. Desde lasCloudWatch Explorador de logs, coloque el cursor en la barra de búsqueda situada en la parte superior de la ventana.
2. Empieza a escribir un prefijo relacionado con los grupos de registros que estás buscando.
3. CloudWatch Explorador de logsse actualiza automáticamente para mostrar los resultados que coinciden con los términos de búsqueda que especificó en el paso anterior.

Eliminación de grupos

Para eliminar un grupo de logs específico, consulte el procedimiento siguiente.

1. Desde lasCloudWatch Explorador de logs, haga clic con el botón derecho en el Grupo de logs que desea eliminar.
2. Cuando se le pida, confirme que desea eliminar el Grupo de logs actualmente seleccionado.
3. Elegir elSíelimina el grupo de registros seleccionado y, a continuación, actualiza elCloudWatch Explorador de logs.

Refresh

Para actualizar la lista actual de grupos de registros que se muestra en laCloudWatch Explorador de logs, elige laIcono de actualizaciónsituado en eldesde las.

Copiar ARN de grupo de registros

Para copiar el ARN de un grupo de registros específico, siga los pasos que se describen a continuación.

1. Desde lasCloudWatch Explorador de logs, haga clic con el botón derecho en el grupo de registros del que desea copiar un ARN.
2. Elija el iconoCopiar ARNopción del menú.
3. El ARN ahora se copia en el portapapeles local y está listo para pegarse.

CloudWatch Flujos de registro

Un flujo de registro es una secuencia de eventos de registro que comparten la misma fuente.

> **Note**
>
> Al ver transmisiones de logs, tenga en cuenta las propiedades siguientes:
>
> - De forma predeterminada, los flujos de registro se ordenan por la marca de tiempo del evento más reciente.
> - Las columnas asociadas a un flujo de registro se pueden ordenar en orden ascendente o descendente, activando la opciónintercalarubicado en los encabezados de las columnas.
> - Las entradas filtradas solo se pueden ordenar porLog Stream Name (Nombre del flujo de registro):.

Visualización de transmisiones de logs

1. Desde lasCloudWatch Explorador de logshaga doble clic en un Grupo de logs o haga clic en un grupo de logs y seleccioneVer Flujo de registrodesde el menú de contexto.
2. Se abrirá una nueva pestaña en eldocumento, que contiene una lista de flujos de registro asociados al grupo de registros.

Filtrado de logs de

1. Desde lasFlujos de registro, en la pestañadocumentoventana, coloque el cursor en la barra de búsqueda.
2. Empieza a escribir un prefijo relacionado con la secuencia de registro que estás buscando.
3. A medida que escribe, la pantalla actual se actualiza automáticamente para filtrar los Log Streams por su entrada.

Flujos de logs de

Para actualizar la lista actual de secuencias de registro que se muestra en ladocumento, elija lasIcono de actualización, que se encuentra en ladesde lasdesde lasbarra de búsqueda.

ARN de logs de copia

Para copiar el ARN de una secuencia de registro específica, siga los pasos que se describen a continuación.

1. Desde lasFlujos de registro, en la pestañadocumentohaga clic con el botón derecho en la transmisión de logs desde la que desea copiar un ARN.
2. Elija el iconoCopiar ARNopción del menú.
3. El ARN ahora se copia en el portapapeles local y está listo para pegarse.

Flujos de logs

LaFlujo de registrodescarga y almacena el flujo de registro seleccionado localmente, donde se puede acceder a él mediante herramientas y software personalizados para un procesamiento adicional.

1. Desde lasFlujos de registro, en la pestañadocumentohaga clic con el botón derecho en la transmisión de logs que desea descargar.

2. ElegirFlujo de registrodesde lasExportación a un archivo de textodiálogo.
3. Elija la ubicación en la que desea almacenar el archivo localmente y especifique un nombre en el campo de texto proporcionado.
4. Confirme la descarga seleccionandoDE ACUERDO. El estado de la descarga se muestra en laCentro de estado de tareas de Visual Studio

CloudWatch Eventos de registro

Los eventos de logs son registros de actividades guardados por la aplicación o el recurso que monitoriza CloudWatch.

Acciones de registro

Los eventos de registro se muestran en forma de tabla. De forma predeterminada, los eventos se ordenan del más antiguo al más reciente.

Las siguientes acciones están asociadas con los eventos de registro en Visual Studio:

- Modo texto envuelto: Puede alternar el texto envuelto haciendo clic en un evento.
- Botón de ajuste de texto: ubicado en la`document window` **`toolbar`**, este botón activa y desactiva el ajuste de texto para todas las entradas.
- Copiar mensajes en el portapapeles: selecciona los mensajes que quieres copiar, haz clic con el botón derecho en la selección y eligeCopia(Método abreviado`Ctrl + C`).

Consulta de eventos

1. Desde lasdocumento, seleccione una pestaña que contenga una lista de flujos de registro.
2. Haga doble clic en una secuencia de registro o haga clic con el botón derecho en una transmisiónVer Flujo de registrodesde las
3. Desde hastaEventos de registrose abrirá en la pestañadocumento, que contiene una tabla de eventos de registro asociados con la transmisión de registro elegida.

Filtro de logs de eventos

Hay tres formas de filtrar los eventos de registro: por contenido, rango de tiempo o ambos. Para filtrar los eventos de registro por contenido e intervalo de tiempo, empieza por filtrar los mensajes por contenido o intervalo de tiempo y, a continuación, filtra los resultados por el otro método.

Para filtrar los eventos del registro por contenido:

1. Desde lasEventos de registro, en la pestañadocumento, coloque el cursor en la barra de búsqueda situada en la parte superior de la ventana.
2. Empieza a escribir un término o frase relacionados con los eventos de registro que estás buscando.
3. A medida que escribe, la pantalla actual comienza a filtrar automáticamente los eventos de registro.

> **Note**
>
> Los patrones de filtro distinguen mayúsculas y minúsculas. Puede mejorar los resultados de búsqueda si incluye términos y frases exactos con caracteres no alfanuméricos entre comillas dobles (*""*). Para obtener información detallada acerca de los patrones de filtros, consulte laSintaxis de patrones y filtrostema en la Amazonía CloudWatch guía.

Para ver los eventos de registro generados durante un intervalo de tiempo específico:

1. Desde lasEventos de registro, en la pestañadocumento, elija lasIcono de calendario, que se encuentra en ladesde las.
2. Utilizando los campos proporcionados, especifique el rango de tiempo en el que desea buscar.
3. Los resultados filtrados se actualizan automáticamente a medida que se especifican las restricciones de fecha y hora.

> **Note**
>
> LaClearborra todos los datos actuales date-and-time selecciones de filtro.

Eventos de logs de actualización

Para actualizar la lista actual de eventos de registro que se muestra en laEventos de registro, elija lasIcono de actualización, que se encuentra en ladesde las.

Acceso adicional a CloudWatchRegistros

Puede acceder CloudWatch logs asociados a otrosAWSservicios y recursos directamente desde elAWSKit de herramientas en Visual Studio.

Lambda

Para ver los flujos de registro que están asociados a una función de Lambda:

> **Note**
>
> Su función de ejecución de Lambda debe tener los permisos adecuados para enviar registros de logs a CloudWatchRegistros. Para obtener más información acerca de los permisos de Lambda que se necesitan CloudWatch Registros, consulte lahttps://docs.aws.amazon.com/lambda/latest/dg/monitoring-cloudwatchlogs.html#monitoring-cloudwatchlogs-prereqs

1. Desde lasAWSToolkit Explorer, amplíeLambda:.
2. haga clic con el botón derecho en la función que desea ver y, aVer registrospara abrir los flujos de registro asociados en eldocumentoventana.

Para ver los flujos de registro mediante la integración de Lambda`function view`:

1. Desde lasAWSToolkit Explorer, amplíeLambda:.
2. haga clic con el botón derecho en la función que desea ver y, aFunción Verpara abrir la vista de funciones en ladocumentoventana.
3. Desde las`function view`, en lasRegistros, se muestran las secuencias de registro asociadas a la función Lambda elegida.

ECS

Para ver los recursos de registro que están asociados con un contenedor de tareas de ECS, complete el siguiente procedimiento.

> **Note**
>
> Para que el servicio Amazon ECS envíe registros a CloudWatch, cada contenedor de una tarea de Amazon ECS determinada debe cumplir con la configuración requerida. Para

obtener información adicional sobre la configuración y configuración necesarias, consulte la guíaUso deAWSControlador de registros.

1. Desde lasAWSToolkit Explorer, amplíeAmazon ECS.
2. Elija el clúster de Amazon ECS que desea ver para abrir un nuevoClúster de ECS, en la pestañadocumentoventana.
3. Desde el menú de navegación, situado en el lado izquierdo de laClúster de ECS, elijaTareaspara obtener una lista de todas las tareas asociadas al clúster.
4. Desde lasTareas, seleccione una tarea y elija laVer registros, ubicado en la esquina inferior izquierda.

   > **Note**
   >
   > Esta pantalla muestra una lista de todas las tareas contenidas en el clúster, la`View Logs`el enlace solo está visible para cada tarea que cumpla con la configuración de registros requerida.
   >
   > - Si una tarea solo está asociada a un único contenedor, elVer registrosabre el flujo de registro de ese contenedor.
   > - Si una tarea está asociada a varios contenedores, elVer registrosabre el enlaceVista CloudWatch Registros para la tarea ECS, utilice laContenedor:para elegir el contenedor para el que quieres ver los registros y, a continuación, seleccionaDE ACUERDO.

5. Se abrirá una nueva pestaña en eldocumentoque muestra los flujos de registro asociados a la selección de contenedores.

Administración de instancias Amazon EC2

AWSExplorador ofrece vistas detalladas de Imágenes de máquina de Amazon (AMI) y las instancias de Amazon Elastic Compute Cloud (Amazon EC2). A partir de estas vistas, puede lanzar una instancia de Amazon EC2 desde una AMI, conectarse a dicha instancia y detener o finalizar la instancia, todo ello desde dentro del entorno de desarrollo de Visual Studio. Puede utilizar la vista de instancias para crear las AMI desde sus instancias. Para obtener más información, consulte Cree una AMI a partir de una instancia de Amazon EC2.

Vistas de imágenes de máquina de Amazon e instancias de Amazon EC2

DesdeAWSExplorador, puede mostrar vistas de Imágenes de máquina de Amazon (AMI) y las instancias de Amazon EC2. EnAWSExplorer, expanda elAmazon EC2Nodo.

Para visualizar la vista de AMI, en el primer subnodo, AMIs, abra el menú contextual (con el botón derecho) y, a continuación, elija View (Vista).

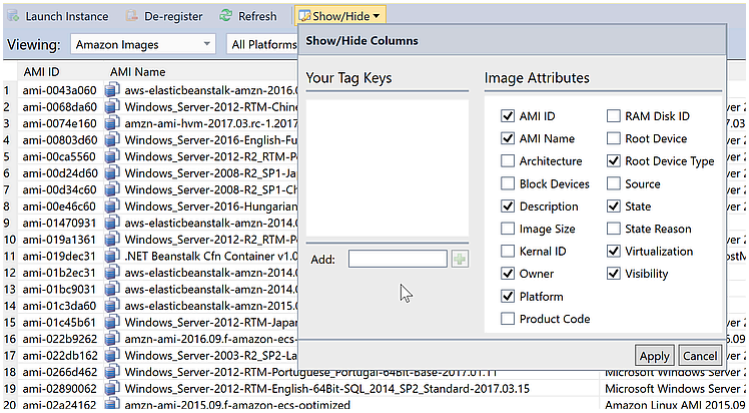
Para visualizar la vista de instancias de Amazon EC2, en el nodo Instances (Instancias), abra el menú contextual (con el botón derecho) y, a continuación, elija View (Vista).

Para visualizar cualquiera de las dos vistas, haga doble clic en el nodo adecuado.

- Las vistas se asignan al ámbito de la región especificada enAWSExplorador (por ejemplo, la región EE.UU. Oeste (Norte de California).
- Para reorganizar la columnas, haga clic en ellas y arrástrelas. Para ordenar los valores en una columna, haga clic en el encabezado de la misma.
- Puede utilizar las listas desplegables y el cuadro de filtro en Viewing (Visualización) para configurar las vistas. La vista inicial muestra las AMI de cualquier tipo de plataforma (Windows o Linux) que son propiedad de la cuenta especificada enAWSExplorador.

Mostrar/ocultar columnas

También puede elegir el menú desplegable Show/Hide (Mostrar/Ocultar) en la parte superior de la vista para configurar las columnas que se muestran. Su elección de columnas persistirá si cierra la vista y vuelve a abrirla.



IU Show/Hide Columns (Mostrar/Ocultar columnas) para vistas de AMI e instancias

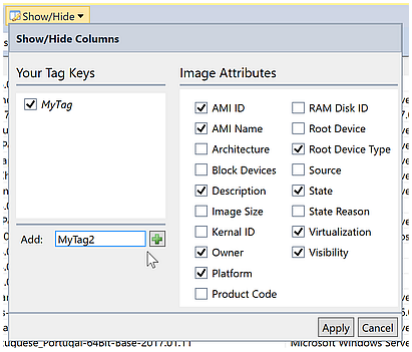
Etiquetado de AMI, instancias y volúmenes

También puede utilizar laMostrar/ocultarLista desplegable para añadir etiquetas para AMI, instancias de Amazon EC2 o volúmenes de su propiedad. Las etiquetas son pares nombre-valor que le permiten adjuntar metadatos a sus AMI, instancias y volúmenes. Los nombres de etiquetas están asignados a su cuenta y también de forma independiente a las AMI y las instancias. Por ejemplo, no habría conflicto si utiliza el mismo nombre de etiqueta para sus AMI y sus instancias. Los nombres de las etiquetas no distinguen entre mayúsculas y minúsculas.

Para obtener más información acerca de las etiquetas de, consulteUso de etiquetasen laGuía del usuario de Amazon EC2 para instancias de Linux.

Para agregar una etiqueta

1. En el cuadro Add (Añadir), escriba un nombre para la etiqueta. Elija el botón verde con el signo más (+) y, a continuación, elija Apply (Aplicar).



   Añada una etiqueta a una AMI o instancia de Amazon EC2

   La etiqueta nueva se muestra en cursiva, lo cual indica que aún no se han asociado valores a dicha etiqueta.

   En la vista de lista, el nombre de la etiqueta aparece como una columna nueva. Cuando se ha asociado al menos un valor con la etiqueta, la etiqueta será visible en laAWS Management Console.

2. Para añadir un valor para la etiqueta, haga doble clic en una celda en la columna de dicha etiqueta y escriba un valor. Para eliminar el valor de la etiqueta, haga doble clic en la celda y elimine el texto.

   Si desactiva la etiqueta en la lista desplegable Show/Hide (Mostrar/Ocultar), la columna correspondiente desaparece de la vista. La etiqueta se conserva, junto con cualquier valor de la etiqueta asociado con AMI, instancias o volúmenes.

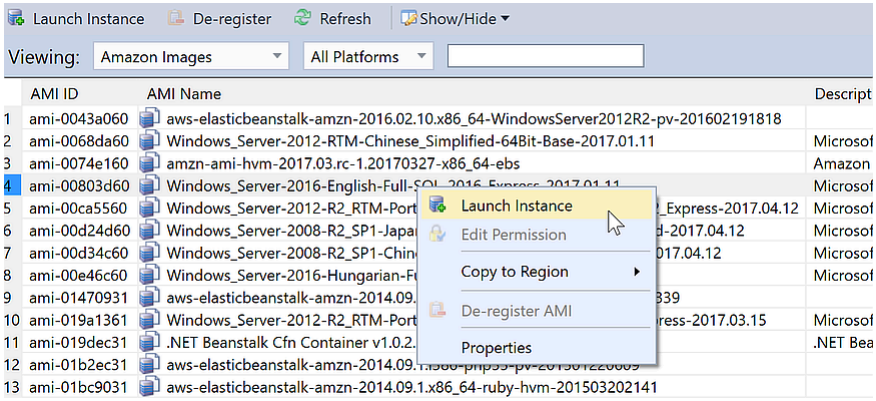
> **Note**
>
> Si borra una etiqueta en elMostrar/ocultarlista desplegable que no tiene valores asociados, elAWSToolkit eliminará la etiqueta por completo. Ya no aparecerán en la vista de lista o en la lista desplegable Show/Hide (Mostrar/Ocultar). Para utilizar dicha etiqueta de nuevo, utilice el cuadro de diálogo Show/Hide (Mostrar/Ocultar) para volver a crearla.

Lanzamiento de una instancia de Amazon EC2

AWSExplorer ofrece toda la funcionalidad necesaria para lanzar una instancia de Amazon EC2. En esta sección, seleccionaremos una Imagen de máquina de Amazon (AMI), la configuraremos y, a continuación, la iniciaremos como una instancia de Amazon EC2.

Para lanzar una instancia de Amazon EC2 de Windows Server

1. En la parte superior de la vista de la AMI, en la lista desplegable de la izquierda, seleccione Amazon Images (Imágenes de Amazon). En la lista desplegable de la derecha, seleccione Windows. En el cuadro de filtro, escriba `ebs` para Elastic Block Storage. La vista podría tardar unos minutos en actualizarse.
2. Elija una AMI en la lista, abra el menú contextual (con el botón derecho) y, a continuación elija Launch Instance (Lanzar instancia).



Lista de AMI

3. En el cuadro de diálogo Launch New Amazon EC2 Instance (Lanzar instancia de Amazon EC2 nueva), configure la AMI para su aplicación.

Tipo de instancia

Elija el tipo de instancia EC2 que se va a lanzar. Puede encontrar una lista de tipos de instancias e información sobre precios en la página Precios de Amazon EC2.

Nombre

Escriba un nombre para la instancia. Este nombre no puede tener más de 256 caracteres.

Par de claves

El par de claves se utiliza para obtener la contraseña de Windows que utiliza para iniciar sesión en la instancia EC2 mediante el Protocolo de escritorio remoto (RDP). Elija un par de claves para los que tendrá acceso a la clave privada o elija la opción para crear un par de claves. Si crea el par de claves en el Toolkit, el Toolkit puede almacenar la clave privada automáticamente.

Los pares de claves almacenados en el Toolkit están cifrados. Puede encontrarlos en`%LOCALAPPDATA%\AWSToolkit\keypairs`(típicamente: `C:\Users\<user>\AppData\Local\AWSToolkit\keypairs`). Puede exportar el key pair cifrado a un`.pem`file.

a. En Visual Studio, seleccioneVistay haga clic enAWSExplorador.
b. Haga clic en Amazon EC2 y seleccione Key Pairs (Pares de clave).
c. Se mostrarán los pares de claves y los creados/administrados por el Toolkit marcados como Stored in AWSToolkit.
d. Haga clic con el botón derecho en el par de claves que ha creado y seleccione Export Private Key (Exportar clave privada). La clave privada no estará cifrada y se almacenará en la ubicación especificada.

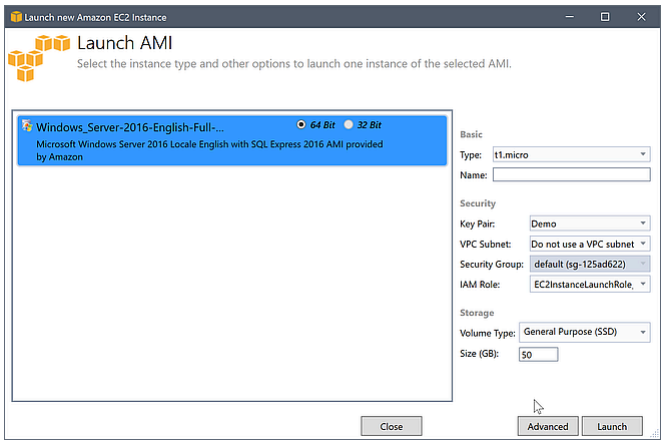
Security Group

El grupo de seguridad controla el tipo de tráfico de red que aceptará la instancia EC2. Elija un grupo de seguridad que permitirá tráfico entrante en el puerto 3389, el puerto utilizado por RDP, para que pueda conectarse a la instancia EC2. Para obtener información sobre cómo utilizar el Toolkit para crear grupos de seguridad, consulteAdministración de grupos de seguridad desdeAWSExplorador.

Perfil de instancia

El perfil de instancia es un contenedor lógico para un rol de IAM. Cuando elija un perfil de instancia, asocia el rol de IAM correspondiente a la instancia EC2. Los roles de IAM se configuran con políticas que especifican el acceso a Amazon Web Services y recursos de

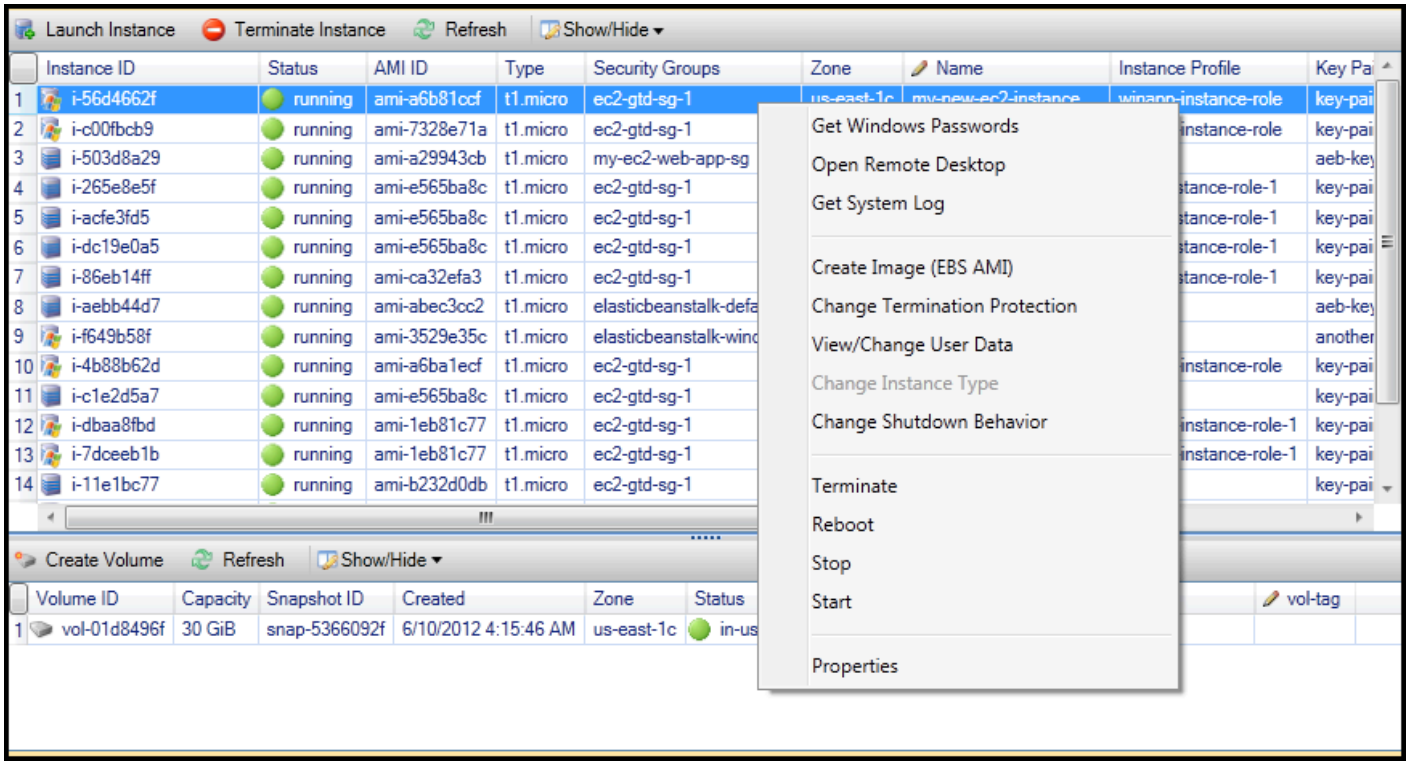
la cuenta. Cuando una instancia EC2 está asociada con un rol de IAM, el software de la aplicación que se ejecuta en la instancia se ejecuta con los permisos especificados por el rol de IAM. Esto permite que el software de la aplicación se ejecute sin tener que especificar ningúnAWSCredenciales propias, lo que hace que sea más seguro. Para obtener más información sobre roles de IAM, vaya a la Guía del usuario de IAM.



Cuadro de diálogo Launch AMI (Lanzar AMI) de EC2

4. Elija Launch.

EnAWSExplorer, en elInstanciassubnodo deAmazon EC2, abra el menú contextual (con el botón derecho del ratón) y luego seleccioneVista. LaAWSToolkit muestra la lista de instancias de Amazon EC2 asociada con la cuenta activa. Es posible que tenga que elegir Refresh (Actualizar) para ver su instancia nueva. Cuando la instancia aparece por primera vez, puede estar en estado pendiente, pero transcurridos unos minutos, hace la transición a estado de ejecución.



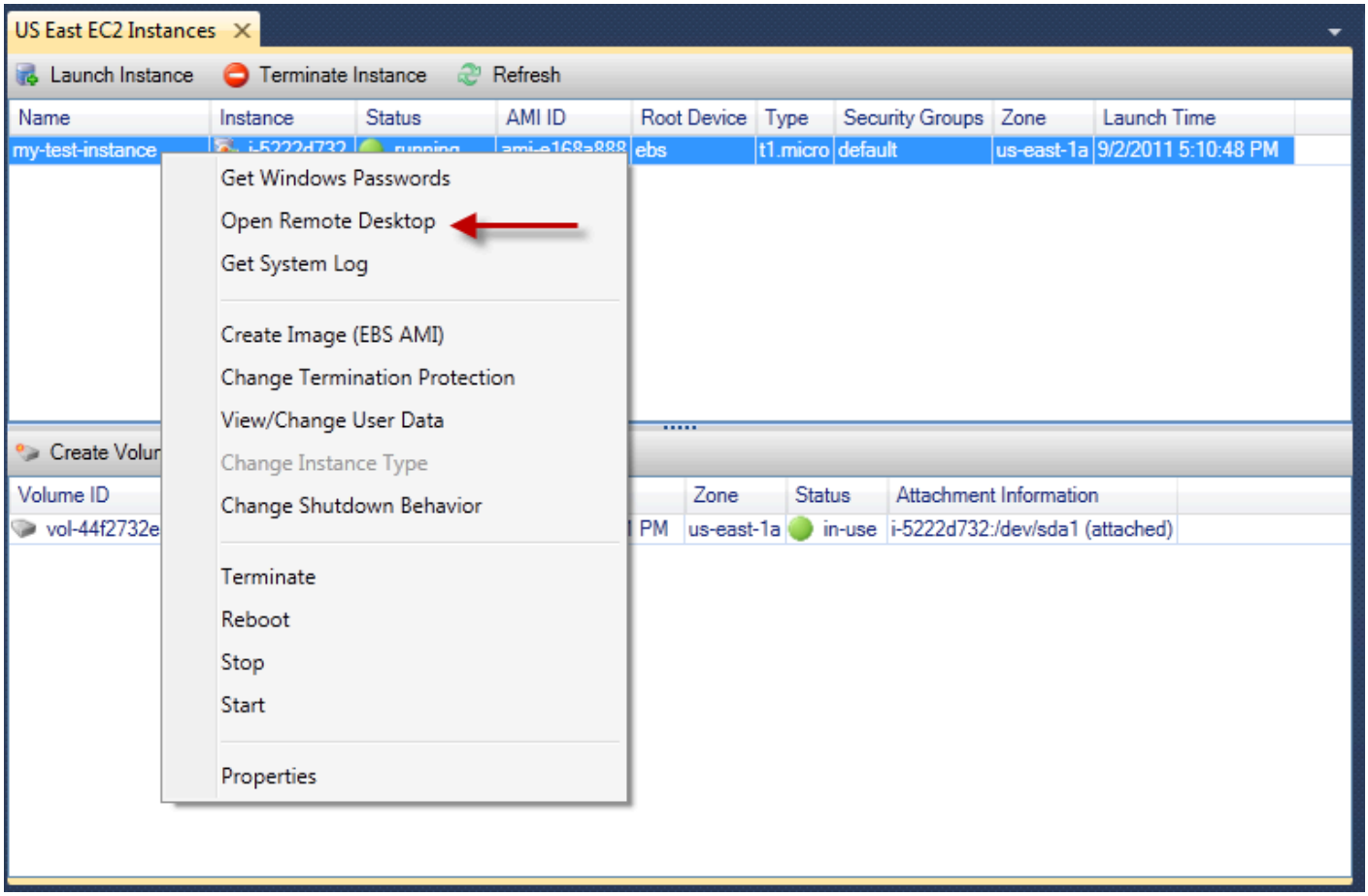
Conexión a una instancia de Amazon EC2

Puede utilizar el escritorio remoto de Windows para conectarse a una instancia de Windows Server. Para la autenticación, elAWSEl Toolkit le permite recuperar la contraseña de administrador de la instancia o simplemente puede utilizar el key pair almacenado asociado a la instancia. En el siguiente procedimiento, vamos a utilizar el par de claves almacenado.

Para conectar a una instancia de Windows Server con el escritorio remoto de Windows

1. En la lista de instancias EC2, haga clic con el botón derecho en la instancia de Windows Server a la que desea conectarse. Desde el menú contextual, elija Open Remote Desktop (Abrir escritorio remoto).

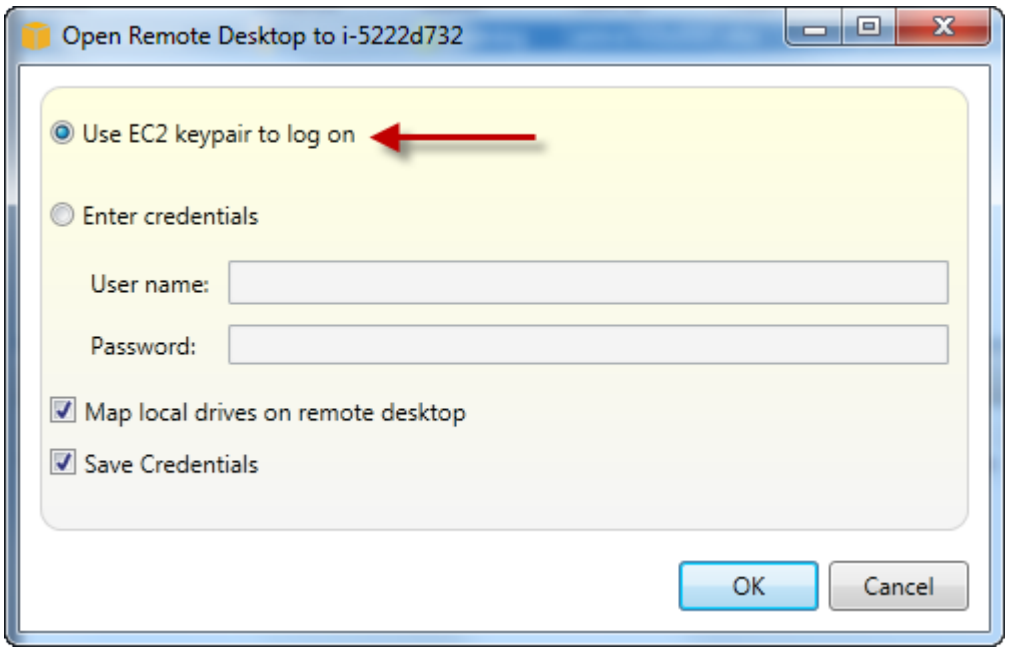
   Si desea autenticar mediante la contraseña de administrador, debería elegir Get Windows Password (Obtener contraseña de Windows).



Menú contextual de instancias EC2

2. En el cuadro de diálogo Open Remote Desktop (Abrir escritorio remoto), elija Use EC2 keypair to log on (Usar par de claves de EC2 para iniciar sesión) y, a continuación, elija OK (Aceptar).

   Si no almacenó un key pair con laAWSToolkit, especifique el archivo PEM que contiene la clave privada.

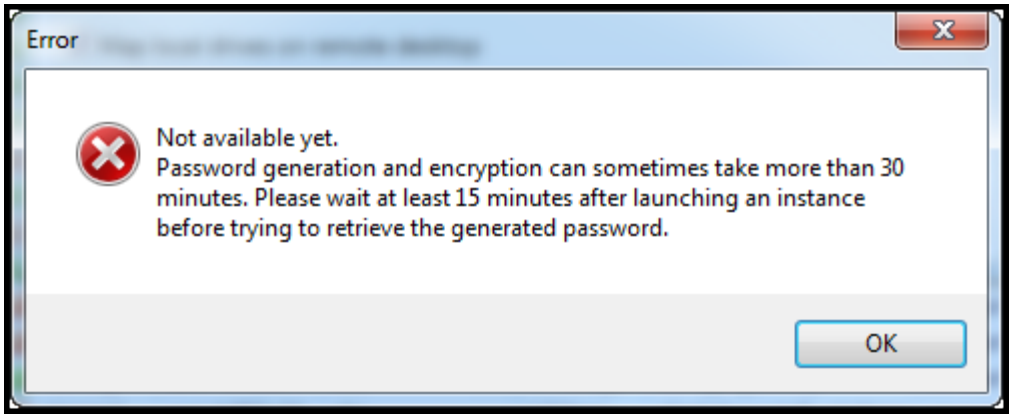


Cuadro de diálogo Open Remote Desktop (Abrir Escritorio remoto)

3. Se abrirá la ventana Remote Desktop (Escritorio remoto). No tiene que iniciar sesión porque la autenticación se produjo con el par de claves. Funcionará como administrador en la instancia Amazon EC2.

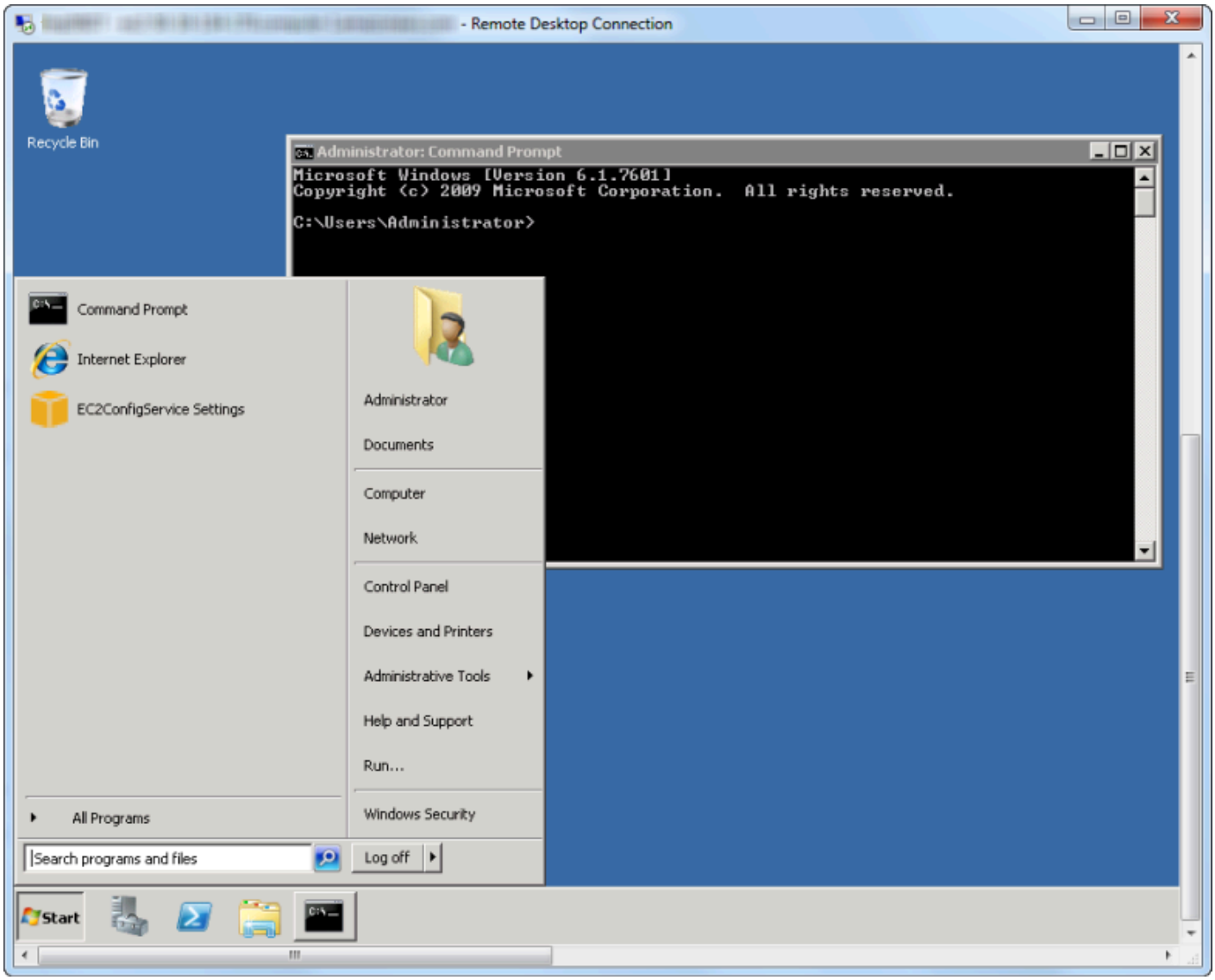
   Si la instancia EC2 se ha iniciado recientemente, es posible que no pueda conectarse por dos motivos posibles:

   - Es posible que el servicio de escritorio remoto todavía no esté funcionando. Espere unos minutos e inténtelo de nuevo.
   - Es posible que la información de la contraseña todavía no se haya transferido a la instancia. En este caso, verá un cuadro de mensajes parecido al siguiente.



Contraseña aún no disponible

La siguiente captura de pantalla muestra un usuario conectado como administrador a través del escritorio remoto.



Escritorio remoto

Finalización de una instancia de Amazon EC2

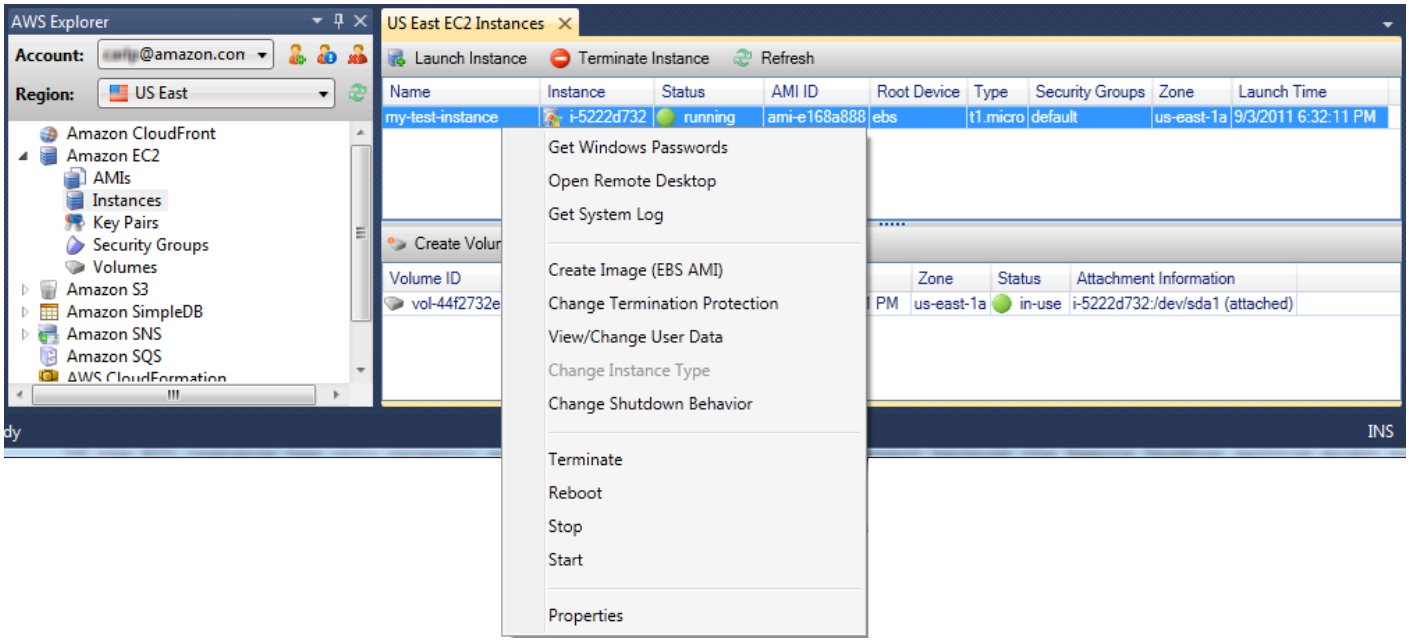
Uso deAWSToolkit, puede detener o finalizar una instancia de Amazon EC2 en ejecución de Visual Studio. Para detener la instancia, la instancia EC2 debe estar utilizando un volumen de Amazon EBS. Si la instancia EC2 no está utilizando un volumen de Amazon EBS, entonces, su única opción es para terminar la instancia.

Si interrumpe la instancia, se conservan los datos almacenados en el volumen de EBS. Si el usuario termina la instancia, todos los datos almacenados en el dispositivo de almacenamiento local de la instancia se perderán. En cualquier caso, interrupción o eliminación, no se le seguirá cobrando por la instancia EC2. Sin embargo, si interrumpe la instancia, se le seguirá cobrando por el almacenamiento de EBS que persiste después de que se interrumpe la instancia.

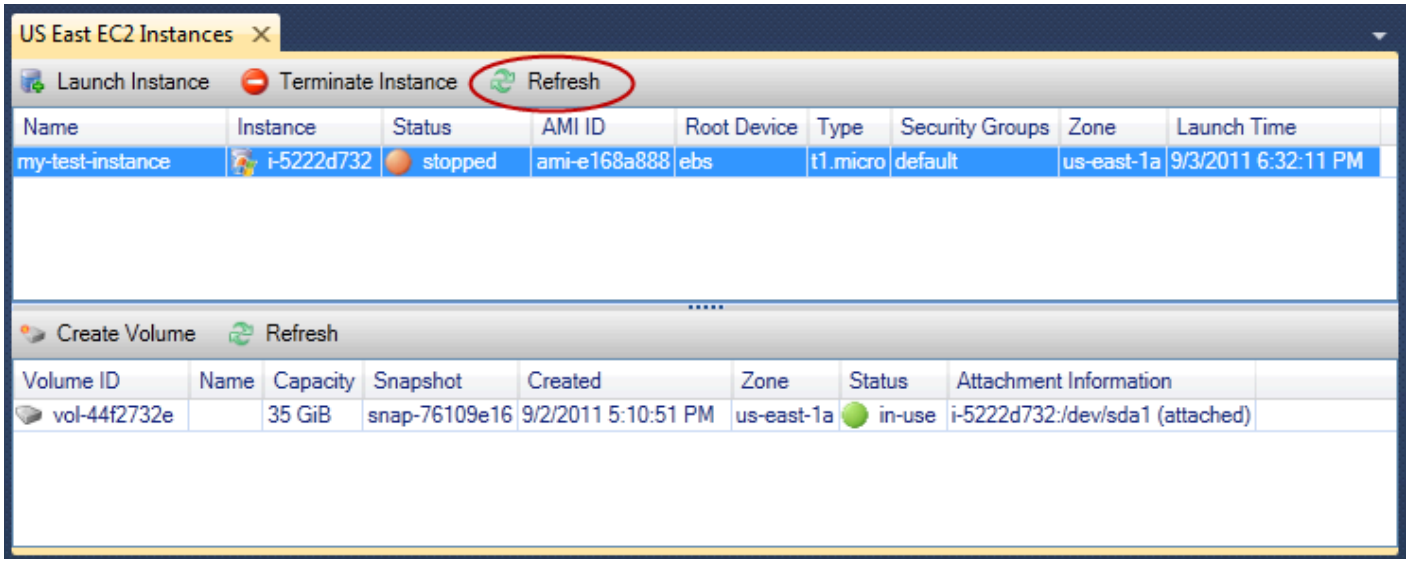
Para terminar una instancia también puede utilizar el escritorio remoto para conectarse a la instancia y, a continuación, desde Windows.iniciaMenú, useShutdown. Puede configurar la instancia para que se interrumpa o termine en esta situación.

Para interrumpir una instancia de Amazon EC2

1. EnAWSExplorer, expanda elAmazon EC2Nodo, abra el menú contextual (con el botón derecho del ratón) deInstanciasy luego seleccioneVista. En la lista Instances (Instancias), haga clic con el botón derecho en la instancia que desea interrumpir y elija Stop (Detener) desde el menú contextual. Elija Yes (Sí) para confirmar que desea interrumpir la instancia.

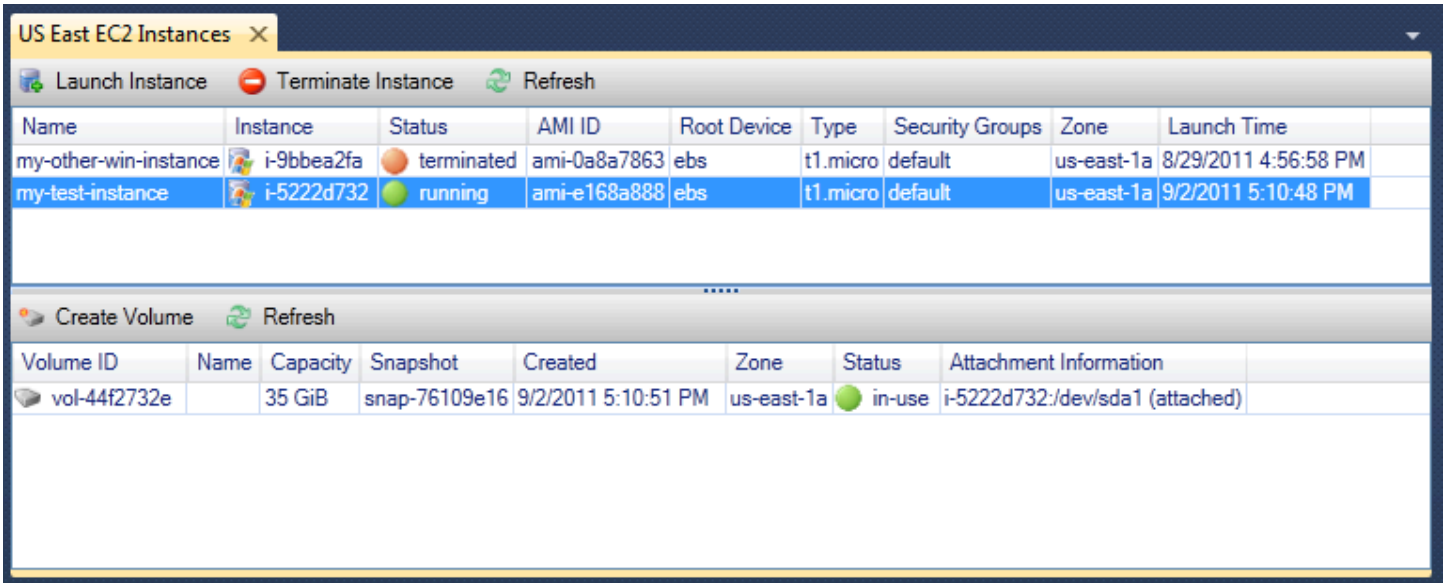


2. En la parte superior de la lista Instances (Instancias), elija Refresh (Actualizar) para ver el cambio en el estado de la instancia de Amazon EC2. Dado que interrumpimos en lugar de finalizar la instancia, el volumen de EBS asociado con la instancia sigue estando activo.



Las instancias terminadas siguen estando visibles

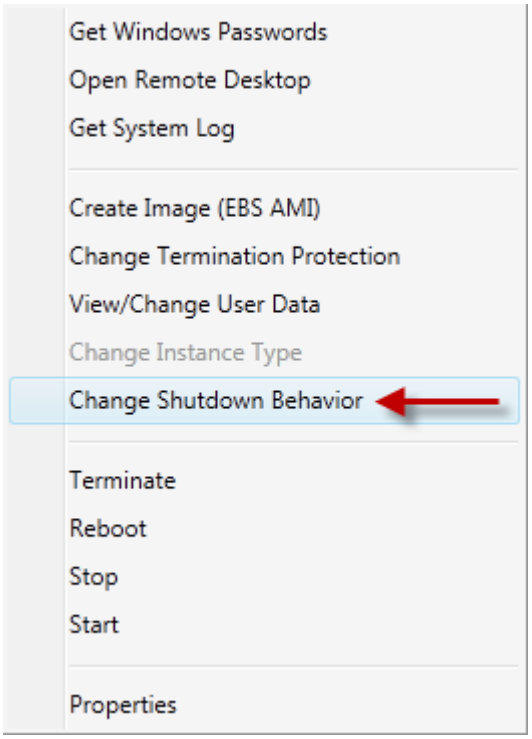
Si termina una instancia, seguirá apareciendo en la lista Instance (Instancia) junto con las instancias en ejecución o interrumpidas. Al final,AWSReclama estos casos y desaparecen en la lista. No se le cobrarán las instancias cuyo estado sea terminado.



Para especificar el comportamiento de una instancia EC2 en el apagado

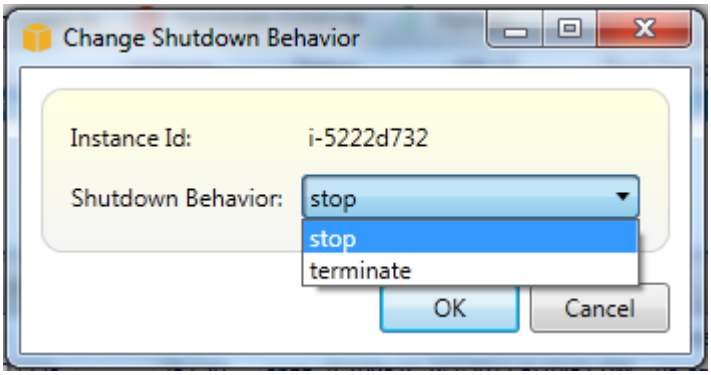
LaAWSToolkit le permite especificar si una instancia de Amazon EC2 se interrumpirá o terminará siShutdownse selecciona de lainiciaMenú.

1. En la lista Instances (Instancias), haga clic con el botón derecho en una instancia de Amazon EC2 y, a continuación, elija Change shutdown behavior (Cambiar el comportamiento de cierre).



Elemento del menú Change Shutdown Behavior (Cambiar el comportamiento de cierre)

2. En el cuadro de diálogo Change Shutdown Behavior, elija Stop o Terminate en la lista desplegable Shutdown Behavior.



Administración de instancias Amazon ECS

AWSExplorer ofrece vistas detalladas de clústeres de Amazon Elastic Container Service (Amazon ECS) y repositorios de contenedores. Puede crear, eliminar y administrar los detalles del clúster y del contenedor en el entorno de desarrollo de Visual Studio.

Modificación de las propiedades del servicio

Puede ver los detalles del servicio, los eventos del servicio y las propiedades del servicio desde la vista del clúster.

1. EnAWSExplorador, abra el menú contextual (clic con el botón derecho) del clúster cuYA administración y, a continuación, elijaVista.
2. En la vista ECS Cluster, haga clic en Services (Servicios) a la izquierda y, a continuación, haga clic en la pestaña Details (Detalles) en la vista de detalles. Puede hacer clic en Events (Eventos) para ver los mensajes y en Deployments (Implementaciones) para ver el estado de implementación.
3. Haga clic en Edit. Puede cambiar el número de tareas y el porcentaje mínimo y máximo de tareas en buen estado que desee.
4. Haga clic en Save (Guardar) para aceptar los cambios o en Cancel (Cancelar) para restablecer los valores existentes.

Detención de una tarea

Puede ver el estado actual de las tareas y detener una o varias tareas en la vista del clúster.

Para detener una tarea

1. EnAWSExplorador, abra el menú contextual (clic con el botón derecho) del clúster cuya tareas desea detener y, a continuación, elijaVista.
2. En la vista ECS Cluster, haga clic en Tasks (Tareas) a la izquierda.
3. Asegúrese de que la opción Desired Task Status (Estado de la tarea deseado) está establecida en `Running`. Elija las tareas individuales que desea detener y, a continuación, haga clic en Stop (Detener) o haga clic en Stop All (Detener todo) para seleccionar y detener todas las tareas en ejecución.
4. En el cuadro de diálogo Stop Tasks (Detener tareas), elija Yes (Sí).

Eliminación de un servicio

Puede eliminar los servicios de un clúster desde la vista del clúster.

Para eliminar un servicio del clúster

1. EnAWSExplorador, abra el menú contextual (clic con el botón derecho) del clúster cuya un servicio desea eliminar y, a continuación, elijaVista.
2. En la vista ECS Cluster, haga clic en Services (Servicios) a la izquierda y, a continuación, haga clic en Delete (Eliminar).
3. En el cuadro de diálogo Delete Cluster (Eliminar clúster), si existe un balanceador de carga y un grupo de destino en su clúster, puede elegir eliminarlos con el clúster. No se utilizarán cuando se elimine el servicio.
4. En el cuadro de diálogo Delete Cluster (Eliminar clúster), elija OK (Aceptar). Cuando se elimine el clúster, se quitará deAWSExplorador.

Eliminación de un clúster

Puede eliminar un clúster de Amazon Elastic Container Service deAWSExplorador.

Para eliminar un clúster

1. EnAWSExplorador, abra el menú contextual (clic con el botón derecho) del clúster que desea eliminar en elClústeresnodo deAmazon ECSy luego seleccioneBorrar.
2. En el cuadro de diálogo Delete Cluster (Eliminar clúster), elija OK (Aceptar). Cuando se elimine el clúster, se quitará deAWSExplorador.

Creación de un repositorio

Puede crear un repositorio de Amazon Elastic Container Registry desdeAWSExplorador.

Para crear un repositorio

1. EnAWSExplorador, abra el menú contextual (clic con el botón derecho) deRepositorios denodo bajoAmazon ECSy luego seleccioneCrear repositorio.
2. En el cuadro de diálogo Create Repository (Crear repositorio), escriba un nombre de repositorio y después elija OK (Aceptar).

Eliminación de un repositorio

Puede eliminar un repositorio de Amazon Elastic Container Registry de desdeAWSExplorador.

Para eliminar un repositorio

1. EnAWSExplorador, abra el menú contextual (clic con el botón derecho) deRepositorios denodo bajoAmazon ECSy luego seleccioneEliminar repositorio.
2. En el cuadro de diálogo Delete Repository (Eliminar repositorio), puede elegir eliminar el repositorio aunque contenga imágenes. De lo contrario, solo se eliminará si está vacío. Haga clic en Yes (Sí).

Administración de grupos de seguridad desde laAWSExplorador

El Toolkit for Visual Studio le permite crear y configurar grupos de seguridad para utilizarlos con instancias de Amazon Elastic Compute Cloud (Amazon EC2) yAWS CloudFormation. Cuando lanza instancias de Amazon EC2 o implementa una aplicación en laAWS CloudFormation, debe especificar un grupo de seguridad que se asociará a las instancias de Amazon EC2. (Implementación en laAWS CloudFormationcrea instancias de Amazon EC2.)

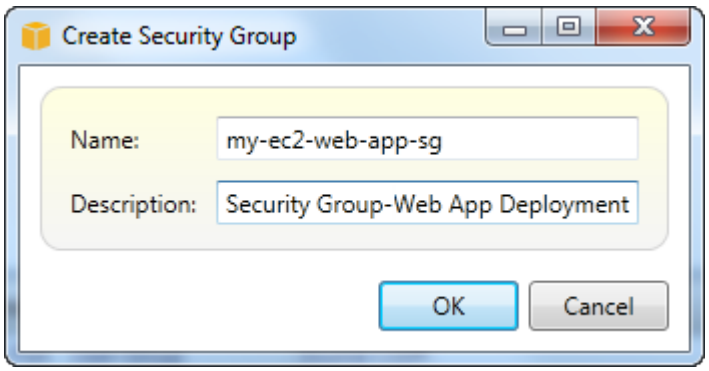
Un grupo de seguridad actúa como un firewall para el tráfico de red entrante. El grupo de seguridad especifica qué tipos de tráfico de red se permiten en una instancia de Amazon EC2. También puede especificar que se aceptará tráfico entrante procedente de determinadas direcciones IP solamente o de usuarios especificados u otros grupos de seguridad solamente.

Creación de un grupo de seguridad

En esta sección, vamos a crear un grupo de seguridad. Una vez que se haya creado, el grupo de seguridad no tendrá ningún permiso configurado. La configuración de permisos se realiza por medio de una operación adicional.

Para crear un grupo de seguridad

1. EnAWSExplorer, debajo de laAmazon EC2, abra el menú contextual (botón derecho del ratón) en laGrupos de seguridadnodo y, a continuación, elijaVista.
2. En la pestaña EC2 Security Groups (Grupos de seguridad de EC2), elija Create Security Group (Crear grupo de seguridad).
3. En el cuadro de diálogo Create Security Group (Crear grupo de seguridad), escriba un nombre y una descripción para el grupo de seguridad y, a continuación, elija OK (Aceptar).

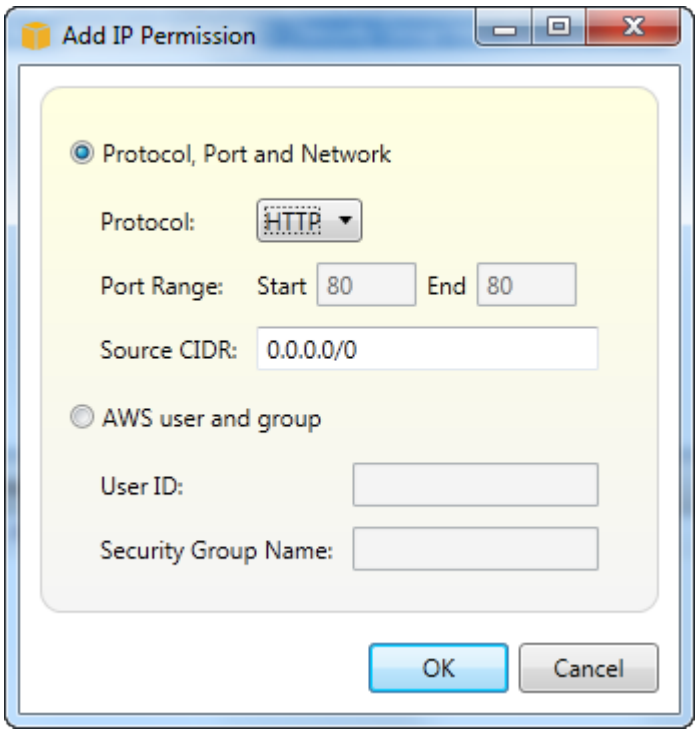


Adición de permisos a los grupos de seguridad

En esta sección, añadiremos permisos al grupo de seguridad para permitir el tráfico web a través de los protocolos HTTP y HTTPS. También permitiremos que otros equipos se conecten a través del Protocolo de escritorio remoto (RDP) de Windows.

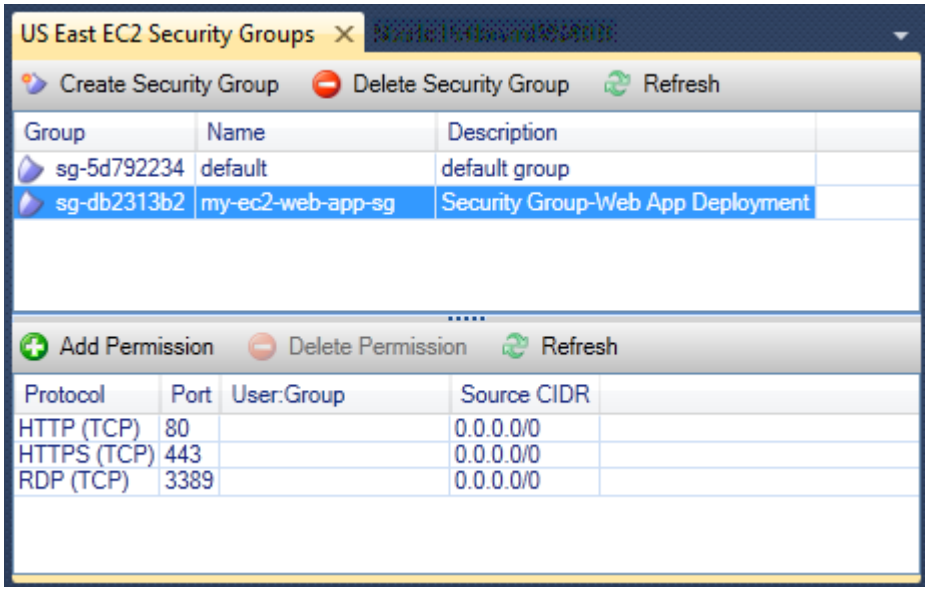
Para añadir permisos a un grupo de seguridad

1. En la pestaña EC2 Security Groups (Grupos de seguridad de EC2), elija un grupo de seguridad y, a continuación, elija el botón Add Permission (Añadir permiso).
2. En el cuadro de diálogo Add IP Permission (Añadir permiso de IP), elija el botón de opción Protocol, Port and Network (Protocolo, puerto y red) y, a continuación, en la lista desplegable Protocol (Protocolo), elija HTTP. El rango de puertos se ajusta automáticamente al puerto 80, el puerto predeterminado para HTTP. El campo Source CIDR (CIDR de origen) se establece en 0.0.0.0/0 de forma predeterminada, lo que especifica que se aceptará el tráfico de la red HTTP desde cualquier dirección IP externa. Seleccione OK (Aceptar).



Abra el puerto 80 (HTTP) para este grupo de seguridad.

3. Repita este proceso para HTTPS y RDP. Los permisos de los grupos de seguridad deben tener ahora el siguiente aspecto.



También puede establecer permisos en el grupo de seguridad especificando un ID de usuario y un nombre de grupo de seguridad. En este caso, las instancias de Amazon EC2 de este grupo de seguridad aceptarán todo el tráfico de red entrante procedente de instancias de Amazon EC2 en el

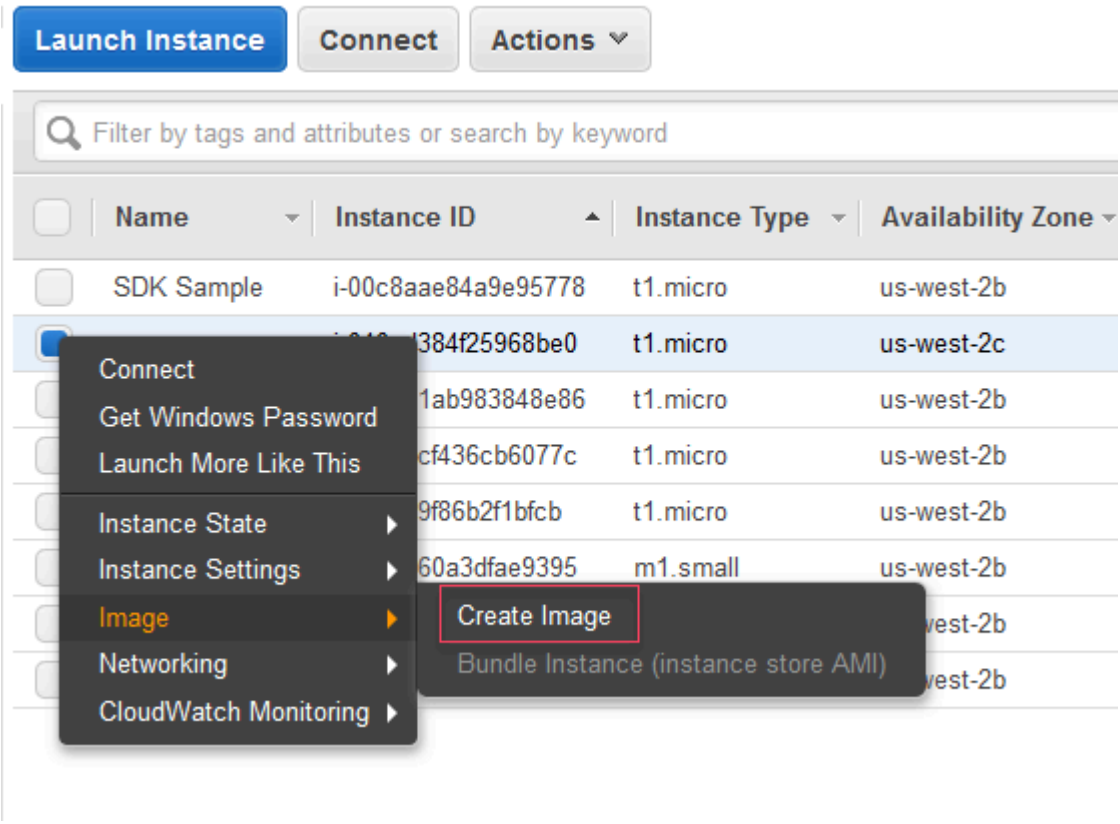
grupo de seguridad especificado. También debe especificar el ID de usuario como una manera de desambiguar el nombre del grupo de seguridad; los nombres de los grupos de seguridad no tienen que ser únicos en todos losAWS. Para obtener más información sobre los grupos de seguridad, consulte la documentación de EC2.

Cree una AMI a partir de una instancia de Amazon EC2

Desde la vista Amazon EC2 Instances (Instancias de Amazon EC), puede crear Imágenes de máquina de Amazon (AMI) desde instancias en ejecución o interrumpidas. Para obtener información más detallada acerca de las AMI, consulte el tema Amazon Machine Images (AMI) de la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Windows.

Creación de una AMI a partir de una instancia

1. Haga clic con el botón derecho en la instancia que desee utilizar como base para su AMI y elija Create Image (Crear imagen) desde el menú contextual.

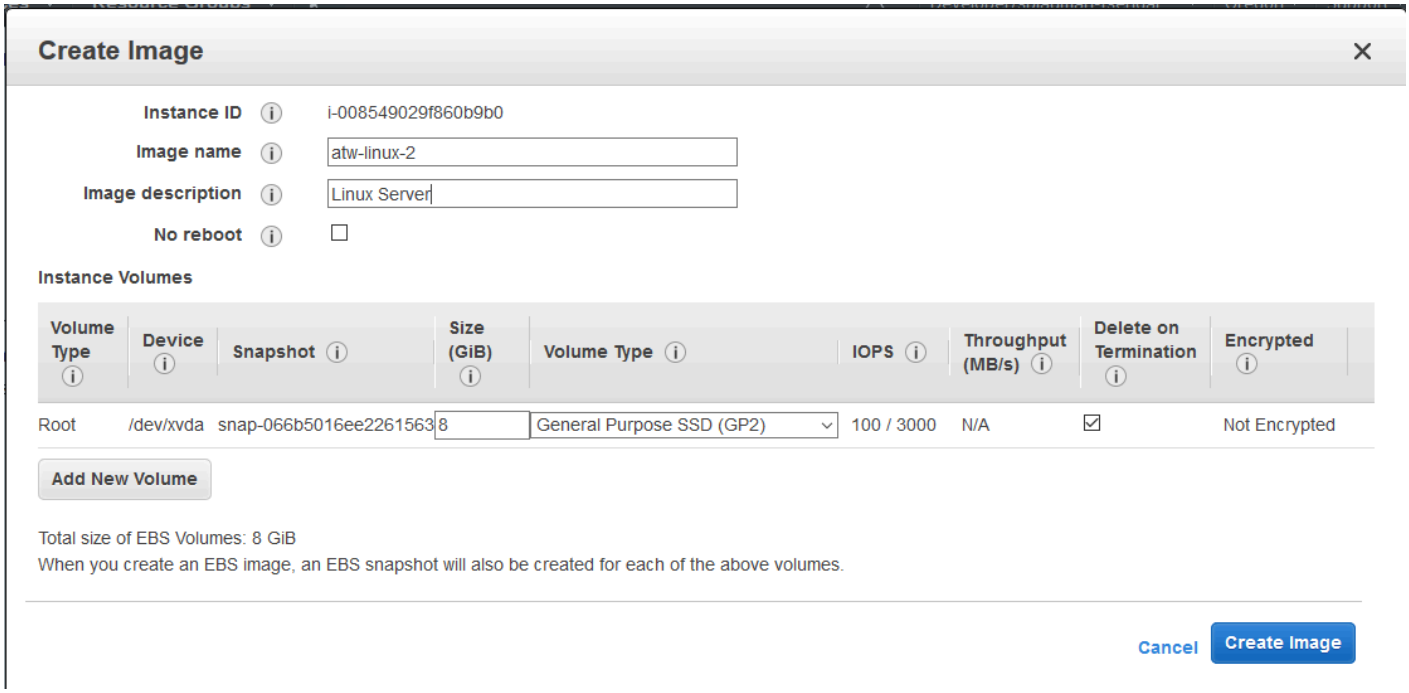


Menú contextual Create Image (Crear imagen)

2. En el cuadro de diálogo Create Image (Crear imagen), escriba un nombre y una descripción únicos, a continuación, elija Create Image (Crear imagen). De forma predeterminada, Amazon

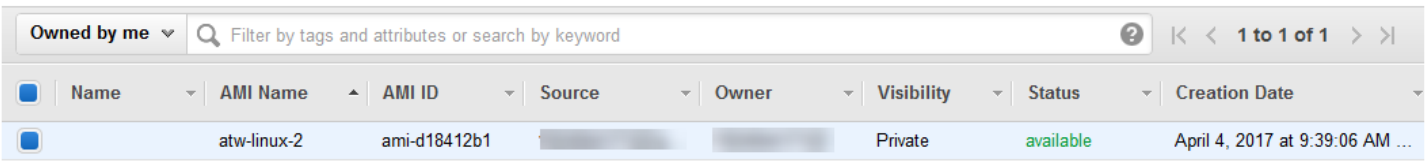
EC2 apaga la instancia; toma instantáneas de todos los volúmenes asociados; crea y registra la AMI y después reinicia la instancia. Elige Sin reinicio si no quieres que se cierre la instancia.

> **Warning**
>
> Si elige No reboot (Sin reiniciar), no podemos garantizar la integridad del sistema de archivos de la imagen creada.



Cuadro de diálogo Create Image (Crear imagen)

La AMI puede tardar unos minutos en crearse. Una vez creado, aparecerá en la vista AMIs delAWS Explorador. Para mostrar esta vista, haga doble clic en el nodo Amazon EC2 | AMIS delAWS Explorador. Para consultar las AMI, desde la lista desplegable Viewing (Visualización), elija Owned By Me (De mi propiedad). Es posible que tenga que elegir Refresh (Actualizar) para ver su AMI. Cuando la AMI aparece por primera vez, puede estar en estado pendiente, pero transcurridos unos minutos, hace la transición a estado disponible.



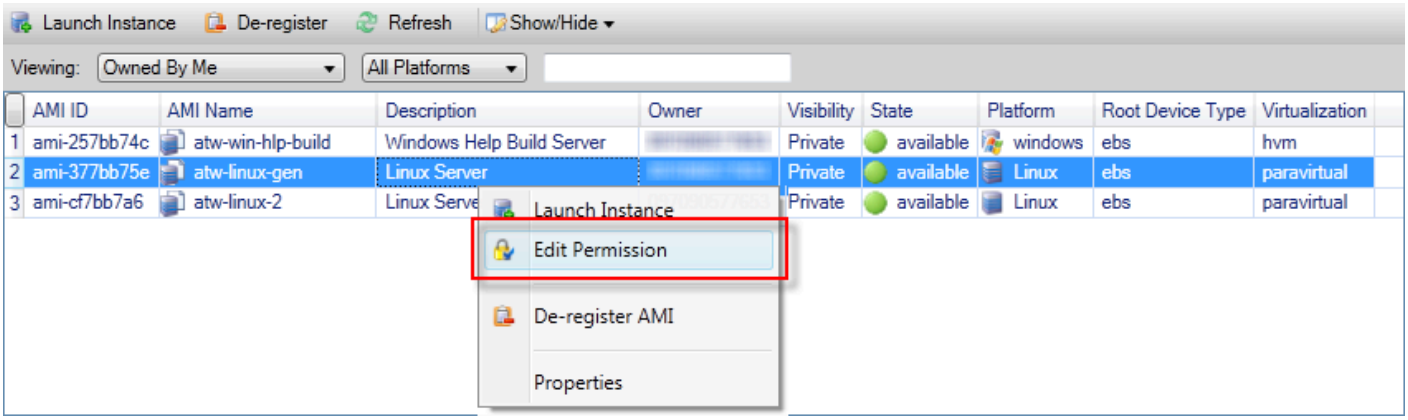
Lista de AMI creadas

Definición de los permisos de lanzamiento en una imagen de máquina de Amazon (AMI)

Puede configurar los permisos de lanzamiento de las imágenes de máquina de Amazon (AMI) en laAMI dever enAWSExplorador. Puede usar el cuadro de diálogo Set AMI Permissions (Configurar permisos de AMI) para copiar los permisos de las AMI.

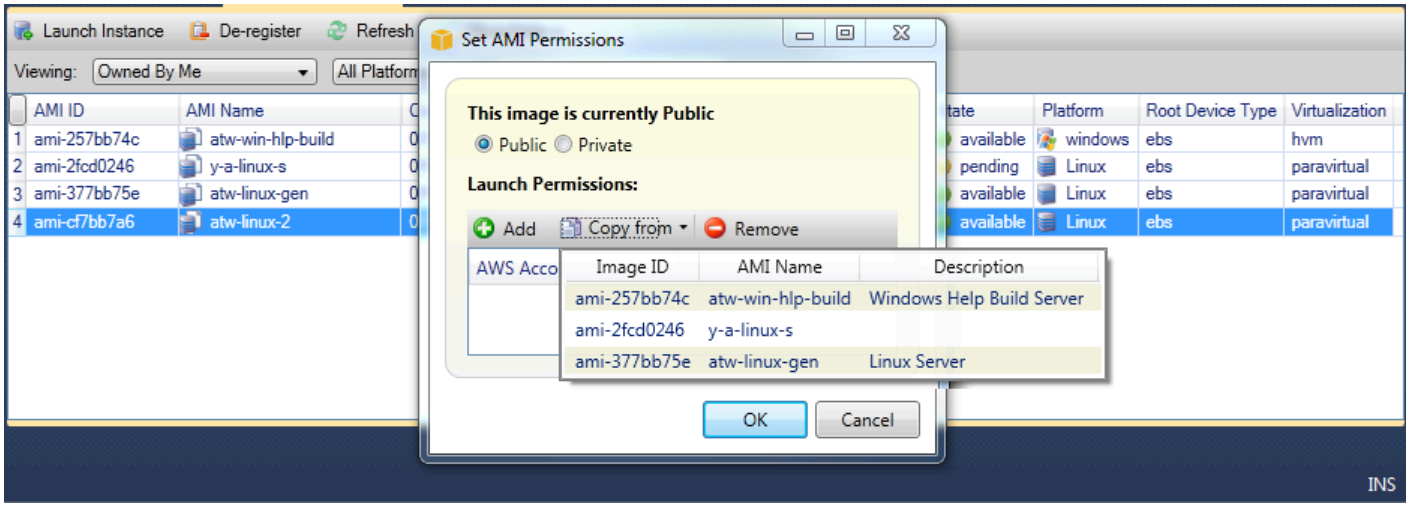
Para definir permisos en una AMI

1. En el navegadorAMI dever enAWSExplorador, abra el menú contextual (clic con el botón derecho) de una AMI y, a continuación, elijaEditar permiso.



2. Existen tres opciones disponibles en el cuadro de diálogo Set AMI Permissions (Establecer permisos de AMI):
   - Para otorgar permiso de lanzamiento, elijaAñadiry escriba el número de cuenta de laAWSusuario al que está otorgando permiso de lanzamiento.
   - Para eliminar un permiso de lanzamiento, elija el número de cuenta para elAWSusuario del que desea eliminar un permiso de lanzamiento y elijaRemove.
   - Para copiar los permisos de una AMI en otra, seleccione una AMI en la lista y elija Copy from (Copiar desde). Los usuarios que tienen permisos de lanzamiento en la AMI elegida, obtendrán permisos de lanzamiento en la AMI actual. Puede repetir este proceso con otras AMI en la lista Copy-from (Copiar desde) para copiar permisos de varias AMI en la AMI de destino.

     LaCopiar datos de con(lista) solo contiene las AMI pertenecientes a la cuenta que estaba activa cuando elAMI dela vista se ha mostrado desdeAWSExplorador. Como resultado, la lista Copy-from (Copiar desde) podría no mostrar ninguna AMI si la cuenta activa no posee otras AMI.



Cuadro de diálogo Copy AMI permissions (Copiar permisos de AMI)

Amazon Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de Amazon Web Services en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que usaría en su propio centro de datos, con los beneficios que supone utilizar la infraestructura escalable deAWS. Para obtener más información, vaya a la Guía del usuario de Amazon VPC.

El Toolkit for Visual Studio permite a un desarrollador obtener acceso a la funcionalidad de VPC de un modo similar al expuesto por elAWS Management Consolesino del entorno de desarrollo de Visual Studio. LaAmazon VPCNodo deAWSExplorador incluye subnodos para las siguientes áreas.

- VPC
- Subredes
- Direcciones IP elásticas
- Gateways de Internet
- ACL de red
- Tablas de ruteo
- Grupos de seguridad

Creación de una VPC pública-privada para la implementación conAWS Elastic Beanstalk

En esta sección se describe cómo crear una Amazon VPC que contenga subredes públicas y privadas. La subred pública contiene una instancia Amazon EC2 que realiza la conversión de direcciones de red (NAT) para permitir que las instancias de la subred privada se comuniquen con la Internet pública. Las dos subredes deben residir en la misma zona de disponibilidad (AZ).

Esta es la configuración mínima de VPC requerida para implementar un entorno de AWS Elastic Beanstalk en una VPC. En este caso, las instancias Amazon EC2 que alojan la aplicación se encuentran en la subred privada y el balanceador de carga de Elastic Load Balancing que dirige el tráfico entrante hacia la aplicación reside en la subred pública.

Para obtener más información sobre la conversión de direcciones de red (NAT), vaya a Instancias NAT en la Guía del usuario de Amazon Virtual Private Cloud. Si desea ver un ejemplo del procedimiento para configurar su implementación para que use una VPC, consulte Implementación en Elastic Beanstalk.

Para crear una VPC de subred pública-privada

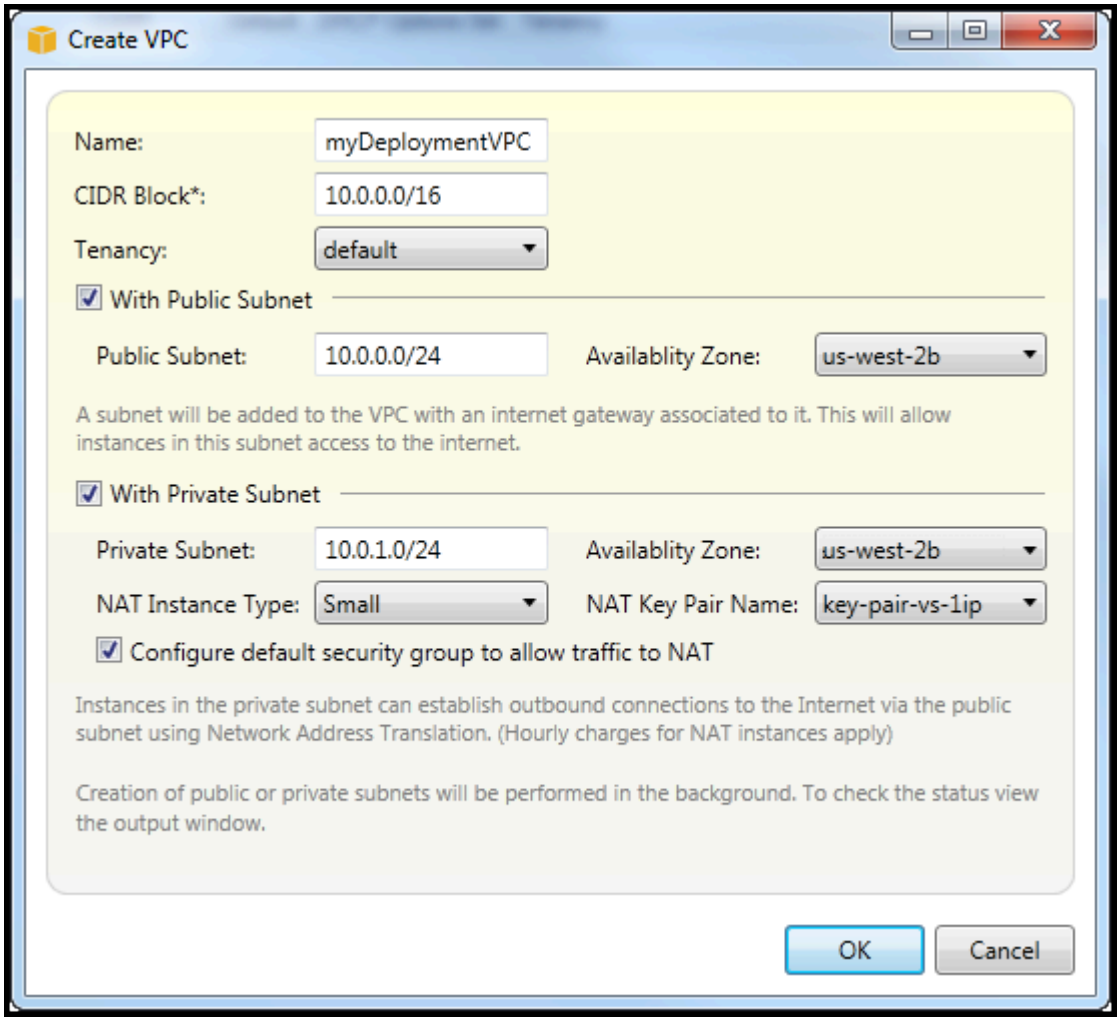
1. En el navegadorAmazon VPCNodo enAWSExplorer, abra elVPCSubnodo y, después,Crear una VPC.

2. Configure la VPC del modo siguiente:
   - Escriba un nombre para la VPC.
   - Active las casillas de verificación With Public Subnet (Con subred pública) y With Private Subnet (Con subred privada).

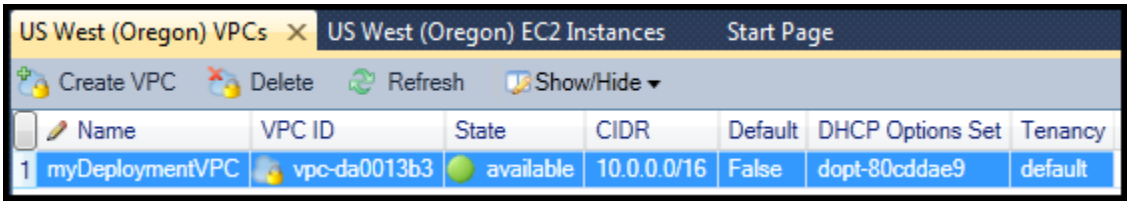
- En el cuadro de lista desplegable Availability Zone (Zona de disponibilidad) de cada subred, elija una zona de disponibilidad. Asegúrese de usar la misma zona de disponibilidad para las dos subredes.
- Para la subred privada, en NAT Key Pair Name (Nombre de par de claves de NAT), proporcione un par de claves. Este key pair se usa para la instancia Amazon EC2 que realiza la conversión de direcciones de red de la subred privada a la Internet pública.
- Active la casilla de verificación Configure default security group to allow traffic to NAT (Configurar el grupo de seguridad predeterminado para permitir el tráfico a NAT).

Escriba un nombre para la VPC. Active las casillas de verificación With Public Subnet (Con subred pública) y With Private Subnet (Con subred privada). En el cuadro de lista desplegable Availability Zone (Zona de disponibilidad) de cada subred, elija una zona de disponibilidad. Asegúrese de usar la misma zona de disponibilidad para las dos subredes. Para la subred privada, en NAT Key Pair Name (Nombre de par de claves de NAT), proporcione un par de claves. Este key pair se usa para la instancia Amazon EC2 que realiza la conversión de direcciones de red de la subred privada a la Internet pública. Active la casilla de verificación Configure default security group to allow traffic to NAT (Configurar el grupo de seguridad predeterminado para permitir el tráfico a NAT).

Seleccione OK (Aceptar).

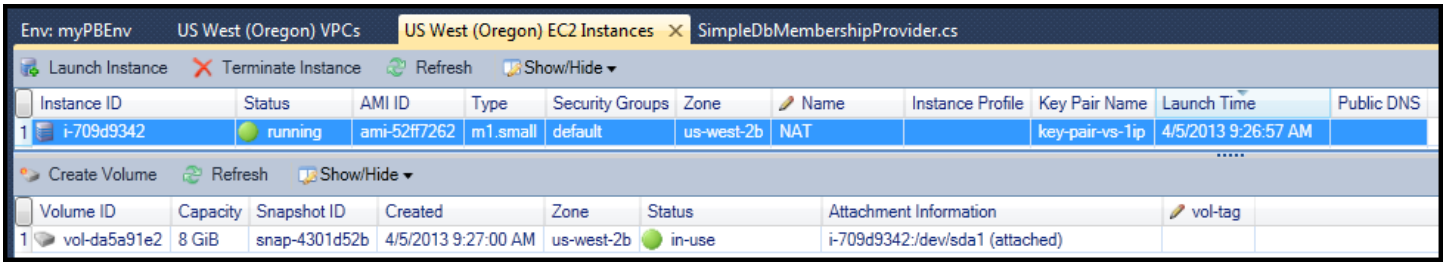


Puede ver la nueva VPC enVPCPestaña enAWSExplorador.



La instancia NAT podría tardar unos minutos en lanzarse. Cuando esté disponible, puede verla ampliandoAmazon EC2Nodo enAWSExplorer y, a continuación, abrir elInstanciassubnodo.

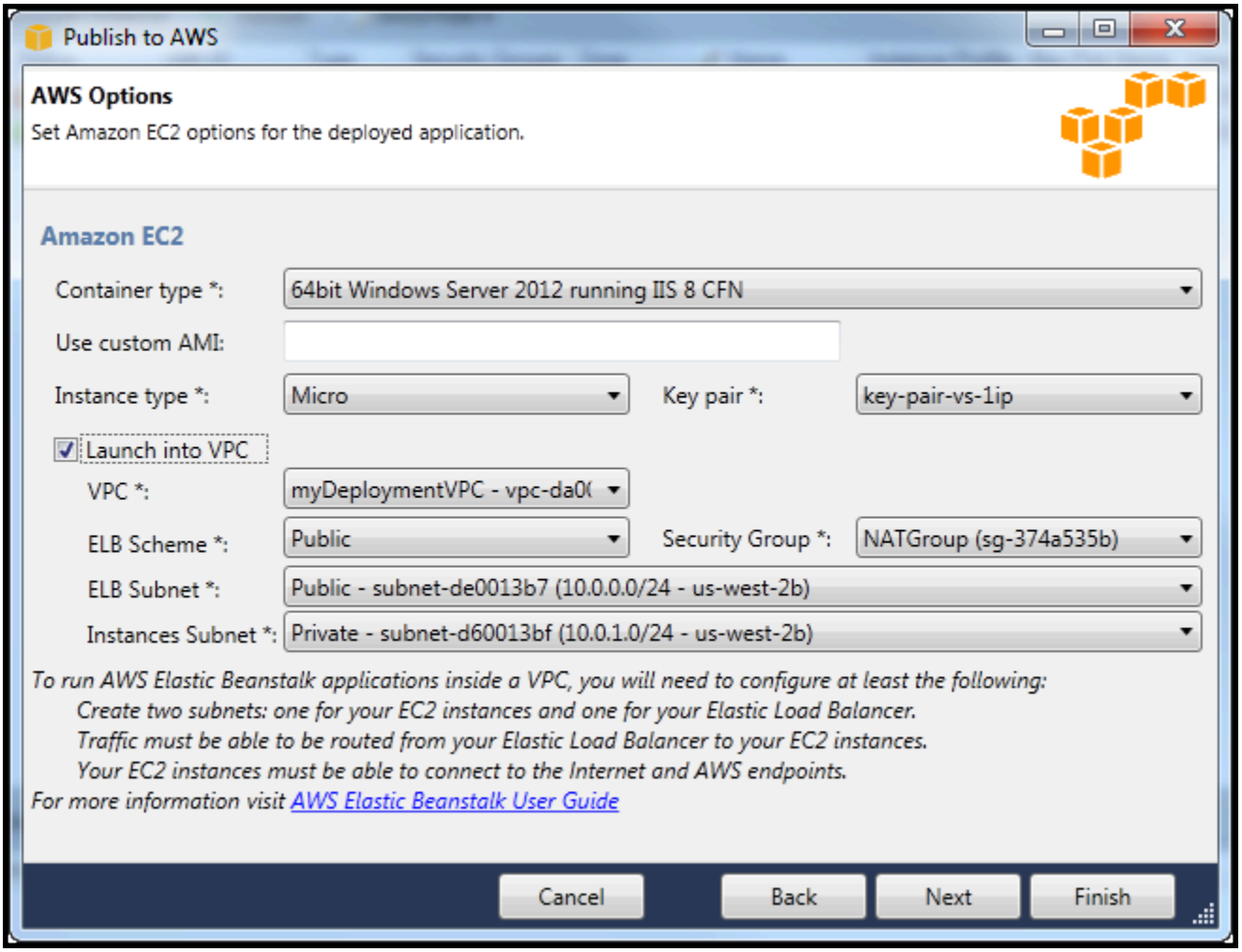
UnAWS Elastic Beanstalk(Amazon EBS) se crea para la instancia NAT automáticamente. Para obtener más información sobre Elastic Beanstalk, visiteAWS Elastic Beanstalk(EBS)en laGuía del usuario de Amazon EC2 para instancias de Linux.



Siimplementar una aplicación en unAWS Elastic Beanstalkentornoy elija lanzar el entorno en una VPC, el kit de herramientas rellenará elPublicación enAmazon Web Servicescuadro de diálogo con la información de configuración de la VPC.

El Toolkit rellena el cuadro de diálogo solo con información de las VPC que se han creado en el Toolkit, no de las VPC creadas con laAWS Management Console. Esto se debe a que cuando el Toolkit crea una VPC, etiqueta los componentes de la VPC para que esta pueda obtener acceso a su información.

En la siguiente captura de pantalla del asistente de implementación, se muestra un ejemplo de un cuadro de diálogo que se ha rellenado automáticamente con valores de una VPC creada en el Toolkit.



Para eliminar un VPC

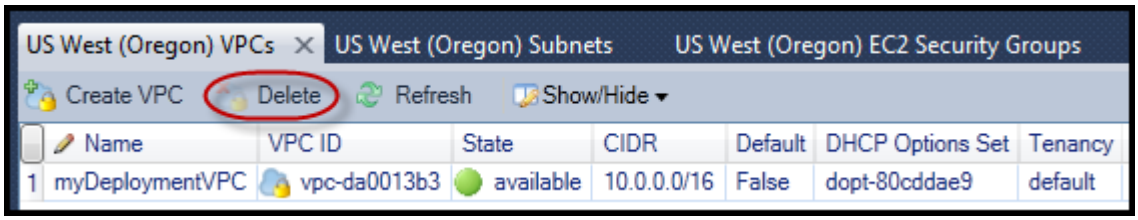
Para eliminar la VPC, debe terminar primero las instancias Amazon EC2 de la VPC.

1. Si ha implementado una aplicación en un entorno de AWS Elastic Beanstalk en la VPC, elimine el entorno. Esto terminará las instancias Amazon EC2 que alojan su aplicación junto con el balanceador de carga de Elastic Load Balancing.

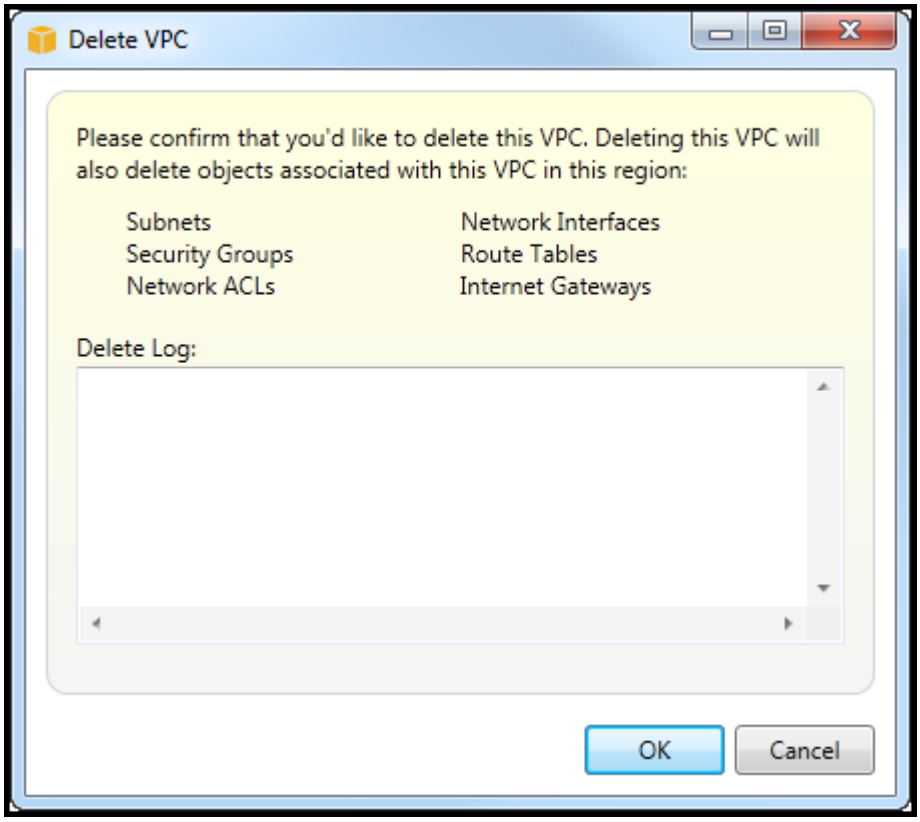
   Si intenta terminar directamente las instancias que alojan su aplicación sin eliminar el entorno, el servicio Auto Scaling creará automáticamente nuevas instancias para reemplazar a las eliminadas. Para obtener más información, vaya a la Guía del usuario de Auto Scaling.
2. Elimine la instancia NAT de la VPC.

   No es necesario eliminar el volumen de Amazon EBS asociado con la instancia NAT para eliminar la VPC. Sin embargo, si no elimina el volumen, se seguirá aplicando un costo adicional por él aunque se hayan eliminado la instancia NAT y la VPC.

3. En la pestaña VPC, elija el enlace Delete (Eliminar) para eliminar la VPC.



4. En el cuadro de diálogo Delete VPC (Eliminar VPC), elija OK (Aceptar).



Uso del editor AWS CloudFormation de plantillas para Visual Studio

El Toolkit for Visual Studio incluye AWS CloudFormation un editor de plantillas AWS CloudFormation y proyectos de plantillas para Visual Studio. Entre las características compatibles se incluyen las siguientes:

- Crear plantillas nuevas (vacías o copiadas de una pila o plantilla de ejemplo existente) utilizando el tipo de proyecto de AWS CloudFormation plantilla suministrado.

- Edición de plantillas con validación JSON automática, finalización automática, plegado de código y resaltado de sintaxis.
- Sugerencia automática de funciones intrínsecas y parámetros de referencia de recursos para los valores de los campos de la plantilla.
- Elementos de menú para realizar acciones comunes en la plantilla desde Visual Studio.

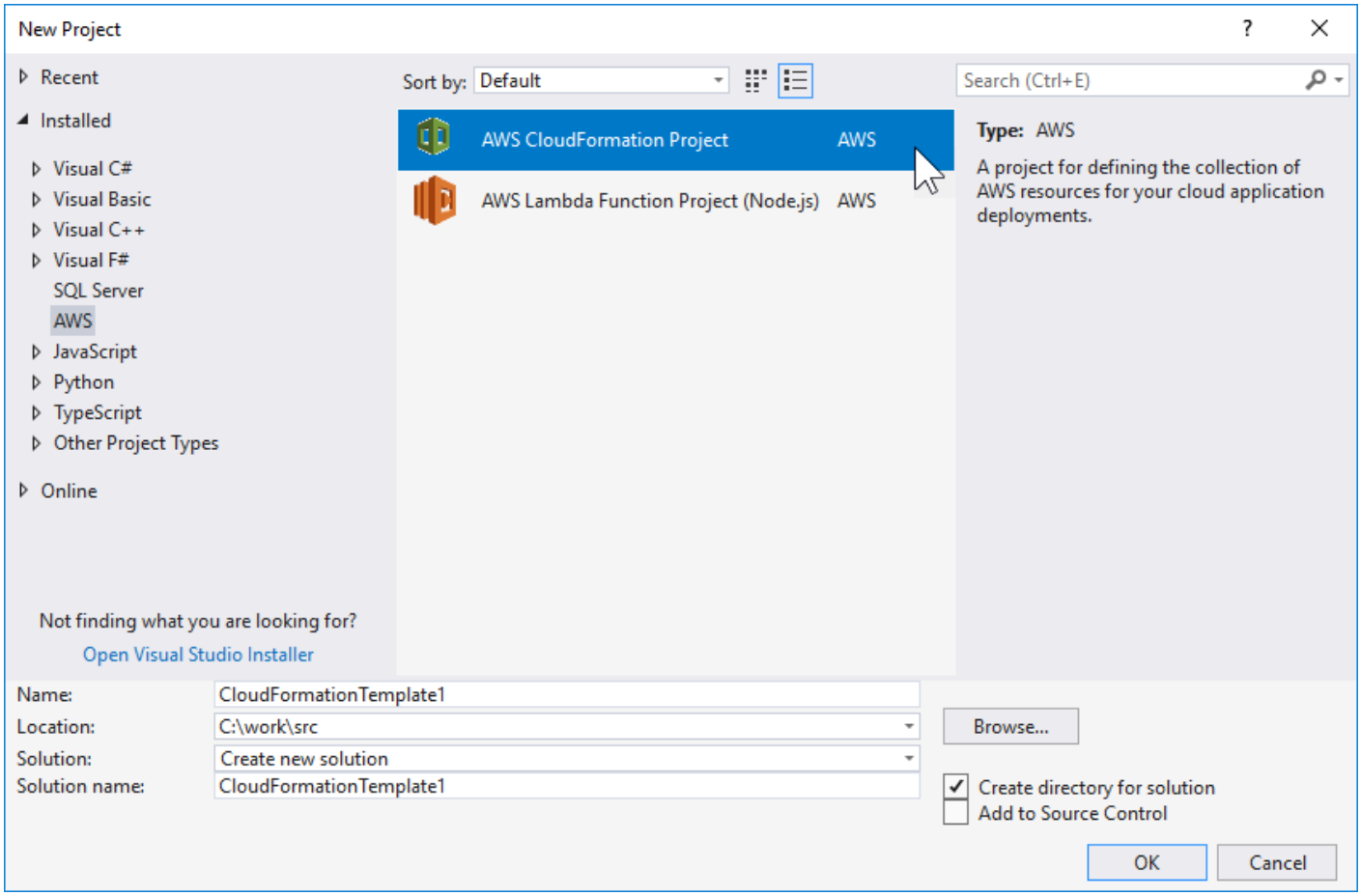
Temas

Creación de un proyecto de plantilla de AWS CloudFormation en Visual Studio

Para crear un proyecto de plantilla

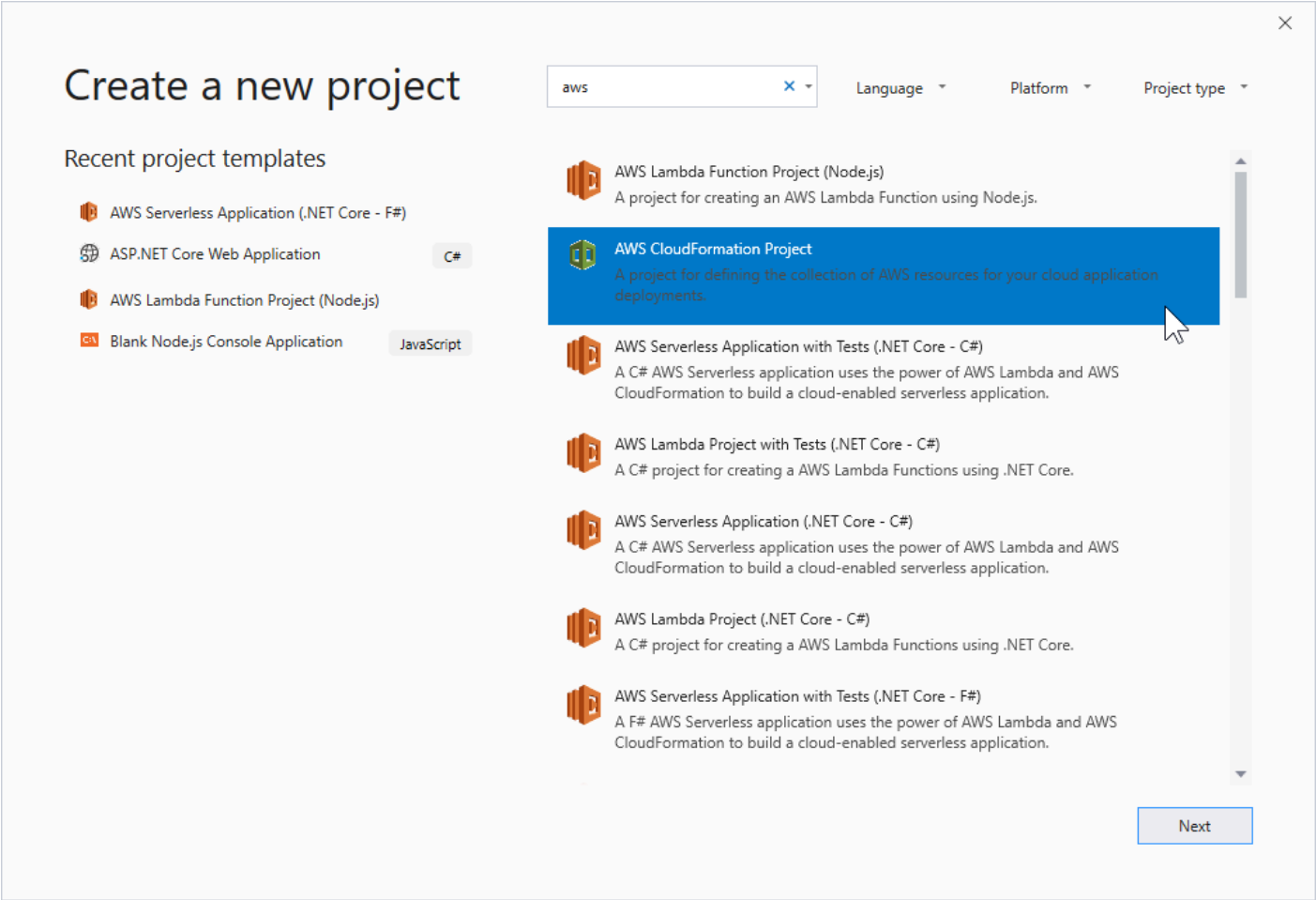
1. En Visual Studio, elija File (Archivo), elija New (Nuevo) y, a continuación, elija Project (Proyecto).
2. Para Visual Studio 2017:

   En el navegadorNuevo proyecto deCuadro de diálogo, expandirInstaladoy seleccionarAWS.



Para Visual Studio 2019:

En el cuadro de diálogo New Project (Nuevo proyecto), asegúrese de que los cuadros desplegables Language (Lenguaje), Platform (Plataforma) y Project type (Tipo de proyecto) están definidos en "All ..." (Todo...) e introduzca aws en el campo Search (Buscar).



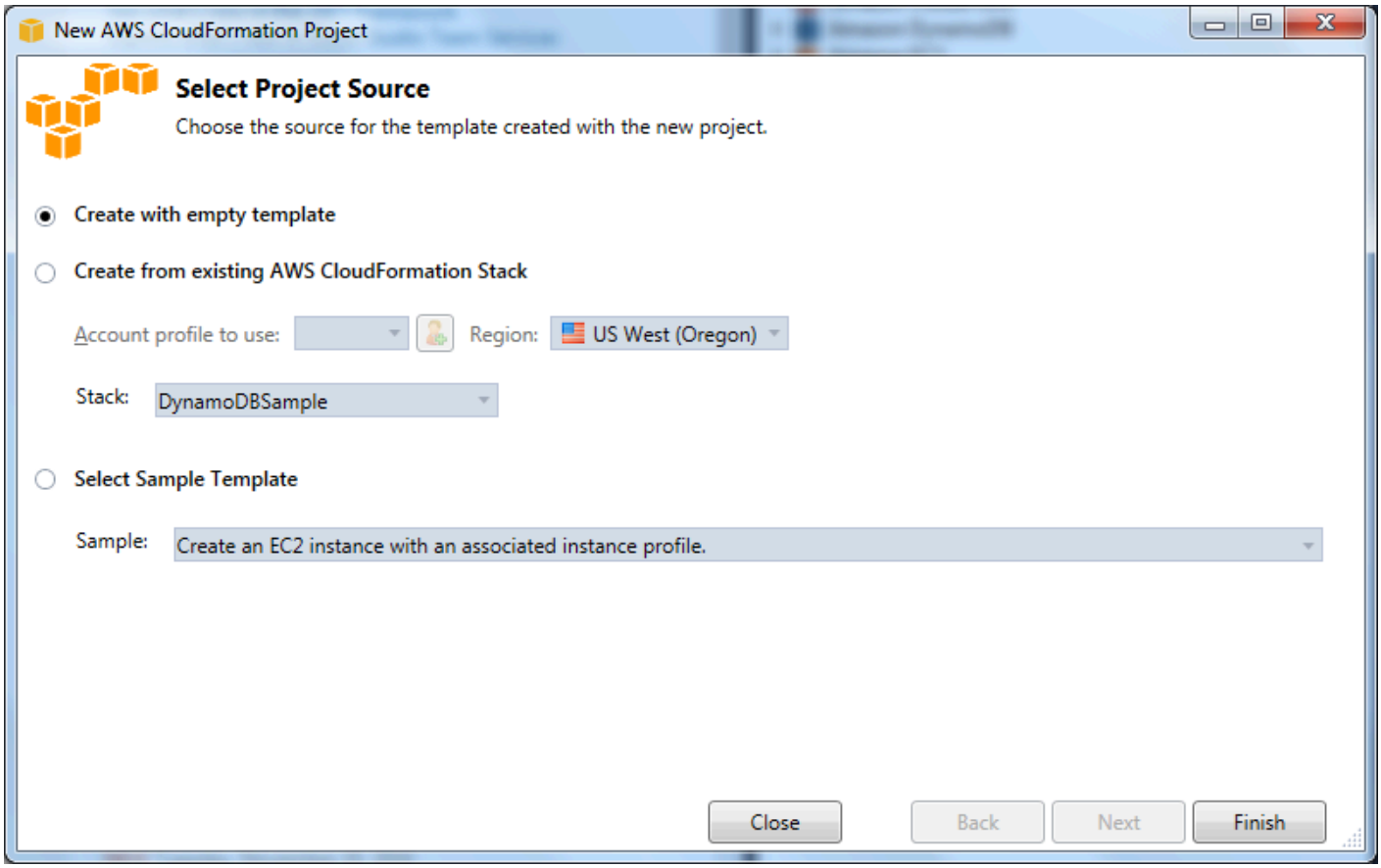
3. Seleccione elAWSProyecto CloudFormationplantilla de.
4. Para Visual Studio 2017:

   Introduzca los valores de Name (Nombre), Location (Ubicación) deseados, etc., para su proyecto de plantilla y haga clic en OK (Aceptar).

   Para Visual Studio 2019:

   Haga clic en Next (Siguiente). En el siguiente cuadro de diálogo, introduzca los valores de Name (Nombre), Location (Ubicación) deseados, etc., para su proyecto de plantilla y haga clic en Create (Crear).
5. En la página Select Project Source (Seleccionar origen del proyecto), elija el origen de la plantilla que creará:
   - Create with empty template (Crear con plantilla vacía) genera una plantilla nueva de AWS CloudFormation vacía.

- Crear a partir de existenteAWS|CFN| pilagenera una plantilla a partir de una pila existente en suAWSaccount. (La pila no tiene que tener un estado de `CREATE_COMPLETE`).
- Select sample template (Seleccionar plantilla de muestra) genera una plantilla a partir de una de las plantillas de ejemplo de AWS CloudFormation.

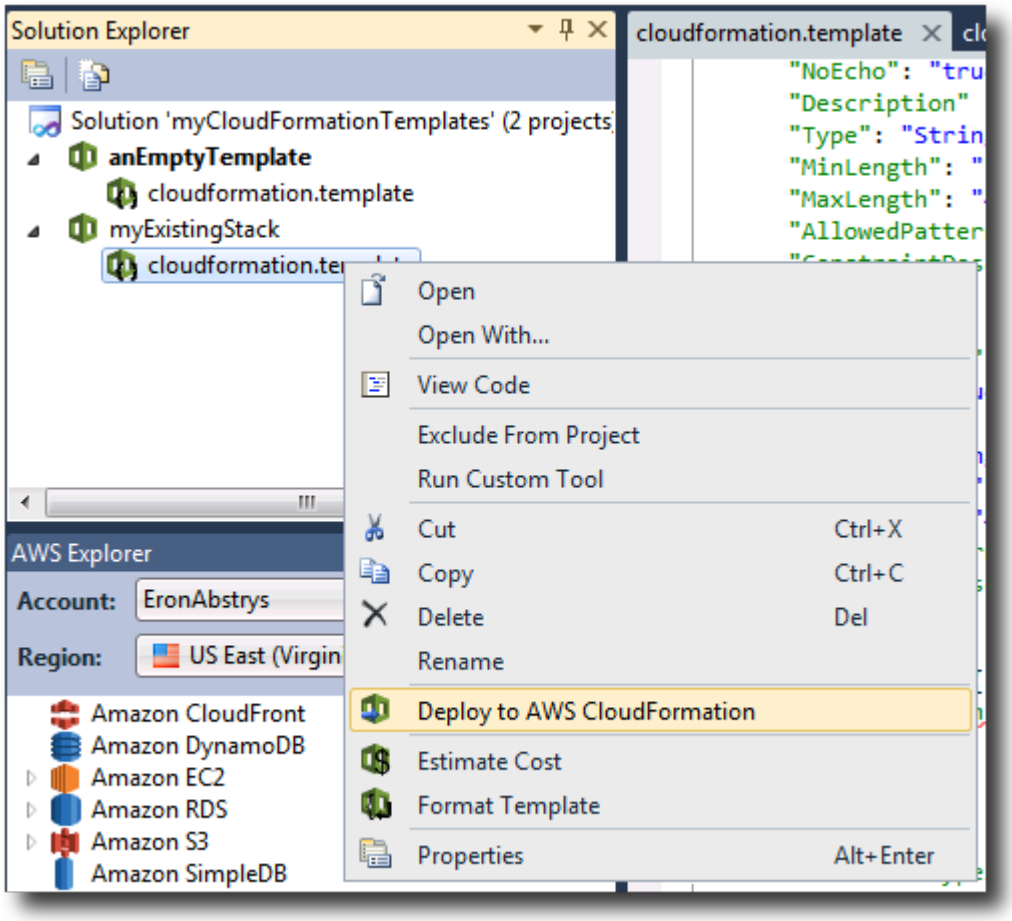


6. Para completar la creación de su proyecto de plantilla de AWS CloudFormation, elija Finish (Finalizar).

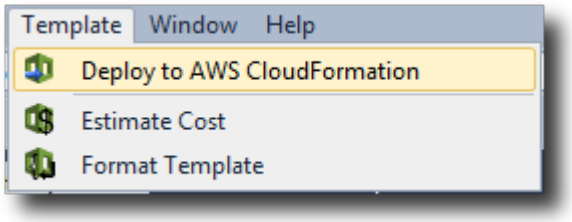
Implementación de una plantilla de AWS CloudFormation en Visual Studio

Para implementar una plantilla de CFN

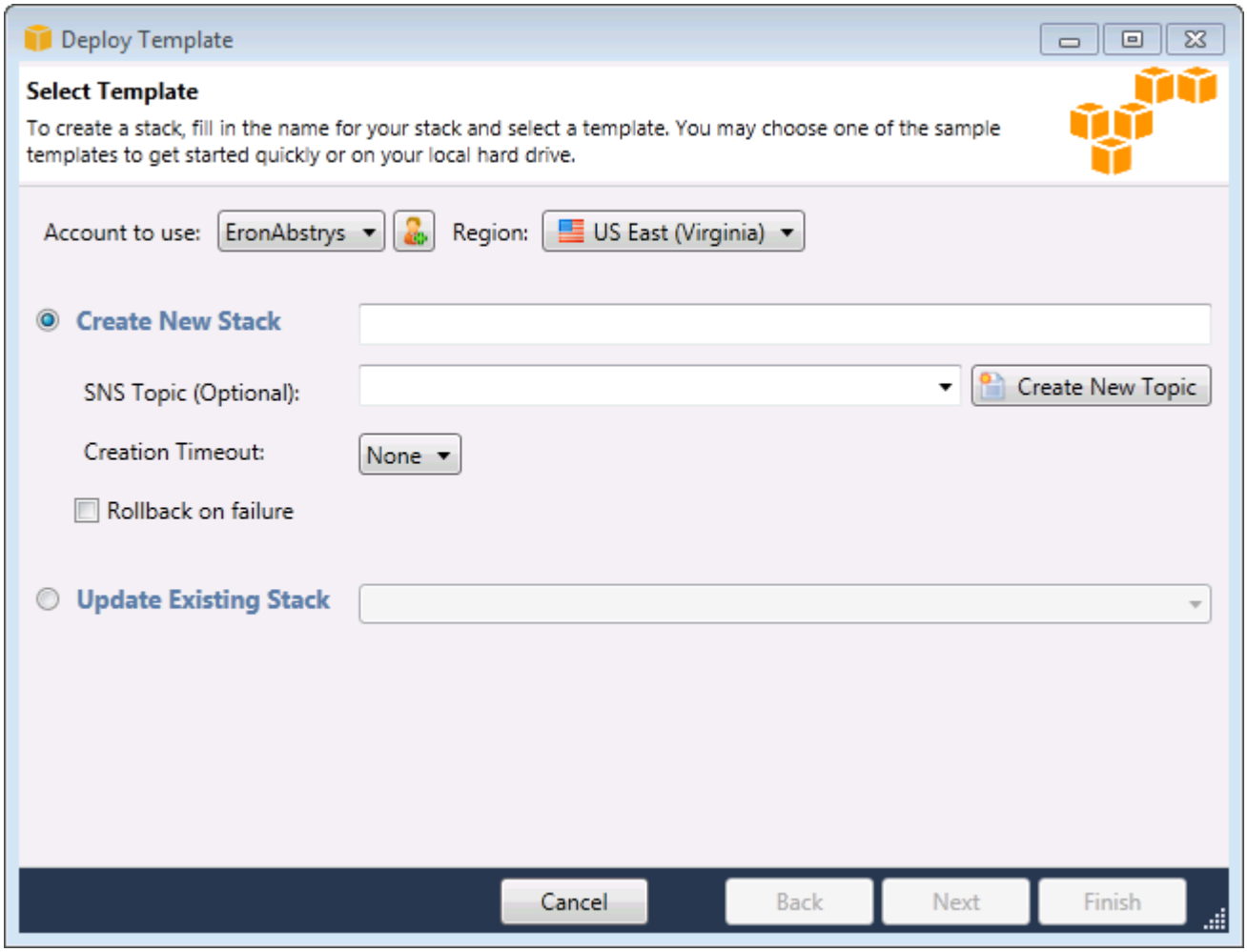
1. En Solution Explorer, abra el menú contextual (clic con el botón derecho) correspondiente a la plantilla que desee implementar y elijaImplementar enAWS CloudFormation.



Como alternativa, para implementar la plantilla que está editando, en laTemplate (Plantilla)menú, elijaImplementar enAWS CloudFormation.



2. En la páginaImplementar plantillapágina, elija laCuenta de AWSpara lanzar la pila y la región en la que se lanzará.

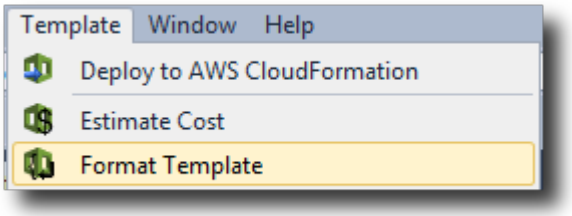


3. Elija Create New Stack (Crear pila nueva) y escriba un nombre para la pila.
4. Elija una (o ninguna) de las siguientes opciones:
   - Para recibir notificaciones acerca del progreso de la pila, en la lista desplegable SNS Topic (Tema de SNS), elija un tema de SNS. También puede crear un tema de SNS eligiendo Create New Topic (Crear tema nuevo) y escribiendo una dirección de correo electrónico en el cuadro.
   - Use Creation Timeout (Tiempo de espera de la creación) para especificar cuánto tiempo debe permitir AWS CloudFormation que transcurra para la creación de la pila antes de considerar que se ha producido un error (y restaurar el estado anterior, a menos que la opción Rollback on failure (Restauración en caso de error) esté desactivada).
   - Use Rollback on failure (Restauración en caso de error) si desea que la pila se revierta (es decir, se elimine a sí misma) en caso de error. Deje esta opción desactivada si desea que la pila permanezca activa, a efectos de depuración, incluso si se no ha podido completar el lanzamiento.
5. Elija Finish (Finalizar) para lanzar la pila.

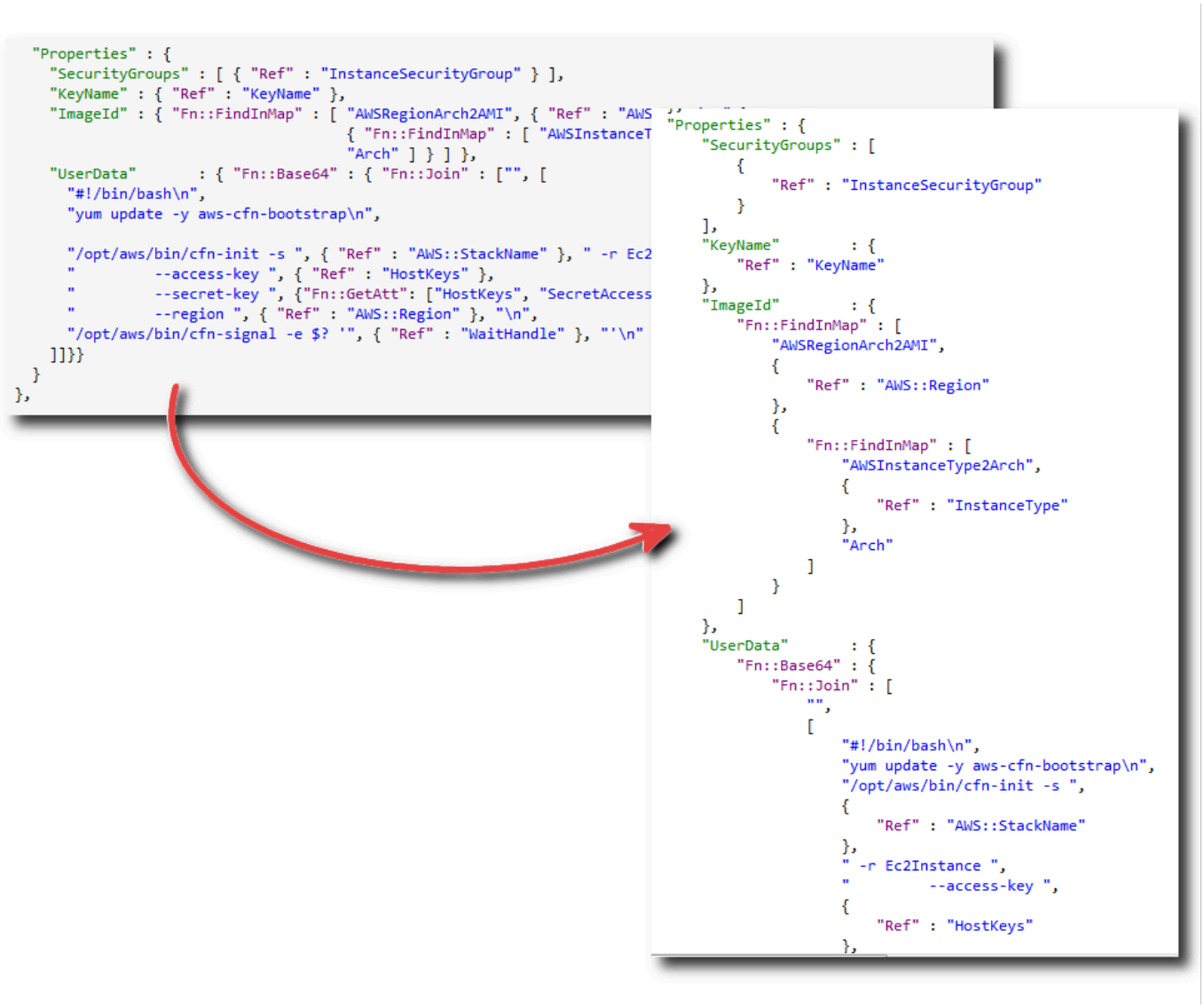
Dar formato a una plantilla de AWS CloudFormation en Visual Studio

- En Solution Explorer, abra el menú contextual (clic con el botón derecho) de la plantilla y elija Format Template (Dar formato a plantilla).

  Como alternativa, para dar formato a la plantilla que está editando, en el menú Template (Plantilla), elija Format Template (Dar formato a plantilla).

  El formato de su código JSON se ajustará para que su estructura se presente con claridad.



Uso de Amazon S3 desdeAWSExplorador

Amazon Simple Storage Service (Amazon S3) le permite almacenar y recuperar datos desde cualquier conexión a Internet. Todos los datos que almacena en Amazon S3 están asociados a su cuenta y, de forma predeterminada, solo usted puede obtener acceso a ellos. Toolkit for Visual Studio le permite almacenar datos en Amazon S3 y ver, administrar, recuperar y distribuir esos datos.

Amazon S3 utiliza el concepto de buckets, que se puede entender como algo similar a los sistemas de archivos o las unidades lógicas. Los buckets pueden contener carpetas, que son similares a los directorios, y objetos, que son similares a los archivos. En esta sección, utilizaremos estos conceptos mientras describimos la funcionalidad de Amazon S3 presentada por Toolkit for Visual Studio.

> **Note**
>
> Para usar esta herramienta, su política de IAM debe conceder permisos para `els3:GetBucketAcl`,`s3:GetBucket`, `ys3:ListBucket`acciones. Para obtener más información, consulteInformación general deAWSPolíticas de IAM.

Creación del bucket de Amazon S3

El bucket es la unidad de almacenamiento más básica de Amazon S3.

Para crear un bucket de S3

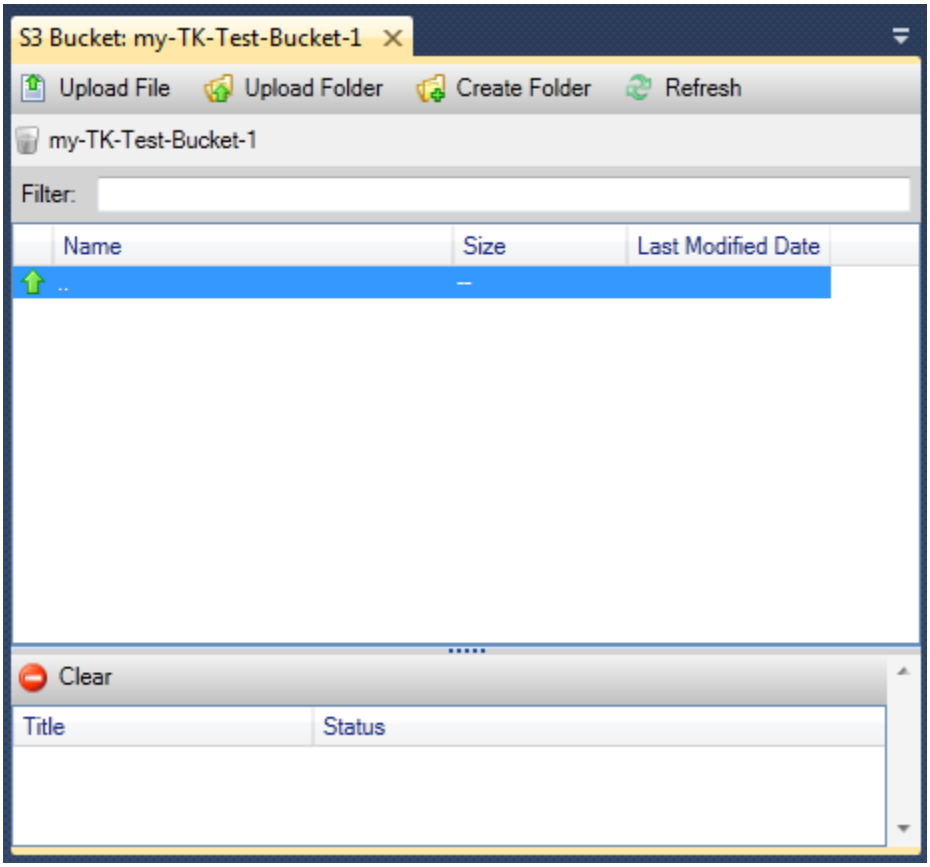
1. EnAWSExplorador, abra el menú contextual (con el botón derecho del ratón) de laAmazon S3nodo y, a continuación, elijacrear un bucket.
2. En el cuadro de diálogo Create Bucket (Crear bucket), escriba un nombre para el bucket. Los nombres de bucket deben ser únicos enAWS. Para obtener información acerca de otras restricciones, consulte la documentación de Amazon S3.
3. Seleccione OK (Aceptar).

Administración de buckets de Amazon S3 desdeAWSExplorador

EnAWSExplorador, las siguientes operaciones están disponibles cuando se abre un menú contextual (clic con el botón derecho) para un bucket de Amazon S3.

Browse

Muestra una vista de los objetos contenidos en el bucket. Aquí puede crear carpetas o cargar archivos o directorios y carpetas completos desde el equipo local. En el panel inferior se muestran los mensajes de estado relativos al proceso de carga. Para borrar esos mensajes, elija el icono Clear (Borrar). También puede obtener acceso a esta vista del bucket haciendo doble clic en el nombre del bucket enAWSExplorador.



Properties

Muestra un cuadro de diálogo en el que puede hacer lo siguiente:

- Establecer permisos de Amazon S3 de para:
  - usted como propietario del bucket
  - todos los usuarios que han sido autenticado enAWS.
  - todos los usuarios con acceso a Internet
- Activar el registro para el bucket.
- Configurar una notificación utilizando Amazon Simple Notification Service (Amazon SNS), de modo que, si utiliza Almacenamiento de redundancia reducida (RRS), reciba una notificación en caso de que se produzca una pérdida de datos. RRS es una opción de almacenamiento de Amazon S3 que ofrece menos durabilidad que el almacenamiento estándar, pero con un costo inferior. Para obtener más información, consulte Preguntas frecuentes sobre Amazon Simple Storage Service (S3).
- Crear un sitio web estático usando los datos del bucket.

Auto Scaling

Permite configurar políticas de AWS Identity and Access Management (IAM) para un bucket. Para obtener más información, vaya a la documentación de IAM y a los casos de uso de IAM y S3.

Create Pre-Signed URL

Permite generar una URL de tiempo limitado que se puede distribuir para proporcionar acceso al contenido del bucket. Para obtener más información, consulte Cómo crear una URL prefirmada.

View Multi-Part Uploads

Permite ver las cargas multiparte. Amazon S3 es compatible con la división de las cargas de objetos de gran tamaño en partes para mejorar la eficiencia del proceso de carga. Para obtener más información, vaya a la explicación de las cargas multiparte en la documentación de S3.

Eliminar

Permite eliminar el bucket. Solo se pueden eliminar los buckets vacíos.

Carga de archivos y carpetas en Amazon S3

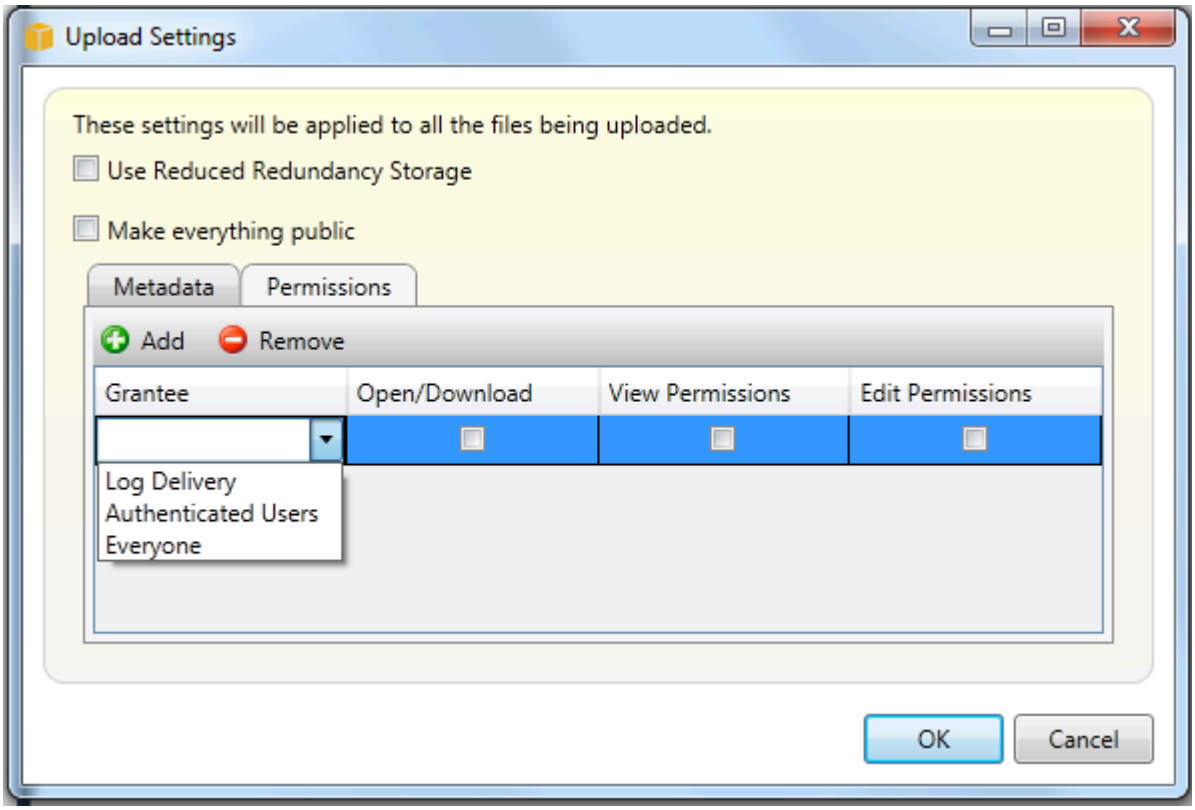
Puede usarAWSExplorador para transferir archivos o carpetas completas desde el equipo local a cualquiera de sus buckets.

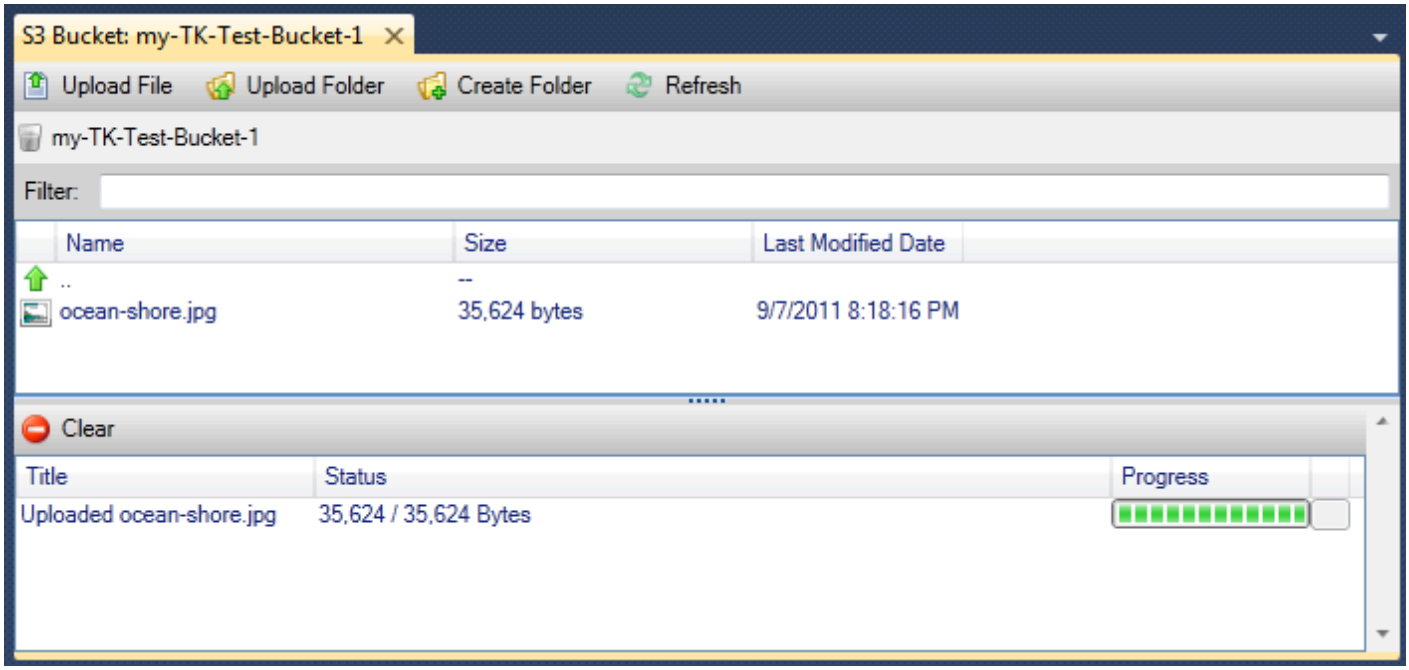
> **Note**
>
> Si carga archivos o carpetas que tienen el mismo nombre que los archivos o carpetas que ya existen en el bucket de Amazon S3, los archivos cargados sobrescribirán los archivos existentes sin advertencia.

Para cargar un archivo en S3

1. EnAWSExplorer, expanda laAmazon S3y haga doble clic en un bucket o abra el menú contextual (clic con el botón derecho) del bucket y elijaNavegar.
2. En la vista Browse (Explorar) del bucket, elija Upload File (Cargar archivo) o Upload Folder (Cargar carpeta).
3. En el cuadro de diálogo para abrir archivos, vaya hasta los archivos que desea cargar, selecciónelos y, a continuación, elija Open (Abrir). Si desea cargar una carpeta, vaya hasta ella, selecciónela y, a continuación, elija Open (Abrir).

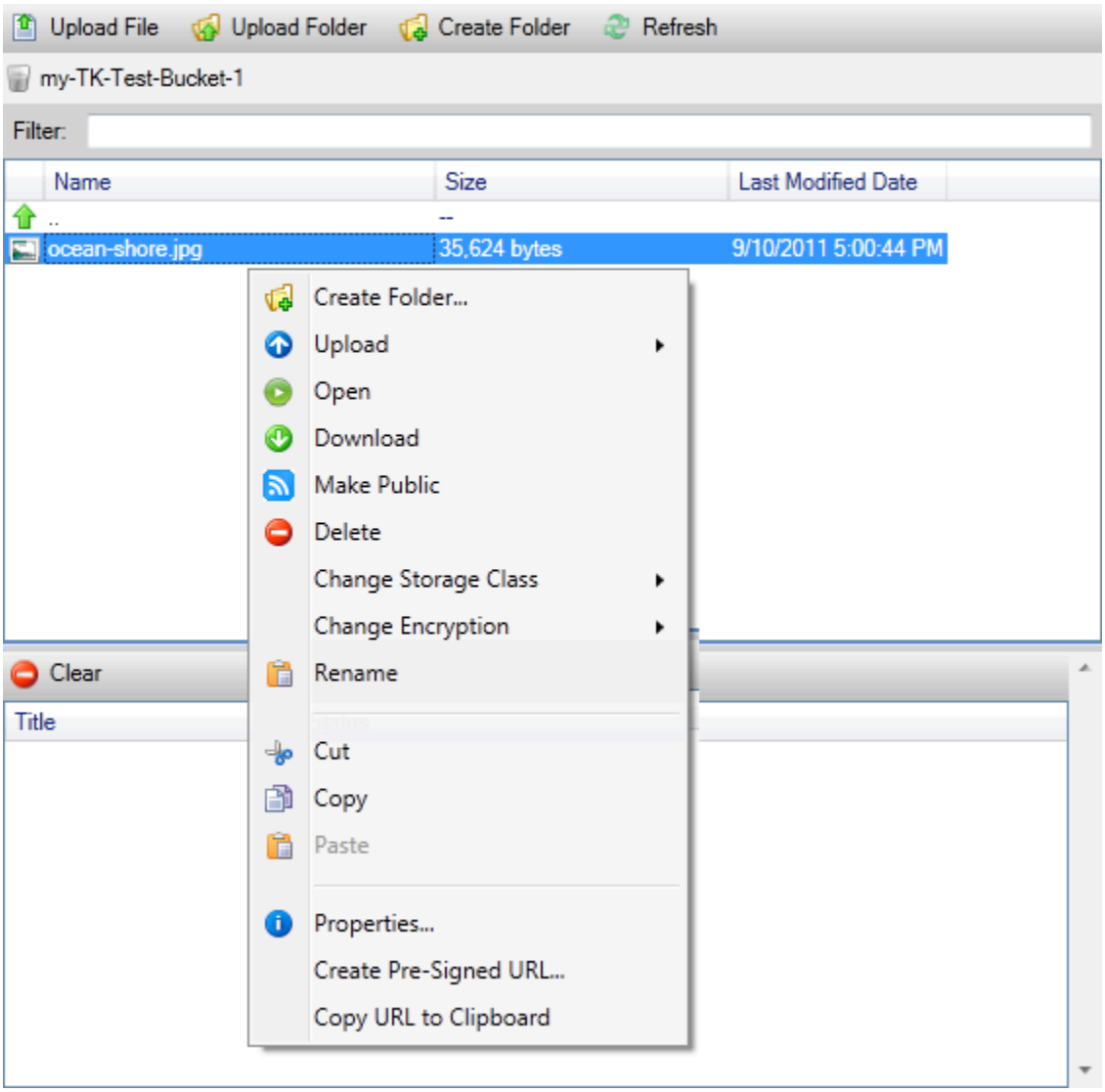
El cuadro de diálogo Upload Settings (Cargar configuración) le permite definir los metadatos y los permisos en los archivos o en la carpeta que desea cargar. Activar la casilla de verificación Make everything public (Publicar todo) equivale a configurar los permisos Open/Download (Abrir/Descargar) como Everyone (Todos). Puede seleccionar la opción para usar Reduced Redundancy Storage para los archivos cargados.





Operaciones de archivos de Amazon S3 desdeAWSToolkit for Visual Studio

Si elige un archivo en la vista de Amazon S3 y abre el menú contextual (clic con el botón derecho), puede realizar diversas operaciones en el archivo.



Create Folder

Permite crear una carpeta en el bucket actual. (Es equivalente a elegir el enlace Create Folder (Crear carpeta).

Cargar

Permite cargar archivos o carpetas. (Es equivalente a elegir los enlaces Upload File (Cargar archivo) o Upload Folder (Cargar carpeta)).

Open (Pendiente)

Intenta abrir el archivo seleccionado en el navegador predeterminado. En función del tipo de archivo y las capacidades de su navegador predeterminado, el archivo podría no mostrarse. Es posible que el navegador solo lo descargue.

Descargar

Abre un cuadro de diálogo de árbol de carpetas para permitirle descargar el archivo seleccionado.

Make Public

Establece los permisos del archivo seleccionado en Open/Download (Abrir/Descargar) y en Everyone (Todos). (Equivale a activar la casilla de verificación Make everything public (Publicar todo) en el cuadro de diálogo Upload Settings (Cargar configuración)).

Eliminar

Elimina los archivos o las carpetas que se han seleccionado. También puede eliminar archivos o carpetas eligiéndolos y pulsando `Delete`.

Change Storage Class

Establece la clase de almacenamiento en Standard o en Reduced Redundancy Storage (RRS). Para ver el ajuste de clase de almacenamiento actual, elija Properties (Propiedades).

Change Encryption

Permite establecer el cifrado del lado del servidor en el archivo. Para ver el ajuste de cifrado actual, elija Properties (Propiedades).

Cambio de nombre

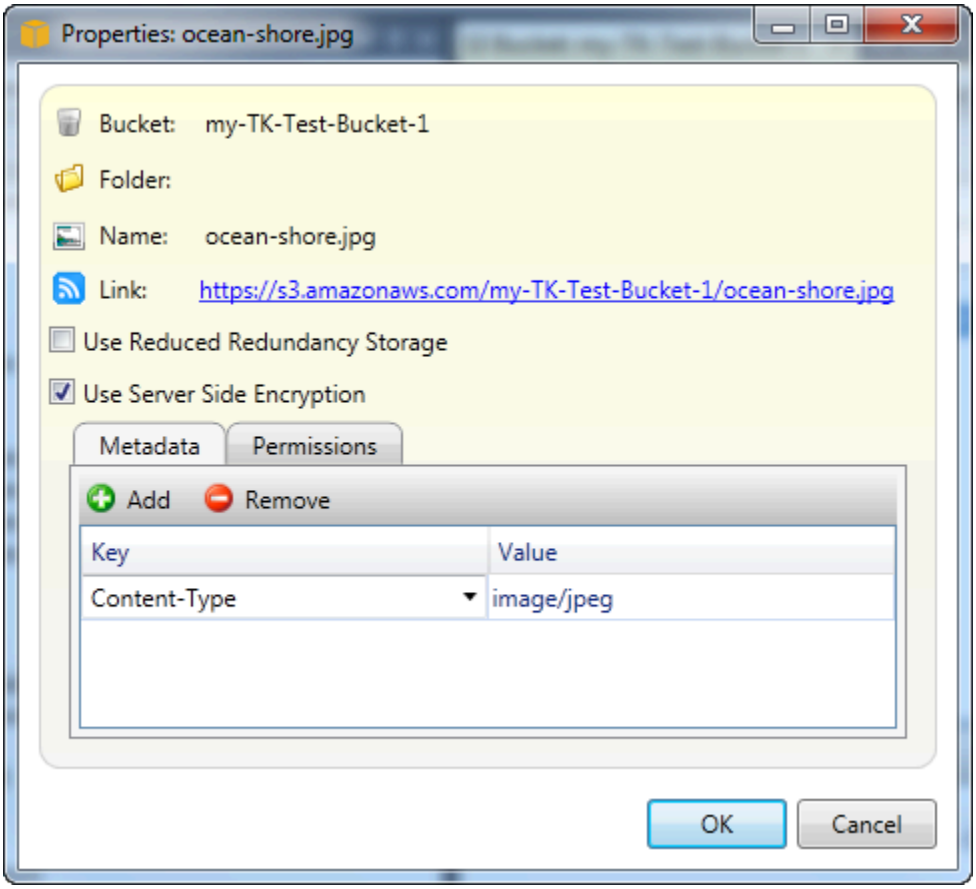
Permite cambiar el nombre de un archivo. No se puede cambiar el nombre de una carpeta.

Cut | Copy | Paste

Permite cortar, copiar y pegar archivos o carpetas entre carpetas o entre buckets.

Properties

Muestra un cuadro de diálogo que le permite definir los metadatos y los permisos para el archivo, así como cambiar el almacenamiento del archivo entre Reduced Redundancy Storage (RRS) y Standard y definir el cifrado del lado del servidor para el archivo. Este cuadro de diálogo también muestra un enlace https al archivo. Si elige este enlace, Toolkit for Visual Studio abre el archivo en el navegador predeterminado. Si tiene los permisos del archivo establecidos en Open/Download (Abrir/Descargar) y en Everyone (Todos), otras personas podrán obtener acceso al archivo a través de este enlace. En lugar de distribuir este enlace, le recomendamos que cree y distribuya direcciones URL prefirmadas.



Create Pre-Signed URL

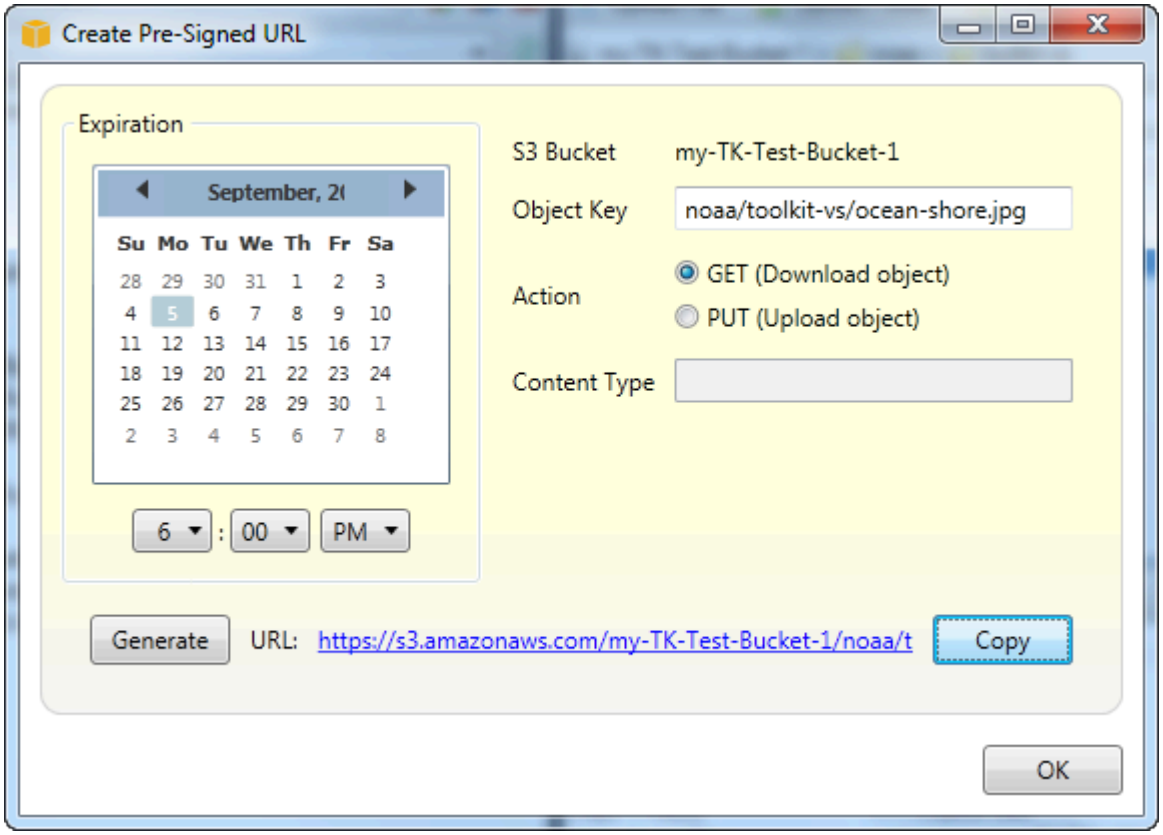
Permite crear una URL prefirmada de tiempo limitado que puede distribuir para permitir que otras personas tengan acceso al contenido que haya almacenado en Amazon S3.

Cómo crear una URL prefirmada

Puede crear una URL prefirmada para un bucket o para algunos archivos de un bucket. Otras personas pueden utilizar esta dirección URL para tener acceso al bucket o a los archivos. La dirección URL caducará después de un periodo de tiempo que se especifica al crear la URL.

Para crear una URL prefirmada

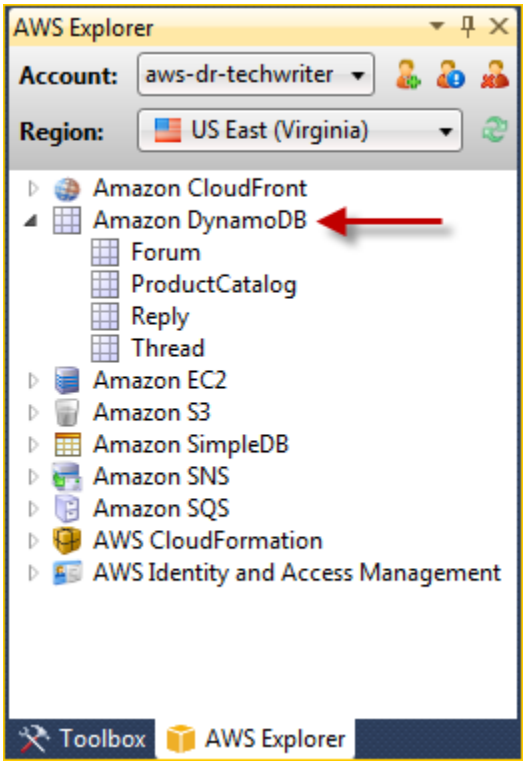
1. En el cuadro de diálogo Create Pre-Signed URL (Crear URL prefirmada), defina la fecha y la hora de vencimiento de la URL. El valor predeterminado es una hora después de la hora actual.
2. Elija el botón Generate (Generar).
3. Para copiar la URL en el portapapeles, elija Copy (Copiar).



Uso de DynamoDB desdeAWSExplorador

Amazon DynamoDB es un servicio de base de datos no relacional rentable y rápido, de alta disponibilidad y de alta escalabilidad. DynamoDB elimina las limitaciones tradicionales de escalabilidad del almacenamiento de datos y, al mismo tiempo, mantiene una baja latencia y un desempeño previsible. El Toolkit for Visual Studio proporciona funcionalidad para trabajar con DynamoDB en un contexto de desarrollo. Para obtener más información sobre DynamoDB, consulteDynamoDBen el sitio web de Amazon Web Services.

En el Toolkit for Visual Studio,AWSEl Explorador muestra todas las tablas de DynamoDB asociadas con el activoCuenta de AWS.



Creación de una tabla de DynamoDB

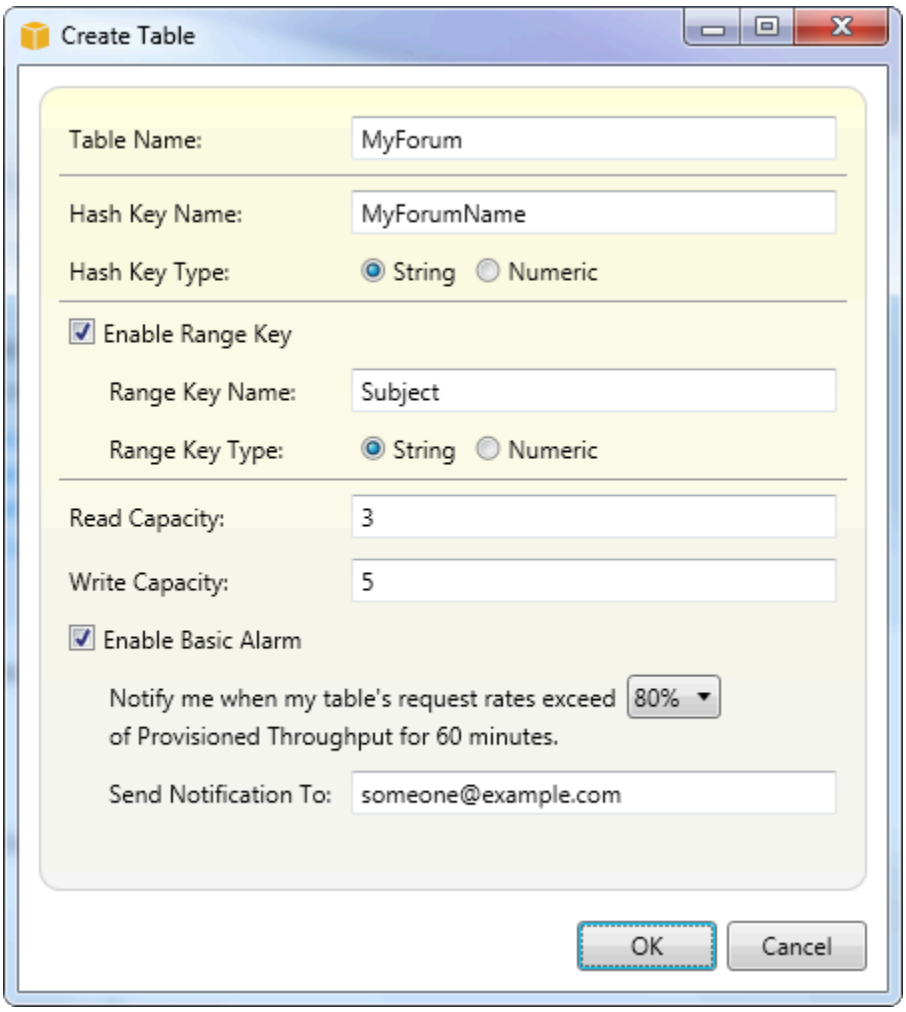
Puede utilizar Toolkit for Visual Studio para crear una tabla de DynamoDB.

Para crear una tabla de enAWSExplorador

1. EnAWSExplorador, abra el menú contextual (botón derecho del ratón) deAmazon DynamoDBy luego elijaCREATE TABLE.
2. En el asistente Create Table (Crear tabla), en Table Name (Nombre de la tabla), escriba un nombre para la tabla.
3. En el navegadorNombre de clave hash, escriba un atributo de clave hash principal y desde elTipo de clave hashbotones, elija el tipo de clave hash. DynamoDB crea un índice hash sin ordenar a partir del atributo de clave principal y un índice de rango ordenado opcional a partir del atributo de clave principal de rango. Para obtener más información sobre el atributo de clave hash principal, vaya aClave principalen laGuía para desarrolladores de Amazon DynamoDB.
4. (Opcional) Seleccione Enable Range Key (Habilitar clave de rango). En el campo Range Key Name (Nombre de clave de rango), escriba un atributo de clave de rango y, a continuación, elija un tipo de clave de rango con los botones Range Key Type (Tipo de clave de rango).
5. En el campo Read Capacity (Capacidad de lectura), escriba el número de unidades de capacidad de lectura. En el campo Write Capacity (Capacidad de escritura), escriba el número de unidades

de capacidad de escritura. Debe especificar un mínimo de tres unidades de capacidad de lectura y cinco unidades de capacidad de escritura. Para obtener más información acerca de las unidades de capacidad de lectura y escritura, consulte la sección sobre desempeño provisionado en DynamoDB.

6. (Opcional) Seleccione Enable Basic Alarm (Habilitar alarma básica) para recibir una alerta cuando las tasas de solicitud de la tabla sean demasiado altas. Elija el porcentaje de desempeño aprovisionado por 60 minutos que debe superarse antes de que se envíe la alerta. En Send Notifications To (Enviar notificaciones a), escriba una dirección de correo electrónico.
7. Haga clic en OK (Aceptar) para crear la tabla.

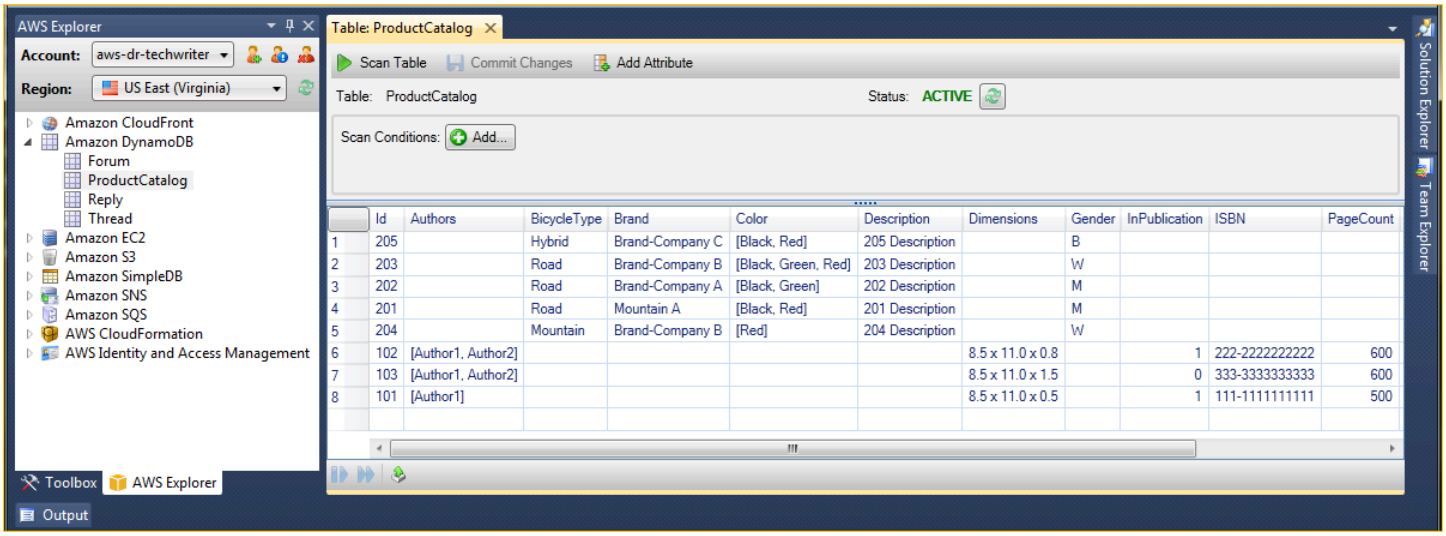


Para obtener más información sobre tablas de DynamoDB, visiteConceptos de modelos de datos: tablas, elementos y atributos.

Visualización de una tabla de DynamoDB como una cuadrícula

Para abrir una vista de cuadrícula de una de sus tablas de DynamoDB, enAWSExplorer, haga doble clic en el subnodo que corresponde a la tabla. En la vista de cuadrícula, puede ver los elementos, atributos y valores almacenados en la tabla. Cada fila corresponde a un elemento en la tabla. Las columnas de la tabla corresponden a los atributos. Cada celda de la tabla contiene los valores asociados con dicho atributo para dicho elemento.

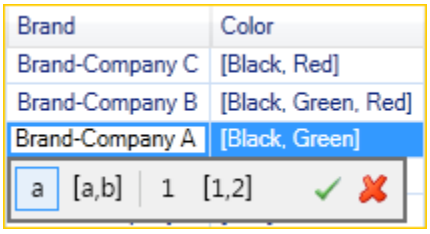
Un atributo puede tener un valor que es una cadena o un número. Algunos atributos tienen un valor que consta de un conjunto de cadenas o números. Los valores establecidos se muestran como una lista separada por comas delimitados entre corchetes.



	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

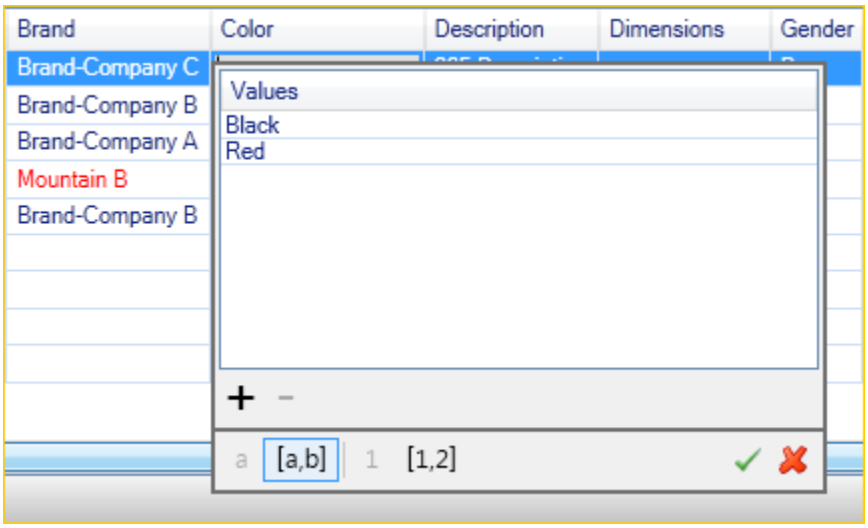
Edición y adición de atributos y valores

Haga doble clic en una celda para editar los valores del atributo correspondiente al elemento. Para atributos de valor de conjunto, también puede añadir o eliminar valores individuales desde el conjunto.



Además de cambiar el valor de un atributo, también puede, con algunas limitaciones, cambiar el formato del valor de un atributo. Por ejemplo, cualquier valor numérico puede convertirse en un valor de cadena. Si tiene un valor de cadena, cuyo contenido es un número, como, por ejemplo, 125, el

editor de celdas le permite convertir el formato de ese valor de cadena a número. También puede convertir un valor individual en un valor de conjunto. Sin embargo, por lo general, no es posible convertir un valor de conjunto en un valor individual, excepto si el valor de conjunto tiene, de hecho, un solo elemento en el conjunto.

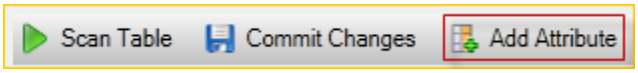


Después de editar el valor del atributo, elija la marca de verificación verde para confirmar los cambios. Si desea desechar los cambios, elija la X roja.

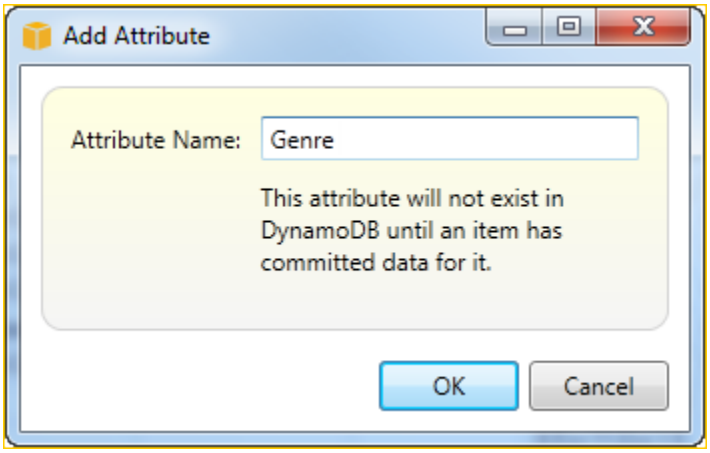
Una vez que confirme los cambios, el valor del atributo se mostrará en rojo. Esto indica que el atributo se ha actualizado, pero que el valor nuevo no se ha vuelto a escribir en la base de datos de DynamoDB. Para volver a escribir los cambios en DynamoDB, elijaConfirmar cambios. Para desechar los cambios, elija Scan Table (Escanear tabla) y cuando el Toolkit pregunte si desea confirmar los cambios antes del análisis, elija No.

Adición de un atributo

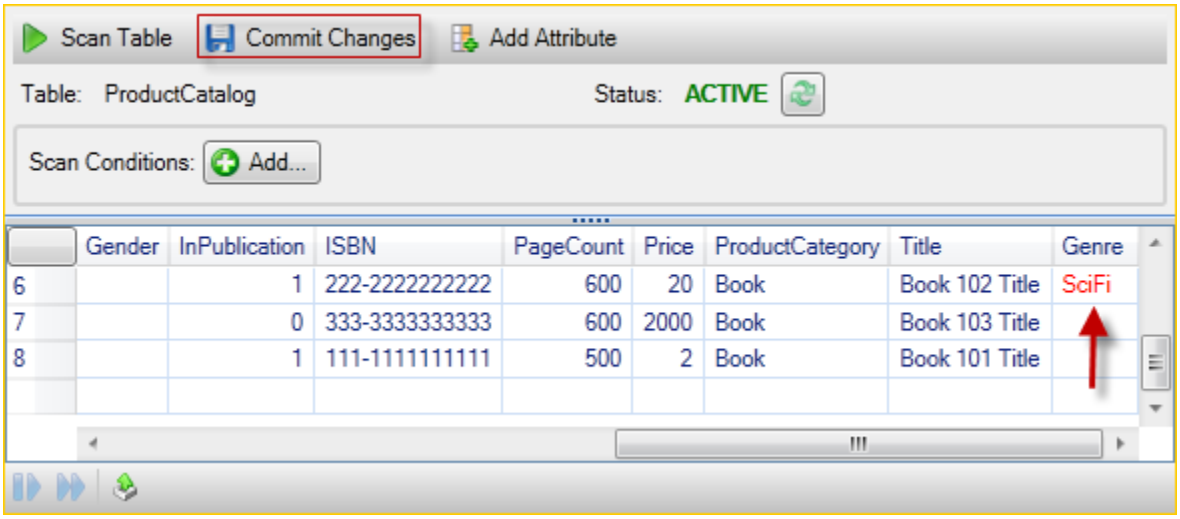
En la vista de cuadrícula, también puede añadir atributos a la tabla. Para añadir un atributo nuevo, elija Add Attribute (Añadir atributo).



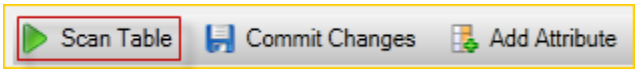
En el cuadro de diálogo Add Attribute (Añadir atributo), escriba un nombre para el atributo y, a continuación, elija OK (Aceptar).



Para que el atributo nuevo forme parte de la tabla, debe añadirle un valor para al menos un elemento y, a continuación, elegir el botón Commit Changes (Confirmar cambios). Para desechar el nuevo atributo, simplemente cierre la vista de cuadrícula de la tabla sin elegir Commit Changes (Confirmar cambios).



Análisis de una tabla de DynamoDB

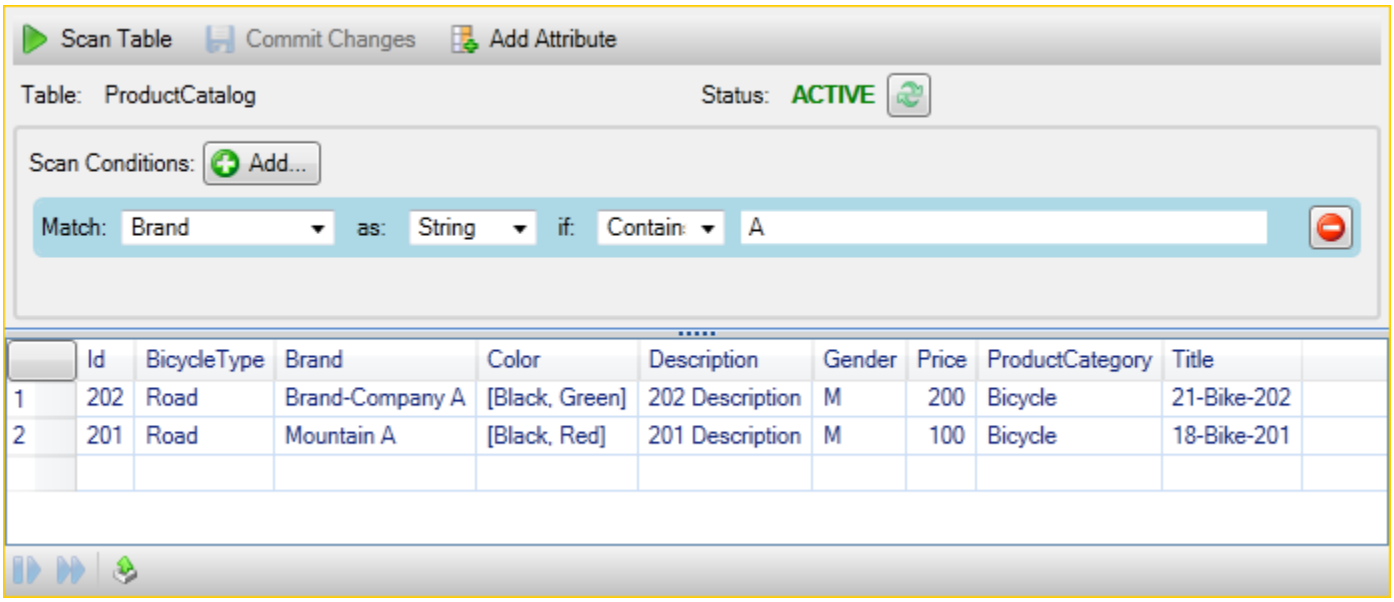


Puede realizar análisis en las tablas de DynamoDB desde el Toolkit. En un análisis, usted define un conjunto de criterios y el análisis devuelve todos los elementos de la tabla que cumplan sus criterios. Los análisis son operaciones caras y deben utilizarse con cuidado para evitar interrumpir el tráfico de producción de mayor prioridad en la tabla. Para obtener más información sobre el uso de la operación de análisis, vaya aGuía para desarrolladores de Amazon DynamoDB.

Para realizar un análisis en una tabla de DynamoDB desdeAWSExplorador

1. En la vista de cuadrícula, elija el botón scan conditions: add (condiciones de análisis: añadir).
2. En el editor de cláusula de análisis, elija el atributo para realizar la comparación, cómo debe interpretarse el valor del atributo (cadena, número, valor del conjunto), cómo debe asociarse (por ejemplo Begins With o Contains), y el valor literal con el que debe coincidir.
3. Añada más cláusulas de análisis, según sea necesario, para la búsqueda. El análisis devolverá únicamente aquellos elementos que coincidan con los criterios de todas sus cláusulas de análisis. El análisis hará una comparación que distingue entre mayúsculas y minúsculas al realizar la comparación con los valores de cadena.
4. En la barra de botones en la parte superior de la vista de cuadrícula, elija Scan Table (Analizar tabla).

Para eliminar una cláusula de análisis, elija el botón rojo con la línea blanca que se encuentra a la derecha de cada cláusula.



	Id	BicycleType	Brand	Color	Description	Gender	Price	ProductCategory	Title
1	202	Road	Brand-Company A	[Black, Green]	202 Description	M	200	Bicycle	21-Bike-202
2	201	Road	Mountain A	[Black, Red]	201 Description	M	100	Bicycle	18-Bike-201

Para volver a la vista de la tabla que incluye todos los elementos, elimine todas las cláusulas de análisis y, a continuación, elija Scan Table (Analizar tabla) de nuevo.

Paginación de los resultados del análisis

En la parte inferior de la vista hay tres botones.

Los dos primeros botones azules proporcionan paginación para los resultados del análisis. El primer botón mostrará una página adicional de resultados. El segundo botón mostrará diez páginas adicionales de resultados. En este contexto, una página es igual a 1 MB de contenido.

Exportación del resultado del análisis a CSV

El tercer botón exporta los resultados del análisis actual a un archivo CSV.

Uso deAWS CodeCommitcon Visual Studio Team Explorer

Puede usarAWS Identity and Access Management(IAM) para crear credenciales de Git y utilizarlas para crear y clonar repositorios desde Team Explorer.

Tipos de credenciales para AWS CodeCommit

MásAWS Toolkit for Visual Studiolos usuarios conocen la configuraciónAWSperfiles de credenciales que contienen sus claves de acceso y secretas. Estos perfiles de credenciales se usan en Toolkit for Visual Studio para habilitar las llamadas a las API del servicio, por ejemplo, para obtener una lista de los buckets de Amazon S3 enAWSExplorer o para lanzar una instancia de Amazon EC2. La integración de AWS CodeCommit con Team Explorer también utiliza estos perfiles de credenciales. Sin embargo, para trabajar con Git se necesitan más credenciales, en particular, las credenciales de Git para las conexiones HTTPS. Puede leer acerca de estas credenciales (un nombre de usuario y una contraseña) enConfiguración de usuarios HTTPS mediante credenciales de Giten laAWS CodeCommitGuía del usuario de.

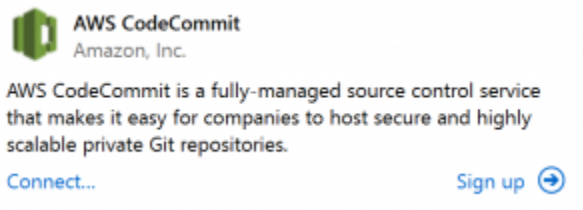
Puede crear las credenciales de Git paraAWS CodeCommitsolo para cuentas de usuario de IAM. No puede crearlas para una cuenta raíz. Puede crear hasta dos conjuntos de estas credenciales para el servicio y, aunque puede marcar un conjunto de credenciales como inactivo, los conjuntos inactivos siguen contando para el límite de dos conjuntos. Tenga en cuenta que puede eliminar y volver a crear credenciales en cualquier momento. Cuando se utilizaAWS CodeCommitdesde Visual Studio, su tradicionalAWSLas credenciales se utilizan para trabajar con el servicio, por ejemplo, cuando se crean y se enumeran repositorios. Al trabajar con los repositorios de Git alojados en AWS CodeCommit, se utilizan las credenciales de Git.

Como parte de la compatibilidad conAWS CodeCommit, Toolkit for Visual Studio crea y administra de forma automática estas credenciales de Git y las asocia con suAWSperfil de credenciales. No es necesario que se preocupe por tener a mano el conjunto correcto de credenciales para realizar operaciones de Git en Team Explorer. Una vez que te conectes a Team Explorer con tuAWSperfil de

credenciales, las credenciales de Git asociadas se utilizan automáticamente siempre que trabaje con un control remoto de Git.

Conexión a AWS CodeCommit

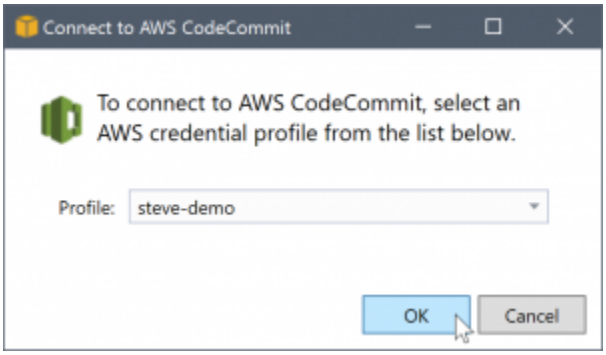
Al abrir la ventana de Team Explorer en Visual Studio 2015 o posterior, verá una entrada de AWS CodeCommit en la sección Hosted Service Providers de Manage Connections.



ElegirInscribirseabre la página principal de Amazon Web Services en una ventana del navegador. Qué ocurre cuando se eligeConectardepende de si Toolkit for Visual Studio puede encontrar un perfil de credenciales conAWSclaves de acceso y secretas para permitirle realizar llamadas aAWSen su nombre. Es posible que haya configurado un perfil de credenciales usando la nueva página Getting Started que se muestra en el IDE cuando el Toolkit for Visual Studio no puede encontrar credenciales almacenadas localmente. O puede haber estado utilizando Toolkit for Visual Studio, elAWS Tools for Windows PowerShell, o elAWS CLIy ya lo hanAWSperfiles de credenciales disponibles para utilizar Toolkit for Visual Studio.

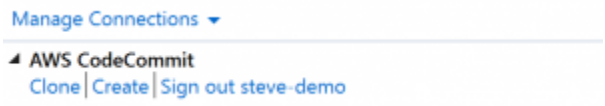
Cuando eligeConectar, Toolkit for Visual Studio inicia el proceso de búsqueda de un perfil de credenciales para usarlo en la conexión. Si Toolkit for Visual Studio no puede encontrar un perfil de credenciales, abre un cuadro de diálogo que le invita a escribir las claves de acceso y secretas de suCuenta de AWS. Es aconsejable utilizar una cuenta de usuario de IAM y no las credenciales raíz. Además, como ya se ha indicado, las credenciales de Git que pueden ser necesarias solo se pueden crear para los usuarios de IAM. Una vez que se proporcionen las claves de acceso y secretas y se cree el perfil de credenciales, la conexión entre Team Explorer y AWS CodeCommit estará lista para el uso.

Si Toolkit for Visual Studio encuentra más de unoAWSperfil de credenciales, se le pedirá que seleccione la cuenta que desea utilizar en Team Explorer.



Si tiene un único perfil de credenciales, Toolkit for Visual Studio omite el cuadro de diálogo de selección de perfil y la conexión se establece de inmediato:

Cuando se establece una conexión entre Team Explorer y AWS CodeCommit a través de los perfiles de credenciales, el cuadro de diálogo de invitación se cierra y se muestra el panel de conexión.

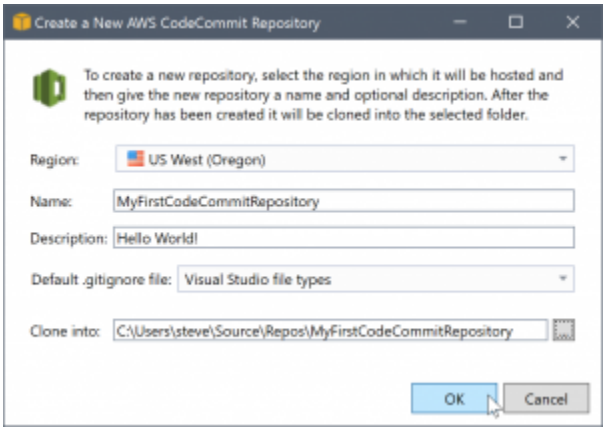


Dado que no hay repositorios clonados localmente, el panel solo muestra las operaciones que puede llevar a cabo: Clon,Crear, yCierre de sesión. Al igual que otros proveedores,AWS CodeCommiten Team Explorer se puede vincular a un soloAWSperfil de credenciales en un momento dado. Si desea cambiar de cuenta, utilice Sign out (Cerrar sesión) para eliminar la conexión con el fin de poder comenzar una nueva conexión con una cuenta diferente.

Ahora que ha establecido una conexión, puede crear un repositorio haciendo clic en el enlace Create (Crear).

Crear un repositorio

Al hacer clic en elCrearlink, elCrear un nuevoAWS CodeCommitRepositorioSe abre el cuadro de diálogo.



Los repositorios de AWS CodeCommit están organizados por región, por lo que en Region (Región) puede seleccionar la región en la que se debe alojar el repositorio. La lista tiene todas las regiones en las que se admite AWS CodeCommit. Debe proporcionar el nombre (obligatorio) y la descripción (opcional) del nuevo repositorio.

El comportamiento predeterminado del cuadro de diálogo es añadir el nombre del repositorio como sufijo a la ubicación de carpeta del nuevo repositorio (la ubicación de la carpeta se actualiza a medida que se escribe el nombre). Para utilizar un nombre de carpeta diferente, edite la ruta de carpeta Clone into (Clonar en) cuando haya terminado de escribir el nombre del repositorio.

También puede optar por crear automáticamente un archivo `.gitignore` inicial para el repositorio. AWS Toolkit for Visual Studio proporciona un valor predeterminado integrado para los tipos de archivos de Visual Studio. También puede optar por no usar ningún archivo o por usar un archivo personalizado ya existente que desee reutilizar en varios repositorios. Solo tiene que seleccionar Use custom (Usar personalizado) en la lista e ir hasta el archivo personalizado que desea usar.

Una vez que tenga el nombre y la ubicación de un repositorio, estará preparado para hacer clic en OK (Aceptar) y comenzar a crear el repositorio. Toolkit for Visual Studio pide al servicio que cree el repositorio y, a continuación, clone el nuevo repositorio localmente, añadiendo una confirmación inicial al archivo .gitignore si se está utilizando uno. Este es el momento en el que se comienza a trabajar con el repositorio remoto de Git, por lo que ahora Toolkit for Visual Studio necesita obtener acceso a las credenciales de Git que se han descrito anteriormente.

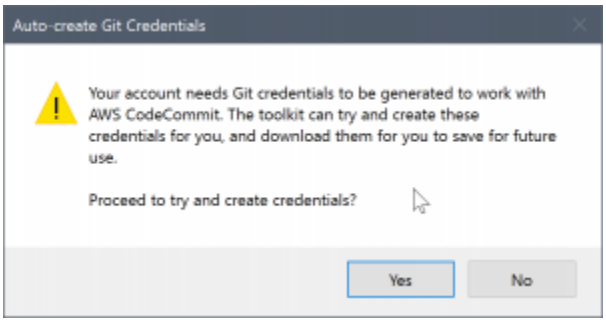
Configuración de las credenciales de Git

Hasta este punto has estado usandoAWSclaves de acceso y secretas para solicitar que el servicio cree su repositorio. Ahora tiene que trabajar con Git para realizar la operación clonación, y Git no entiendeAWSclaves de acceso y secretas. En su lugar, debe proporcionar las credenciales de

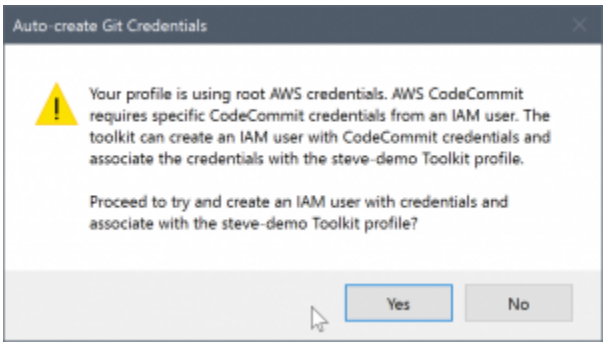
nombre de usuario y contraseña que Git debe usar en una conexión HTTPS con el repositorio remoto.

Como se indica en Configuración de las credenciales de Git, las credenciales de Git que va a utilizar deben estar asociadas a un usuario de IAM. No puede generarlas para las credenciales raíz. Siempre debe configurar suAWSperfiles de credenciales para contener claves de acceso y secretas de los usuarios de IAM y no claves raíz. Toolkit for Visual Studio puede intentar configurar las credenciales de Git paraAWS CodeCommitpara ti, y asociarlos con elAWSperfil de credenciales que utilizaste para conectar en Team Explorer anteriormente.

Cuando eligeDE ACUERDOen laCrear un nuevoAWS CodeCommitRepositorioy cree correctamente el repositorio, el Toolkit for Visual Studio comprueba elAWSperfil de credenciales que está conectado en Team Explorer para determinar si las credenciales de Git paraAWS CodeCommitexisten y se asocian localmente al perfil. En caso afirmativo, Toolkit for Visual Studio indica a Team Explorer instrucciones para comenzar la operación de clonación en el nuevo repositorio. Si no hay credenciales de Git disponibles localmente, Toolkit for Visual Studio comprueba el tipo de credenciales de la cuenta que se han utilizado en la conexión en Team Explorer. Si las credenciales son para un usuario de IAM, tal y como se recomienda, se muestra el siguiente mensaje.



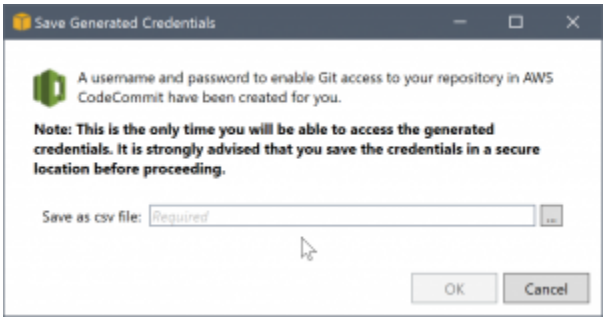
Si las credenciales son credenciales raíz, se muestra en su lugar el siguiente mensaje.



En ambos casos, Toolkit for Visual Studio ofrece intentar hacer el trabajo para crear las credenciales de Git necesarias. En el primer caso, lo único que tiene que crear es un conjunto de credenciales de Git para el usuario de IAM. Cuando se está usando una cuenta raíz, Toolkit for Visual Studio

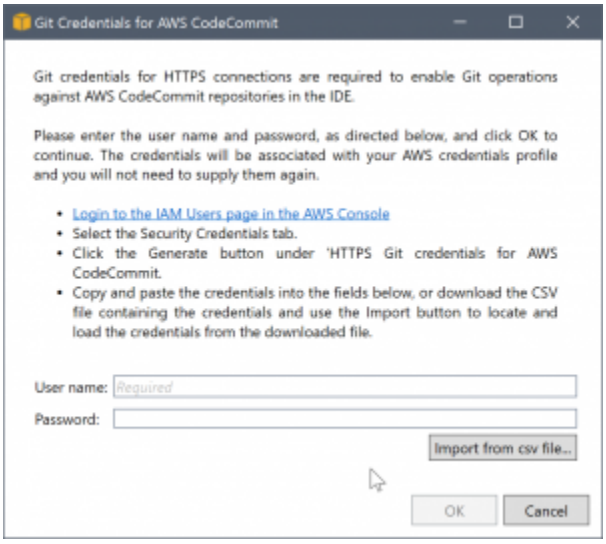
intenta primero crear un usuario de IAM y, a continuación, crea nuevas credenciales de Git para ese nuevo usuario. Si el Toolkit for Visual Studio tiene que crear un nuevo usuario, aplica elAWS CodeCommitPolítica administrada por usuarios avanzados en esa nueva cuenta de usuario. Esta política permite el acceso únicamente a AWS CodeCommit y permite que todas las operaciones se realicen con AWS CodeCommit, excepto la eliminación del repositorio.

Durante el proceso de creación de las credenciales, solo puede verlas una vez. Por ello, Toolkit for Visual Studio le pide que guarde las credenciales que se acaban de crear como `.csv`archivo antes de continuar.



Es muy recomendable hacerlo y es importante guardarlas en una ubicación segura.

Puede haber casos en los que Toolkit for Visual Studio no pueda crear credenciales automáticamente. Por ejemplo, es posible que ya haya creado el número máximo de conjuntos de credenciales de Git paraAWS CodeCommit(dos) o que no tenga los derechos de programación requeridos para que Toolkit for Visual Studio haga el trabajo por usted (si está registrado como un usuario de IAM). En estos casos, puede iniciar sesión enAWS Management ConsolePara administrar las credenciales u obtenerlas de su administrador. A continuación puede introducirlos en elCredenciales de Git paraAWS CodeCommitCuadro de diálogo, que muestra Toolkit for Visual Studio.

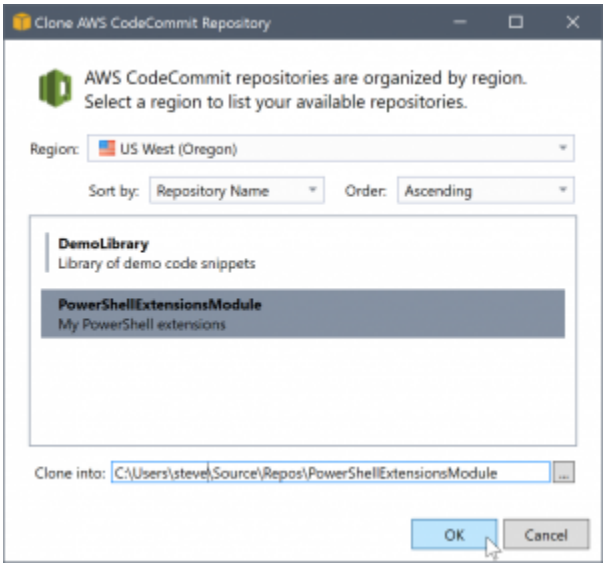


Ahora que las credenciales de Git están disponibles, la operación de clonación para el nuevo repositorio continúa (vea la indicación de progreso de la operación en Team Explorer). Si ha optado por aplicar un archivo `.gitignore` predeterminado, se confirma en el repositorio con el comentario "Initial Commit".

Estos son todos los pasos necesarios para configurar las credenciales y crear un repositorio en Team Explorer. Una vez que se tienen las credenciales necesarias, lo único que el usuario verá cuando cree nuevos repositorios en el futuro es elCrear un nuevoAWS CodeCommitRepositoriocuadro de diálogo en sí.

Clonación de un repositorio

Para clonar un repositorio, vuelva al panel de conexión de AWS CodeCommit en Team Explorer. Haga clic en el botón .Clonenlace para abrir elClonAWS CodeCommitRepositorioy, a continuación, seleccione el repositorio que desea clonar y la ubicación en el disco en la que desea guardarlo.



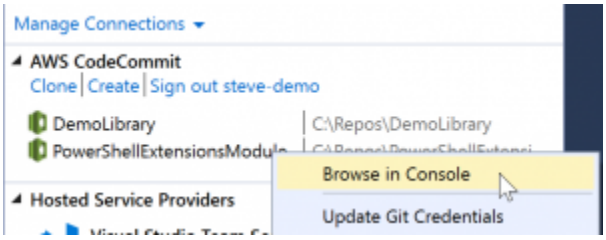
Una vez que elija la región, Toolkit for Visual Studio consultará el servicio para descubrir los repositorios que están disponibles en esa región y los mostrará en la parte de lista central del cuadro de diálogo. El nombre y la descripción opcional de cada repositorio también se muestran. Puede reordenar la lista para ordenarla por el nombre del repositorio o por la fecha de la última modificación, y ordenarla de forma ascendente o descendente.

Tras seleccionar el repositorio, puede elegir la ubicación en la que desea clonarlo. De manera predeterminada, es la misma ubicación del repositorio utilizada en otros complementos de Team Explorer, pero puede escribir cualquier otra ubicación o ir hasta ella. De forma predeterminada, el nombre del repositorio se añade como sufijo a la ruta seleccionada. Sin embargo, si desea una ruta concreta, solo tiene que editar el cuadro de texto después de seleccionar la carpeta. El texto que aparezca en el cuadro de texto al hacer clic en OK (Aceptar) será la carpeta en la que encontrará el repositorio clonado.

Después de seleccionar el repositorio y una ubicación de carpeta, haga clic en OK (Aceptar) para continuar con la operación de clonación. Como sucedía al crear un repositorio, puede ver el progreso de la operación de clonación en Team Explorer.

Trabajar con repositorios

Al clonar o crear repositorios, recuerde que los repositorios locales para la conexión se muestran en la lista del panel de conexión en Team Explorer bajo los enlaces de la operación. Estas entradas le ofrecen una forma cómoda para obtener acceso al repositorio y examinar el contenido. Solo tiene que hacer clic con el botón derecho en el repositorio y elegir Browse in Console (Explorar en la consola).



También puede utilizar Update Git Credentials (Actualizar credenciales de Git) para actualizar las credenciales de Git almacenadas asociadas con el perfil de credenciales. Esto resulta útil si ha rotado las credenciales. El comando abre elCredenciales de Git paraAWS CodeCommitCuadro de diálogo en el que puede escribir o importar las nuevas credenciales.

Las operaciones de Git en los repositorios funcionan del modo esperado. Puede confirmar localmente y, cuando esté preparado para compartir, usará la opción de sincronización de Team Explorer. Porque las credenciales de Git ya están almacenadas localmente y están asociadas a nuestra conexiónAWSPerfil de credenciales, no se pedirá que se suministren de nuevo para las operaciones realizadas enAWS CodeCommitremoto.

Uso de CodeArtifact en Visual Studio

AWS CodeArtifactes un servicio de repositorio de artefactos totalmente administrado que permite a las organizaciones almacenar y compartir de forma segura paquetes de software utilizados para el desarrollo de aplicaciones. Puede utilizar CodeArtifact con herramientas de compilación y gestores de paquetes populares, como las CLI NuGet y .NET Core y Visual Studio. También puede configurar CodeArtifact para extraer paquetes de un repositorio público externo, comoNuget.org.

En CodeArtifact, los paquetes se almacenan en repositorios que luego se almacenan dentro de un dominio. LaAWS Toolkit for Visual Studiosimplifica la configuración de Visual Studio con sus repositorios CodeArtifact, lo que facilita el consumo de paquetes en Visual Studio desde CodeArtifact directamente y Nuget.org.

Agregue su repositorio CodeArtifact como fuente de paquetes NuGet

Para consumir paquetes de su CodeArtifact, deberá agregar su repositorio como fuente de paquetes en elAdministrador de paquetes NuGeten Visual Studio

Para añadir el repositorio como origen de paquetes

1. EnAWSExplorer, navegue hasta su repositorio enAWS CodeArtifactNodo.

2. Abra el menú contextual (clic secundario) para el repositorio que desea agregar y seleccionePunto de enlace de origen NuGet Copia.
3. Vaya aFuentes de paquetesdebajo de laAdministrador de paquetes NuGetNodo enHerramientas > Opcionesmenú.
4. EnFuentes de paquetes, seleccione el signo más (+), edite el nombre y pegue la URL del endpoint de origen NuGet que copió anteriormente en elFuente.
5. Seleccione la casilla de verificación situada junto a la fuente de paquetes recién agregada para habilitarlo.

> **Note**
>
> Recomendamos añadir una conexión externa aNuget.orga su CodeArtifact y deshabilitando elnuget.orgorigen de paquetes en Visual Studio. Cuando se utiliza una conexión externa, todas las dependencias se extraen deNuget.orgse almacenan en CodeArtifact. SiNuget.orgdesaparece por cualquier motivo, los paquetes que necesita seguirán estando disponibles. Para obtener más información acerca de las conexiones externas, consulteAgregar una conexión externaen laAWS CodeArtifactGuía del usuario de.

6. ElegirDE ACUERDOpara cerrar el menú.

Para obtener más información sobre el uso de CodeArtifact con Visual Studio, consulteUso de CodeArtifact con Visual Studioen laAWS CodeArtifactGuía del usuario de.

Amazon RDS deAWSExplorador

Amazon Relational Database Service (Amazon RDS) es un servicio que le permite aprovisionar y administrar sistemas de bases de datos relacionales SQL en la nube. Amazon RDS admite tres tipos de sistemas de bases de datos:

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

Para obtener más información, consulte la Amazon RDS User Guide.

Muchas de las funcionalidades que se tratan aquí también están disponible a través de laAWSConsola de administración depara Amazon RDS.

Temas

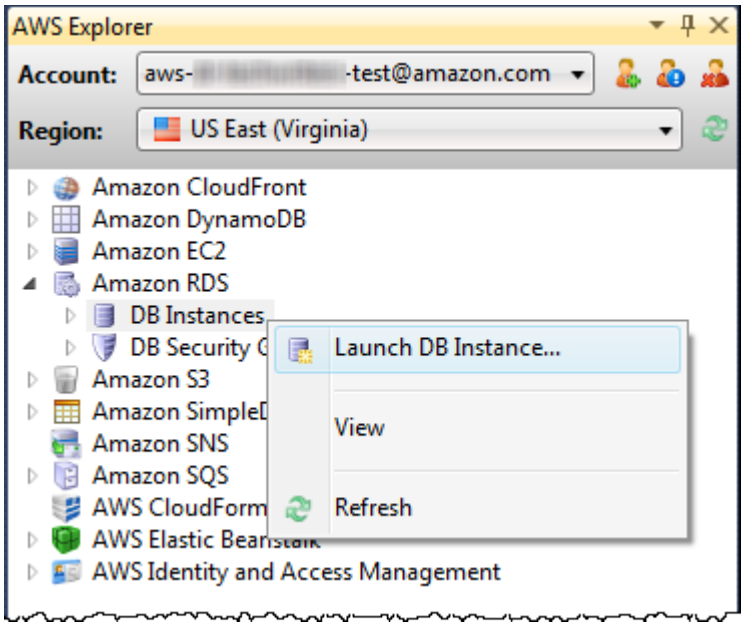
- Lanzar una instancia de base de datos de Amazon RDS
- Cree una base de datos de Microsoft SQL Server en una instancia de RDS
- Grupos de seguridad de Amazon RDS

Lanzar una instancia de base de datos de Amazon RDS

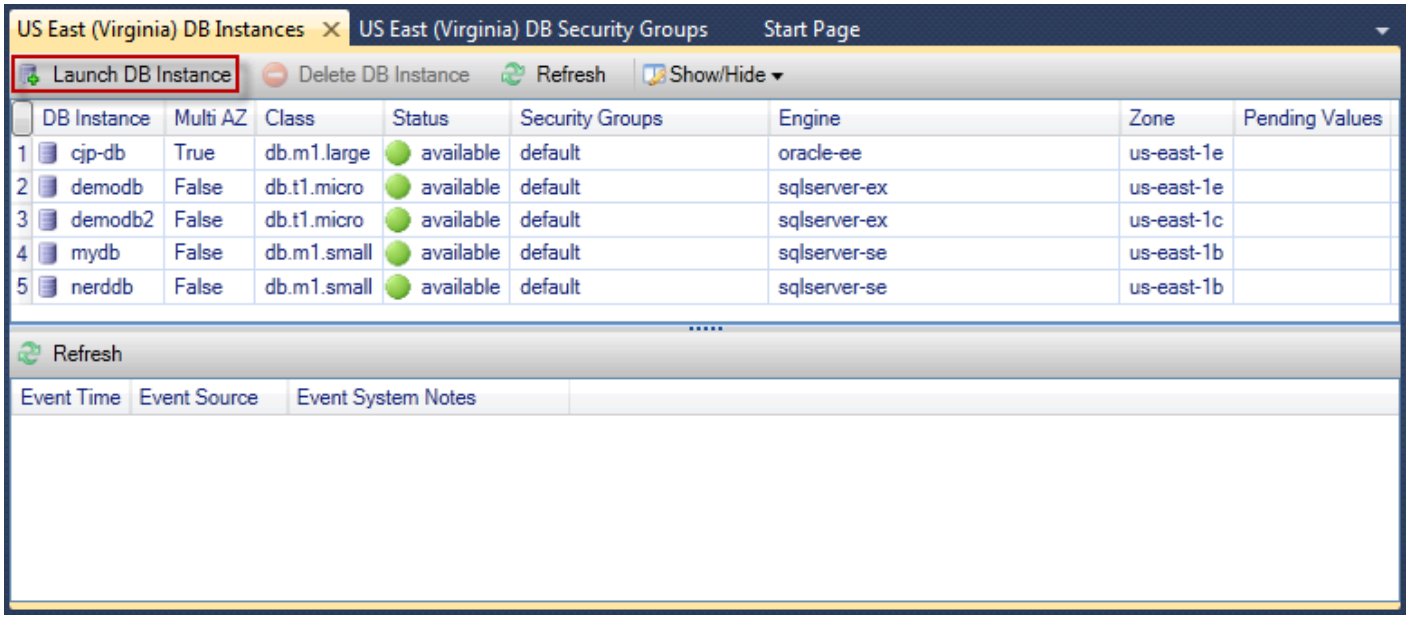
conAWSExplorador, puede lanzar una instancia de cualquiera de los motores de base de datos compatibles con Amazon RDS. En el siguiente tutorial se muestra la experiencia del usuario al lanzar una instancia de Microsoft SQL Server Standard Edition, pero la experiencia del usuario es similar para todos los motores compatibles.

Para lanzar una instancia de Amazon RDS

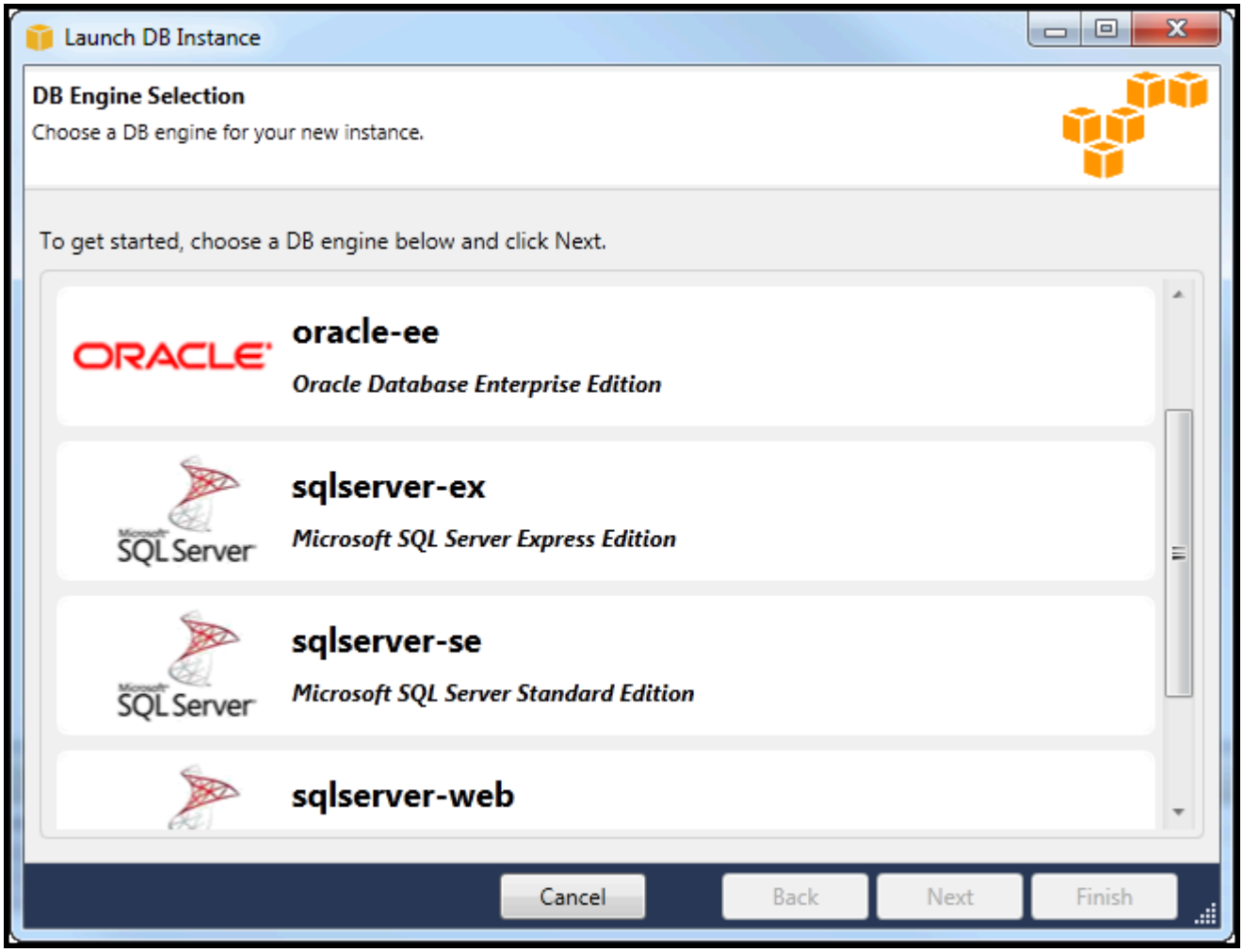
1. EnAWSExplorador, abra el menú contextual (con el botón derecho del ratón) delAmazon RDSnodo y eligeLaunch DB Instance.



   De forma alternativa, en la pestaña DB Instances (Instancias de base de datos), elija Launch DB Instance (Lanzar instancia de base de datos).



2. En el cuadro de diálogo DB Engine Selection (Selección de motor de base de datos), elija el tipo de motor de base de datos que se lanzará. Para este tutorial, elija Microsoft SQL Server Standard Edition (sqlserver-se) y, a continuación, elija Next (Siguiente).



3. En el cuadro de diálogo DB Engine Instance Options (Opciones de instancias del motor de base de datos), elija las opciones de configuración.

   En la sección DB Engine Instance Options and Class (Opciones de instancias del motor de base de datos y clase), puede especificar los siguientes ajustes.

   License Model

Tipo de motor	Licencia
Microsoft SQL Server	licencia incluida
MySql	licencia pública general
Oracle	Bring-Your-Own-License

El modelo de licencia varía en función del tipo de motor de base de datos. Tipo de motor Licencia Microsoft SQL Server licencia incluida MySql licencia pública general Oracle Bring-Your-Own-License

Versión de instancia de base de datos

Elija la versión del motor de base de datos que le gustaría utilizar. Si solo se admite una versión, se selecciona de forma predeterminada.

DB Instance Class

Elija la clase de instancia para el motor de base de datos. Los precios para las clases de instancia varían. Para obtener más información, consulte Precios de Amazon RDS.

Realice un despliegue Multi-AZ

Seleccione esta opción para crear un despliegue Multi-AZ para mejorar la disponibilidad y durabilidad de los datos. Amazon RDS aprovisiona y mantiene una copia en espera de su base de datos en una zona de disponibilidad diferente para la conmutación por error automática en caso de que se produzcan interrupciones inesperadas o programadas. Para obtener información sobre los precios de despliegues Multi-AZ, consulte la sección de precios de la página de detalles Amazon RDS. Esta opción no es compatible con Microsoft SQL Server.

Actualice versiones secundarias automáticamente

Seleccione esta opción para tenerAWSrealice actualizaciones de versión secundaria automáticamente en sus instancias de RDS.

En la sección RDS Database Instance (Instancia de base de datos de RDS), puede especificar los siguientes ajustes.

Allocated Storage (Almacenamiento asignado)

Motor	Mínimo (GB)	Máximo (GB)
MySQL	5	1024
Oracle Enterprise Edition	10	1024

Motor	Mínimo (GB)	Máximo (GB)
Microsoft SQL Server Express Edition	30	1024
Microsoft SQL Server Standard Edition	250	1024
Microsoft SQL Server Web Edition	30	1024

Los mínimos y máximos para el almacenamiento asignado dependerán del tipo de motor de base de datos. Motor Mínimo (GB) Máximo (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

Especifique un nombre para la instancia de base de datos. Este nombre no distingue entre mayúsculas y minúsculas. Se muestran en minúsculas enAWSExplorador.

Master User Name (Nombre de usuario maestro)

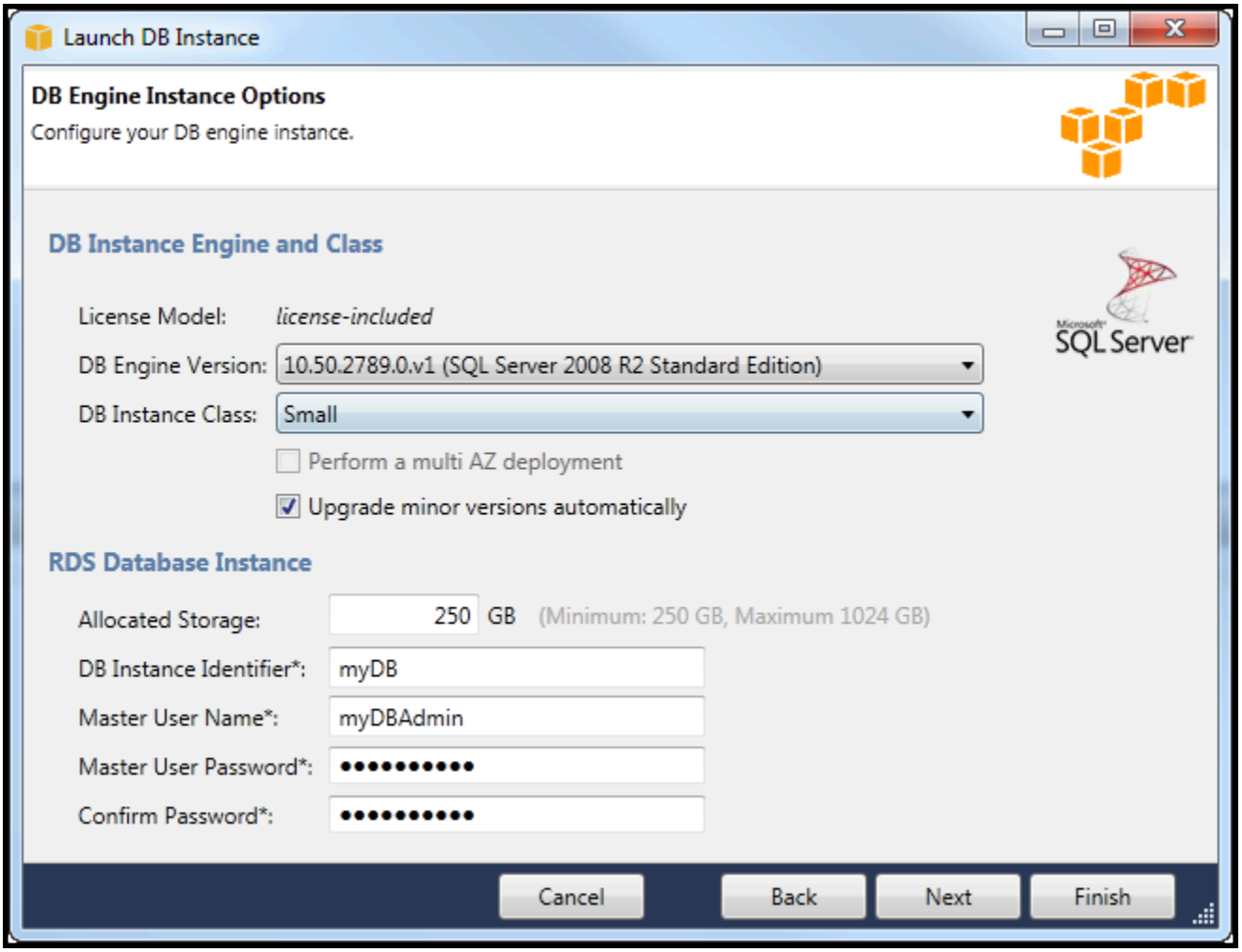
Escriba un nombre para el administrador de la instancia de base de datos.

Master User Password

Escriba una contraseña para el administrador de la instancia de base de datos.

Confirmar contraseña

Escriba la contraseña de nuevo para verificar que es correcta.



1. En el cuadro de diálogo Additional Options (Opciones adicionales), puede especificar los siguientes ajustes.

   Database Port (Puerto de base de datos)

   Este es el puerto TCP que utilizará la instancia para comunicarse en la red. Si su equipo obtiene acceso a Internet a través de un firewall, establece este valor en un puerto a través del cual el firewall permite el tráfico.

   Zona de disponibilidad

   Utilice esta opción si desea que la instancia se lance en una zona de disponibilidad concreta en su región. La instancia de base de datos que ha especificado podría no estar disponible en todas las zonas de disponibilidad en una región determinada.

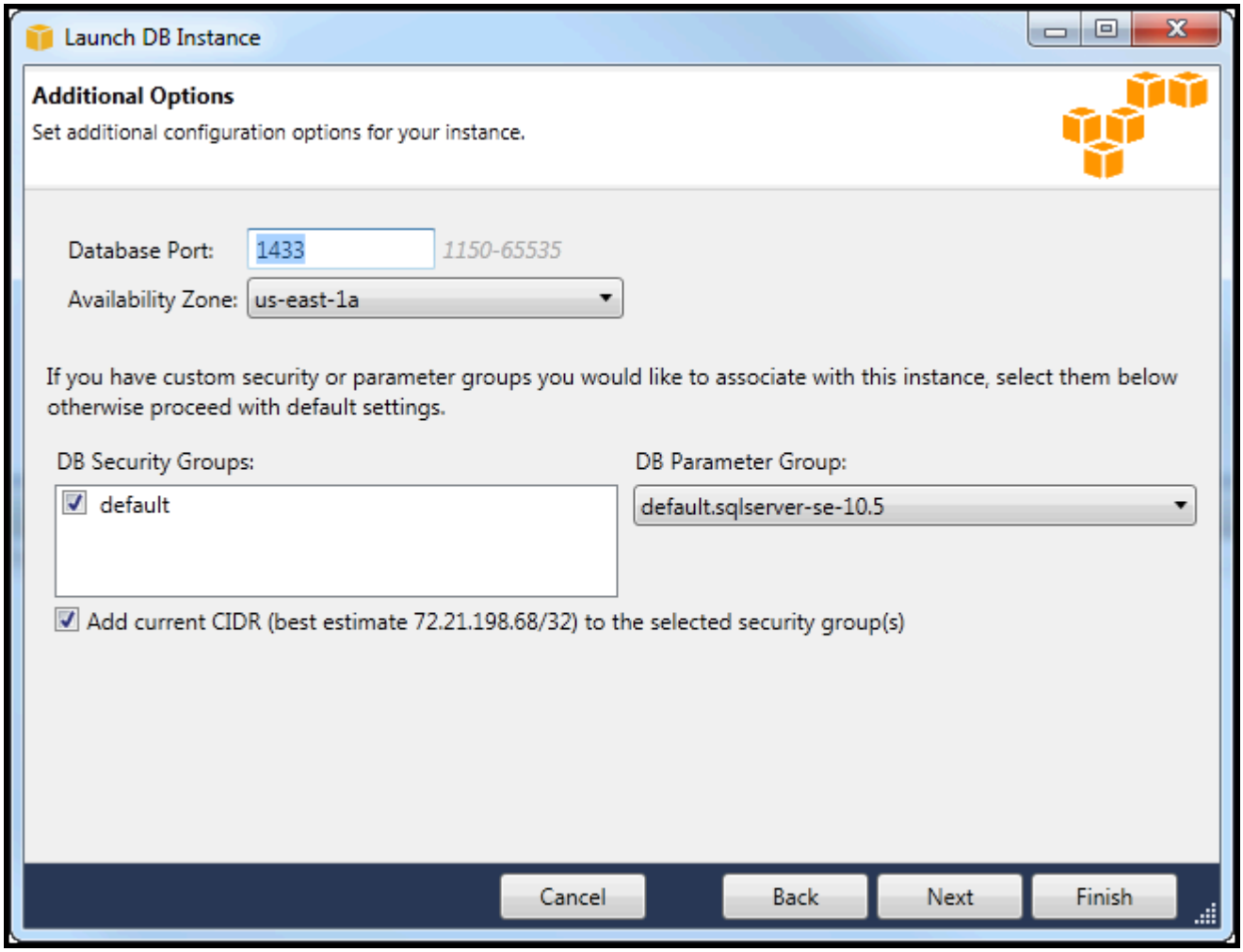
Grupo de seguridad de RDS

Seleccione un grupo de seguridad de RDS (o grupos) para asociar con su instancia. Los grupos de seguridad de RDS especifican la dirección IP, las instancias de Amazon EC2 yCuentas de AWSque tienen permiso para acceder a la instancia. Para obtener más información sobre los grupos de seguridad de RDS, consulte Grupos de seguridad de Amazon RDS. El Toolkit for Visual Studio intenta determinar su actual dirección IP y ofrece la opción de añadir esta dirección a los grupos de seguridad asociados a la instancia. Sin embargo, si el equipo obtiene acceso a Internet a través de un firewall, la dirección IP que el Toolkit genera para su equipo podría no ser precisa. Para determinar qué dirección IP utilizar, consulte al administrador del sistema.

DB Parameter Group (Grupo de parámetros de base de datos)

(Opcional) En este menú desplegable, elija un grupo de parámetros de base de datos para asociar con la instancia. Grupos de parámetros de bases de datos le permite cambiar la configuración predeterminada para la instancia. Para obtener más información, consulte la Guía del usuario de Amazon Relational Database Service y este artículo.

Cuando haya especificado los ajustes en este cuadro de diálogo, seleccione Next (Siguiente).

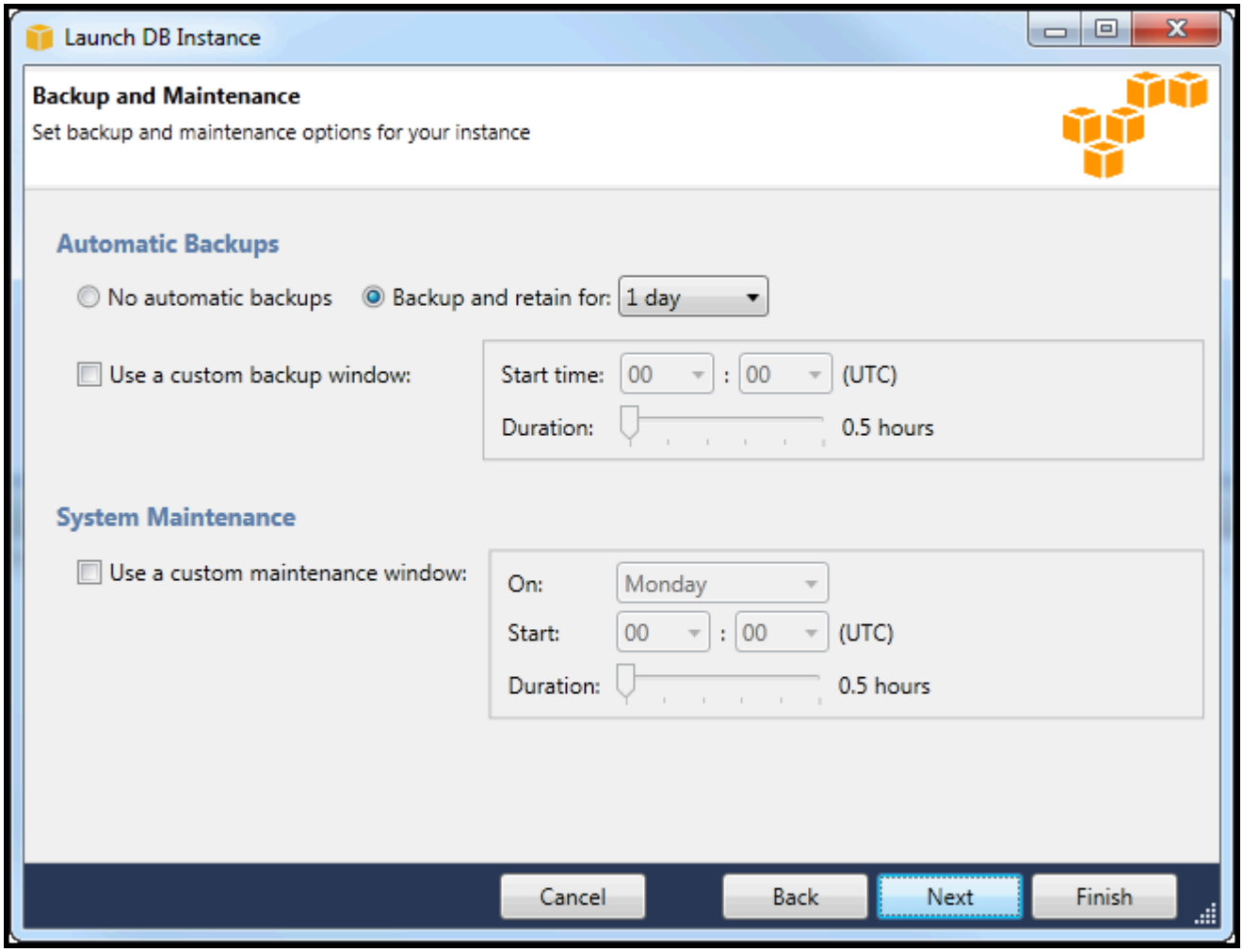


2. LaBackup y mantenimientoEl cuadro de diálogo le permite especificar si Amazon RDS debe realizar una copia de seguridad de la instancia y, en caso afirmativo, durante cuánto tiempo conservar la copia de seguridad. También puede especificar un periodo de tiempo durante el que deben realizarse las copias de seguridad.

   Este cuadro de diálogo también le permite especificar si desea que Amazon RDS realice el mantenimiento del sistema en su instancia. El mantenimiento incluye parches rutinarios y actualizaciones secundarias de la versión.

   El periodo de tiempo especificado para el mantenimiento del sistema no puede solaparse con el periodo especificado para las copias de seguridad.

   Elija Next (Siguiente).



3. El cuadro de diálogo final en el asistente le permite revisar los ajustes de la instancia. Si necesita modificar los ajustes, utilice el botón Back (Atrás). Si todos los ajustes son correctos, elija Launch (Lanzar).

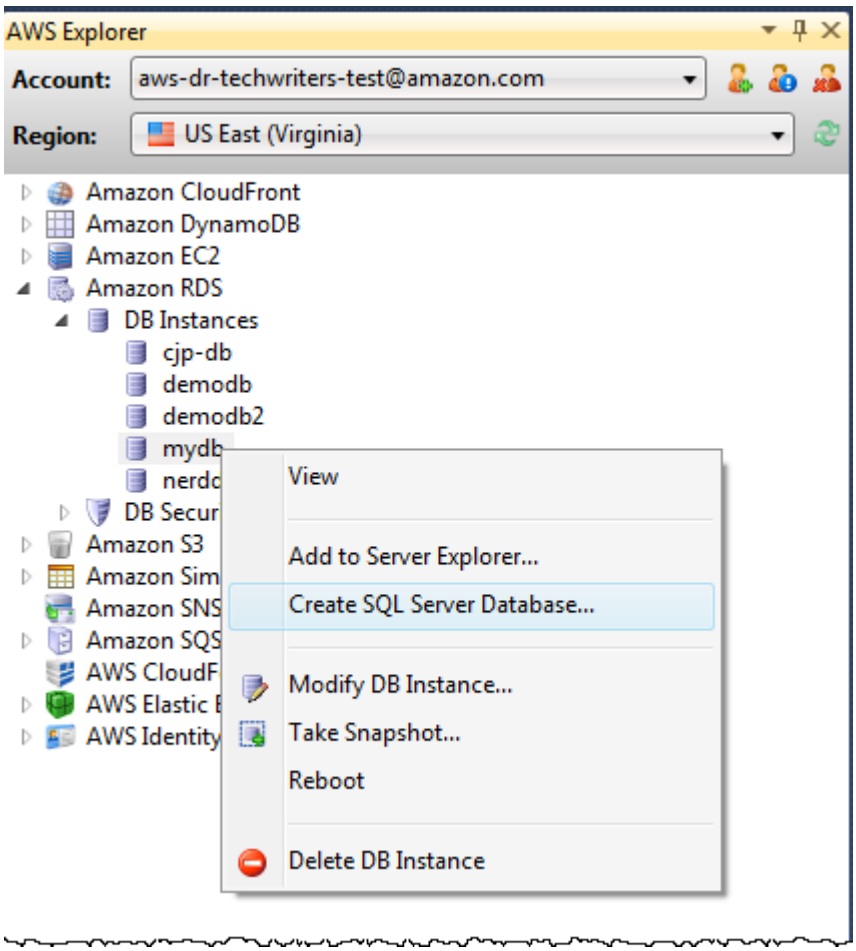
Cree una base de datos de Microsoft SQL Server en una instancia de RDS

Microsoft SQL Server está diseñado de forma que, después del lanzamiento de una instancia de Amazon RDS, debe crear una base de datos de SQL Server en la instancia de RDS.

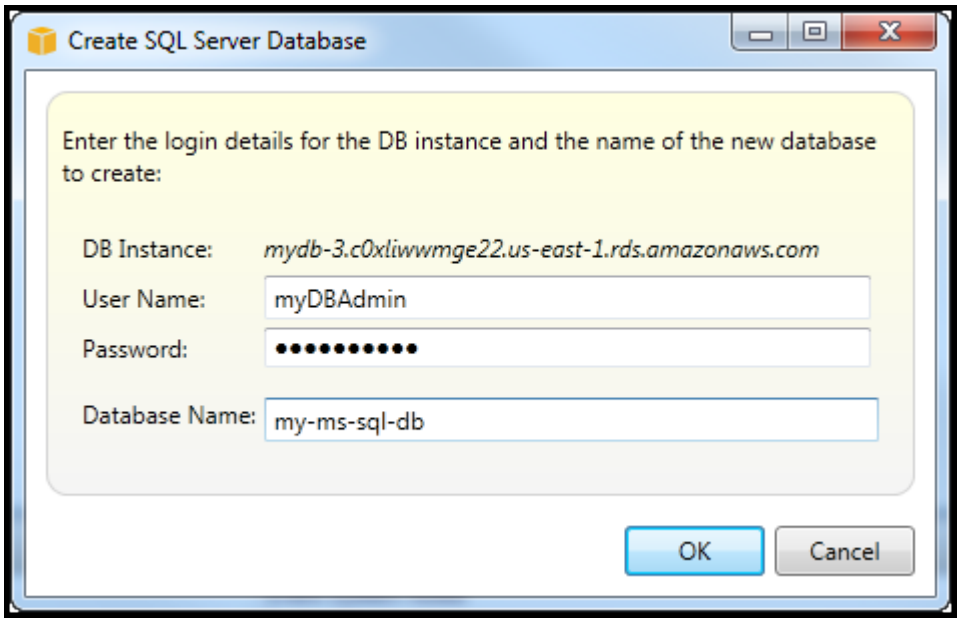
Para obtener información acerca de cómo crear una instancia de Amazon RDS, consulteLanzar una instancia de base de datos de Amazon RDS.

Para crear una base de datos de Microsoft SQL Server

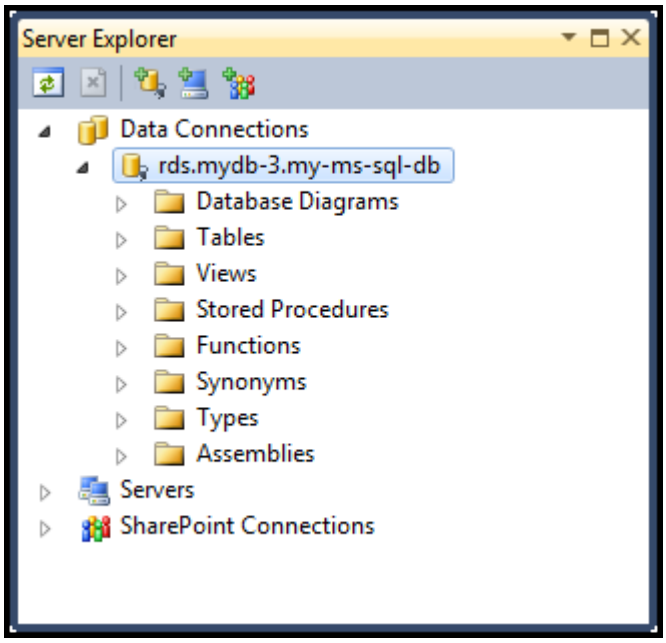
1. EnAWSExplorador, abra el menú contextual (con el botón derecho) del nodo que corresponde a su instancia RDS para Microsoft SQL Server y elijaCrear base de datos de SQL Server.



2. En el cuadro de diálogo Create SQL Server Database (Crear base de datos de SQL Server), escriba la contraseña que especificó al crear la instancia de RDS, escriba un nombre para la base de datos de Microsoft SQL Server y, a continuación, elija OK (Aceptar).



3. El Toolkit for Visual Studio crea la base de datos de Microsoft SQL Server y la añade al Server Explorer de Visual Studio.



Grupos de seguridad de Amazon RDS

Los grupos de seguridad de Amazon RDS le permiten administrar el acceso de red a sus instancias de Amazon RDS. Con los grupos de seguridad, debe especificar conjuntos de direcciones IP mediante la notación CIDR y solo el tráfico de la red procedente de dichas direcciones es reconocido por la instancia de Amazon RDS.

Aunque funcionan de forma similar, los grupos de seguridad de Amazon RDS son diferentes de los grupos de seguridad de Amazon EC2. Es posible añadir un grupo de seguridad de EC2 a su grupo de seguridad de RDS. Cualquier instancia EC2 que sea miembro del grupo de seguridad de EC2 puede obtener acceso, a continuación, a las instancias de RDS que son miembros del grupo de seguridad de RDS.

Para obtener más información acerca de los grupos de seguridad de Amazon RDS, vaya aGrupos de seguridad de RDS. Para obtener más información acerca de los grupos de seguridad de Amazon EC2, vaya aGuía del usuario de EC2.

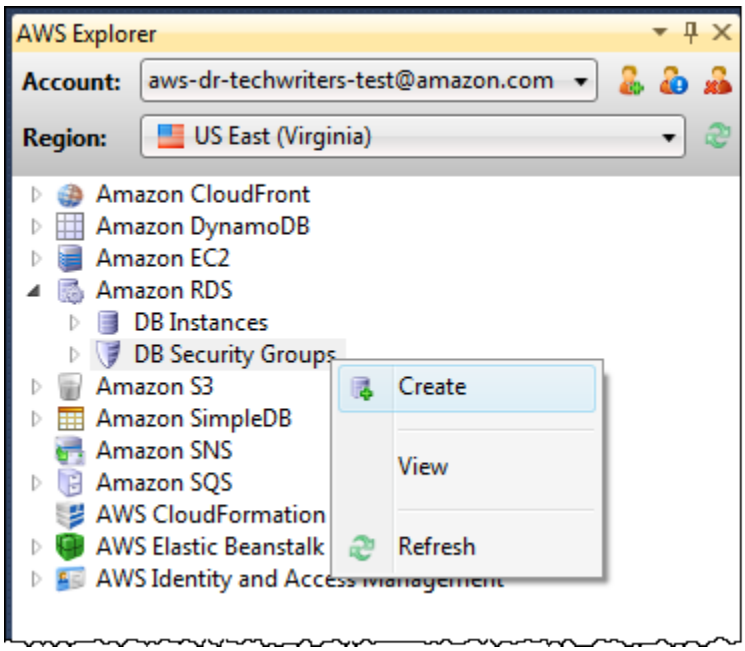
Creación de un grupo de seguridad de Amazon RDS

Puede utilizar Toolkit for Visual Studio para crear un grupo de seguridad de RDS. Si utiliza elAWSToolkit para lanzar una instancia de RDS, el asistente le permitirá especificar un grupo de

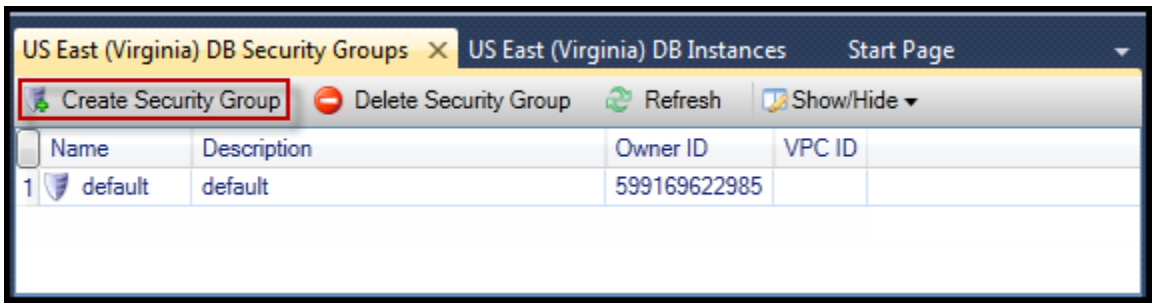
seguridad de RDS para su uso con la instancia. Puede utilizar el siguiente procedimiento para crear ese grupo de seguridad antes de iniciar el asistente.

Para crear un grupo de seguridad de RDS

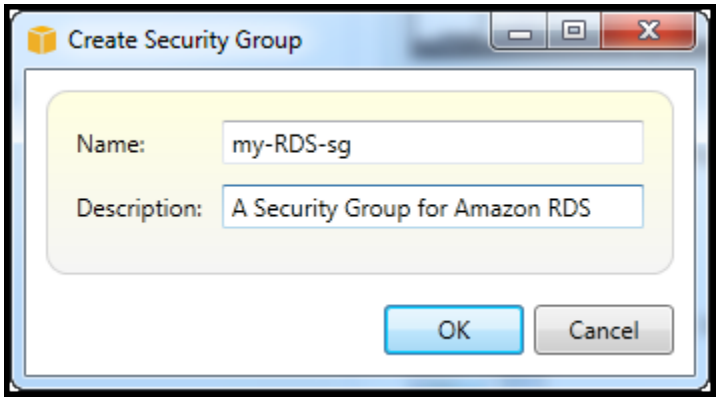
1. EnAWSExplorer, expanda laAmazon RDS, abra el menú contextual (con el botón derecho del ratón) delGrupos de seguridad de base de datossubnodo y eligeCrear.



   Para otras opciones, en elGrupos de seguridadpestaña, elijaCreación del grupo de seguridad. Si no se muestra esta pestaña, abra el menú contextual (con el botón derecho) para el subnodo DB Security Groups (Grupos de seguridad de base de datos) y elija View (Vista).



2. En el cuadro de diálogo Create Security Group (Crear grupo de seguridad), escriba un nombre y una descripción para el grupo de seguridad y, a continuación, elija OK (Aceptar).



Establezca permisos de acceso para un grupo de seguridad de Amazon RDS

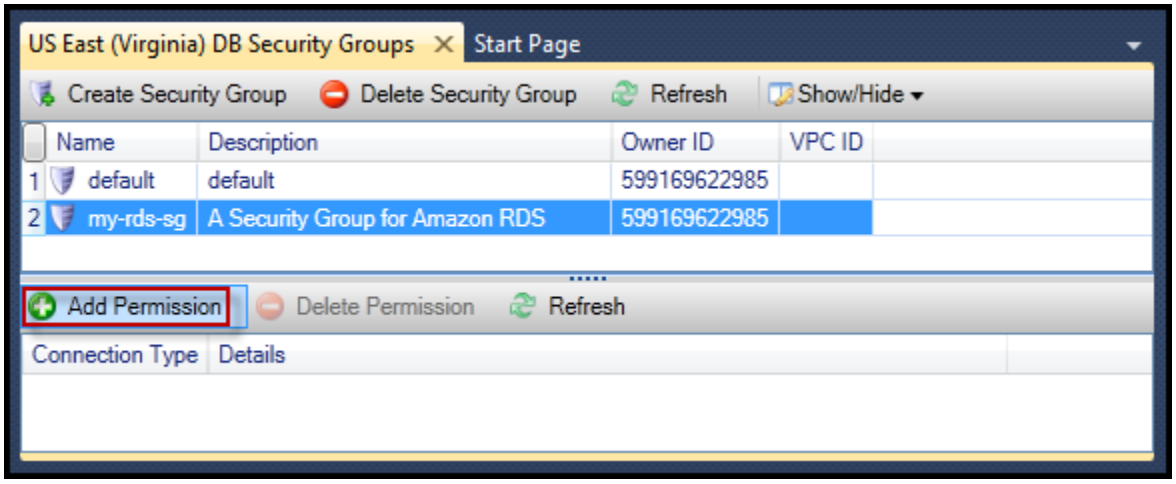
De forma predeterminada, un grupo de seguridad de Amazon RDS nuevo no proporciona acceso a la red. Para habilitar el acceso a instancias de Amazon RDS que utilizan el grupo de seguridad, utilice el siguiente procedimiento para establecer sus permisos de acceso.

Para establecer el acceso para un grupo de seguridad de Amazon RDS

1. En la pestaña Security Groups (Grupos de seguridad), en la vista de lista elija el grupo de seguridad. Si el grupo de seguridad no aparece en la lista, seleccione Refresh (Actualizar). Si el grupo de seguridad sigue sin figurar en la lista, verifique que está viendo la lista para obtener la correctaAWSregion. Security Groupen las pestañas delAWSEl kit de herramientas es específico de cada región.

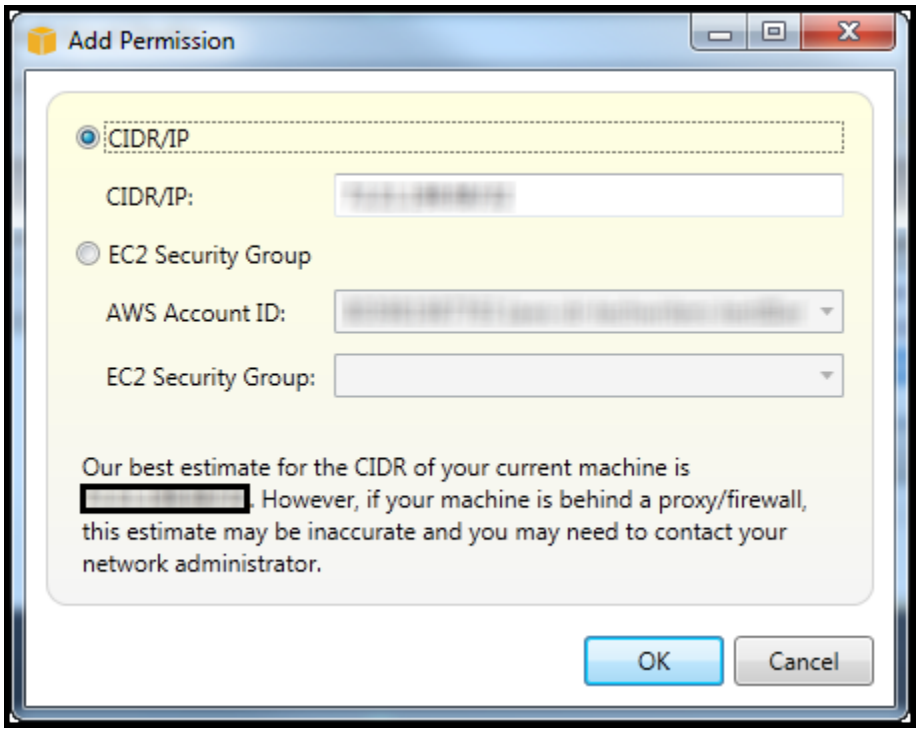
   Si noSecurity Groupaparecen pestañas, enAWSExplorador, abra el menú contextual (con el botón derecho del ratón) delGrupos de seguridad de base de datossubnodo y eligeVista.

2. Elija Add Permission (Añadir permiso).



Botón Add Permissions (Añadir permisos) en la pestaña Security Groups (Grupos de seguridad)

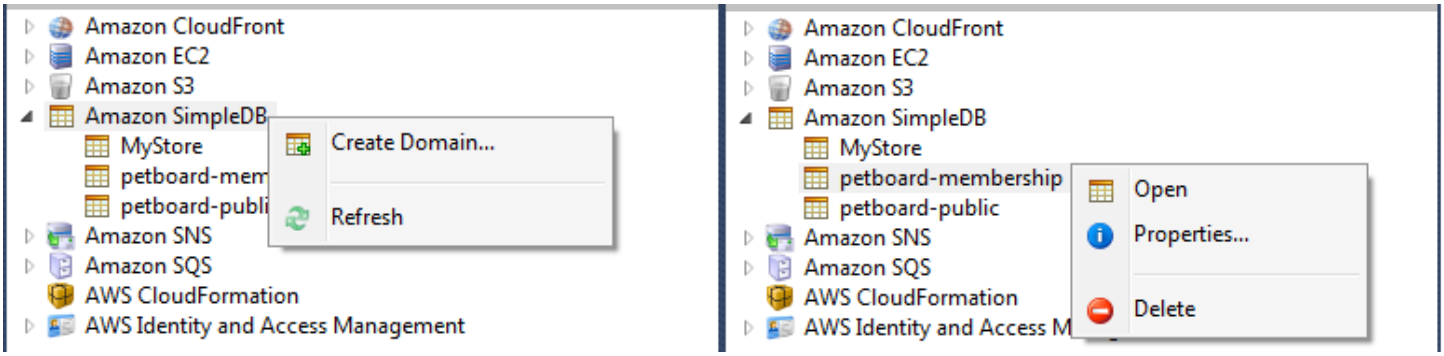
3. En el cuadro de diálogo Add Permission (Añadir permiso), puede utilizar la notación CIDR para especificar qué direcciones IP pueden obtener acceso a su instancia de RDS o puede especificar qué grupos de seguridad de EC2 pueden obtener acceso a su instancia de RDS. Cuando elijaGrupo de seguridad de la EC2, puede especificar el acceso para todas las instancias EC2 asociadas a unCuenta de AWStiene acceso o puede elegir un grupo de seguridad de EC2 en la lista desplegable.



LaAWSToolkit intenta determinar su dirección IP y rellenar automáticamente el cuadro de diálogo con la especificación CIDR adecuada. Sin embargo, si el equipo obtiene acceso a Internet a través de un firewall, el CIDR determinado por el Toolkit podría no ser preciso.

Uso de Amazon SimpleDB deAWSExplorador

AWSAWS Explorer muestra todos los dominios de Amazon SimpleDB asociados con el activoAWSaccount. DesdeAWSExplorador, puede crear o eliminar dominios de Amazon SimpleDB.

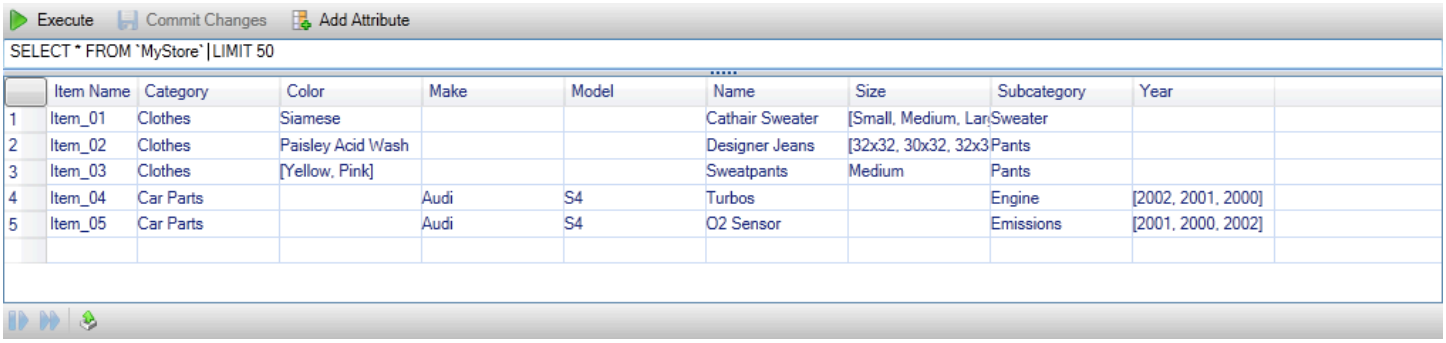


Create, delete, or open Amazon SimpleDB domains associated with your account

Ejecución de consultas y edición de resultados

AWSAWS Explorer también puede mostrar una vista de cuadrícula de un dominio de Amazon SimpleDB desde la que puede ver los elementos, atributos y valores en dicho dominio. Puede ejecutar consultas de manera que solo se muestre un subconjunto de los elementos del dominio. Al hacer doble clic en una celda, puede editar los valores para el atributo correspondiente de ese elemento. También puede añadir nuevos atributos al dominio.

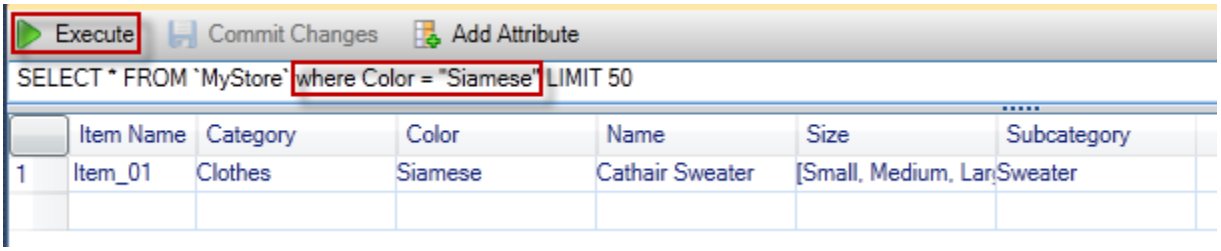
El dominio que se muestra aquí es del ejemplo de Amazon SimpleDB incluido con elAWS SDK for .NET.



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

Amazon SimpleDB grid view

Para ejecutar una consulta, edite la consulta en el cuadro de texto en la parte superior de la vista de cuadrícula y, a continuación, seleccione Execute (Ejecutar). La vista se filtra para mostrar solo los elementos que coincidan con la consulta.



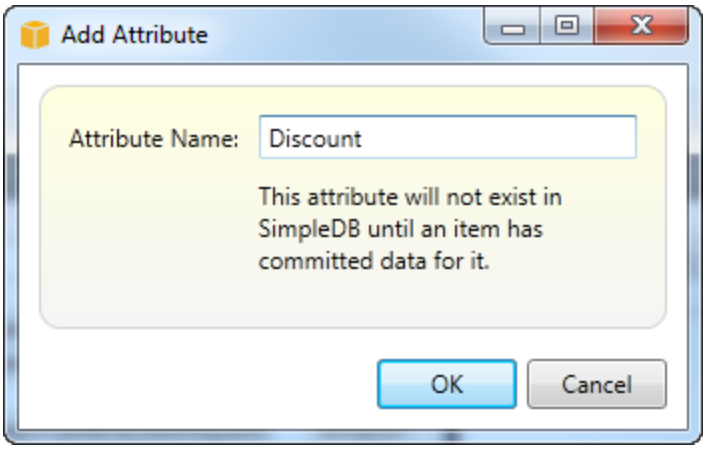
	Item Name	Category	Color	Name	Size	Subcategory
1	Item_01	Clothes	Siamese	Cathair Sweater	[Small, Medium, Lar	Sweater

Execute query from AWS Explorer

Para editar los valores asociados con un atributo, haga doble clic en la celda correspondiente, edite los valores y, a continuación, elija Commit Changes (Confirmar cambios).

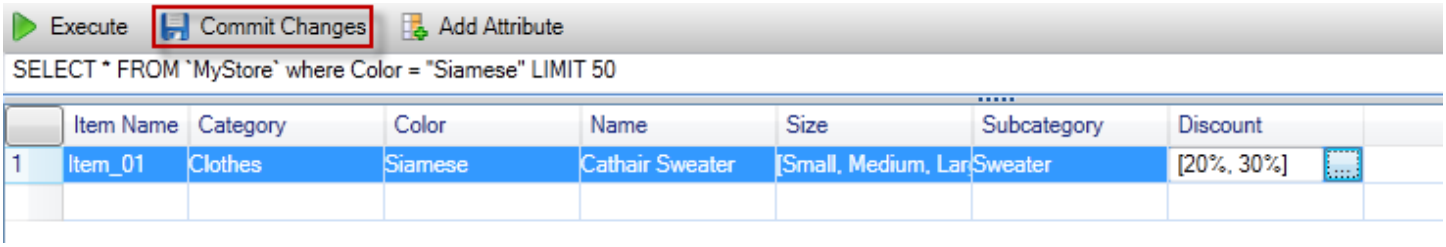
Adición de un atributo

Para añadir un atributo, en la parte superior de la vista, seleccione Add Attribute (Añadir atributo).



Add Attribu dialog box

Para que el atributo forme parte del dominio, debe añadir un valor para al menos un elemento y, a continuación, elegir Commit Changes (Confirmar cambios).



Commit changes for a new attribute

Paginación de los resultados de la consulta

Hay tres botones en la parte inferior de la vista.

Paginate and export buttons

Los dos primeros botones proporcionan paginación para los resultados de la consulta. Para visualizar una página adicional de resultados, elija el primer botón. Para visualizar diez páginas adicionales de resultados, elija el segundo botón. En este contexto, una página es igual a 100 filas o el número de resultados especificado por el valor LÍMITE, si se ha incluido en la consulta.

Exportar a CSV

El último botón exporta los resultados actuales a un archivo CSV.

Uso de Amazon SQS desdeAWSExplorador

Amazon Simple Queue Service (Amazon SQS) es un servicio de cola flexible que permite transferir mensajes entre diferentes procesos de ejecución en una aplicación de software. Las colas de Amazon SQS se encuentran en elAWS, pero los procesos que transfieren los mensajes pueden estar ubicados localmente, en instancias Amazon EC2 o en alguna combinación de estas. Amazon SQS es ideal para coordinar la distribución del trabajo entre varios equipos.

El Toolkit for Visual Studio permite ver las colas de Amazon SQS asociadas con la cuenta activa, crear y eliminar colas y enviar mensajes a través de las colas. (Por «cuenta activa», se entiende la cuenta seleccionada enAWSExplorador.)

Para obtener más información acerca de Amazon SQS, consulte laIntroducción a SQSen laAWS.

Creación de una cola

Puede crear una cola de Amazon SQS desdeAWSExplorador. El ARN y la URL de la cola se basarán en el número de la cuenta activa y en el nombre especificado para la cola en el momento de la creación.

Para crear una cola

1. EnAWSExplorador, abra el menú contextual (clic con el botón derecho) delAmazon SQSnodo y, a continuación, elijaCREATE QUEUE.
2. En el cuadro de diálogo Create Queue (Crear cola), especifique el nombre de la cola, el tiempo de espera de visibilidad predeterminado y el retraso de entrega predeterminado. El tiempo de espera de visibilidad predeterminado y el retraso de entrega predeterminado se especifican en segundos. El tiempo de espera de visibilidad predeterminado es la cantidad de tiempo que un mensaje será invisible para los procesos receptores potenciales después de que un proceso concreto haya adquirido el mensaje. El retraso de entrega predeterminado es la cantidad de tiempo que transcurre desde el momento en que el mensaje se envía hasta el momento en que pasa a ser visible para los procesos receptores potenciales.
3. Seleccione OK (Aceptar). La nueva cola aparecerá como un subnodo bajo el nodo Amazon SQS.

Eliminación de una cola

Puede eliminar colas deAWSExplorador. Si elimina una cola, todos los mensajes asociados con ella dejarán de estar disponibles.

Para eliminar una cola

1. EnAWSExplorador, abra los menús contextuales (con el botón derecho del ratón) de la cola que desea eliminar y, a continuación, elijaBorrar.

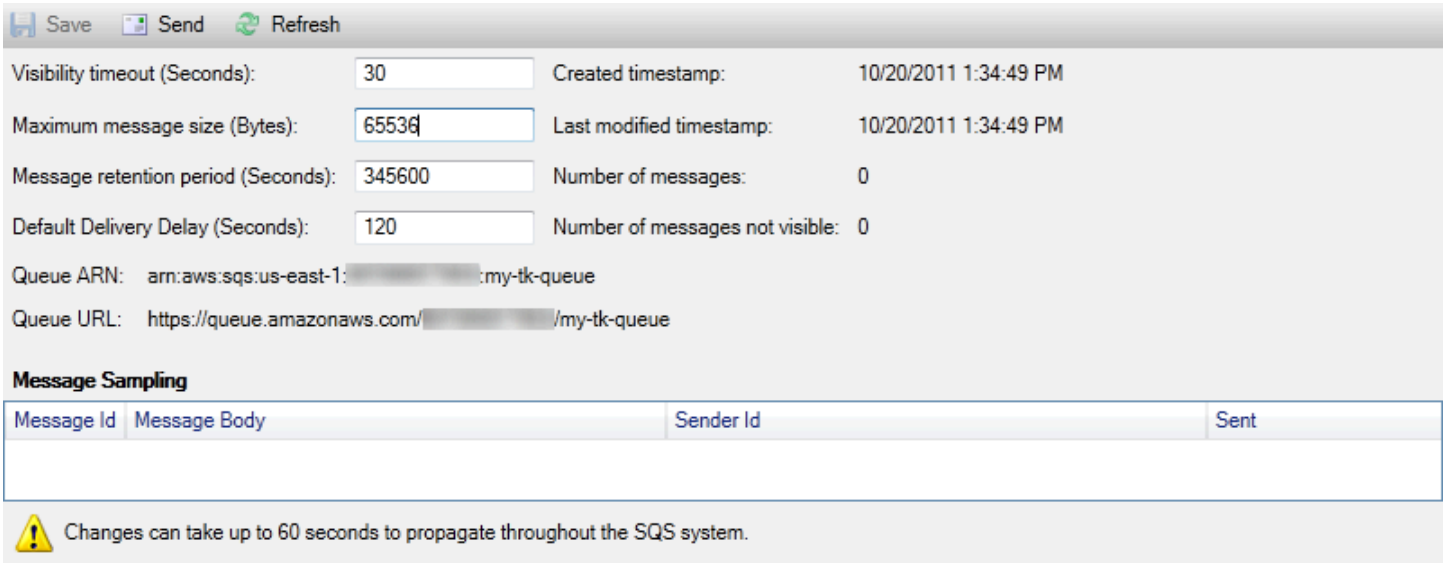
Administrar las propiedades de la cola

Puede ver y editar las propiedades de cualquiera de las colas que se muestran enAWSExplorador. También puede enviar mensajes a la cola desde esta vista de propiedades.

Para administrar las propiedades de la cola

- EnAWSExplorador, abra el menú contextual (con el botón derecho del ratón) de la cola cuyas propiedades desea administrar y, a continuación, elijaCola de visualización.

  En la vista de las propiedades de la cola, puede editar el tiempo de espera de visibilidad, el tamaño máximo de mensaje, el periodo de retención de mensajes y el retraso de entrega predeterminado. El retraso de entrega predeterminado se puede reemplazar al enviar un mensaje. En la siguiente captura de pantalla, el texto ilegible es el componente de número de cuenta del ARN y la URL de la cola.



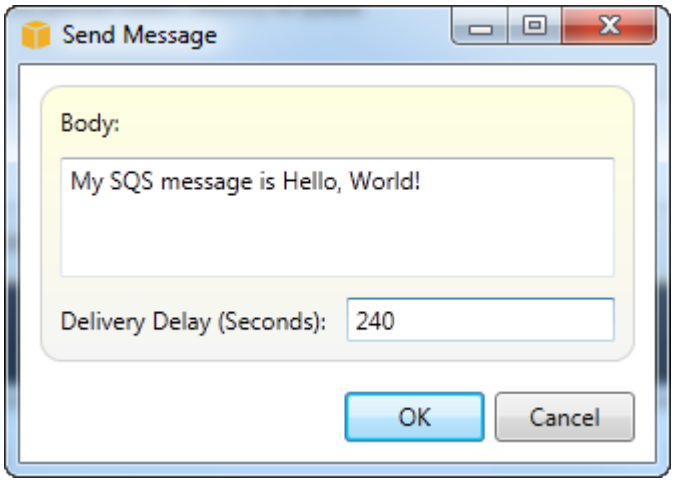
SQS queue properties view

Envío de un mensaje a una cola

Desde la vista de las propiedades de una cola, puede enviar un mensaje a la cola.

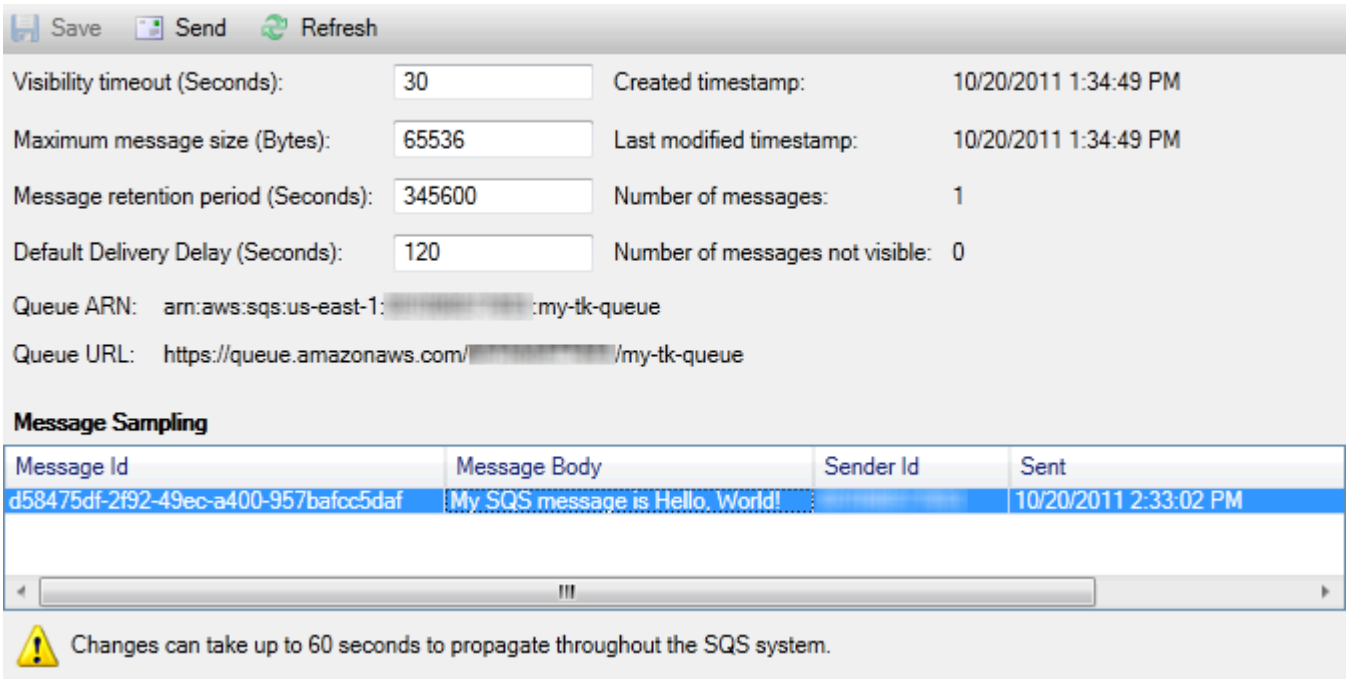
Para enviar un mensaje

1. En la parte superior de la vista de propiedades de la cola, elija el botón Send (Enviar).
2. Escriba el mensaje. (Opcional) Escriba un retraso de entrega que sustituirá al retraso de entrega predeterminado para la cola. En el siguiente ejemplo, se ha sustituido el retraso por un valor de 240 segundos. Seleccione OK (Aceptar).



Envíos de mensajes dialog box

3. Espere aproximadamente 240 segundos (cuatro minutos). El mensaje aparecerá en la sección Message Sampling (Muestreo de mensajes) de la vista de propiedades de la cola.



SQS properties view with sent message

La marca temporal de la vista de propiedades de la cola es la hora a la que se eligió el botón Send (Enviar). No incluye el retraso. Por lo tanto, la hora a la que el mensaje aparece en la cola y está disponible para los receptores podría ser posterior a esta marca temporal. La marca temporal se muestra en la hora local de su equipo.

Identity and Access Management

AWS Identity and Access Management(IAM) le permite administrar de una forma más segura el acceso a suCuentas de AWSy recursos. Con IAM, puede crear varios usuarios en su principal (nodo raíz)Cuenta de AWS. Esos usuarios pueden tener sus propias credenciales: contraseña, ID de clave de acceso y clave secreta, pero todos los usuarios de IAM comparten un único número de cuenta.

Puede administrar el nivel de acceso a los recursos de cada usuario de IAM adjuntando políticas de IAM al usuario. Por ejemplo, puede adjuntar a un usuario de IAM una política que le dé acceso al servicio de Amazon S3 y a los recursos relacionados de la cuenta de la que usted es titular, pero que no le proporcione acceso a otros servicios o recursos.

Para administrar el acceso de un modo más eficiente, puede crear grupos de IAM, que son conjuntos de usuarios. Al adjuntar una política al grupo, afecta a todos los usuarios que son miembros de ese grupo.

Además de administrar los permisos en el nivel de los usuarios y los grupos, IAM también admite el concepto de roles de IAM. Como en el caso de los usuarios y los grupos, puede adjuntar políticas a los roles de IAM. A continuación, puede asociar el rol de IAM con una instancia de Amazon EC2. Las aplicaciones que se ejecutan en la instancia EC2 pueden obtener acceso aAWSutilizando los permisos proporcionados por el rol de IAM. Para obtener más información acerca del uso de los roles de IAM con el Toolkit, consulte Creación de un rol de IAM. Para obtener más información acerca de IAM, consulte laIAM User Guide.

Creación y configuración de un usuario de IAM

Los usuarios de IAM le permiten conceder a otras personas acceso a suCuenta de AWS. Dado que puede adjuntar políticas a los usuarios de IAM, puede limitar con precisión los recursos a los que puede obtener acceso un usuario de IAM y las operaciones que puede llevar a cabo en esos recursos.

Como práctica recomendada, todos los usuarios que obtienen acceso a unCuenta de AWSdeberían hacerlo como usuarios de IAM, incluso el propietario de la cuenta. De este modo, se garantiza que si las credenciales de uno de los usuarios de IAM se ven comprometidas, se pueden desactivar únicamente esas credenciales. No es necesario desactivar o cambiar las credenciales raíz de la cuenta.

Desde Toolkit for Visual Studio, puede asignar permisos a un usuario de IAM adjuntándole una política de IAM o asignando el usuario a un grupo. Los usuarios de IAM que están asignados a un grupo obtienen sus permisos de las políticas adjuntadas al grupo. Para obtener más información, consulte Creación de un grupo de IAM y Adición de un usuario de IAM a un grupo de IAM.

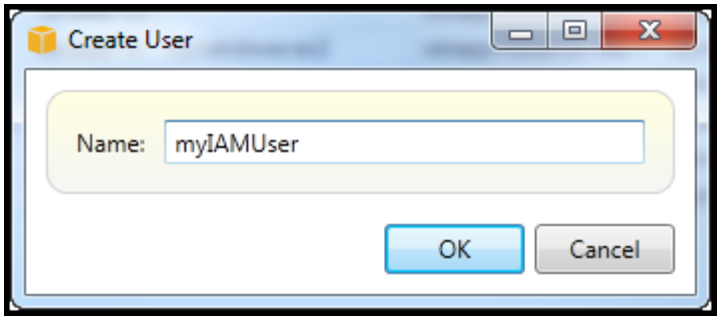
En el Toolkit for Visual Studio, también puede generarAWScredenciales (ID de clave de acceso y clave secreta) para el usuario de IAM. Para obtener más información, consulte Generación de credenciales para un usuario de IAM.

Toolkit for Visual Studio admite la especificación de las credenciales de usuario de IAM para obtener acceso a los servicios a través deAWSExplorador. Como normalmente los usuarios de IAM no tienen acceso completo a todos los Amazon Web Services, algunas de las funcionalidades deAWSPuede que Explorer no esté disponible. Si usaAWSExplorador para cambiar los recursos cuando la cuenta activa es un usuario de IAM y, a continuación, cambia la cuenta activa a la cuenta raíz, los cambios podrían no estar visibles hasta que actualice la vista enAWSExplorador. Para actualizar la vista, elija el botón de actualización ().

Para obtener información acerca de cómo configurar usuarios de IAM en elAWS Management Console, vaya aTrabajo con usuarios y gruposen la guía del usuario de IAM.

Para crear un usuario de IAM

1. EnAWSExplorer, expanda laAWS Identity and Access Management, abra el menú contextual (con el botón derecho del ratón) deUsuarios dey luego enCrear usuario.
2. En el navegadorCrear usuario, escriba un nombre para el usuario de IAM y elijaDE ACUERDO. Este es el IAMnombre descriptivo. Para obtener información acerca de las restricciones de los nombres de los usuarios de IAM, vaya a laIAM User Guide.



Create an IAM user

El nuevo usuario aparecerá como un subnodo enUsuarios debajo elAWS Identity and Access Managementnodo.

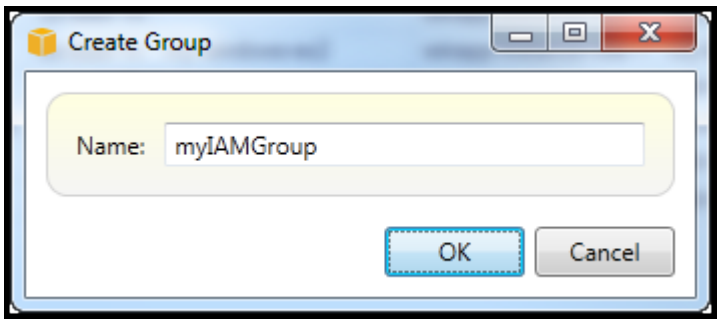
Para obtener información acerca de cómo crear una política y asociarla al usuario, consulte Creación de una política de IAM.

Creación de un grupo de IAM

Los grupos proporcionan una forma de aplicar políticas de IAM a un conjunto de usuarios. Para obtener información acerca de cómo administrar los usuarios y los grupos de IAM, vaya aTrabajo con usuarios y gruposen la guía del usuario de IAM.

Para crear un grupo de IAM

1. EnAWSExplorer, enIdentity and Access Management, abra el menú contextual (con el botón derecho del ratón) deGroupsy eligeCreación de un grupo.
2. En el navegadorCreación de un grupo, escriba un nombre para el grupo IAM y elijaDE ACUERDO.



Create IAM group

El nuevo grupo de IAM aparecerá bajo elGroupssubnodo deIdentity and Access Management.

Para obtener información acerca del procedimiento para crear una política y adjuntarla al grupo de IAM, consulteCrear una política de IAM.

Adición de un usuario de IAM a un grupo de IAM

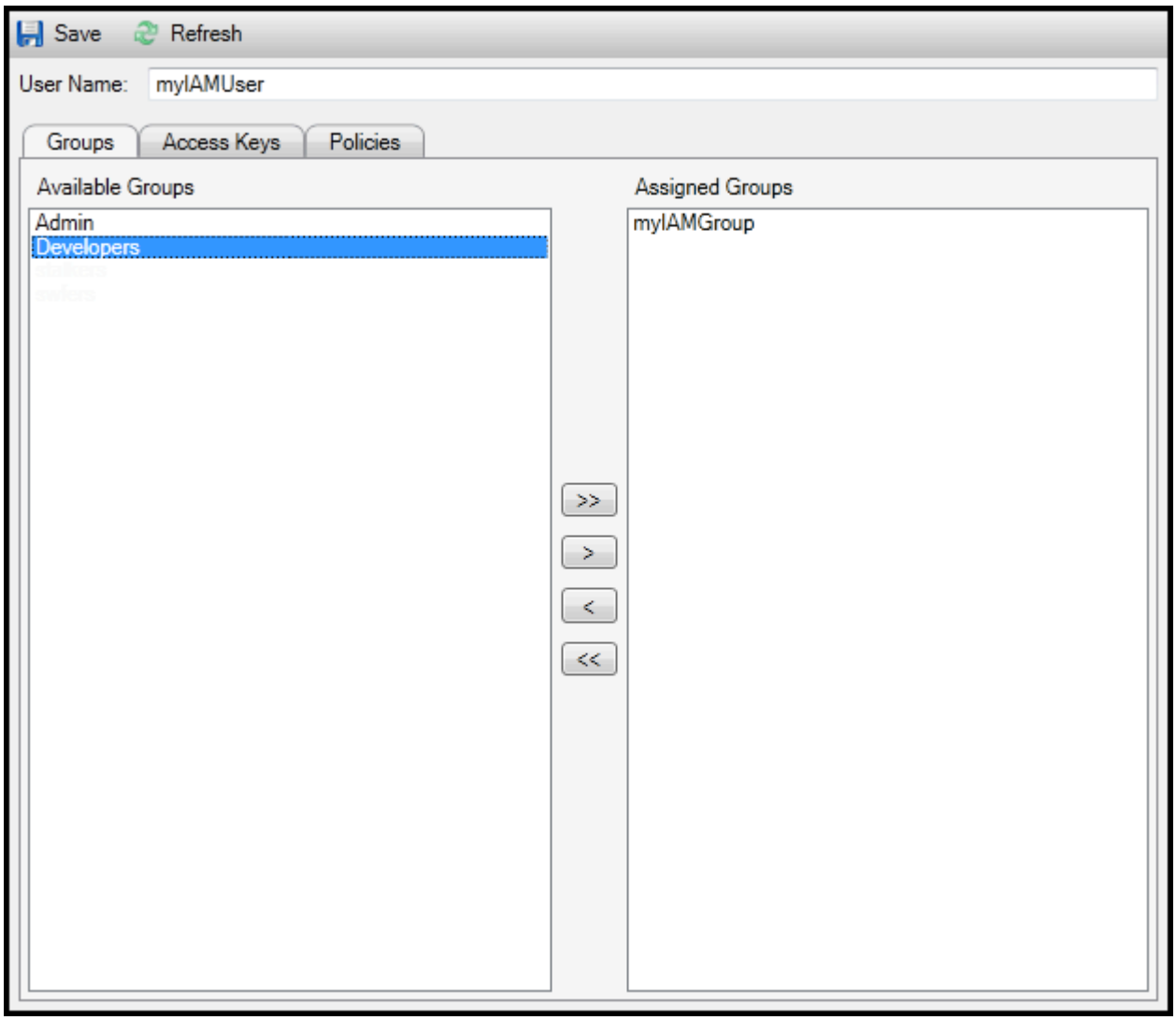
Los usuarios de IAM que son miembros de un grupo de IAM obtienen sus permisos de acceso de las políticas adjuntadas al grupo. El objetivo de un grupo de IAM es facilitar la administración de permisos en un conjunto de usuarios de IAM.

Para obtener información acerca de cómo las políticas adjuntadas a un grupo de IAM interactúan con las políticas adjuntadas a los usuarios de IAM que son miembros de ese grupo de IAM, vaya aAdministración de políticas de IAM en la guía del usuario de IAM.

EnAWSExplorer, los usuarios de IAM se añaden a los grupos de IAM en elUsuarios desubnodo, no elGroupssubnodo.

Para agregar un usuario de IAM a un grupo de IAM

1. EnAWSExplorer, enIdentity and Access Management, abra el menú contextual (con el botón derecho del ratón) deUsuarios dey eligeEditar.



Assign an IAM user to a IAM group

2. El panel izquierdo de laGroupsmuestra los grupos de IAM disponibles. El panel derecho muestra los grupos de los que el usuario de IAM especificado ya es miembro.

   Para añadir el usuario de IAM a un grupo, en el panel izquierdo, elija el grupo de IAM y, a continuación, elija el>Botón.

   Para eliminar el usuario de IAM de un grupo, en el panel derecho, elija el grupo de IAM y, a continuación, elija el<Botón.

   Para añadir el usuario de IAM a todos los grupos de IAM, elija la>>Botón. Del mismo modo, para eliminar el usuario de IAM de todos los grupos, elija la<<Botón.

   Para seleccionar varios grupos, elíjalos en secuencia. No es necesario que mantenga pulsada la tecla Control. Para borrar un grupo de la selección, basta con elegirlo una segunda vez.

3. Cuando haya terminado de asignar el usuario de IAM a los grupos de IAM, elijaGuardar.

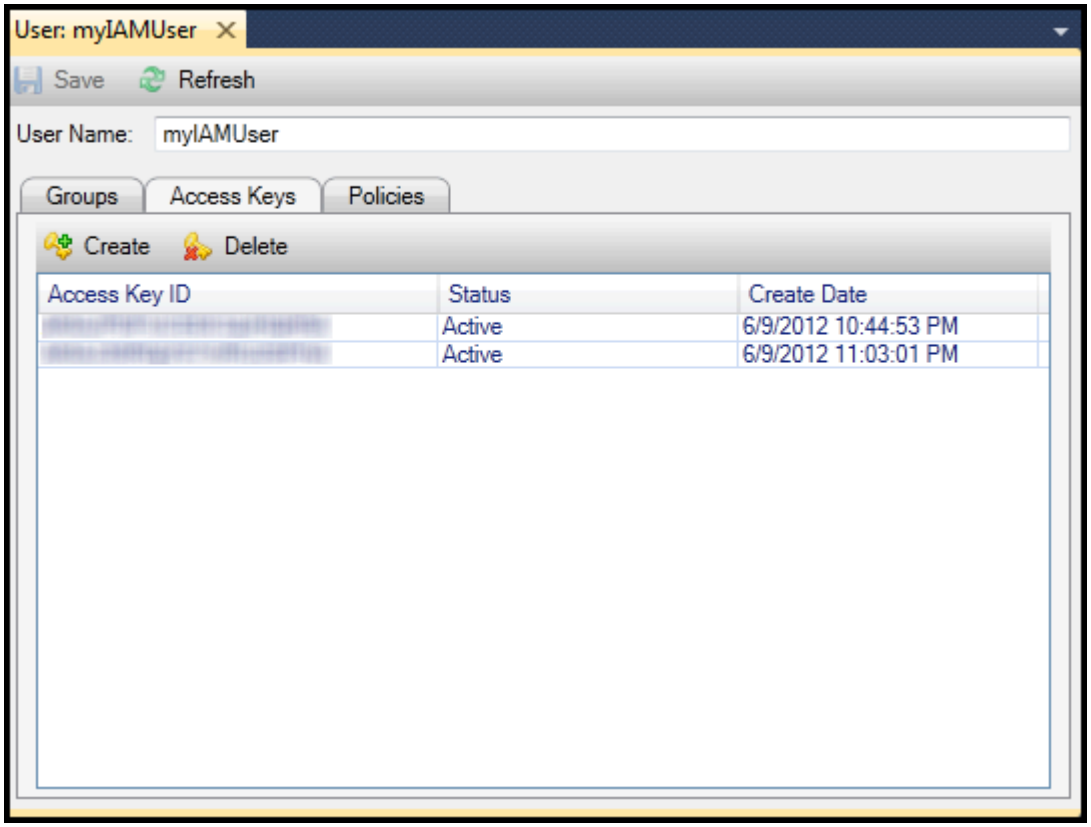
Generación de credenciales para un usuario de IAM

Con Toolkit for Visual Studio, puede generar el ID de clave de acceso y la clave secreta que se utilizan para realizar llamadas a la APIAWS. Estas claves también se pueden especificar para obtener acceso a Amazon Web Services a través del Toolkit. Para obtener más información acerca de la especificación de credenciales para su uso con el Toolkit, consulte creds. Para obtener más información acerca de cómo administrar las credenciales de forma segura, consulte[Prácticas recomendadas para administrarAWSClaves de acceso](#).

El Toolkit no se puede utilizar para generar una contraseña para un usuario de IAM.

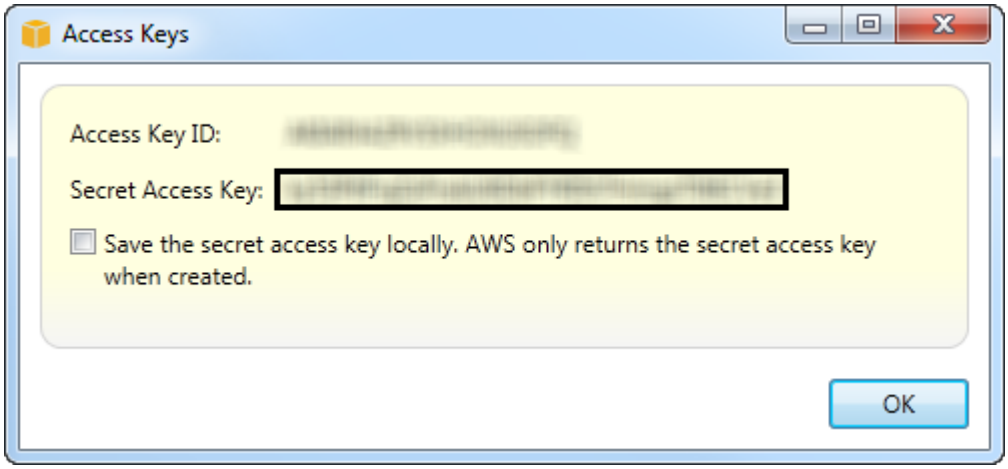
Para generar credenciales para un usuario de IAM

1. EnAWSExplorer, abra el menú contextual (clic con el botón derecho) de un usuario de IAM y elijaEditar.



2. Para generar credenciales, en la pestaña Access Keys (Claves de acceso), elija Create (Crear).

Solo puede generar dos conjuntos de credenciales por cada usuario de IAM. Si ya tiene dos conjuntos de credenciales y necesita crear un conjunto adicional, debe eliminar uno de los conjuntos existentes.

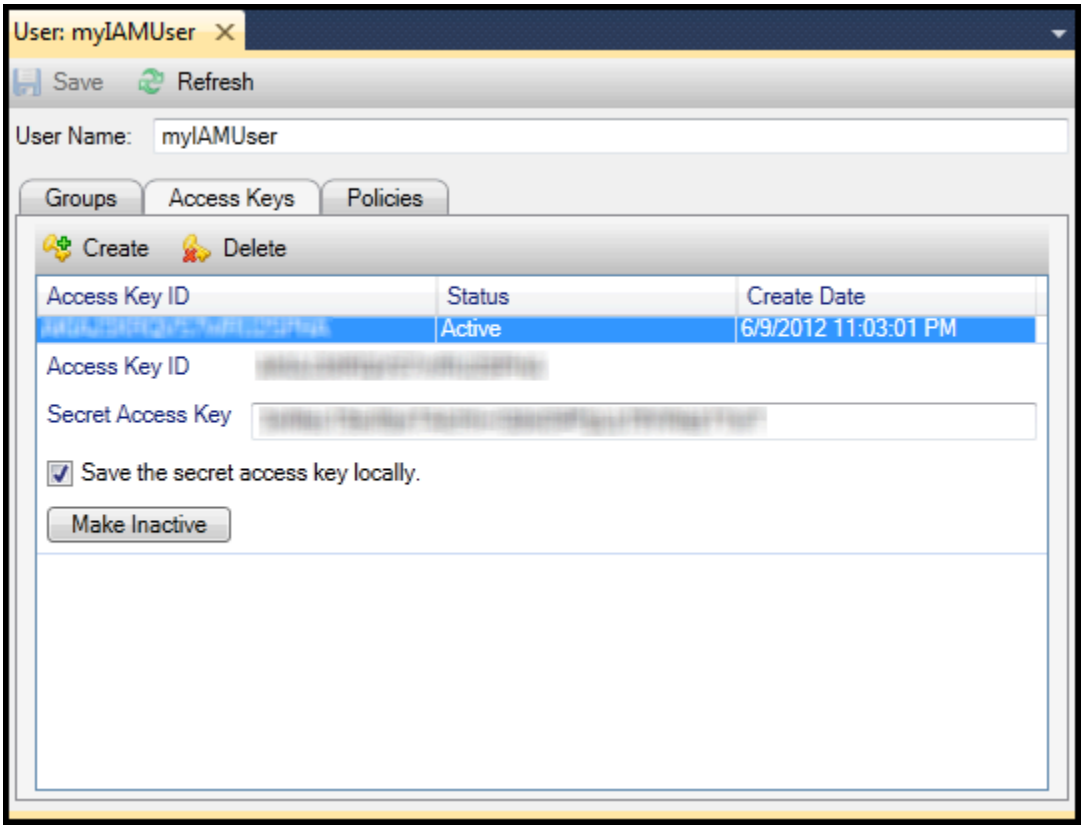


reate credentials for IAM user

Si desea que el Toolkit guarde una copia cifrada de la clave de acceso secreta en la unidad local, seleccioneGuarda la clave de acceso secreta localmente.AWSsolo devuelve la clave de acceso secreta cuando se crea. También puede copiar la clave de acceso secreta en el cuadro de diálogo y guardarla en un lugar seguro.

3. Seleccione OK (Aceptar).

Después de generar las credenciales, puede verlas en la pestaña Access Keys (Claves de acceso). Si ha seleccionado la opción que hace que el Toolkit guarde localmente la clave secreta, se mostrará aquí.



Create credentials for IAM user

Si ha guardado la clave secreta usted mismo y quiere que el Toolkit también la guarde, en el cuadro Secret Access Key (Clave de acceso secreta), escriba la clave de acceso secreta y, a continuación, seleccione Save the secret access key locally (Guardar localmente la clave de acceso secreta).

Para desactivar las credenciales, elija Make Inactive (Desactivar). (Puede hacerlo si sospecha que las credenciales se han visto comprometidas. Puede volver a activar las credenciales si tiene la certeza de que están seguras).

Creación de un rol de IAM

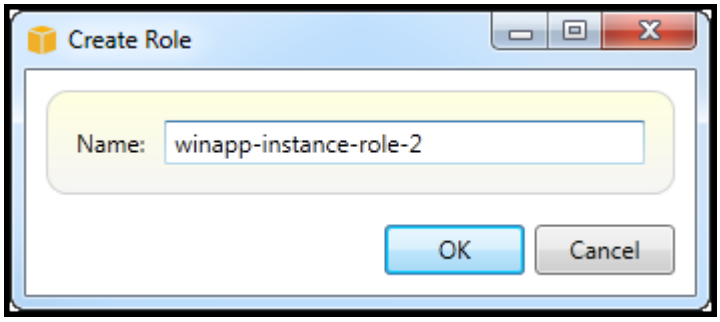
Toolkit for Visual Studio admite la creación y la configuración de roles de IAM. Como en el caso de los usuarios y los grupos, puede adjuntar políticas a los roles de IAM. A continuación, puede asociar el rol de IAM con una instancia de Amazon EC2. La asociación con la instancia EC2 se realiza a través de un perfil de instancia, que es un contenedor lógico para el rol. Las aplicaciones que se ejecutan en la instancia EC2 obtienen automáticamente el nivel de acceso especificado por la política asociada al rol de IAM. Esto se cumplirá aunque la aplicación no haya especificado otroAWSCredenciales de .

Por ejemplo, puede crear un rol y adjuntarle una política que limite su acceso únicamente a Amazon S3. Después de asociar este rol a una instancia EC2, puede ejecutar una aplicación en la instancia y la aplicación tendrá acceso a Amazon S3, pero no a otros servicios o recursos. La ventaja de este método es que no tendrá que preocuparse por transferir y almacenar de forma segura.AWScredenciales de la instancia EC2.

Para obtener más información acerca de los roles de IAM, consulte.Uso de roles de IAM en la guía del usuario de IAM. Para ver ejemplos de programas que accedenAWSutilizando el rol de IAM asociado a una instancia de Amazon EC2, vaya a laAWSguías para desarrolladores deJava,.NET,PHPy Ruby (Configuración de las credenciales mediante IAM,Creación de un rol de IAM, yUso de políticas de IAM).

Para crear un rol de IAM

1. EnAWSExplorer, enIdentity and Access Management, abra el menú contextual (con el botón derecho del ratón) deRoles dey luego enCreación de roles.
2. En el navegadorCreación de un rol, escriba un nombre para el rol de IAM y elijaDE ACUERDO.



Create IAM role

El nuevo rol de IAM aparecerá enRoles deenIdentity and Access Management.

Para obtener información acerca de cómo crear una política y asociarla al rol, consulte Creación de una política de IAM.

Crear una política de IAM

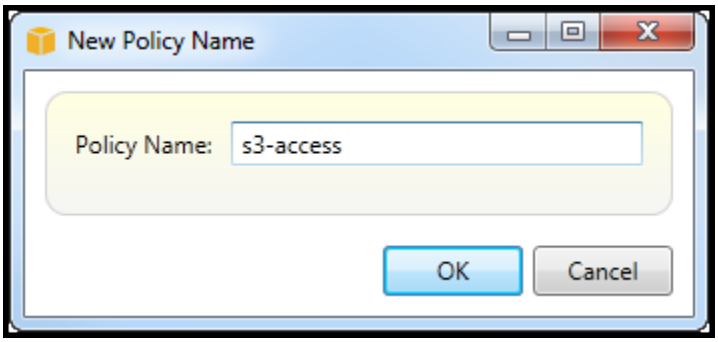
Las políticas son fundamentales para IAM. Las políticas se pueden asociar a IAMentitiescomo usuarios, grupos o roles de. Las políticas especifican el nivel de acceso habilitado para un usuario, un grupo o un rol.

Para crear una política de IAM

EnAWSExplorer, expanda laAWS Identity and Access Managementnodo y, a continuación, expanda el nodo para el tipo de entidad (Groups,Roles de, o bienUsuarios de) a la que adjuntará la política. Por ejemplo, abra un menú contextual para un rol de IAM y elijaEditar.

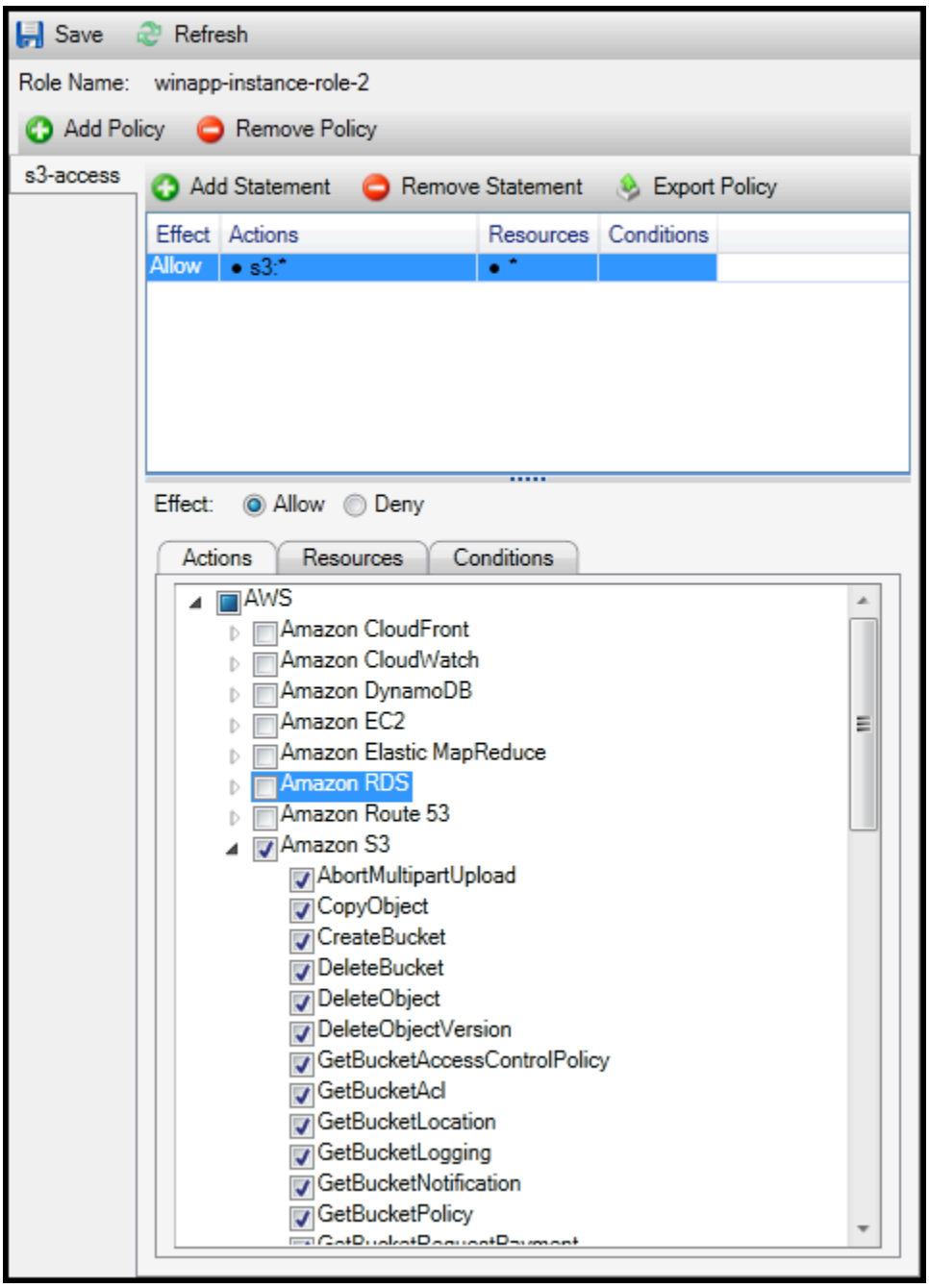
En elAWSExplorador. Elija el enlace Add Policy (Añadir política).

En el cuadro de diálogo New Policy Name (Nombre de la política nueva), escriba un nombre para la política (por ejemplo, s3-access).



New Policy Name dialog box

En el editor de políticas, añada declaraciones de políticas para especificar el nivel de acceso que se debe asignar al rol (en este ejemplo, se ha asociado winapp-instance-role-2 a la política). En este ejemplo, una política proporciona acceso completo a Amazon S3, pero no a otros recursos.



Specify IAM policy

Para obtener un control de acceso más preciso, puede expandir los subnodos del editor de políticas para permitir o no permitir las acciones asociadas con Amazon Web Services.

Una vez editada la política, elija el enlace Save (Guardar).

AWS Lambda

Desarrolle e implemente sus funciones Lambda de C# basadas en .NET Core con. AWS Toolkit for Visual Studio AWS Lambda es un servicio informático que le permite ejecutar código sin aprovisionar ni administrar servidores. El Toolkit for Visual Studio AWS Lambda incluye plantillas de proyectos de.NET Core para Visual Studio.

Para obtener más información al respecto AWS Lambda, consulte la Guía para desarrolladores de AWS Lambda.

Para obtener más información acerca de.NET Core, consulte la guía de Microsoft.NET Core. Para obtener información acerca de los requisitos previos y las instrucciones de instalación de .NET Core para las plataformas Windows, macOS y Linux, consulte .NET Core Downloads.

En los temas siguientes se describe cómo trabajar con el AWS Lambda uso del Toolkit for Visual Studio.

Temas

- Proyecto básico de AWS Lambda
- Proyecto básico de AWS Lambda : creación de una imagen de Docker
- Tutorial: Cree y pruebe una aplicación sin servidor con AWS Lambda
- Tutorial: creación de una aplicación de Lambda con Amazon Rekognition
- Tutorial: Uso de Amazon Logging Frameworks AWS Lambda para crear registros de aplicaciones

Proyecto básico de AWS Lambda

Puede crear una función Lambda mediante plantillas de proyecto de Microsoft.NET Core, en. AWS Toolkit for Visual Studio

Creación de un proyecto de Lambda con .NET Core en Visual Studio

Puede usar plantillas y planos de Lambda-Visual Studio para acelerar la inicialización del proyecto. Los planos de Lambda contienen funciones preescritas que simplifican la creación de una base de proyecto flexible.

> **Note**
>
> El servicio Lambda tiene límites de datos en diferentes tipos de paquetes. Para obtener información detallada sobre los límites de datos, consulte el tema Cuotas de Lambda en la Guía del usuario de AWS Lambda.

Para crear un proyecto Lambda en Visual Studio

1. En Visual Studio, expanda el menú Archivo, expanda Nuevo y, a continuación, elija Proyecto.
2. En el cuadro de diálogo Nuevo proyecto, establezca los cuadros desplegables Idioma, Plataforma y Tipo de proyecto en «Todos» y, a continuación, escriba aws lambda en el campo de búsqueda. Elija la AWS plantilla Lambda Project (.NET Core - C#).
3. En el campo Nombre, introduzca**`AWSLambdaSample`**, especifique la ubicación del archivo que desee y, a continuación, seleccione Crear para continuar.
4. En la página de selección de planos, seleccione el esquema de función vacía y, a continuación, elija Finalizar para crear el proyecto de Visual Studio.

Revisión de los archivos del proyecto

Hay dos archivos de proyecto que revisar: `aws-lambda-tools-defaults.json` y `Function.cs`.

En el siguiente ejemplo, se muestra el `aws-lambda-tools-defaults.json` archivo, que se crea automáticamente como parte del proyecto. Puede configurar las opciones de construcción mediante los campos de este archivo.

> **Note**
>
> Las plantillas de proyecto de Visual Studio contienen muchos campos diferentes; tenga en cuenta lo siguiente:
>
> - function-handler: especifica el método que se ejecuta cuando se ejecuta la función Lambda
> - Al especificar un valor en el campo del controlador de funciones, ese valor se rellena previamente en el asistente de publicación.
> - Si cambia el nombre de la función, clase o ensamblaje, también necesitará actualizar el campo correspondiente en el archivo. `aws-lambda-tools-defaults.json`

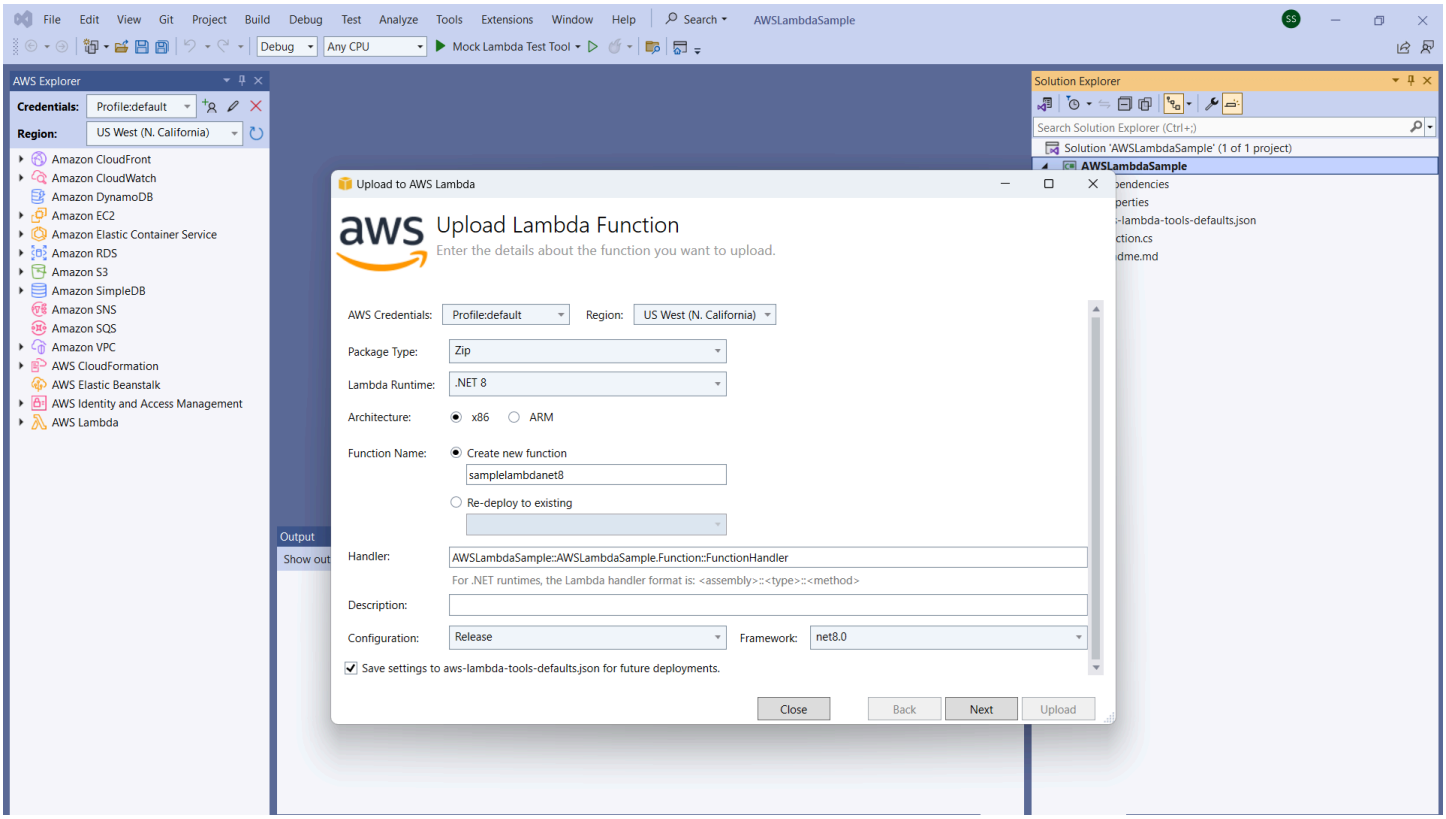
```
{
  "Information": [
    "This file provides default values for the deployment wizard inside Visual Studio
 and the AWS Lambda commands added to the .NET Core CLI.",
    "To learn more about the Lambda commands with the .NET Core CLI execute the
 following command at the command line in the project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

Examine el archivo `Function.cs`. `Function.cs` define las funciones de C# que se expondrán como funciones de Lambda. Este `FunctionHandler` es la funcionalidad de Lambda que tiene lugar cuando se ejecuta la función de Lambda. En este proyecto, hay una función definida: `FunctionHandler`, que llama a `ToUpper()` en el texto de entrada.

Ahora, el proyecto ya está listo para la publicación en Lambda.

Publicar en Lambda

El procedimiento y la imagen siguientes muestran cómo cargar la función en Lambda mediante. AWS Toolkit for Visual Studio



Publicar la función en Lambda

1. Navegue hasta el AWS Explorador expandiendo Ver y seleccionando AWS Explorador.
2. En el Explorador de soluciones, abra el menú contextual del proyecto que desee publicar (haga clic con el botón derecho) y, a continuación, seleccione Publicar en AWS Lambda para abrir la ventana Cargar función Lambda.
3. En la ventana Cargar función Lambda, complete los siguientes campos:

    a. Tipo de paquete: elija**`Zip`**. Se creará un archivo ZIP como resultado del proceso de compilación y se cargará en Lambda. Como alternativa, puede elegir Package Type**`Image`**. El tutorial: Creación de imágenes de Docker en un proyecto Lambda básico describe cómo publicar mediante Package Type. **`Image`**

    b. Lambda Runtime: elija su Lambda Runtime en el menú desplegable.

    c. Arquitectura: seleccione la radial para la arquitectura que prefiera.

    d. Nombre de la función: seleccione la radial para Crear nueva función y, a continuación, introduzca un nombre para mostrar para la instancia de Lambda. Tanto el AWS explorador como las AWS Management Console pantallas hacen referencia a este nombre.

e. Controlador: utilice este campo para especificar un controlador de funciones. Por ejemplo: **`AWSLambdaSample::AWSLambdaSample.Function::FunctionHandler`**.

f. (Opcional) Descripción: introduce un texto descriptivo para que se muestre con la instancia, desde dentro del. AWS Management Console

g. Configuración: elija la configuración que prefiera en el menú desplegable.

h. Marco: elija el marco que prefiera en el menú desplegable.

i. Guardar configuración: seleccione esta casilla para guardar la configuración actual `aws-lambda-tools-defaults.json` como predeterminada para futuras implementaciones.

j. Seleccione Siguiente para pasar a la ventana de detalles de funciones avanzadas.

4. En la ventana Detalles de funciones avanzadas, complete los siguientes campos:

   a. Nombre del rol: elija un rol asociado a su cuenta. El rol proporciona credenciales temporales para cualquier llamada de AWS servicio realizada mediante el código de la función. Si no tiene un rol, desplácese hasta encontrar el nuevo rol basado en la política AWS gestionada en el selector desplegable y, a continuación, seleccione AWSLambdaBasicExecutionRole. Este rol tiene permisos de acceso mínimos.

   > **Note**
   >
   > Su cuenta debe tener permiso para ejecutar la ListPolicies acción de IAM; de lo contrario, la lista de nombres de rol estará vacía y no podrá continuar.

   b. (Opcional) Si la función Lambda accede a los recursos de una Amazon VPC, seleccione las subredes y los grupos de seguridad.

   c. (Opcional) Defina las variables de entorno que necesite la función Lambda. Las claves se cifran automáticamente con la clave de servicio predeterminada, que es gratuita. Como alternativa, puede especificar una AWS KMS clave, por lo que hay que pagar. KMS es un servicio administrado que se puede usar para crear y controlar las claves de cifrado que se utilizan para cifrar los datos. Si tiene una AWS KMS clave, puede seleccionarla de la lista.

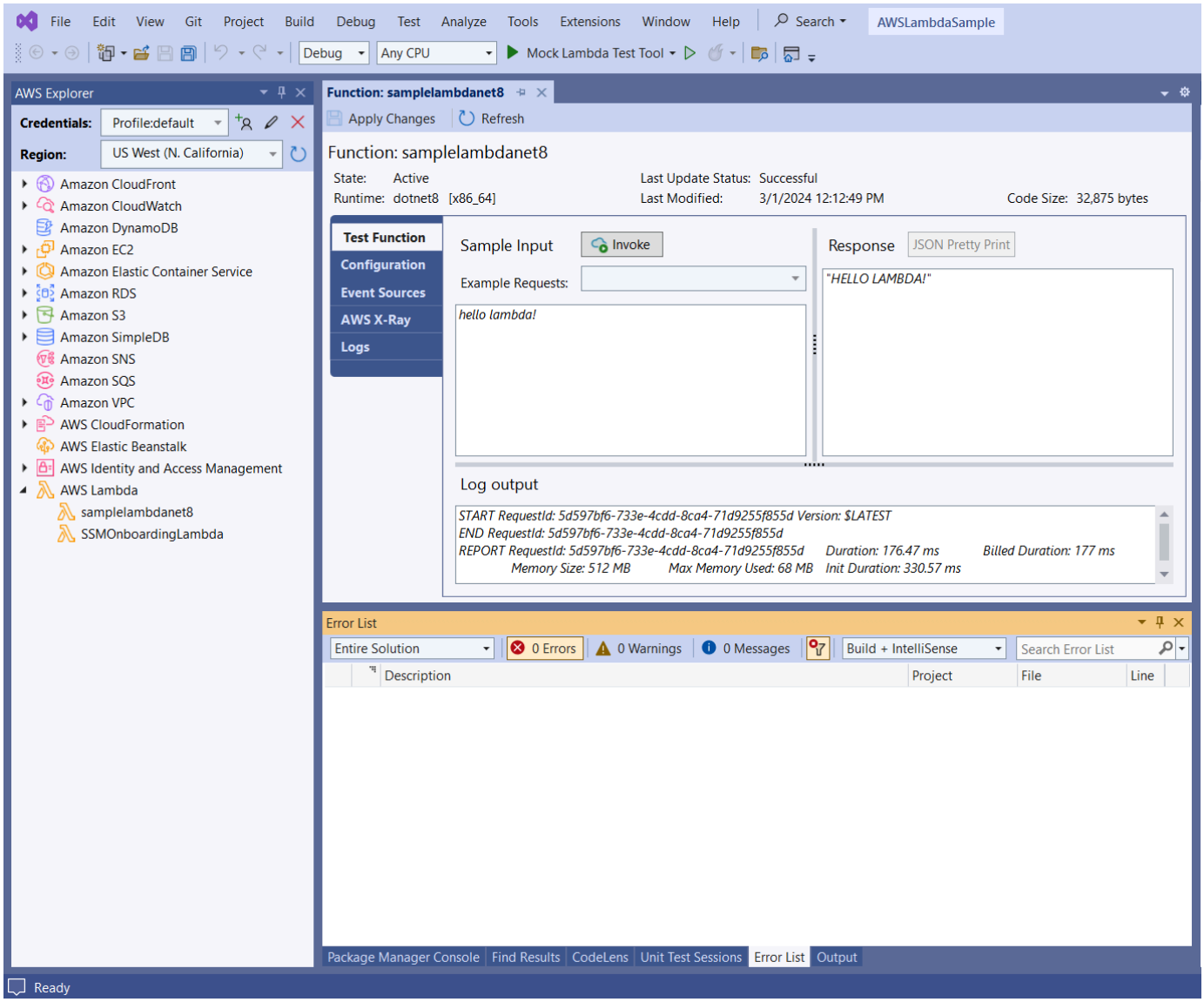
5. Seleccione Cargar para abrir la ventana de la función de carga e iniciar el proceso de carga.

   > **Note**
   >
   > La página de la función de carga se muestra mientras la función se carga en. AWS Para mantener abierto el asistente tras la carga y poder ver el informe, desactive Cerrar

automáticamente el asistente una vez completado correctamente en la parte inferior del formulario antes de que se complete el proceso de carga.
Una vez cargada la función, la función de Lambda estará activa. Se abre la página de visualización Función: y aparece la configuración de la nueva función de Lambda.

6. `hello lambda!`En la pestaña Función de prueba, introduzca el campo de entrada de texto y, a continuación, seleccione Invocar para invocar manualmente la función Lambda. El texto aparece en la pestaña Respuesta, convertido a mayúsculas.

> **Note**
>
> Puede volver a abrir Función: acceda en cualquier momento haciendo doble clic en la instancia implementada ubicada en el Explorador de AWS , debajo del nodo AWS Lambda.



7. (Opcional) Para confirmar que ha publicado correctamente la función Lambda, inicie sesión en Lambda AWS Management Console y, a continuación, seleccione Lambda. La consola muestra todas las funciones de Lambda publicadas, incluida la que acaba de crear.

Eliminación

Si no va a seguir desarrollando con este ejemplo, elimine la función que ha implementado para que no se le facturen los recursos no utilizados de la cuenta.

> **Note**
>
> Lambda supervisa automáticamente las funciones de Lambda por usted e informa de las métricas a través de Amazon. CloudWatch Para supervisar su función y solucionar sus problemas, consulte el tema Solución de problemas y supervisión de funciones AWS Lambda con CloudWatch Amazon en AWS Lambda la Guía para desarrolladores.

Para eliminar la función

1. Desde el AWS Explorador, expanda el AWS Lambdanodo.
2. Haga clic con el botón secundario en la instancia implementada y, a continuación, seleccione Eliminar.

Proyecto básico de AWS Lambda : creación de una imagen de Docker

Puede usar el Toolkit for Visual Studio para implementar AWS Lambda la función como una imagen de Docker. Con Docker, tiene más control sobre su tiempo de ejecución. Por ejemplo, puede elegir tiempos de ejecución personalizados, como .NET 8.0. La imagen de Docker se despliega de la misma forma que cualquier otra imagen de contenedor. Este tutorial es muy similar al Tutorial: proyecto básico de Lambda, con dos diferencias:

- Se incluye un Dockerfile en el proyecto.
- Se elige una configuración de publicación alternativa.

Para obtener más información sobre las imágenes de contenedor de Lambda, consulte Paquetes de implementación de Lambda en la Guía para desarrolladores de AWS Lambda .

Para obtener información adicional sobre cómo trabajar con Lambda AWS Toolkit for Visual Studio, consulte el AWS Toolkit for Visual Studio tema Uso de las AWS Lambda plantillas de esta Guía del usuario.

Creación de un proyecto de Lambda con .NET Core en Visual Studio

Puede usar plantillas y blueprints de Lambda Visual Studio para acelerar la inicialización del proyecto. Los planos de Lambda contienen funciones preescritas que simplifican la creación de una base de proyecto flexible.

Para crear un proyecto de Lambda con .NET Core en Visual Studio

1. En Visual Studio, expanda el menú Archivo, expanda Nuevo y, a continuación, elija Proyecto.
2. En el cuadro de diálogo Nuevo proyecto, establezca los cuadros desplegables Idioma, Plataforma y Tipo de proyecto en «Todos» y, a continuación, escriba **`aws lambda`** en el campo de búsqueda. Elija la AWS plantilla Lambda Project (.NET Core - C#).
3. En el campo Nombre del proyecto, introduzca**`AWSLambdaDocker`**, especifique la ubicación del archivo y, a continuación, seleccione Crear.
4. En la página Seleccionar esquema, elija el blueprint.NET 8 (Container Image) y, a continuación, elija Finalizar para crear el proyecto de Visual Studio. Ahora puede revisar la estructura y el código del proyecto.

Revisión de los archivos del proyecto

En las siguientes secciones se examinan los tres archivos de proyecto creados mediante el blueprint.NET 8 (Container Image):

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

1. Dockerfile

A `Dockerfile` realiza tres acciones principales:

- `FROM`: Establece la imagen base que se utilizará en esta imagen. Esta imagen base proporciona el tiempo de ejecución de.NET, el tiempo de ejecución de Lambda y un script del intérprete de comandos que facilita un punto de entrada para el proceso de Lambda .NET.
- `WORKDIR`: Establece el directorio de trabajo interno de la imagen como`/var/task`.
- `COPY`: Copiará los archivos generados a partir del proceso de creación desde su ubicación local al directorio de trabajo de la imagen.

Las siguientes son `Dockerfile` acciones opcionales que puede especificar:

- `ENTRYPOINT`: La imagen base ya incluye un`ENTRYPOINT`, que es el proceso de inicio que se ejecuta cuando se inicia la imagen. Si desea especificar el suyo propio, anulará ese punto de entrada de base.
- `CMD`: Indica AWS qué código personalizado desea ejecutar. Espera un nombre completo para su método personalizado. Esta línea debe incluirse directamente en el Dockerfile o puede especificarse durante el proceso de publicación.

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

El siguiente es un ejemplo de un Dockerfile creado por el blueprint.NET 8 (Container Image).

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

WORKDIR /var/task

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

2. aws-lambda-tools-defaults.json

El `aws-lambda-tools-defaults.json` archivo se utiliza para especificar los valores predeterminados del asistente de implementación del Toolkit for Visual Studio y de la CLI de.NET Core. En la siguiente lista se describen los campos que puede configurar en el `aws-lambda-tools-defaults.json` archivo.

- `profile`: establece tu AWS perfil.

- `region`: establece la AWS región en la que se almacenan los recursos.
- `configuration`: establece la configuración utilizada para publicar la función.
- `package-type`: establece el tipo de paquete de despliegue en una imagen de contenedor o en un archivo de archivos.zip.
- `function-memory-size`: establece la asignación de memoria para la función en MB.
- `function-timeout`: El tiempo de espera es la cantidad máxima de tiempo en segundos que puede ejecutarse una función Lambda. Puede ajustarlo en incrementos de 1 segundo hasta un valor máximo de 15 minutos.
- `docker-host-build-output-dir`: establece el directorio de salida del proceso de compilación que se correlaciona con las instrucciones de. `Dockerfile`
- `image-command`: es un nombre completo para su método, el código que desea que ejecute la función Lambda. La sintaxis es la siguiente: `{Assembly}::{Namespace}.{ClassName}::{MethodName}`. Para obtener más información, consulte Firmas de controlador. Si se establece `image-command` aquí, este valor se rellena de forma automática en el asistente de publicación de Visual Studio más adelante.

A continuación, se muestra un ejemplo de un aws-lambda-tools-defaults archivo.json creado mediante el blueprint.NET 8 (Container Image).

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

3. Function.cs

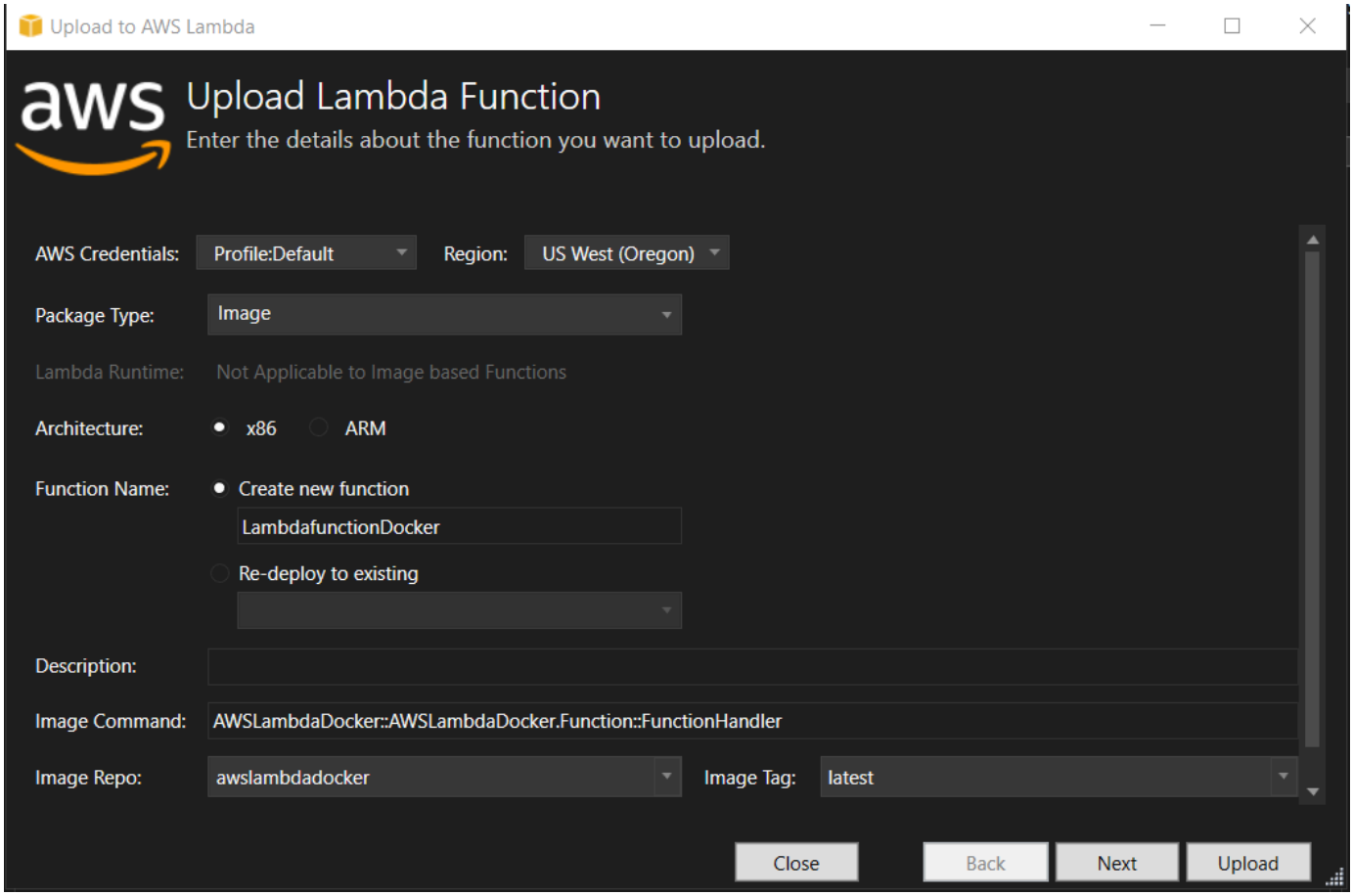
El `Function.cs` archivo define las funciones de c# que se expondrán como funciones Lambda. `FunctionHandler` es la funcionalidad de Lambda que tiene lugar cuando se ejecuta la función de Lambda. En este proyecto, `FunctionHandler` invoca `ToUpper()` el texto introducido.

Publicación en Lambda

Las imágenes de Docker generadas por el proceso de compilación se cargan en Amazon Elastic Container Registry (Amazon ECR). Amazon ECR es un registro de contenedores de Docker completamente gestionado que facilita a los desarrolladores el almacenamiento, la administración y la implementación de imágenes de contenedores de Docker. Amazon ECR aloja la imagen, a la que Lambda hace referencia para proporcionar la funcionalidad Lambda programada cuando se invoca.

Para publicar su función en Lambda

1. En el Explorador de soluciones, abra el menú contextual del proyecto (haga clic con el botón derecho) y, a continuación, seleccione AWS Lambda Publicar en para abrir la ventana Cargar función Lambda.
2. En la página Cargar función Lambda, haga lo siguiente:



a. En Tipo de paquete, se ha seleccionado **`Image`** automáticamente como su tipo de paquete porque el asistente de publicación detectó un `Dockerfile` en su proyecto.

b. En Nombre de la función, introduzca un nombre para mostrar para la instancia de Lambda. Este nombre es el nombre de referencia que aparece tanto en el Explorador de AWS en Visual Studio como en la AWS Management Console.

c. En Descripción, escriba el texto que se mostrará con la instancia en la AWS Management Console.

d. En Comando de imagen, introduzca una ruta completa al método que desee que ejecute la función de Lambda:
`AWSLambdaDocker::AWSLambdaDocker.Function::FunctionHandler`

> **Note**
>
> Cualquier nombre de método que se introduzca aquí anulará cualquier instrucción del CMD en el Dockerfile. Introducir el comando Image es opcional solo SI su `Dockerfile` incluye un `CMD` para indicar cómo iniciar la función de Lambda.

e. En Repositorio de imagen, introduzca el nombre de un Amazon Elastic Container Registry nuevo o existente. La imagen de Docker que crea el proceso de compilación se carga en este registro. La definición de Lambda que se publique hará referencia a esa imagen de Amazon ECR.

f. En Etiqueta de la imagen, introduzca una etiqueta de Docker para asociarla a su imagen en el repositorio.

g. Elija Siguiente.

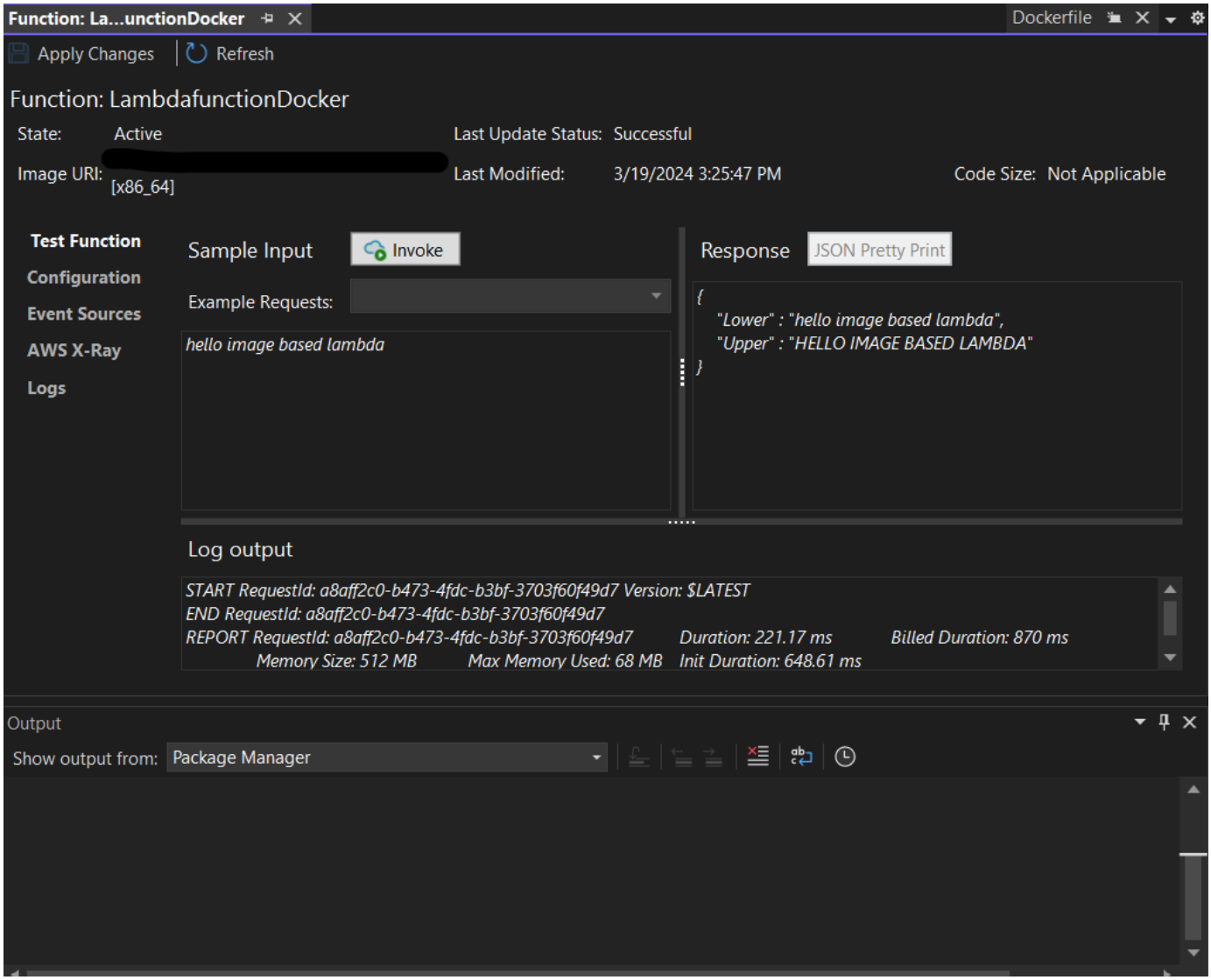
3. En la página Detalles avanzados de la función, en Nombre del rol, elija un rol asociado a su cuenta. El rol se utiliza para proporcionar credenciales temporales para las llamadas a los servicios de Amazon Web Services realizadas por el código en la función. Si no tiene un rol, elija Nuevo rol basado en la política AWS gestionada y, a continuación, elija. AWSLambdaBasicExecutionRole

> **Note**
>
> Su cuenta debe tener permiso para ejecutar la ListPolicies acción de IAM; de lo contrario, la lista de nombres de rol estará vacía.

4. Seleccione Cargar para iniciar los procesos de carga y publicación.

> **Note**
>
> Se mostrará la página Cargando función durante la carga de la función. A continuación, el proceso de publicación crea la imagen en función de los parámetros de configuración, genera el repositorio de Amazon ECR si es necesario, carga la imagen en el repositorio y crea la Lambda que hace referencia al repositorio con esa imagen.
> Una vez cargada la función, se abre la página de Función y muestra la configuración de la nueva función de Lambda.

5. Para invocar manualmente la función de Lambda, en la pestaña Probar función, escriba en el campo de entrada de texto libre de la solicitud y, a continuación, seleccione Invocar. El texto, convertido a mayúsculas, aparecerá en Respuesta.



6. Para ver el repositorio, en el Explorador de AWS , en Amazon Elastic Container Service, seleccione Repositorios.

   Puede volver a abrir Función: acceda en cualquier momento haciendo doble clic en la instancia implementada ubicada en el Explorador de AWS , debajo del nodo AWS Lambda.

> **Note**
>
> Si la ventana del AWS explorador no está abierta, puede acoplarla desde Ver ->AWS Explorador

7. Consulte las opciones de configuración adicionales específicas de la imagen en la pestaña Configuración. Esta pestaña ofrece una forma de anular los datos de `ENTRYPOINT`, `CMD` y `WORKDIR` que pueden haberse especificado en el Dockerfile. Descripción es la descripción que introdujo (de hacerlo) durante la carga o publicación.

Eliminación

Si no va a seguir desarrollando con este ejemplo, recuerde eliminar la función y la imagen de ECR que se implementaron para que no se le facturen los recursos no utilizados de la cuenta.

- Las funciones se pueden eliminar haciendo clic con el botón derecho en la instancia implementada ubicada en el Explorador de AWS , debajo del nodo AWS Lambda.
- Los repositorios se pueden eliminar en el Explorador de AWS , desde Amazon Elastic Container Service -> Repositorios.

Siguientes pasos

Para obtener información sobre cómo crear y probar imágenes de Lambda, consulte Uso de imágenes de contenedor con Lambda.

Para obtener información sobre la implementación de imágenes de contenedores, sus permisos y la anulación de los valores de configuración, consulte Funciones de configuración.

Tutorial: Cree y pruebe una aplicación sin servidor con AWS Lambda

Puede crear una aplicación Lambda sin servidor mediante AWS Toolkit for Visual Studio una plantilla. Las plantillas del proyecto Lambda incluyen una para una aplicación AWS sin servidor, que es la AWS Toolkit for Visual Studio implementación del modelo de aplicaciones AWS sin servidor (SAM).AWS Con este tipo de proyecto, puede desarrollar un conjunto de AWS Lambda funciones e implementarlas con los AWS recursos necesarios como una aplicación completa, que se utiliza AWS CloudFormation para organizar la implementación.

Para obtener información sobre los requisitos previos y la configuración de AWS Toolkit for Visual Studio, consulte Uso de plantillas AWS Lambda en AWS el Toolkit for Visual Studio.

Temas

- Creación de un nuevo proyecto de aplicación sin servidor de AWS

- Revisión de los archivos de la aplicación sin servidor
- Implementación de la aplicación sin servidor
- Prueba de la aplicación sin servidor

Creación de un nuevo proyecto de aplicación sin servidor de AWS

AWS Los proyectos de aplicaciones sin servidor crean funciones Lambda con una AWS CloudFormation plantilla sin servidor. AWS CloudFormation Las plantillas le permiten definir recursos adicionales, como bases de datos, añadir funciones de IAM e implementar varias funciones a la vez. Esto difiere de los proyectos de AWS Lambda, que se centran en desarrollar e implementar una sola función de Lambda.

El siguiente procedimiento describe cómo crear un nuevo proyecto de aplicación AWS sin servidor.

1. En Visual Studio, expanda el menú Archivo, expanda Nuevo y, a continuación, elija Proyecto.
2. En el cuadro de diálogo Nuevo proyecto, asegúrese de que los cuadros desplegables Idioma, Plataforma y Tipo de proyecto estén configurados en «Todos...» e introdúzcalos **`aws lambda`** en el campo de búsqueda.
3. Seleccione la plantilla Aplicación sin servidor de AWS con pruebas (.NET Core - C#).

   > **Note**
   >
   > Es posible que la plantilla AWS Serverless Application with Tests (.NET Core - C#) no aparezca en la parte superior de los resultados.

4. Haga clic en Siguiente para abrir el cuadro de diálogo Configurar su nuevo proyecto.
5. En el cuadro de diálogo Configure su nuevo proyecto, introduzca **`ServerlessPowertools`** el nombre y, a continuación, complete los campos restantes según sus preferencias. Pulse el botón Crear para pasar al cuadro de diálogo de selección de planos.
6. En el cuadro de diálogo Seleccionar esquema, elija Powertools como AWS Lambda plano y, a continuación, elija Finalizar para crear el proyecto de Visual Studio.

Revisión de los archivos de la aplicación sin servidor

En las siguientes secciones se ofrece una visión detallada de los tres archivos de aplicaciones sin servidor creados para el proyecto:

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

1. plantilla sin servidor

Un `serverless.template` archivo es una AWS CloudFormation plantilla para declarar sus funciones sin servidor y otros recursos. AWS El archivo incluido en este proyecto contiene una declaración para una sola función de Lambda que se expondrá a través de Amazon API Gateway como una HTTP `*Get*` operación. Puede editar esta plantilla para personalizar la función existente o añadir más funciones y otros recursos que necesite su aplicación.

A continuación se muestra un ejemplo de un archivo `serverless.template`:

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

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

Observe que muchos de los campos de `...AWS:: Serverless::Function...` declaración son similares a los campos de la implementación de un proyecto de Lambda. El registro, las métricas y el rastreo de Powertools se configuran mediante las siguientes variables de entorno:

- POWERTOOLS_SERVICE_NAME= ServerlessGreeting
- POWERTOOLS_LOG_LEVEL=Información
- POWERTOOLS_LOGGER_CASE= PascalCase
- POWERTOOLS_TRACER_CAPTURE_RESPONSE=Verdadero
- PowerTools_Tracer_Capture_Error=Verdadero
- POWERTOOLS_METRICS_NAMESPACE= ServerlessGreeting

Para obtener definiciones y detalles adicionales sobre las variables de entorno, consulte el sitio web Powertools para obtener referencias. AWS Lambda

2. Functions.cs

`Functions.cs`es un archivo de clase que contiene un método de C# asignado a una sola función declarada en el archivo de plantilla. La función Lambda responde a `HTTP Get` los métodos de API Gateway. A continuación se muestra un ejemplo del `Functions.cs` archivo:

```
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`proporciona los valores predeterminados para el asistente de AWS implementación en Visual Studio y los AWS Lambda comandos agregados a la CLI de.NET

Core. El siguiente es un ejemplo del `aws-lambda-tools-defaults.json` archivo incluido en este proyecto:

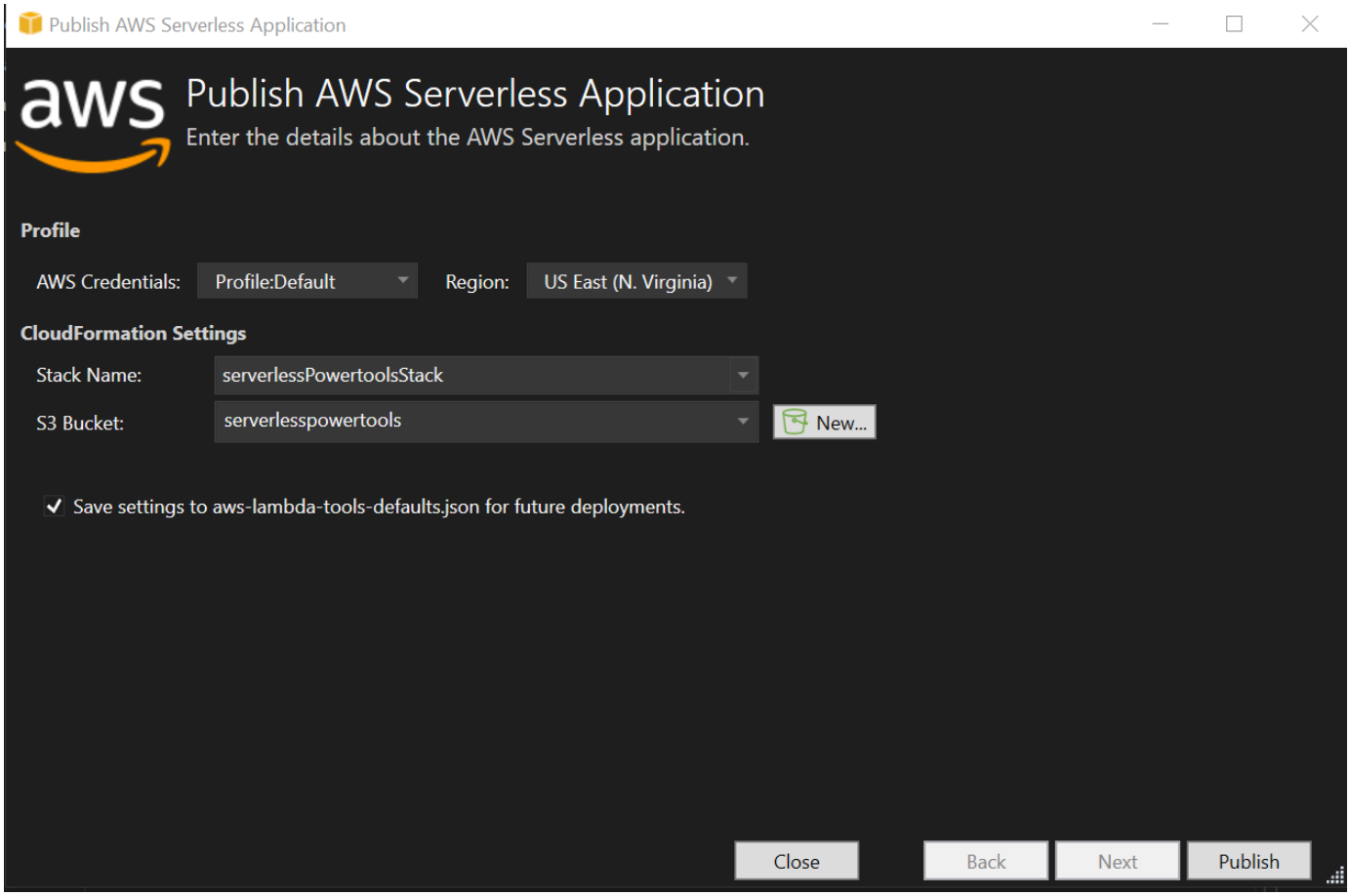
```
{
  "profile": "Default",
  "region": "us-east-1",
  "configuration": "Release",
  "s3-prefix": "ServerlessPowertools/",
  "template": "serverless.template",
  "template-parameters": ""
}
```

Implementación de la aplicación sin servidor

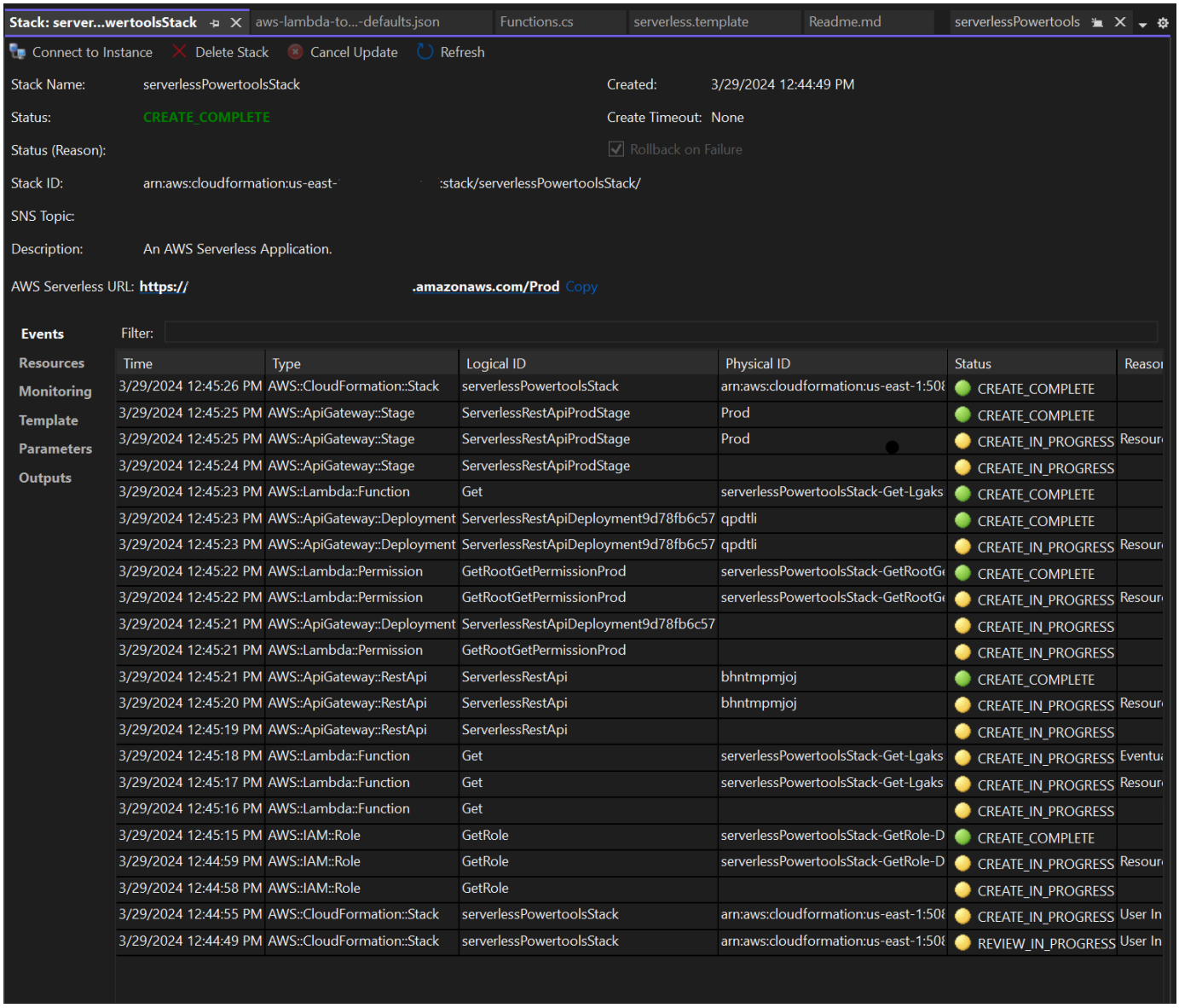
Para implementar su aplicación sin servidor, complete los siguientes pasos

1. En el Explorador de soluciones, abra el menú contextual del proyecto (haga clic con el botón derecho) y seleccione Publicar en AWS Lambda para abrir el cuadro de diálogo Publicar aplicación AWS sin servidor.
2. En el cuadro de diálogo Publicar una aplicación AWS sin servidor, introduzca un nombre para el contenedor de la AWS CloudFormation pila en el campo Nombre de la pila.
3. En el campo Bucket de S3, elija un depósito de Amazon S3 en el que se cargará el paquete de aplicaciones o elija Nuevo... pulse e introduzca el nombre de un nuevo bucket de Amazon S3. A continuación, seleccione Publicar para publicar e implementar la aplicación.

> **Note**
>
> La AWS CloudFormation pila y el bucket de Amazon S3 deben estar en la misma AWS región. El resto de los ajustes del proyecto se definen en el `serverless.template` archivo.



4. La ventana de vista de pila se abre durante el proceso de publicación. Cuando se completa la implementación, el campo Estado muestra:`CREATE_COMPLETE`.



Prueba de la aplicación sin servidor

Cuando se complete la creación de la pila, podrá ver la aplicación mediante la URL AWS sin servidor. Si ha completado este tutorial sin agregar funciones o parámetros adicionales, al acceder a su URL AWS sin servidor, se muestra la siguiente frase en su navegador web:. `Hello Powertools for AWS Lambda (.NET)`

Tutorial: creación de una aplicación de Lambda con Amazon Rekognition

En este tutorial se muestra cómo crear una aplicación de Lambda que utilice Amazon Rekognition para etiquetar objetos de S3 con las etiquetas detectadas.

Para obtener información sobre los requisitos previos y la configuración de AWS Toolkit for Visual Studio, consulte Uso de plantillas AWS Lambda en AWS el Toolkit for Visual Studio.

Creación de un proyecto Image Rekognition de Lambda con .NET Core

El siguiente procedimiento describe cómo crear una aplicación Amazon Rekognition Lambda a partir del. AWS Toolkit for Visual Studio

> **Note**
>
> Tras su creación, la aplicación tiene una solución con dos proyectos: el proyecto fuente que contiene el código de la función de Lambda para implementarlo en Lambda y un proyecto de prueba que utiliza xUnit para probar la función localmente.
> A veces, Visual Studio no puede encontrar todas las NuGet referencias de sus proyectos. Esto se debe a que los blueprints requieren dependencias de las que hay que recuperar. NuGet Cuando se crean nuevos proyectos, Visual Studio solo extrae referencias locales y no referencias remotas. NuGet Para corregir NuGet errores: haga clic con el botón derecho en las referencias y seleccione Restaurar paquetes.

1. En Visual Studio, expanda el menú Archivo, expanda Nuevo y, a continuación, elija Proyecto.
2. En el cuadro de diálogo Nuevo proyecto, asegúrese de que los cuadros desplegables Idioma, Plataforma y Tipo de proyecto estén configurados en «Todos...» e introdúzcalos **`aws lambda`** en el campo de búsqueda.
3. Seleccione la plantilla AWS Lambda With Tests (.NET Core - C#).
4. Haga clic en Siguiente para abrir el cuadro de diálogo Configurar su nuevo proyecto.
5. En el cuadro de diálogo Configure su nuevo proyecto, introduzca ImageRekognition «» como nombre y, a continuación, complete los campos restantes según sus preferencias. Pulse el botón Crear para pasar al cuadro de diálogo de selección de planos.
6. En el cuadro de diálogo Seleccionar esquema, elija el esquema Detectar etiquetas de imagen y, a continuación, elija Finalizar para crear el proyecto de Visual Studio.

> **Note**
>
> Este esquema proporciona código para escuchar los eventos de Amazon S3 y utiliza Amazon Rekognition para detectar etiquetados y añadirlos al objeto de S3 como etiquetas.

Revisión de los archivos del proyecto

En las siguientes secciones se examinan estos archivos de proyecto:

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

1. Function.cs

Dentro del `Function.cs` archivo, el primer segmento de código es el atributo de ensamblaje, ubicado en la parte superior del archivo. De forma predeterminada, Lambda solo acepta parámetros de entrada y tipos de retorno. `System.IO.Stream` Debe registrar un serializador para usar clases mecanografiadas para los parámetros de entrada y los tipos de retorno. El atributo assembly registra el serializador JSON de Lambda, que se utiliza `Newtonsoft.Json` para convertir flujos en clases mecanografiadas. Puede definir el serializador en el nivel del conjunto o del método.

A continuación, se muestra un ejemplo del atributo assembly:

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

La clase tiene dos constructores. El primero es un constructor predeterminado que se utiliza cuando Lambda invoca la función. Este constructor crea los clientes de los servicios Amazon S3 y Amazon Rekognition. El constructor también recupera las AWS credenciales de estos clientes de la función de IAM que usted asigna a la función al implementarla. La AWS región de los clientes se establece en la región en la que se ejecuta la función Lambda. En este blueprint, solo desea añadir etiquetas al objeto de Amazon S3 si el servicio Amazon Rekognition tiene un nivel mínimo de confianza en la etiqueta. Este constructor comprueba la variable de entorno `MinConfidence` para determinar

el nivel de confianza aceptable. Puede configurar esta variable de entorno cuando implemente la función de Lambda.

A continuación, se muestra un ejemplo del constructor de primera clase de: `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}");
    }
}
```

El siguiente ejemplo demuestra cómo se puede utilizar el segundo constructor para realizar pruebas. El proyecto de prueba configura sus propios clientes S3 y Rekognition y los pasa a:

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

A continuación, se muestra un ejemplo del `FunctionHandler` método incluido en el archivo. `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` es el método al que Lambda llama después de construir la instancia. Observe que el parámetro de entrada es de tipo `S3Event` y no `Stream`. Puede hacerlo gracias al serializador JSON de Lambda registrado. El `S3Event` contiene toda la información acerca del evento activado en S3. La función recorre cíclicamente todos los objetos de S3 que forman parte del evento e indica a Rekognition que detecte etiquetas. Una vez que las etiquetas se han detectado, se añaden como etiquetas al objeto de S3.

> **Note**
>
> El código contiene llamadas a`Console.WriteLine()`. Cuando la función se ejecuta en Lambda, todas las llamadas se `Console.WriteLine()` redirigen a Amazon CloudWatch Logs.

2. aws-lambda-tools-defaults.json

El `aws-lambda-tools-defaults.json` archivo contiene los valores predeterminados que el blueprint ha establecido para rellenar previamente algunos de los campos del asistente de despliegue. También resulta útil para configurar las opciones de línea de comandos para la integración con la CLI de.NET Core.

Para acceder a la integración de la CLI de.NET Core, navegue hasta el directorio del proyecto de la función y escriba**`dotnet lambda help`**.

> **Note**
>
> El controlador de funciones indica a qué método debe llamar Lambda en respuesta a la función invocada. El formato de este campo es:. `<assembly-name>::<full-type-name>::<method-name>` El espacio de nombres debe incluirse con el nombre del tipo.

Implementación de la función

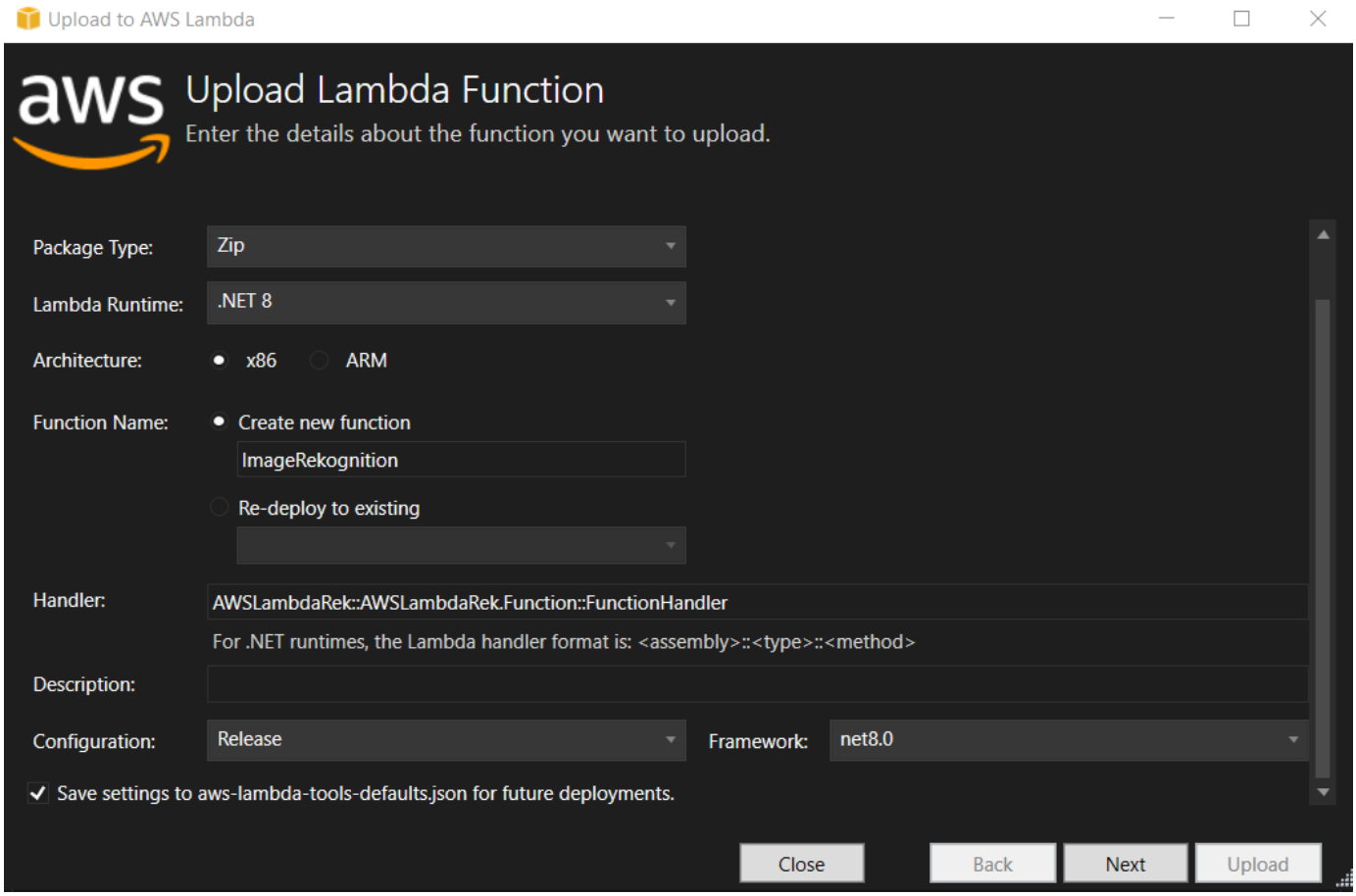
El siguiente procedimiento describe cómo implementar la función Lambda.

1. En el Explorador de soluciones, haga clic con el botón derecho en el proyecto de Lambda y seleccione Publicar en AWS Lambda para abrir la ventana Cargar a. AWS Lambda

   > **Note**
   >
   > Los valores preestablecidos se recuperan del `aws-lambda-tools-defaults.json` archivo.

2. En la AWS Lambda ventana Cargar a, introduzca un nombre en el campo Nombre de la función y, a continuación, pulse el botón Siguiente para acceder a la ventana de detalles avanzados de la función.

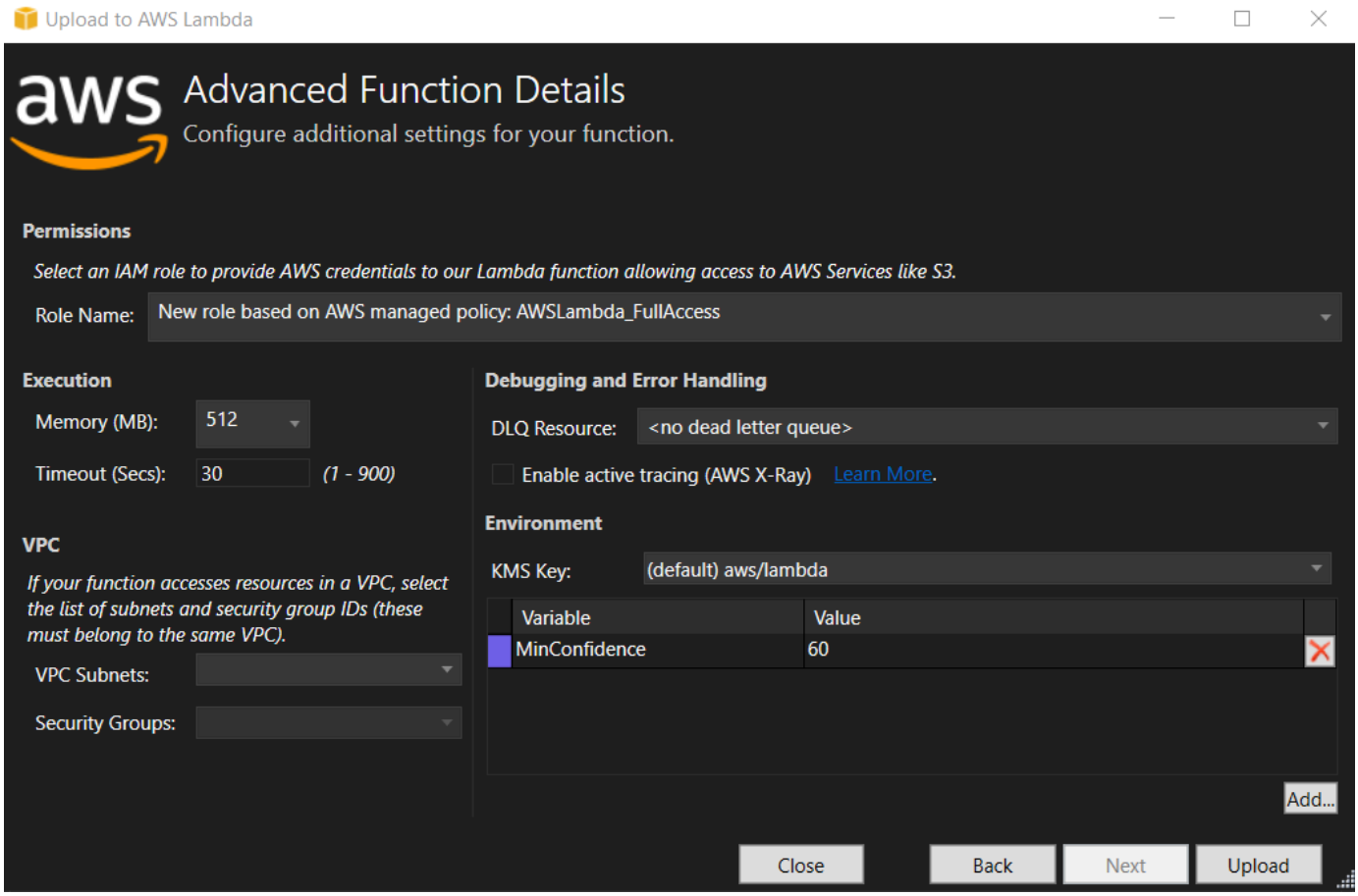
   > **Note**
   >
   > En este ejemplo, se utiliza el nombre de la función**`ImageRekognition`**.



3. En la ventana Detalles de funciones avanzadas, seleccione un rol de IAM que dé permiso para que su código acceda a sus recursos de Amazon S3 y Amazon Rekognition.

> **Note**
>
> Si sigue este ejemplo, seleccione el rol. `AWSLambda_FullAccess`

4. Establezca la variable de entorno en 60 y, `MinConfidence` a continuación, seleccione Cargar para iniciar el proceso de implementación. El proceso de publicación finaliza cuando se muestra la vista de funciones en el AWS explorador.



5. Tras una implementación exitosa, configure Amazon S3 para que envíe sus eventos a su nueva función desde la pestaña Fuentes de eventos.
6. En la pestaña Fuentes de eventos, pulse el botón Añadir y, a continuación, seleccione el bucket de Amazon S3 que desee conectar con su función Lambda.

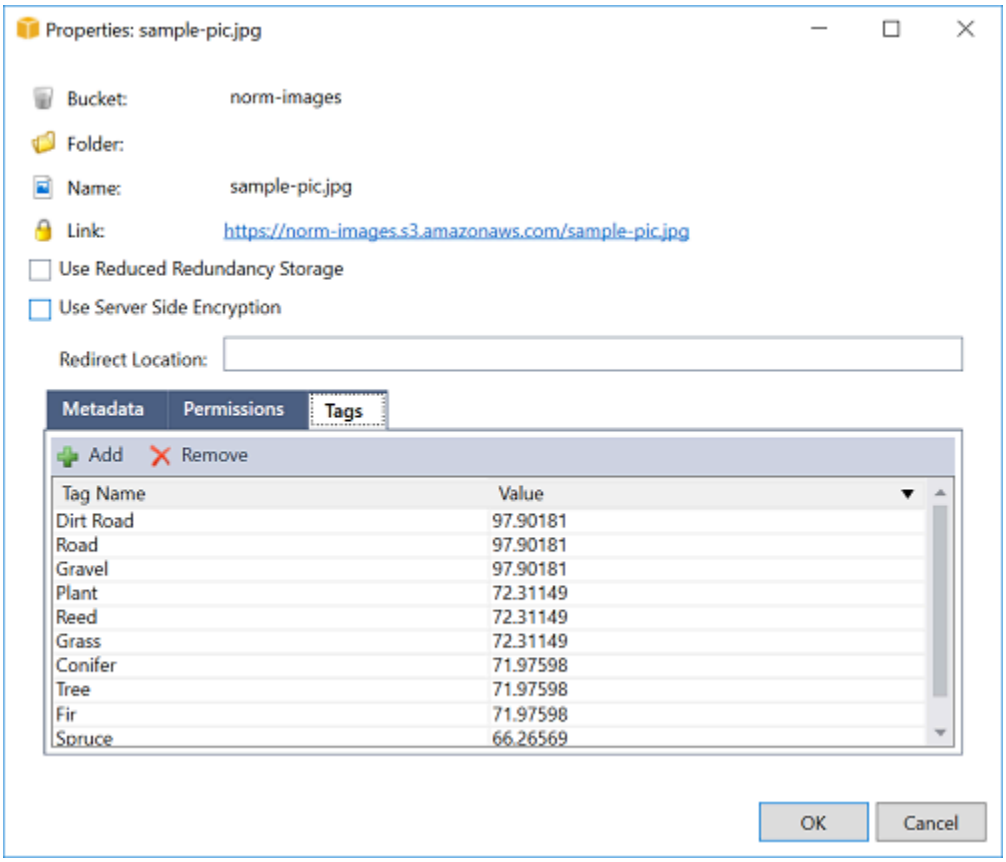
> **Note**
>
> El depósito debe estar en la misma AWS región que la función Lambda.

Prueba de la función

Ahora que la función se ha implementado y que se ha configurado un bucket de S3 como origen de eventos para ella, abra el navegador de buckets de S3 desde el Explorador de AWS para el bucket seleccionado. A continuación, cargue algunas imágenes.

Cuando se haya completado la carga, puede confirmar que su función se ha ejecutado comprobando los registros en la vista de la función. O bien, haga clic con el botón derecho del ratón en las

imágenes del navegador del bucket y elija Properties (Propiedades). En la pestaña Tags (Etiquetas), puede ver las etiquetas que se han aplicado al objeto.



Tutorial: Uso de Amazon Logging Frameworks AWS Lambda para crear registros de aplicaciones

Puedes usar Amazon CloudWatch Logs para monitorear, almacenar y acceder a los registros de tu aplicación. Para incluir los datos de registro en CloudWatch Logs, utilice un AWS SDK o instale el agente de CloudWatch Logs para supervisar determinadas carpetas de registro. CloudWatch Logs está integrado con varios marcos de registro populares de.NET, lo que simplifica los flujos de trabajo.

Para empezar a trabajar con CloudWatch Logs y los marcos de registro de.NET, añada el NuGet paquete y la fuente de salida de CloudWatch Logs adecuados a su aplicación y, a continuación, utilice la biblioteca de registros como lo haría normalmente. Esto permite a la aplicación registrar los mensajes con su framework de.NET, enviarlos a CloudWatch Logs y mostrar los mensajes de registro de la aplicación en la consola de CloudWatch Logs. También puede configurar métricas y alarmas desde la consola de CloudWatch registros, en función de los mensajes de registro de la aplicación.

Los marcos de registro de.NET compatibles incluyen:

- nLog: para verlo, consulte el paquete nLog de nuget.org.
- Log4net: Para verlo, consulte el paquete Log4net de nuget.org.
- Marco de registro de ASP.NET Core: para verlo, consulte el paquete de marco de registro ASP.NET Core de nuget.org.

A continuación se muestra un ejemplo de un `NLog.config` archivo que permite tanto a CloudWatch los registros como a la consola como salida para los mensajes de registro añadiendo el `AWS.Logger.NLog` NuGet paquete y el destino a ellos. 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>
```

Todos los complementos de registro se basan en las AWS credenciales AWS SDK for .NET y las autentican mediante un proceso similar al del SDK. En el siguiente ejemplo, se detallan los permisos que requieren las credenciales del complemento de registro para acceder a CloudWatch los registros:

> **Note**
>
> Los complementos de registro AWS de.NET son un proyecto de código abierto. Para obtener información, ejemplos e instrucciones adicionales, consulte los temas de ejemplos e instrucciones del GitHub repositorio AWS Logger.NET.

```
{
```

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

Implementación en AWS

El Toolkit for Visual Studio permite el despliegue de aplicaciones enAWS Elastic Beanstalk contenedores oAWS CloudFormation pilas.

> **Note**
>
> Si está utilizando Visual Studio Express Edition:
>
> - Puede usar la CLI de Docker para implementar aplicaciones en contenedores de Amazon ECS.
> - Puede usar la consolaAWS de administración para implementar aplicaciones en contenedores de Elastic Beanstalk.
>
> Para las implementaciones de Elastic Beanstalk, primero debe crear un paquete de implementación web. Para obtener más información, consulte Cómo: Crear un paquete de implementación web en Visual Studio. Para la implementación de Amazon ECS, debe tener una imagen de Docker. Para obtener más información, consulte Visual Studio Tools para Docker.

Temas

Trabajo con Publicación enAWSen Visual Studio Studio Studio

Publicación enAWSes una experiencia de implementación interactiva que le ayuda a publicar sus aplicaciones.NET enAWSdestinos de implementación, con soporte de aplicaciones de .NET Core 3.1 3.1 y posterior. Trabajo con Publicación enAWSmantiene el flujo de trabajo dentro de Visual Studio al hacer que estas funciones de implementación estén disponibles, directamente desde su IDE:

- La capacidad de implementar la aplicación con un solo clic.

- Recomendaciones de implementación basadas en su aplicación.
- Creación automática de Dockerfile, según sea relevante y requerido por el entorno de destino de la implementación (destino de implementación).
- Configuración optimizada para crear y empaquetar sus aplicaciones, según lo requiera el objetivo de implementación.

> **Note**
>
> Para obtener información adicional sobre la publicación de aplicaciones de.NET Framework, consulte la guíaCreación e implementación de aplicaciones .NET en Elastic Beanstalk También puede acceder a Publicación enAWSde la CLI de .NET. Para obtener más información, consulte laImplementar aplicaciones .NET enAWSguide.

Temas

Requisitos previos

Para publicar correctamente las aplicaciones.NET en unAWS, instale lo siguiente en el dispositivo local:

- .NET Core 3.1+ (que incluye .NET5 y .NET6): Para obtener información adicional sobre estos productos e información de descarga, visite laSitio de descargas de Microsoft.
- Node.js 14.x 14.x versión posterior: Se necesita Node.js para ejecutarAWS Cloud Development Kit (AWS CDK). Para descargar u obtener más información sobre Node.js, visite laNode.js sitio de descarga.

> **Note**
>
> Publicación enAWSutilizaAWS CDKpara implementar su aplicación y toda su infraestructura de implementación como un solo proyecto. Para obtener más información acerca deAWS CDKconsulte lasCloud Development Kitguide.

- (Opcional) Docker se utiliza cuando se implementa en un servicio basado en contenedores, como Amazon ECS. Para obtener más información y descargar Docker, consulte la sección de Docker enDocker descargar Dockersitio:.

Tipos de aplicaciones admitidos

Antes de publicar en un destino nuevo o existente, comience por crear o abrir uno de los siguientes tipos de proyectos en Visual Studio:

- Aplicación de ASP.NET Core en
- Aplicación de consola .NET
- Blazor WebAssembly aplicación

Publicación de aplicaciones enAWSdestinos

Al publicar en un nuevo destino, Publicar enAWSle guiará durante el proceso, haciendo recomendaciones y utilizando configuraciones comunes. Si necesita publicar en un destino que se configuró anteriormente, sus preferencias se almacenan y se pueden ajustar, o están disponibles inmediatamente para la implementación con un solo clic.

Publicar en un nuevo objetivo

A continuación se describe cómo configurar la publicación enAWSpreferencias de implementación, cuando publica en un nuevo destino.

1. De lasAWSExplorador, expanpanda las opcionesCredencialesmenú desplegable y elijaAWSperfil que corresponde a la región yAWSlos servicios que se requieren para la implementación.
2. Expanda la capacidadRegiónmenú desplegable y elijaAWSregión que contiene elAWSservicios que son necesarios para la implementación.
3. De Visual Studio StudioExplorador de solucionesabra el menú contextual (con el botón derecho) del nombre del proyecto y elijaPublicación enAWS. Esto se abriráPublicación enAWS.
4. DesdePublicación enAWS, eligePublicación en New Targetpara configurar una nueva implementación.

> **Note**
>
> Para modificar las credenciales de implementación predeterminadas, seleccione o haga clic en elEditarenlace ubicado junto a laCredencialessección, enPublicación enAWS. Para omitir el proceso de configuración de destino, seleccionePublicar en un objetivo existentey, a continuación, elija la configuración que prefiera de la lista de los destinos de implementación anteriores.

5. De lasPublicación de Destinos enpanel, elija un panelAWSservicio para administrar la implementación de su aplicación.
6. Cuando esté satisfecho con la configuración elijaPublicaciónpara iniciar el proceso de implementación.

> **Note**
>
> Tras iniciar un despliegue,Publicación enAWSmuestra las siguientes actualizaciones de estado:
>
> - Durante el proceso de despliegue,Publicación enAWSmuestra información sobre el progreso de la implementación.
> - Tras el proceso de implementación,Publicación enAWSindica si la implementación de la implementación se ha realizado correctamente o
> - Tras una implementación exitosa, elRecursosofrece información adicional sobre el recurso que se creó. Esta información variará en función del tipo de configuración de la implementación y la aplicación.

Publicar en un objetivo existente

A continuación se describe cómo volver a publicar la aplicación.NET en unAWStarget.

1. De lasAWSExplorador, expanpanda las opcionesCredencialesmenú desplegable y elijaAWSperfil que corresponde a la región yAWSlos servicios que se requieren para la implementación.
2. Expanda la capacidadRegiónmenú desplegable y elijaAWSregión que contiene elAWSservicios que son necesarios para la implementación.

3. De Visual Studio StudioExplorador de soluciones, haga clic con el botón derecho del ratón en el nombre del proyectoPublicación enAWSabrirPublicación enAWS.
4. DesdePublicación enAWS, eligePublicar en un objetivo existentepara seleccionar el entorno de implementación de una lista de destinos existentes.

> **Note**
>
> Si ha publicado recientemente alguna solicitud enAWSCloud, esas aplicaciones se muestran en Publicar enAWS.

5. Seleccione el destino de publicación en el que desea implementar la aplicación y haga clic enPublicaciónpara iniciar el proceso de implementación.

Implementación de unAWS LambdaProyectos con la CLI de .NET Core

AWS Toolkit for Visual Studio incluye plantillas de proyecto de AWS Lambda .de NET Core para Visual Studio. Puede implementar funciones de Lambda creadas en Visual Studio usando la interfaz de línea de comandos (CLI) de .NET Core.

Temas

- Requisitos previos
- Temas relacionados
- Lista de los comandos de Lambda disponibles a través de la CLI de .NET Core
- Publicación de un proyecto de .NET Core Lambda desde la CLI de .NET Core

Requisitos previos

Antes de trabajar con la CLI de .NET Core para implementar funciones de Lambda, debe cumplir los siguientes requisitos previos:

- Asegúrese de que Visual Studio 2015 Update 3 de esté instalado.
- Instalar.NET Core para Windows.
- Configure la CLI de .NET Core para que funcione con Lambda. Para obtener más información, consulteCLI de .NET Coreen laAWS LambdaGuía para desarrolladores.

- Instalar Toolkit for Visual Studio. Para obtener más información, consulte Instalación del AWS Toolkit for Visual Studio.

Temas relacionados

Los siguientes temas relacionados pueden ser útiles a la hora de usar la CLI de .NET Core para implementar funciones de Lambda:

- Para obtener más información sobre las funciones de Lambda, consulte¿Qué es ?AWSLambdaen laAWS LambdaGuía para desarrolladores.
- Para obtener información acerca de la creación de funciones de Lambda en Visual Studio, consulteAWS Lambda.
- Para obtener más información acerca de Microsoft .NET Core, consulte.NET Coreen la documentación en línea de Microsoft.

Lista de los comandos de Lambda disponibles a través de la CLI de .NET Core

Para obtener una lista de los comandos Lambda que están disponibles a través de la interfaz de línea de comandos (CLI) de .NET Core

1. Abra una ventana de símbolo del sistema y vaya a la carpeta que contiene un proyecto de creado con .NET Core Lambda de Visual Studio.
2. Escriba `dotnet lambda --help`.

```
C:\Lambda\AWSLambda1\AWSLambda1>dotnet lambda --help
    AWS Lambda Tools for .NET Core functions
    Project Home: https://github.com/aws/aws-lambda-dotnet
    .
    Commands to deploy and manage Lambda functions:
    .
            deploy-function         Deploy the project to Lambda
            invoke-function         Invoke the function in Lambda with an optional
 input
            list-functions          List all of your Lambda functions
            delete-function         Delete a Lambda function
```

```
            get-function-config     Get the current runtime configuration for a Lambda
function
            update-function-config  Update the runtime configuration for a Lambda
function
   .
   Commands to deploy and manage AWS serverless applications using AWS CloudFormation:
   .
            deploy-serverless       Deploy an AWS serverless application
            list-serverless         List all of your AWS serverless applications
            delete-serverless       Delete an AWS serverless application
   .
   Other Commands:
   .
            package                 Package a Lambda project into a .zip file ready for
deployment
   .
   To get help on individual commands, run the following:

            dotnet lambda help <command>
```

Publicación de un proyecto de .NET Core Lambda desde la CLI de .NET Core

En las siguientes instrucciones, se presupone que ha creado una función de .NET Core de AWS Lambda en Visual Studio.

1. Abra una ventana de símbolo del sistema y vaya a la carpeta que contiene el proyecto de creado con .NET Core Lambda de Visual Studio.
2. Escriba `dotnet lambda deploy-function`.
3. Cuando se le pida, escriba el nombre de la función que desee implementar. Puede ser un nombre nuevo o el nombre de una función ya existente.
4. Cuando se le pida, escriba elAWSRegión (la región en la que se implementará su función Lambda).
5. Cuando se le pida, seleccione o cree el rol de IAM que Lambda asumirá al ejecutar la función.

Cuando la ejecución finaliza correctamente, se muestra el mensaje New Lambda function created (Se ha creado una nueva función Lambda).

```
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
```

Si implementa una función que ya existe, la función de implementación solo pedirá elAWSRegión .

```
C:\Lambda\AWSLambda1\AWSLambda1>dotnet lambda deploy-function
Executing publish command
Deleted previous publish folder
... invoking 'dotnet publish', working folder 'C:\Lambda\AWSLambda1\AWSLambda1\bin
\Release\netcoreapp1.0\publish'
... publish: Publishing AWSLambda1 for .NETCoreApp,Version=v1.0
... publish: Project AWSLambda1 (.NETCoreApp,Version=v1.0) was previously compiled.
 Skipping compilation.
... publish: publish: Published to C:\Lambda\AWSLambda1\AWSLambda1\bin\Release
\netcoreapp1.0\publish
... publish: Published 1/1 projects successfully
```

```
Zipping publish folder C:\Lambda\AWSLambda1\AWSLambda1\bin\Release
\netcoreapp1.0\publish to C:\Lambda\AWSLambda1\AWSLamb
da1\bin\Release\netcoreapp1.0\AWSLambda1.zip
Enter Function Name: (AWS Lambda function name)
DotNetCoreLambdaTest
Enter AWS Region: (The region to connect to AWS services)
us-west-2
Updating code for existing function
```

Una vez que la función Lambda se haya implementado, estará lista para el uso. Para obtener más información, consulteEjemplos de cómo utilizarAWSLambda:.

Lambda monitoriza automáticamente las funciones de Lambda e informa sobre las métricas a través de Amazon CloudWatch. Para monitorizar y resolver problemas de la función Lambda, consulteSolución de problemas y monitorizaciónAWSFunciones de Lambda con Amazon CloudWatch.

Implementar en Elastic Beanstalk

AWS Elastic Beanstalkes un servicio que simplifica el proceso de aprovisionamientoAWSrecursos para su aplicación. Elastic Beanstalk proporciona todos losAWSinfraestructura necesaria para implementar su aplicación. Esta infraestructura incluye:

- Las instancias Amazon EC2 que alojan los ejecutables y el contenido de su aplicación.
- Un grupo de Auto Scaling para mantener el número correcto de instancias Amazon EC2 para garantizar la compatibilidad con su aplicación.
- Un balanceador de carga de Elastic Load Balancing que dirija el tráfico entrante a la instancia Amazon EC2 con más ancho de banda.

El Toolkit for Visual Studio proporciona un asistente que simplifica la publicación de aplicaciones a través de Elastic Beanstalk. Este asistente se describe en las secciones siguientes.

Para obtener más información acerca de Elastic Beanstalk, consulteDocumentación de Elastic Beanstalk.

Temas

- Implemente una aplicación ASP.NET tradicional en Elastic Beanstalk
- Implementación de una aplicación ASP.NET Core en Elastic Beanstalk (Legacy)

- Cómo especificar elAWSCredenciales de seguridad para una aplicación
- Cómo volver a publicar su aplicación en un entorno de Elastic Beanstalk (Legacy)
- Implementaciones personalizadas de aplicaciones de Elastic Beanstalk
- Implementaciones personalizadas de ASP.NET Core Elastic Beanstalk
- Support varias aplicaciones para .NET y Elastic Beanstalk

Implemente una aplicación ASP.NET tradicional en Elastic Beanstalk

En esta sección se describe cómo usar el asistente Publicar en Elastic Beanstalk, incluido como parte del kit de herramientas de Visual Studio, para implementar una aplicación a través de Elastic Beanstalk. Para practicar, puede utilizar una instancia de un proyecto de inicio de aplicación web creado en Visual Studio o usar su propio proyecto.

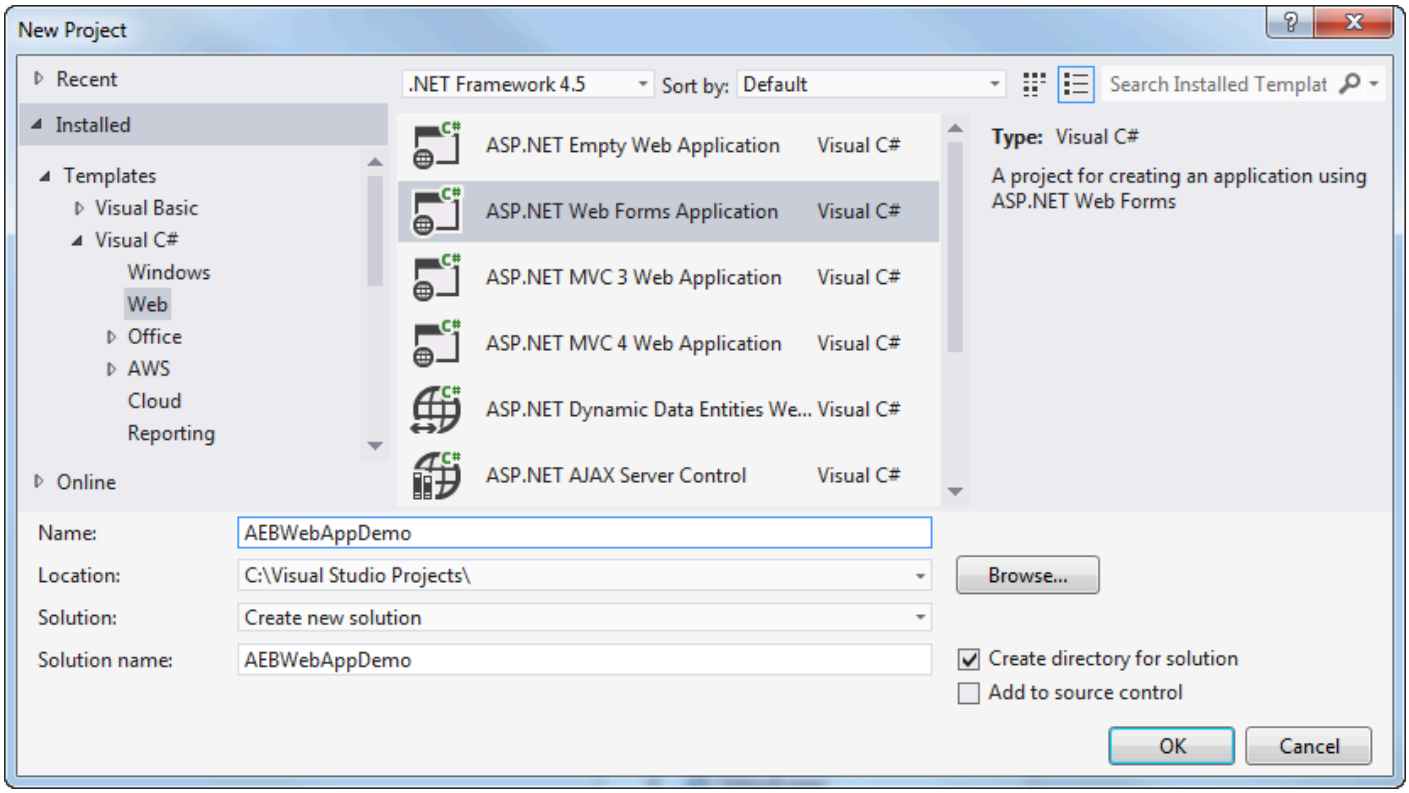
> **Note**
>
> El asistente también es compatible con la implementación de aplicaciones ASP.NET Core. Para obtener información sobre ASP.NET Core, consulte la guía de herramientas de implementación deAWS .NET y laAWS tabla de contenido actualizada de Implementación en.

> **Note**
>
> Para poder utilizar el asistente Publish to Elastic Beanstalk (Publicar en Elastic Beanstalk), debe descargar e instalar Web Deploy. El asistente se basa en Web Deploy para implementar aplicaciones web y páginas web en servidores web de Internet Information Services (IIS).

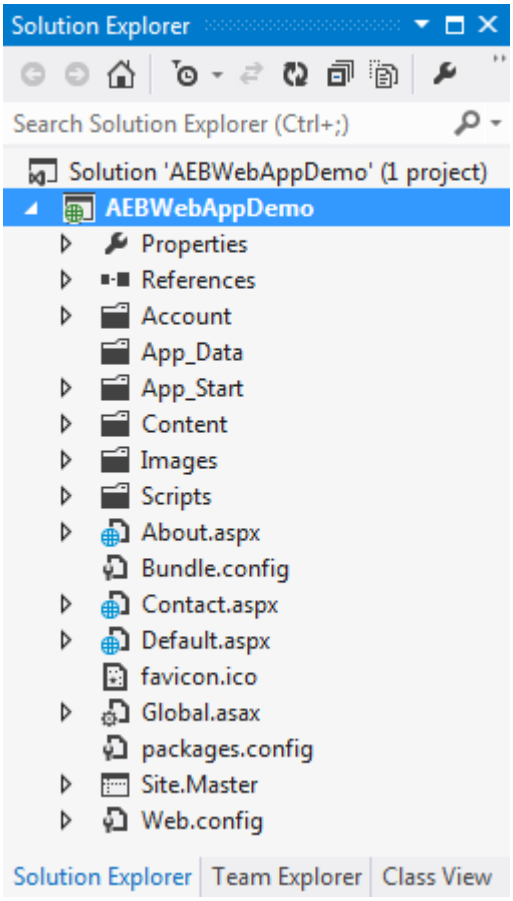
Para crear un proyecto de inicio de aplicación web de muestra

1. En Visual Studio, desde el menú File (Archivo), elija New (Nuevo) y, a continuación, elija Project (Proyecto).
2. En el panel de navegación del cuadro de diálogo Nuevo proyecto, expanda Instalado, expanda Plantillas, expanda Visual C# y, a continuación, elija Web.

3. En la lista de plantillas de proyectos web, elija cualquier plantilla que contenga las palabras `Web` y `Application` en su descripción. Para este ejemplo, elija ASP.NET Web Forms Application (Aplicación de formularios Web Forms ASP.NET).

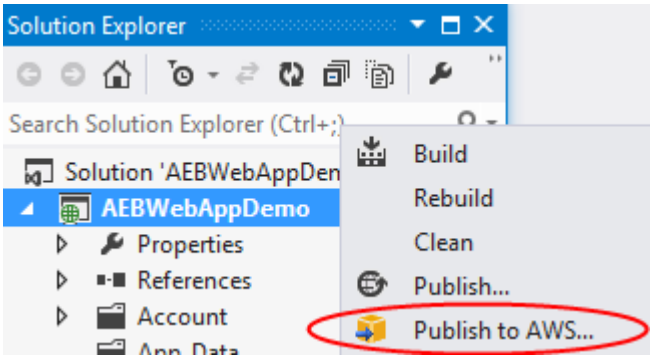


4. En el cuadro Name (Nombre), escriba `AEBWebAppDemo`.
5. En el cuadro Location (Ubicación), escriba la ruta hasta una carpeta de soluciones en su equipo de desarrollo o elija (Examinar) y, a continuación, busque y elija una carpeta de soluciones y elija Select Folder (Seleccionar carpeta).
6. Confirme que se ha seleccionado el cuadro Crear directorio para la solución. En la lista desplegable Solution (Solución), confirme que se ha seleccionado Create new solution (Crear solución nueva) y, a continuación, elija OK (Aceptar). Visual Studio creará una solución y un proyecto basados en la plantilla del proyecto ASP.NET Web Forms Application. Visual Studio mostrará, a continuación, Solution Explorer donde aparecerán la solución y el proyecto nuevos.

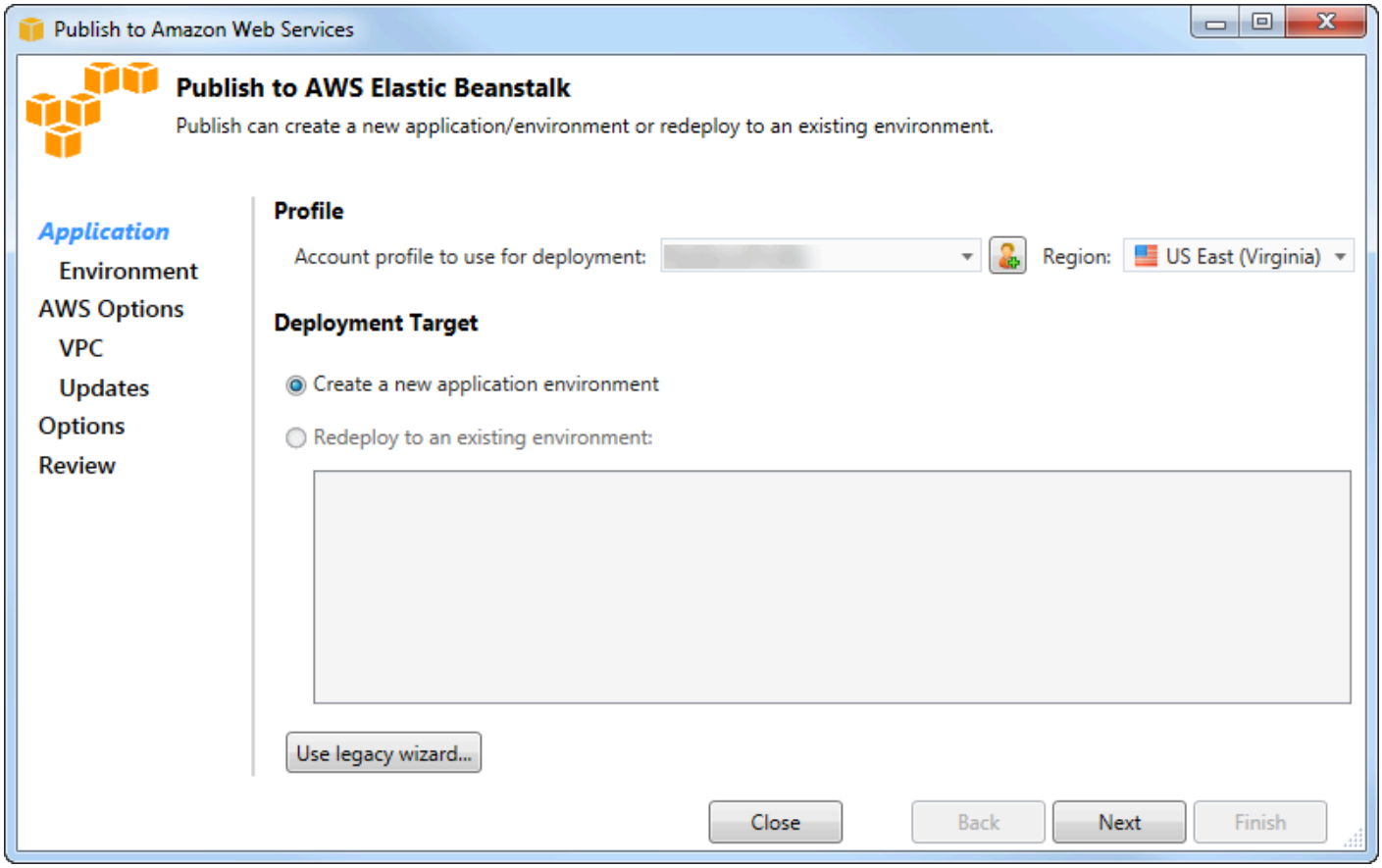


Para implementar una aplicación utilizando el asistente Publish to Elastic Beanstalk

1. En el Explorador de soluciones, abra el menú contextual (haga clic con el botón derecho) de la carpeta de proyectos de AEBWebAppDemo del proyecto que creó en la sección anterior o abra el menú contextual de la carpeta de proyectos de su propia aplicación y elija Publicar enAWS Elastic Beanstalk.



   Aparece el asistente Publish to Elastic Beanstalk (Publicar en Elastic Beanstalk).



2. En Perfil, en la lista desplegable Perfil de cuenta que se usará en la implementación, elija el perfil deAWS cuenta que desea usar para la implementación.

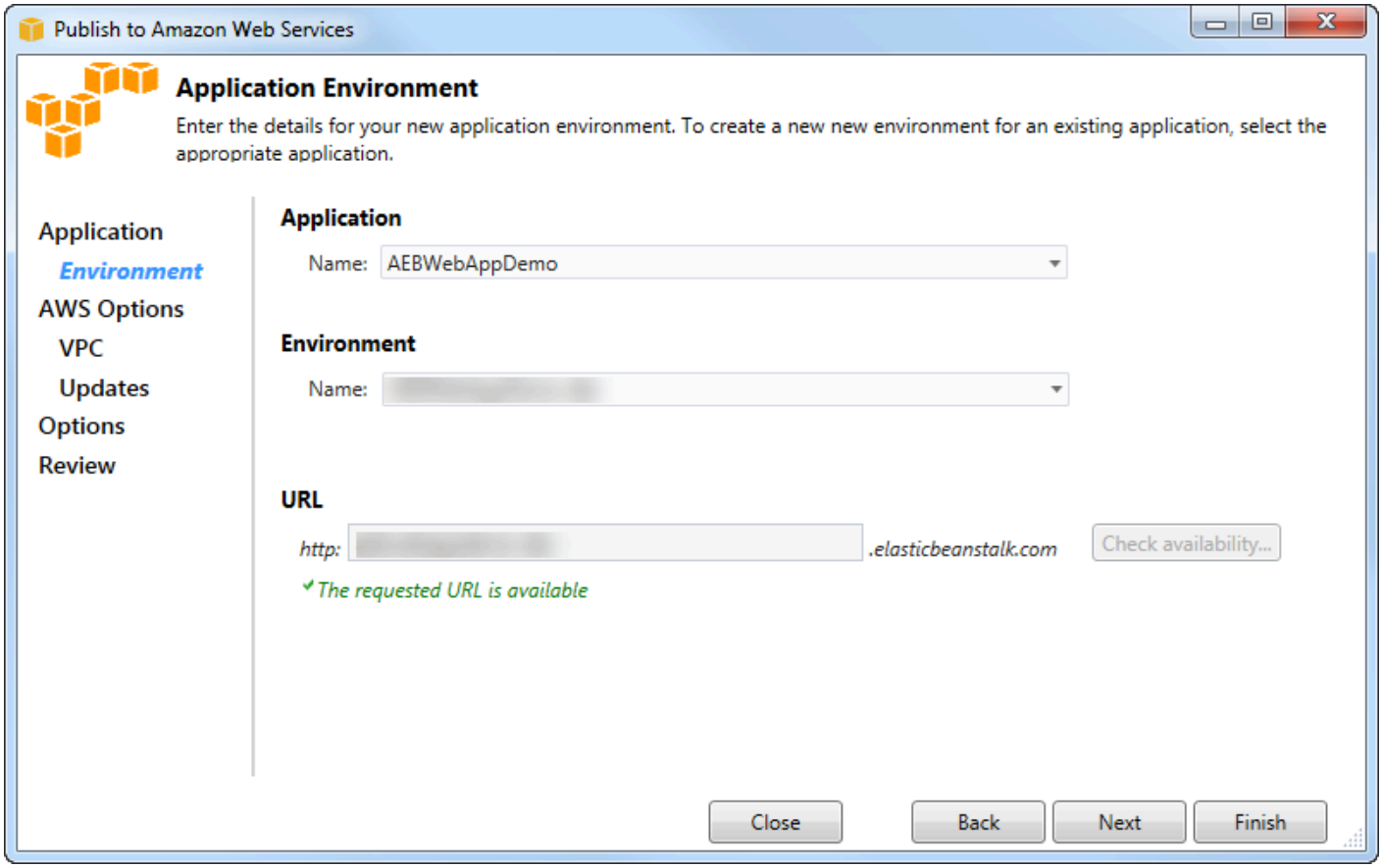
   De manera opcional, si tienes unaAWS cuenta que quieres usar, pero aún no has creado unAWS perfil para ella, puedes elegir el botón con el símbolo más (+) para añadir un perfil deAWS cuenta.

3. En la lista desplegable Región, elija la región en la que desea que Elastic Beanstalk implemente la aplicación.

4. En Deployment Target (Destino de implementación), puede elegir entre Create a new application environment (Crear un nuevo entorno de aplicación) para realizar una implementación inicial de una aplicación o Redeploy to an existing environment (Volver a implementar en un entorno existente) para volver a implementar una aplicación implementada anteriormente. (Es posible que las implementaciones anteriores se hayan realizado con el asistente o con la obsoleta herramienta de implementación independiente). Si elige Redeploy to an existing environment (Volver a implementar en un entorno existente), podría producirse un retraso mientras el asistente recupera información de implementaciones anteriores que se están ejecutando en este momento.

> **Note**
>
> Si elige Redeploy to an existing environment (Volver a implementar en un entorno existente), elija un entorno en la lista y, a continuación, elija Next (Siguiente); el asistente le llevará directamente a la página Application Options (Opciones de la aplicación). Si opta por esta ruta, avance hasta llegar a las instrucciones que aparecen más adelante en esta sección que describen cómo utilizar la página Application Options (Opciones de la aplicación).

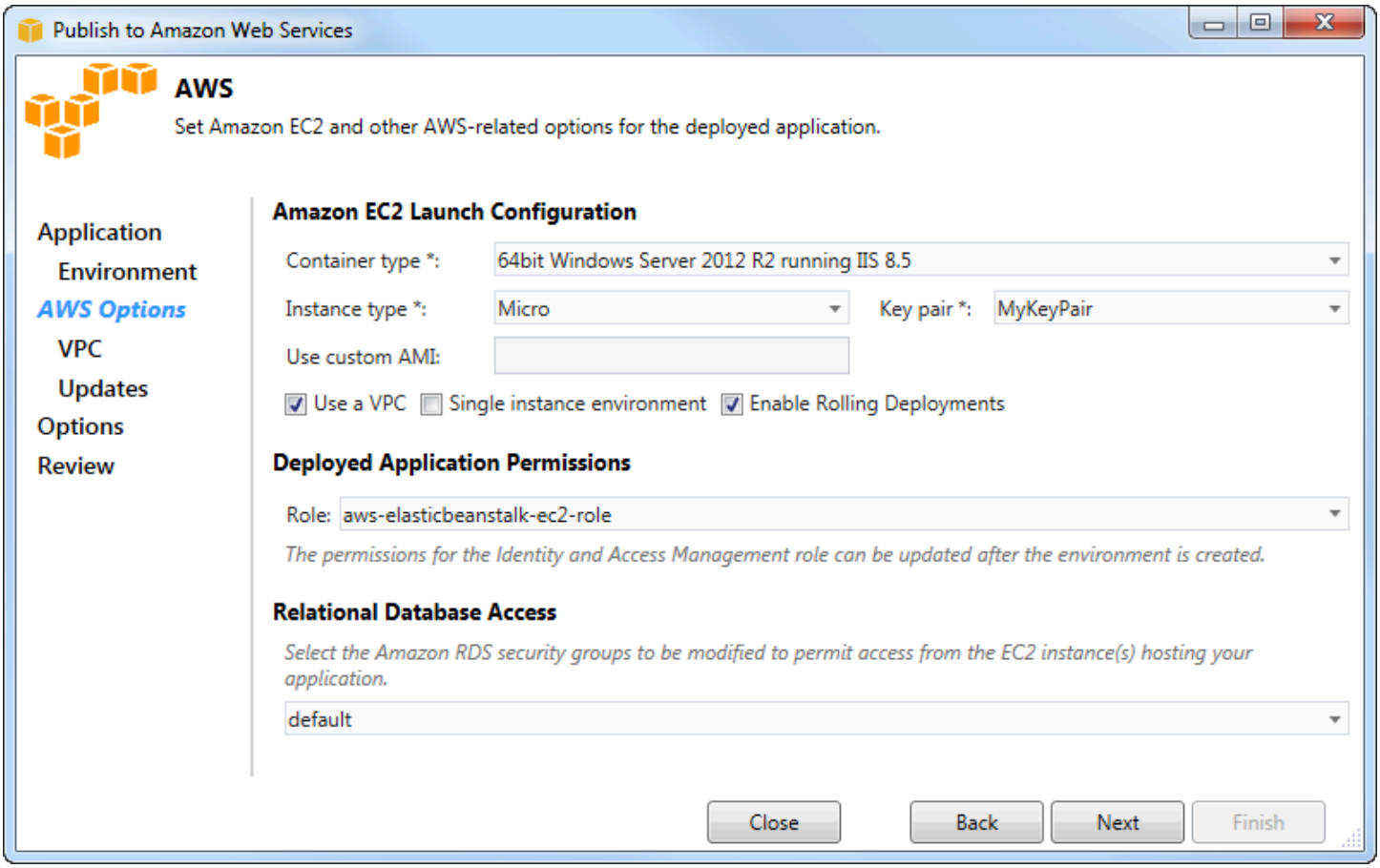
5. Elija Next (Siguiente).



6. En la página Application Environment (Entorno de la aplicación), en el área Application (Aplicación), la lista desplegable Name (Nombre) propone un nombre predeterminado para la aplicación. Para cambiar el nombre predeterminado, seleccione otro nombre en la lista desplegable.
7. En el área Entorno, en la lista desplegable de nombres, escriba un nombre para su entorno de Elastic Beanstalk. En este contexto, el término entorno hace referencia a la infraestructura que Elastic Beanstalk proporciona para su aplicación. Es posible que ya se haya propuesto un nombre

predeterminado en esta lista desplegable. Si aún no se ha propuesto un nombre predeterminado, puede escribir uno o elegir uno en la lista desplegable, si hay nombres adicionales disponibles. El nombre del entorno no puede tener una longitud superior a 23 caracteres.

8. En el área URL, el cuadro propone un subdominio predeterminado de `.elasticbeanstalk.com` que será la URL para su aplicación web. Para cambiar el subdominio predeterminado, escriba un nombre nuevo de subdominio.
9. Elija Check availability (Comprobar disponibilidad) para comprobar que la dirección URL para su aplicación web no se esté utilizando ya.
10. Si puede utilizarse la dirección URL para su aplicación web, elija Next (Siguiente).



1. En la página de AWSopciones, en Amazon EC2 Launch Configuration, en la lista desplegable de tipos de contenedor, elija el tipo de imagen de máquina de Amazon (AMI) que se utilizará en la aplicación.
2. En la lista desplegable de tipos de instancias, especifique el tipo de instancia de Amazon EC2 que desea utilizar. Para este ejemplo, recomendamos que utilice Micro. Esto reducirá al mínimo el

costo asociado con la ejecución de la instancia. Para obtener más información sobre los costos de Amazon EC2, consulte la página Precios de EC2.

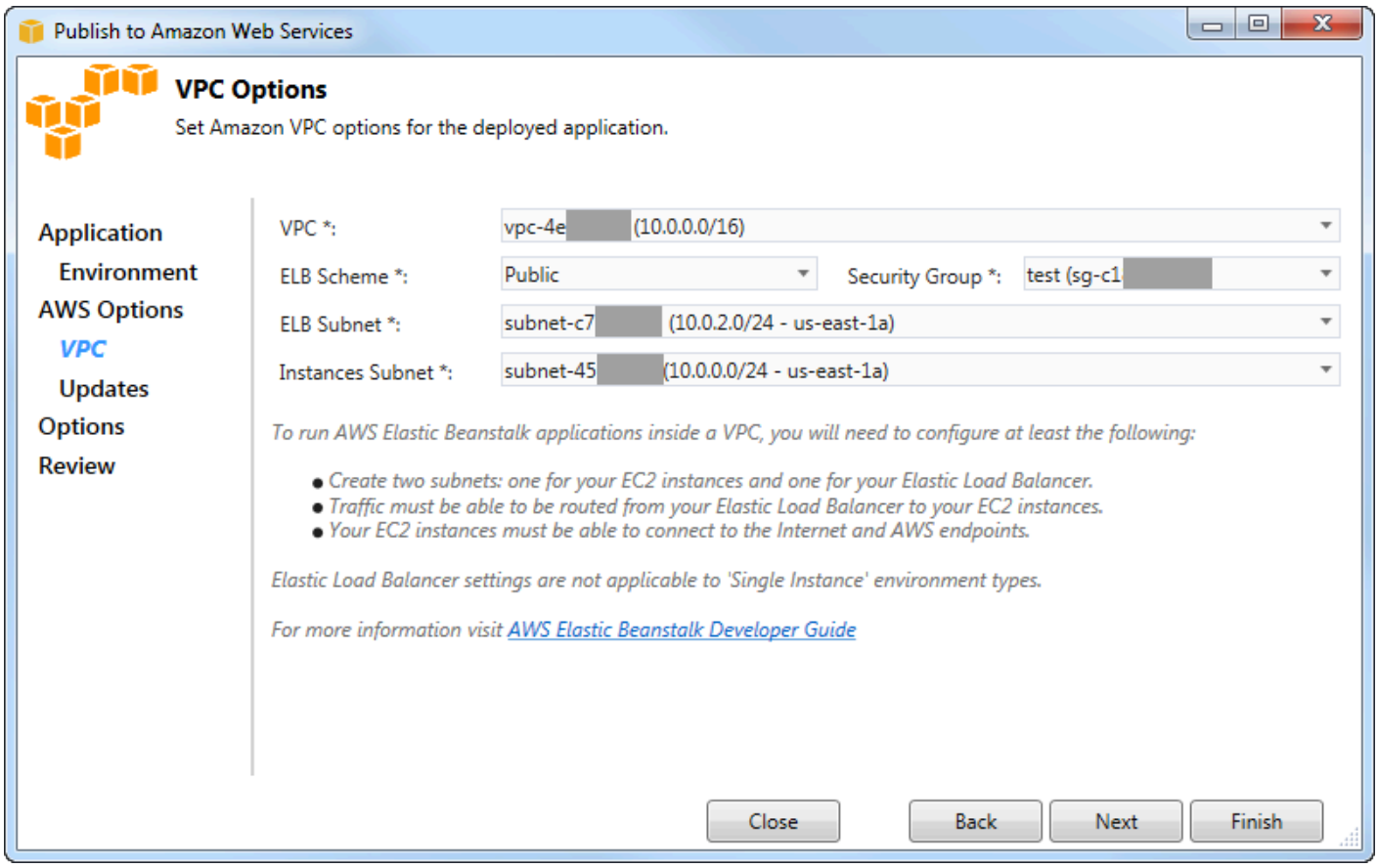
3. En la lista desplegable de pares de claves, elija un key pair de instancias de Amazon EC2 para iniciar sesión en las instancias que se utilizarán para su aplicación.
4. En el cuadro Use custom AMI (Utilizar AMI personalizada), puede especificar una AMI personalizada que sustituirá a la AMI especificada en la lista desplegable Container type (Tipo de contenedor). Para obtener más información sobre cómo crear una AMI personalizada, consulte Uso de AMI personalizadas en la Guía para desarrolladores deAWS Elastic Beanstalk y cree una AMI a partir de una instancia de Amazon EC2.
5. Si desea lanzar sus instancias en una VPC, seleccione el cuadro Use a VPC (Usar una VPC).
6. Si lo desea, si desea lanzar una única instancia de Amazon EC2 y, a continuación, implementar su aplicación en ella, seleccione la casilla Entorno de instancia única.

   Si selecciona esta casilla, Elastic Beanstalk seguirá creando un grupo de Auto Scaling, pero no lo configurará. Si desea configurar el grupo Auto Scaling más adelante, puede usar elAWS Management Console.
7. Si desea controlar las condiciones bajo las cuales se implementa su aplicación a las instancias, seleccione el cuadro Enable Rolling Deployments (Habilitar implementaciones continuas). Únicamente puede seleccionar este cuadro si no ha seleccionado el cuadro Single instance environment (Entorno de instancia individual).
8. Si su aplicación utilizaAWS servicios como Amazon S3 y DynamoDB, la mejor manera de proporcionar credenciales es utilizar un rol de IAM. En el área Permisos de aplicaciones implementados, puede elegir un rol de IAM existente o crear uno que el asistente utilizará para lanzar su entorno. Las aplicaciones que utilicen elAWS SDK for .NET usarán automáticamente las credenciales proporcionadas por este rol de IAM al realizar una solicitud a unAWS servicio.
9. Si su aplicación accede a una base de datos de Amazon RDS, en la lista desplegable del área Acceso a bases de datos relacionales, seleccione las casillas situadas junto a los grupos de seguridad de Amazon RDS que el asistente actualice para que sus instancias de Amazon EC2 puedan acceder a esa base de datos.
10. Elija Next (Siguiente).
    - Si seleccionó Use a VPC (Usar una VPC), aparecerá la página VPC Options (Opciones de VPC).
    - Si seleccionó Enable Rolling Deployments (Habilitar implementaciones continuas), pero no seleccionó Use a VPC (Usar una VPC), aparecerá la página Rolling Deployments (Implementaciones continuas). Avance hasta llegar a las instrucciones que aparecen

más adelante en esta sección que describen cómo utilizar la página Rolling Deployments (Implementaciones continuas).

- Si no seleccionó Use a VPC (Usar una VPC) o Enable Rolling Deployments (Habilitar implementaciones continuas), aparecerá la página Application Options (Opciones de la aplicación). Avance hasta llegar a las instrucciones que aparecen más adelante en esta sección que describen cómo utilizar la página Application Options (Opciones de la aplicación).

11. Si seleccionó Use a VPC (Usar una VPC), especifique información en la página VPC Options (Opciones de VPC) para lanzar su aplicación en una VPC.



Se tiene que haber creado ya la VPC. Si creó la VPC en el Toolkit for Visual Studio, el Toolkit for Visual Studio llenará esta página por usted. Si creó la VPC en la consolaAWS de administración, escriba la información sobre la VPC en esta página.

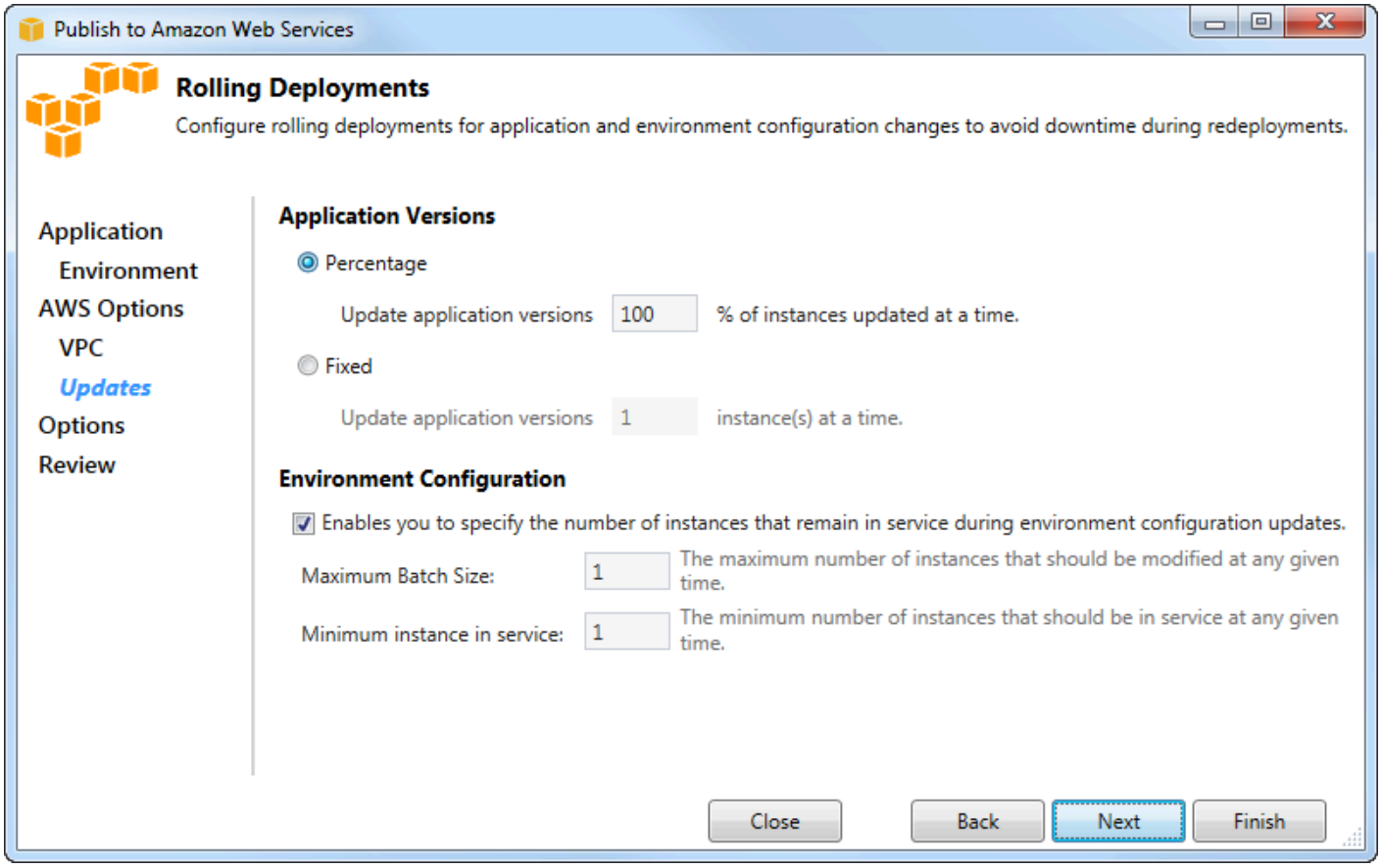
Consideraciones clave para la implementación en una VPC

- La VPC necesita al menos un subred pública y una subred privada.

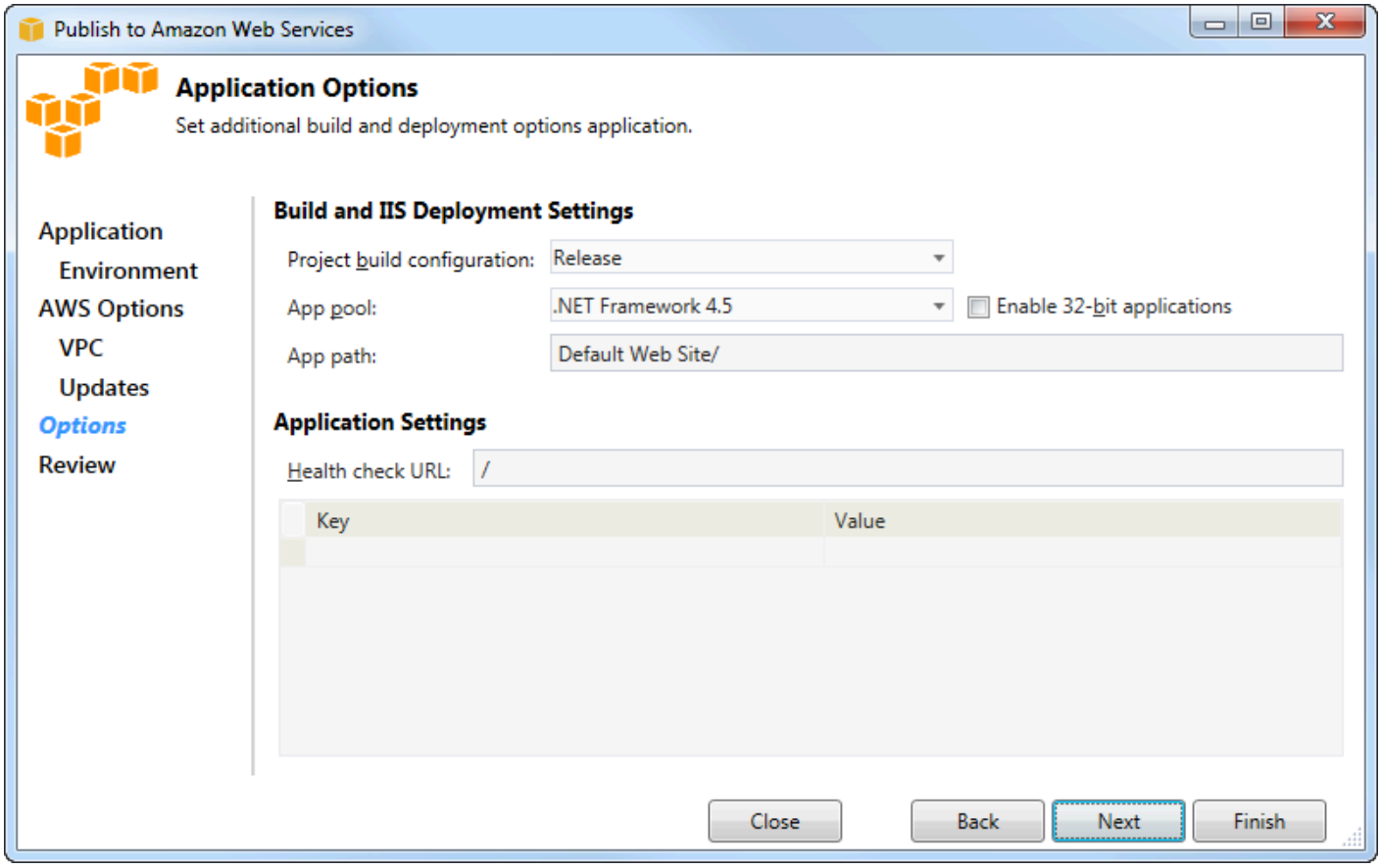
- En la lista desplegable ELB Subnet (Red de ELB), especifique la subred pública. El Toolkit for Visual Studio implementa el balanceador de cargas de Elastic Load Balancing para su aplicación en la subred pública. La subred pública está asociada a una tabla de ruteo que tiene una entrada que señala a una gateway de Internet. Puede reconocer una puerta de enlace de Internet porque tiene un ID que comienza por `igw-` (por ejemplo, `igw-83cddaex`). Las subredes públicas que se crean con el Toolkit for Visual Studio tienen valores de etiqueta que las identifican como públicas.
- En la lista desplegable Instances Subnet (Subred de instancias), especifique la subred privada. El Toolkit for Visual Studio implementa las instancias de Amazon EC2 de su aplicación en la subred privada.
- Las instancias de Amazon EC2 de su aplicación se comunican desde la subred privada a Internet a través de una instancia de Amazon EC2 en la subred pública que realiza la traducción de direcciones de red (NAT). Para habilitar esta comunicación, necesitará un grupo de seguridad VPC que permita que el tráfico fluya desde la subred privada a la instancia NAT. Especifique este grupo de seguridad VPC en la lista desplegable Security Group (Grupo de seguridad).

Para obtener más información sobre cómo implementar una aplicación de Elastic Beanstalk en una VPC, consulte la Guía para desarrolladores deAWS Elastic Beanstalk.

1. Una vez que haya completado toda la información en la página VPC Options (Opciones de VPC), elija Next (Siguiente).
   - Si seleccionó Enable Rolling Deployments (Habilitar implementaciones continuas), aparecerá la página Rolling Deployments (Implementaciones continuas).
   - Si no seleccionó Enable Rolling Deployments (Habilitar implementaciones continuas), aparecerá la página Application Options (Opciones de la aplicación). Avance hasta llegar a las instrucciones que aparecen más adelante en esta sección que describen cómo utilizar la página Application Options (Opciones de la aplicación).
2. Si seleccionó Enable Rolling Deployments (Habilitar implementaciones continuas), debe especificar información en la página Rolling Deployments (Implementaciones continuas) para configurar cómo se implementan las versiones nuevas de las aplicaciones a las instancias en un entorno equilibrado de carga. Por ejemplo, si tiene cuatro instancias en su entorno y desea cambiar el tipo de instancia, puede configurar el entorno para cambiar dos instancias a la vez. Esto ayuda a garantizar que la aplicación se sigue ejecutando mientras se realizan cambios.



3. En el área Application Versions (Versiones de la aplicación), elija una opción para controlar las implementaciones a un porcentaje o número de instancias a la vez. Especifique el porcentaje o el número deseado.
4. En el área Environment Configuration (Configuración del entorno), seleccione el cuadro si desea especificar el número de instancias que permanecen en servicio durante las implementaciones. Si selecciona esta casilla, especifique el número máximo de instancias que deben modificarse a la vez, el número mínimo de instancias que deben permanecer en servicio a la vez, o ambos.
5. Elija Next (Siguiente).
6. En la página Application Options (Opciones de la aplicación), debe especificar información acerca de los ajustes de la compilación, de Internet Information Services (IIS) y de la aplicación.

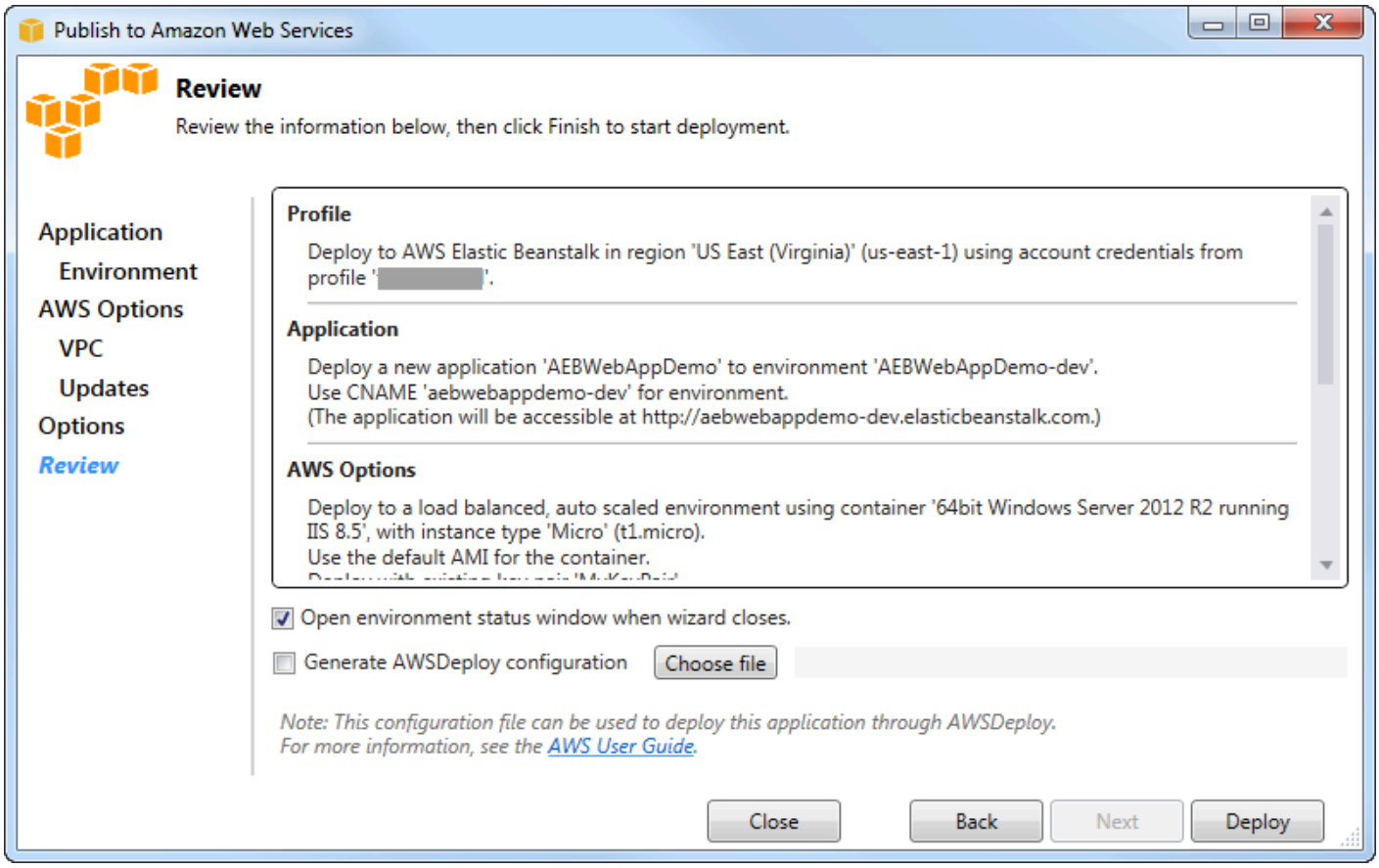


7. En el área Build and IIS Deployment Settings (Configuración de implementación de IIS y de compilación), en la lista desplegable Project build configuration (Configuración de proyecto de compilación), seleccione la configuración de compilación de destino. Si el asistente puede encontrarla, aparece Release (Versión), de lo contrario en el cuadro se muestra la configuración activa.
8. En la lista desplegable App pool (Grupo de aplicaciones), seleccione la versión de .NET Framework que necesita su aplicación. Debería visualizarse la versión de .NET Framework correcta.
9. Si su aplicación es de 32 bits, seleccione el cuadro Enable 32-bit applications (Habilitar aplicaciones de 32 bit).
10. En el cuadro App path (Ruta de la aplicación), especifique la ruta que IIS utilizará para implementar la aplicación. De forma predeterminada, se especifica Default Web Site/ (Sitio web predeterminado/), que normalmente se traduce en la ruta `c:\inetpub\wwwroot`. Si especifica una ruta distinta a Default Web Site/ (Sitio web predeterminado/), el asistente pondrá un redireccionamiento en la ruta Default Web Site/ (Sitio web predeterminado/) que apunte a la ruta que ha especificado.

11. En el área Configuración de la aplicación, en la casilla URL de verificación de Health, escriba una URL para que Elastic Beanstalk compruebe si la aplicación web sigue siendo responsiva. Esta URL es relativa a la URL del servidor raíz. De forma predeterminada, se especifica la URL del servidor raíz. Por ejemplo, si la URL completa es `example.com/site-is-up.html`, escribiría `/site-is-up.html`.
12. En el área correspondiente a Key (Clave) y Value (Valor), puede especificar cualquier par de claves y valores que desee añadir al archivo `Web.config` de su aplicación.

> **Note**
>
> Aunque no se recomienda, puede utilizar el área de Clave y Valor para especificarAWS las credenciales con las que debe ejecutarse la aplicación. El enfoque preferido es especificar un rol de IAM en la lista desplegable de funciones Identity and Access Management de la página de AWSopciones. Sin embargo, si debe usarAWS credenciales en lugar de un rol de IAM para ejecutar la aplicación, elija en la fila de claves AWSAccessKey. En la fila Value (Valor), escriba la clave de acceso. Repita estos pasos para AWSSecretKey.

13. Elija Next (Siguiente).



14. En la página Review (Revisar), revise las opciones que configuró y seleccione el cuadro Open environment status window when wizard closes (Abrir ventana de estado de entorno cuando se cierra el asistente).
15. Si todo parece estar correcto, elija Deploy (Implementar).

> **Note**
>
> Al implementar la aplicación, la cuenta activa incurrirá en cargos por losAWS recursos utilizados por la aplicación.

La información sobre la implementación aparecerá en la barra de estado de Visual Studio y en la ventana Output (Salida). Esta operación puede tardar varios minutos. Cuando se haya completado la implementación, aparecerá un mensaje de confirmación en la ventana Output (Salida).

16. Para eliminar la implementación, en elAWS Explorador, expanda el nodo Elastic Beanstalk, abra el menú contextual (haga clic con el botón derecho) del subnodo de la implementación y, a continuación, elija Eliminar (Eliminar). Este proceso de eliminación puede tardar unos minutos.

Implementación de una aplicación ASP.NET Core en Elastic Beanstalk (Legacy)

> **Important**
>
> Esta documentación hace referencia a los servicios y funciones anteriores. Para obtener guías y contenido actualizados, consulte la guía de herramientas deAWS implementación.NET y laAWS tabla de contenido actualizada de Implementación en.

AWS Elastic Beanstalkes un servicio que simplifica el proceso de aprovisionamiento deAWS recursos para su aplicación. AWS Elastic Beanstalkproporciona toda laAWS infraestructura necesaria para implementar su aplicación.

El Toolkit for Visual Studio permite implementar aplicaciones de ASP.NET CoreAWS con Elastic Beanstalk. ASP.NET Core es el rediseño de ASP.NET con una arquitectura modularizada que minimiza el costo de dependencia y optimiza su aplicación para ejecutarla en la nube.

AWS Elastic Beanstalktambién facilita la implementación de aplicaciones en una variedad de idiomas diferentesAWS. Elastic Beanstalk admite tanto las aplicaciones ASP.NET tradicionales como las aplicaciones de ASP.NET Core. En este tema se describe la implementación de aplicaciones ASP.NET Core.

Con el asistente de implementación

La forma más sencilla de implementar aplicaciones ASP.NET Core en Elastic Beanstalk es con Toolkit for Visual Studio.

Si ha usado el conjunto de herramientas antes para la implementación de aplicaciones ASP. NET tradicionales, encontrará que la experiencia para ASP.NET Core es muy similar. En los pasos que se indican a continuación, le guiaremos a través de la experiencia de implementación.

Si no ha utilizado nunca este conjunto de herramientas, lo primero que tendrá que hacer después de instalar el conjunto de herramientas es registrar susAWS credenciales de con el conjunto de herramientas. Consulte Cómo especificar las credencialesAWS de seguridad para su aplicación en la documentación de Visual Studio para obtener más información sobre cómo hacerlo.

Para implementar una aplicación web de ASP.NET Core, haga clic con el botón derecho en el proyecto en el Explorador de soluciones y seleccione Publicar enAWS...

En la primera página del asistente Publish toAWS Elastic Beanstalk Deployment, elija crear una nueva aplicación de Elastic Beanstalk. Una aplicación Elastic Beanstalk es una colección lógica de componentes de Elastic Beanstalk, que incluye entornos, versiones, y configuraciones de entorno. El asistente de implementación genera una aplicación que, a su vez, contiene una colección de versiones de aplicaciones y entornos. Los entornos contienen losAWS recursos reales que ejecutan una versión de la aplicación. Cada vez que implementa una aplicación, se crea una nueva versión de la aplicación y el asistente apunta al entorno hacia dicha versión. Puede obtener más información sobre estos conceptos en la sección sobre componentes de Elastic Beanstalk.

A continuación, establezca nombres para la aplicación y su primer entorno. Cada entorno tiene un CNAME exclusivo asociado que puede utilizar para obtener acceso a la aplicación cuando la implementación se haya completado.

La siguiente página, AWSOpciones, permite configurar el tipo deAWS recursos que se van a utilizar. En este ejemplo, deje los valores predeterminados, excepto para la sección Key pair (Par de claves). Key pair le permite recuperar la contraseña de administrador de Windows para poder iniciar sesión en el equipo. Si todavía no ha creado un par de claves sería aconsejable que seleccionara Create new key pair (Crear par de claves nuevo).

Permisos

La página de permisos se usa para asignarAWS credenciales a las instancias de EC2 que ejecutan la aplicación. Esto es importante si su aplicación los usaAWS SDK for .NET para acceder a otrosAWS servicios. Si no está utilizando otros servicios de su aplicación puede dejar esta página como la página predeterminada.

Opciones de la aplicación

Los detalles en la página Application Options (Opciones de la aplicación) son diferentes a los especificados a la hora de implementar aplicaciones de ASP.NET tradicionales. A continuación, debe especificar la configuración de compilación y el marco utilizado para empaquetar la aplicación y también debe especificar la ruta de recursos de IIS para la aplicación.

Después de completar la página Application Options (Opciones de la aplicación), haga clic en Next (Siguiente) para revisar los ajustes y, a continuación, haga clic en Deploy (Implementar) para iniciar el proceso de implementación.

Comprobación del estado del entorno

Después de empaquetar y cargar la aplicaciónAWS, puede comprobar el estado del entorno de Elastic Beanstalk abriendo la vista de estado del entorno desde elAWS explorador de Visual Studio.

Los eventos se muestran en la barra de estado dado que el entorno es online. Una vez que se ha completado todo, el estado del entorno pasa a estar en buen estado. Puede hacer clic en la URL para ver el sitio. Desde aquí, también puede extraer los registros del entorno o del escritorio remoto a las instancias de Amazon EC2 que forman parte de su entorno de Elastic Beanstalk.

La primera implementación de cualquier aplicación llevará un poco más de tiempo que las reimplementaciones posteriores, ya que crea nuevosAWS recursos. Mientras realiza la iteración en su aplicación durante la implementación, puede volver a realizar la implementación rápidamente. Para ello, vuelva atrás con el asistente o haga clic con el botón derecho en el proyecto y seleccione la opción Republish (Volver a publicar).

Vuelva a publicar los paquetes de la aplicación con la configuración de la ejecución anterior mediante el asistente de implementación y cargue el paquete de aplicaciones en el entorno de Elastic Beanstalk existente.

Cómo especificar elAWSCredenciales de seguridad para una aplicación

LaAWScuenta que especifiques en laCómo publicar en Elastic Beanstalkwizard es elAWSque el asistente utilizará para la implementación en Elastic Beanstalk.

Aunque no se recomienda, es posible que también deba especificarAWScredenciales de cuenta que su aplicación utilizará para accederAWSservicios después de que se haya desplegado. La estrategia recomendada es especificar un rol de IAM. En el navegadorCómo publicar en Elastic Beanstalk, esto se hace a través deIdentity and Access Managementen elAWSOpciones(Se ha creado el certificado). En el heredadoCómo publicar en Amazon Web Services, esto se hace a través deIAM Roleen elAWSOpciones(Se ha creado el certificado).

Si debe utilizarAWScredenciales de la cuenta en lugar de una función de IAM, puede especificar laAWSCredenciales de la cuenta de la aplicación de una de las siguientes formas:

- Hacer referencia a un perfil correspondiente aAWSCredenciales de la cuenta en`appSettings`elemento del proyecto`Web.config`file. (Para crear un perfil, consulteConfiguraciónAWSCredenciales.) En el siguiente ejemplo se especifican unas credenciales cuyo nombre de perfil es `myProfile`.

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

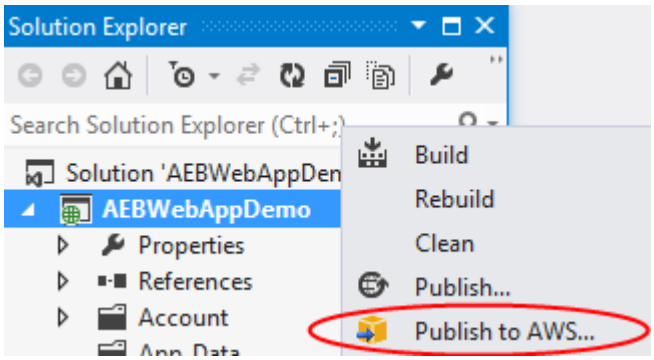
- Si utiliza elCómo publicar en Elastic Beanstalkasistente, en laOpciones de la aplicación, en elClavefila deClaveyValor, seleccioneAWSAccessKey. En la fila Value (Valor), escriba la clave de acceso. Repita estos pasos paraAWSSecretKey.
- Si está utilizando el asistente heredado Publish to Amazon Web Services (Publicar en Amazon Web Services), en la página Application Options (Opciones de la aplicación), en el área Application Credentials (Credenciales de la aplicación), elija Use these credentials (Utilizar estas credenciales) y escriba de nuevo la clave de acceso y la clave de acceso secreta en los cuadros Access Key (Clave de acceso) y Secret Key (clave secreta).

Cómo volver a publicar su aplicación en un entorno de Elastic Beanstalk (Legacy)

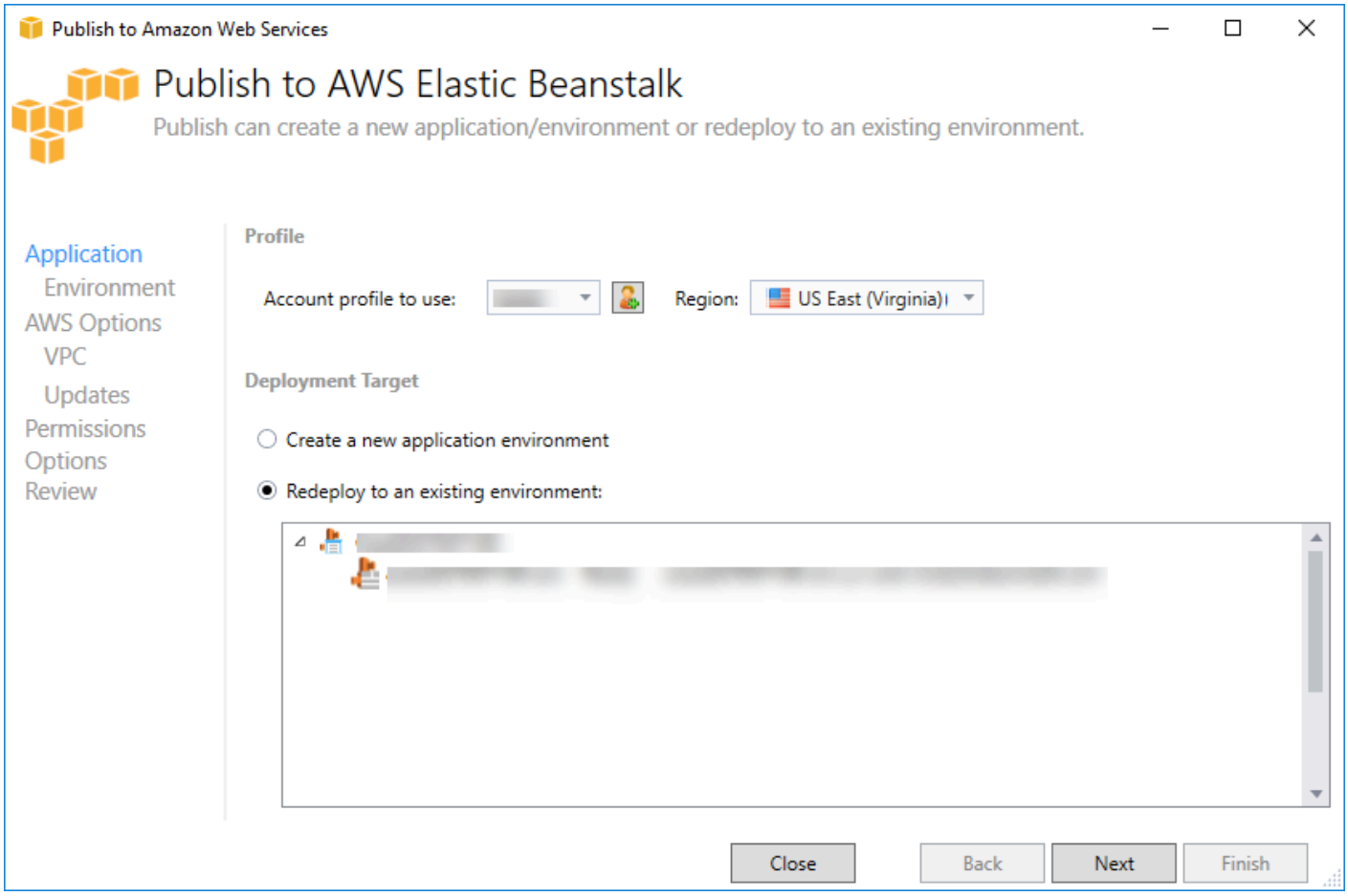
> **Important**
>
> Esta documentación hace referencia a los servicios y funciones anteriores. Para obtener guías y contenido actualizados, consulte la guía de herramientas deAWS implementación.NET y laAWS tabla de contenido actualizada de Implementación en.

Puede realizar iteraciones en su aplicación realizando cambios discretos y, a continuación, volver a publicar una nueva versión en su entorno de Elastic Beanstalk ya lanzado.

1. En Solution Explorer (Explorador de soluciones), abra el menú contextual (haga clic con el botón derecho) de la carpeta deWebAppDemo proyectos de AEB correspondiente al proyecto que publicó en la sección anterior y, a continuación, elija Publish to (Publicar en)AWS Elastic Beanstalk.

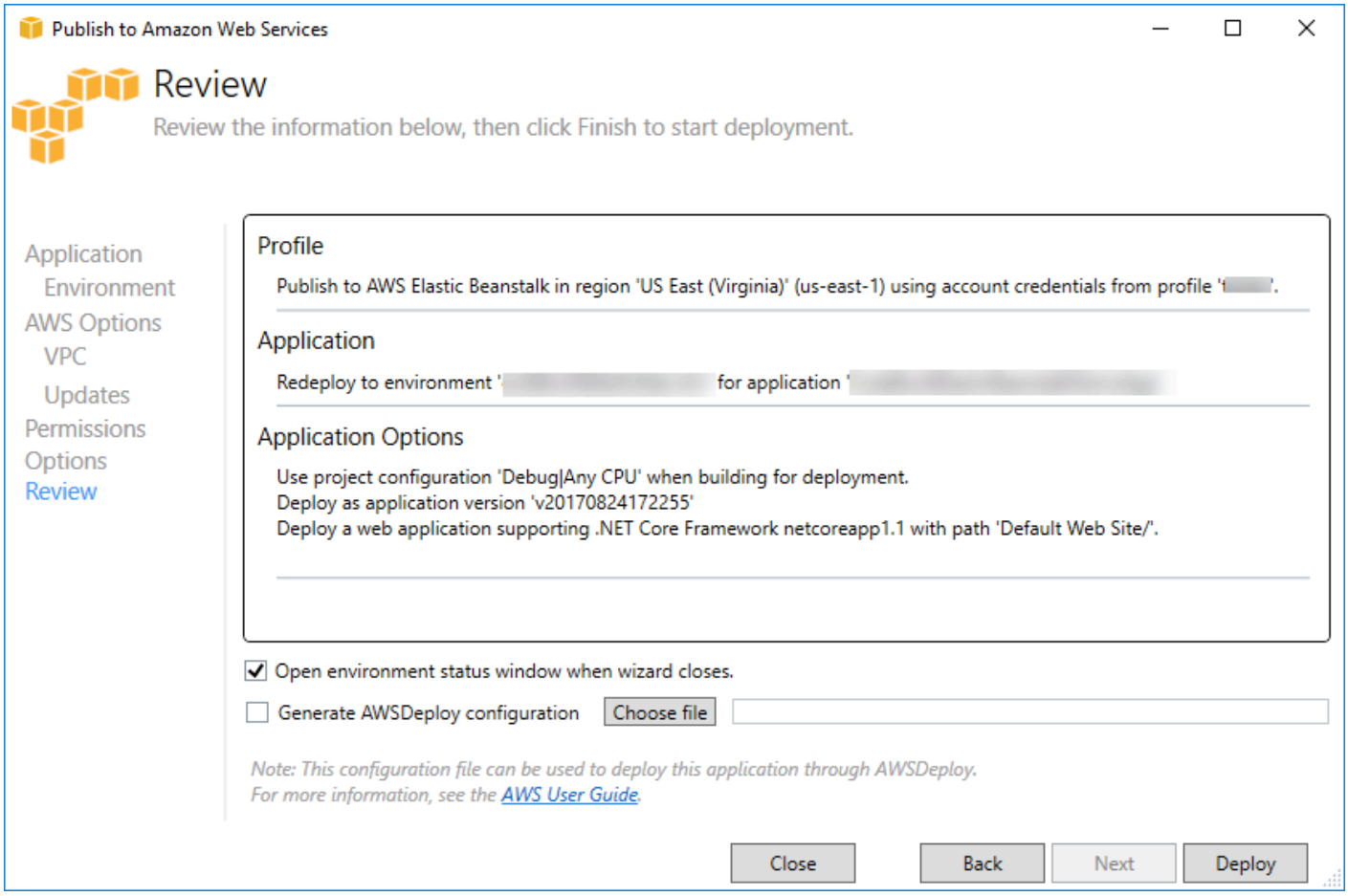


   Aparece el asistente Publish to Elastic Beanstalk (Publicar en Elastic Beanstalk).



2. Seleccione Redeploy to an existing environment (Volver a implementar en un entorno existent) y elija el entorno en el que publicó previamente el proyecto. Haga clic en Next (Siguiente).

   Aparece el asistente Review (Revisar).



3. Haga clic en Deploy (Implementar). La aplicación volverá a realizar la implementación en el mismo entorno.

No puede volver a publicar si la aplicación está en proceso de lanzamiento o finalización.

Implementaciones personalizadas de aplicaciones de Elastic Beanstalk

En este tema se describe cómo el manifiesto de implementación del contenedor de Microsoft Windows para admite implementaciones de aplicaciones personalizadas.

Las implementaciones de aplicaciones personalizadas son una característica eficaz para los usuarios avanzados que desean aprovechar la capacidad de Elastic Beanstalk para crear y administrar susAWSrecursos, pero desea tener un control completo sobre cómo se implementa su aplicación. En una implementación de aplicación personalizada, debe crear scripts de Windows PowerShell para las tres acciones diferentes que realiza Elastic Beanstalk. La acción de instalación se utiliza cuando se inicia una implementación, el reinicio se utiliza cuando la API `RestartAppServer` se llama desde el

Toolkit o la consola web y la desinstalación se invoca en cualquier implementación anterior cada vez que se realiza una nueva implementación.

Por ejemplo, suponga que hay una aplicación de ASP.NET que desea implementar y que el equipo de documentación ha escrito un sitio web estático que se debe incluir con la implementación. Para hacerlo, escriba su manifiesto de implementación de la siguiente forma:

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

Los scripts mostrados para cada acción deben estar en el paquete de la aplicación en relación con el archivo de manifiesto de la implementación. En este ejemplo, el paquete de la aplicación contendrá

también un archivo documentation.zip que incluye un sitio web estático creado por su equipo de documentación.

El script `install.ps1` extrae el archivo zip y configura la ruta de IIS.

```
Add-Type -assembly "system.io.compression.filesystem"
[io.compression.zipfile]::ExtractToDirectory('./documentation.zip', 'c:\inetpub\wwwroot
\documentation')

powershell.exe -Command {New-WebApplication -Name documentation -PhysicalPath  c:
\inetpub\wwwroot\documentation -Force}
```

Dado que la aplicación se ejecuta en IIS, la acción de reinicio invocará un restablecimiento de IIS.

```
iisreset /timeout:1
```

Para los scripts de desinstalación, es importante limpiar todos los ajustes y archivos utilizados durante la fase de instalación. De esta forma, durante la fase de instalación de la nueva versión, podrá evitar conflictos con las implementaciones anteriores. En este ejemplo, debe eliminar la aplicación IIS del sitio web estático y eliminar los archivos del sitio web.

```
powershell.exe -Command {Remove-WebApplication -Name documentation}
Remove-Item -Recurse -Force 'c:\inetpub\wwwroot\documentation'
```

Con estos archivos de script y el archivo documentation.zip incluido en el paquete de la aplicación, la implementación crea una aplicación de ASP.NET y, a continuación, implementa el sitio de documentación.

En este caso, se ha elegido un ejemplo sencillo que implementa un sitio web estático simple, pero con la implementación de aplicaciones personalizada puede implementar cualquier tipo de aplicación y dejar que Elastic Beanstalk administre laAWSrecursos para ello.

Implementaciones personalizadas de ASP.NET Core Elastic Beanstalk

En este tema se describe cómo funciona la implementación y lo que se puede hacer para personalizar las implementaciones al crear aplicaciones de ASP.NET Core con Elastic Beanstalk y Toolkit for Visual Studio.

Después de completar el asistente de implementación en Toolkit for Visual Studio, el Toolkit empaqueta la aplicación y la envía a Elastic Beanstalk. El primer paso para crear el paquete de

la aplicación es utilizar la nueva interfaz de línea de comandos (CLI) de dotnet para preparar la aplicación para la publicación mediante el uso del comando publish. El marco de trabajo y la configuración se pasan de la configuración del asistente al comando publish. Por tanto, si ha seleccionado Release (Versión) para `configuration` y netcoreapp1.0 para `framework`, el Toolkit ejecutará el siguiente comando:

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

Cuando el comando publish (publicar) termine, el Toolkit escribirá el manifiesto de la nueva implementación en la carpeta de publicación. El manifiesto de despliegue es un archivo JSON denominadoaws-windows-deployment-manifest.json, que el contenedor de Elastic Beanstalk Windows (versión 1.2 o posterior) lee para determinar cómo se debe implementar la aplicación. Por ejemplo, en el caso de una aplicación de ASP.NET Core que desea implementar en la raíz de IIS, el Toolkit genera un archivo de manifiesto que tiene este aspecto:

```
{
  "manifestVersion": 1,
  "deployments": {

    "aspNetCoreWeb": [
      {
        "name": "app",
        "parameters": {
          "appBundle": ".",
          "iisPath": "/",
          "iisWebSite": "Default Web Site"
        }
      }
    ]
  }
}
```

La propiedad `appBundle` indica dónde tienen relación los bits de la aplicación con el archivo de manifiesto. Esta propiedad puede apuntar a un directorio o a un archivo ZIP. Las propiedades `iisPath` e `iisWebSite` indican en qué ubicación de IIS se debe alojar la aplicación.

Personalización del manifiesto

El Toolkit solo escribe el archivo de manifiesto si no existe aún en la carpeta de publicación. Si el archivo existe, el Toolkit actualiza las propiedades `appBundle`, `iisPath` e `iisWebSite` en la primera aplicación que aparece en la sección `aspNetCoreWeb` del manifiesto. Esto le permite añadir

aws-windows-deployment-manifest.json a su proyecto y personalizar el manifiesto. Si desea hacerlo para una aplicación web de ASP.NET Core en Visual Studio, añada un nuevo archivo JSON a la raíz del proyecto y llámelo aws-windows-deployment-manifest.json.

El manifiesto debe tener el nombre aws-windows-deployment-manifest.json y debe estar en la raíz del proyecto. El contenedor de Elastic Beanstalk buscará el manifiesto en la raíz y, si lo encuentra, invocará las herramientas de implementación. Si el archivo no existe, el contenedor de Elastic Beanstalk vuelve a las antiguas herramientas de implementación, que suponen que el archivo es unmsdeployarchivo.

Para garantizar que el comando `publish` de la interfaz de línea de comandos (CLI) de dotnet incluye el manifiesto, actualice el archivo `project.json` para incluir el archivo de manifiesto en la sección `include` de `publishOptions`.

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

Ahora que ha declarado el manifiesto para que se incluya en el paquete de la aplicación, puede seguir configurando la forma en que desea implementar la aplicación. Puede personalizar la implementación más allá de lo que admite el asistente de implementación.AWSha definido un esquema JSON paraarchivo aws-windows-deployment-manifest.jsony cuando se instaló Toolkit for Visual Studio, la configuración registró la URL del esquema.

Cuando abra `windows-deployment-manifest.json`, verá la URL del esquema seleccionada en el cuadro desplegable Schema. Puede ir a la URL para obtener una descripción completa de lo que se puede definir en el manifiesto. Con el esquema seleccionado, Visual Studio proporcionará IntelliSense mientras se edita el manifiesto.

Una posible personalización consiste en configurar el grupo de aplicaciones de IIS bajo el que se ejecutará la aplicación. El siguiente ejemplo muestra cómo puede definir un grupo de aplicaciones

de IIS ("customPool") que recicla el proceso cada 60 minutos y lo asigna a la aplicación utilizando `"appPool": "customPool"`.

```
{
  "manifestVersion": 1,
  "iisConfig": {
    "appPools": [
      {
        "name": "customPool",
        "recycling": {
          "regularTimeInterval": 60
        }
      }
    ]
  },
  "deployments": {
    "aspNetCoreWeb": [
      {
        "name": "app",
        "parameters": {
          "appPool": "customPool"
        }
      }
    ]
  }
}
```

Además, el manifiesto puede declarar scripts de Windows PowerShell para ejecutarlos antes y después de las acciones de instalación, reinicio y desinstalación. Por ejemplo, el siguiente manifiesto ejecuta el script de Windows PowerShell `PostInstallSetup.ps1` para realizar más trabajo de configuración una vez que la aplicación de ASP.NET Core se ha implementado en IIS. Cuando añada scripts de este tipo, asegúrese de que se añaden a la sección include de publishOptions en el archivo `project.json`, como hizo con el archivo `aws-windows-deployment-manifest.json`. Si no, los scripts no se incluirán como parte del comando publish (publicar) de la interfaz de línea de comandos (CLI) de dotnet.

```
{
  "manifestVersion": 1,
  "deployments": {
    "aspNetCoreWeb": [
      {
```

```
        "name": "app",
        "scripts": {
          "postInstall": {
            "file": "SetupScripts/PostInstallSetup.ps1"
          }
        }
      }
    ]
  }
}
```

¿Qué ocurre con los archivos .ebextensions?

El Elastic Beanstalk.ebextensionsLos archivos de configuración son compatibles con los demás contenedores de Elastic Beanstalk. Para incluir .ebextensions en una aplicación de ASP.NET Core, añada el directorio `.ebextensions` en la sección `include` de `publishOptions` en el archivo `project.json`. Para obtener más información acerca de .ebextensions, consulte la Elastic Beanstalk Developer Guide.

Support varias aplicaciones para .NET y Elastic Beanstalk

Con el manifiesto de la implementación, tiene la posibilidad de implementar varias aplicaciones en el mismo entorno de Elastic Beanstalk.

El manifiesto de la implementación es compatible con aplicaciones web ASP.NET Core así como archivos msdeploy para aplicaciones ASP.NET tradicionales. Imagine una situación en la que usted haya desarrollado una nueva aplicación sorprendente mediante ASP.NET Core para el frontend y un proyecto de API web para una API de extensiones. También tiene una aplicación de administración que escribió mediante ASP.NET tradicional.

El asistente de implementación del conjunto de herramientas se centra en la implementación de un proyecto individual. Para aprovechar la implementación de varias aplicaciones, tendrá que construir el paquete de la aplicación a mano. Para empezar, escriba el manifiesto. En este ejemplo, escribirá el manifiesto en la raíz de su solución.

La sección de implementación del manifiesto tiene dos elementos secundarios: una matriz de aplicaciones web ASP.NET Core para su implementación y una matriz de archivos msdeploy para su implementación. Para cada aplicación, establezca la ruta de IIS y la ubicación de los bits de la aplicación relativos al manifiesto.

```
{
```

```
  "manifestVersion": 1,
  "deployments": {

    "aspNetCoreWeb": [
      {
        "name": "frontend",
        "parameters": {
          "appBundle": "./frontend",
          "iisPath": "/frontend"
        }
      },
      {
        "name": "ext-api",
        "parameters": {
          "appBundle": "./ext-api",
          "iisPath": "/ext-api"
        }
      }
    ],
    "msDeploy": [
      {
        "name": "admin",
        "parameters": {
          "appBundle": "AmazingAdmin.zip",
          "iisPath": "/admin"
        }
      }
    ]
  }
}
```

Con el manifiesto escrito, utilizará Windows PowerShell para crear el paquete de la aplicación y actualizar un entorno de Elastic Beanstalk existentes para ejecutarla. El script se escribe suponiendo que se ejecutará desde la carpeta que contiene la solución de Visual Studio.

Lo primero que tiene que hacer en el script es configurar una carpeta de área de trabajo en la que crear el paquete de la aplicación.

```
$publishFolder = "c:\temp\publish"

$publishWorkspace = [System.IO.Path]::Combine($publishFolder, "workspace")
$appBundle = [System.IO.Path]::Combine($publishFolder, "app-bundle.zip")
```

```
If (Test-Path $publishWorkspace){
  Remove-Item $publishWorkspace -Confirm:$false -Force
}
If (Test-Path $appBundle){
  Remove-Item $appBundle -Confirm:$false -Force
}
```

Una vez que haya creado la carpeta, ha llegado el momento de preparar el frontend. Al igual que con el asistente de implementación, utilice la CLI de dotnet para publicar la aplicación.

```
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
```

Observe que la subcarpeta “frontend” se utilizó para la carpeta de salida, que se corresponde con la carpeta que estableció en el manifiesto. Ahora tiene que hacer lo mismo para el proyecto de API web.

```
Write-Host 'Publish the ASP.NET Core extensibility API'
$publishExtAPIFolder = [System.IO.Path]::Combine($publishWorkspace, "ext-api")
dotnet publish .\src\AmazingExtensibleAPI\project.json -o $publishExtAPIFolder -c
 Release -f netcoreapp1.0
```

El sitio de administración es una aplicación ASP.NET tradicional, por lo que no puede utilizar la CLI de dotnet. Para la aplicación de administración, debe utilizar msbuild, transfiriendo el paquete de destino de compilación para crear el archivo msdeploy. De forma predeterminada, el destino del paquete crea el archivo msdeploy en la carpeta `obj\Release\Package`, por lo que tendrá que copiar el archivo en el área de trabajo de publicación.

```
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
```

Para indicar al entorno de Elastic Beanstalk qué debe hacer con todas estas aplicaciones, copie el manifiesto de su solución en el área de trabajo de publicación y, a continuación, comprima la carpeta.

```
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)
```

Ahora que tiene el paquete de la aplicación, puede ir a la consola web y cargar el archivo a un entorno de Elastic Beanstalk. También puede seguir usando laAWSCmdlets de PowerShell para actualizar el entorno de Elastic Beanstalk con el paquete de la aplicación. Asegúrese de que ha establecido el perfil y la región actuales en el perfil y la región que contienen su entorno de Elastic Beanstalk mediante`Set-AWSCredentials`y`Set-DefaultAWSRegion`Cmdlets de .

```
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
```

Compruebe el estado de la actualización en el conjunto de herramientas o la consola web de la página de estado del entorno de Elastic Beanstalk. Cuando finalice, podrá acceder a cada una de las aplicaciones que implementó en la ruta de IIS establecida en el manifiesto de implementación.

Implementación en Amazon EC2 Container Service

> **Important**
>
> El nuevoPublicación enAWSestá diseñada para simplificar la forma en que publica las aplicaciones.NET enAWS. Es posible que se le pregunte si desea cambiar a esta experiencia de publicación después de elegirPublique contenedores enAWS. Para obtener más información, consulte Trabajo con Publicación enAWSen Visual Studio Studio Studio.

Amazon Elastic Container Service es un servicio de administración de contenedores de alto desempeño y alta escalabilidad que admite contenedores Docker y permite ejecutar fácilmente aplicaciones en un clúster administrado de instancias de Amazon EC2.

Para implementar aplicaciones en Amazon Elastic Container Service, los componentes de la aplicación se deben desarrollar para ejecutarse en un contenedor de Docker. Un contenedor Docker es una unidad estandarizada de desarrollo de software que contiene todo lo que la aplicación de software necesita para ejecutarse: código, tiempo de ejecución, herramientas del sistema, bibliotecas del sistema, etc.

Toolkit for Visual Studio proporciona un asistente que simplifica la publicación de aplicaciones a través de Amazon ECS. Este asistente se describe en las secciones siguientes.

Para obtener más información sobre Amazon ECS, consulte laDocumentación de Elastic. Incluye una introducción a los aspectos básicos de Docker y a la creación de un clúster.

Temas

- Especifique .AWSCredenciales para su aplicación de ASP.NET Core 2
- Implementación de una aplicación ASP.NET Core 2.0 en Amazon ECS (Fargate) (Legacy)
- Implementación de una aplicación de ASP.NET Core 2.0 en Amazon ECS (EC2)

Especifique .AWSCredenciales para su aplicación de ASP.NET Core 2

Existen dos tipos de credenciales cuando implementa su aplicación en un contenedor de Docker: las credenciales de implementación y las credenciales de la instancia.

Las credenciales de implementación las utiliza el contenedor Publish Container toAWSasistente para crear el entorno en Amazon ECS. Incluyen cosas como las tareas, los servicios, los roles de IAM, un repositorio de contenedores de Docker y, si lo elige, un balanceador de carga.

Las credenciales de la instancia las utiliza la instancia (incluida su aplicación) para obtener acceso a diferentes servicios de AWS. Por ejemplo, si su aplicación de ASP.NET Core 2.0 lee y escribe en objetos de Amazon S3, necesitará los permisos adecuados. Puede proporcionar credenciales diferentes con métodos distintos en función del entorno. Por ejemplo, su aplicación de ASP.NET Core 2 podría estar diseñada para entornos de desarrollo y producción. Podría utilizar una instancia de Docker local y credenciales para desarrollo y un rol definido en producción.

Especificación de credenciales de implementación

LaAWScuenta que especifique en elPublicación de contenedor enAWSasistente es laAWScuenta que el asistente utilizará para la implementación en Amazon ECS. El perfil de cuenta debe tener permisos para Amazon Elastic Compute Cloud, Amazon Elastic Container Service yAWS Identity and Access Management.

Si observa que hay opciones que faltan en las listas desplegables, esto puede deberse a que carece de permisos. Por ejemplo, si ha creado un clúster para su aplicación pero no lo ve en laPublicación de contenedor enAWSpágina Clúster del asistente. añada los permisos que faltan y pruebe el asistente de nuevo.

Especificación de credenciales de instancias de desarrollo

Para los entornos que no sean de producción, puede configurar sus credenciales en el archivo appsettings.<environment>.json. Por ejemplo, para configurar sus credenciales en el archivo appsettings.Development.json en Visual Studio 2017:

1. Añada el paquete de NuGet AWSSDK.Extensions.NETCore.Setup a su proyecto.
2. AñadirAWSconfiguración de appsettings.Development.json. La configuración siguiente establece `Profile` y `Region`.

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

Especificación de credenciales de instancias de producción

En el caso de las instancias de producción, le recomendamos que utilice un rol de IAM para controlar a lo que su aplicación (y el servicio) pueden tener acceso. Por ejemplo, para configurar un rol de IAM con Amazon ECS como la entidad principal del servicio con permisos para Amazon Simple Storage Service y Amazon DynamoDB desde laAWS Management Console:

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.

2. En el panel de navegación de la consola de IAM, seleccione Roles y, a continuación, seleccione Create role.
3. Elija el iconoAWSService (Servicio)tipo de rol y, a continuación, elijaEC2 Container Service.
4. Elija el caso de uso EC2 Container Service Task (Tarea de servicio de contenedor de EC2). Los casos de uso son definidos por el servicio de modo tal que ya incluyen la política de confianza que el servicio mismo requiere. A continuación, elija Next (Siguiente): Permisos.
5. Elija las políticas de permisos AmazonS3FullAccess y AmazonDynamoDBFullAccess. Seleccione la casilla situada junto a cada política y, a continuación, elijaSiguiente: Review (Revisar),
6. En Role name (Nombre del rol), escriba un nombre o sufijo de nombre para el rol que pueda ayudarle a identificar su finalidad. Los nombres de rol deben ser únicos en su cuenta de AWS. No distinguen entre mayúsculas y minúsculas. Por ejemplo, no puede crear funciones denominado tanto `PRODROLE` y `prodrole`. Dado que varias entidades pueden hacer referencia al rol, no puede editar el nombre del rol después de crearlo.
7. (Opcional) En Role descripción, escriba una descripción para la nueva función.
8. Revise el rol y, a continuación, seleccione Create role.

Puede utilizar este rol comoRol de tareaen elDefinición de tarea ECSPágina de laPublicación de contenedor enAWSasistente.

Para obtener más información, consulte Uso de roles basados en servicios.

Implementación de una aplicación ASP.NET Core 2.0 en Amazon ECS (Fargate) (Legacy)

> **Important**
>
> Esta documentación hace referencia a los servicios y funciones anteriores. Para obtener guías y contenido actualizados, consulte la guía de herramientas deAWS implementación.NET y laAWS tabla de contenido actualizada de Implementación en.

En esta sección se describe cómo utilizar elAWS asistente Publish Container para, incluido como parte del Toolkit for Visual Studio, para implementar una aplicación ASP.NET Core 2.0 contenerizada dirigida a Linux a través de Amazon ECS mediante el tipo de lanzamiento de Fargate. Como las aplicaciones web están diseñadas para que se ejecuten continuamente, esta aplicación se implementará como un servicio.

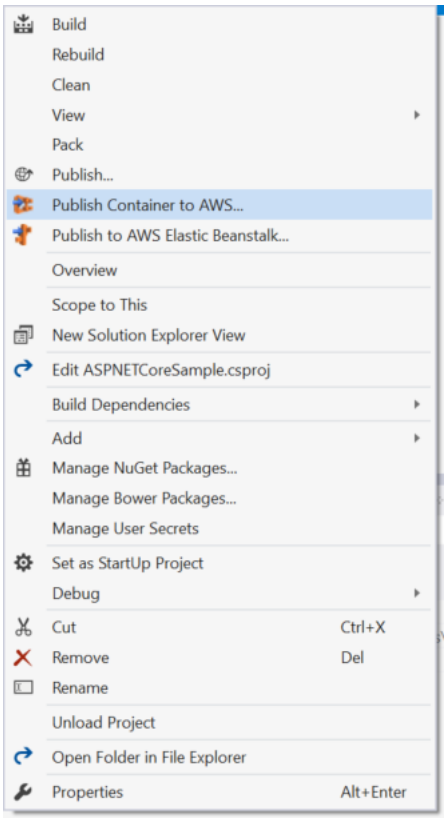
Antes de publicar el contenedor

Antes de usar elAWS asistente Publish Container para implementar su aplicación ASP.NET Core 2.0:

- Especifique susAWS credenciales y realice la configuración con Amazon ECS.
- Instalar Docker. Dispone de diferentes opciones de instalación, entre las que se incluye Docker para Windows.
- En Visual Studio, cree (o abra) un proyecto para una aplicación contenerizada de ASP.NET Core 2.0 dirigida a Linux.

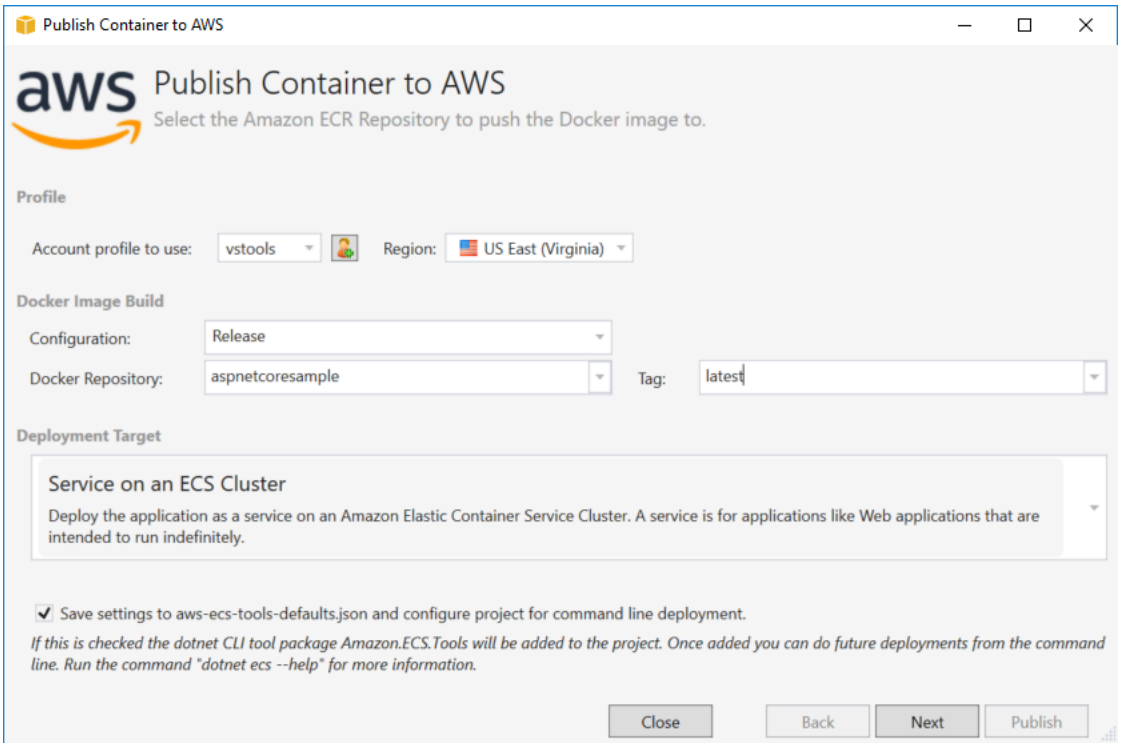
Acceso al contenedor de publicación para elAWS asistente

Para implementar una aplicación contenerizada de ASP.NET Core 2.0 dirigida a Linux, haga clic con el botón derecho en el proyecto en el Explorador de soluciones y seleccione Publicar contenedor enAWS.



También puede seleccionar Publicar contenedorAWS en en el menú Compilar de Visual Studio.

Publicar contenedor enAWS Wizard



Account profile to use (Perfil de la cuenta que se va a usar): seleccione el perfil de la cuenta que se va a usar.

Region (Región): elija la región de implementación. El perfil y la región se utilizan para configurar los recursos del entorno de implementación y para seleccionar el registro de Docker predeterminado.

Configuration (Configuración): seleccione la configuración de compilación de la imagen de Docker.

Docker Repository (Repositorio de Docker): elija un repositorio de Docker existente o escriba el nombre de un nuevo repositorio. Este es el repositorio al que se enviará el contenedor de compilación.

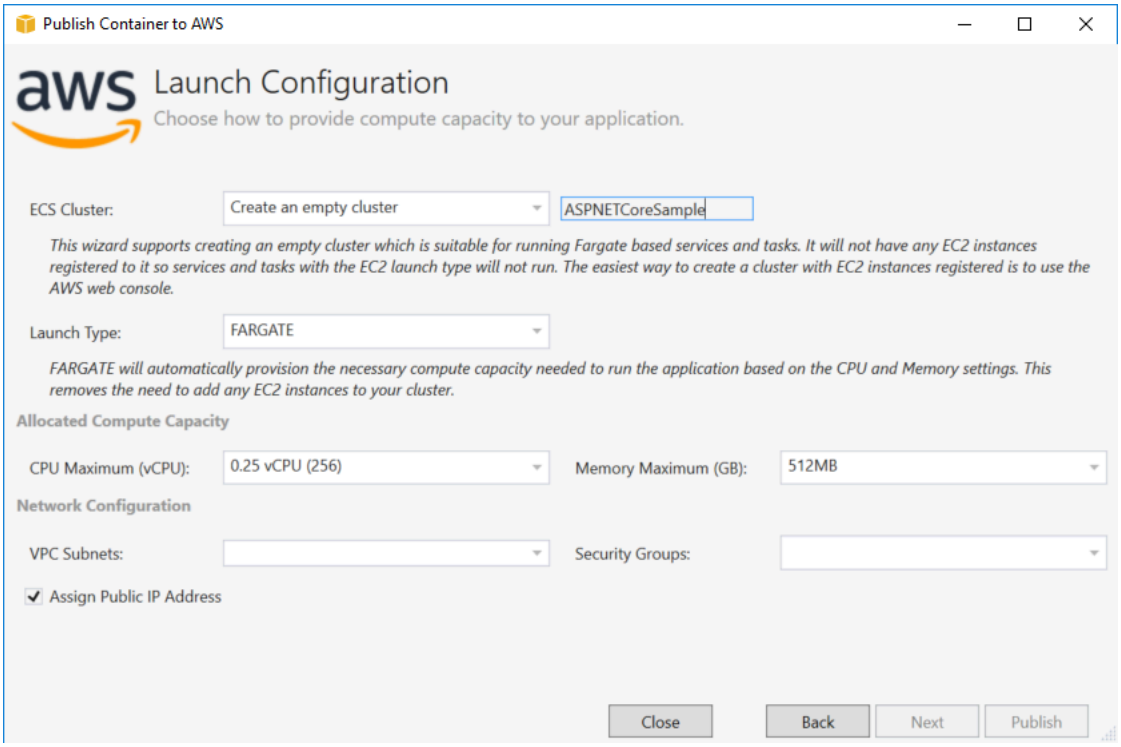
Tag (Etiqueta): seleccione una etiqueta existente o escriba el nombre de una nueva etiqueta. Las etiquetas pueden realizar un seguimiento de detalles importantes como la versión, las opciones u otros elementos exclusivos de la configuración del contenedor de Docker.

Deployment Target (Destino de la implementación): seleccione Service on an ECS Cluster (Servicio en un clúster de ECS). Utilice esta opción de implementación cuando su aplicación esté diseñada para ejecutarse de manera prolongada (como una aplicación web ASP.NET).

Guarde la configuración en el proyecto**`aws-docker-tools-defaults.json`** y configúrelo para la implementación de la línea de comandos: marque esta opción si desea la flexibilidad de implementar

desde la línea de comandos. Use `dotnet ecs deploy` desde el directorio del proyecto para implementar y ejecute el comando `dotnet ecs publish` en el contenedor.

Página Launch Configuration



ECS Cluster (Clúster de ECS): elija el clúster que ejecutará la imagen de Docker. Si decide crear un clúster vacío, proporcione un nombre para el nuevo clúster.

Launch Type (Tipo de lanzamiento): elija FARGATE.

CPU Maximum (vCPU) (Máxima CPU (vCPU): elija la cantidad máxima de capacidad de computación necesaria para su aplicación. Para ver los intervalos permitidos de valores de CPU y memoria, consulte el tamaño de la tarea.

Memory Maximum (GB) (Memoria máxima (GB): seleccione la cantidad máxima de memoria disponible para su aplicación.

VPC Subnets (Redes de VPC): elija una o varias subredes en una VPC. Si elige más de una subred, las tareas se distribuirán entre ellas. Esto puede mejorar la disponibilidad. Para obtener más información, consulte VPC y subredes predeterminadas.

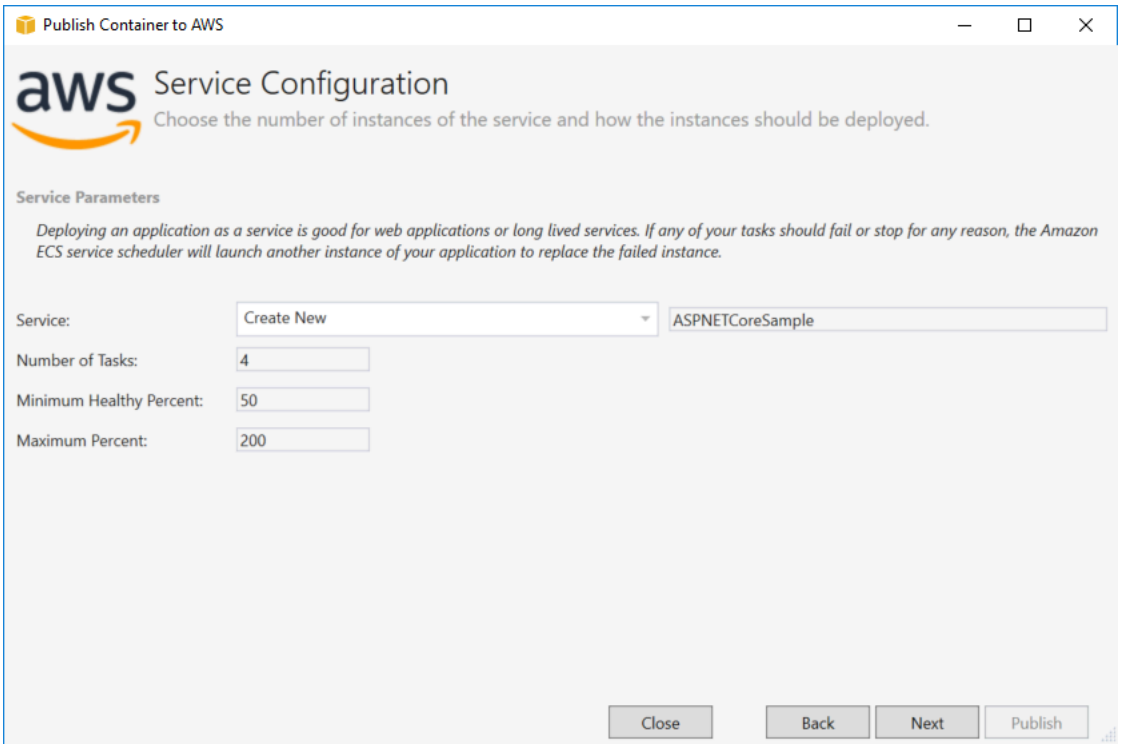
Security Groups (Grupos de seguridad): elija un grupo de seguridad.

Los grupos de seguridad actúan como un firewall para las instancias asociadas de Amazon EC2 y controlan el tráfico entrante y saliente en el nivel de instancia.

Los grupos de seguridad predeterminados están configurados para permitir el tráfico entrante de las instancias asignadas al mismo grupo de seguridad y todo el tráfico IPv4 saliente. Es necesario que el tráfico saliente esté permitido para que el servicio pueda obtener acceso al repositorio del contenedor.

Assign Public IP Address (Asignar dirección IP pública): active esta opción para hacer que su tarea esté accesible desde Internet.

Página Service Configuration



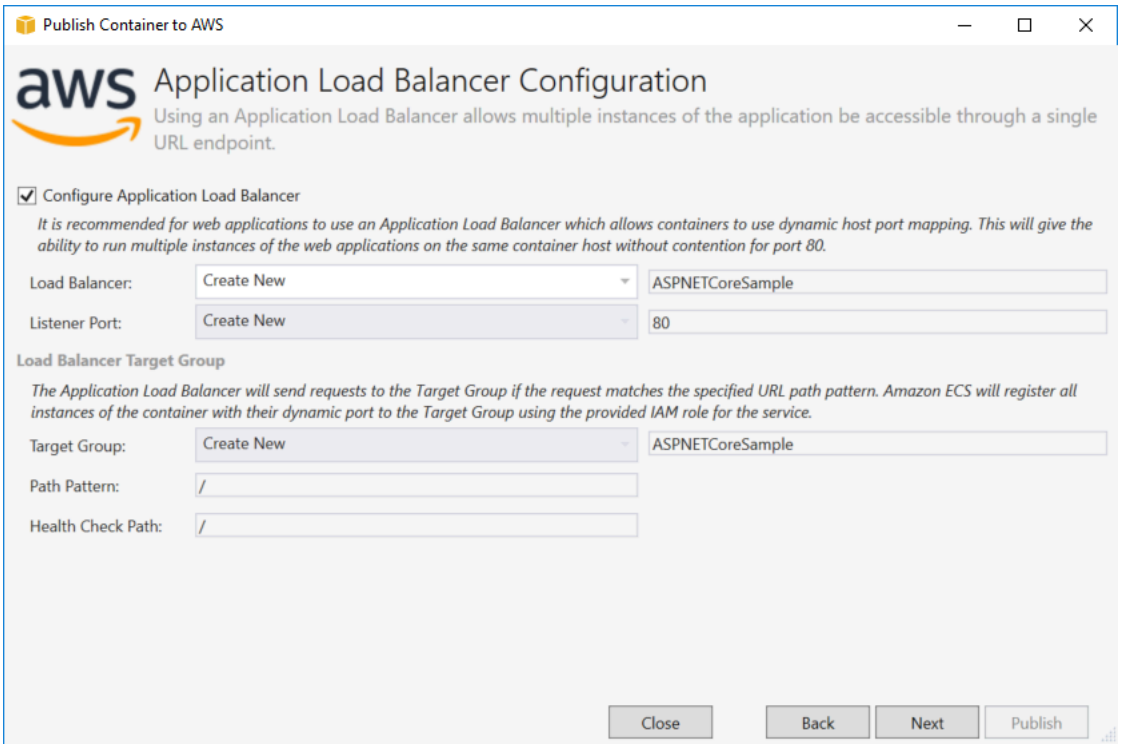
Service (Servicio): seleccione uno de los servicios de la lista desplegable para implementar el contenedor en un servicio existente. O bien elija Create New (Crear nuevo) para crear un nuevo servicio. Los nombres de servicio deben ser únicos dentro de un clúster, pero puede tener servicios con el mismo nombre en varios clústeres dentro de una región o en varias regiones.

Number of Tasks (Número de tareas): el número de tareas que desea implementar y mantener en ejecución en el clúster. Cada tarea es una instancia de su contenedor.

Minimum Healthy Percent (Porcentaje mínimo en buen estado): el porcentaje de tareas que deben permanecer en estado `RUNNING` durante la implementación, redondeado al entero superior más próximo.

Maximum Percent (Porcentaje máximo): el porcentaje de tareas que deben permanecer en estado `RUNNING` o `PENDING` durante la implementación, redondeado al entero inferior más próximo.

Página Application Load Balancer



Configure Application Load Balancer (Configurar balanceador de carga de la aplicación): seleccione esta opción para configurar un balanceador de carga de la aplicación.

Load Balancer (Balanceador de carga): seleccione un balanceador de carga o elija Create New (Crear nuevo) y escriba el nombre de un nuevo balanceador de carga.

Listener Port (Puerto de escucha): seleccione un puerto de escucha existente o elija Create New (Crear nuevo) y escriba un número de puerto. El puerto predeterminado, `80`, es adecuado para la mayoría de las aplicaciones web.

Grupo objetivo: seleccione el grupo de destino en el que Amazon ECS registrará las tareas del servicio.

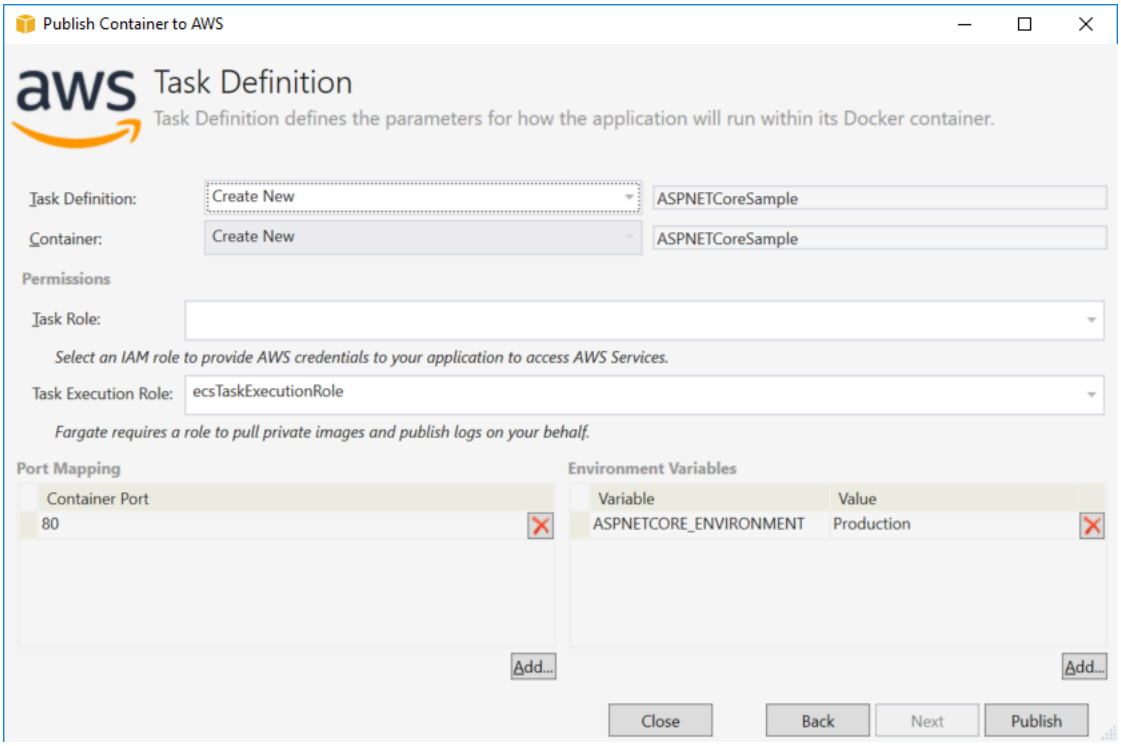
Path Pattern (Patrón de ruta): el balanceador de carga usará el direccionamiento basado en rutas. Acepte la opción `/` predeterminada o proporcione un patrón diferente. Los patrones de ruta

distinguen entre mayúsculas y minúsculas, su longitud máxima es de 128 caracteres y contienen un conjunto específico de caracteres.

Health Check Path (Ruta de comprobación de estado): la ruta de ping que es el destino para los destinos en las comprobaciones de estado. De forma predeterminada, es `/`. Especifique otra ruta si es necesario. Si la ruta que especifica no es válida, no se superará la comprobación de estado y se considerará que está en mal estado.

Si implementa varios servicios y cada servicio se implementa en una ruta o ubicación diferente, necesitará rutas de comprobación personalizadas.

Página Task Definition



Task Definition (Definición de tarea): seleccione una definición de tarea existente o elija Create New (Crear nueva) y escriba el nombre de una nueva definición de tarea.

Container (Contenedor): seleccione un contenedor existente o elija Create New (Crear nuevo) y escriba el nombre de un nuevo contenedor.

Función de tarea: seleccione un rol de IAM que tenga las credenciales que su aplicación necesita para acceder aAWS los servicios. Así es cómo se pasan las credenciales a la aplicación. Consulte cómo especificar las credencialesAWS de seguridad para su aplicación.

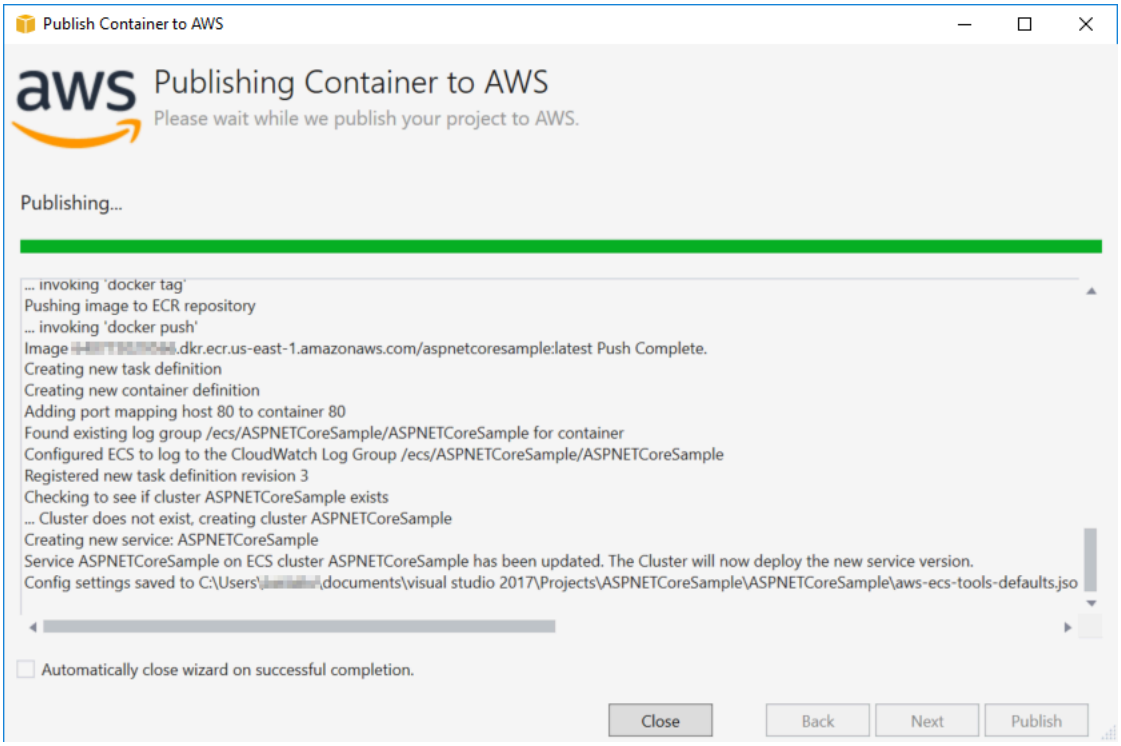
Función de ejecución de tareas: seleccione un rol con permisos para extraer imágenes privadas y publicar registros. AWS Fargate lo utilizará por usted.

Port Mapping (Mapeo de puerto): elija el número de puerto del contenedor asociado al puerto de host asignado automáticamente.

Environment Variables (Variables de entorno): añada, modifique o elimine las variables de entorno del contenedor. Puede modificarlas para adaptarlas a su implementación.

Cuando esté satisfecho con la configuración, haga clic en Publish (Publicar) para iniciar el proceso de implementación.

Contenedor de publicación paraAWS



Los eventos se muestran durante la implementación. El asistente se cierra automáticamente una vez completado correctamente. Puede invalidarlo desactivando la casilla situada en la parte inferior de la página.

Puedes encontrar la URL de tus nuevas instancias en elAWS explorador. Expanda Amazon ECS and Clusters y haga clic en su clúster.

Implementación de una aplicación de ASP.NET Core 2.0 en Amazon ECS (EC2)

En esta sección se describe cómo utilizar laPublicación de contenedor enAWSasistente, que se proporciona como parte de Toolkit for Visual Studio, para implementar una aplicación de ASP.NET Core 2.0 en un contenedor en Linux a través de Amazon ECS mediante el tipo de lanzamiento de EC2. Como las aplicaciones web están diseñadas para que se ejecuten continuamente, esta aplicación se implementará como un servicio.

Antes de publicar el contenedor

Antes de usar laPublicación de contenedor enAWSpara implementar la aplicación de ASP.NET Core 2.0:

- Especifique suAWScredencialesyConfiguración con Amazon ECS.
- Instalar Docker. Dispone de diferentes opciones de instalación, entre las que se incluye Docker para Windows.
- Cree un clúster de Amazon ECS en función de las necesidades de su aplicación web. Para ello, solo necesita realizar unos pocos pasos.
- En Visual Studio, cree (o abra) un proyecto para una aplicación de ASP.NET Core 2.0 en un contenedor dirigida a Linux.

Acceso al contenedor Publish Container toAWSasistente

Para implementar una aplicación de ASP.NET Core 2.0 en un contenedor en Linux, haga clic con el botón derecho en Solution Explorer (Explorador de soluciones) y seleccionePublicación de contenedor enAWS.

También puede seleccionarPublicación de contenedor enAWSen el menú Compilar de Visual Studio.

Publicación de contenedor enAWSAsistente

Account profile to use (Perfil de la cuenta que se va a usar): seleccione el perfil de la cuenta que se va a usar.

Region (Región): elija una región de implementación. El perfil y la región se utilizan para configurar los recursos del entorno de implementación y para seleccionar el registro de Docker predeterminado.

Configuration (Configuración): seleccione la configuración de compilación de la imagen de Docker.

Docker Repository (Repositorio de Docker): elija un repositorio de Docker existente o escriba el nombre de un nuevo repositorio. Este es el repositorio al que se enviará la imagen del contenedor compilada.

Tag (Etiqueta): seleccione una etiqueta existente o escriba el nombre de una nueva etiqueta. Las etiquetas pueden realizar un seguimiento de detalles importantes como la versión, las opciones u otros elementos exclusivos de la configuración del contenedor de Docker.

Deployment (Implementación): seleccione Service on an ECS Cluster (Servicio en un clúster de ECS). Utilice esta opción de implementación cuando su aplicación esté diseñada para ejecutarse de manera prolongada (como una aplicación web ASP.NET Core 2.0).

Guardar configuración en**`aws-docker-tools-defaults.json`**y configurar el proyecto para la implementación de la línea de comandos- Seleccione esta opción si desea poder implementar desde la línea de comandos. Use `dotnet ecs deploy` desde el directorio del proyecto para implementar y ejecute el comando `dotnet ecs publish` en el contenedor.

Página Launch Configuration

ECS Cluster (Clúster de ECS): elija el clúster que ejecutará la imagen de Docker. Puedecrear un clúster de ECSUtilizando laAWSConsola de administración.

Launch Type (Tipo de lanzamiento): elija EC2. Para utilizar el tipo de lanzamiento de Fargate, consulte Implementación de una aplicación de ASP.NET Core 2.0 en Amazon ECS (Fargate).

Página Service Configuration

Service (Servicio): seleccione uno de los servicios de la lista desplegable para implementar el contenedor en un servicio existente. O bien elija Create New (Crear nuevo) para crear un nuevo servicio. Los nombres de servicio deben ser únicos dentro de un clúster, pero puede tener servicios con el mismo nombre en varios clústeres dentro de una región o en varias regiones.

Number of Tasks (Número de tareas): el número de tareas que desea implementar y mantener en ejecución en el clúster. Cada tarea es una instancia de su contenedor.

Minimum Healthy Percent (Porcentaje mínimo en buen estado): el porcentaje de tareas que deben permanecer en estado `RUNNING` durante la implementación, redondeado al entero superior más próximo.

Maximum Percent (Porcentaje máximo): el porcentaje de tareas que deben permanecer en estado `RUNNING` o `PENDING` durante la implementación, redondeado al entero inferior más próximo.

Placement Templates (Plantillas de ubicación): seleccione una plantilla de ubicación de las tareas.

Cuando se lanza una tarea en un clúster, Amazon ECS debe determinar dónde ubicar la tarea en función de los requisitos especificados en la definición de tareas, tales como CPU y memoria. Del mismo modo, cuando se reduce la escala del número de tareas, Amazon ECS debe determinar qué tareas debe terminar.

La plantilla de ubicación controla el modo en que las tareas se lanzan en un clúster:

- AZ Balanced Spread (Distribución equilibrada AZ): distribuye las tareas en las zonas de disponibilidad y entre las instancias de contenedor dentro de cada zona de disponibilidad.
- AZ Balanced BinPack (Distribución equilibrada BinPack): distribuye las tareas en las zonas de disponibilidad y entre las instancias de contenedor con la menor memoria disponible.
- BinPack: distribuye las tareas en función de la cantidad mínima de CPU o memoria disponible.
- One Task Per Host (Una tarea por host): coloca como máximo una tarea del servicio en cada instancia de contenedor.

Para obtener más información, consulte Ubicación de tareas de Amazon ECS.

Página Application Load Balancer

Configure Application Load Balancer (Configurar balanceador de carga de la aplicación): seleccione esta opción para configurar un balanceador de carga de la aplicación.

Select IAM role for service (Seleccionar rol de IAM para servicio): seleccione un rol existente o elija Create New (Crear nuevo) para crear uno nuevo.

Load Balancer (Balanceador de carga): seleccione un balanceador de carga o elija Create New (Crear nuevo) y escriba el nombre de un nuevo balanceador de carga.

Listener Port (Puerto de escucha): seleccione un puerto de escucha existente o elija Create New (Crear nuevo) y escriba un número de puerto. El puerto predeterminado, `80`, es adecuado para la mayoría de las aplicaciones web.

Target Group (Grupo de destino): de forma predeterminada, el balanceador de carga envía las solicitudes a los destinos registrados mediante el protocolo y el puerto que ha especificado para el grupo de destino. Puede anular este puerto al registrar cada destino en el grupo de destino.

Path Pattern (Patrón de ruta): el balanceador de carga usará el direccionamiento basado en rutas. Acepte la opción / predeterminada o proporcione un patrón diferente. Los patrones de ruta distinguen entre mayúsculas y minúsculas, su longitud máxima es de 128 caracteres y contienen un conjunto específico de caracteres.

Health Check Path (Ruta de comprobación de estado): la ruta de ping que es el destino para los destinos en las comprobaciones de estado. De forma predeterminada, es / y es adecuado para las aplicaciones web. Especifique otra ruta si es necesario. Si la ruta que especifica no es válida, no se superará la comprobación de estado y se considerará que está en mal estado.

Si implementa varios servicios y cada servicio se implementa en una ruta o ubicación diferente, es posible que necesite rutas de comprobación personalizadas.

Página ECS Task Definition

Task Definition (Definición de tarea): seleccione una definición de tarea existente o elija Create New (Crear nueva) y escriba el nombre de una nueva definición de tarea.

Container (Contenedor): seleccione un contenedor existente o elija Create New (Crear nuevo) y escriba el nombre de un nuevo contenedor.

Memory (MiB) (Memoria (MiB): proporcione valores para Soft Limit (Límite flexible) o Hard Limit (Límite invariable) o para ambos.

El límite flexible (en MiB) de memoria que reservar para el contenedor. Docker intenta mantener la memoria del contenedor dentro del límite flexible. El contenedor puede consumir más memoria, hasta el el límite máximo especificado con el parámetro de memoria (si procede) o toda la memoria disponible en la instancia del contenedor, lo que ocurra primero.

El límite máximo (en MiB) de memoria a presentar al contenedor. Si su contenedor intenta superar la memoria especificada aquí, se cancela el contenedor.

Rol de tarea- Seleccione una tarea para un rol de IAM que conceda al contenedor permiso para llamar a laAWSAPIs especificadas en sus políticas asociadas en su nombre. Así es cómo se pasan las credenciales a la aplicación. ConsulteCómo especificarAWScredenciales de seguridad para su aplicación.

Port Mapping (Asignaciones de puerto): añada, modifique o elimine las asignaciones de puerto del contenedor. Si hay un balanceador de carga, el puerto de host estará establecido de forma predeterminada en 0 y la asignación de puertos será dinámica.

Environment Variables (Variables de entorno): añada, modifique o elimine las variables de entorno del contenedor.

Cuando esté satisfecho con la configuración, haga clic en Publish (Publicar) para iniciar el proceso de implementación.

Publicación de un contenedor enAWS

Los eventos se muestran durante la implementación. El asistente se cierra automáticamente una vez completado correctamente. Puede invalidarlo desactivando la casilla situada en la parte inferior de la página.

Puede encontrar la dirección URL de sus nuevas instancias en laAWSExplorador. Expanda Amazon ECS and Clusters y haga clic en su clúster.

Solución de problemas del AWS Toolkit for Visual Studio

Las siguientes secciones contienen información general sobre la solución de problemas relacionados con los AWS servicios del kit de herramientas AWS Toolkit for Visual Studio y cómo trabajar con ellos.

> **Note**
>
> La información set-up-specific de instalación y solución de problemas está disponible en el tema Solución de problemas de instalación, que se encuentra en esta Guía del usuario.

Temas

Solución de problemas y prácticas recomendadas

A continuación, se recomiendan las prácticas recomendadas para solucionar AWS Toolkit for Visual Studio problemas.

- Intente recrear el problema o error antes de enviar un informe.
- Tome notas detalladas de cada paso, configuración y mensaje de error durante el proceso de recreación.
- Recopile los registros del AWS kit de herramientas. Para obtener una descripción detallada de cómo localizar los registros del AWS kit de herramientas, consulte el procedimiento Cómo localizar los AWS registros, que se encuentra en este tema de la guía.
- Compruebe si hay solicitudes abiertas o soluciones conocidas, o bien notifique el problema no resuelto en la sección AWS Toolkit for Visual Studio Problemas del AWS Toolkit for Visual Studio GitHub repositorio.

¿Cómo localizar los registros del kit de AWS herramientas?

1. En el menú principal de Visual Studio, expanda Extensiones.

2. Elija el kit de AWS herramientas para expandir el menú del kit de AWS herramientas y, a continuación, elija Ver los registros del kit de herramientas.
3. Cuando se abra la carpeta de registros del AWS kit de herramientas en su sistema operativo, clasifique los archivos por fecha y busque cualquier archivo de registro que contenga información relevante sobre su problema actual.

Visualización y filtrado de escaneos de seguridad de Amazon Q

Para ver sus escaneos de seguridad de Amazon Q en Visual Studio, abra la Lista de errores de Visual Studio expandiendo el encabezado Ver en el menú principal de Visual Studio y seleccionando Lista de errores.

De forma predeterminada, la lista de errores de Visual Studio muestra todas las advertencias y errores de su base de código. Para filtrar los resultados del análisis de seguridad de Amazon Q de la lista de errores de Visual Studio, cree un filtro siguiendo este procedimiento.

> **Note**
>
> Los resultados del análisis de seguridad de Amazon Q solo son visibles después de ejecutar el análisis de seguridad y detectar problemas.
> Los resultados del análisis de seguridad de Amazon Q aparecen como advertencias en Visual Studio. Para ver los resultados de los escaneos de seguridad de Amazon Q de tu lista de errores, debes seleccionar la opción Advertencias en el encabezado de la lista de errores.

1. En el menú principal de Visual Studio, expanda el encabezado Ver y elija Lista de errores para abrir el panel Lista de errores.
2. En el panel Lista de errores, haga clic con el botón derecho en la fila del encabezado para abrir el menú contextual.
3. En el menú contextual, expanda Mostrar columnas y, a continuación, seleccione Herramienta en el menú expandido.
4. La columna Herramienta se añade a la lista de errores.
5. En el encabezado de la columna Herramienta, selecciona el icono de filtro y elige Amazon Q para filtrar los resultados de los escaneos de seguridad de Amazon Q.

Seguridad para AWS Toolkit for Visual Studio

La seguridad en la nube de Amazon Web Services (AWS) es la máxima prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes. La seguridad es una responsabilidad compartida entre usted AWS y usted. En el modelo de responsabilidad compartida, se habla de “seguridad de la nube” y “seguridad en la nube”:

Seguridad de la nube: AWS se encarga de proteger la infraestructura en la que se ejecutan todos los servicios que se ofrecen en la AWS nube y de proporcionarle servicios que pueda utilizar de forma segura. Nuestra responsabilidad en materia de seguridad es nuestra máxima prioridad AWS, y auditores externos comprueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los programas de AWS conformidad.

Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice y otros factores, como la confidencialidad de sus datos, los requisitos de su organización y las leyes y reglamentos aplicables.

Este AWS producto o servicio sigue el modelo de responsabilidad compartida a través de los servicios específicos de Amazon Web Services (AWS) a los que da soporte. Para obtener información sobre la seguridad de los AWS servicios, consulte la página de documentación sobre la seguridad del AWS servicio y AWS los servicios que se encuentran dentro del ámbito de aplicación de AWS las medidas de conformidad establecidas por el programa de conformidad.

Temas

Protección de datos en AWS Toolkit for Visual Studio

El modelo de se aplica a protección de datos en AWS Toolkit for Visual Studio. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan

todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Toolkit for Visual Studio u Servicios de AWS otro tipo de herramientas mediante la consola, la API AWS CLI AWS o los SDK. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Identity and Access Management

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice. AWS

Usuario del servicio: si Servicios de AWS solía hacer su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una función de AWS, consulte Solución de problemas de AWS identidad y acceso o consulte la guía del usuario de la Servicio de AWS que está utilizando.

Administrador de servicios: si está a cargo de AWS los recursos de su empresa, probablemente tenga acceso total a ellos AWS. Su trabajo consiste en determinar a qué AWS funciones y recursos deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM AWS, consulte la guía del usuario del Servicio de AWS que está utilizando.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS. Para ver ejemplos de políticas AWS

basadas en la identidad que puede utilizar en IAM, consulte la guía del usuario de la Servicio de AWS que está utilizando.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren

que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales.

Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.

- Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una

solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico.

Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de

Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo Servicios de AWS trabajar con IAM

Para obtener una visión general de cómo Servicios de AWS trabajar con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Para obtener información sobre cómo utilizar una función específica Servicio de AWS con IAM, consulte la sección de seguridad de la guía del usuario del servicio correspondiente.

Solución de problemas de AWS identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con un AWS IAM.

Temas

- No estoy autorizado a realizar ninguna acción en AWS
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS recursos

No estoy autorizado a realizar ninguna acción en AWS

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `awes:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 awes:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `awes:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS recursos

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que

asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si AWS es compatible con estas funciones, consulte¿Cómo Servicios de AWS trabajar con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información acerca del uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Validación de la conformidad de este AWS producto o servicio

Para saber si un programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.

- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: este documento técnico describe cómo las empresas pueden crear aplicaciones aptas para AWS la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Este AWS producto o servicio sigue el modelo de responsabilidad compartida a través de los servicios específicos de Amazon Web Services (AWS) a los que da soporte. Para obtener información sobre la seguridad de los AWS servicios, consulte la página de documentación sobre la

seguridad del AWS servicio y AWS los servicios que se encuentran dentro del ámbito de aplicación de AWS las medidas de conformidad establecidas por el programa de conformidad.

Resiliencia de este AWS producto o servicio

La infraestructura AWS global se basa en Regiones de AWS zonas de disponibilidad.

Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia.

Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS

Este AWS producto o servicio sigue el modelo de responsabilidad compartida a través de los servicios específicos de Amazon Web Services (AWS) a los que da soporte. Para obtener información sobre la seguridad de los AWS servicios, consulte la página de documentación sobre la seguridad del AWS servicio y AWS los servicios que se encuentran dentro del ámbito de aplicación de AWS las medidas de conformidad establecidas por el programa de conformidad.

Seguridad de la infraestructura para este AWS producto o servicio

Este AWS producto o servicio utiliza servicios gestionados y, por lo tanto, está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a este AWS producto o servicio a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Este AWS producto o servicio sigue el modelo de responsabilidad compartida a través de los servicios específicos de Amazon Web Services (AWS) a los que da soporte. Para obtener información sobre la seguridad de los AWS servicios, consulte la página de documentación sobre la seguridad del AWS servicio y AWS los servicios que se encuentran dentro del ámbito de aplicación de AWS las medidas de conformidad establecidas por el programa de conformidad.

Análisis de configuración y vulnerabilidad en AWS Toolkit for Visual Studio

El Kit de herramientas para Visual Studio se publica en Visual Studio Marketplace a medida que se desarrollan nuevas características o correcciones. Estas actualizaciones a veces incluyen actualizaciones de seguridad, por lo que es importante mantener el Kit de herramientas para Visual Studio al día.

Para comprobar que las actualizaciones automáticas de las extensiones estén habilitadas:

1. Abra el administrador de extensiones seleccionando Herramientas, Extensiones y actualizaciones (Visual Studio 2017) o Extensiones, Administrar extensiones (Visual Studio 2019).
2. Seleccione Cambiar la configuración de extensiones y actualizaciones (Visual Studio 2017) o Cambiar la configuración de extensiones (Visual Studio 2019).
3. Ajuste la configuración de su entorno.

Si decide deshabilitar las actualizaciones automáticas de extensiones, asegúrese de comprobar si hay actualizaciones del Kit de herramientas para Visual Studio cada cierto tiempo, según precise su entorno.

Historial documental de la Guía AWS Toolkit for Visual Studio del usuario

Última actualización de la documentación: 21 de abril de 2021

Historial de documentos

En la siguiente tabla se describen los cambios recientes importantes de la Guía del AWS Toolkit for Visual Studio usuario. Para obtener notificaciones sobre las actualizaciones de esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Actualizaciones y mantenimiento del contenido	Actualización del contenido para adaptarlo a los cambios en la interfaz de usuario y en las directrices de AWS estilo.	6 de marzo de 2024
Actualizaciones y mantenimiento del contenido	Actualización del contenido para adaptarlo a los cambios en la interfaz de usuario y en las directrices de AWS estilo.	6 de marzo de 2024
Actualizaciones y mantenimiento del contenido	Actualización del contenido para adaptarlo a los cambios en la interfaz de usuario y en las directrices de AWS estilo.	6 de marzo de 2024
Actualizaciones y mantenimiento del contenido	Actualización del contenido para adaptarlo a los cambios en la interfaz de usuario y en las directrices de AWS estilo.	6 de marzo de 2024
Actualizaciones y mantenimiento del contenido	Actualización del contenido para adaptarlo a los cambios en la interfaz de usuario y en las directrices de AWS estilo.	6 de marzo de 2024

Actualizaciones de configuración y autenticación	Se han actualizado los temas de configuración y autenticación para mejorar la seguridad y la experiencia de incorporación del kit de herramientas. Consulte las tablas de contenidos de los temas Introducción y Autenticación y acceso para ver los cambios.	22 de junio de 2023
Autenticación y acceso	Proporcionar AWS credenciales ahora es autenticación y acceso. Refactorizar el TOC y los subtemas para cumplir con los requisitos de AWS estilo y seguridad.	4 de mayo de 2023
Actualizaciones de las secciones y temas de configuración	Se han actualizado las secciones y temas de Configuración del AWS Toolkit for Visual Studio de esta Guía del usuario para mejorar la experiencia de incorporación del AWS Toolkit for Visual Studio.	30 de enero de 2023
Actualizaciones de las secciones y temas de configuración	Se han actualizado las secciones y temas de Configuración del AWS Toolkit for Visual Studio de esta Guía del usuario para mejorar la experiencia de incorporación del AWS Toolkit for Visual Studio.	30 de enero de 2023

Se AWS Toolkit for Visual Studio agregó información de 2022	Se agregó soporte para Visual Studio 2022 a AWS Toolkit for Visual Studio.	20 de diciembre de 2022
Actualizaciones de la AWS guía Publicar para	La actualización de la documentación refleja los cambios efectuados en el servicio para el lanzamiento en GA.	6 de julio de 2022
Actualizaciones en el título y reubicación	Se han llevado a cabo pequeños cambios en el título para reflejar mejor el contenido. La guía ahora se encuentra en la AWS guía Publicar para.	6 de julio de 2022
Implementación para AWS: actualizaciones de títulos y contenido	La sección de la guía, titulada formalmente: Implement ación mediante el AWS kit de herramientas, tiene una tabla de contenido (TOC) actualizada y ahora se titula: Implementación en. AWS Las siguientes guías han dejado de estar en desuso y ya no están disponibles: Implement ación en Elastic Beanstalk (Legacy) e Implementación en (Legacy). AWS CloudForm ation El contenido actualizado sobre la implementación en Elastic Beanstalk y Cloudform ation se encuentra en la tabla de contenido (TOC) actualiza da de esta guía.	6 de julio de 2022

Ahora, Implementación de una aplicación de ASP.NET Core 2.0 en ECS (Fargate) es una guía heredada	Esta documentación hace referencia a servicios y características heredados . Para obtener guías y contenido actualizados, consulte la guía de herramientas de implementación de .NET para AWS y la Tabla de contenido actualizada de Implementación en AWS.	6 de julio de 2022
Ahora, Implementación de una aplicación ASP.NET (.NET Core) es una guía heredada	Esta documentación hace referencia a servicios y características heredados . Para obtener guías y contenido actualizados, consulte la guía de herramientas de implementación de .NET para AWS y la Tabla de contenido actualizada de Implementación en AWS.	6 de julio de 2022
Ahora, Implementación de una aplicación ASP.NET (.NET Core) es una guía heredada	Esta documentación hace referencia a servicios y características heredados . Para obtener guías y contenido actualizados, consulte la guía de herramientas de implementación de .NET para AWS y la Tabla de contenido actualizada de Implementación en AWS.	6 de julio de 2022

Nuevo tema de la guía: Trabajar con CloudWatch registros en Visual Studio	Se creó un nuevo tema de información general para la guía de integración de Amazon CloudWatch Logs en Visual Studio.	29 de junio de 2022
Nuevo tema de la guía: Configuración de la integración de CloudWatch Logs para Visual Studio	Se creó una nueva sección de configuración para la guía de integración de Amazon CloudWatch Logs en Visual Studio.	29 de junio de 2022
CloudWatch Integración de registros para Visual Studio	Se creó una nueva guía para la integración de Amazon CloudWatch Logs en Visual Studio, que incluye los temas de la guía: Configuración de CloudWatch registros para Visual Studio y Trabajo con CloudWatch registros en Visual Studio.	29 de junio de 2022
Publica en AWS	Publicar en ya no AWS está en la vista previa. Se actualiza para reflejar los cambios en la interfaz de usuario y las mejoras en las sugerencias de publicación.	1 de junio de 2022
La nueva versión Publicar en AWS está disponible para su vista previa	Experiencia de implement ación mejorada que proporcio na orientación sobre qué AWS servicio es el adecuado para su aplicación.	21 de octubre de 2021

Soporte de SSO y MFA para credenciales AWS	Se actualizó para documenta r la nueva compatibilidad con el inicio de sesión AWS único (IAM Identity Center) y la autenticación multifactorial en las credenciales. AWS	21 de abril de 2021
Proyecto básico AWS Lambda : creación de una imagen de Docker	Se ha añadido compatibilidad con imágenes del contenedor de Lambda.	1 de diciembre de 2020
Contenido de seguridad	Se ha añadido contenido de seguridad.	6 de febrero de 2020
Proporcionar credenciales AWS	Se ha actualizado con información sobre la creación de perfiles de credenciales en el archivo compartido credentials de AWS .	20 de junio de 2019
Uso del proyecto AWS Lambda en el AWS kit de herramientas para Visual Studio	Se agregó soporte para Visual Studio 2019 al AWS Toolkit for Visual Studio.	28 de marzo de 2019
Tutorial: creación de una aplicación de Lambda con Amazon Rekognition	Se agregó soporte para Visual Studio 2019 al AWS Toolkit for Visual Studio.	28 de marzo de 2019
Tutorial: Creación y prueba de una aplicación sin servidor con Lambda AWS	Se agregó soporte para Visual Studio 2019 al AWS Toolkit for Visual Studio.	28 de marzo de 2019
Configuración del AWS Toolkit for Visual Studio	Se agregó soporte para Visual Studio 2019 a AWS Toolkit for Visual Studio.	28 de marzo de 2019

Implementación de una aplicación de ASP.NET Core 2.0 (Fargate)	Se agregó soporte para Visual Studio 2019 al AWS Toolkit for Visual Studio.	28 de marzo de 2019
Implementación de una aplicación de ASP.NET Core 2.0 (EC2)	Se agregó soporte para Visual Studio 2019 al AWS Toolkit for Visual Studio.	28 de marzo de 2019
Creación de un proyecto AWS CloudFormation de plantilla en Visual Studio	Se agregó soporte para Visual Studio 2019 al AWS Toolkit for Visual Studio.	28 de marzo de 2019
Vistas detalladas de Container Service	Se agregó información sobre las vistas detalladas de los clústeres y repositorios de contenedores de Amazon Elastic Container Service que proporciona AWS Explorer.	16 de febrero de 2018
Implementación en Amazon EC2 Container Service	Se ha agregado informaci ón sobre la implementación en Amazon EC2 Container Service.	16 de febrero de 2018
Implementación de Container Service mediante Fargate	Se agregó información sobre cómo implementar una aplicación ASP.NET Core 2.0 en contenedor dirigida a Linux a través de Amazon ECS utilizando el tipo de lanzamien to Fargate.	16 de febrero de 2018

Implementación de Container Service mediante EC2	Se ha añadido información sobre cómo implementar una aplicación ASP.NET Core 2.0 en contenedores dirigida a Linux a través de Amazon ECS mediante el tipo de lanzamiento de EC2.	16 de febrero de 2018
Credenciales para implementar en Amazon EC2 Container Service	Se ha agregado información acerca de cómo especificar credenciales al implementar en Amazon EC2 Container Service.	16 de febrero de 2018

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.